Оглавление

[Введение 2](#_Toc139904058)

[Связи MikroTik с инфраструктурными системами 3](#_Toc139904059)

[Ansible 3](#_Toc139904060)

[Dude 3](#_Toc139904061)

[Oxidized 3](#_Toc139904062)

[CAPsMAN 3](#_Toc139904063)

[RADIUS 3](#_Toc139904064)

[ELK 4](#_Toc139904065)

[Роли MikroTik в инфраструктуре ОРС 5](#_Toc139904066)

[Маршрутизаторы для магазинов 5](#_Toc139904067)

[Точки доступа для ТСД в магазинах 5](#_Toc139904068)

[Маршрутизаторы для сотрудников КРГ 6](#_Toc139904069)

[Прочие роли 6](#_Toc139904070)

[Инструкции 7](#_Toc139904071)

[Первичная настройка MikroTik для магазина 7](#_Toc139904072)

[Донастройка MikroTik 11](#_Toc139904073)

[MikroTik в качестве точки доступа 13](#_Toc139904074)

[MikroTik для КРГ 14](#_Toc139904075)

[PPPoE MikroTik 15](#_Toc139904076)

[Dude сканирование подсети 18](#_Toc139904077)

[Актуализация данных в Oxidized 28](#_Toc139904078)

# Введение

В основной части глав данного документа описана концепция работы системы и основные её направления. В разделе «Инструкции» представлены инструкции к решению типовых задач по настройке.

Сетевые устройства MikroTik в инфраструктуре ОРС «Читай-Город» выступают в качестве:

- Маршрутизаторов для магазинов;

- Точек доступа для ТСД в магазинах;

- Маршрутизаторов для сотрудников КРГ;

- Корневых маршрутизаторов в филиалах офисов и ДЦ;

- Маршрутизаторов под нетиповые задачи в рамках инфраструктурных ИТ проектов.

# Связи MikroTik с инфраструктурными системами

## Ansible

Для осуществления централизованного управления маршрутизаторами MikroTik используется Ansible. Поскольку данная система используется не только для управления роутерами, описание работы с ней в контексте маршрутизаторов MikroTik находится в соответствующем разделе документации по Ansible. Для работы системы на маршрутизаторах создан пользователь awxadmin с полными правами. Доступ осуществляется по ключу. Данные для доступа к системе находятся в файле access\_data.

## Dude

В данном случае Dude используется для сканирования подсети магазинов на наличие новых маршрутизаторов MikroTik и добавления их в Oxidized. Dude сервер можно развернуть на любом маршрутизаторе MikroTik, поддерживающем подключение внешних накопителей. Инструкция - «Dude сканирование подсети».

## Oxidized

Для осуществления резервного копирования и отслеживания изменения конфигураций маршрутизаторов используется Oxidized. Для работы системы на маршрутизаторах создан пользователь «Ansible» с правами на чтение. Доступ осуществляется по ключу. Инструкция - «Актуализация данных в Oxidized». Авторизация для веб-интерфейса реализована с помощью Nginx в качестве реверс-прокси. Данные для доступа к системе находятся в файле access\_data.

## CAPsMAN

CAPsMAN решает проблему нехватки IP адресов для ТСД в магазинах. Он не требует систематического внесения изменений в конфигурацию и рассчитан на автономную работу. Развернут на CCR, данные для доступа к системе находятся в файле access\_data.

## RADIUS

На маршрутизаторах MikroTik, выступающих в качестве основных маршрутизаторов магазинов, включена доменная авторизация пользователей через RADIUS сервер. Актуализация RADIUS клиентов выполняется сервисом актуализации Zabbix. RADIUS сервер развернут на Windows Server, данные для доступа находятся в файле access\_data.

## ELK

Маршрутизаторы MikroTik отправляют логи об авторизации пользователей на сервер с ELK. Сервис развернут на Ubuntu Server, данные для доступа находятся в файле access\_data.

# Роли MikroTik в инфраструктуре ОРС

## Маршрутизаторы для магазинов

В этой роли роутеры MikroTik выступают основными маршрутизаторами в магазинах сети.

Настройка маршрутизаторов для магазинов выполняется в 2 этапа:

- Первичная настройка;

- Донастройка после наладки хотя бы одного интернет-канала в магазине.

Сделано это для упрощения настройки маршрутизаторов в магазине силами подрядчика при неверно выданных настройках интернет-каналов или прочих проблемах с каналом. Первичная настройка используется при отправке роутера в новый магазин или замене сгоревшего роутера в уже открытом магазине.

Донастройка используется, когда роутер уже стабильно работает и не предполагается изменений конфигурации силами подрядчика или сотрудников магазина. В ходе этой процедуры устанавливается единый пароль администратора, неизвестный техподдержке. Сотрудники техподдержки авторизуются под доменными учетными записями. Суммарно донастройка включает в себя:

- Обновление линии ROS на long term;

- Смену схемы маршрутизации на рекурсивную;

- Загрузку открытого ключа на маршрутизатор и создание пользователя для Ansible;

- Настройку доменной авторизации;

- Настройку отправки логов в ELK;

- Смену пароля администратора.

Инструкции по первичной настройке и донастройке находятся в разделе «Инструкции» данного документа.

## Точки доступа для ТСД в магазинах

Точками доступа могут выступать непосредственно точки доступа MikroTik (в магазинах Москвы и области), в таком случае как правило реализуется полное либо почти полное покрытие магазина Wi-Fi. Также точками доступа могут служить маршрутизаторы по типу hAP Lite, они покрывают небольшую область магазина.

Точки доступа работают с CAPsMAN, развернутым на CCR в ДЦ. В настройке есть единственный нюанс – если используется устройство мощнее hAP Lite, identity устройства необходимо начинать с «24\_», если же используется hAP Lite – с «hAP\_». Связано это с тем, что в некоторые hAP Lite зашит только 1 профиль страны (russia3), что не даст ему подключиться к интерфейсу CAPsMAN с identity «24\_». Это можно исправить только перепрошивкой hAP Lite с помощью Netinstall, т.к. ему не хватит памяти загрузить прошивку и обновиться на горячую. Поэтому под такие роутеры создан отдельный профиль с Identity «hAP\_».

Инструкция по настройке в разделе «Инструкции» - «Настройка точек доступа MikroTik».

## Маршрутизаторы для сотрудников КРГ

Роутеры MikroTik используются сотрудниками контрольно-ревизионной группы при проведении масштабных инвентаризаций в магазинах. С технической точки зрения это самая простая конфигурация из представленных в этом документе, но есть 2 **важные** особенности:

- Пароль администратора и Wi-Fi на роутере должен иметь значение «Password123»;

- Версия ROS маршрутизатора должна быть не выше 6.44.6.

Связано это с тем, что сотрудники КРГ используют маршрутизаторы следующим образом: приходят в магазин, отключают от сети один из ПК и вставляют на его место свой маршрутизатор, при этом в маршрутизаторе прописывается адрес этого ПК.

Поскольку сотрудники КРГ - не специалисты в плане взаимодействия с сетевым оборудованием, для них было разработано десктопное приложение, в которое они прописывают нужные настройки. Поэтому в некоторых случаях может потребоваться даунгрейд версии RouterOS. Инструкция по настройке в разделе «Инструкции».

## Прочие роли

Корневые маршрутизаторы в филиалах офисов и ДЦ и маршрутизаторы под нетиповые задачи в рамках инфраструктурных ИТ проектов настраиваются индивидуально под задачу, поэтому нет смысла описывать их настройку в инструкции. Но настоятельно рекомендуется ознакомиться с их конфигурацией. Сделать это можно экспортом настроек в терминале WinBox или подключившись к маршрутизатору по ssh. Адреса и логины/пароли в файле «access\_data»

# Инструкции

## Первичная настройка MikroTik для магазина

Для настройки удобнее всего использовать WinBox (https://mt.lv/winbox64).

1) Сброс роутера:

- Отключить кабель питания, если он подключен;

- Зажать кнопку RES на передней панели роутера;

Изображение выглядит как текст, электроника

Автоматически созданное описание

- С зажатой кнопкой RES подключить кабель питания;

- Дождаться пока индикатор PWR не начнет мигать, после чего отпустить кнопку.

На данном этапе роутер сброшен на дефолтную конфигурацию, необходимо сбросить его полностью. Для этого нужно:

- Подключить роутер 2 портом напрямую к ПК;

- Открыть WinBox, во вкладке Neighbors должен отобразиться роутер:

Изображение выглядит как текст, снимок экрана, линия, число

Автоматически созданное описание

- Нажать по мак адресу роутера, затем нажать кнопку Connect. Если роутер сброшен корректно, зайти можно под пользователем admin без пароля

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

- В появившемся окне «RouterOS Default Configuration» нажать «OK», затем перейти в System -> Reset Configuration, в открывшемся окне поставить две нижние галки, нажать «Reset Configuration» и «Yes» в окне подтверждения

Изображение выглядит как текст, снимок экрана, дисплей, программное обеспечение

Автоматически созданное описание

Роутер полностью сброшен, зайти на него можно вышеописанным образом.

2) Настройка роутера:

Для удобства настройки роутера используется скрипт 2wan-v1.5.rsc.

- Открыть файл скрипта блокнотом и подставить свои значения в переменные в соответствии с их описанием (если часть данных, например настройки одного из каналов, неизвестна, нужно оставить значения по умолчанию):

# w1addr - адрес первого канала вида 1.1.1.2/30

# w1gate - шлюз первого канала вида 1.1.1.1

# w1srcnat - адрес первого канала вида 1.1.1.2

# w2addr - адрес второго канала вида 2.2.2.2/30

# w2gate - шлюз второго провайдера вида 2.2.2.1

# w2srcnat - адрес второго канала вида 2.2.2.2

# l1addr - локальный адрес роутера вида 172.16.100.1/28

# l1net - локальная подсеть вида 172.16.100.0/28

# bcnet - локальная сеть офиса

# secret - Preshared Key

# ident - название магазина

# pswd - пароль роутера

- Сохранить файл и скопировать всё его содержимое (Ctrl + A);

- Зайти на роутер с помощью WinBox;

- Перейти в System -> Scripts, нажать «+», откроется окно нового скрипта, в поле «Source» вставить скопированное ранее содержимое файла;

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

- В этом же окне нового скрипта нажать по очереди «Apply» и «Run Script». Если значения введены корректно, через несколько секунд название роутера сменится на то, что было указано в скрипте. Если это произошло – роутер настроен правильно и готов к отправке в магазин. В противном случае необходимо сбросить его повторно и найти ошибку во введенных значениях

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание

## Донастройка MikroTik

Предполагается, что маршрутизатор приведён к конфигурации по инструкции «Первичная настройка MikroTik для магазина»

1) Обновление линии ROS на long term:

- Предупредить сотрудников о прошивке роутера, чтобы они его **не перезагрузили**. В противном случае потребуется трудновыполнимая в рамках магазина процедура восстановления;

- Перейти в System -> Packages, нажать «Check for Updates»;

- В окне «Check for Updates» в «Channel» выбрать «long term» и нажать кнопку «Check for Updates», после появления информации об обновлении появится кнопка «Download&Install», нажать её. После нажатия запустится скачивание и обновление роутера;

Изображение выглядит как текст, электроника, снимок экрана, дисплей

Автоматически созданное описание

Если информация об обновлении не появилась после «Check for Updates», возможно есть проблемы с резолвом доменных имен. Канал обязательно нужно выбирать «long term», прочие версии работают нестабильно.

2) Смена схемы маршрутизации на рекурсивную:

- Активировать «**Safe Mode**»

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание

- Определить типы получений настроек каналов связи: статика, DHCP или PPPoE.

- Нижеописанные скрипты выполняются тем же образом, что и в «Первичной настройке» (копированием тела скрипта в новый скрипт в System -> Scripts с последующим его исполнением через «Apply» и «Run script» )

- Исходя из типов каналов выполнить нужные скрипты из секции «Recursive Routing» в файле «finish\_tuning.txt»:

--- Если оба провайдера выдают настройки статикой (ip адрес, маска, шлюз), нужно выполнить только скрипт «Static WAN1/WAN2»;

--- Если один из провайдеров выдает настройки по DHCP, необходимо сначала выполнить скрипт «Static WAN1/WAN2», затем один из скриптов «DHCP WAN1 / Static WAN2» или «DHCP WAN2 / Static WAN1» в зависимости от того, какой провайдер выдает настройки по DHCP;

--- Если один из провайдеров использует PPPoE, нужно выполнить только скрипт «PPPoE» без выполнения скрипта «Static WAN1/WAN2»;

3) Загрузка открытого ключа, создание пользователя для Ansible, настройка доменной авторизации и отправки логов в ELK, смена админского пароля:

- Поместить открытый ключ «awxkey.pub» в память роутера, сделать это можно перетянув файл ключа из папки или с рабочего стола в окно WinBox;

- Выполнить блок скрипты «Ansible users», «RADIUS» и «ELK», эти скрипты можно выполнять одним блоком;

- Если всё прошло успешно – отключить «**Safe Mode**», роутер донастроен;

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание

- При возникновении каких-либо **ошибок** можно закрыть WinBox, подтвердив выход нажатием «Yes». В таком случае «Safe Mode» откатит маршрутизатор на те настройки, что были до его активации. **Дебажить** скрипты можно вводя команды непосредственно в консоль по очереди (вкладка New Terminal).

## MikroTik в качестве точки доступа

1) Сброс устройства:

Для настройки любого устройства MikroTik в качестве точки доступа необходимо полностью сбросить его как в инструкции «Первичная настройка MikroTik для магазина».

2) Настройка:

- Заменить значения переменных в файле «AP.rsc» своими

# localAddress - адрес точки вида 172.16.100.2/28

# localGate - внутренний адрес роутера вида 172.16.100.1

# pswd - пароль точки

# ident - имя точки в формате 24\_pidМагазина\_AP или hAP\_pidМагазина\_AP в зависимости от устройства. В случае использования hAP Lite нужно выбрать второй вариант, в противном случае – первый.

- Сохранить и залить скрипт через System -> Scripts аналогичным как в инструкции «Первичная настройка MikroTik для магазина» образом;

- При корректном подключении к CAPsMAN в разделе «Wireless» появляется информация о сети;

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

- Если подключиться не удается – информации нет, нужно искать причину.

Изображение выглядит как текст, снимок экрана, дисплей, Шрифт

Автоматически созданное описание

## MikroTik для КРГ

1) Сброс устройства:

Для настройки любого устройства MikroTik в качестве точки доступа необходимо полностью сбросить его как в инструкции «Первичная настройка MikroTik для магазина».

2) Настройка:

- Выполнить скрипт «KRG.rsc» через System -> Scripts аналогичным как в инструкции «Первичная настройка MikroTik для магазина» образом. Данный скрипт универсален и не требует изменения каких-либо значений.

## PPPoE MikroTik

Все действия данной инструкции нужно выполнять с активированным «**Safe Mode**» во избежание потери управления маршрутизатором

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание

1) Настройка PPPoE клиента:

- Interfaces -> «+» -> PPPoE Client;

- В появившемся клиенте необходимо во вкладке «General»указать интерфейс, к которому подключен канал, имя клиента не менять;  
Изображение выглядит как текст, снимок экрана, дисплей, число

Автоматически созданное описание

- Во вкладке «Dial Out» нужно ввести настройки, выданные провайдером (имя пользователя и пароль), профиль оставить «default», выставить все галки в блоке «Allow», убрать галки с «Dial On Demand»и «Add Default Route»;

Изображение выглядит как текст, снимок экрана, дисплей, число

Автоматически созданное описание

- В IP -> Firewall -> NAT выбрать запись нужного интерфейса, открыть её. Во вкладке «General» в параметре «Out Interface» указать созданный PPPoE-клиент;

Изображение выглядит как текст, снимок экрана, число, дисплей

Автоматически созданное описание

- Во вкладке «Action» в параметре «Action» указать «Masquerade»;

Изображение выглядит как текст, снимок экрана, дисплей, число

Автоматически созданное описание

- Открыть терминал через «New Terminal» в левой колонке и по очереди выполнить команды:

/ppp profile add change-tcp-mss=no name=PPPoE remote-address=10.253.252.251 use-upnp=no

/interface pppoe-client set pppoe-out1 dial-on-demand=no add-default-route=no profile=PPPoE

- Если канал поднялся и не отваливается в течение 2-3 минут, можно выйти из «Safe Mode», настройка завершена.

## Dude сканирование подсети

1) Подготовка роутера:

- Найти MirkoTik, в котором предусмотрена возможность подключения внешних накопителей (sd карты или флешки);

- В выключенный роутер вставить накопитель, включить;

- Настроить роутер по инструкции «Первичная настройка MikroTik для магазина»;

- Подключить роутер 1 портом к сети офиса, зайти на него через WinBox;

- Перейти в IP -> DHCP Client -> +, в новом клиенте выбрать «WAN1» и нажать OK, маршрутизатор должен получить адрес;

Изображение выглядит как текст, снимок экрана, дисплей, программное обеспечение

Автоматически созданное описание

- Перейти в IP -> Firewall -> NAT, открыть строку с WAN1, во вкладке «Action» параметр «Action» заменить на «masquerade», нажать OK;

Изображение выглядит как текст, снимок экрана, дисплей, программное обеспечение

Автоматически созданное описание

- Теперь с маршрутизатора должны пинговаться устройства из внутренней сети:

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

- Перейти в System -> Disks, там должен отобразиться вставленный накопитель;

Изображение выглядит как снимок экрана, текст, линия, График

Автоматически созданное описание

- Выбрать накопитель и нажать «Eject Drive», затем «Format Drive», в «File System» указать «ext3», нажать «Start» и дождаться окончания форматирования;

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

- После завершения форматирования должна отобразиться информация о новом диске.

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Автоматически созданное описание

2) Установка Dude:

- Необходимо обновить маршрутизатор до последней Long Term прошивки (инструкция по обновлению есть в инструкции «Донастройка MikroTik»);

- Перейти в System -> Resources, найти значения «Architecture Name» и «Version»;

Изображение выглядит как текст, снимок экрана, число, дисплей

Автоматически созданное описание

- Перейти на загрузочную страницу MikroTik Software (<https://mikrotik.com/download>), там необходимо найти версию RouterOS (в примере этой инструкции это 6.48.7 Long-term) и свою архитектуру процессора (в данном примере mmips) исходя из значений, которые отображены в System -> Resources. Необходимо скачать «Extra packages» для нужной версии ROS и архитектуры, а также Dude клиент, который находится в секции «General»

Изображение выглядит как текст, снимок экрана, число, программное обеспечение

Автоматически созданное описание

Изображение выглядит как текст, снимок экрана, число, Шрифт

Автоматически созданное описание

- Dude клиент и сервер должны быть одной версии;



- Dude клиент (файл .exe) можно запустить, он установится как обычное приложение;

- Из скачанного архива «all\_packages» необходимо достать «dude … .npk» и переместить его в память маршрутизатора через WinBox (можно просто перетянуть файл с рабочего стола в область WinBox);

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

- Перезагрузить роутер через System -> Reboot, пакет будет установлен и в панели слева появится вкладка «Dude»;

Изображение выглядит как текст, снимок экрана, число, Шрифт

Автоматически созданное описание

- Перейти в Dude -> Settings, поставить галку «Enabled», в «Data Directory» указать путь до папки в формате «/disk1/dude» (при необходимости заменить disk1 на свой диск)и нажать «Apply»;

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание

- Через несколько секунд/минут в зависимости от мощности роутера статус должен смениться на «Running», а на диске должно появиться множество файлов, это значит, что Dude сервер готов к работе.

Изображение выглядит как текст, электроника, снимок экрана, дисплей

Автоматически созданное описание

3) Сканирование подсети:

- Открыть установленный Dude клиент, в параметре «Server» указать адрес роутера, порт оставить по умолчанию, имя пользователя и пароль также ввести от роутера, нажать «Connect»;

Изображение выглядит как текст, линия, снимок экрана, Шрифт

Автоматически созданное описание

- Если всё введено верно, откроется окно Dude;

Изображение выглядит как текст, снимок экрана, число, дисплей

Автоматически созданное описание

- Для начала сканирования необходимо нажать «Discover». Сканировать можно любые подсети на предмет любых сетевых устройств, в данном примере сканируем подсеть магазинов на предмет сетевых устройств MikroTik. Для этого в параметре «Scan Networks» указываем «172.16.0.0/16»

Изображение выглядит как текст, снимок экрана, дисплей, число

Автоматически созданное описание

- Во вкладке «Services» оставить только mikrotik, ping и routeros management;

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

- В «Device Types» оставить только MikroTik Device и RouterOS;

Изображение выглядит как текст, снимок экрана, число, Шрифт

Автоматически созданное описание

- Нажать «Discover», начнется сканирование. За его прогрессом можно следить в строке снизу. Сначала появляется все подряд, затем остаются только роутеры MikroTik;

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Автоматически созданное описание

- Также посмотреть состояние выполняемого сканирования можно во вкладке Network Maps -> Local -> Settings, там же его можно отменить при необходимости;

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

- В данном случае можно отменить сканирование по достижении подсети 172.16.100.0, т.к. там уже точно нет магазинов. Для этого необходимо выделить сканирование и нажать «-»;

- Для выгрузки результатов нужно перейти в «Devices» в колонке слева и нажать «CSV», сервер отдаст CSV файл с содержимым представленной таблицы;Изображение выглядит как текст, снимок экрана, число, Шрифт

Автоматически созданное описание

- Остается только распарсить .csv любым удобным образом. В данном примере можно импортировать .csv в книгу Excel и подтянуть к ip адресам названия магазинов и тип устройств из выгрузки WS, чтобы понять какие устройства были найдены.

Изображение выглядит как текст, снимок экрана, число, программное обеспечение

Автоматически созданное описание

## Актуализация данных в Oxidized

1) Сформировать актуальный список устройств:

Oxidized отслеживает конфигурации по файлу router.db, включающий все устройства, которые с которых необходимо собирать конфигурацию в формате host\_name:OS:ip\_address

Изображение выглядит как текст, электроника, снимок экрана, дисплей

Автоматически созданное описание

Т.е. в нашем случае используется маска pidМагазина-модель\_роутера:routeros:ip\_адрес.

Формировать такой файл удобнее всего в Excel с помощью формул ПРОСМОТРX и СЦЕП. После формирования списка в Excel файле его можно скопировать в router.db, открытый блокнотом и прокинуть на машину через WinSCP, либо же сразу вставить содержимое в документ на машине. Файл нужно положить в /home/oxidized/.config/oxidized.

2) Перезапустить Oxidized:

После того, как актуальный файл помещен на машину нужно перезапустить службу oxidized (sudo systemctl restart oxidized.service).