# Восстановление паролей

## Краткая теория

Администратор сети при утере пароля на консольное подключение к маршрутизатору или пароля на переход в привилегированный режим вынужден решать проблему их восстановления. Решается она переходом в режим ROMMON и изменением значения конфигурационного регистра. Значением регистра по умолчанию является 0x2102:

|  |
| --- |
| Регистр в шестнадцатеричном представлении |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2 | | | | 1 | | | | 0 | | | | 2 | | | |
| Позиции битов | | | | | | | | | | | | | | | |
| **15** | **14** | **13** | **12** | **11** | **10** | **9** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** | **0** |
| Регистр в двоичном представлении | | | | | | | | | | | | | | | |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |

В контексте решения задачи восстановления пароля в регистре следует поменять значение 6-го бита. По умолчанию данный бит выставлен в 0. Если же этот бит имеет значение 1, то при загрузке IOS[[1]](#footnote-1) в RAM[[2]](#footnote-2) конфигурационный файл startup-config игнорируется и, следовательно, в RAM создается пустой файл running-config. Это позволит войти в привилегированный режим, минуя требование ввода пароля. После чего из NVRAM[[3]](#footnote-3) следует вызвать running-config со всеми настройками (в том числе и с неизвестными паролями). Затем следует назначить новые пароли и измененный конфиг сохранить в NVRAM.

## Содержание работы

Откройте файл lost\_password.pka. Поместите на рабочее поле модели сети PC и подключитесь от него к маршрутизатору консольным кабелем.

Используя терминальную программу, убедитесь в том, что доступ в пользовательский режим заблокирован паролем.

Выключите и включите питание маршрутизатора и, перейдя в окно терминальной программы, дайте команду прерывания загрузки IOS в RAM (Ctrl+Break[[4]](#footnote-4)).

В открывшемся режиме редактирования ROMMON [[5]](#footnote-5)введите команду изменения конфигурационного регистра

ROMMON>confreg **0x2142**

Вновь выключите и включите питание маршрутизатора и дождитесь окончания загрузки IOS. При этом в RAM будет создан пустой runnung-config. Проверьте конфиг командой

Router#sh ru

Перейдите в привилегированный режим и дайте команду загрузки файла startup-config в RAM

Router#copy st ru

Введите новые пароли на консольный вход и в привилегированный режимы (cisco и class, соответственно)

Router(config)#line con **0**

Router(config-line)#password **cisco**

Router(config-line)#login

Router(config-line)#exit

Router(config)#enable secret **class**

Текущее значение конфигурационного регистра можно увидеть в конце вывода команды

Router#show version

Верните прежнее значение конфигурационного регистра

Router(config)#config-register **0x2102**

Сохраните измененную конфигурацию в NVRAM

Router#copy ru st

Выключите и включите вновь питание маршрутизатора и убедитесь в том, что вы уже имеете доступ к командной строке операционной системы. Также можно для проверки паролей перезагрузить IOS командой

Router#reload

Проверьте измененное значение конфигурационного регистра

Router#show version

## Выводы

Назначение паролей на доступ к маршрутизатору не гарантирует полную безопасность маршрутизатора, поскольку они могут быть легко взломаны. Следует по возможности сетевые устройства размещать в помещениях, защищенных по периметру (решетки, замки), что позволит свести к минимуму возможность прямого доступа к ним. Также рекомендуется отдельно хранить копию конфигурационного файла.

1. Операционная система маршрутизатора [↑](#footnote-ref-1)
2. Оперативная память маршрутизатора [↑](#footnote-ref-2)
3. Внешняя память маршрутизатора [↑](#footnote-ref-3)
4. Или попробуйте Ctrl+C [↑](#footnote-ref-4)
5. ROMmon – Read Only Memory (память только для считывания) monitor (монитор). ROM – это внешняя память маршрутизотора, в которой хранится значение конфигурационного регистра. Хотя она служит лишь для считывания информации, её содержимое можно перезаписывать, используя режим ROMMON [↑](#footnote-ref-5)