Configuration Management

Overview

This article describes a set of commands used for configuration management.

Configuration Undo/Redo

Any action done in GUI or any command executed from the CLI is recorded in `/system history`. You can undo or redo any action by running undo or redo commands from the CLI or by clicking on Undo, Redo buttons from the GUI.

A simple example to demonstrate the addition of firewall rule and how to undo and redo the action:

```
[admin@v7_ccr_bgp] /ip/firewall/filter> add chain=forward action=drop
[admin@v7_ccr_bgp] /ip/firewall/filter> print
Flags: X - disabled, I - invalid; D - dynamic
0 X chain=input action=drop protocol=icmp src-address=10.155.101.1 log=no
log-prefix=""

1 chain=forward action=drop

[admin@v7_ccr_bgp] /ip/firewall/filter> /system/history/print
Flags: U - undoable, R - redoable, F - floating-undo
Columns: ACTION, BY, POLICy
ACTION BY POLIC
F filter rule added admin write
U --- write
[admin@v7_ccr_bgp] /ip/firewall/filter>
```

We have added firewall rule and in `/system history` we can see all what is being done.

Let's undo everything:

```
[admin@v7_ccr_bgp] /ip/firewall/filter> /undo
[admin@v7_ccr_bgp] /ip/firewall/filter> print
Flags: X - disabled, I - invalid; D - dynamic
0 X chain=input action=drop protocol=icmp src-address=10.155.101.1 log=no
log-prefix=""

[admin@v7_ccr_bgp] /ip/firewall/filter>
```

As you can see firewall rule disappeared.
Now redo the last change:

```
[admin@v7_ccr_bgp] /ip/firewall/filter> /redo
[admin@v7_ccr_bgp] /ip/firewall/filter> print
Flags: X - disabled, I - invalid; D - dynamic
0 X chain=input action=drop protocol=icmp src-address=10.155.101.1 log=no
log-prefix=""

1 chain=forward action=drop

[admin@v7_ccr_bgp] /ip/firewall/filter>
```

System history is capable of showing exact CLI commands that will be executed during Undo or Redo actions even if we perform the action from GUI, for example, detailed history output after adding TCP accept rule from WinBox:

```
[admin@v7_ccr_bgp] /system/history> print detail
Flags: U - undoable, R - redoable, F - floating-undo
 F redo=
      /ip firewall filter add action=accept chain=forward disabled=no log=no \
          log-prefix="" protocol=tcp
    undo=/ip firewall filter remove *4 action="filter rule added" by="admin"
    policy=write time=oct/10/2019 18:51:05

 F redo=/ip firewall filter add action=accept chain=forward
    undo=/ip firewall filter remove *3 action="filter rule added" by="admin"
    policy=write time=oct/10/2019 18:49:03


U redo="" undo="" action="---" by="" policy=write time=sep/27/2019 13:07:35
[admin@v7_ccr_bgp] /system/history>
```

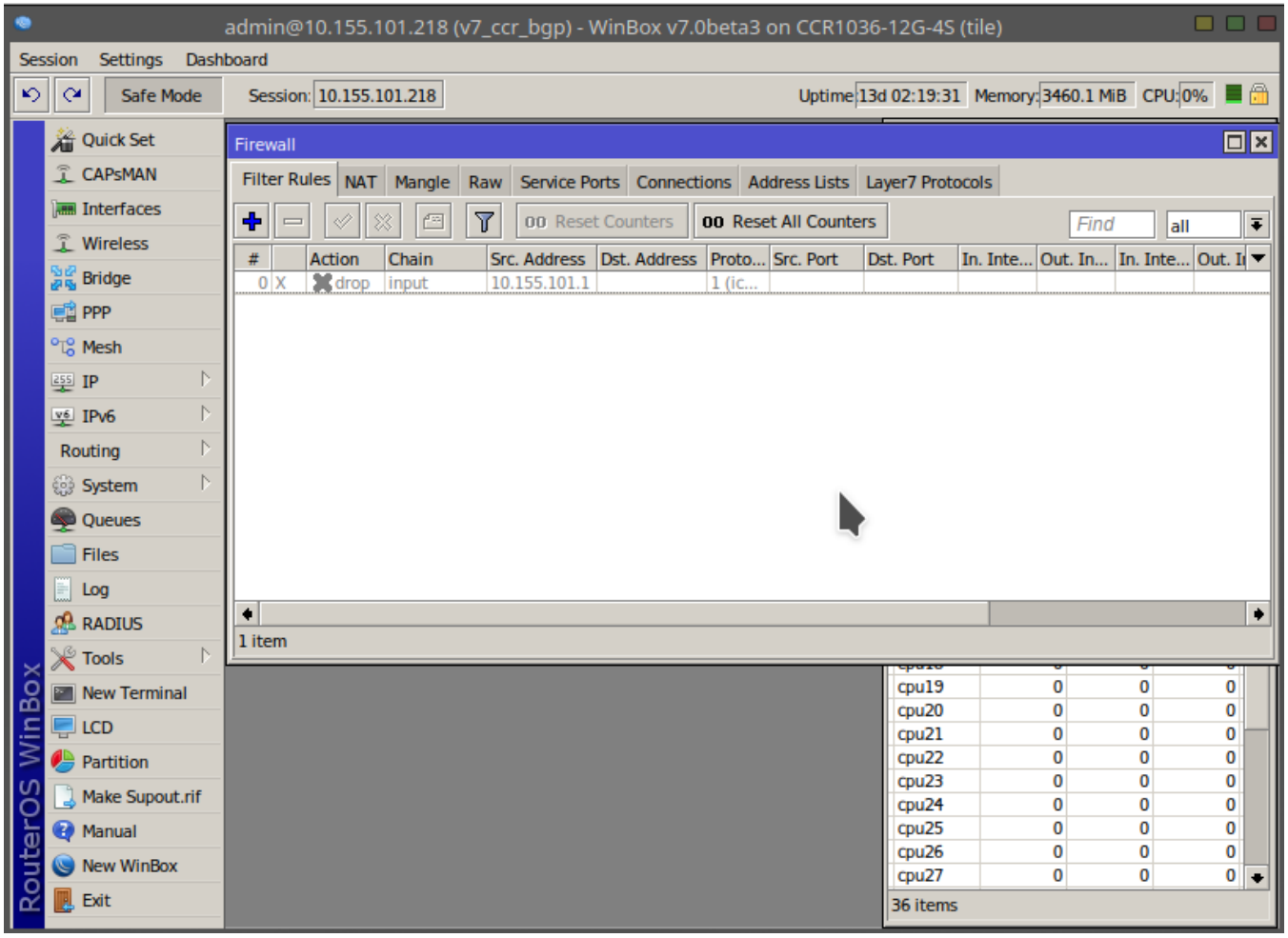
Safe Mode

Sometimes it happens that the router's configuration is changed in a way that will make the router inaccessible (except local console). Usually, this is done by accident, but there is no way to undo the last change when the connection to the router is already cut. Safe mode can be used to minimize such risk.

Safe mode is entered by pressing **Ctrl-X**. To save changes and quit safe mode, press **Ctrl-X** again. To exit without saving the made changes, hit **Ctrl-D**

```
[admin@MikroTik] ip route>[CTRL]+[X]
[Safe Mode taken]

[admin@MikroTik] ip route<SAFE>
```



Message **Safe Mode taken** is displayed and prompt changes to reflect that session is now in safe mode. In WinBox safe mode is enabled by toggling the **Safe Mode** toggle button on the left side of the toolbar.

All configuration changes that are made (also from other login sessions), while the router is in safe mode, are automatically undone if the safe mode session terminates abnormally. You can see all such changes that will be automatically undone tagged with an **F** flag in system history:

```
[admin@MikroTik] ip route>
[Safe Mode taken]

[admin@MikroTik] ip route<SAFE> add
[admin@MikroTik] ip route<SAFE> /system history print
Flags: U - undoable, R - redoable, F - floating-undo
  ACTION                                   BY                POLICY
F route added                              admin             write
```

Now, if telnet connection, WinBox terminal (if the safe mode was enabled on WinBox terminal window), or WinBox connection is cut, then after a while (TCP timeout is **9** minutes) all changes that were made while in safe mode will be undone. Exiting session by **Ctrl-D** also undoes all safe mode changes, while **/quit** does not.

If another user tries to enter safe mode, he's given the following message:

```
[admin@MikroTik] >
Hijacking Safe Mode from someone - unroll/release/don't take it [u/r/d]:
```

- [u] - undoes all safe mode changes, and puts the current session in safe mode.
- [r] - keeps all current safe mode changes, and puts the current session in a safe mode. The previous owner of safe mode is notified about this:

```
[admin@MikroTik] ip firewall rule input
[Safe mode released by another user]
```

- [d] - leaves everything as-is.

If too many changes are made while in safe mode, and there's no room in history to hold them all (currently history keeps up to 100 most recent actions), then the session is automatically put out of the safe mode, no changes are automatically undone. Thus, it is best to change the configuration in small steps, while in safe mode. Pressing **Ctrl-X** twice is an easy way to empty the safe mode action list.

System Backup/Restore

System backup is the way to completely clone routers configuration in binary format. The backup file contains not just configuration, but also statistics data, logs, etc. The backup file is best used to save and restore configuration on the same device, for moving configuration to other devices, use export files instead.

> Backup files contain sensitive information (passwords, keys, certificates). The file can be encrypted, but even then backups should be stored only in a secure location.

Restoring backup files should be done only on the same router or on a similar router when the previous router fails. A backup must not be used to clone configuration on multiple network routers.

Example to save and load backup file:

```
[admin@MikroTik] > system backup save name=test password=123
Configuration backup saved
[admin@MikroTik] > file print
# NAME TYPE SIZE CREATION-TIME
0 test.backup backup 12567 sep/08/2004 21:07:50
[admin@MikroTik] >
[admin@MikroTik] > system backup load name=test password=123
Restore and reboot? [y/N]:
y
Restoring system configuration
System configuration restored, rebooting now
```

Import/Export

RouterOS allows to export and import of parts of the configuration in plain text format. This method can be used to copy bits of configuration between different devices, for example, clone the whole firewall from one router to another.

An export command can be executed from each individual menu (resulting in configuration export only from this specific menu and all its sub-menus) or from the root menu for complete config export.

Following command parameters are accepted:

Property	Description
compact	Output only modified configuration, the default behavior
file	Export configuration to a specified file. When the file is not specified export output will be printed to the terminal
hide-sensitive	Hide sensitive information, like passwords, keys, etc.
verbose	With this parameter, the export command will output whole configuration parameters and items including defaults.

For example export configuration from `/ip address` menu and save it to file:

```
[admin@MikroTik] > /ip address print
Flags: X - disabled, I - invalid, D - dynamic
#   ADDRESS            NETWORK         BROADCAST       INTERFACE
0   10.1.0.172/24      10.1.0.0        10.1.0.255      bridge1
1   10.5.1.1/24        10.5.1.0        10.5.1.255      ether1
[admin@MikroTik] > /ip address export file=address
[admin@MikroTik] > /file print
# NAME                             TYPE         SIZE       CREATION-TIME
0  address.rsc                      script       315        dec/23/2003 13:21:48
[admin@MikroTik] >
```

By default export command writes only user-edited configuration, RouterOS defaults are omitted.

For example, IPSec default policy will not be exported, and if we change one property then only our change will be exported:

```
[admin@rack1_b4] /ip ipsec policy> print
Flags: T - template, X - disabled, D - dynamic, I - inactive, * - default
0 T * group=default src-address=::/0 dst-address=::/0 protocol=all
      proposal=default template=yes
[admin@rack1_b4] /ip ipsec policy> export
# apr/02/1970 17:59:14 by RouterOS 6.22
# software id = DB0D-LK67
#
[admin@rack1_b4] /ip ipsec policy> set 0 protocol=gre
[admin@rack1_b4] /ip ipsec policy> export
# apr/02/1970 17:59:30 by RouterOS 6.22
# software id = DB0D-LK67
#
/ip ipsec policy
set 0 protocol=gre
```

Notice the ***** flag, it indicates that entry is system default and cannot be removed manually.

Here is the list of all menus containing default system entries

Menu	Default Entry
/interface wireless security-profiles	default
/ppp profile	"default", "default-encryption"
/ip hotspot profile	default
/ip hotspot user profile	default
/ip ipsec policy	default
/ip ipsec policy group	default
/ip ipsec proposal	default
/ip ipsec mode-conf	read-only
/ip smb shares	pub
/ip smb users	guest
/ipv6 nd	any
/mpls interface	all
/routing bfd interface	all
/routing bgp instance	default

/routing ospf instance	default
/routing ospf area	backbone
/routing ospf-v3 instance	defailt
/routing ospf-v3 area	backbone
/snmp community	public
/tool mac-server mac-winbox	all
/tool mac-server	all
/system logging	"info", "error", "warning", "critical"
/system logging action	"memory", "disk", "echo", "remote"
/queue type	"default", "ethernet-default", "wireless-default", "synchronous-default", "hotspot-default", "only-hardware-queue", "multi-queue-ethernet-default", "default-small"

Configuration Import

Root menu command import allows running configuration script from the specified file. Script file (with extension ".rsc") can contain any console command including complex scripts.

For example, load saved configuration file

```
[admin@MikroTik] > import address.rsc
Opening script file address.rsc

Script file loaded and executed successfully
[admin@MikroTik] >
```

Import command allows to specify following parameters:

Property	Description
from-line	Start executing the script from the specified line number
file-name	Name of the script (.rsc) file to be executed.
verbose	Reads each line from the file and executes individually, allowing to debug syntax or other errors more easily.

Auto Import

It is also possible to **automatically** execute scripts after uploading to the router with FTP or SFTP. The script file must be named with extension *.auto.rsc. Once the commands in the file are executed, a new *.auto.log file is created which contains import success or failure information.

> ".auto.rsc" in the filename is mandatory for a file to be automatically executed.

Configuration Reset

RouterOS allows resetting configuration with `/system reset-configuration` command

This command clears all configuration of the router and sets it to the factory defaults including the login name and password ('admin' with an empty password). For more details on the default configuration see the list.

After the configuration reset command is executed router will reboot and load the default configuration.

The backup file of the existing configuration is stored before reset. That way you can easily restore any previous configuration if reset is done by mistake.

If the router has been installed using Netinstall and had a script specified as the initial configuration, the reset command executes this script after purging the configuration. To stop it from doing so, you will have to reinstall the router.

It is possible to override default reset behavior with the parameters below:

Property	Description
keep-users	Do not remove existing users from the configuration
no-defaults	Do not load default configuration, just clear configuration
skip-backup	Skip automatic backup file generation before reset
run-after-reset	Run specified .rsc file after reset. That way you can load your custom configuration.

For example hard reset configuration without loading default config and skipping backup file:

```
[admin@MikroTik] > /system reset-configuration no-defaults=yes skip-backup=yes
Dangerous! Reset anyway? [y/N]: y
```

And the same using Winbox: