TR-069

TR069-client implements CPE WAN Management Protocol (CWMP) for remote device management, which is standardized by the Broadband Forum (BBF). CWMP works over IP network using HTTP(S) to communicate with an Auto Configuration Server (ACS), which can monitor, configure attributes and update the firmware of a remote device. Typically used by ISPs to manage CPEs, but also can be used for Network Infrastructure Device management.

Requires tr069-client package.

Configuration Settings

Sub-menu: `/tr069-client`

TR069-client menu parameters:

Writable Settings

Client configuration settings.

Property	Description
enabled	enable/disable CWMP protocol
acs-url	URL of ACS. Examples: "https://example.com:8080/path/", "https://192.168.1.100/"
username	HTTP authentication username (used by CPE to "login" into ACS)
password	HTTP authentication password (used by CPE to "login" into ACS)
periodic-inform-enabled	enable/disable CPE periodical session initiation. Timer is started after every successful session. When session is started by periodic interval then Inform RPC contains "2 PERIODIC" event. Maps to "Device.ManagementServer.PeriodicInformEnable" Parameter
periodic-inform-interval	timer interval of periodic inform. Maps to "Device.ManagementServer.PeriodicInformInterval"
client-certificate	certificate of client/CPE, which can be used by ACS for extra authentication

Read-only Settings

Read only parameters to monitor state of the client.

Property	Description
status	informative status of CWMP. • disabled - protocol disabled, • waiting-URL - protocol enabled, but ACS URL not configured, • running - CWMP is configured correctly and will communicate with ACS on events
last-session-error	user-friendly error description indicating why the previous session didn't finish successfully
retry-count	consecutive unsuccessful session count. If > 0, then last-session-error should indicate error. Resets to 0 on a successful session, disabled protocol or reboot

Commands

Command	Description
reset-tr069-config	completely resets and forgets tr069-client configuration and state (without affecting other ROS configurations). Use when CWMP goes into unresponsive/hanged state and should be restored without re-installation of the RouterOS.

CWMP Session

CWMP client usually starts communication(Session) with ACS on different events - first boot, reboot, periodic interval, remote request, value change etc. In each session, CPE and ACS can call RPCs to be "executed" on the other side. CPE always starts with Inform RPC, which contains connection reason, device info and some Parameter values depending on configuration. When CPE has nothing more to say, then ACS executes its RPCs (which most of the time are Parameter management RPCs).

Parameters and Data Models

Parameters are simple name+value pairs and each vendor can decide which Parameters to support in its devices. A combination of all supported Parameters is called Data Model (DM). BBF defines three root Data Models(TR-098, TR-181:1, TR-181:2) on which vendors should base their supported Parameters. **RouterOS Data Model is based on "TR-181 Issue 2 Amendment 11"**, which is the newest DM and recommended by BBF.

RouterOS TR069 client supported parameter reference document:

File	Modified
HTML File current.html v7.13 - RouterOS TR069 client supported parameter reference document	Feb 28, 2024 by Confluence Helper

Download RPC

RouterOS Update (1 Firmware Upgrade Image)

CWMP standard defines that CPE's firmware can be updated using Download RPC with FileType="1 Firmware Upgrade Image" and single URL of a downloadable file (HTTP and HTTPS are supported). Standard also states that downloaded file can be any type and vendor specific process can be applied to finish firmware update. Because MikroTik's update is package based (and also for extra flexibility), an XML file is used to describe firmware upgrade/downgrade. For now, XML configuration supports providing multiple URLs of files, which will be downloaded and applied similarly as regular RouterOS update through firmware/package file upload.

An example of RouterOS bundle package and tr069-client package update (don't forget to also update tr069-client package). An XML file should be put on some HTTP server, which is accessible from CPE for download. Also, downloadable RouterOS package files should be accessible the same way (can be on any HTTP server). Using ACS execute Download RPC with URL pointing to XML file (e.g. "https://example.com/path/upgrade.xml") with contents:

```
<upgrade version="1" type="links">
   <config/>
   <links>
       <link>
          <url>https://example.com/routeros-mipsbe-X.Y.Z.npk</url>
       </link>
       <link>
          <url>https://example.com/tr069-client-X.Y.Z-mipsbe.npk</url>
       </link>
   </links>
</upgrade>
```

CPE will download XML, parse/validate its contents, download files from provided URLs and try to upgrade. The result will be reported with TransferComplete RPC.

> **Note**
>
> Always make firmware updates incremental - first, update locally tested device and make sure that CWMP communication is resumed with a new version and required ROS functionality works. Secondly, repeat steps by updating groups of CPEs incrementally. We do not recommend updating all remote devices at once.
>
> **Warning:** Use HTTPS in production for firmware management

Configuration Change (3 Vendor Configuration File)

The same Download RPC can be used to perform complete configuration overwrite (as intended by standard) OR configuration alteration (when URL's filename extension is ".alter").

Alter configuration

RouterOS has a lot of configuration attributes and not everything can be ported to CWMP Parameters, that's why RouterOS provides a possibility to execute its powerful scripting language to configure any attribute. A configuration alteration (which is really a regular script execution) can be performed using Download RPC FileType="3 Vendor Configuration File" with downloadable file extension ".alter". This powerful feature can be used to configure any ROS attributes which are not available through CWMP Parameters.

Overwrite all configurations

Full ROS configuration overwrite can be performed using Download RPC FileType="3 Vendor Configuration File" with any URL file name (except with ".alter" extension).

Warning: Provided configuration file(script) must be "smart" enough to apply configuration correctly right after reboot. This is especially important when using uploaded configuration file with Upload RPC, because it only contains values export. Some things that should be added manually:

- delay at beginning, for interfaces to show up;
- hidden passwords for users;
- certificates.

RouterOS default configuration change (X MIKROTIK Factory Configuration File)

This vendor specific FileType allows the change of the RouterOS default configuration script that is executed when **/system reset-configuration** command is executed (or the other means when router configuration is being reset).

> **Note**
>
> If the default configuration script is changed it will not be displayed by **/system default-configuration print** as it is the case if that script is altered via Netinstall tool. That command will always show the default script set up by MikroTik
>
> **Warning:** Use this with caution as the failure of uploaded script may render device inoperable and/or inaccessible by the ACS

FactoryReset RPC

This is CWMP standard RPC, which performs RouterOS configuration factory-reset. The reset process is performed in the same way as executing the command:

```
/system reset-configuration skip-backup=yes
```

Note that the default factory configuration can be different for each device (see [1]) and execution of this command removes all configurations and executes internally stored default-configuration script.

Best Practices Guide for preparing CPE with custom factory settings for TR069 https://wiki.mikrotik.com/wiki/Tr069-best-practices

Upload RPC

Upload current configuration (1 Vendor Configuration File)

The result of this is file uploaded to the ACS same as the output of **/export** command in the RouterOS

Upload log file (2 Vendor Log File)

The result of this is file uploaded to the ACS is similar to the output of **/log print** command in the RouterOS

Upload default configuration (X MIKROTIK Factory Configuration File)

The result of this is file uploaded to the ACS that has contents of the current set default configuration script that will be executed if **/system reset-configuration** command is executed. It may differ from one returned using **/system default-configuration print**.

Security

- HTTP should only be used when testing initial setup in the secured/private network because Man-in-the-middle attacker could read/change configuration parameters. **In the production environment, HTTPS is a MUST**.
- CWMP's incoming connection validation by design is safe because CPE will not communicate with any other device except previously configured ACS. Connection Request only signals CPE to start a new connection + new session with previously configured ACS.

Tested ACSs

Ordering is alphabetical. MikroTik does not imply any one vendor superiority of another. If some ACS is missing you can notify us of the existence of it, and it might be added to the list.

Commercial

We have tested and verified to be working the following commercial ACS solutions:

- AVSystem
- Axiros
- Friendly Tech

Open Source

- GenieACS

Note: these ACS systems below seem to be not maintained and thus is not suggested as useful options

- FreeACS
- LibreACS