MikroTik – TR069

MiRO TRAINING

Hannes Willemse

MikroTik Certified Trainer
MTCNA – MTCWE – MTCRE – MTCTCE

What is TR069

The CPE WAN Management Protocol (CWMP), published by The Broadband Forum as **TR-069**, specifies a standard communication mechanism for the remote management of end-user devices. It defines a protocol for the secure auto-configuration of a **TR-069** device and incorporates other management functions into a common framework.

www.friendly-tech.com

What is TR069 designed for?

TR-069 enables remote and safe configuration of network devices called CPE. Configuration is managed by a central server called an ACS.

https://www.avsystem.com

What is an ACS

Auto Configuration Server - software that manages devices remotely.
AVSystem UMP is an example of the ACS.

https://www.avsystem.com

What is an CPE

Customer Premises Equipment - any equipment used by customers which can be managed by the ACS. CPE is commonly called a device.

https://www.avsystem.com

How to connect a device to the ACS?

- ACS URL - an Internet address of the ACS, which is accessible from this device.
- Periodic Inform Interval - defines a frequency of communication with the ACS.
- Username and password - verification data is optional. It depends on the ACS requirements and an expected security level.

https://www.avsystem.com

What does the communication between the device and the ACS look like?

- The connection between the device and the ACS is not permanent.
- The device establishes the connection with the ACS only at specific points in time. It usually lasts several seconds, just enough to exchange all necessary messages between CPE and the ACS. This short exchange of messages is called a provisioning session.

https://www.avsystem.com

The provisioning session

- Session initialization
- Authentication
- Device identification
- Tasks execution on the device
- Session closure

https://www.avsystem.com

When does the device start a session with the ACS?

- The ACS URL is saved or changed on the device or the device is reset to factory settings (the device communicates it as **BOOTSTRAP**).
- A new periodic visit is to begin according to the value set in Periodic Inform Interval (the device communicates it as **PERIODIC**).

https://www.avsystem.com

When does the device start a session with the ACS?

- The device responds to the ACS request for immediate connection (the device communicates it as **CONNECTION REQUEST**).
- A value of a parameter for which active notification is enabled changes (the device communicates it as **VALUE CHANGE).**
- The device is reset or is reconnected to the power supply (the device communicates it as **BOOT**).

When does the device start a session with the ACS?

- During one of the previous sessions the ACS ordered the device to initiate the contact with ScheduleInform command (the device communicates it as **SCHEDULED**).
- The device wants to report execution of previously ordered download or upload methods (the device communicates it as **TRANSFER COMPLETE**).
- The device wants to confirm a previously ordered diagnostic (the device communicates it as **DIAGNOSTIC COMPLETE**).

When does the device start a session with the ACS?

- The manufacturer of the device can add custom events that will also make the device connect to the ACS.

https://www.avsystem.com

Why should I be aware of reasons for session initialization?

- You can order the device to perform various tasks depending on a particular context, for example, when the device connects for the first time.
- You can analyze reasons for last visits and find out abnormalities regarding device's activities.

https://www.avsystem.com

Can the ACS initialize a session with the device?

No, it cannot. The session can be started only by the device. However, the **ACS can send a request** to establish connection, that is Connection Request, which makes the device contact the ACS if it is properly implemented.

https://www.avsystem.com

Is TR-069 secure?

Yes, it is. TR-069 provides several mechanisms that guarantee robust security.

Authentication

Username and password, SSL/TLS certificates

Communication

HTTPS

Other

Firewall - IP addresses limited to a safe pool

What are the benefits of managing devices via TR-069?

- It offers a greater control over devices' settings in comparison to managing them using configuration files.
- It shortens time needed for installing the devices at the customers' premises thanks to sending the initial configuration automatically.
- It reduces a number of engineers' visits thanks to a possibility of performing crucial operations remotely.

What are the benefits of managing devices via TR-069?

- Changing configuration, turning services off/on and performing diagnosis.
- It facilitates maintenance work such as upgrading device's firmware and backing up its configuration. What is more, these long lasting operations can be scheduled to take place off-peak hours.
- It reduces failures thanks to network optimization settings for devices, for example by setting the best Wi-Fi channels.

What are the benefits of managing devices via TR-069?

- It automates the control of the network state through monitoring.
- It collects data that can be used in business analysis, for example, detecting active users to whom additional offers can be made.

https://www.avsystem.com

TR069 vs SNMP

Feature	SNMP	TR-069
The concept	Protocol to communicate with specific CPE	The TR-069 is a standard to communicate with all CPEs. TR-069 is not only a protocol but includes business rules.
Supported commands from server side	SNMP includes only: Get/Set and traps.	TR-069 includes : Set /Get, traps, create object, Delete object, File download, File upload, Reboot, reset, diagnostics commands (Ping, loopback, etc) + support of additional RPCs

TR069 vs SNMP

Feature	SNMP	TR-069
Zero Touch provisioning	Per CPE type (if available)	Yes, part of the standard
Diagnostics and monitoring	Per CPE type (if available)	Yes, part of the standard
Data Monitoring	No	Yes
Enforcing Carrier's policy on CPE & Access Control	No	Yes
Firmware upgrade	Not part of the protocol	Yes
Security	Not part of the protocol	Full security
More adopted by the main carriers	No	Yes
Built-in ability to manage multiple types of CPEs	No. Each CPE type requires customizations	In-dependant of CPE vendor or CPE type.

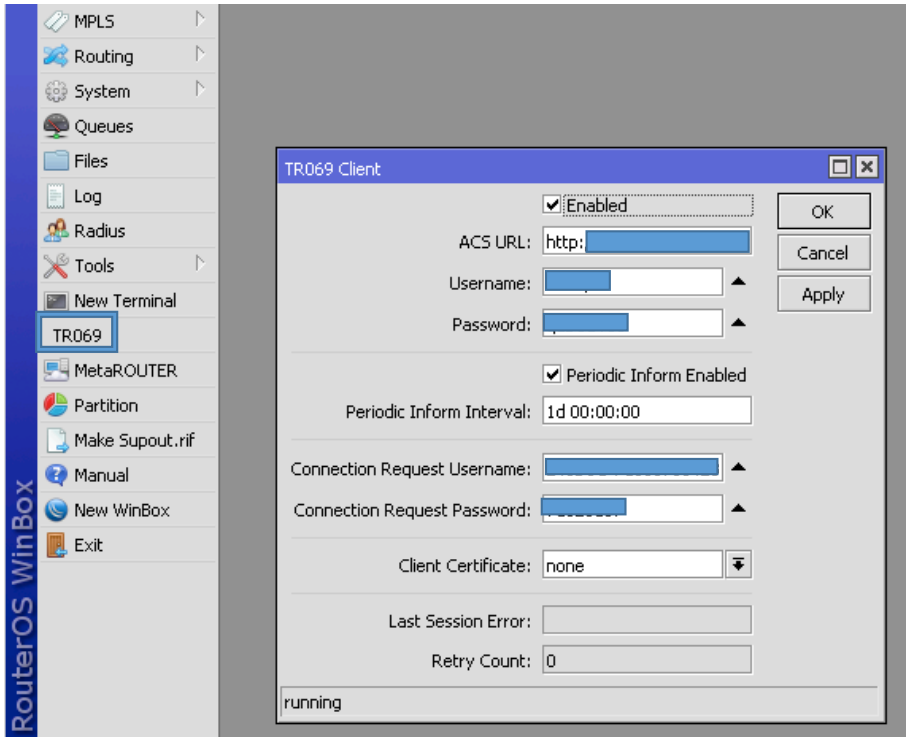
What is a RPC

Remote Procedure Call (**RPC**) is a protocol that one program can use to request a service from a program located in another computer on a network without having to understand the network's details. A procedure call is also sometimes known as a function call or a subroutine call.

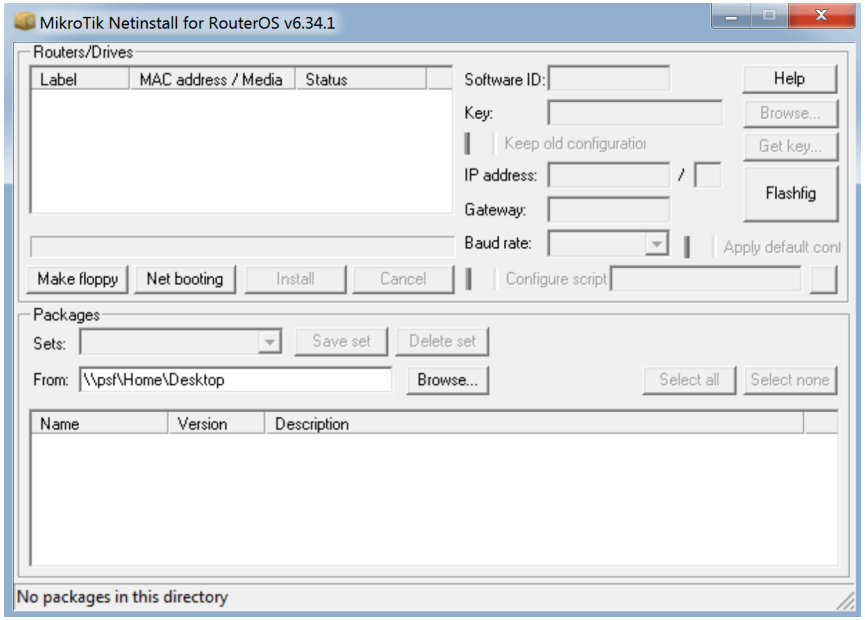
searchmicroservices.techtarget.com

What do I need to implement TR069 on a MikroTik

What do I need to implement TR069 on a MikroTik



What do I need to implement TR069 on a MikroTik



What do I need to implement TR069 on a MikroTik

https://wiki.mikrotik.com/wiki/Manual:Flashfig