

A cloud-based solution to configure home and small office routers



Aalto University

Andi Bidaj, Ashok Rajendran, Debopam Bhattacharjee

Markku Antikainen, Tuomas Aura

Aalto University, Finland



Introduction

The project aims to enable management and configuration of home and small office routers from the cloud. The routers connect through TLS tunnels to the cloud and are identified based on the pre-installed TLS Certificate fingerprints. The cloud currently supports client devices with Linux-based open-source firmwares OpenWrt and DD-WRT.

Support for:



Key Features

- **Ubiquitous access:** Configuration of routers from anywhere on the Internet.
- **Open-source firmware support:** Support for OpenWrt and DD-WRT.
- **Firmware-based customized solution:** DD-WRT client software developed in PHP, OpenWrt client software developed in Lua.
- **Scalability and performance:** Server-side implementation using Node.js.
- **Security:** TLS tunnel between device and the cloud. Password-based user authentication.
- **Open Source:** To be published online soon.

Functionality

- **Configuration:** Configuring the router from the cloud.
- **Delegation:** Delegating tasks related to device management and configuration to others.
- **Device alert:** Devices send alert messages to the cloud under certain circumstances which are then reported to the end users.
- **One-click debugging:** All necessary debugging information and configuration files may be downloaded by the end-user as a single archive on the click of a button.
- **Arbitrary shell-command execution:** The user may run an arbitrary shell command on his device through the cloud.
- **Configuration roll-back:** Device configuration can be rolled back to a previously saved configuration in case of any issue.

Ownership Handover

3 cases handled:

- Old owner **gracefully** (notifies the cloud) hands over the device to the new owner along **with device history**.
- Old owner requests an ownership handover **without sharing device history**.
- Ownership decided **based on physical access** to the device.

Cloud Architecture

- **Device-Cloud interface:** The cloud exposes a set of REST-APIs which are called by the devices through a secured tunnel.
- **Web Server-User interface:** The user interface interacts with the server via REST API calls.
- The 2 interfaces described above are decoupled but use the same backend datastore.

Security Model

- **TLS tunnel** between the **device and the cloud**.
- Devices identified based on the fingerprints of **pre-installed certificates**.
- **TLS tunnel** between the **user and the cloud**.
- Ownership established only when user connects to the cloud through the device (**TLS within tunnel**).
- Once ownership is established, user can access the device from anywhere

