eduroam Troubleshooting 2.0

Stefan Winter, RESTENA Foundation, stefan.winter@restena.lu (Presenter, Author)

Stefan Winter graduated in Computer Science at the University of Karlsruhe, Germany, in September 2004, with a specialisation in telematics and foundations of Computer Science. He is working as R&D Engineer for the Luxembourg Research and Education Network RESTENA, where network roaming and identity federations are in the focus of his activities. He led the R&D work for eduroam during several incarnations of the GEANT projects. He is member of the eduroam Operational Team in Europe (leading the development of the eduroam CAT software) and the Global eduroam Governance Committee.

Keywords eduroam, expert system, diagnostics, real-time support, user experience

Introduction

Unbeknownst to all but the most technology-savvy end users connecting to an eduroam hotspot, there is a surprising number of architectural components which all need to function nominally for the connection and subsequent network usage experience to work smoothly. During national, and even more so international, roaming, these components are operated by a multitude of different entities, and there is no global oversight over all the components involved. Additionally, even when all components individually work as expected, interoperability issues sometimes cause issues of their own (e.g. undue VLAN assignments).

As a consequence, failures – if any – almost always only affect a subset of the architecture, are typically not discovered in real-time by operations personnel, and are hard to reproduce for anyone who is not on the path and/or nearby.

eduroam R&D is focusing on improvements on diagnostics and fault-finding and communication between all operators, both reactively (giving users real-time and active guidance in case of connection problems) and proactively (by monitoring the involved components and corresponding log files).

The Jigsaw Puzzle

A successful use of eduroam (authentication and subsequent use of IP resources) requires the following elements to work:

On the eduroam Service Provider (SP, “hotspot”) side

- end-user device (has to be configured correctly)
- SP’s local network properties (DHCP with sufficient IP pool etc.)
- SP’s wireless infrastructure (coverage, encryption level, network SSID, RADIUS uplink, ...)
- SP’s outbound internet connectivity (no manual proxies, support for IP fragmentation, ...)

For all involved proxy legs, which can be as much as four (in the case of international roaming), the following elements are also needed:

- network connectivity between RADIUS servers (support for IP fragmentation, ...)
- RADIUS servers (request routing, ...)

Finally, on the eduroam Identity Provider (IdP) side, the following elements need to work

- inbound network connectivity (support for IP fragmentation, ...)
- RADIUS server
- authentication backend

It is thus a significant challenge (and ongoing effort) to create, operate and refine a monitoring system which can infer the overall system status in real-time from individual measurements and provide understandable and actionable insights to the inquiring party (which may be an end user or eduroam administrator).

End-User Connection Diagnostics (Technology Preview available by TNC18)

By the time of TNC18, a web portal for end-users and administrators is available which will, on demand, trigger diagnostic investigations for user connections. As user-interactive input, it merely requires the realm or name of the IdP; additional input regarding the SP position is derived from location information. The investigation will cover at least: all proxy servers (SP-side, international, IdP-side), the network connectivity between these proxies, the network connectivity between the IdP-side national proxy and the IdP itself, and the RADIUS server of the IdP.

Further components of this system (unlikely to be ready by TNC18) include: hardware monitor probes at hotspots (enabling a more thorough investigation of the SP deployment itself), and diagnostic applications on popular end-user devices (enabling a more thorough investigation of issues at the exact location and time).

The user will be presented with the result of the findings: a ranked list of architecture components which are possibly the source of the problem, ranked according to the confidence level of being the root cause.

Considering that end-user configuration issues are a likely cause which can not be found out with infrastructure diagnostics, the system will ask the user further questions about the nature of his problem, and will produce a recommendation for the user.

Should diagnostics have identified an actual problem outside the user's responsibility, the system will automatically notify the respective component operator and will request them to take appropriate action.

Administrator Information Exchange (Technology Preview available by TNC18)

Some issues in eduroam are of less technical nature, and cannot be uncovered in an automated way. As example 1, an SP operator has detected abuse of the network and needs to contact the responsible eduroam IdP to sanction the user in question. Or, as example 2, an eduroam IdP receives a user complaint about a protocol which is guaranteed to be open as per eduroam policy is not. He needs to contact the responsible SP, because port filtering is done on the SP local deployment.

The processes for contacting IdPs, SPs, or national proxy operators is currently manual (e-mail based, and often requiring manual escalations until the link between all parties is established).

By TNC18, a web-based communication platform is going to be available which leverages the information in the eduroam Database (including contact points for operators) to provide a structured way of communication which will instantly identify the parties to involve and execute the initial communication in real-time. The form-based system guides the requesting party in a way that ensures that all required information is included in the request (e.g. for abuse complaints, the system will require the MAC address of the user, the timestamp of authentication, and the realm of the user – only this triplet of information enables the IdP to take action at all).

Advanced Proactive Monitoring (Work ongoing by TNC18)

The above tools are all reactive: a user or administrator has to have become aware of a problem, and needs to take action him- or herself. This is not optimal in at least two ways: one, by that time, annoyance on the side of the person with problems has already manifested, and two, in the time between the start of the problem and the time the first user is annoyed enough to report it, there is a significant chance that others are already suffering from the same issues; the "dark figure" of disgruntled users is much higher.

As a possible way out, malfunctions are often detectable in an automated way. Naturally, eduroam Operations already has a monitoring system which checks the most important spots (national and international proxies) in predefined intervals. However, only server states of these proxies are monitored; any issues with particular IdPs that are being transported over these proxies hide in the – excessive – amount of logs on each system, and these logs are not under constant supervision by a human operator.

eduroam R&D is planning to create a system that collects logs from various measurement points, and lets these be analysed by a pre-trained neural network ("deep learning") so that the accompanying algorithms can identify issues in the infrastructure at the very moment they start to occur, with subsequent yet timely alerting of responsible personnel.

By TNC18, an early architectural overview of the solution is likely completed and can be sketched. Further work on this item is planned for the GN4-3 project.