overview

Elements of the eduroam infrastructure

Confederation top-level RADIUS Server (TLR)

The confederation top-level RADIUS Servers, at the time of writing, are located in the Netherlands and Denmark for the European confederation, and Australia and Hong Kong for the Asian and Pacific region. Each have a list of connected country domains (.nl, .dk, .au, .cn etc.) serving the appropriate National Roaming Operators (NROs). They accept requests for federation domains for which they are authoritative, and subsequently forward them to the associated RADIUS server for that federation (and transport the result of the authentication request back). Requests for federation domains they are not responsible for are forwarded to the proper confederation TLR.

Federation-Level RADIUS servers (FLRs)

A federation RADIUS server has a list of connected IdP and SP servers and the associated realms.Typically, a FLR is authoritative for all RADIUS realms ending in its own top-level domain (e.g. a FLR for Antarctica would be authoritative for *.aq); it may also serve a number of domains in other top-level domains (e.g. .com, .net, .org, ...) but it is not authoritative for those entire top-level domains.

The FLR receives requests from the confederation servers and IdP/SP it is connected to and forwards them to the proper server. For its authoritative top-level domain, it rejects requests for non-existent realms inside the top-level domain.

IdP and SP RADIUS infratructure

eduroam IdPs operate a RADIUS server which is responsible for authenticating its own users, by checking the credentials against a local identity management system.

eduroam SPs operate RADIUS capable equipment like Access Points or switches (see below). Large SPs typically also deploy an own RADIUS server, which is then responsible for forwarding requests from visiting users to the respective federation RADIUS server. Upon proper authentication of a user the SP RADIUS server may assign a VLAN to the user. Small SPs which do not require VLAN assignments can connect their RADIUS equipment directly to their FLR server, if the FLR permits that mode of operation.

Institutions which opt to be eduroam IdP and eduroam SP at the same time can have one RADIUS server that fulfills both roles simultaneously. This is the most popular deployment model in eduroam.

Note that the IdP RADIUS server is the most complex of all. Whereas the other RADIUS servers merely proxy requests, the IdP server also needs to handle the requests, and therefore needs to be able to terminate EAP requests and perform identity management system lookups.

Identity Management System

The Identity Management System of eduroam IdPs contains the information of the end users; for instance usernames and passwords. They must be kept up-to-date by the responsible IdP. An IdP RADIUS server will query the Identity management system to parform the actual authentication for a user as he tries to log in.

Supplicants

A supplicant is a piece of software (often built into the Operating System but also available as a separate program) that uses the 802.1X protocol to send authentication request information using EAP. Supplicants are installed and operate on end-user computing devices (e.g. notebooks, PDAs, WiFi-enabled cell phones, and so on).

Access Points

Access Points are Wireless LAN access devices conformant to IEEE 802.11 and need to be IEEE 802.1X capable. They must be able to forward access requests coming from a supplicant to the SP RADIUS server, to give network access upon proper authentication, and to possibly assign users to specific VLANs based on information received from the RADIUS server. Furthermore Access Points exchange keying material (initialisation vectors, public and session keys, etc.) with client systems to prevent session hijacking.

Switches

Switches need to be able to forward access requests coming from a supplicant to the SP RADIUS server, to grant network access upon proper authentication and to possibly assign users to specific VLANs based on information received from the RADIUS server.