iLight/GigaPoP eduroam Discussion

Campus Network Engineering

By: James W. Dickerson Jr.
May 10, 2017

INDIANA UNIVERSITY

What is eduroam?

- eduroam (education roaming) is an international roaming service for users in research, higher education and further education.
- Authentication of users is performed by their home institution, using the same credentials as when they access the network locally, while authorization to access the Internet and possibly other resources is handled by the visited institution.

What is eduroam?

- Having started in Europe, eduroam has gained momentum throughout the research and education community and is now available in 72 territories.
- The authentication of a user is carried out at their Identity Provider (IdP), using their specific authentication method.
  - eduroam IdPs operate a RADIUS server which is responsible for authenticating its own users, by checking the credentials against a local identity management system.

What is eduroam?

- The authorization decision allowing access to the network resources upon proper authentication is done by the Service Provider (SP), typically a WiFi hotspot (University campus, etc.).
  - 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.

How Does It Work?

- eduroam requires that the chosen EAP method must allow
  - mutual authentication (i.e. the user can verify that he is connected to "his" IdP whereever the user is
  - encryption of the credentials used (i.e. only the user and his IdP will see the actual credential exchange; it will be invisible to the Service Provider and all intermediate proxies)

How Does It Work?

- Some popular EAP methods in use in eduroam are:
  - PEAP ("Protected EAP") - a Microsoft protocol that establishes a TLS tunnel, and sends usernames and passwords in MS-CHAPv2 hashes inside)
  - TTLS ("Tunneled TLS") - an IETF protocol that establishes a TLS tunnel, and sends usernames and passwords in multiple configurable formats inside)
  - TLS ("Transport Layer Security") - an IETF protocol that authenticates users and the IdP with two X.509 certificates
  - FAST ("Flexible Authentication via Secure Tunneling") - a Cisco protocol that establishes a TLS tunnel, and sends usernames and passwords in a custom way inside)

How Does It Work?

» eduroam allows any user from an eduroam participating site to get network access at any institution connected to eduroam. Depending on local policies at the visited institutions, eduroam participants may also have additional resources at their disposal.

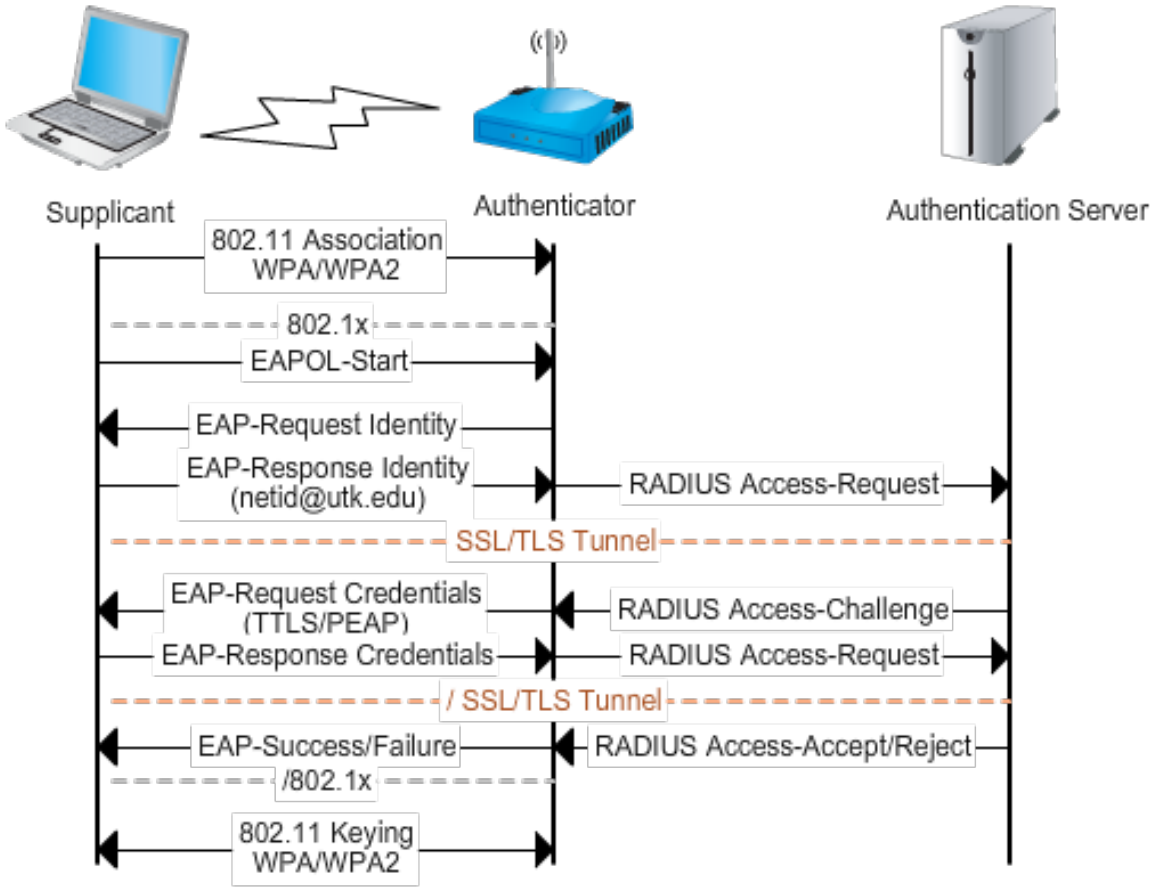
How Does It Work?

» The user credentials are kept secure because eduroam does not share them with the site you're visiting. Instead they are forwarded to the user's home institution, where they can be verified and validated.

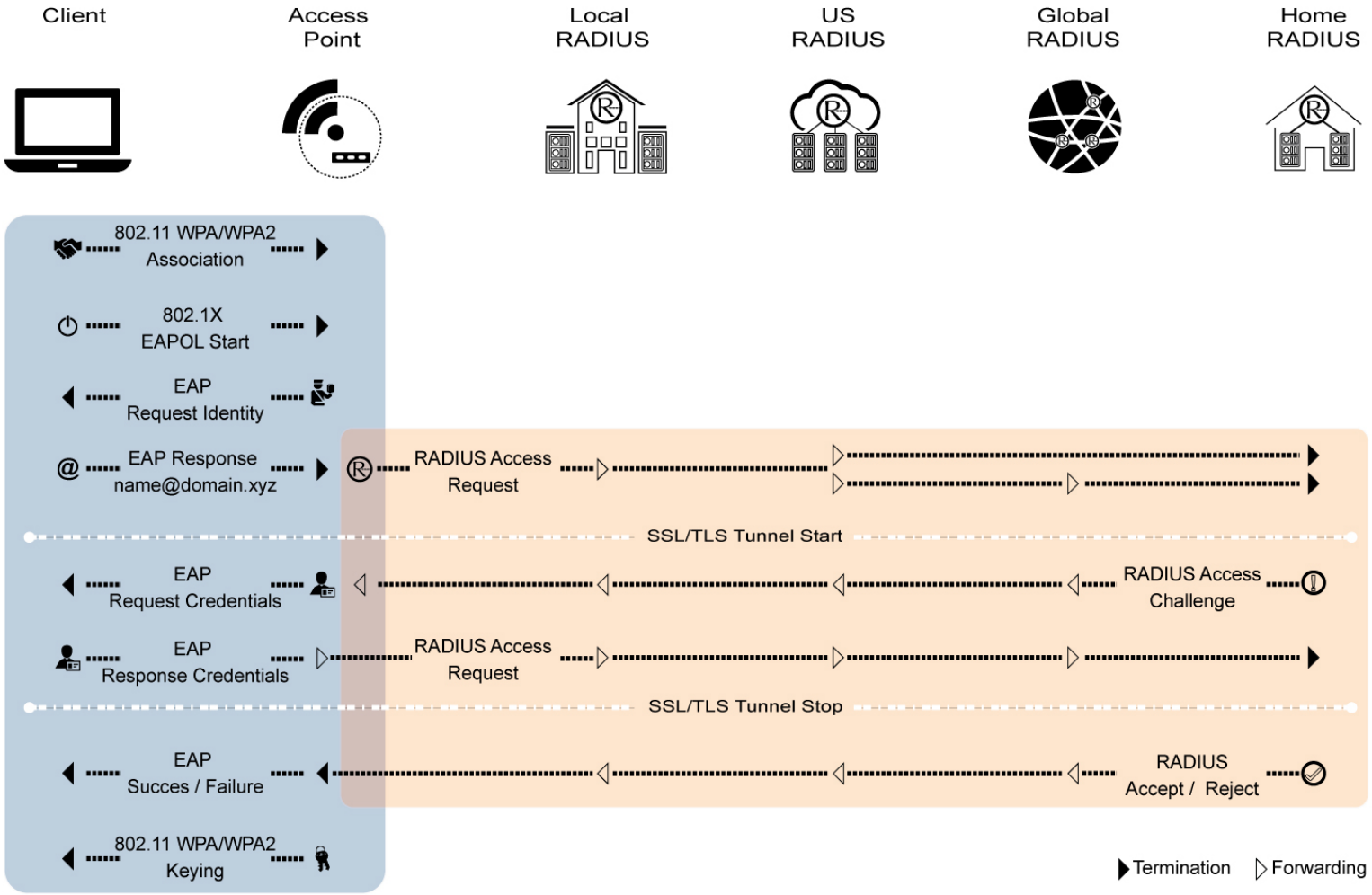
How Does It Work?

» The system uses a network of servers run by the institutions, and the participating National Research and Education Networks (NRENs) to securely route these requests back to your home institute. All this happens seamlessly and virtually instantly – all thanks to eduroam!

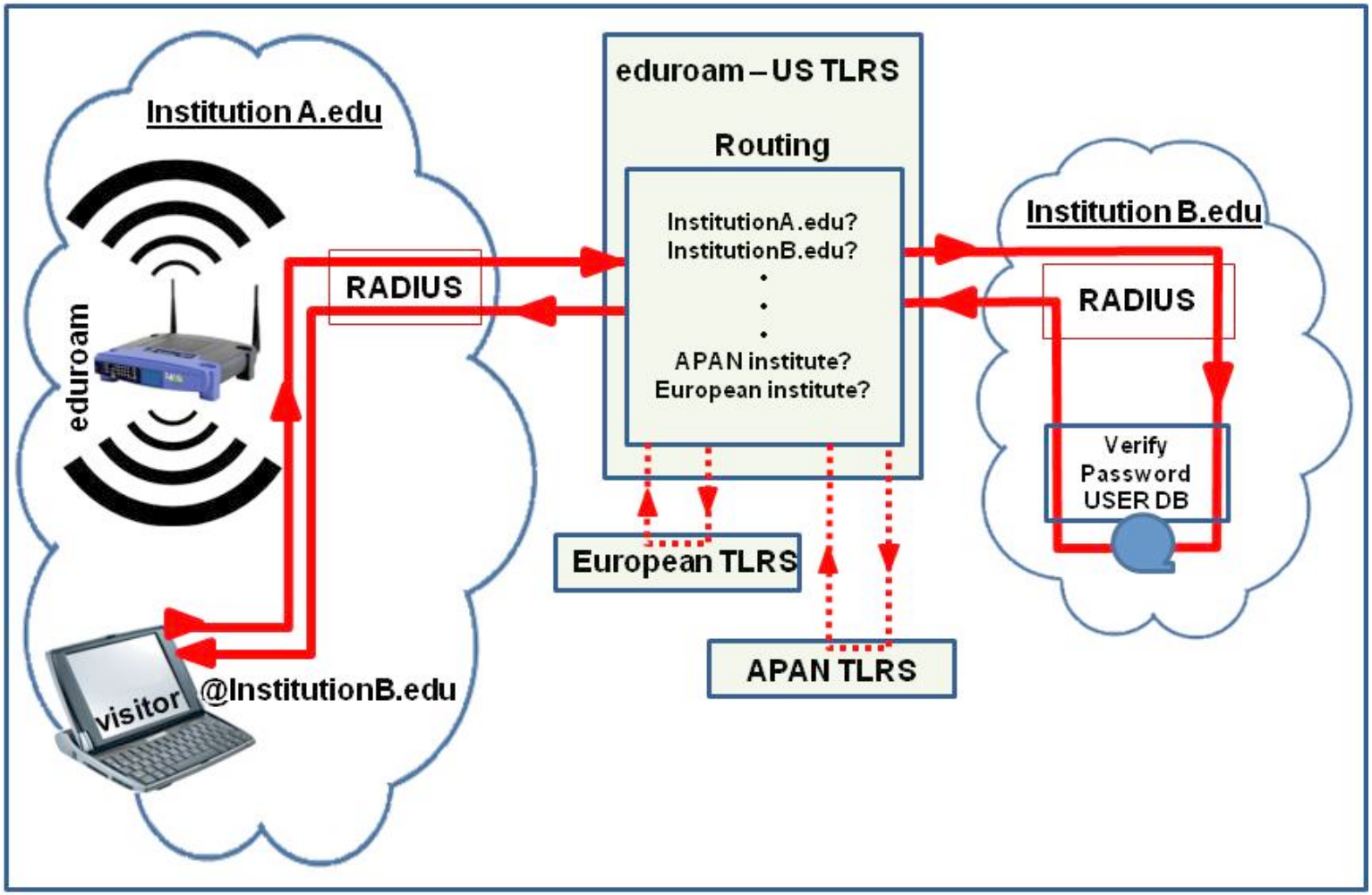
How Does It Work?



How Does It Work?



How Does It Work?



Advantages of Eduroam

- eduroam is based on the most secure encryption and authentication standards in existence today. Its security by far exceeds typical commercial hotspots.
- Be aware though that when using the general Internet at an eduroam hotspot, the local site security measures at that hotspot will apply to you as well. For example, the firewall settings at the visited place may be different from those you are used to at home, and as a guest you may have access to fewer services on the Internet than you have at home.

Advantages of Eduroam

- eduroam requires the use of 802.1x which provides end-to-end encryption to ensure that your private user credentials are only available to your home institution.
- The certificate of your home institution is the only point you need to trust regardless of who operates any intermediate infrastructure.

Configuration & Tools

- https://wiki.geant.org/display/H2eduroam/eduroam+set+up
- https://www.eduroam.us/
- https://cat.eduroam.org/

Sources

- https://en.wikipedia.org/wiki/Eduroam
- https://www.eduroam.org/what-is-eduroam/
- https://www.eduroam.org/eduroam-security/
- https://www.incommon.org/eduroam/faq.html
- https://www.eduroam.us/node/10