EDUROAM

HEZRON MWANGI
Systems Administrator
hmwangi@kenet.or.ke

2nd May 2014

What is Eduroam?

- Eduroam stands for EDUcation ROAMing.
- Eduroam is the secure, world-wide roaming access service developed for the international research and education community.
- Eduroam allows students, researchers and staff from participating institutions to obtain Internet connectivity across campus and when visiting other participating institutions by simply opening their laptop.

eduroam

kenet
Kenya Education Network

About Eduroam

- The eduroam initiative started in 2003 within TERENA's Task Force on Mobility, TF-Mobility.
- The task force created a test bed to demonstrate the feasibility of combining a RADIUS-based infrastructure with 802.1X standard technology to provide roaming network access across research and education networks.
- eduroam allows any eduroam-enabled user to get network access at any institution connected to eduroam.
- Today eduroam is a federation of federations (confederation); single federations are run at national level and they are all connected to a regional confederation.

eduroam

kenet
Kenya Education Network

Eduroam Infrastructure

- Eduroam technology is based on 802.1X standard and a hierarchy of RADIUS proxy servers.
- The role of the RADIUS hierarchy is to forward the users' credentials to the users' home institution, where they can be verified and validated.
- When a user requests authentication, the user's realm determines where the request is routed to.
- The realm is the suffix of the user-name, delimited with '@', and is derived from the organisation's DNS domain name.

eduroam

kenet
Kenya Education Network

Eduroam Infrastructure Cont'd

- Every institution that wants to participate in eduroam connects its institutional RADIUS-server to the national top-level RADIUS (NTLR) server of the country where the institution is located.
- The NTLR is normally operated by the National Research and Education Network (NREN) of that country.
- The country-level servers have a complete list of the participating eduroam institutions in that country.
- This is sufficient to guarantee national roaming.
- For international roaming, a regional top-level RADIUS server is needed in order to roam the users request to the right country.

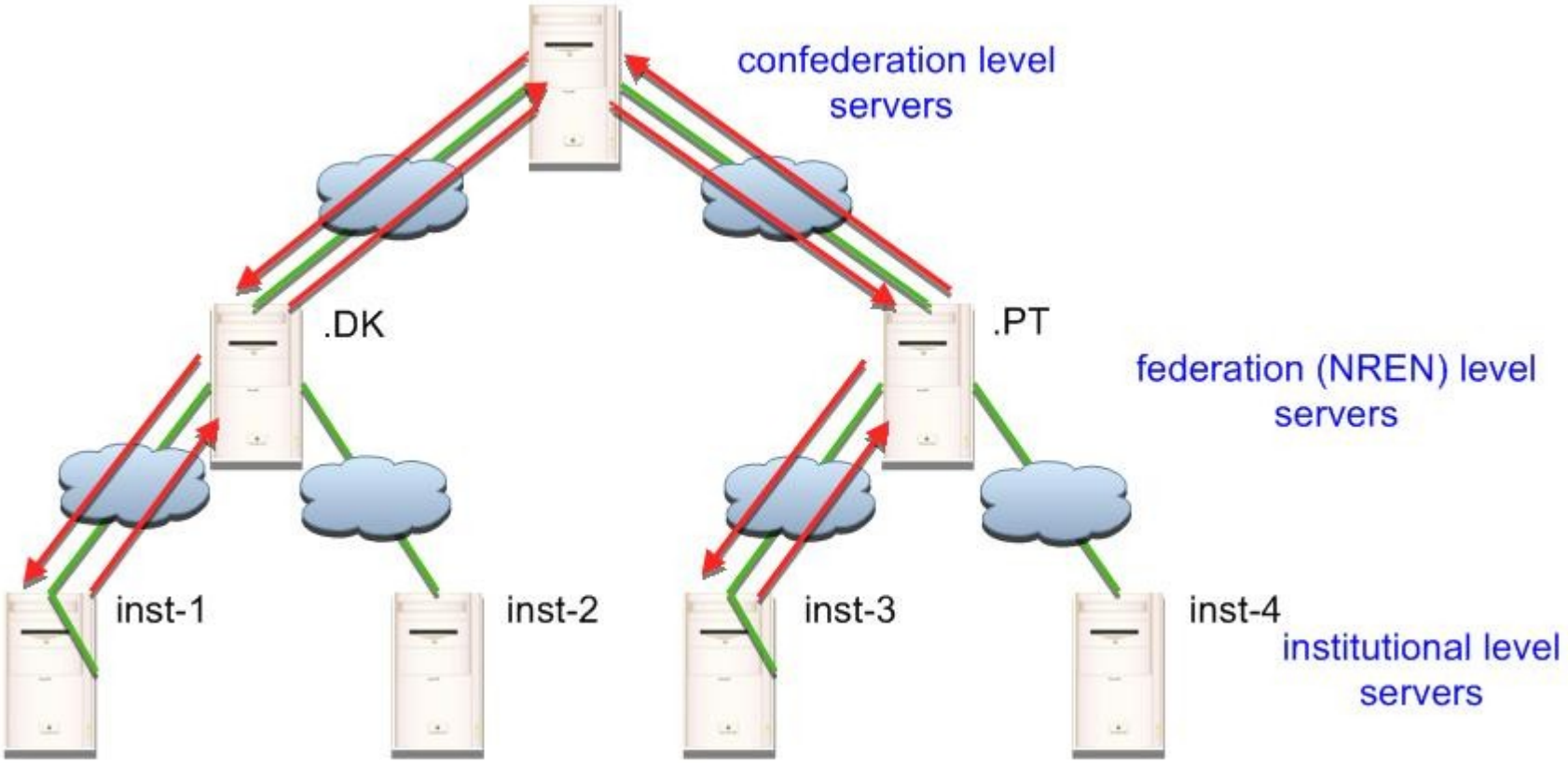
eduroam

kenet
Kenya Education Network

Elements of the eduroam infrastructure

- Confederation top-level RADIUS Server (TLR)
- Federation-Level RADIUS servers (FLRs)
- IdP and SP RADIUS infratructure
- Identity Management System
- Supplicants
- Access Points
- Switches

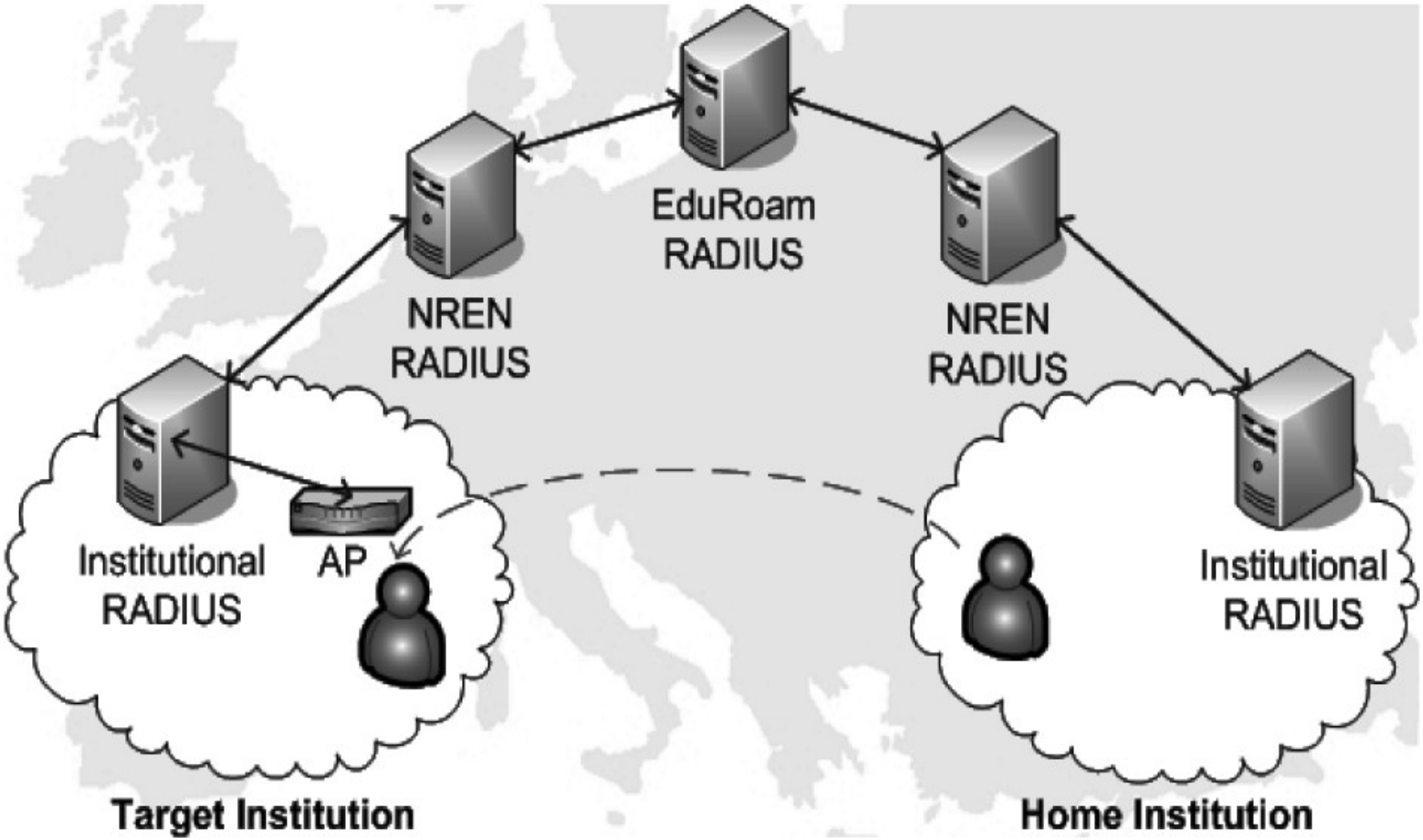
Hierarchy of Radius Servers



eduroam

kenet
Kenya Education Network

Hierarchy of Radius Servers



eduroam

kenet
Kenya Education Network

Overview of Eduroam

- RADIUS servers connect to each other dynamically using the protocol RADIUS/TLS.
- The access points or switches use the IEEE 802.1X standard that encompasses the use of the Extensible Authentication Protocol (EAP).
- EAP is a container that carries the actual authentication data inside, the so-called EAP methods. There are many EAP methods an IdP can choose from.
- 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)

eduroam

kenet
Kenya Education Network

EAP Methods

- 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).

EAP Methods Cont'd

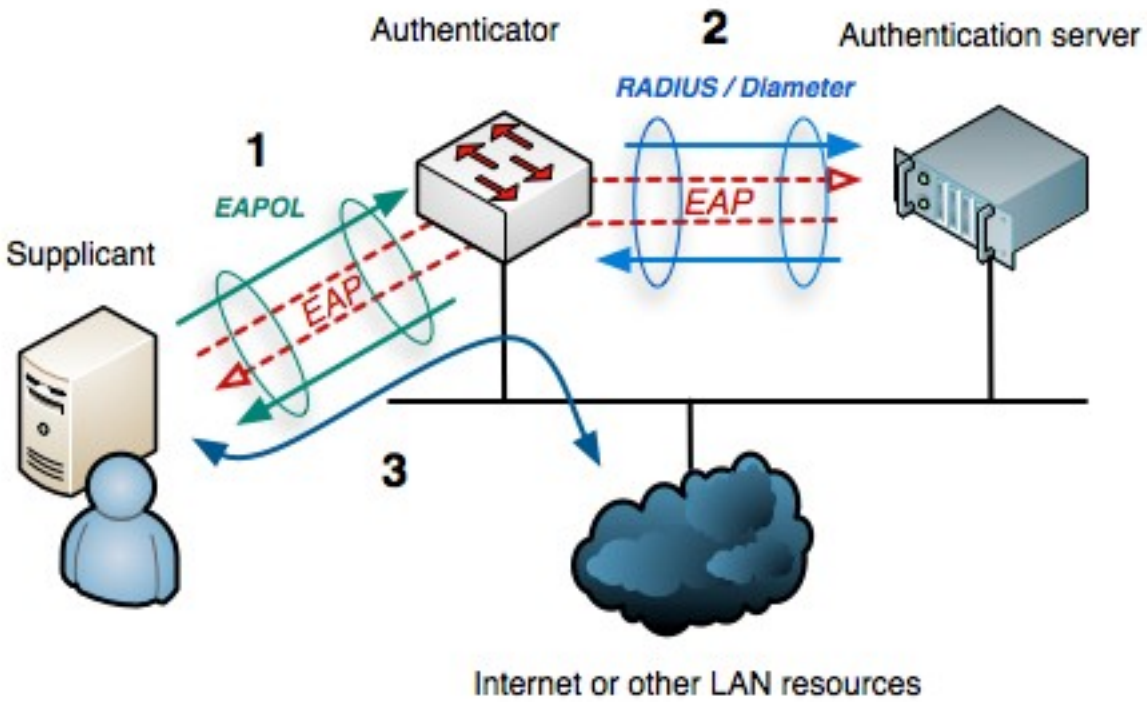
- RADIUS transports the user's name in an attribute User-Name, which is visible in cleartext to all intermediate hosts on the way.
- Some EAP methods allow to put a different User-Name into the RADIUS packet than in the EAP payload. In that case, the following terms are used:
    - outer identity: this is the User-Name in the RADIUS packet and visible to all intermediate parties
    - inner identity: this is the actual user identificator. It is only visible to the user himself and the Identity Provider

EAP Methods Cont'd

- When using such EAP methods, the real username is not visible in RADIUS (it will only see the outer identity). Doing so will enhance the user's privacy, and is encouraged.
- Outer identities should be in the format "@realm" (nothing left of the @ sign.
- The realm part still must be the correct one as it is used to route the request to the respective Identity Provider.
- Once the IdP server decrypts the TLS tunnel in the EAP payload, it gets the inner identity and can authenticate the user.
- After successful authentication by the Identity Provider and authorisation by the Service Provider, this SP grants network access to the user, possibly by placing the user in a specific VLAN intended for guests.

Architectural Components

- Database of Users
- Authentication server (Radius)
- Access Point (authenticator)
- Supplicant (module to authenticate)



eduroam

kenet
Kenya Education Network

Database Options

- LDAP
- SQL
- Active Directory
- Text File
- RADIUS

Advantages of database Authentication

- Centralized management
- Enhanced security
- Detailed logs (Accounting)
- Scalable architecture
- RADIUS open protocol

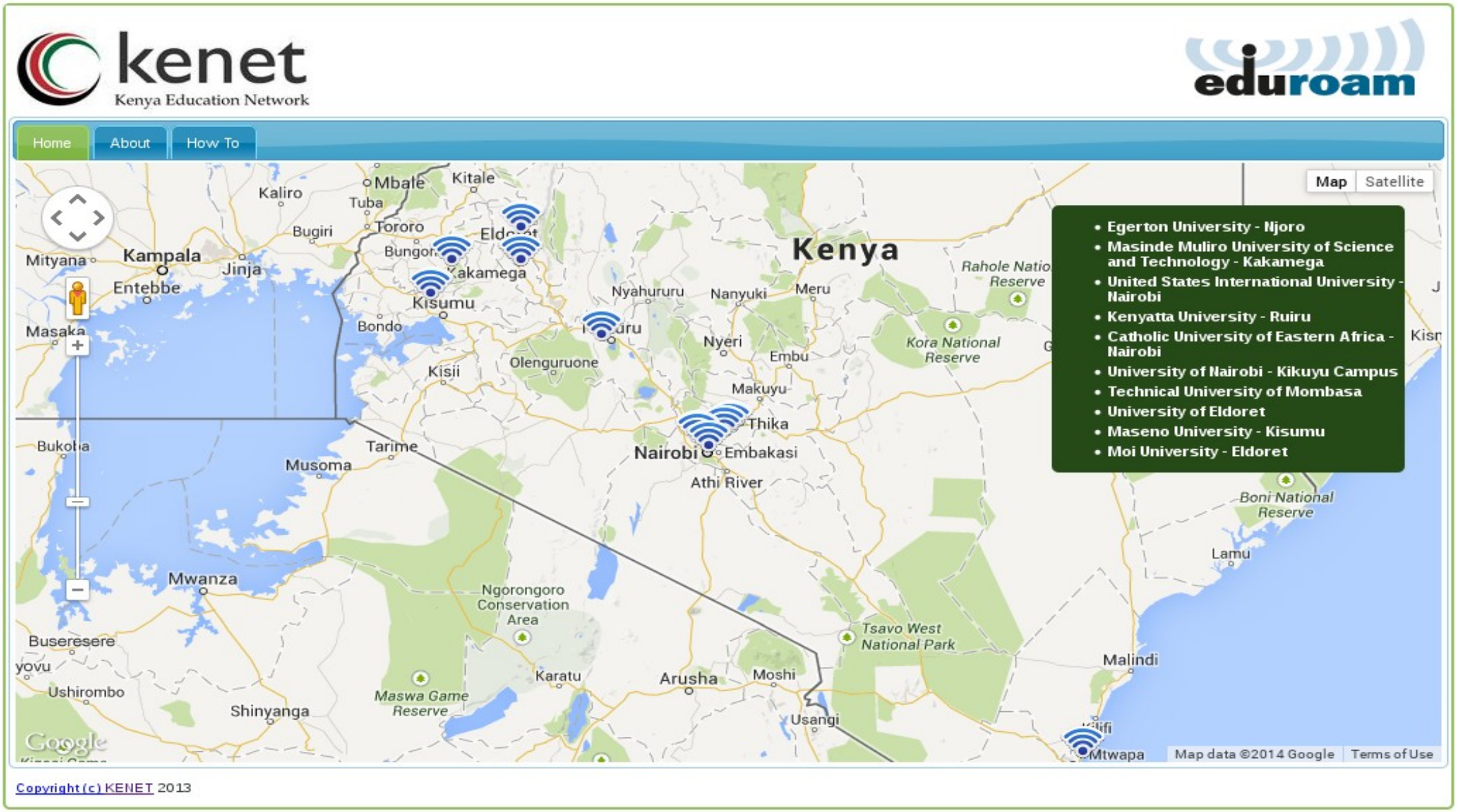
eduroam

kenet
Kenya Education Network

Challenges

- Updating database with current details.
- RADIUS configuration may be challenging.
- Some existing databases do not have ldap compatibility.

Where is eduroam?



Where is eduroam?

Having started in Europe, eduroam has gained momentum throughout the research and education community world wide and is now available in 60 territories world wide.

eduroam

kenet
Kenya Education Network

Q/A

THANK YOU!