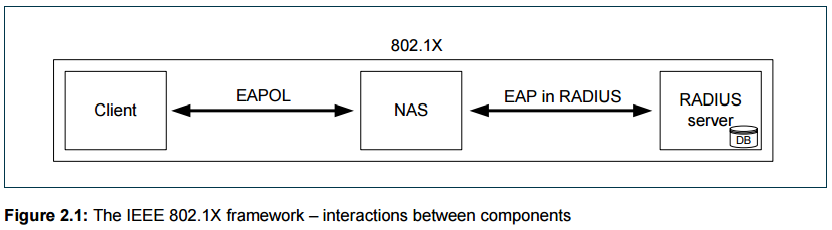
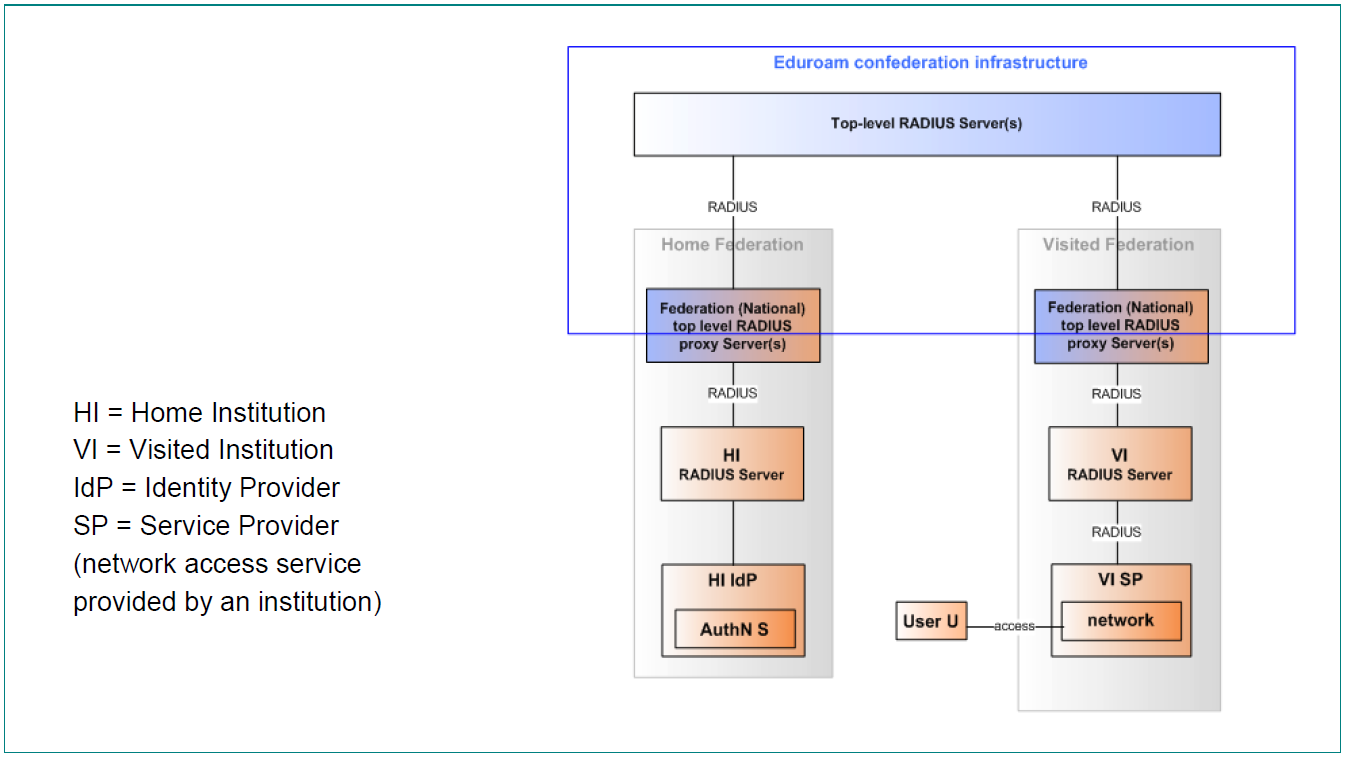
Eduroam技术架构

Eduroam的技术基础是802.1X标准和层次化的RADIUS代理服务器。它允许来自于某个eduroam机构的用户在支持eduroam的伙伴机构中获得使用无线网络的权限。为访客提供eduroam无线网络的机构可以针对eduroam访客设置自己的管理策略。

下图展示了802.1X和RADIUS的基本关系。其中，Client为用户终端/Supplicant，NAS为用户要接入无线网络的无线控制器，RADIUS服务器为用户身份权威机构的认证服务器。



RADIUS层次架构如下图所示，其中的Home Institution为eduroam idp（用户身份权威机构）。Visited Institution为eduroam sp（用户访问机构）。IdP/HI通过所在国家的顶级RADIUS proxy Server、顶级RADIUS Server和SP所在国家的顶级RADIUS proxy server与SP/VI建立通道，完成用户在访问机构的认证过程，支持用户接入访问机构的eduroam网络。



RADIUS层次架构的作用是：把用户身份转发到用户身份所属的机构，在那里验证用户身份的有效性。通常，eduroam采用的用户身份描述方式是“uid@realm”，其中的“uid”是用户在身份权威机构的本地身份，“realm”是机构域名。比如一个北京大学用户的eduroam id是[testuid@pku.edu.cn](mailto:testuid@pku.edu.cn)。RADIUS层次架构的转发动作依据realm（即pku.edu.cn）完成。

从逻辑上看，Client和NAS在用户作为访客所在的网络中，RADIUS服务器在用户身份权威机构中。用户访问机构和用户身份权威机构可以是任何支持eduroam的机构，可以是一个国家中两个不同的机构，也可以是在不同国家中。



Eduroam逻辑架构

每一个想要加入eduroam的机构需要把它的RADIUS服务器连接到所在国家的FLR（Federation Level RADIUS服务器）。FLR通常由国家教育科研网运行。FLR有这个国家中参加eduroam机构的完整清单。通过这种机制保证了不同国家eduroam机构之间的成功漫游。

对于国际漫游来讲，还需要配置地区级别的顶级RADIUS服务器，它的作用是实现地区之间的用户请求漫游。目前，两个顶级TLR（Top Level RADIUS）部署在欧洲。中国和TLR之间的逻辑关系如下图所示。



图 eduroam@cn和全球eduroam TLR的逻辑关系

下面以北京大学某位老师到欧洲某个学校访问为例，演示eduroam工作流程。首先，北京大学的某位老师到欧洲访问，希望通过当地的eduroam无线网络接入到互联网。当地eduroam无线网络的RADIUS服务器@tenera.nl检测到有id为testuid@pku.edu.cn的用户申请使用eduroam，根据realm（pku.edu.cn），通过RADIUS服务器的层次关系和TLR找到.cn的RADIUS服务器，进一步找到.edu.cn和pku.edu.cn的RADIUS服务器。pku.edu.cn的RADIUS服务器验证用户身份。验证结果以同样的路径返回到@tenera.nl的RADIUS服务器，允许用户接入当地eduroam无线网络。



图 eduroam工作流程样例