Infrastructure requirements for eduroam subscribers

While the equipment needed to deploy eduroam is, for most organizations, minimal and inexpensive there are four components which are hard requirements. Here is an overview of those four required components.

Wired network infrastructure

What:

- Network connectivity to site
- Local network (wiring, PoE switches)

Why: Because eduroam is a means for authenticating access to existing networks and **not** a network itself, your institution will need to have an internet connection. You will also need to have a local network set up and ready to provide connectivity for wireless access points. Your local network and internet connection must have sufficient capacity to serve your staff, student, and/or teacher users.

802.1x Enterprise compliant wireless infrastructure

What:

- Wireless APs, 802.1x Enterprise compliant
- Controller or management system for wireless APs

Why:

802.1x is a wireless security protocol that is the basis for the eduroam service. It allows operators of wireless networks to authenticate users, ensuring that they are who they say they are and provides your staff with some basic information about their use of the network to help with troubleshooting or dealing with abusive behavior.

This means it's a requirement that your wireless access points be able to support the 802.1x protocol. Fortunately, many current enterprise grade access points are 802.1x compliant right out of the box (please note that most consumer grade access points may **not** be 802.1x compliant). You may need to check your wireless APs and controllers or management system are all 802.1x compliant.

Identity store

What:

- An authentication server (Microsoft Active Directory, LDAP, Google ID, Kerberos, Samba, etc)
- User accounts populated onto server

Why:

Because authenticating users is core to eduroam, your institution will need to have an identity store to handle that authentication process for your staff, faculty, or students. This is fairly straightforward if you're already using an authentication service like Microsoft Active Directory or Open LDAP for managing access to email or other staff resources. Use of these servers for the eduroam service is a fairly simple and straightforward process. If you're relying on a Student Information Service (SIS) to handle access to learning resources you'll need to stand up a dedicated server to use eduroam.

RADIUS Server

What:

- Server running a variant of RADIUS (FreeRADIUS, Microsoft NPS, ClearPass, etc)
- Configurations made to the local network to allow it to route authentication requests

Why:

RADIUS is an authentication protocol which is central to how eduroam operates. It's responsible for taking a user request to access a network, sending it back to the user's home institution where it can be approved or denied, and then routing the answer back to where the user is trying to access the network. Your local network must be able to send and receive RADIUS traffic for eduroam to work. RADIUS does not require much computing power to operate and the needed configuration updates to your network are simple and safe.