Why Institute for Advanced Study Joined this Global Secure Wireless Initiative and Why You Should Too
The Institute for Advanced Study is one of the world’s leading centers for theoretical research and intellectual inquiry. The Institute exists to encourage and support curiosity-driven research in the sciences and humanities—the original, often speculative thinking that produces advances in knowledge that change the way we understand the world.

Currently, a permanent Faculty of approximately thirty eminent academics guides the work of the Schools and each year awards fellowships to some two hundred visiting Members, from about one hundred universities and research institutions throughout the world.
Secure wireless when IAS Scholars travel

Secure wireless for visitors to IAS campus
Library resources Princeton University

PU Guest only allowed access 1 week/mo!
What?
Where?
Why?
How?
eduroam (education roaming) 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 (education roaming) is the secure, world-wide roaming access service developed for the international research and education community.

Use your school's Wi-Fi authentication at any eduroam hotspot in the world and join instantly and securely.
Globally

74 territories
Nationally

451 Institutions via I2
Regionally

Princeton University
Institute for Advanced Study
Rutgers (NB)
Future: Your Institution
Future: NJEDge events
3 in NJ
IAS: eduroam users came from **152** unique institutions
eduroam user experience

Open laptop/device
Select SSID = eduroam
Connection!
eduroam - benefits for IT

Eliminates guest accounts

Can still control bandwidth

Improves security for visitors

Allows access resource control
IT Time Investment

Existing 802.1X SSID? ~2 Hours
IT Financial Investment

Cost for NJEDge/I2 members

Nada
5 Easy Step to Set up eduroam

1. Submit a request to join at www.eduroam.us
2. Exchange IP address & shared radius secret with eduroam.us
3. Connect your radius server to eduroam-US federation
4. Broadcast a 802.1X ssid called eduroam
5. Advertise the service to your community
Jargon Alert!

Service Provider (SP)

Identity Provider (IDP)
Broadcasting SSID eduroam

Configured eduroam access to internet

Forwarding radius request up eduroam chain

Can be any organization
Peers with eduroam radius servers
Radius connects to directory services
Authenticate user’s credentials
Can only be academic institution
No Radius

Service Provider

Identity Provider
user@ias.edu on IAS Campus

IAS

Service Provider (SP)

Identity Provider (IDP)
eduroam is a federation of radius servers
User credentials are never seen by SP
Implementation

Create a new radius pool for eduroam.us radius servers

Exchange radius secrets with eduroam.us

Broadcast 802.X SSID called eduroam

Add eduroam to 802.1X provisioning tool
Adding eduroam to radius

# Creating eduroam server pool in FreeRadius

```plaintext
home_server_pool eduroam {
  type = fail-over
  home_server = tlr1.eduroam.us
  home_server = tlr2.eduroam.us
}
```
Configuring the user device

eduroam Configuration Assistant Tool (CAT)
https://cat.eduroam.edu
Configuring CAT
Choose an installer to download

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Installer Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS Windows 10</td>
<td>i</td>
</tr>
<tr>
<td>MS Windows 8, 8.1</td>
<td>i</td>
</tr>
<tr>
<td>MS Windows 7</td>
<td>i</td>
</tr>
<tr>
<td>MS Windows Vista</td>
<td>i</td>
</tr>
<tr>
<td>Apple OS X El Capitan</td>
<td>i</td>
</tr>
<tr>
<td>Apple OS X Yosemite</td>
<td>i</td>
</tr>
<tr>
<td>Apple OS X Mavericks</td>
<td>i</td>
</tr>
<tr>
<td>Apple OS X Mountain Lion</td>
<td>i</td>
</tr>
<tr>
<td>Apple OS X Lion</td>
<td>i</td>
</tr>
<tr>
<td>Apple iOS mobile devices (iOS 7 and above)</td>
<td>i</td>
</tr>
<tr>
<td>App's iOS mobile devices (iOS 5 and 6)</td>
<td>i</td>
</tr>
<tr>
<td>Linux</td>
<td>i</td>
</tr>
<tr>
<td>Chrome OS</td>
<td>i</td>
</tr>
<tr>
<td>Android 6.0 Marshmallow</td>
<td>i</td>
</tr>
<tr>
<td>Android 5.0 Lollipop</td>
<td>i</td>
</tr>
<tr>
<td>Android 4.4 KitKat</td>
<td>i</td>
</tr>
<tr>
<td>Android 4.3</td>
<td>i</td>
</tr>
<tr>
<td>EAP</td>
<td>i</td>
</tr>
<tr>
<td>EAP config</td>
<td>i</td>
</tr>
</tbody>
</table>
CAT isn’t a WPA2 supplicant

MS Windows 7 and Vista do not come with a WPA2 supplicant
Properly configures user’s credentials (user@institution)

Installs digitally signed cert by TERENA.

Configures security settings on your device

Reduce Help Desk Calls
eduroam is a federation built on Trust
All eduroam users have signed an user compliance statement.
eduroam is a federation of radius servers
Outer Tunnel

Packet identifier: 0x2a (42)
Length: 210

Authenticator: b0969b7f08729e109ac645e06ca57dfe
[The response to this request is in frame 31]

Attribute Value Pairs
- AVP: l=19 t=User-Name(1): anonymous@ias.edu
- AVP: l=6 t=Framed-MTU(12): 1400
- AVP: l=24 t=Called-Station-Id(39): 64ae.0c57.d4a0:eduroam
- AVP: l=16 t=Calling-Station-Id(31): 10bf.4896.aaa6

Frame (frame), 252 bytes  Packets: 68 · Display... Profile: Default
Inner Tunnel TLS
### Inner Tunnel TLS Credentials

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Time</th>
<th>Source IP</th>
<th>Destination Port</th>
<th>Type</th>
<th>Access-Request/Access-Accept (id)</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 2015-11-17 22:32:31.462</td>
<td>192.168.0.50</td>
<td>64.57.22.74</td>
<td>RADIUS</td>
<td>339</td>
<td>Access-Request(1)(id=49)</td>
</tr>
<tr>
<td>17 2015-11-17 22:32:31.545</td>
<td>64.57.22.74</td>
<td>192.168.0.50</td>
<td>RADIUS</td>
<td>213</td>
<td>Access-Accept(2)(id=49)</td>
</tr>
</tbody>
</table>

**Secure Sockets Layer**

- **TLSv1 Record Layer**: Application Data Protocol: Application Data
  - Content Type: Application Data (23)
  - Version: TLS 1.0 (0x0301)
  - Length: 80

**Encrypted Application Data**: `8792756cf37f21aa9821a3817dcd72166bbae5025a321d4...

- **AVP**: l=6 t=NAS-Port-Type(61): Wireless-002.11(19)
- **AVP**: l=6 t=NAS-Port(5): 279
- **AVP**: l=6 t=NAS-Port-Id(87): 279
- **AVP**: l=18 t=State(24): cc57b7d4ca5f12e3ac82b4110b115453
- **AVP**: l=6 t=NAS-IP-Address(4): 192.168.0.50

Payload is encrypted application, Packets: 68, Displayed: 68 (100.0%), Load time: 0s, Profile: Default
## 802.1X Encryption: EAP

<table>
<thead>
<tr>
<th>EAP-Type</th>
<th>Native Supplicant Support</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
</table>
| FAP-TLS   | Windows (XP, Vista, 7), Mac OS X, Linux, iOS (iPhone, iPod Touch, iPad), Android (v1.6+) | • Validates client as well as infrastructure  
• Reduced risk of being Phished  
• Blocking user access is via certificate revocation | • PKI infrastructure is required  
• Users must configure supplicant to use certificate  
• Identity may be exposed in TLS exchange depending on contents of certificate |
| EAP-TTLS  | Mac OS X, Linux, iOS (iPhone, iPod Touch, iPad), Android (v1.6+)                        |                                                                      | • No native supplicant support on Microsoft Windows  
• Potential for Man-in-the-Middle attacks |
| EAP-PEAP  | Windows (XP, Vista, 7), Mac OS X, Linux, iOS (iPhone, iPod Touch, iPad), Android (v1.6+) | • Works on many platforms                                           | • Potential for Man-in-the-Middle attacks  
• Identity may be exposed during Phase 1 of exchange |
RFC5281 states that "When either client or server receives a certificate as part of the TLS handshake, it should validate the certification path to a trusted root."
eduroam @
conference.njedge.net/2015/
https://www.youtube.com/watch?v=TVCmcMZS3uA&feature=youtu.be