Federated Wi-Fi Access for Scholars Worldwide: Costs & Benefits
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
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

76 territories
Nationally

418 Institutions
IAS (summer 2015) 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
5 Easy Step to Set up eduroam

1. Submit a request to join at [www.eduroam.us](http://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)
Service Provider

- Broadcasting SSID eduroam
- Configured eduroam access to internet
- Forwarding radius request up eduroam chain

Can be any organization
Identity Provider

- Peers with eduroam radius servers
- Radius connects to directory services
- Authenticate user’s credentials

Can only be academic institution
user@ias.edu on IAS Campus

IAS

Service Provider (SP)

Identity Provider (IDP)
user@ias.edu on Princeton U

Princeton University

Service Provider (SP)

IAS

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
- Broadcast 802.X SSID called eduroom
- Exchange radius secrets with eduroam.us via OpenPGP
- Add eduroom to 802.1X provisioning tool
Configuring the user device

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

<table>
<thead>
<tr>
<th>Windows</th>
<th></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></td>
</tr>
<tr>
<td>MS Windows Vista</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Apple OS X</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>El Capitan</td>
<td>i</td>
</tr>
<tr>
<td>Yosemite</td>
<td>i</td>
</tr>
<tr>
<td>Mavericks</td>
<td>i</td>
</tr>
<tr>
<td>Mountain Lion</td>
<td>i</td>
</tr>
<tr>
<td>Lion</td>
<td>i</td>
</tr>
<tr>
<td>iOS mobile devices (iOS 7 and above)</td>
<td>i</td>
</tr>
<tr>
<td>iOS mobile devices (iOS 5 and 6)</td>
<td>i</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Linux</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chrome OS</th>
<th></th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>EAP</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>EAP config</td>
<td>i</td>
</tr>
</tbody>
</table>
Properly configures user’s credentials

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

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2015-11-17 22:32:25.592</td>
<td>Cisco_5a:ab:6a</td>
<td>Cisco_5a:ab:6a</td>
<td>LOOP</td>
<td>50</td>
</tr>
<tr>
<td>2</td>
<td>2015-11-17 22:32:30.745</td>
<td>192.168.0.50</td>
<td>64.57.22.74</td>
<td>RADIUS</td>
<td>252</td>
</tr>
<tr>
<td>3</td>
<td>2015-11-17 22:32:30.986</td>
<td>64.57.22.74</td>
<td>192.168.0.50</td>
<td>RADIUS</td>
<td>106</td>
</tr>
</tbody>
</table>

Packet identifier: 0x2a (42)
Length: 210

Authenticator: b0969b7f08729e109ac645e06ca57dfe

[The response to this request is in frame 3]

- 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(30): 64ae.0c57.d4a0:eduroam
  - AVP: l=16 t=Calling-Station-Id(31): 10bf.4806.aaa6

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

Handshake Type: Certificate (11)
  Length: 3042
  Certificates Length: 3039
  Certificates (3039 bytes)
    Certificate Length: 1282
      Certificate (pkcs-9-at-emailAddress=network@ias.edu,id-at-commonName=radius.ias.edu,id-at-commonName=IAS Certificate Authority,pkcs-9-at-emailAddress=network@ias.edu)
        Certificate Length: 1751
        Certificate (id-at-commonName=IAS Certificate Authority,pkcs-9-at-emailAddress=network@ias.edu)

  TLSv1 Record Layer: Handshake Protocol: Server Key Exchange
  TLSv1 Record Layer: Handshake Protocol: Server Hello Done
  AVP: l=18 t=Message-Authenticator(80): 085db9a55a49a733494968d5d6b0c09b

Text item (text), 253 bytes
Packets: 68 · Displayed: 68 (100.0%) · Load time: 0:... · Profile: Default
Inner Tunnel TLS Credentials

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: 8792756cf37f21aaa9821a3817dcd72166bbae6825a321d4...
- AVP: l=6 t=NAS-Port-Type(61): Wireless-802.11(19)
- AVP: l=6 t=NAS-Port(5): 279
- AVP: l=5 t=NAS-Port-Id(87): 279
- AVP: l=18 t=State(24): cc5707d4ca5f12e3ac82b4110b115463
- AVP: l=6 t=NAS-IP-Address(4): 192.168.0.50
- AVP: l=8 t=NAS-Identifier(32): ep1142

Payload is encrypted

Packets: 68 • Displayed: 68 (100.0%) • Load time: 0:...
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>
| EAP-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 |
Inner Tunnel

- CHAP
- MSCHAP
- MSCHAPv2
- PAP
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 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.