eduroam AU: Status and Directions

Neil Witheridge
Authentication & Authorisation Services
Technical Manager
AARNet

This work is licensed under a Creative Commons Attribution 4.0 International License.
Quick Recap: “What is eduroam”

eduroam = common SSID “eduroam”, 802.1x, RADIUS using Realms for Remote Authentication
Quick Recap: “What is eduroam”

eduroam = common SSID “eduroam”, 802.1x, RADIUS using Realms for Remote Authentication

1. Authentication
2. Access

End-user Device

username@oxford.ac.uk
password

eduroam User-Name is institutional username + user’s ‘realm’

Institutional RADIUS Server

Institutional RADIUS Server

Top-Level RADIUS Server

Top-Level RADIUS Server

National RADIUS Server

National RADIUS Server

Wireless Access Point

Visited Institution Service Provider (SP)

1st May 2015

eduroam AU Status and Directions - THETA2015

SLIDE 3 - COPYRIGHT 2015
Quick Recap: “What is eduroam”

- **Identity Federation**
  - Institutional identity management and authentication trusted based on policy compliance

- **Eduroam – Education Roaming**
  - WPA2-Enterprise, 802.1x
  - RADIUS, Tunneled EAP Protocol

- **NRO – National Roaming Operator (AARNet)**
  - NRS – National RADIUS Server
  - TLRS – Top Level (i.e. Regional) RADIUS Server

- **Institutional Participants (IdP+SP, SP-only)**
  - Identity Provider (IdP), user authentication
  - Service Provider (SP), provide network access
Quick Recap: eduroam Protocols

- Use of tunneled EAP for secure authentication

---

User visits institution & connects to visited institution network via eduroam

**WPA2/AES** (wireless encryption)
IEEE 802.1x (on 802.11)

**User's mobile device**
Configured to connect automatically to "eduroam" SSID

**Username@realm**
**Password**

**Visited Institution**
eduroam Service Provider

**Wireless Access Point**

**Home Institution**
eduroam Identity Provider

**IdP Institution**
RADIUS Server

**Regional/National RADIUS Servers**

**RADIUS**

**PEAP, TTLS** (encrypted tunnel)
Outer-authentication

**MSCHAPv2, PAP** (user authentication)
Inner-authentication

---

1st May 2015
eduroam AU Status and Directions - THETA2015
eduroam AU Current Status

- eduroam AU uptake
  - Currently 58 IdP+SP + 8 SP-only participants
  - Universities (100% AU Universities)
  - Research institutions (e.g. CSIRO, ANSTO)
  - Research service providers (e.g. INTERSECT)
  - Hospitals & Medical Research (e.g. NSW Health, SAHMRI)
  - Also several Colleges, TAFEs, K-12 Schools

- Eduroam Advisory Group
  - Extending eduroam AU footprint to High Schools

- Eduroam usage statistics (graphs on next slides)
Life-time Trend (start->1Q2015)

**IdP – remote authentications by ‘home’ institutions**

- Users travelling to AU institutions
- Users travelling to OS institutions

**SP – network accesses by visited institutions**

- Users from AU institutions
- Users from OS institutions
OS Visitors during 2014

Total: 27312
• eduroam is a Trust Federation
  – Trust is based on policy compliance
• eduroam Global Policy ("eduroam Compliance Statement")
  – Created by the Global eduroam Governance Committee
    • NROs must be a signatory and comply
    • Appendices describe technical req’s for IdPs and SPs
• eduroam AU Policy (current 4.2, not aligned with eCS)
  – Requirements for AU IdPs and SPs
• Institution’s network Acceptable Use Policy (AUP)
  – Users must comply with their home institution AUP
  – AUP embodies AARNet Access Agreement
Global eduroam Governance Committee

Secretary of GeGC: Brook Schofield (GEANT Association)

- Africa:
  Samia El Haddout, CNRST/MARWAN
  Simeon Miteff, SANReN/TENET

- Europe:
  Paul Dekkers, SURFnet
  Miroslav Milinović, SRCE
  Scott Armitage, Loughborough Uni

- Latin America:
  Leandro Marcos de Oliveira Guimares, RNP
  Alejandro Lara, REUNA

- North America:
  Chris Phillips, CANARIE
  Philippe Hanset, Internet2 (ANYROAM LLC operates on behalf of Internet2)

- Asia Pacific:
  Hideaki Goto, Tohoku University
  Neil Witheridge, AARNet

Non-voting technical experts:
Klaas Wierenga, Chair of TF-MNM (Mobility and Network Middleware)
Stefan Winter, RESTENA

Secretary of TF-MNM: Nicole Harris (GEANT Association)
eduroam AU Future Directions

• Improvements targeted

Administration

Device Configuration
Public vs Protected Info & Services

• Restricted access is required for:
  – Administration – deployment data entry
    – DjNRO Admin tool
  – End-User Support
    • Institutional Device Configuration set-up
      – Configuration Assistant Tool (CAT)
    • Test authentications for Troubleshooting
  – Detailed Institutional Usage Metrics
    • Who visited who, nationally & internationally

• Access via institution’s SAML IdP & AAF registration
  – Access via “AARNet Conext” (SURFnet’s OpenConext)
  – Use of VHO for admins without an IdP
eduroam Technical Trends

• Improvements in both WiFi and eduroam protocols to avoid problems
• Leveraging evolution of WiFi Protocols
  – Hotspot 2.0 (in particular, IEEE 802.11u)
• eduroam Protocols
  – evolving to deliver scalability and lower admin burden
  – RADIUS/TCP + TLS
    • TCP: avoid issues related to unreliable transport with UDP
    • TLS: secure the communication at the transport layer
  – Dynamic Discovery
    • Don’t rely on hierarchy defined in configuration
eduroam History in Asia Pacific (APAC)

- AU/NZ participation
  - Started with eduroam Project Group (2007-10)

- APAC countries currently participating:
  - Australia (.au), Hong Kong (.hk), India (.in), Japan (.jp), Korea (.kr), Macao (.mo), New Zealand (.nz), Taiwan (.tw), Singapore (.sg), Thailand (.th)

- Pending eCS Signing:
  - Philippines (.ph), Malaysia (.my),

- Have shown interest:
  - China (.cn), Papua New Guinea (.png)

- Planning to participate via AARNet:
  - Fiji/Oceania (USP) (.fj)
TEIN funded project: XeAP
Extending eduroam in the Asia Pacific

• AARNet submission in response to TEIN request to lead a project collaboratively with regional eduroam participants to increase eduroam footprint in the Asia Pacific
• Also creating an APAC eduroam Confederation
• 5 TEIN beneficiary countries to be chosen as targets: candidates include Bangladesh, Cambodia, Indonesia, Pakistan, Sri Lanka, Vietnam
• Will also improve eduroam generally, and promote improved participation by existing APAC NROs: e.g. Malaysia, The Philippines, Thailand
Summary of Work over 2015/16

- eduroam AU Website & Wiki, institutional engagement
- Ancillary Services
  - Administration (using DjNRO)
  - Monitoring (IdP + SP, use of test accounts)
  - Metrics (aggregate and institutional)
  - Support (policy for provision by institutions)
    - End-user device configuration
      - Configuration Assistant Tool (CAT)
    - Troubleshooting via test accounts & log access
  - Templates & Checklists
    - Institutional eduroam Website template
    - Operability Testing and Auditing checklists
- Protocol upgrades and XeAP project