eduroam(Radius based Federation)

Deokjai Choi (Chonnam National University, Korea)

2015. 8. 18
WHAT IS eduroam?

eduroam:

• EDUcation ROAMing
• Provides secure internet access for academic roamers.
• User experience - “Open your laptop and be online.”
WHY eduroam?

Researchers:

- Travel with WLAN-enabled notebooks.
- Want transparent, secure network access.
- Want similar experience at visited institution as home.

Experience facilitated by seamless sharing of network resources.

Better for roamers, easier for administrators.
Europe

- 2003: Started as pilot under TERENA TF-Mobility
- Since Sept 2004: ops&dev of European eduroam funded by GEANT.
- 2007: European eduroam confederation policy agreed, & Operation Team (OT) formed
  - OT deployed eduroam global database, support services
- 2008: Production service commenced
History of eduroam

- APAN

  - 2006: eduroam Project Group commenced
  - 2008: eduroam AU (incl. NZ) Pilot Service commenced
    - eduroam NROs in Hong Kong, Japan, Macao, Taiwan
  - 2011: eduroam production service commenced
  - 2014: REANNZ became eduroam NZ NRO
History of eduroam

- Canada
  - 2010 (BCNet), transferred responsibility to CANARIE 2011

- US
  - 2012 Internet2 announced offering eduroam service to US institutions

> 2012: Africa, South America
### Global eduroam 현황

<table>
<thead>
<tr>
<th>Category</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of independent sovereign states in the world</td>
<td>195</td>
</tr>
<tr>
<td>Number of countries listed by GeGC</td>
<td>85</td>
</tr>
<tr>
<td>* GeGC : Global eduroam Governance Committee</td>
<td></td>
</tr>
<tr>
<td>Number of signatory NROs Globally</td>
<td>67 -&gt; 69</td>
</tr>
<tr>
<td>Number of NROs in global database</td>
<td>66</td>
</tr>
<tr>
<td>Number of service locations registered in eduroam db</td>
<td>11492</td>
</tr>
<tr>
<td>Number of NROs being monitored by monitor.eduroam.org</td>
<td>46 (all under EU TLRS except CA)</td>
</tr>
<tr>
<td>Number of Institutions using F-Ticks</td>
<td>36 (all under EU TLRS except CA)</td>
</tr>
<tr>
<td>Number of Institutions using CAT</td>
<td>587</td>
</tr>
</tbody>
</table>

- From NWitheridge’s presentation at TNC 2014 -
Asia-Pacific eduroam 현황

Asia-Pacific Confederation is being prepared.
AUTHENTICATION AND 802.1x

User

EAPOL

EAP over RADIUS

f.i. LDAP

Jan@hangook.ac.kr

Authenticator (AP or switch)

RADIUS server
Institution A

User DB

Internet

교직원 VLAN

Guest VLAN

학생 VLAN

Data signalling

Data

전남대학교

CHONNAM NATIONAL UNIVERSITY

eduroam
HOW DO THE PIECES FIT TOGETHER? AN EXAMPLE

User

User

joe@hangelog.ac.kr

User

User

教직원 VLAN

학생 VLAN

Guest VLAN

Central RADIUS Proxy server

RADIUS server University A

RADIUS server University B

User DB

User DB

XYZnet

• Trust: RADIUS & policy documents
• 802.1X + EAP
• (VLAN assignment)
802.1x Authentication (EAP-PEAP/EAP-TTLS)

Supplicant (사용자단말)
- 무선구간 암호화 AES
- EAP 메시지

Authenticator (AP&콘트롤러)
- Radius 메시지
- Shared Key를 이용 암호화된 채널로 통신

인증서버 (Radius & Radius Proxy)
- Radius 메시지

로밍센터 (Radius Proxy)
- Shared Key를 이용 암호화된 채널로 통신

사용자 단말 설정값
1. 무선보안모드 : WPA2-Enterprise
2. 무선암호화방식 : AES
3. EAP유토템 : PEAP / EAP-TTLS
4. 인증프로토콜 : MS-CHAPv2 / PAP

AP&콘트롤러 설정값
1. SSID명 : eduroam (WPA2-AES)
2. 인증서버 : IP, Port, Shared-Key
3. 파밀서버 : IP, Port, Shared-Key

인증서버 설정값
1. Radius client : IP, Port, Shared-Key (AP 또는 Radius 등)
2. 서버용 인증서 설치(TLS)
3. 사용자 DB 연동(패스워드 암호화)
4. 사용할 인증프로토콜 종류 설정
   EAP-PEAP (MS-CHAPv2), EAP-TTLS (PAP)
5. Radius Proxy 설정(로밍센터로 연동시)
MAIN COMPONENTS OF eduroam

Network Access Server (NAS):
  • Wireless Access Point or
  • 802.1x compatible wired switch.

Client with configured supplicant.

Hierarchy of RADIUS Authentication Servers (AS).

IEEE 802.1x.

IEEE 802.1q.
  • Standard for VLAN assignment.
eduroam service KEY Points

- Eduroam value proposition realized
  - becoming increasingly global
- Global expansion brings challenges
  - Trust (importance of Policy & Proof of Compliance)
  - Scalability of infrastructure
- Resourcing
  - Shoe-string budgets
- Ease of deployment & participation
- Global collaboration
  - Shared effort in development of ancillary services
1. NRO (National Roaming Operator)
   KISTI = Korea NRO

2. RO (Roaming Operator)
   For colleges and universities in Korea
   Chonnam National University

3. IdP (Identity Provider)
   Each university will provide Idp service for its users.
   Normally, each university will play roles of Idp and SP.

4. SP (Service Provider)
   Visiting university will play a role of SP for the visitor.
   * Telecommunication provider which provides Aps for the campus will play a role of SP only.
NRO : Things to do

Entity which is approved by RC(Roaming Confederation). If there is no RC, it should be approved by GeGC. NRO has a responsibility to take care of eduroam service for the country.
※RC(Roaming Confederation) : a set of NROs which locate nearby, and approved by GeGC such as Europe RC.
※GeGC(Global eduroam Governance Committee) : consists of NROs and RCs, and operated by TERENA

- Responsibility for eduroam service for the country.
- Determines each IDP is legally registered education/research organization for the country.
- Determines each SP is adequate or not.
- Should have communication channel with other NRO
- Should publicize the available SP according to the GeGC guideline.
- Should have communication channel with all SPs to solve the problems or needs.
- Should put technical people, available eduroam sites, Idp lists, RC policy etc through web
- Should maintain enough log information to track users.
- Should register eduroam name and logo to its own country.
RO 역할(eduroam 서비스 구성도)

*kr에 대해 KISTI로 전달

Korea RO KISTI

기 연동된 KAIST, GIST 등 을 제외한 *.ac.kr에 대해 교육기관RO로 전달

• 교육기관 RO에 속하지 않은 요청에 대해 KISTI로 전달
• 통신사 USIM 정보를 이용한 접속 필터링
• .com / co.kr 등 레/from 필터링
• 루핑 방지를 위한 루 설정

Federation level

Institutional level

전국대학 RO 전남대

Keduroam으로 서비스 중인 35개 대학 eduroam 으로 SSID 변경

KAIST

GIST

전남대

CHONNAM NATIONAL UNIVERSITY
IdP Roles

Entity which manages user ID and provides authentication for its users.
Idp should be also SP, and it is called home organization.

- Should agree to global policy as well as domestic policy
- Should understand its own authentication servers (product name, version, functions)
- Should open firewall to other RO’s authentication server
- Should set aside staffs for eduroam, helpdesk, security
- Should configure or modify radius server according to the RO’s guide.
- Should prepare test account for automatic monitoring by RO.
- Should guide how to use to its own member, and provide web link to NRO.
- Should notify the logging items and usage of those logging information
SP Roles

Entity which provides WLAN service to the valid user, and called visiting organization. Normally, each member university will be a SP as well as Idp. Sometimes, telecommunication provider can play a role of SP only.

- Should agree to global as well as domestic policy.
- It is recommended to use VLAN to separate visitors traffic (very important)
- Should broadcast “eduroam” SSID
- Should keep the log file to defend itself from security issues.
- Should notify the logging information and the reason of the logging
Trends

- **Next generation roaming service**
  - “Next generation” i.e RADIUS over TCP using TLS
  - Dynamic Discovery
  - Seek advice from GeGC

- **“Moonshot”: ID Federation based on Radius**
  - **authentication**: Radius / for rich authorisation semantics
  - From only wi-fi to various services
Moonshot builds on the eduroam technologies

- EAP (RFC 3748): strong mutual authentication
- RADIUS (RFC 2865): federation between domains

To this, Moonshot adds

- SAML, for rich authorisation semantics
- Integration using operating system security APIs
  - SSPI: Windows
  - GSS-API (RFC 2078): Other operating systems
  - SASL (RFC 4422): Windows and other operating systems
Deployment requirements

Most Higher Education organisations are nearly Moonshot-ready today

• A connection to eduroam

• A RADIUS server (any modern RADIUS product should support pre-production testing today). There is also an experimental capability to integrate FreeRADIUS with the Shibboleth IdP

• Moonshot client and server plug-in
  • Linux: packaging available for Debian & RHEL; Scientific Linux soon
  • Windows: native support using prototype plugin
  • Mac: Packaging almost complete for Snow Leopard and Lion

• Moonshot Identity Selector to facilitate the selection of an identity to use, for GUI environments (Windows, Mac & Linux)
Architecture

SSH client  (1) Credentialing

SSH server  (2) SSH negotiation

RADIUS server  (3) Authentication

(4) RADIUS

(5) Attributes

(6) SSH session

OpenSSH used as example of application; many others also apply
Application support

Most modern applications use *at least one* of the security APIs supported by Moonshot.

Correctly written applications will ‘just work’ without modification or recompilation.

Less correctly written applications may require minor modifications.

Project Moonshot is testing applications and sending patches upstream.
PuTTY → OpenSSH
IE → Apache

Project Moonshot

User login
- Username:
- Password:
- Log in
  - Create new account
  - Request new password

Windows Security
- Connecting to rand.mit.de.padl.com.
- lukeh@MIT.DE.PADL.COM
- Remember my credentials
- Use another account
- OK
- Cancel

Read more

Waiting for http://rand.mit.de.padl.com/...
Outlook 2010 ➔ Exchange 2010
감사합니다!