Sharing eduroam and ID Federation Experience

2015 8. 19.

SungKuk Kim   k2@jnu.ac.kr
Chonnam National University in Korea
Contents

I. eduroam
- becoming an NRO
- deploy National RADIUS Servers
- FreeRadius config files
- Virtual Server
- Which EAP type to deploy
- Garbage data filtering
- Dynamic VLAN
- eduroam LAB Diagram

II. ID Federation
- Radius Federation & SAML Federation
- Building Test Environment using Shibboleth
- Future Plan
Before Start ..

In the weekend, building small house and managing home remotely using Raspberry Pi is fun. It is hard but fun. I control electricity, boiler etc
I. Becoming an NRO

- Understand eduroam service & national customers
- Agree to Global eduroam Compliance Statement (GeCS)
- Decide on national eduroam operational objectives
- Create national eduroam policy
  - Liaise with national R&E institutions
- Create national eduroam website
- Define joining process and forms
  - Test & auditing checklist
- Deploy national RADIUS infrastructure
- Deploy Ancillary Services
  - Administration
  - Monitoring & Metrics
  - End-user Support
- Prepare resources to provide National eduroam support (e.g. staffing)
  - ticketing system
  - create mail-lists & confirm participants
Deploy National RADIUS Servers

- Study and decide on protocols
- Move away from conventional RADIUS towards RADIUS over TCP with TLS and with dynamic discovery?
  - Issue down the track is one of inertia
  - Start from scratch with the right solution, or least effort migration path to the best solution

- RADIUS Servers
  - High Availability
  - Monitored
  - Logging

- If not an existing RADIUS server, choose an implementation
  - CISCO, Microsoft, FreeRadius, Radiator
RADIUS over TCP using TLS

Uses TLS instead of shared secrets between RADIUS peers.

Standardisation activity in IETF

- RFC6613 RADIUS over TCP
- RFC6614 Transport Layer Security (TLS) Encryption for RADIUS

Support by RADIUS implementations

- FreeRadius v3

For a full description, see

The eduroam architecture for network roaming
draft-wierenga-ietf-eduroam-05.txt

Trials undertaken and new NROs encouraged to adopt

- More guidance required from European eduroam Operations Team
- No APAN NROs use RADIUS over TCP using TLS
NRO Role: Technical Expertise

- NRO, in participating in global eduroam, has responsibility to provide expertise
  - to institutions it serves
  - contribute to global eduroam technical evolution
- Protocol stacks involved are deep
- Wireless protocols are evolving
- Advising eduroam support and analysing problems requires in-depth knowledge
When you start,.....
Each eduroam-enabled institution may use different:

- Equipment.
- Software.
- Topology.

Details of eduroam configuration depend upon factors above...

...But broad principles are the same on any platform.

- We also used Microsoft NPS in the first, but later moved to Freeradius. The reason was we do not enough Fund, but we wanted to control the functions as we want to do.
- I’d like to recommend to use one product such as FreeRadiusV3, and extend to other Radius products.
* If you become an RO, you will meet many products.
Various vendor products (Korea Case)

CISCO ACS

Aruba ClearPass

Juniper Steel-Belt
With no support Proxy

A10 Networks ......

Microsoft NPS with
Active Directory

In the beginning, we
used MS NPS.

Roughly 90% of the users are managed by SQL Server (Oracle, MS-SQL, My-SQL..),
another 10% would be by Directory Service such as LDAP.
FreeRadius Config files

AP, Radius Server...
clients.conf

Roaming Rule
proxy.conf

FreeRADIUS Authn Type config
eap.conf

Virtual Server
default
eduroam (NRPS Request)

Outer-tunnel = Routing
inner-tunnel
ID, PW

radiusd.conf

sql.conf
users
ippool
ldap
Supported EAP authentication types (by FreeRADIUS)

- EAP-TLS(x.509 client certificates)
- **EAP-TTLS(Server certificate, Funk Soft) ID/PW**
  - If SHA1 hash is used as an encryption tool, and because of that, if clear-text cannot be used, then use **EAP-TTLS(PAP)**
    - Separate TTLS connection program required
- **PEAP(server certificate, MS, Cisco etc) ID/PW**
  - Passwords in clear-text OR NT-hash
    - Without connection program, around 12 steps should be done by user
- EAP-GTC(clear-text separate general token distribution plug-in required
- LEAP / EAP-MD5
Which EAP type to deploy – eap.conf

- Because of very strong privacy law (12.3.30), personal information such as id, password should be hashed

  Without encryption using NT-Hash, we used SHA-224/256/384/512 to encrypt password

  => In Korea, many colleges use RDBMS

<table>
<thead>
<tr>
<th></th>
<th>clear-text</th>
<th>NT-hash</th>
<th>MD5 hash</th>
<th>Salted MD5 hash</th>
<th>SHA1 hash</th>
<th>Salted SH1 hash</th>
<th>Unix Crypt</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAP</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>CHAP</td>
<td>o</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Digest</td>
<td>o</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>MS-Chap</td>
<td>o</td>
<td>o</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>PEAP</td>
<td>o</td>
<td>o</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>EAP-MSCHEAPv2</td>
<td>o</td>
<td>o</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Cisco LEAP</td>
<td>o</td>
<td>o</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>EAP-GTC</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>EAP-MD5</td>
<td>o</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>EAP-SIM</td>
<td>o</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

Because of DB encryption problems:
1. EAP-TTLS(PAP) recommended
2. If you want to use EAP-PEAP(MS-CHAPv2), you may use separate NT-hash password table.

For EAP-TTLS(PAP), EAP-GTC, separate connection program required
Realm Issue

id => id@jnu.ac.kr : many input errors

Examples of erroneous input

oy2e0917@ac.kr
1100111@kusan.co.kr
shaoyi@nuch.ar.kr ....

- There are some universities which use more than one domain name. Then they need to choose domain for roaming, and advertise it.
- There are many reasons to have more than one domain.
  - @jnu.ac.kr @chonnam.ac.kr @chonnam.edu
  
- @jnue.kr @jnue.ac.kr
Policy - Garbage data filtering

• Policy.conf contains lists of rules...can use this file to create rules e.g.
  – Does username/realm contain whitespace?
  – Does realm end in whitespace or contain illegal characters?
  – Are there multiple @’s
  – Is it a ‘valid realm’ (has at least one . )
  – Does the realm have double dots – realm..ac.kr?
  – ar.kr ? @ac.kr ?
  – 3gppnetwork.org

• Can simply name a rule e.g. ‘valid_eduroam_user’

• Call that from authorize {}

  • Telco’s smart phone USIM authentication request data
    0450050259106997@wlan.mnc005.mcc450.3gppnetwork.org
Virtual-Server (default, inner-tunnel.....)

- One of the core assets of FreeRADIUS
- Not XEN/VMware style – it’s like Apache host definitions
- 3 default servers with 2.1.12
  - default, inner-tunnel, control-socket
- Many others waiting to be used – eg DHCP ....
- Create a new VS – ‘eduroam’ for requests that come from the NRPS
- Can be very minimal – just needs to authenticate users and deal with accounting
eduroam VS (minimal)

server eduroam {
  authorize {
    preprocess
    suffix
    ntdomain
    auth_log
    eap {
      ok = return
    }
  }
  authenticate {
    Auth-Type EAP {
      eap
      ok = return
    }
  }
  preacct {
    preprocess
    acct_unique
    suffix
    ntdomain
  }
}

accounting {
  if (Acct-Session-Time != 0) {
    detail
  }
  else {
    ok
  }
  attr_filter.accounting_response
}

post-auth {
  reply_log
  Post-Auth-Type REJECT {
    attr_filter.access_reject
  }
}

# end of eduroam VS

client roaming1.eduroam.kr {
  secret = secret
  nastype = other
  shortname = NRPS1
  virtual_server = eduroam
}

Requests from roaming1.eduroam.kr will now go through the ‘eduroam’ server – avoiding all other logic/rules/methods
Attribute filtering

- Used to having control of you own servers...you set the attributes for your NAS (e.g. To place user on a VLAN)
- When request proxied off, the REMOTE server can be setting things
- Might be okay if they are using different kit (VSA might not match) but bad news if using same kit
- Uncomment the filtering in pre-proxy and post-proxy
- Edit the filters to match initialize VLAN attribute
VLAN Configuration

1. VLAN per SSID : AP Controller setting (Static VLAN)
   
   Same policy should be applied to the whole user who use same eduroam ssid.

   If visitor tries to connect using visiting school’s SSID, Radius or controller should use filtering.

2. Radius should direct VLAN assignment based on user (Dynamic VLAN)
   
   After understanding who is the user, based on title or realm, VLAN should be assigned.

   Configured at post-auth section

   Tunnel-Type = VLAN
   Tunnel-Medium-Type = IEEE-802
   Tunnel-Private-Group-Id = ‘VLAN name’
FreeRadius dynamic VLAN ‘home’ Authentication

When local user uses service locally

Title: Authentication Flow Chart: Home User

<table>
<thead>
<tr>
<th>Internal AP's</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request From Client</td>
<td></td>
</tr>
<tr>
<td>authorization</td>
<td>Result Home User</td>
</tr>
<tr>
<td>PrepOCSS</td>
<td>conitonly</td>
</tr>
<tr>
<td>Send to Inner-Tunnel</td>
<td></td>
</tr>
<tr>
<td>Request From Client</td>
<td></td>
</tr>
<tr>
<td>post-auth</td>
<td>Reply from Inner-Tunnel</td>
</tr>
<tr>
<td>RSVP-Radius-Attr replaceme</td>
<td>update reply attr filter</td>
</tr>
</tbody>
</table>

Virtual Server: default

<table>
<thead>
<tr>
<th>Virtual Server: inner-tunnel</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorization</td>
</tr>
<tr>
<td>PrepOCSS</td>
</tr>
</tbody>
</table>

Identity Store: AD, LDAP, SQL...

VLAN per user group such as staffs, students, visitors
For visitor cases

If realm is not for local university, assign guest VLAN
( @jnu.ac.kr is not -> guest )
When my member visits other university

Among member of university, only student and faculty, and staff should be allowed, otherwise should be rejected.

(Valid User)
(alumni, retired staffs, civilian who allowed to use library)
Let’s persuade each university staffs~

- What if contacted on holiday?
- It is too busy to do other work because of limited human resources. . . ^_^

We are happy~~
Easy is the best

It is serving people~~ Let’s work together
This is service for us, and our next generation~~~

Same understanding among IT managers...
Guiding material: Sample docs, video, Sticker, CAT (Client Assistant Tool)

Help with wireless  eduroam Access Guidelines (eduroam 접속 안내)

- Procedures to access Free WiFi Service at eduroam Institutions for Chonnam National University
  Staff and Students: Chonnam National University staff and students can access the eduroam service while they are on campus.

  Pre-requisites: To access eduroam service:
  - Must be a registered Chonnam National University student or staff with a valid JNU Portal account.
  - Have a valid JNU email address.

  If you are not a Chonnam National University Staff or Student with a valid portal ID, you can use campus wireless service with JNU SSID, but not eduroam. This excludes the use of eduroam services, including SSID, and is only for employees and students with a valid portal ID.

  For Windows 8.1/8/7, you may download the WiFi auto-configuration program HERE to configure the WiFi Profile automatically. Windows 8.1/8/7 users can download a custom profile for eduroam that includes additional profile settings.

You must configure your PC or smartphone using eduroam. eduroam should be connected to your PC or smartphone. To configure:
- Procedure for Windows 8.1/8/7 (manually setup)
  - Manually configure the WiFi settings (Bluetooth connection)
- Procedure for Windows 10 (manually setup)
  - Manually configure the WiFi settings (Bluetooth connection)
- Procedure for Windows 11 (manually setup)
  - Manually configure the WiFi settings (Bluetooth connection)
- Procedure for Windows Vista (manually setup)
  - Manually configure the WiFi settings (Bluetooth connection)
- Procedure for Mac
  - Manually configure the WiFi settings (Bluetooth connection)

Getting technical support from vendor is encouraged.
Eduroam LAB Diagram

The same physical equipment

192.168.0.1
Wire / NAT / DHCP

192.168.0.200
VM-Host(Note-Book)
Hyper-v, Vm-ware, Virtual-box
windows2008R2

Universitas Indonesia
192.168.0.1

@ui.ac.id

192.168.0.2~100

VM_UI
Active Directory

192.168.0.211

192.168.0.210

192.168.0.212

VM_RO
VM_ITB
My-SQL

VM Network Bridge

Institut Teknologi Bandung
192.168.0.1

@itb.ac.id

192.168.0.2~100

Remote AP

192.168.0.2~100

Chonnam National University eduroam

Alvin will present simplified configuration of the above figure with your language.
Eduroam LAB Equipment

Chonnam National University Remote AP (Real eduroam)

FAT AP(home)
-Multi SSID
-NAT, VPN, ......
-802.1x WPA2-Enterprise
Radius Federation & SAML Federation (web base)

inter Federation (eduGain) ...

SAML MiddleWare
- JAVAA
- PHP
- .NET
- Python

Radius Server
- Idp + SP

A university
- LDAP, SQL
- SAML Idp
- SAML SP

B university
- LDAP, SQL
- SAML Idp
- SAML SP

Radius Proxy

DS (metadata Discover Service)

https Redirect

Roaming Operator (RO)
Building Test Environment using Shibboleth

http://jnusp.jnu.ac.kr

Login button (https://jnuidp.jnu.ac.kr/secure/index.php)

ldp Redirect

https://jnuidp.jnu.ac.kr

test001 user login

OpenLDAP
Building Test Environment using Shibboleth

![Image of Shibboleth login](https://jnusp.jnu.ac.kr/secure/)

**test01 user Login OK**

Attribute Value

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Value(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ePPN/codePersonPrincipalId</td>
<td><a href="mailto:test001@ac.kr">test001@ac.kr</a></td>
</tr>
<tr>
<td>eduPersonTargetId</td>
<td><a href="https://jnusp.jnu.ac.kr/idp/shibboleth/https://jnusp.jnu.ac.kr/idp/shibboleth/EDU">https://jnusp.jnu.ac.kr/idp/shibboleth/https://jnusp.jnu.ac.kr/idp/shibboleth/EDU</a> Person ID: <a href="mailto:test001@ac.kr">test001@ac.kr</a></td>
</tr>
<tr>
<td>Affiliation (eduPersonAffiliation)</td>
<td>member</td>
</tr>
<tr>
<td>Scoped Attribute (personScopedAttribute)</td>
<td><a href="mailto:member@ac.kr">member@ac.kr</a></td>
</tr>
<tr>
<td>Entitlement (eduPersonEntitlement)</td>
<td>NOT RECEIVED</td>
</tr>
<tr>
<td>Email address (mail)</td>
<td><a href="mailto:test001.email@ac.kr">test001.email@ac.kr</a></td>
</tr>
<tr>
<td>Surname (cn)</td>
<td>test001</td>
</tr>
<tr>
<td>CommonName (cn)</td>
<td>test001.test001.cn</td>
</tr>
</tbody>
</table>

Details of current session information

- **Session Expiration** (duration inactivity): 465 minute(s)
- **Client Address**: 156. 88. 125. 95
- **SSO Protocol**: urn:oasis:names:tc:SAML:2.0:protocol
- **Identity Provider**: https://jnusp.jnu.ac.kr/idp/shibboleth
- **Authentication Time**: 2015-03-09T01:27:36Z
- **Authentication Context Class**: urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
- **Authentication Context DocId**: [value]
Lesson and Future Plan

- After test using VM, we have better understanding the federations service. (We need to study—there are many reference materials)

- We’d like to study and provide SAML Federation Service with eduroam community.

- Our position for federations is good, since we, university staff, understand university more than anyone. This is our strength for federations service.

- To do list for ID Federation ...
  - understand trend domestically as well as internationally
  - study other countries’ policy and technical documents
  - deploy pilot system (collaboration with video conference)
  - As an RO and IDP, it is crucial to understand other university situation
  - interoperable test with KISTI SimpleSAMLPhp which is being deployed
Terima kasih!