eduroam configurations for Member organization

15 August 2019

Minseok Jang (msjang@kisti.re.kr)
Researcher
KREONET Center / Div. of National Supercomputing
Korea Institute of Science and Technology Information (KISTI)

Institutional Technical Pre-Requisite

- Identity Management
  - LDAP, Active Directory, IMAP
  - REALM supported
  - Test Account
- WiFi Infrastructure
  - Coverage Map
  - IEEE 802.1x
- Network Access
  - ISP, if not NREN
  - AUP(Acceptable Use Policy)
- IT Support
  - HelpDesk

Institutional Wireless Infrastructure

- 802.1x capable
- Broadcast of ‘eduroam’ SSID
  - Whole word must be in lower case
  - Issue of overlapping hotspots
    - e.g. eduroam-uniX
    - Potential of IEEE 802.11u to alleviate issue
- Wireless coverage across campuses
  - Availability of coverage maps
- Encryption support (WPA2-Enterprise required) Tunneled EAP protocol
  - Choice of inner-authentication depending on identity store
- Limitations of WiFi Supplicants on various platforms

Institutional RADIUS Server (IRS) 1/2

Requirements for proxied RADIUS requests

- RADIUS attributes
  - Filtering to release only required attributes
  - Generate Chargeable-User-Identity (CUI) for IdP role
  - Include Operator-Name (ON) for SP role
- Terminate (i.e. don’t proxy) accounting requests
- Configure bogus realm black-listing
  - E.g. *.3gppnetwork.org
- Reject request with badly formatted username (e.g. invalid characters)
- Use Status-Server to handle non-responsive servers

Institutional RADIUS Server (IRS) 2/2

- Deployment considerations
  - Time synchronization (NTP)
  - Server redundancy (high-availability deployment)
  - Load balancing
- RADIUS request logging
  - Trust model - ability to trace a network access to a real user
  - Traceability of users achieved by logging
  - Attributes to be logged
    - DateTimeStamp, User-Name (outer EAP identity) i.e. realm, Chargeable-User-Identifier, NAS-IP-Address (IP address of adjacent RADIUS client, i.e. NAS or proxy server), Operator-Name (identifier for institution providing network access), Calling-Station-ID (MAC address of user device), authentication response (Accept or Reject)

Today’s Session

Overview

- Install Prerequisite for Trainee’s PC
- Install IRS using ansible
- Test Local and Remote Account
- Add More Test Users
- Add a Realm to BlackHole Routing
- Check Client Secret
- Check NRS Settings in Client and Proxy Configs
- Compare Configs
- Compare Local and Remote Auth Flow

(For Left Time)

- Add Blackhole Routing
- ...

Install Prerequisite for Trainee's PC

- Terminal SW
  - MobaXterm for Windows
  - iTerm for OSX
  - Basic Terminal for Linux
- WireShark for All OS
  - Packet Capturing and Analyzing Tool
  - (In this session) RADIUS packets captured by tcpdump, downloed to PC, will be opened with WireShark
- Code Compare and Merge Tool; Meld for All OS
  - Windows : download and install
  - OSX : download and install
  - Linux : intall using YUM or APT
- TextEditor (Atom, Sublime, …) for All OS
  - (Mandatory for Windows) NotePad in Windows cannot open Linux config file correctly

NOTICE / IMPORTANT

This Session for IRS (Institutional RADIUS Server).

Connect to IRS, NOT NRS !

Practice the following slides in IRS !

This slides added after retrospection on XeAP 2018 sessions.

Install IRS using ansible 1/2

NOTICE

- eduroam-imap-playbook
  - Ansible scripts for eduroam deployment (Install, Config, Test)
  - Authored by SAFIER, Modified by KROENET under MIT License
  - Presented at TNC18 - eduroam for GSuite users? Yes you can!

- Check Linux Version - Ubuntu 18.04

```
# sudo cat /etc/issue
Ubuntu 18.04 LTS
```

- Install GIT, Ansible

```
sudo apt update;
sudo apt -y install git ansible
```

- Clone Ansible Script

```
git clone https://github.com/msjang/eduroam-imap-playbook
```

Install IRS using ansible 2/2

- IRS Settings - Change Ansible Group Variable

  Change the following file; group_vars/all. It is used to create IRS configs.

```
cd eduroam-imap-playbook;
vi group_vars/all
```

```
# The upstream eduroam federation-level RADIUS servers
# These are for sample, not working; get yours from your NRO
eduroam_flr_servers:
  - hostname: eduroam.kr
    ip: 138.44.179.8
    port: 1812
    secret: secret_key_between_nro_and_irs

# Your realm for eduroam (usually your primary DNS name)
radius_realm: xeap.kr

# Details of test account(s) to create within your realm
radius_local_users:
  - username: eduroam
    password: xeap2018

...
```

- Install IRS - Run Ansible

```
ansible-playbook -i inventories/development site.yml
```

Test Local and Remote Account

- rad_eap_test

```
# rad_eap_test
Parameters :
-H <address> - Address of radius server
-P <port> - Port of radius server
...
```

- Test Local Account

```
# rad_eap_test -H localhost -P 1812 -S testing123 -m WPA-EAP -s eduroam \
  -e TTLS -2 PAP -u eduroam@xeap.kr -p xeap2018
access-accept; 0
```

```
# rad_eap_test -H localhost -P 1812 -S testing123 -m WPA-EAP -s eduroam \
  -e TTLS -2 PAP -u eduroam@xeap.kr -p xeap2019
access-reject; 0
```

- Test Remote Account

```
# rad_eap_test -H localhost -P 1812 -S testing123 -m WPA-EAP -s eduroam \
  -e TTLS -2 PAP -u eduroam@xeap.au -p xeap2018
access-accept; 0
```

Add More Test Users

- Add Test User to Config File; ID: bob, PW: hello

```
sudo vi /etc/freeradius/3.0/users
```

```
...
# You can include local (non-PAM) users like this:
# icecold     Realm == "kisti.re.kr", Cleartext-Password := "snowwhite"
# otheruser   Realm == "kisti.re.kr", Cleartext-Password := "swordfish", Expiration := "25 May 2099"

eduroam       Realm == "kisti.re.kr", Cleartext-Password := "xeap2018"
bob           Realm == "kisti.re.kr", Cleartext-Password := "hello"

# This catches all remaining users and sends them to PAM
DEFAULT       Virtual-Server == eduroam-inner-tunnel, Pam-Auth := "pam-imap-radius", Auth-Type := PAM
...
```

- Restart FreeRadius

```
sudo service freeradius restart
```

- Test New User

```
# rad_eap_test -H localhost -P 1812 -S testing123 -m WPA-EAP -s eduroam \
  -e TTLS -2 PAP -u bob@xeap.kr -p hello
access-accept; 0
```

Add a Realm to BlackHole Routing

- Add a Realm to BlackList; xeap.au

```
sudo vi /etc/freeradius/3.0/proxy.conf
```

```
...
# blackhole routing - EAP-SIM/MNOs
realm "~\\.3gppnetwork\\.org$" {
    nostrip
}

# realm xeap.au {
    nostrip
}

...
```

- Restart FreeRadius

```
sudo service freeradius restart
```

- Test New User

```
# rad_eap_test -H localhost -P 1812 -S testing123 -m WPA-EAP -s eduroam \
  -e TTLS -2 PAP -u eduroam@xeap.au -p xeap2018
access-reject; 0
```

Check Client Secret

- Secret, testing123, is used for RADIUS test in localhost
  Secret is used for each RADIUS communications between two entities.

```
# rad_eap_test -H localhost -P 1812 -S testing123 -m WPA-EAP -s eduroam ...
```

- Secret is defined in clients.conf for each client addresses.

```
function PRINT(){ grep -v '#' $1 | sed -e '/^ *$/d'; };
PRINT /etc/freeradius/3.0/clients.conf
```

```
# PRINT /etc/freeradius/3.0/clients.conf
client localhost {
        ipaddr = 127.0.0.1
        proto = *
        secret = testing123
        require_message_authenticator = no
        limit {
                max_connections = 16
                lifetime = 0
                idle_timeout = 30
        }
}
client localhost_ipv6 {
        ipv6addr        = ::1
        secret                  = testing123
}
$INCLUDE clients-eduroam-flrs.conf
```

Check NRS Settings in Client and Proxy Configs

- CASE 1 : USER → IRS → NRS → …
  - RADIUS Client : IRS
  - RADIUS Server : NRS
- CASE 2 : USER → … → NRS → IRS
  - RADIUS Client : NRS
  - RADIUS Server : IRS
- Settings for NRS can be found both clients.conf and proxy.conf in IRS

```
# PRINT /etc/freeradius/3.0/clients-eduroam-flrs.conf
...
client NRS {
                ipaddr = 150.183.96.51
                secret = MySharedSecret
                require_message_authenticator = yes
                shortname = NRS
                nastype = other
                virtual_server = eduroam
}
...
```

```
# PRINT /etc/freeradius/3.0/proxy.conf
...
home_server NRS {
                type = auth+acct
                ipaddr = 150.183.96.51
                secret = MySharedSecret
                port = 1812
                require_message_authenticator = yes
                status_check = status-server
}
…
home_server_pool EDUROAM {
                type = fail-over
                home_server = NRS
                ...
}
…
realm "~.+$" {
                pool = EDUROAM
                nostrip
}
...
```

Compare Configs 1/4

- Check Running and Original (backed up) Configs

```
# sudo ls /etc/freeradius/
3.0    backup_3.0
```

- ZIP config

```
sudo tar zcf /home/kisti/config.tgz /etc/freeradius/
```

- Download config.tgz to Your PC
  - (Windows) Use MobaXTerm
  - (Linux, OSX)

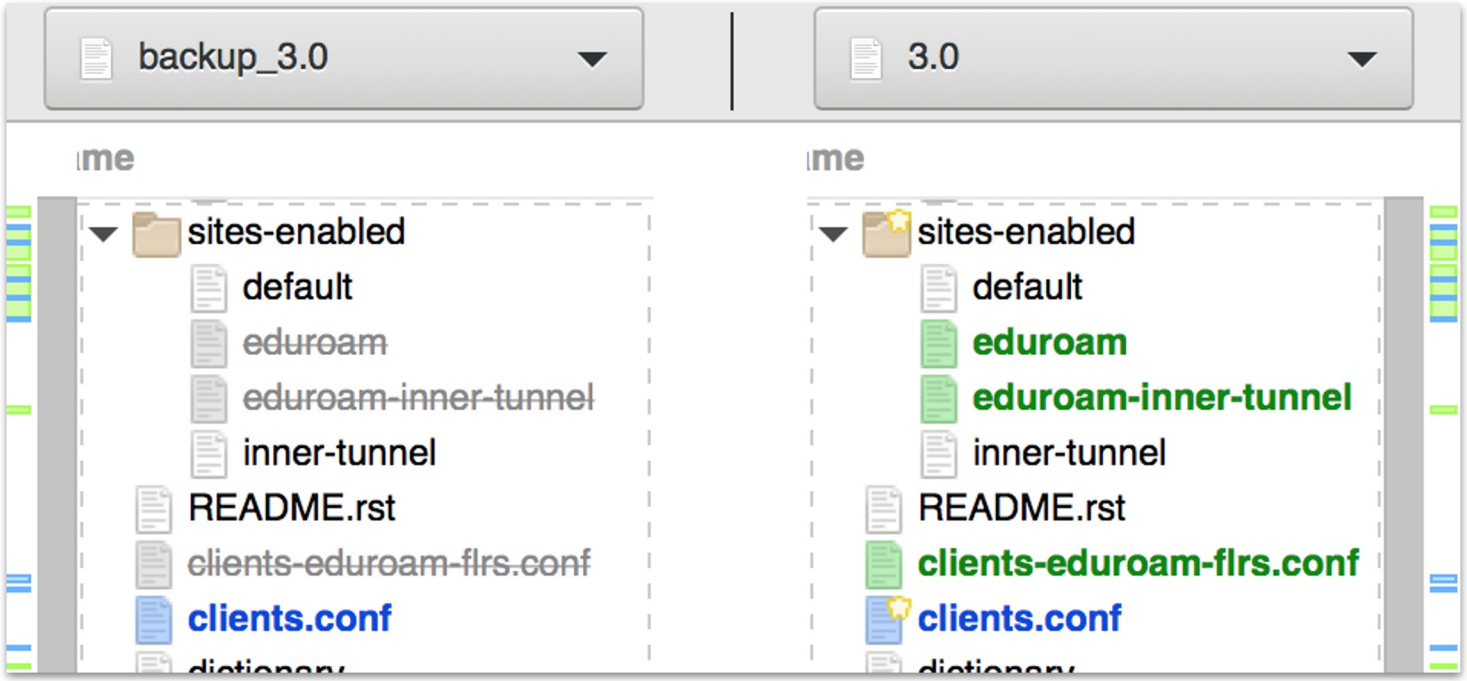
```
YOUR_PC# scp <ID>@<SERVER_IP>:/home/kisti/config.tgz .
```

- UnZIP configs.tgz
  - (Windows) Use Default UnArchiver Program, or BandiZip
  - (Linux, OSX)

```
YOUR_PC# tar zxf config.tgz
```

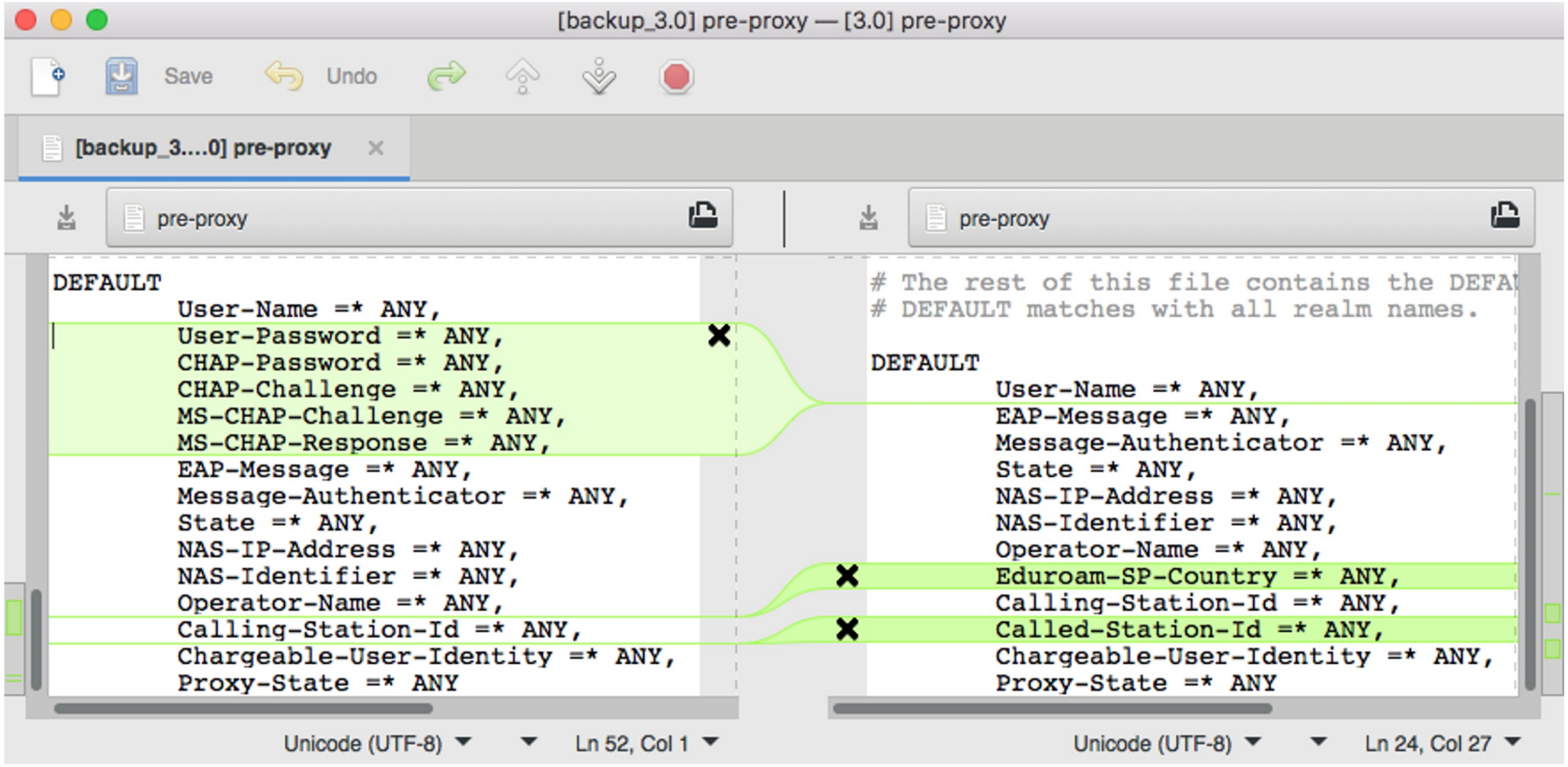
Compare Configs 2/4

- Compare Directories; Original vs Current



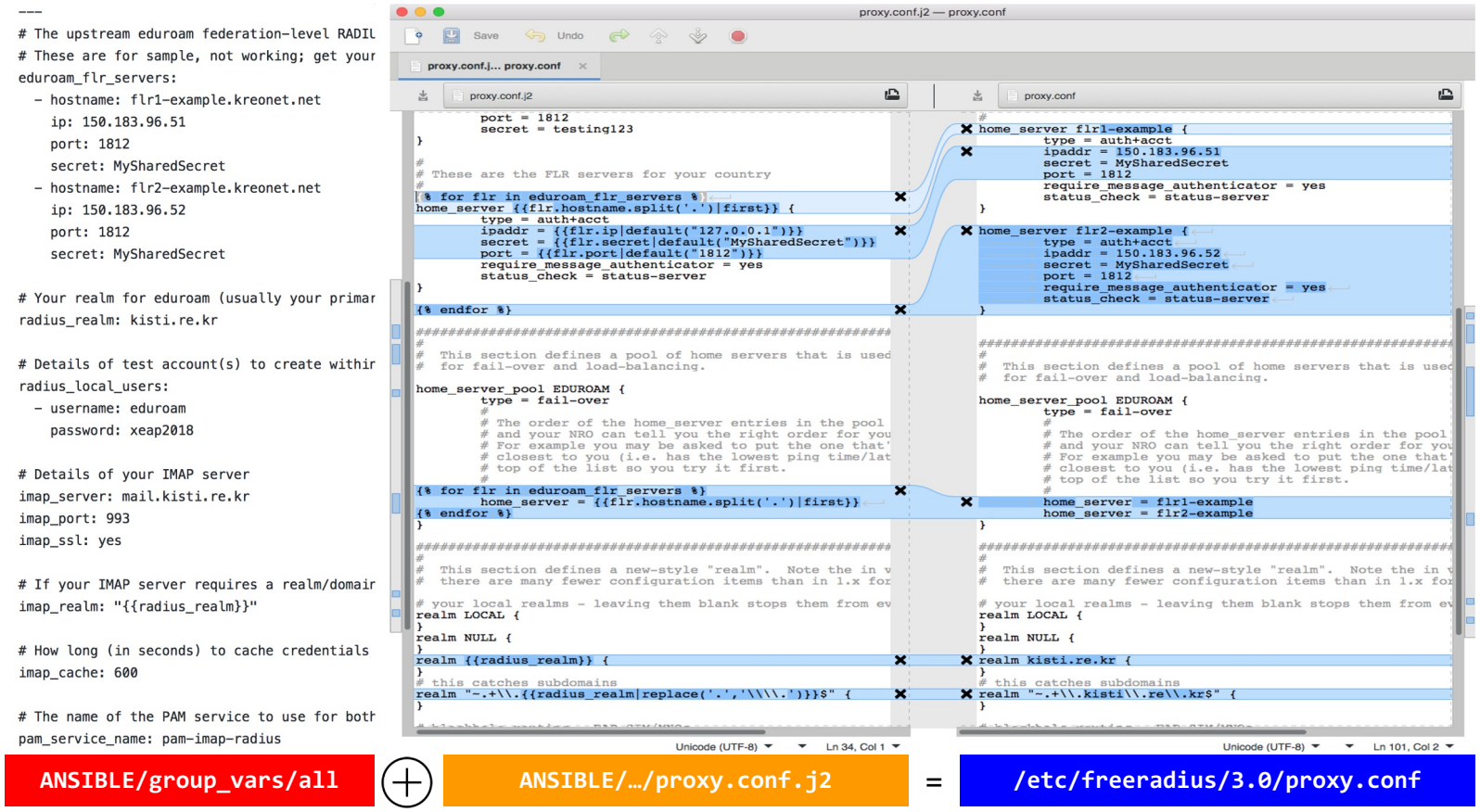
Compare Configs 3/4

- Compare pre-proxy; Original vs Current
  - /etc/../mods-config/attr_filter/pre-proxy



Compare Configs 4/4

- Compare proxy.conf; Ansible Template vs Current
  - Before compare, download and unarchive [eduroam-imap-playbook] to your PC



Compare Configs (advanced)

- Find Modified Configs in Terminal

```
sudo -s;
cd /etc/freeradius/;
diff -qr backup_3.0/ 3.0/ | grep -v Only | awk '{ print $4 }'
```

```
# diff -qr backup_3.0/ 3.0/ | grep -v Only | awk '{ print $4 }'
3.0/certs/ca.cnf
3.0/certs/client.cnf
3.0/certs/inner-server.cnf
3.0/certs/server.cnf
3.0/certs/xpextensions
3.0/clients.conf
3.0/mods-config/attr_filter/pre-proxy
3.0/mods-config/files/authorize
3.0/mods-enabled/eap
3.0/policy.d/cui
3.0/proxy.conf
3.0/radiusd.conf
3.0/users
```

- Find Added Configs in Terminal

```
diff -qr backup_3.0 3.0 | grep "Only in 3.0" | grep -v certs | sed -e 's#Only in ##g; s#: #/#g'
```

```
# diff -qr backup_3.0 3.0 | grep "Only in 3.0" | grep -v certs | sed -e 's#Only in ##g; s#: #/#g'
3.0/clients-eduroam-flrs.conf
3.0/mods-available/f_ticks
3.0/mods-enabled/f_ticks
3.0/mods-enabled/pam
3.0/sites-available/eduroam
3.0/sites-available/eduroam-inner-tunnel
3.0/sites-enabled/eduroam
3.0/sites-enabled/eduroam-inner-tunnel
```

Compare Local and Remote Authentication Flow 1/5

Local Auth Test with Logging and Packet Capture (Test eduroam@xeap.kr in xeap.kr)

- Prepare 3 ssh terminals connected to your IRS (xeap.kr)
- Type The following Commands
  - Press Ctrl + C after test to shutdown process in terminal 1,2

TERMINAL 1

```
sudo tcpdump -i any port 1812 -w internal-test.pcap -vv
```

```
# tcpdump -i any port 1812 -w internal-test.pcap -vv
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
Got 0
Got 14
^C
14 packets captured
```

TERMINAL 2

```
sudo service freeradius stop;
sudo LD_PRELOAD=/lib/x86_64-linux-gnu/libpam.so.0 freeradius -X | tee internal-test.log
```

```
# LD_PRELOAD=/lib/x86_64-linux-gnu/libpam.so.0 freeradius -X | tee internal-test.log
FreeRADIUS Version 3.0.16
...
(0) Received Access-Request Id 0 from 127.0.0.1:41323 to 127.0.0.1:1812 length 155
(0)   User-Name = "eduroam@xeap.kr"
...
(0) suffix: Checking for suffix after "@"
(0) suffix: Looking up realm "xeap.kr" for User-Name = "eduroam@xeap.kr"
(0) suffix: Found realm "xeap.kr"
(0) suffix: Adding Stripped-User-Name = "eduroam"
(0) suffix: Adding Realm = "xeap.kr"
(0) suffix: Authentication realm is LOCAL
...
(0) Sent Access-Accept Id 6 from 127.0.0.1:1812 to 127.0.0.1:41323 length 0
...
```

TERMINAL 3

```
rad_eap_test -H 127.0.0.1 -P 1812 -S testing123 -m WPA-EAP -s eduroam -e TTLS -2 PAP \
-u eduroam@xeap.kr -p xeap2018
```

```
# rad_eap_test -H 127.0.0.1 -P 1812 -S testing123 -u eduroam@xeap.kr -p xeap2018 -m WPA-EAP -s eduroam -e TTLS -2 PAP
access-accept; 0
```

Compare Local and Remote Authentication Flow 2/5

Remote Auth Test with Logging and Packet Capture (Test eduroam@xeap.au in xeap.kr)

- Prepare 3 ssh terminals connected to your IRS (xeap.kr)
- Type The following Commands
  - Press Ctrl + C after test to shutdown process in terminal 1,2

TERMINAL 1

```
sudo tcpdump -i any port 1812 -w external-test.pcap -vv
```

```
# tcpdump -i any port 1812 -w external-test.pcap -vv
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
Got 0
Got 14
^C
14 packets captured
```

TERMINAL 2

```
sudo service freeradius stop;
sudo LD_PRELOAD=/lib/x86_64-linux-gnu/libpam.so.0 freeradius -X | tee external-test.log
```

```
# LD_PRELOAD=/lib/x86_64-linux-gnu/libpam.so.0 freeradius -X | tee external-test.log
FreeRADIUS Version 3.0.16
...
(0) Received Access-Request Id 0 from 127.0.0.1:39427 to 127.0.0.1:1812 length 155
(0)   User-Name = "eduroam@xeap.au"
...
(0) suffix: Checking for suffix after "@"
(0) suffix: Looking up realm "xeap.au" for User-Name = "eduroam@xeap.au"
(0) suffix: Found realm "~.+$"
(0) suffix: Adding Realm = "xeap.au"
(0) suffix: Proxying request from user eduroam@xeap.au to realm ~.+$
...
(0) Sent Access-Accept Id 6 from 127.0.0.1:1812 to 127.0.0.1:41323 length 0
...
```

TERMINAL 3

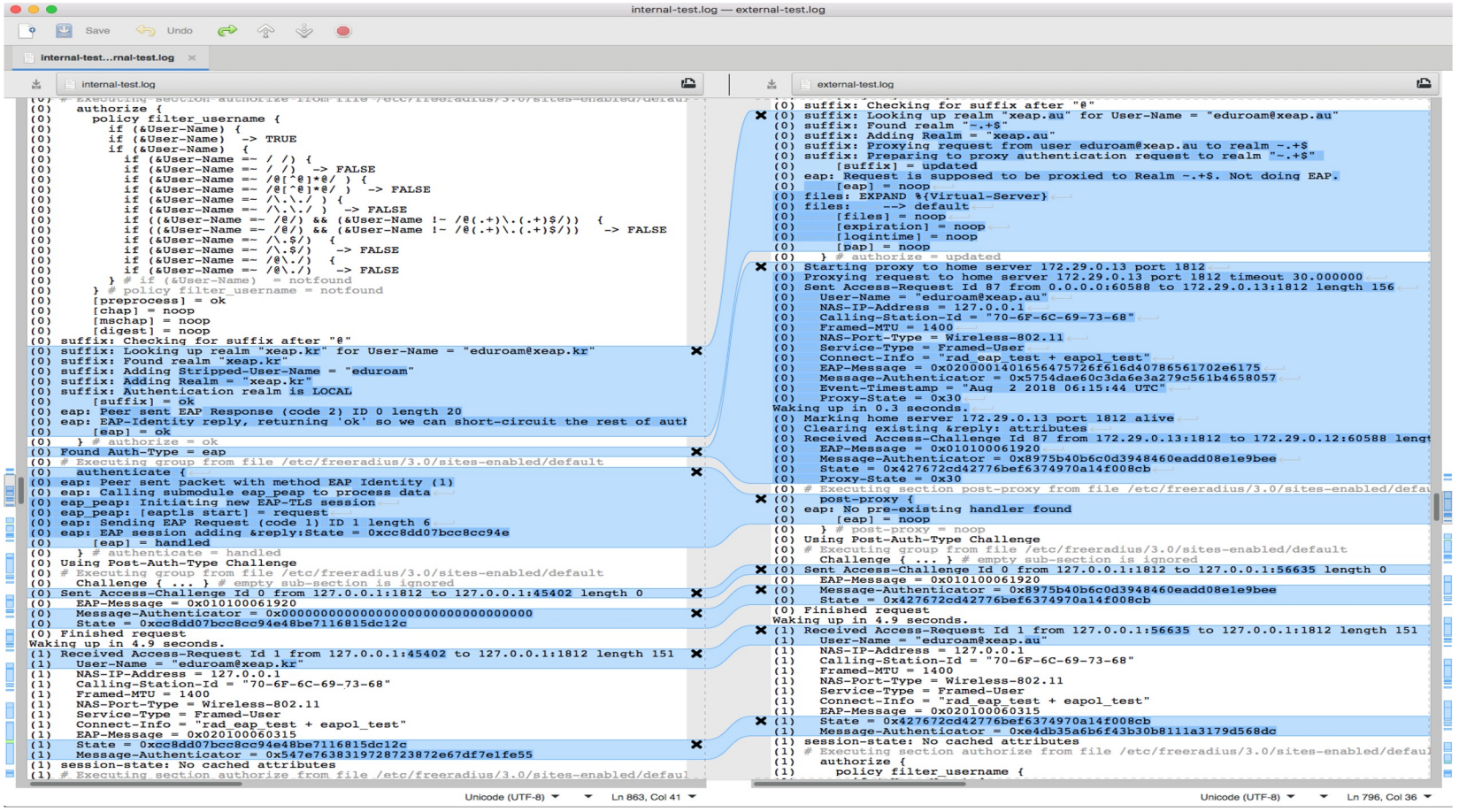
```
rad_eap_test -H 127.0.0.1 -P 1812 -S testing123 -m WPA-EAP -s eduroam -e TTLS -2 PAP
-u eduroam@xeap.au -p xeap2018
```

```
# rad_eap_test -H 127.0.0.1 -P 1812 -S testing123 -u eduroam@xeap.kr -p xeap2018 -m WPA-EAP -s eduroam -e TTLS -2 PAP
access-accept; 0
```

Compare Local and Remote Authentication Flow 3/5

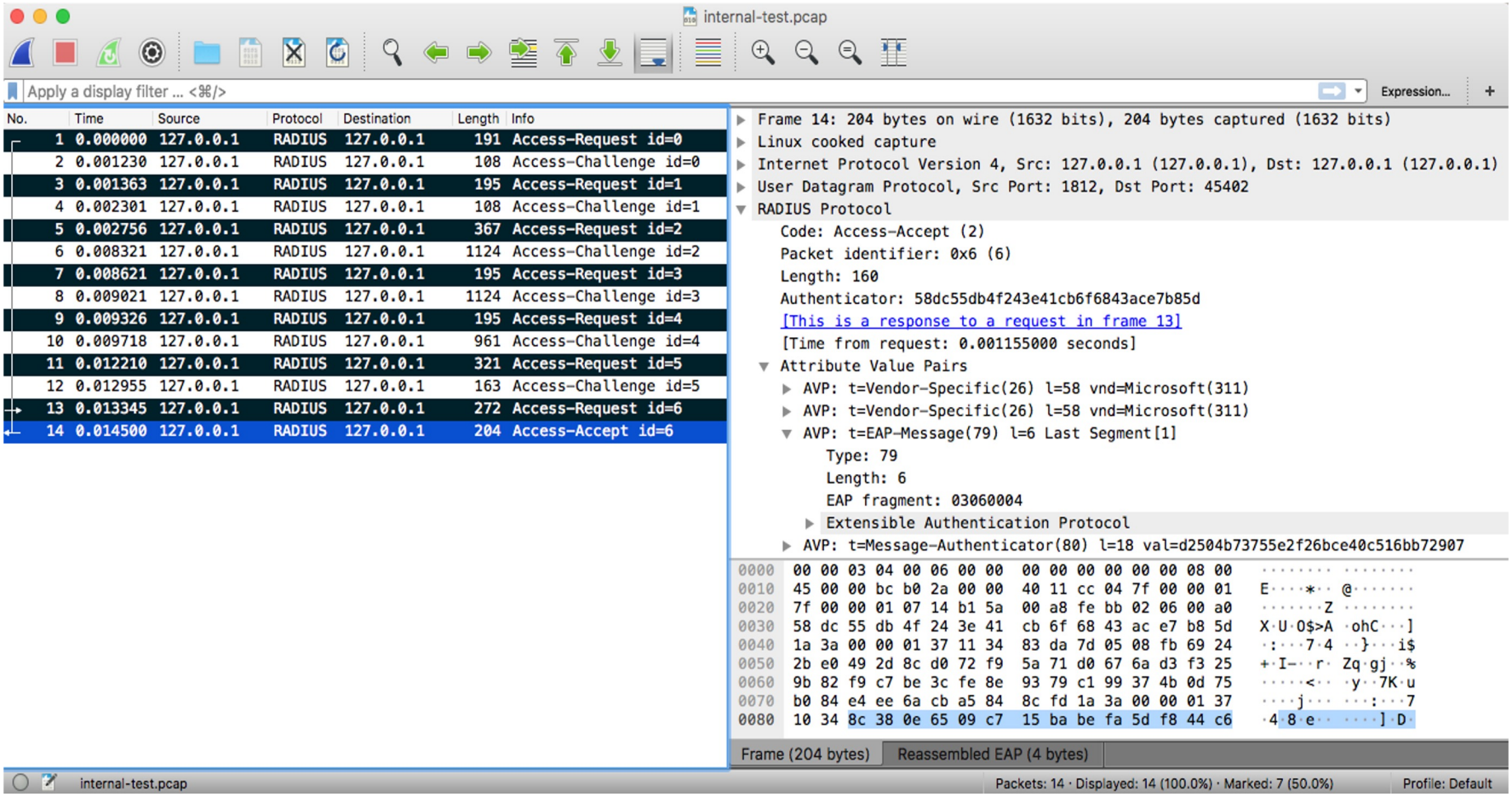
Compare FreeRadius Logs between Local and Remote Authentication

- Before compare, all logs and pcap files should be copied to your PC



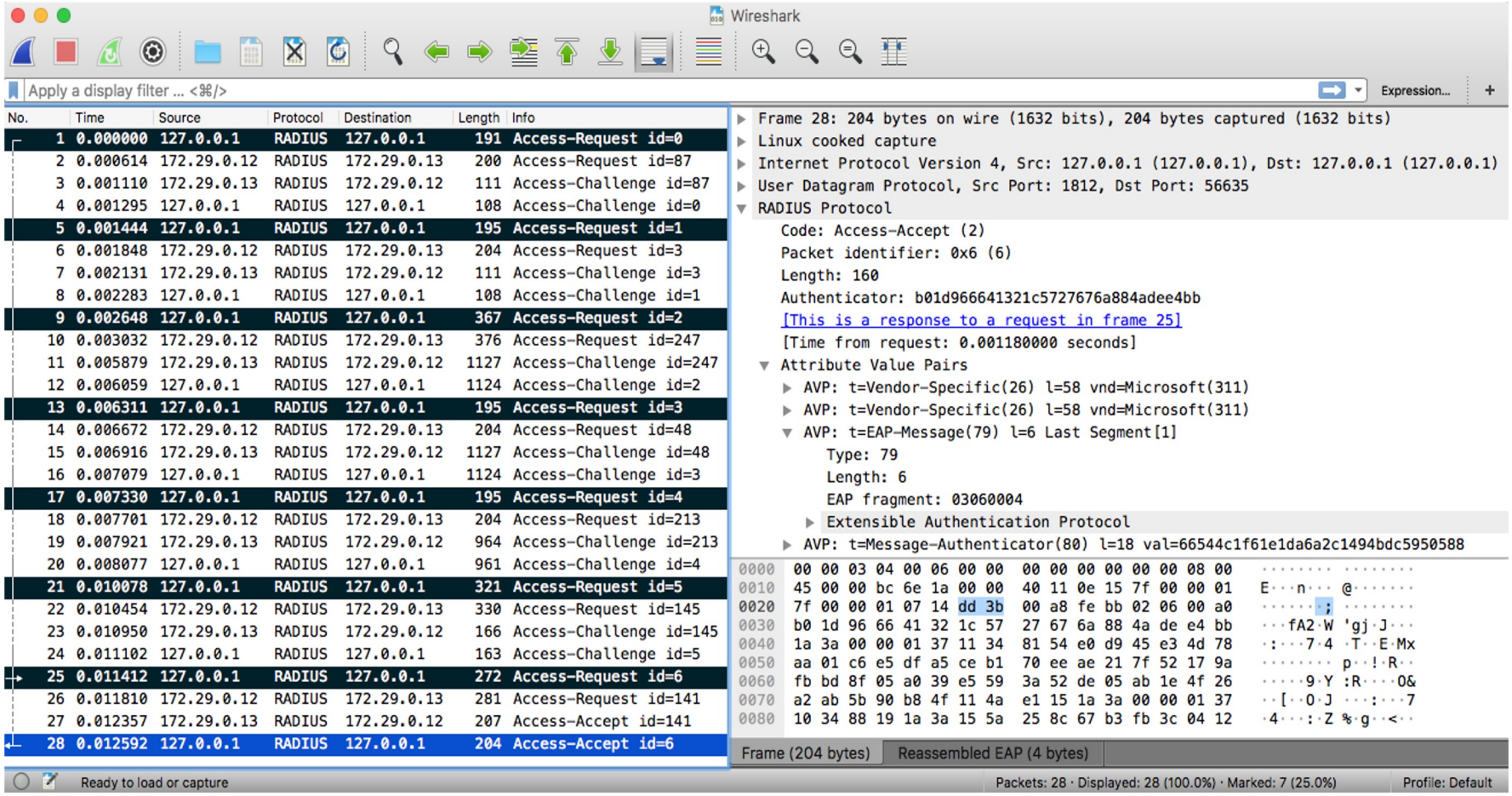
Compare Local and Remote Authentication Flow 4/5

Open Radius Packets from Local Authentication with WireShark



Compare Local and Remote Authentication Flow 5/5

Open Radius Packets from Remote Authentication with WireShark



Q&A

Thank you

Ask More Questions to:

- Minseok Jang msjang@kisti.re.kr

For Left Time

What would be improved of IRS?

1. Improve Logging config
   - Ref. Logging Guide @ FreeRadius Wiki
2. Add Lock-Out feature
   - Lock-out : Disable account after X auth fails in Y seconds
   - Anyone can Brute-Force on eduroam to find out one's password
   - Ref1. MS Windows Server has Lock-Out Feature in NPS server
   - Ref2. LockOut Guide @ FreeRadius Wiki
   - Ref3. SQL Guide @ FreeRadius Wiki
3. Improve Blackhole Routing using inner-tunnel
   - Ref. Rejecting auth from a specific realm @ FreeRadius Mailing List, 2009
4. Use Commercial SSL Server Certificate on RADIUS server
   - Some Institute use Comercial SSL Server Certificate to improve their Security
   - Comercial Server Cert can be applied similar way in the following reference;
     Ref. Use Let's Encrypt Certificates with FreeRADIUS
5. Examples on CUI (Chargeable User Identity)
   - Ref1. Chargeable User Identity for eduroam: with FreeRADIUS implementation guide @ Jisc
   - Ref2. Configuring an eduroam FreeRADIUS 3.0 server@ diamond.ac.uk
   - Ref3. Chargeable User Identity, RFC4372
6. Hardening TLS for WLAN 802.1X Authentication

Feedback & Request

Discuss among forks on the following issues

- Goods and Lacks on this session
- Request for Next XeAP Workshop

Retrospection on XeAP 2018 Session 3

- Huge tech divergence between trainees
  - Novice for Linux ~ current eduroam operator
- Many trainees practice commands for IRS in NRS