Implementación del Servicio de Movilidad eduroam en la UNMSM

Implementation of Service Mobility eduroam in San Marcos

Rossina Isabel Gonzales Calienes[1]

Facultad de Ingeniería Electrónica y Eléctrica, Universidad Nacional Mayor de San Marcos, Lima, Perú

Resumen— Este trabajo presenta los resultados del proyecto piloto eduroam en la UNMSM, que tiene como objetivo registrar todos los dispositivos access point, ubicados en las Facultades y Dependencias de la Universidad (que soporten el protocolo de autenticación IEEE 802.1x) al servidor RADIUS.

Abstract— This paper presents the results of the pilot eduroam in San Marcos, which aims to record every access point devices, located in the Faculties and Units of the University (that support IEEE 802.1x authentication protocol) to the RADIUS server.

Palabras clave— RAAP, eduroam, Wi-Fi, 802.11b/g, Servidor RADIUS,Autenticación y Cifrado EAP

Keys words— RAAP, eduroam, Wi-Fi 802.11b/g, RADIUS server, EAP Authentication and Encryption.[1]

I. INTRODUCCIÓN

eduroam es el servicio mundial de movilidad segura desarrollado para la comunidad de educación y de investigación, que permite acceso inalámbrico a Internet dentro del campus universitario y fuera de el cuando se visita instituciones participantes que también cuentan con el servicio eduroam.

Eduroam es una iniciativa que asume el Grupo de Trabajo de Movilidad (GT-Movilidad) de la RedCLARA, con la finalidad de contribuir a la mejora de la infraestructura de la red Latinoamericana, y proporcionar acceso seguro de los usuarios a sus Redes Nacionales de Investigación y Educación (RNIE) a través de procedimientos de autenticación de usuario, y conseguir la implementación de una solución funcional basada en la movilidad. A nivel nacional se encuentra el servidor RADIUS de la federación (FTLR), el cual tiene una lista de servidores IdP y los dominios asociados. Este servidor FTLR recibe solicitudes de los IdP y servidores de la confederación que están conectadas, para reenviarlas desde ellos al servidor apropiado, o en caso de una solicitud de un destino para una confederación a un servidor de la confederación.

En abril de 2012 el Comité de Gobernanza Mundial de eduroam (GeGC) reconoce al Perú como Operador Roaming de eduroam permitiendo que el servicio se extienda a las Universidades, Instituciones y Centros de investigación de todo el país a través de eduroam-pe operado por INICTEL-UNI como nodo de la Red Académica Peruana (RAAP).

Desde el 14 de febrero del 2014 la Universidad Nacional Mayor de San Marcos - UNMSM ya forma parte de los más de 5,000 puntos (Universidades, instituciones y centros de investigación, y Hotspot de Proveedores de Servicio del mundo) adheridos a la iniciativa de eduroam.

II. MARCO TEÓRICO

*A. ¿Qué es **eduroam**?*

Eduroam (contracción de **education roaming**) es el servicio mundial de movilidad segura desarrollado para la comunidad académica y de investigación. **eduroam** persigue el lema "*abre tu portátil y estás conectado*".

El servicio permite que estudiantes, investigadores y personal de las instituciones participantes tengan conectividad Internet a través de su propio campus y cuando visitan otras instituciones participantes.

eduroam-pe forma parte del espacio de movilidad mundial operado por redes académicas europeas y TERENA *(Trans-European Research and Education Networking Association)*las cuales cubren a Europa a través de **eduroam** Europa, y se extienden a **eduroam Canadá**, **eduroam US**, y **eduroam APAN** (Asia y Pacífico).

En la Fig. 1, se aprecia el mapa con la ubicación geográfica de los países que ofrecen el Servicio de Movilidad mundial **eduroam** y en la Fig. 2, se muestra

[1] Rossina Gonzales Calienes, E-mail: rgonzalesc1@unmsm.edu.pe
Recibido: Setiembre 2014 / Aceptado: Octubre 2014

la ubicación de los puntos de Servicio **eduroam** en Lima-Perú entre ellos la UNMSM.

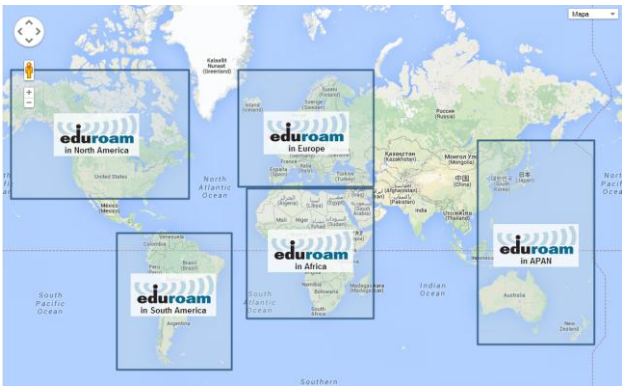

Fig.1. Despliegue a nivel mundial del Servicio de Movilidad mundial **eduroam.**

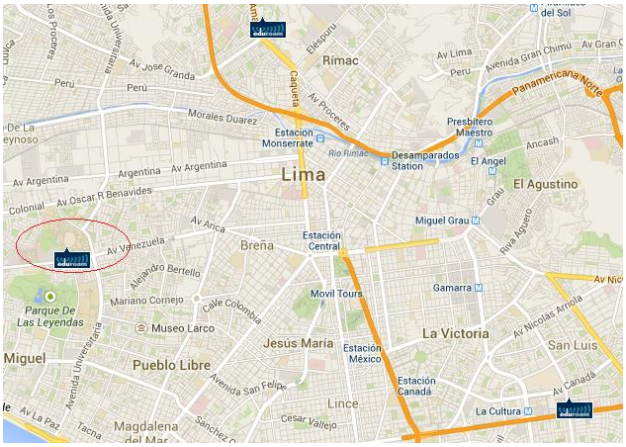

Fig. 2. La UNMSM considerada entre los 03 puntos de Servicio **eduroam** en Lima- Perú.

*B. ¿Cómo trabaja **eduroam**?*

Cuando el usuario se conecta a la red suministra sus credenciales al autenticador (dispositivo de control de acceso) para que lo verifique. Las credenciales deberían siempre incluir un nombre de usuario y un dominio que se traduce en una credencial que se parece a una dirección e-mail: pepe@institucion_B.pe (user@dominio.topleveldomain), [1].

En la Fig. 3, se observa que el usuario visitante Pepe utiliza la red, y el servidor RADIUS de la Institución A (local) se dará cuenta de que el dominio del usuario no es el dominio del cual se sirve. Allí es donde el mecanismo de RADIUS proxy ingresa y asegura de que las credenciales EAP encapsuladas sean transportadas hacia el servidor RADIUS de la Institución B (*home RADIUS server*). De hecho, el servidor RADIUS sólo tiene que remitir la petición a un servidor RADIUS de alto nivel (higher-level RADIUS proxy server). Este servidor proxy conoce a todos los servidores RADIUS en la constelación de *roaming* y reenvía la solicitud al servidor que se sabe puede mantener este dominio. Es decir, si el dominio del usuario visitante pertenece a una institución del país, la solicitud es enviada al servidor RADIUS Proxy nacional y de allí al servidor RADIUS de la institución de donde proviene el usuario; si el dominio del usuario visitante pertenece a una institución de otro país, la solicitud es enviada al servidor RADIUS Proxy nacional para derivarla al servidor RADIUS (Top-level) de Europa, el cual encamina la solicitud hasta el servidor RADIUS Proxy nacional de donde proviene el usuario visitante. El home RADIUS server, se instala en la red de origen del visitante, ya sea en el mismo país o en el extranjero, donde el usuario se autentica contra una base de datos de usuario local. El servidor RADIUS local sólo tiene que saber a qué proxy deben ser enviadas las peticiones de usuario desconocido.

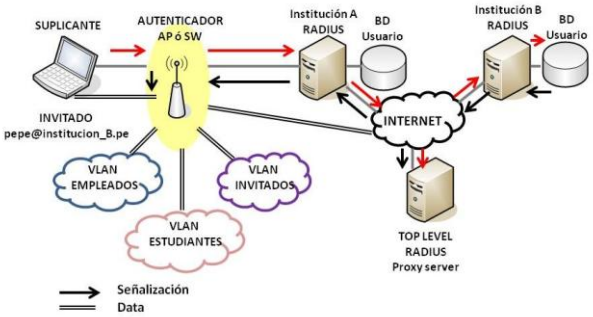

Fig. 3. Infraestructura de red del Servicio de Movilidad **eduroam**

*1. Proceso de autenticación y autorización en **eduroam***

En base a la Fig. 4, se explica dicho proceso:

(1) El dispositivo móvil de Rosa se une a SSID **eduroam.**

(2) El cliente sobre el dispositivo móvil de Rosa envía una solicitud de conexión a la red **eduroam** de INICTEL como rgonzalesc1@unmsm.edu.pe.

(3) El servidor local RADIUS de INICTEL (que está conectado a la infraestructura inalámbrica de INICTEL) reconoce que el dominio de Rosa (@unmsm.edu.pe) no es local, por lo que reenvía la solicitud al servidor RADIUS nacional.

(4) El servidor RADIUS nacional envía la solicitud al destino apropiado, dominio unmsm.edu.pe.

(5) El servidor RADIUS de UNMSM, envía un certificado de desafío (certificate challenge) de regreso a Rosa. Este es el paso que permitirá a Rosa estar segura que el SSID eduroam de INICTEL es un miembro de confianza de la red de **eduroam**.

(6) Si el certificado fue cargado previamente en el dispositivo de Rosa, el dispositivo aceptará el

certificado y establece un túnel encriptado SSL/TLS entre el dispositivo de Rosa y el servidor RADIUS home (origen) es decir el servidor RADIUS de UNMSM.

(7) Una vez establecido el túnel encriptado entre el dispositivo de Rosa y el servidor RADIUS de UNMSM, las credenciales de Rosa son enviadas a través del túnel encriptado SSL/TLS entre el dispositivo de Rosa y el servidor RADIUS de UNMSM para la verificación. Este paso de autenticación permite al servidor RADIUS conectarse al Servicio de Directorio de la institución.

(8) Sobre la autenticación exitosa, el servidor RADIUS de UNMSM envía un Access-accept y algún material clave a la infraestructura de INICTEL (fuera del túnel SSL) y algún material clave privado a Rosa (dentro del túnel).

(9) La infraestructura inalámbrica **eduroam** de INICTEL negocia con el dispositivo de Rosa el intercambio de la clave de encriptación para permitir el acceso a la red y habilitar la encriptación entre el dispositivo de Rosa y los puntos de acceso inalámbrico de INICTEL.

(10) Luego Rosa puede conectarse a SSID **eduroam** en INICTEL y disponer de la conectividad autenticada y encriptada entre su dispositivo y la red inalámbrica de INICTEL.

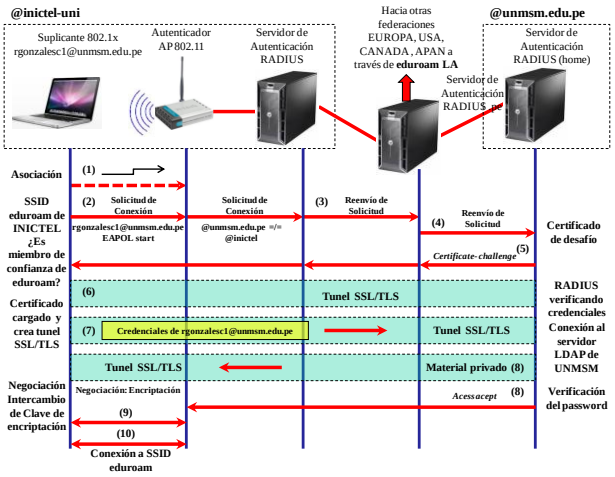

Fig. 4: Proceso de autenticación y autorización en **eduroam**

*C. Infraestructura de **eduroam***

1. Definiciones y conceptos generales

Suplicante: Es un producto de software (a veces es parte del sistema operativo o como un programa separado) que usa el protocolo IEEE 802.1x para enviar la información de solicitud de autenticación usando EAP. Los suplicantes son instalados y operan en dispositivos de cómputo de usuarios finales (Notebooks, tablets, PDA, teléfonos celulares (smartphones) con Wi-Fi habilitado, entre otros) [2].

Access Point (autenticador): Son dispositivos de acceso LAN inalámbrico conforme al estándar IEEE 802.11 y necesitan tener la capacidad IEEE 802.1x. Deben tener la capacidad de reenviar las solicitudes de acceso desde un suplicante al servidor RADIUS del Proveedor de Servicio (red visitada), para dar acceso a red luego de una correcta autenticación, permitiendo la asignación de usuarios a una VLAN específica basada en la información recibida desde el servidor RADIUS. Además los access point intercambian material clave (vectores de inicialización, claves públicas y sesiones, etc.) con sistemas de clientes para impedir sesiones hijacking.

Switches: Necesitan ser capaces de reenviar las solicitudes de acceso que viene de un suplicante al servidor RADIUS del Proveedor de Servicio, para permitir el acceso a red tras una apropiada autenticación y posiblemente asignar usuarios a VLANs específicas basadas en la información recibida del servidor RADIUS.

2. Estándar IEEE 802.1x

Una red habilitada con el estándar IEEE 802.1x, permite el acceso a red solo a usuarios autorizados, esto se logra cuando se tiene creado previamente la cuenta del usuario. El sistema operativo debe soportar IEEE 802.1x, [3] [4] [5].

La ventaja para el usuario es que puede desplazarse libremente de una red a otra. Las redes pueden ser fijas o inalámbricas. En el caso de redes inalámbricas esto es importante, ya que no depende el estar físicamente conectado a un switch para conseguir conectividad como sucede en redes fijas.

El principio de funcionamiento de IEEE 802.1x se centra en que los switches y access point que realizan la autenticación IEEE 802.1x sólo permitirán el tráfico 802.1x cuando los usuarios se conecten a estos dispositivos. Una vez que los usuarios han sido autenticados y autorizados se permitirá cursar su tráfico a través de ellos.

Para el caso de redes alambradas Ethernet se habilitará en el puerto del switch para el usuario autenticado, y en redes inalámbricas será el acccess point quien negociará una clave única con la interfaz inalámbrica del usuario autenticado. La clave negociada durante la autenticación 802.1x es dinámica, además de ser única para cada usuario y también cambiante.

La clave única se usa para encriptar el tráfico entre el usuario y el access point.

La autorización en IEEE 802.1x se realiza a través del Protocolo de Autenticación Extensible (EAP - Extensible Authentication Protocol), que permite que las solicitudes de clientes sea reenviado al servidor de autenticación, bajo el uso de diversos métodos de autenticación.

3. Arquitectura

Las tramas 802.1x añaden funcionalidad a los componentes existentes en una red. Por lo tanto, no son necesarios componentes adicionales.

En una red fija, el terminal (PC o portátil, por ejemplo) tiene que tener una tarjeta de red (NIC), y el sistema operativo debe tener una funcionalidad que se le denomina suplicante 802.1x en la tarjeta, este es el cliente.

El puerto al que se conectará la terminal se encuentra en un switch que tiene activado 802.1x. Al switch se le denomina el autenticador.

Sobre la base de comandos 802.1x, el switch puede abrir y cerrar una conexión en el puerto. El tercer componente de la arquitectura es el servidor de autenticación. En general, un switch preguntará a un servidor RADIUS para verificar si el usuario está permitido a usar el puerto, y a que VLAN debe ir el tráfico.

Cuando 802.1x se aplica a una red inalámbrica, un dispositivo de control de acceso inalámbrico sustituye al switch como el autenticador. No es relevante qué protocolo de transporte inalámbrico (802.11b ó protocolos como el 802.11g) se utiliza.

Cuando un usuario se conecta a la red suministra sus credenciales al autenticador (el dispositivo de control de acceso) que verifica esto usando el RADIUS backend. Las credenciales deberían siempre incluir un nombre de usuario y un dominio que se traduce en una credencial que se parece a una dirección e-mail (user@dominio.topleveldomain).

Si un usuario visitante utiliza la red, el servidor RADIUS local se dará cuenta de que el dominio del usuario no es el dominio del cual se sirve. Ahí es donde el mecanismo de RADIUS proxy entra y asegura de que las credenciales EAP encapsuladas sean transportadas hacia el home RADIUS server. De hecho, el servidor RADIUS sólo tiene que remitir la petición a un servidor RADIUS de alto nivel (higher-level RADIUS proxy server). Este servidor proxy conoce a todos los servidores RADIUS en la constelación de roaming y reenvía la solicitud al servidor que se sabe puede mantener este dominio.

El home RADIUS server, se instala en la red de origen (home network) del visitante, ya sea en el mismo país o en el extranjero, donde el usuario se autentica contra una base de datos de usuario local.

El servidor RADIUS local sólo tiene que saber a qué proxy deben ser enviadas las peticiones de usuario desconocido.

Cuando una nueva red entra en este acuerdo de roaming, sólo el proxy tiene que ser actualizado.

Respecto a la pila de protocolos del formato IEEE 802.1x, la información de autenticación se realiza sobre el protocolo de autenticación extensible (EAP, RFC 2284), un protocolo que permite el uso de cualquier método de autenticación, como nombre de usuario/contraseña, certificados, OTP (One Time Password, por ejemplo a través de SMS) o credenciales SIM-card de operadores móviles. Estos mecanismos se aplican en los tipos de EAP: MD5, TLS, TTLS, MS-CHAPv2, PEAP, Mob@c, y EAP-SIM.

Tanto el solicitante y el home RADIUS server deberían utilizar el mismo tipo de EAP. El dispositivo de control de acceso, switch o servidores proxy RADIUS no tienen que ser conscientes del tipo de EAP.

En la actualidad, TLS (Transport Layer Security), TTLS (Túnel Transport Layer Security) y PEAP (EAP protegido) son los candidatos más serios para su aplicación inmediata. Pruebas adicionales se realizaron con la autenticación basada en el envío de contraseñas a través de SMS.

TLS, TTLS y PEAP configuraran una conexión TLS entre el cliente y el dispositivo de control de acceso basado en un certificado de servidor RADIUS. Este mecanismo de autenticación mutua puede impedir ataques Man in the Middle. Entonces TLS usa un certificado de cliente para autenticar al usuario, mientras que TTLS es generalmente utilizado para el transporte de nombre de usuario/ contraseña. Dado que tanto TTLS y PEAP son protocolos de túnel, cualquier otro protocolo puede ser utilizado sobre ellos. MOBAC es un ejemplo de esto, implementando One Time Password a través de SMS.

Si el usuario está verificado apropiadamente contra el proceso final de autenticación de origen (home authentication backend), que puede ser LDAP, por ejemplo, él será autenticado y el home RADIUS server pasa un acuse de recibo al dispositivo de control de acceso. Cuando un usuario se encuentra en su red de origen (home network), el servidor RADIUS puede decir al autenticador en cual tráfico de VLAN de usuario debe residir. Entonces, el dispositivo de control de acceso pasa el tráfico de usuario en esta VLAN hasta la de-autenticación. La conmutación VLAN se basa en el estándar 802.1Q. Un visitante ingresará en una VLAN-huésped determinada por el servidor RADIUS de la red visitada.

En esta etapa del proceso, la conectividad Ethernet se proporciona, después del cual los mecanismos habituales para la obtención de conectividad IP pueden desempeñar su papel, como ofrecer al cliente una dirección IP a través de DHCP. De hecho, cualquier cosa es posible en la capa 3, después del proceso de autenticación: no sólo el protocolo IP, cualquier otro protocolo de capa 3 puede ser transportado (IPv6, IPSec, IPX, PPPoE etc.) y cualquier mecanismo de la capa 3 (VPN, Multicast, etc NAT) encuentra una capa dos transparente, capa de transporte.

Cuando el usuario retira el cable o sale del área de cobertura de un dispositivo de control de acceso inalámbrico, el dispositivo de control de acceso detecta la interrupción de la conexión y el puerto será cerrado. Cada vez más Suplicantes también tienen incorporado la posibilidad de desconectarse de una red, y que les permite volver a conectarse con credenciales diferentes para acceder a otras VLAN [5].

4. Escalabilidad

Como se mencionó antes, el servidor RADIUS local sólo tiene que saber a qué proxy deben ser enviadas las solicitudes de usuario desconocido.

Cuando una nueva red entra en este acuerdo de roaming, sólo el proxy tiene que ser actualizado.

Para ampliar o extender esta infraestructura de roaming a una escala Europea, un proxy RADIUS sobre un nivel internacional es el único componente que debe ser agregado [5].

Cuando una nueva institución ingresa a la constelación, sólo su dominio tiene que ser ingresado al servidor Proxy RADIUS, no en los servidores de otras instituciones. Lo mismo ocurre cuando se agrega un grupo de instituciones en un país que ingresa en la constelación: el nivel superior de servidor Proxy RADIUS (Top Level) debe ser actualizado con el nuevo dominio de alto nivel (high-level), por ejemplo ". nl", tras lo cual el mecanismo de reenvío trabaja por cada institución en la constelación. Siempre es posible realizar relaciones bilaterales entre los servidores que intercambian mucho tráfico, o tráfico que sólo es localmente relevante.

El uso de RADIUS también hace que sea fácil de conectar la infraestructura roaming existente a un operador de red móvil existente (WiFi, GPRS o UMTS). La infraestructura de RADIUS como se describe aquí puede introducir bucles en el flujo de mensajes, que puede conducir a la falla de servidores RADIUS. Para evitar esto, cada servidor RADIUS puede ser obligado a no reenviar mensajes destinados al dominio que maneja. Además, el proxy puede filtrar estos eventos, y observar la cantidad de saltos en los mensajes.

Los dispositivos de control de acceso pueden ser instalados en pares, aunque esto no suele hacerse debido a los altos costos. Además, cada dispositivo de control de acceso puede ser configurado para preguntar a dos (o más) servidores RADIUS. Cuando un servidor RADIUS falla, el otro puede hacerse cargo. El mismo mecanismo se puede utilizar entre servidores RADIUS en la infraestructura proxy.

Puesto que en promedio, el software de los servidores RADIUS no consume muchos recursos de hardware, una computadora de características promedio podría servir decenas de solicitudes de autenticación, o incluso cientos de solicitudes de reenvío por segundo.

La autenticación es sólo necesaria en el comienzo de una sesión de usuario y cuando un usuario se mueve entre los dispositivos de control de acceso, por lo tanto un servidor RADIUS en un nivel proxy nacional puede servir potencialmente miles de sesiones de usuarios al mismo tiempo.

La escalabilidad en términos de rendimiento de procesamiento es implícitamente lograda por el hecho de que cada dispositivo de control de acceso se encarga del cifrado de datos en la capa 2 a la velocidad de cable.

III. METODOLOGÍA

Para el desarrollo de proyecto se realizaron las siguientes tareas :

1. Recolección de información: Se estudió sobre los fundamentos y alcances de eduroam a través de los informes generados por los Grupos de Trabajo de GEANT.

2. Con la disponibilidad de una computadora ubicada físicamente en la Red Telemática de la UNMSM, se realizaron los siguientes pasos:

- Se instaló el Sistema Operativo Linux Debian v. 6.0 en una estación de trabajo con un mínimo con 1GB de Memoria RAM y un espacio de Disco de 8 GB con acceso a Internet para instalar los paquetes de los repositorios Debian Squeeze.
- Conexión a la red LAN de la UNMSM, configurando el puerto de red del switch correspondiente a la VLAN 128 designada para redes Wi-Fi.
- Asignación de una dirección IP: 172.16.128.80; para la interface de red de la estación de trabajo, el cual pertenece a la VLAN 128: 172.16.128.0/21.
- Configuración del nat estático de la dirección privada 172.16.128.80 a la dirección pública 190.81.63.180/29 con permisos totales en ambos sentidos, en el firewall de la Red Telemática para su conexión y acceso remoto.

3. Instalación y configuración de un servidor RADIUS local basado en Linux:

- El archivo "sources.list" donde se enlistan las fuentes o repositorios de Debian debe tener como mínimo lo siguiente en el archivo /etc/apt/sources.list el cualse aprecia en la Fig.5.

```
deb http://ftp.es.debian.org/debian/ squeeze main
deb-src http://ftp.es.debian.org/debian/ squeeze main
deb http://security.debian.org/ squeeze/updates main
deb-src http://security.debian.org/ squeeze/updates main
deb http://ftp.es.debian.org/debian/ squeeze-updates main
deb-src http://ftp.es.debian.org/debian/ squeeze-updates main
```

Fig.5. Archivo /etc/apt/sources.list

Instalación de paquetes y librerías necesarias: `apt-get install freeradius freeradius-ldap freeradius-sql make pkg-config vim nmap mysql-server mysql-client libssl-dev libgnutls-dev libsnmp-dev libmysqlclient-dev libldap-dev libtool libpcap0.8-dev gnutls-bin`

En la Fig. 6 se comprueba la versión actual del paquete openssl.

```
root@radius:~# openssl version
OpenSSL 0.9.8o 01 Jun 2010
root@radius:~#
```

Fig. 6. Versión OpenSSL instalada.

En la Fig. 7 se aprecia la comprobación de la versión actual del paquete freeradius

```
root@radius:~# freeradius -v
freeradius: FreeRADIUS Version 2.1.10, for host x86_64-pc-linux-gnu, built on Se
p 11 2012 at 17:06:46
Copyright (C) 1999-2010 The FreeRADIUS server project and contributors.
There is NO warranty; not even for MERCHANTABILITY or FITNESS FOR A
PARTICULAR PURPOSE.
```

Fig. 7. Paquete FreeRADIUS instalado.

- Creación de una autoridad certificadora y las firmas digitales de los certificados emitidos hacia el servidor RADIUS.
- Creación de un directorio con nombre eduroam dentro de la carpeta "/etc":
  `mkdir /etc/eduroam`
- Dentro del directorio /etc/eduroam, se configuran los certificados digitales y archivos necesarios y se edita archivo: /etc/ssl/openssl.cnf. En la Fig. 8 se aprecia los parámetros modificados:

```
dir             = /etc/eduroam          #
#dir             = ./demoCA
certs           = $dir/certs            #
crl_dir         = $dir/crl              #
database        = $dir/index.txt        #
#unique_subject = no                    #
                                        #
new_certs_dir   = $dir/newcerts         #

certificate     = $dir/ca.crt     # The CA
#certificate    = $dir/cacert.pem
serial          = $dir/serial           #
crlnumber       = $dir/crlnumber        #
                                        #
crl             = $dir/crl.pem          #
private_key     = $dir/private/ca.key # T
#private_key    = $dir/private/cakey.pem
RANDFILE        = $dir/private/.rand    #
```

Fig. 8. Parámetros modificados en el archivo `etc/ssl/openssl.cnf`.

- Instalar los paquetes necesarios para la configuración de una autoridad certificadora con formato estándar x.509 y creación de certificados digitales para los servidores RADIUS y usuarios itinerantes:

```
openssl req -new -x509 -extensions
v3_ca -keyout private/ca.key -out
ca.crt

openssl req -new -keyout
radius.key -out
radius.unmsm.edu.pe.csr -days 3650

cp
/usr/share/doc/freeradius/examples
/certs/xpextensions /etc/eduroam/

openssl ca -policy policy_anything
-out radius.unmsm.edu.pe.crt -
extensions xpserver_ext -extfile
xpextensions -infiles
radius.unmsm.edu.pe.csr

openssl req -new -keyout test.key
-out test.unmsm.edu.pe.csr -days
3650

openssl ca -policy policy_anything
-out test.unmsm.edu.pe.crt -
extensions xpclient_ext -extfile
xpextensions -infiles
test.unmsm.edu.pe.csr

openssl pkcs12 -export -in
test.unmsm.edu.pe.crt -inkey
test.key -out test.p12 -clcerts

openssl x509 -inform PEM -outform
DER -in ca.crt -out ca.der

openssl dhparam -check -text -5
512 -out dh

dd if=/dev/urandom of=random
count=2
```

En la Fig.9 se visualiza las claves GPG generadas para el intercambio de secretos entre servidores RADIUS de la UNMSM y servidor RADIUS confederado Latinoamericano-LATLR, ubicado en el nodo INICTEL-UNI institución miembro de la RAAP. En coordinación con el personal técnico del INICTEL-UNI, se realizó la Generación de claves GPG para el intercambio de secretos entre servidores RADIUS.

Conexión del servidor RADIUS con la base de datos LDAP en donde están almacenados los usuarios

de UNMSM. La Universidad cuenta con un servidor LDAP local (Linux) el cual almacena toda la base de datos de los usuarios de correo electrónico institucional de la UNMSM; y se sincronizan con Google utilizando el aplicativo Google Active Directory Sync.

```
root@radius:~# gpg --list-keys
/root/.gnupg/pubring.gpg
------------------------
pub   2048R/4EB4A594 2012-09-22
uid                  Rossina Gonzales Calienes (Clave GPG d
e Rossina Gonzales) <rgonzalescl@unmsm.edu.pe>
sub   2048R/A2BBD0F9 2012-09-22
```

Fig. 9. Clave GPG generada.

La configuración en el servidor RADIUS es como sigue:

```
ldap {
server = ldap.unmsm.edu.pe:389
identity =
"uid=eduroam,ou=aplicaciones,dc=unms
m,dc=edu,dc=pe"
password = eduROAM,,unmsm-+
basedn = "dc=unmsm,dc=edu,dc=pe"
…
}
```

- Configuración de un Cliente RADIUS (access point o wireless controller), En la Fig. 10 se aprecia dicha configuración al editar el archivo /etc/freeradius/clients.conf:

```
client localhost {
        ipaddr = 127.0.1.1
        secret          = inictel
        require_message_authenticator = no
        shortname       = org-UNMSM
        nastype     = other
}
client Test-AP-UNMSM {
ipaddr = 172.16.128.90
netmask = 32
secret = 123456
require_message_authenticator = no
shortname = ap-UNMSM
nastype = dlink
}

client FTLR-Pe {
ipaddr = 190.12.88.20
netmask = 32
require_message_authenticator = no
secret = inictel
shortname = org-UNMSM
}
```

Fig. 10. Registro de un AP en el servidor RADIUS a clave GPG generada

- Configuración de un access point - AP con el SSID eduroam utilizando los protocolos autenticación y cifrado WPA2 y IEEE 802.1x. En la Fig. 11 se visualiza los parámetros de configuaración para un punto de acceso.

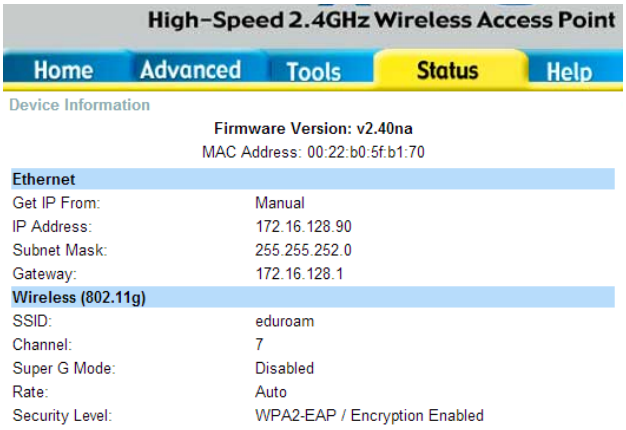

Fig. 11. Parámetros de configuración de un AP

- Culminación de la etapa de autenticación que incluye la relación con la base de datos de credenciales de usuarios @unmsm.edu.pe de toda la universidad, cuyos clientes software están disponibles en **https://cat.eduroam.org/**, desde donde se descargará el suplicante. En la Fig.12 aprecia el sitio web, donde se descarga el software suplicsnte para usuarios de San Marcos.

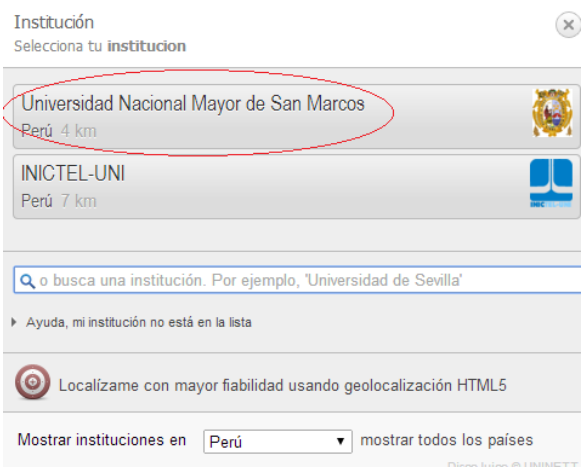

Fig. 12. URL donde se descarga el software suplicante para usuarios de la UNMSM

Finalmente, se comprobó el roaming de acceso (itinerancia) de usuarios de la UNMSM en el INICTEL-UNI.

III. RESULTADOS

El servicio de Movilidad **eduroam** ha sido instalado en la UNMSM como proyecto piloto en las instalaciones de la Red Telemática.
Se ha publicado el servicio en la página web de Red Telemática, por ser la oficina responsable de administrar los servicios TI de la Universidad.

Se recomienda como siguiente paso el despliegue de este servicio en todo el Campus Universitario, el que consistirá en:

- Registrar todos los dispositivos access point - AP, ubicados en las Facultades y Dependencias de la Universidad (que soporten el protocolo de autenticación IEEE 802.1x) al servidor RADIUS.
- Anunciar el SSID **eduroam** en la Wi-Fi y publicarla como la Wi-Fi oficial de la UNMSM.
- Replicar el servicio en las Sedes Externas de la UNMSM.
- Señalizar todas las zonas Wi-Fi **eduroam** a través de la página web de la Universidad.

IV. CONCLUSIONES

eduroam es una plataforma desarrollada para la investigación internacional y la comunidad educativa. El servicio de movilidad **eduroam** implementado en la UNMSM facilitará el acceso a la información de manera sencilla y segura a investigadores, docentes y estudiantes.

REFERENCIAS

[1] Eduroam [OnLine]. Disponible en: http://www.eduroam.pe

[2] S. Winter, T. Kersting, P. Dekkers, L. Guido, S. Papageorgiou, J. Mohacsi, R. Papez, M. Milinovic, D. Penezic, J. Rauschenbach, J. Tomasek, K. Wierenga, T. Wolniewicz, J. Macias-Luna, I. Thomson. "Deliverable DJ5.1.5, 3: Inter-NREN Roaming Infraestructure and Service Support Cookbook". *GEANT2*. 29 de Octubre del 2008,. Third Edition. [Online], Disponible en: http://www.eduroam.org/downloads/docs/GN2-08-230-DJ5.1.5.3-eduroamCookbook.pdf .

[3] E. Dobbelsteijn Movility Task Force.Deriverable D: Inventory of 802.1X-based solutions for inter-NRENs roaming. Version 1.2 [Online], Disponible en: http://www.terena.org/activities/tf-mobility/deliverables/delD/DelD_v1.2-f.pdf

[4] http://www.eduroam.edu.au/tech/install/radius

[5] J. Quiroz, J. Quinto, "Guía del Curso eduroam nivel ldP":, *INICTEL-UNI*, Perú. 2012.