Despliegue del Servicio eduroam en el Campus Universitario de la UNMSM

Rossina Isabel Gonzales Calienes[1]

Red Telemática, Universidad Nacional Mayor de San Marcos, Av. Venezuela Cdra. 35, Ciudad Universitaria, Lima 1- Perú
rgonzalesc1@unmsm.edu.pe

Resumen. El servicio *eduroam (education roaming)* es el servicio mundial de movilidad segura desarrollado para la comunidad de educación e investigación, permitiendo que los estudiantes, investigadores y académicos obtengan conectividad a Internet a través de su propio campus y cuando visitan otras instituciones participantes con solo encender su computadora portátil. El despliegue del proyecto *eduroam* en la UNMSM, consiste en registrar 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. El servidor RADIUS actualmente instalado en la Red Telemática es responsable de la autenticación de sus propios usuarios (locales y visitantes de otras instituciones), y del reenvío de solicitudes de usuarios visitantes al servidor RADIUS confederado Latinoamericano-LATLR, ubicado en el nodo INICTEL-UNI institución miembro de la RAAP. 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.

Palabras Clave: RAAP, *eduroam*, Wi-Fi, 802.11b/g, Servidor RADIUS, Autenticación y Cifrado EAP.

1 Introducción

El servicio *eduroam* es una iniciativa que asume el Grupo de trabajo de Movilidad (GT-Movilidad) de la RedCLARA, con la finalidad de contribuir en 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

[1] Rossina Isabel Gonzales Calienes, Email: rgonzalesc1@unmsm.edu.pe

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***.**

1.1 ¿Qué es eduroam?

El servicio *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.

El servicio *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).

1.2 ¿Cómo trabaja eduroam? [1]

Cuando un usuario se conecta a la red suministra sus credenciales al autenticador (el dispositivo de control de acceso) para que sea verificado. Las credenciales deberán incluir un nombre de usuario y un dominio, las cuales tienen el formato de una dirección e-mail: pepe@institucion_B.pe (user@dominio.topleveldomain).

De la Fig. 1, el usuario visitante Pepe utiliza la red, y el servidor RADIUS de la Institución A (local) se dá cuenta de que el dominio del usuario no es el dominio del cual se sirve. En ese momento, el mecanismo de RADIUS proxy asegura de que las credenciales encapsuladas de seguridad de la información EAP 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.

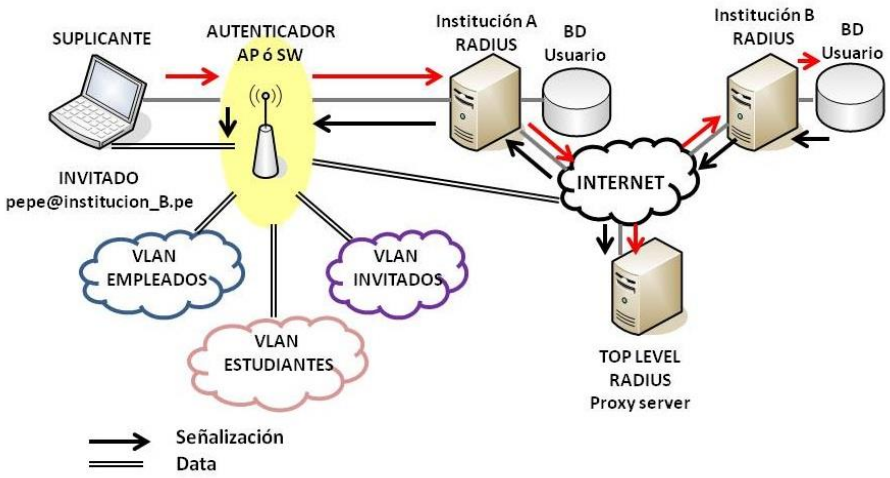

Fig. 1. Infraestructura de red del Servicio de Movilidad *eduroam*

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.

1.2.1 Proceso de Autenticación eduroam

De la Fig. 2, 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.

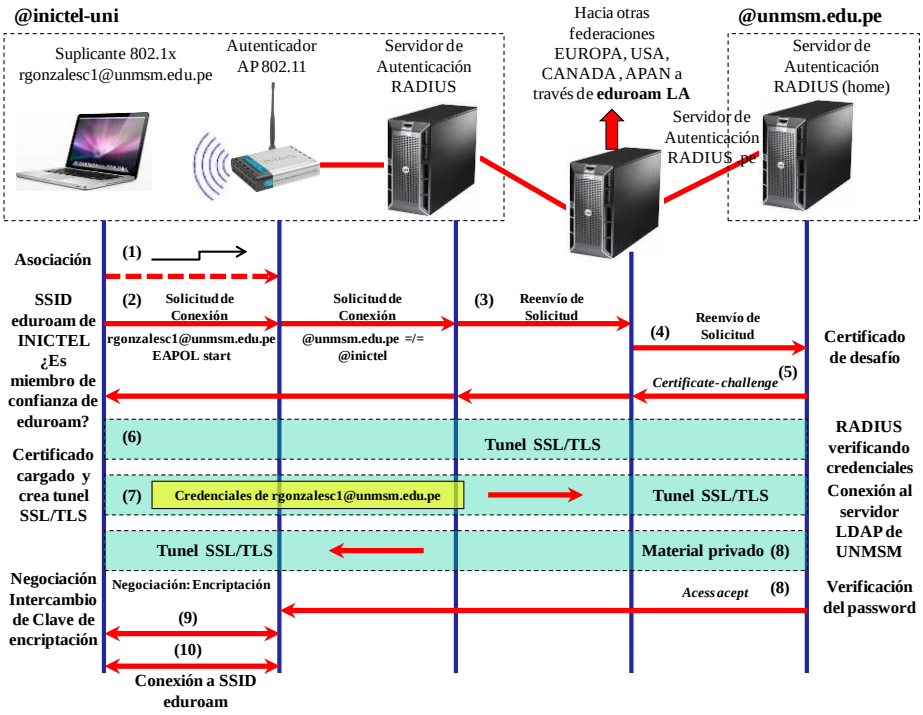

Fig. 2: Proceso de autenticación y autorización en *eduroam*

1.2.2 Definiciones y conceptos generales con respecto a la infraestructura eduroam [2]

Suplicante: Es un 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 (laptops, notebooks, tablets, PDAs y smartphones con Wi-Fi habilitado, entre otros).

Access Point (autenticador): Son dispositivos de acceso LAN inalámbrico que cumplen los estándares IEEE 802.11 y IEEE 802.1x. Tienen la capacidad de reenviar las solicitudes de acceso desde un suplicante al servidor RADIUS del Proveedor de Servicio (red visitada), para dar acceso a la 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 provienen de un suplicante al servidor RADIUS del Proveedor de Servicio, para permitir el acceso a la red tras una apropiada autenticación y asignar usuarios a las VLANs específicas basadas en la información recibida del servidor RADIUS.

Estándar IEEE 802.1x [3] [4] [5]: Una red habilitada con el estándar IEEE 802.1x, permite el acceso a la red solo a los usuarios autorizados.

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 sean reenviadas al servidor de autenticación, bajo el uso de diversos métodos de autenticación.

Arquitectura [5]: En una red fija, el terminal (PC o portátil, por ejemplo) tiene una tarjeta de red (NIC), y el sistema operativo deberá tener una funcionalidad denominada suplicante IEEE 802.1x en la tarjeta, que será el cliente.

El puerto del switch al que se conecta el terminal tiene activado el IEEE 802.1x. Entonces al switch se le denominará el autenticador. Sobre la base de comandos IEEE 802.1x, el switch puede abrir y cerrar una conexión en el puerto.

El tercer componente de la arquitectura es el servidor de autenticación. El switch preguntará al servidor RADIUS para verificar si el usuario está permitido a usar el puerto, y a que VLAN debe ir el tráfico.

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

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), 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.

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.

Si el usuario está verificado apropiadamente contra el proceso final de autenticación de origen (home authentication backend), por ejemplo LDAP, el usuario será autenticado y el home RADIUS server pasará un acuse de recibo al dispositivo de control de acceso.

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.

Escalabilidad [5]: 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 gran escala, se deberá agregar un proxy RADIUS sobre un nivel internacional.

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.

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.

2 Despliegue del Servicio eduroam en el Campus Universitario

Mayormente el acceso a una red inalámbrica implica un trámite engorroso, además de reconfigurar la computadora portátil. Con la implementación del Servicio de Movilidad *eduroam* en la UNMSM el acceso a Internet por redes inalámbricas se hace sencillo y seguro, solo comprobando el usuario y contraseña de la organización de origen, el investigador, docente o estudiante tendrá autorización para usar el acceso inalámbrico en cualquier institución que también tenga desplegado el servicio *eduroam*.

También permitirá a las organizaciones (universidades o institutos de investigación) gestionar de una manera óptima los accesos a recursos informáticos basados en el perfil y privilegios de usuario otorgados por las instituciones de origen.

El servicio *eduroam* facilitará el acceso a la información de manera sencilla y segura a investigadores, docentes y estudiantes en la UNMSM.

El despliegue del servicio *eduroam* en la UNMSM, contempló las siguientes etapas:

2.1 Recopilación de la información

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

2.2 Instalación y configuración del Servidor RADIUS

Con la disponibilidad de una computadora ubicada físicamente en la Red Telemática de la UNMSM, se realizaron las siguientes tareas:

- Instalación del 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 208: 172.16.208.0/21 designada para redes Wi-Fi.
- Asignación de una dirección IP: 172.16.208.5; para la interface de red de la estación de trabajo; y configuración del nat estático de esta dirección privada 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.
- Edición del archivo */etc/apt/sources.list* donde se enlistan las fuentes o repositorios de Debian que deben tener como mínimo lo siguiente:

```
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
```

- 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
```

- Comprobación de la versión actual del paquete *openssl*:
```
root@radius:~# openssl version
OpenSSL 0.9.8o 01 Jun 2010
```

- 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 Sep 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.
You may redistribute copies of FreeRADIUS under the terms of
the
GNU General Public License.
For more information about these matters, see the file named
COPYRIGHT.
```

- 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
```

- Configuración de los certificados digitales y archivos necesarios dentro del directorio */etc/eduroam*.

- Modificación del archivo */etc/ssl/openssl.cnf*. Las líneas resaltadas muestran 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/

certificate       = $dir/ca.crt   # The CA certificate
#certificate      = $dir/cacert.pem
serial            = $dir/serial
crlnumber         = $dir/crlnumber

crl               = $dir/crl.pem
private_key       = $dir/private/ca.key # The private key
```

```
#private_key     = $dir/private/cakey.pem
RANDFILE          = $dir/private/.rand     # private random
number file
```

- Instalación de 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
```

- Generación de las claves GPG 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.

```
root@radius:~# gpg --list-keys
/root/.gnupg/pubring.gpg
------------------------
pub   2048R/4EB4A594 2012-09-22
uid                  Rossina Gonzales Calienes (Clave GPG de
Rossina Gonzales) <rgonzalesc1@unmsm.edu.pe>
sub   2048R/A2BBD0F9 2012-09-22
```

- 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.

- Configuración un cliente LDAP en el servidor RADIUS en el archivo */etc/freeradius/modules/ldap* ; para que este pueda conectarse al servidor LDAP y así poder "logearse" con los usuarios creados del mismo:

```
ldap {
        server = ldap.unmsm.edu.pe
        port = 389
        identity =
"uid=eduroam,ou=aplicaciones,dc=unmsm,dc=edu,dc=pe"
        password = eduROAM,,unmsm-+
        basedn = "dc=unmsm,dc=edu,dc=pe"
        filter = "(uid=%{%{Stripped-User-Name}:-%{User-
Name}})"
        base_filter = "(objectclass=radiusprofile)"
}
```

- Configuración de un Cliente RADIUS (access point o wireless controller), se aprecia dicha configuración al editar el archivo */etc/freeradius/clients.conf*. A continuación se aprecia la configuración del registro de un access point con IP 172.16.208.6 y del wireless controller con IP 172.16.208.10:

```
client Test-AP-UNMSM {
ipaddr = 172.16.208.6
netmask = 32
secret = 123456
require_message_authenticator = no
shortname = ap-UNMSM
nastype = dlink
}

client Controlador-Cisco2 {
ipaddr = 172.16.208.10
netmask = 32
secret = rt1911
require_message_authenticator = no
nastype = cisco-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. 3 se aprecia el sitio web, donde se descarga el software suplicante para usuarios de San Marcos.

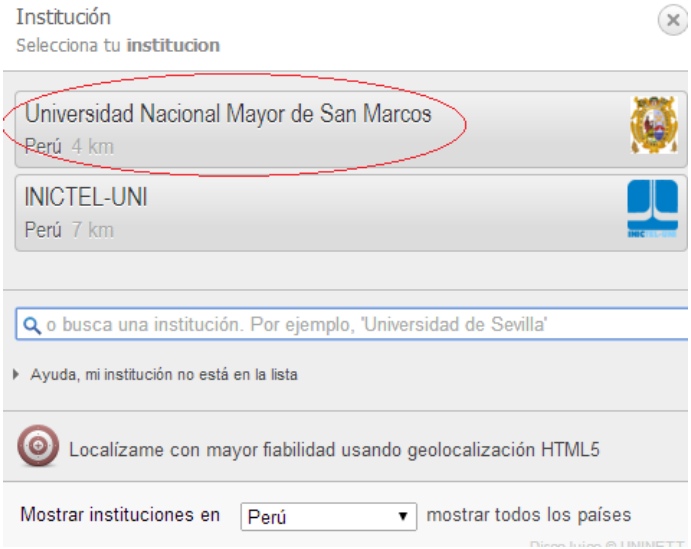

Fig. 3: URL donde se descarga el software suplicante para usuarios de la UNMSM

2.3 Publicación del servicio eduroam en la página web de la Red Telemática

En la Fig. 4. se muestra la página web de la Red Telemática, donde se ofrece el servicio *eduroam*, para la comunidad Sanmarquina.

Fig. 4: Servicio de Movilidad *eduroam***,** publicada en la Pagina Web de la Red Telemática de la UNMSM

2.4 Implementación de la Solución Wireless para el Campus Universitario

En marco a la **Licitación Pública Nº 13-2014-UNMSM "Adquisición de Wireless para el Campus de la UNMSM"** la Universidad adquirió equipamiento de acceso inalámbrico, equipos de comunicación y cableado estructurado; con los que se implementó la plataforma de comunicaciones Wi-Fi de Campus, basado en un controlador inalámbrico que permita gestionar de manera centralizada y segura el acceso a internet inalámbrico en el campus.

El alcance del proyecto consistió en la implementación de una solución wireless cuya finalidad será permitir el acceso a los usuarios docentes, administrativos y alumnos a los servicios de red por el medio inalámbrico. El equipamiento consta de un (01) Wireless LAN Controller Cisco modelo 5508 y cien (100) access points Cisco de las series 1700 y 3700. En la Fig. 5 se muestra topología de red de la Solución Wireless para la UNMSM.

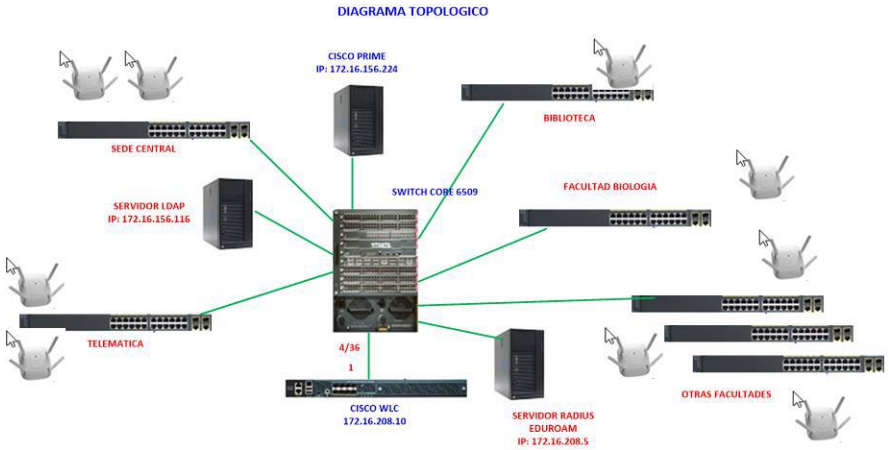

Fig. 5: Topología de red la Solución Wireless para la UNMSM

La Solución de Wireless tiene la finalidad de cubrir una cobertura inalámbrica de acceso a Internet principalmente en auditorios, salas de lectura y oficinas.

El equipo Wireless LAN Controller monitorea y controla los access points (LWAPP), a través de único control sobre todo el parque de access points instalados.

Los 08 access point de Tipo1 - AIR-CAP3702E-A-K9, de mayor potencia de transmisión serán instalados en los auditorios.

Los 92 access point de Tipo 2- AIR-CAP1702I-A-K9 serán designados a las bibliotecas, salas de lectura, pasadizos y oficinas de las Facultades y Dependencias de la Universidad.

La distribución de los equipos access point se aprecia en la Tabla 1.

Tabla 1: Distribución de los Access Point por Facultad y Dependencia

Dependencias y Facultades	Access Point
Sede Central	39
Biblioteca Central	23
Red Telemática	6
Facultad de Ingeniería de Sistemas	6
Facultad de Ciencias Administrativas	3
Facultad de Ciencias Biológicas	2
Facultad de Ciencias Contables	2
Facultad de Derecho	3
Facultad de Ciencias Matemáticas	2
Facultad de Farmacia y Bioquímica	3
Facultad de Química e Ing. Química	2
Centro Preuniversitario	3
Oficina Central de Admisión	3
Total	97

Con el software de gestión y monitoreo Cisco Prime Infraestructure v. 2.1 también adquirido, se ha estructurado por áreas los APs instalados. Tal como se aprecia en la Fig. 6.

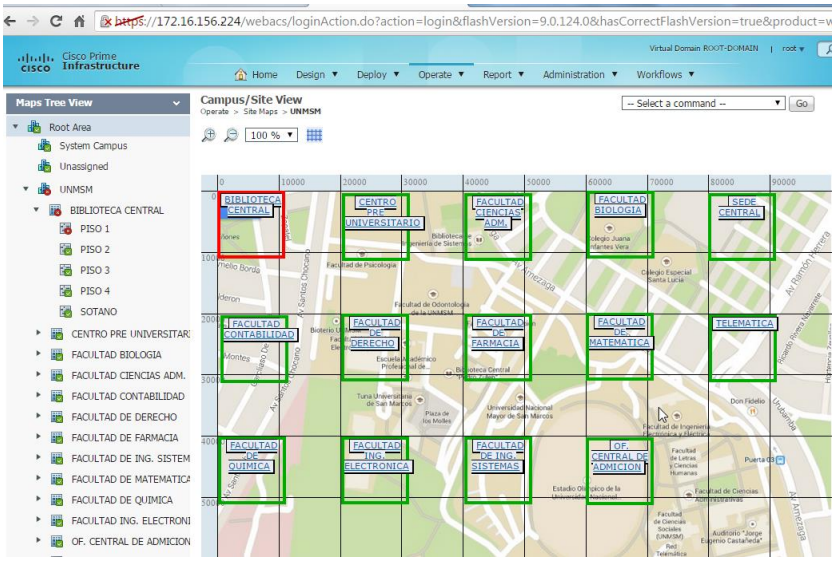

Fig.6: Asociación de los access point por Facultades y Dependencias registrados en el Software de Administración Cisco Prime

Las características técnicas de los equipos contemplados en esta Solución Wireless son las siguientes:

2.4.1 Controladora Inalámbrica - AIR-CT5508-50-K9

Escalabilidad: La controladora es un hardware de propósito específico con una capacidad de soportar hasta 500 access points sin necesidad de cambiar de equipo. Solo se deben agregar las licencias que correspondan para soportar los 500 access points. El proyecto considera contar con 100 access points activos en la Controladora con la capacidad de crecer a 500 access points en total.

Alto Rendimiento: Rendimiento sin bloqueo para redes hasta 802.11 a/b/g/n/ac.

Gestión de Radio Frecuencia de los access points o RF: Proporciona en tiempo real información histórica acerca del manejo de la Radio Frecuencia de los access points el cual es administrado de manera automática por la controladora.

Tiene la capacidad de manejar SSID por túneles separados para permitir tanto el acceso a Internet para los alumnos y al personal de la UNMSM con perfiles independientes.

Alta Disponibilidad: La controladora tiene una fuente redundante y tiene la capacidad de trabajar en activo pasivo en modo automático con una segunda controladora de las mismas capacidades.

Hardware

- El equipo permite una integración con hardware tipo IPS, Firewall, VPN Server, Integridad de clientes con conexión a Active Directory, LDAP, Access Points remotos e interface para servicios externos de seguridad.
- Es capaz de controlar simultáneamente hasta 500 puntos de acceso inalámbricos.
- Soporta como mínimo 7000 usuarios/dispositivos concurrentes conectados.
- Soporta como mínimo 512 VLANs.
- Permite la creación de un máximo de 1024 BSSID y la administración por grupos o por APs de la irradiación de las mismas.

Red

- Controlador de conmutación WLAN de capas L2 y L3
- Capacidad de configuración de VLANS.
- Manejo de Políticas, que permitan el tráfico por SSID o VLAN asociada de la red cableada.
- Roaming entre Puntos de Acceso, VLANS y switches.
- El tiempo de conmutación del "Roaming" en el orden de milisegundos para no afectar las aplicaciones sensibles al tiempo.
- Los estándares soportados: RFC 1519 CIDR, RFC 768 UDP, RFC 791 IP, RFC 792 ICMP, RFC 793 TCP,RFC 826 ARP
- Cumple con los estándares de conectividad: IEEE 802.1x, IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-T, IEEE 802.1Q, IEEE 802.11a/b/g/n/ac,IEEE 802.11i

Seguridad

- La solución cuenta con funcionalidades de Autenticación segura, cifrado y control de acceso usando 802.1x con WPA-Enterprise y WPA2-Enterprise.

- Cuenta con un portal integrado o página web con soporte SSL para hacer la autenticación de usuarios con su contraseña.
- Soporta los siguientes tipos de autenticación estándar: IEEE 802.1X (EAP-TLS), RFC 2548 Microsoft Vendor-Specific RADIUS Attributes, RFC 2716 PPP EAP-TLS, RFC 2865 RADIUS Authentication, RFC 3576 Dynamic Authorization Extensions to RADIUS, RFC 3579 RADIUS Support for EAP, RFC 3580 IEEE 802.1X RADIUS Guidelines, RFC 3748 Extensible Authentication Protocol.
- Soporta los siguientes servidores de autenticación: Base de datos interna, LDAP ó SSL Secure LDAP, RADIUS, TACACS.
- La solución soporta los siguientes tipos de cifrado: WPA-TKIP, WPA-AES, WPA2/802.11i: WPA2-AES, WPA2-TKIP, Secure Sockets Layer (SSL) y TLS: RC4 128-bit y RSA 1024- y 2048-bit.

Administración y Gestión:

- Activación de una cuenta de usuario dedicado únicamente a generar cuentas para los visitantes, de tal forma que no tenga acceso al equipo controlador ni a ninguna funcionalidad del mismo para solamente generar usuarios y contraseñas.
- Administración basada en Web (GUI), línea de comandos (CLI), syslogs, SNMP v.1, v.2 y v.3, MIB II
- Soporte de dispositivos para su visualización y localización de forma simultánea usando el protocolo 802.11.
- El controlador tiene las siguientes Certificaciones: 802.11a/b/g/n/ac, WPA-Enterprise, WPA2-Enterprise.

2.4.2 Dispositivos Access Point: AIR-CAP3702E-A-K9, AIR-CAP1702I-A-K9

Todos los Access Point son de la misma marca del fabricante de la Controladora para garantizar la compatibilidad y funciones de seguridad. Los access point tienen las siguientes características técnicas:

- Permiten la operación en modo gestionado por controlador WLAN para configurar los parámetros inalámbricos, gestión de políticas de seguridad, QoS y monitoreo de RF.
- Permite usuarios en los estándares IEEE 802.11 a/b/g/n/ac.
- Permite las siguientes tasas de transmisión con fallback automático:
    - IEEE 802.11 a / g: 54, 48, 36, 24, 18, 12, 9 y 6 Mbps.
    - IEEE 802.11 b: 11, 9, 6, 5.5,2 ,1 Mbps
    - IEEE 802.11n: (2.4 GHz and 5 GHz)
    - IEEE 802.11ac: (5 GHz)
- Capacidad de seleccionar automáticamente el canal de transmisión.
- Ajuste dinámico del nivel de potencia y el canal de radio con el fin de optimizar el tamaño de la celda de RF.
- Activación y desactivación de divulgación de SSIDs.
- Antenas Integradas: de 2,4 GHz, ganancia de al menos 4 dBi y de 5 GHz, ganancia de al menos 4 dBi.
- Permite al menos 15 SSID
- Soporta al menos 100 dispositivos simultáneos

- Poseer potencia de transmisión no menor de 22 dBm (Tipo 1) y 21 dBm. (Tipo 2) para IEEE 802.11a/b/g/n/ac.
- Implementación de cliente DHCP para la configuración automática en la red.
- Permite alimentación eléctrica a través de PoE y/o PoE+.
- Exploración en bandas de RF 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac.
- Implementa IEEE 802.1x, como mínimo con los siguientes métodos: EAP: EAP-FAST, EAP-TLS, PEAP-MSCHAPv2, EAP- GTC.
- Implementa autenticación WPA-Enterprise y WPA2-Enterprise.
- Realizar análisis de espectro en las frecuencias de 2,4 y 5 GHz, identificación de fuentes de interferencia.

2.4.3 Configuración del Wireless LAN Controller

En las Fig. 7 se observa la dirección IP 172.16.208.10 asignada al equipo Wireless LAN Controller. Y en las Fig. 8 y 9 se aprecian los parámetros de configuración de autenticación para los servidores RADIUS y LDAP respectivamente

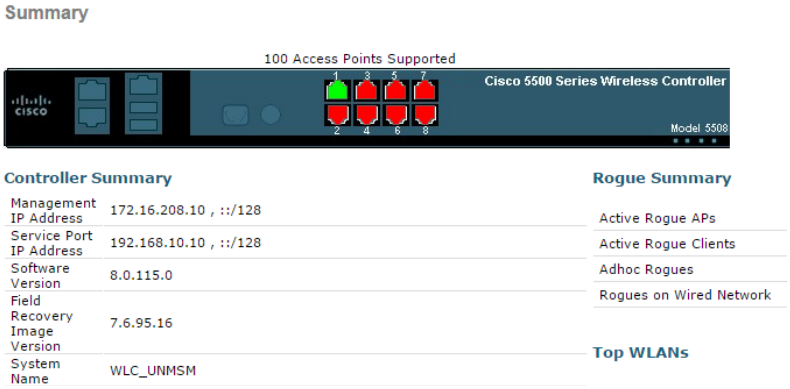

Fig 7: Direccionamiento IP y versión del software

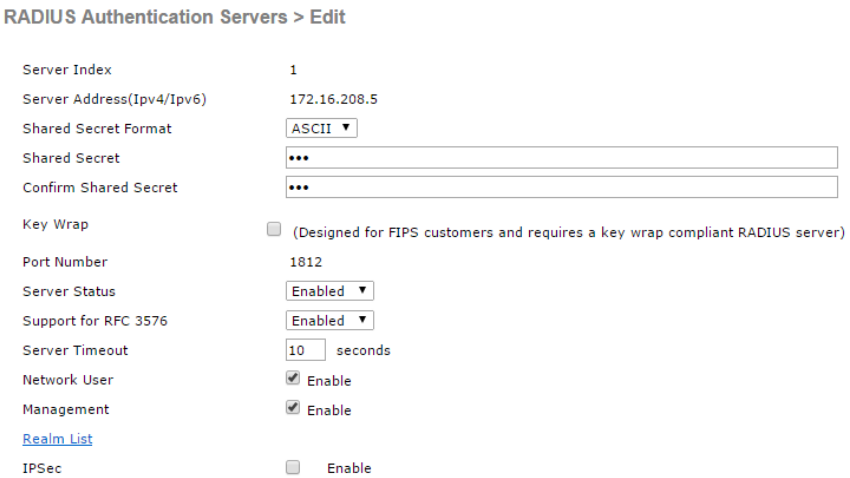

Fig 8. Autenticación con Servidor RADIUS

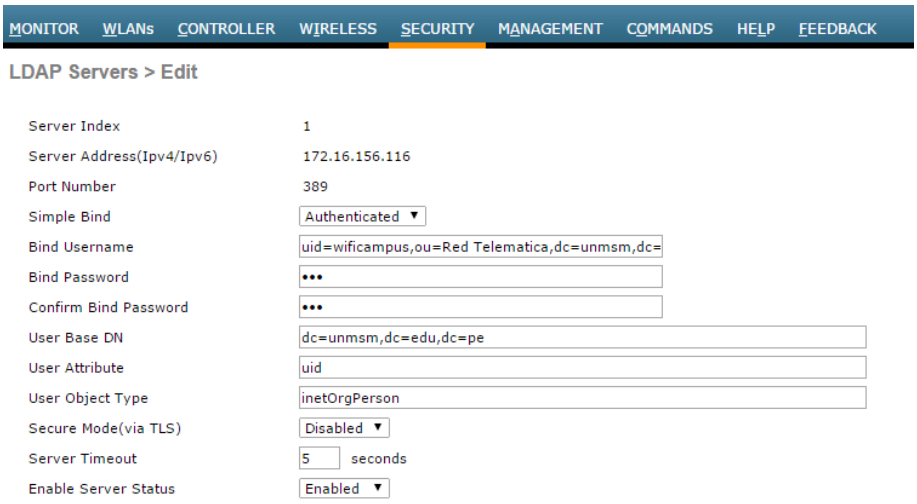

Fig 9. Autenticación con Servidor LDAP

2.5 Pruebas de conectividad

El servicio de *eduroam* en la UNMSM utiliza el sistema WPA2-Enterprise (Wi-Fi Protected Access). La autenticación de los usuarios está basada en el estándar IEEE 802.1x y para transporte en modo seguro de las credenciales de usuario se usa el protocolo EAP-TTLS+PAP.

Es necesario tener instalado en el dispositivo portátil el estándar 802.1x, comúnmente denominado suplicante. Dependiendo el sistema operativo del dispositivo portátil puede ser o no que tenga compatibilidad con el protocolo EAP-TTLS+PAP, en este caso es necesario la instalación del software para disponer del servicio *eduroam* en la UNMSM.

En general el servicio *eduroam* es compatible con diversos sistemas operativos. Se dispone del suplicante para:Windows 8, 7, Vista, XP SP3, Apple MAC OS X Mountain Lion, Apple MAC OS X Lion, Apple iOS mobile devices y Linux.

2.5.1 Configuración para clientes eduroam

Desde una Laptop

- Acceder al sitio oficial de CAT *eduroam* https://cat.eduroam.org/, seleccionar la Institución a la cual pertenece, en este caso la Universidad Nacional Mayor de San Marcos.
- En la Fig. 10 se selecciona y descarga el instalador según el sistema operativo de su portátil. Por ejemplo si seleccionó MS Windows 7 descargará eduroam-W7-UNMdSM.exe.

Fig 10. Descarga el suplicante que corresponde al sistema operativo del computador.

- En la Fig.11 se observa el procedimiento final de la instalación, en la pestaña Cuenta de usuario debe mostrar sus credenciales de usuario ingresadas al momento de instalar el software.

Fig 11. Configuración del software suplicante SecureW2.

- Concluido estos pasos, se comprobará el acceso a Internet, como usuario del servicio de movilidad mundial *eduroam.*

Desde un Smartphone

En la Fig.12 se realiza la configuración con los siguientes parámetros:

- Elegir el SSID UNMSM_eduroam
- Método EAP: TTLS
- Autenticación de fase 2 con PAP
- Colocar en identidad y contraseña las credenciales de usuario del correo institucional de la Universidad Nacional Mayor de San Marcos.

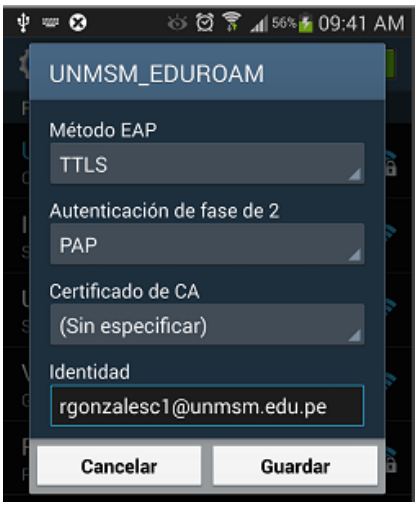

Fig 12. Parámetros de configuración en un Smartphone.

3 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.

4 Recomendaciones

1. Se recomienda registrar los dispositivos access point restantes, ubicados en las Facultades y Dependencias ubicados en el Campus Universitario (que soporten el protocolo de autenticación IEEE 802.1x) al servidor RADIUS.
2. Replicar el servicio en las Sedes Externas de la UNMSM (Facultades, Sedes Hospitalarias, Sedes de provincia).
3. Anunciar el SSID eduroam en la Wi-Fi y publicarla como la Wi-Fi oficial de la UNMSM.
4. Señalizar zonas Wi-Fi eduroam a través de la página web de la Universidad.

Agradecimientos

La autora del presente trabajo desea expresar su agradecimiento al Ing. Nilo Carrasco Oré docente de la UNMSM, por ejecutar la implementación del Proyecto Wireless para el Campus Universitario, durante su gestión como Jefe de la Red Telemática; al Ing. José Luis Quiroz Arroyo y al Ing. Javier Quinto Ancieta del INICTEL-UNI, por su asesoría técnica en la instalación y configuración del Servidor RADIUS en San Marcos.

Referencias

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

[2] M. Milinović, J. Rauschenbach, S. Winter, L. Florio, D. Simonsen, J. Howlett (2008, Enero 07) Deliverable DS5.1.1: eduroam Service Definition and Implementation Plan [Online] Disponible: http://www.niif.hu/files/GN2-07-327v2-DS5_1_1-_eduroam_Service_Definition.pdf

[3] K. Wierenga, S. Winter, R. Arends, R. Castro, P. Dekkers, H. Eertink, L. Guido, J. Leira, M. Linden, M. Milinovic, R. Papez, A. Peddemors, R. Poortinga, J. Rauschenbach, D. Simonsen, M. Sova, M. Stanica (2006, Setiembre 08) Deliverable DJ5.1.4: Inter-NREN Roaming Architecture: Descriptions and Development Items [Online] Disponible: https://www.eduroam.org/downloads/docs/GN2-06-137v5-Deliverable_DJ5-1-4_Inter-NREN_Roaming_Technical_Specification_20060908164149.pdf

[4] 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 (2008, Octubre 29) Deliverable DJ5.1.5, 3: Inter-NREN Roaming Infraestructure and Service Support Cookbook - Third Edition (3rd ed.) [Online] Disponible: http://www.eduroam.org/downloads/docs/GN2-08-230-DJ5.1.5.3-eduroamCookbook.pdf .

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

[6] J. Quiroz, J. Quinto, "Guía de la Segunda Capacitación Específca de eduroam": INICTEL-UNI, 2015.