Implementación del servicio federado EDUROAM en los campus de la Universidad Técnica del Norte

Carlos Alberto Vásquez Ayala, Cristian Paúl Espinel Ramos.

Facultad de Ingeniería en Ciencias Aplicadas, Universidad Técnica del Norte

cavasquez@utn.edu.ec

cpespinelr@utn.edu.ec

Abstract - ***Conectividad y movilidad, es el objetivo principal de EDUROAM, logrando un espacio único para cada usuario que con tan solo sus credenciales (ID y password) se le permitirá el acceso a cualquier dependencia dentro de una institución e incluso a una institución externa perteneciente a la misma federación.***

EDUROAM es, por lo tanto, una infraestructura basada en Free RADIUS que utiliza como tecnología de seguridad 802.1X para permitir la movilidad entre las distintas instituciones que la forman.

Dicho lo anterior, se pretende brindar un servicio de conexión móvil y seguro para los estudiantes, docentes e investigadores de la Universidad Técnica del Norte lo que evitará la constante configuración de los equipos cada vez que se conecten a una distinta red inalámbrica y agilitará el proceso educativo e investigativo de los usuarios.

Índice de Términos – EDUROAM, CEDIA, Federación

I. INTRODUCCIÓN

EDUROAM (education roaming) es el servicio mundial de acceso seguro desarrollado para la comunidad internacional de investigación y educación.

Iniciado en Europa, EDUROAM ha ganado impulso en toda la comunidad de investigación y educación y ahora está disponible en 72 territorios.

Permite a los estudiantes, investigadores y personal de las instituciones participantes obtener conectividad a Internet a través del campus y al visitar otras instituciones participantes simplemente abriendo su computadora portátil.

Cualquier usuario de una institución participante de la federación pueden obtener acceso a la red. Dependiendo de las políticas locales en las instituciones visitadas, los participantes también pueden tener recursos adicionales a su disposición.

Las credenciales de usuario se mantienen seguras porque EDUROAM no las comparte con el sitio que está visitando. En su lugar, se envían a la institución de origen del usuario, donde pueden ser verificados y validados.

El sistema utiliza una red de servidores administrados por las instituciones y las Redes Nacionales de Investigación y Educación (NREN, por sus siglas en inglés) para enviar estas solicitudes de manera segura a su instituto de origen. Todo esto sucede sin problemas y prácticamente al instante - Todo gracias a eduroam. [1]

II. FUNDAMENTOS TEÓRICOS DE EDUROAM

A. Características.

EDUROAM ofrece un servicio multiplataforma, lo que quiere decir que funciona sobre diferentes sistemas operativos tales como:

- Windows.
- Linux.
- iOS.
- Android.

Para poder acceder a este servicio el usuario inalámbrico debe contar con un dispositivo capaz de soportar estándares IEEE 802.11a, b, g ó n, además de soportar autenticación WPA.

B. Redes Inalámbricas.

Una red inalámbrica es una red de datos en la que dos o más terminales se pueden comunicar sin la necesidad de conexión por cables. Estas redes permiten a los usuarios movilizarse por una específica área geográfica mientras permanecen conectados.

Para lograr esta movilidad la red inalámbrica se basa en equipos de borde llamados Access Point, a través de ellos el usuario se autentica para acceder a la red local [2]

Wireless Local Area Network (WLAN)

Una Red Wireless de Área Local (WLAN por sus siglas en ingles), es un sistema de comunicación de datos inalámbrico flexible utilizado como extensión de una LAN cableada o bien como una alternativa a ésta.

Utiliza tecnología de radiofrecuencia lo que permite la movilidad del usuario, está delimitada por la distancia de propagación, 100m en interiores y varios kilómetros en exteriores.

WLAN utiliza tecnologías como IEEE802.11a, 802.11b, 802.15, etc. Para conectividad a través del espectro disperso (2,4; 5 GHz) [3]

C. Gestión de Usuarios

Para realizar la gestión de usuarios se toma en cuenta el concepto de niveles de acceso, otorgando privilegios para cada uno de ellos tomando en consideración que se pueden crear diferentes cuentas.

La gestión de usuarios dentro de EDUROAM se basa en sus condiciones de uso que deberán ser afines a las políticas de seguridad de red de la institución, asignando a cada usuario una credencial única que le permitirá conectarse a la red cuando se encuentre en otra institución afiliada o en su propia institución.

D. Access Point (AP)

Es un dispositivo utilizado mayormente en WLAN, cumple la función de proveer los recursos de la red local hacia los diferentes dispositivos inalámbricos que lo soliciten y es capaz de controlar y regular el acceso por medio del estándar IEEE802.11. También puede ser utilizado como repetidor para servir a estaciones que se encuentren a mayores distancias [4].

E. FreeRadius

FreeRadius es un protocolo que brinda mecanismos de autenticación, autorización y auditoria, para aplicaciones de acceso a redes. Utiliza un daemon que deriva del protocolo RADIUS, aunque éste, como su nombre lo indica, es libre. [5]

Una de las principales características del protocolo es su capacidad de monitorear sesiones, proveyendo notificaciones tanto de inicio de sesión como de su finalización. Utiliza los puertos UDP 1812 y 1813 para enviar estos mensajes, el puerto 1812 se utiliza para los mensajes de autenticación y el puerto 1813 para los mensajes de administración de cuentas.

En EDUROAM FreeRadius cumplirá el rol de receptar las credenciales de usuario donde, de manera local, serán verificadas en la base de datos y validadas para permitir la autenticación y el acceso al servicio. En caso de ser un usuario externo a la institución, FreeRadius se enlazará con el servidor Nacional y este se encargará de conectarse con el servidor de la institución correspondiente.

F. Protocolo 802.1X

"IEEE802.1X permite a los administradores autenticar usuarios en lugar de máquinas y se puede utilizar para que los usuarios se conecten a redes legítimas y autorizadas en lugar de redes impostoras que intentan robar credenciales" [6] Cuando un usuario se conecta a un AP que soporta IEEE802.1X comienza el intercambio de mensajes de autenticación EAP para llevar a cabo la autenticación de usuario con el servidor.

Para cumplir el proceso de conexión el protocolo IEEE 802.1X cuenta con tres participantes que conforman su arquitectura, la función de cada uno de ellos se indica a continuación además la Figura 1 muestra la arquitectura del protocolo.

- Suplicante.

Generalmente se trata del dispositivo solicitante de acceso a la red inalámbrica, generalmente el usuario.

- Autenticador.

Se trata del equipo intermediario que recibe la solicitud del suplicante, un Access Point, por ejemplo, éste actúa como un intermediario en el intercambio de tráfico de autenticación hacia el servidor.

- Servidor de Autenticación.

Se encarga de comprobar las credenciales del usuario suplicante, asigna las prioridades y privilegios establecidos y autoriza el acceso.

La Figura 1 muestra la arquitectura del protocolo en un esquema de conexión entre los tres participantes.

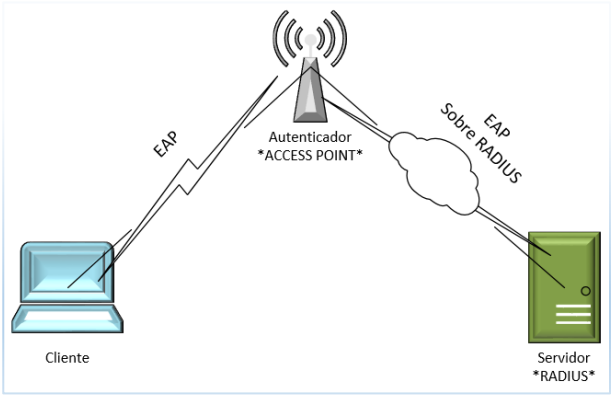

Figura 1. Arquitectura Protocolo IEEE802.1x

La autenticación se basa en el protocolo EAP, el cual utiliza varios mecanismos de autenticación como son MD5, Kerberos, Contraseñas de un solo uso, entre otros. Consiste en un encapsulado que debe ser transportado entre el Suplicante y el Servidor, la Figura 2 muestra la arquitectura 802.1X por capas.

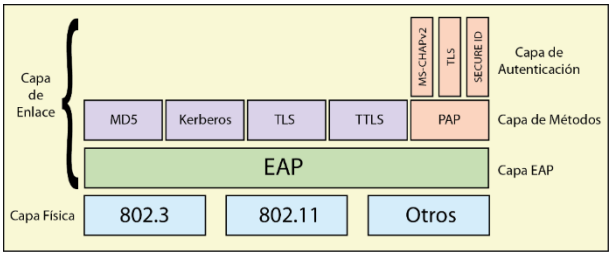

Figura 2.- Arquitectura 802.1x por capas.

EAP es un protocolo de autenticación que lleva a cabo las tareas de AAA y al ser compatible con IEEE 802.1x puede utilizar métodos de autenticación como certificados digitales o identificadores de usuario y contraseña.

Los principales mecanismos de autenticación de EAP se enlistan a continuación:

- PEAP, Protected EAP consiste en un mecanismo de validación basado en usuario y contraseña.
- EAP-TLS, basado en certificados digitales tanto en el cliente como en el servidor.
- EAP-TTLS, se basa en una autenticación de usuario y contraseña los cuales son transmitidos por un túnel creado mediante TLS, a diferencia de EAP-TLS el servidor es el único que requiere certificado. [7]

Al utilizar EAP-TTLS los Access Point no demandarán implantar un método concreto para identificar a los usuarios, simplemente entrarán en acción como pasarela entre el dispositivo móvil y el servidor, en este caso FreeRadius como muestra la Figura 3.

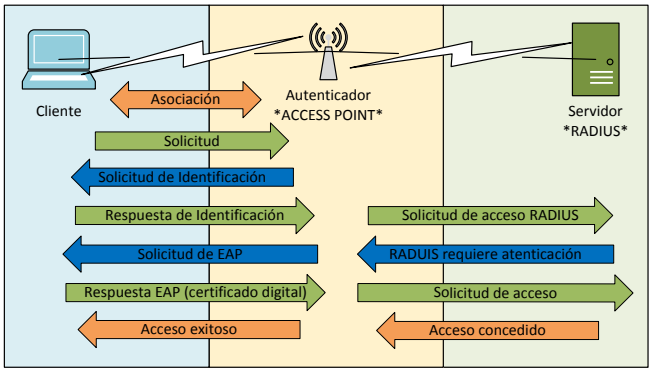

Figura 3. Solicitud de conexión.

G. Base de Datos LDAP.

Lightweight Directory Access Protocol (LDAP) está basado en un conjunto de protocolos abiertos y en el estándar X.500 de compartición de directorios por lo que es capaz de propagar su consulta a otras bases de datos LDAP en todo el mundo, lo que proporciona un "directorio global". Es también un sistema cliente/servidor encargado de organizar la información de forma jerárquica a modo de directorio con el fin de poder acceder a dicha información mediante una consulta,

Entre las ventajas encontramos que una de sus aplicaciones es la autenticación de usuarios basado en Radius controlando el acceso a una red, garantiza además una lectura rápida de los registros asegurando que cada uno de ellos sea único, permite crear múltiples directorios independientes y de forma jerárquica para asignación de privilegios, sencillo de instalar y mantener.

Tomando en cuenta todas las ventajas mostradas, en EDUROAM la base de datos LDAP conformará el directorio de los estudiantes, docentes e investigadores ya que al ser flexible permite desplegar la información que el servidor requiera comprobar. [8]

La estructura de la base de datos que se implementará en la institución y albergará a los usuarios de EDUROAM se encuentra en un orden jerárquico como se muestra en la Figura 4.

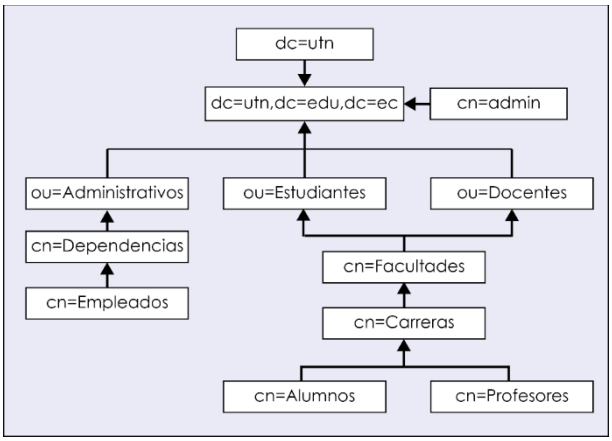

Figura 4.- Estructura jerárquica de la Base de Datos LDAP UTN

H. Certificado Digital.

El certificado digital es un documento digital que contiene una clave pública junto con los datos del usuario, todo esto avalado por una Autoridad de Certificación, este documento tiene la característica de proteger los datos que el usuario facilita, por tal motivo brinda una seguridad adicional dentro de las comunicaciones.

EDUROAM utilizará el certificado digital para acreditar a cada usuario de la institución y a todos aquellos de instituciones pertenecientes al convenio, además garantizará la seguridad durante la conexión a la red federada. [9]

I. Estandar ISO/IECE/IEEE 29148.

El estándar ISO/IEC/IEEE 29148 para el análisis de requerimientos para desarrollo de software, permite la elección adecuada de un Sistema Operativo para la implementación de un servicio mediante la evaluación y consideración de parámetros y requisitos específicos tales como:

- Interfaces de Usuario.
- Interfaces de Software.
- Interfaces de Comunicación.
- Tipos de Información.
- Frecuencia de Uso y Acceso.
- Las Entidades de Datos y sus Relaciones.
- Restricciones de Integridad.
- Restricción de Datos.
- Versión.
- Licencia.
- Rendimiento.
- Interoperabilidad.
- Escalabilidad.
- Seguridad y Fiabilidad.

III. SITUACIÓN ACTUAL DE LA RED DE LA UNIVERSIDAD TÉCNICA DEL NORTE

A. *Infraestructura Actual.*

El campus de la Universidad Técnica del Norte está conformado por los siguientes edificios:

- Planta Central.
- Bienestar Universitario.
- Facultad de Ingeniería en Ciencias Aplicadas.
- Facultad de Ingeniería en Ciencias Agropecuarias y Ambientales.
- Facultad de Ciencias Administrativas y Económicas.
- Facultad de Educación Ciencia y Tecnología.
- Facultad de Ciencias de la Salud.
- Centro Académico de Idiomas.
- Instituto de Postgrado.
- Mecánica y Electricidad.
- Biblioteca.
- Polideportivo.
- Complejo Acuático.
- Gimnasio.
- Auditorio Agustín Cueva.

Actualmente la red inalámbrica de la Universidad Técnica del Norte cuenta con 84 Access Point interiores y con 16 Access Point exteriores, ubicados estratégicamente en cada edificio del campus para lograr la máxima cobertura.

B. *Topología Física de la red de la Universidad Técnica del Norte*

La Figura 5 muestra la conexión de los equipos de core y administración ubicados en el Data Center del DDTI y los equipos de distribución ubicados en cada facultad y dependencia dentro y fuera del campus.

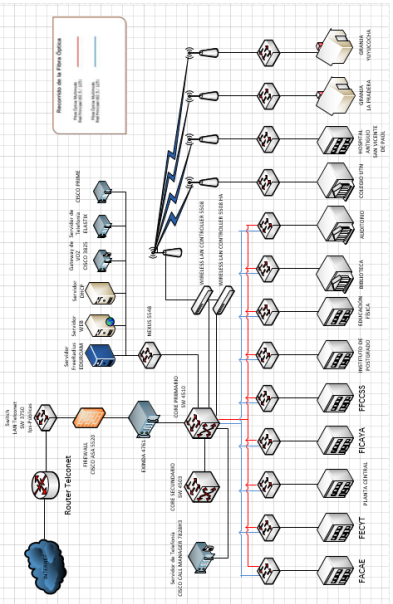

Figura 5.- Topología Física de la Universidad Técnica del Norte.

El mecanismo de Acceso para las diferentes redes Wireless de la institución es el siguiente:

- Wireless Administrativos

El SSID propagado en el campus es "WUTN.Admin", el acceso se realiza mediante contraseña, la cual es configurada en el WLC de la Universidad Técnica del Norte.

- Wireless Docentes

El SSID propagado en el campus es "WUTN.Docentes", los docentes realizan su autenticación por medio de una contraseña y además registrando la dirección MAC de su o sus dispositivos (PC, Smartphone, Tablet), lo que permite que únicamente el dispositivo registrado pueda acceder a la red.

- Wireless Estudiantes

El SSID propagado en el campus es "WUTN.Estudiates", considerando el elevado número de usuarios y la disponibilidad de conexión que se requiere por los mismos, la red de estudiantes es de acceso libre.

- Wireless Eventos

El SSID propagado principalmente es los Auditorios de la Institución es "WUTN.Eventos", el acceso se realiza mediante contraseña, la cual es configurada en el WLC de la Universidad Técnica del Norte.

C. *Ancho de Banda*

La Universidad Técnica del Norte cuenta con un Ancho de banda de 600 Mbps, los cuales son distribuidos prioritariamente entre las actuales dependencias de acuerdo a la necesidad de cada una de ellas, además de garantizar un 55% de ancho de banda a cada estudiante que se conecte a la red WUTN.Estudiantes, esto de acuerdo a las políticas de administración de Ancho de Banda establecidas en el DDTI por el administrador de Redes.

D. *Equipos*

Se instalaron 49 equipos marca CISCO modelo AIR-CAP3702I-A-K9 exclusivos para interiores, 16 equipos marca CISCO modelo AIR-CAP1532E-A-K9 exclusivos para exteriores, además se reubico 32 equipos marca CISCO modelo AIR-LAP1262N-A-K9 y 5 marca CISCO modelo AIR-CAP1602E-A-K9 exclusivos para interiores, para un total de 84 equipos como se indica en la sección III. A.

De acuerdo con el fabricante de los respectivos equipos instalados actualmente en el campus de la Institución, se determina que:

- Equipo AIR CAP3702I-A-K9, exclusivo para interiores, tiene la capacidad de soportar 120 usuarios conectados simultáneamente.
- Equipo AIR LAP1262N-A-K9, exclusivo para interiores, tiene la capacidad de soportar 100 usuarios conectados simultáneamente.

- Equipo AIR-CAP-1532E-A-K9, exclusivo para exteriores, tiene la capacidad de soportar más de 150 usuarios conectados simultáneamente. [10]

Para la marca de Access Point que dispone la Universidad Técnica del Norte se dispone de cuatro modos de operación, dependiendo de IOS o su configuración pueden ser:

- **Modo Local (LIGTHWEIGHT):** Un Access Point que funciona en modo local se vincula de forma automática al Wireless LAN Controller adoptando su configuración automáticamente, en este modo los AP's responden a comandos lwap, capwap.
- **Modo Autónomo:** Funcionan de forma independiente, es decir, no se vinculan al Wireless LAN Controller, por ende, dependen de las configuraciones individuales que el administrador realice.
- **Modo Mesh:** Brinda las funciones de antena para comunicarse con otro Access Point, utiliza la frecuencia de 802.11b y 802.11g, normalmente se utiliza para cubrir grandes distancias, sin embargo, se debe tomar en cuenta que el ancho de banda disminuye.
- **Modo Flex Connect:** Un Access Point en este modo guarda las configuraciones del Wireless LAN Controller, cuando la conexión con el WLC cae el AP en modo Flex Connect se convierte en un WLC secundario que utiliza los recursos locales.

EDUROAM requiere un control centralizado para administrar sus recursos, y puesto que el WLC brinda esa facilidad, todos los equipos inalámbricos que se encuentren instalados en el campus de la Universidad Técnica del Norte deben ser configurados en *Modo Local*.

E. Usuarios

La Tabla 1 muestra el promedio de usuarios conectados simultáneamente en una semana a los equipos interiores de las dependencias de la Universidad Técnica del Norte.

Tabla 1
Promedio Usuarios equipos interiores

Edificio	Promedio Semanal
FACAE	331
FECYT	239
FICAYA	168
FCCSS	216
CAI	168
POSTGRADOS	68
BIENESTAR UNIVERSITARIO	25
PLANTA CENTRAL	83
AUDITORIO	57
PISCINA	24
POLIDEPORTIVO	151
BIBLIOTECA	148
ELECTRICIDAD	40
GIMNASIO	10

La Tabla 2 muestra el promedio de usuarios conectados simultáneamente en una semana a los equipos exteriores de la Universidad Técnica del Norte.

Tabla 2
Promedio Usuarios equipos exteriores

Ubicación	Promedio Semanal
FACAE Exterior Bar	49
FACAE Exterior Gradas	27
FACAE Exterior Parque	22
FECYT Exterior Parque	36
Auditorio Exterior Plaza	2
Auditorio Exterior Canchas	3
Planta Central Exterior	28
Postgrado Exterior Parque	15
Postgrado Exterior Piscina	17
CAI/FICAYA Exterior	29
FICA/FICAYA Exterior	74
FICA/FCCSS Exterior	36
Piscina Exterior	6
FICA Exterior	128
Entrada Norte Canchas	33
Entrada Norte Bienestar	13

De acuerdo a los datos recopilados y en comparación con los datos que el fabricante estipula para los equipos, se concluye lo siguiente:

Los equipos Wireless, tanto interiores como exteriores, tienen la capacidad necesaria para soportar la afluencia continua y simultanea de usuarios.

F. Requerimientos de Hardware y Software

Para la instalación del servidor FreeRadius con base de datos LDAP y administración phpLDAPadmin se recomienda se considere las siguientes características tanto de software como de hardware.

Software.

- Sistema Operativo: Debian 6.0.7.
- FreeRadius.
- Base de Datos LDAP.
- phpLDAPadmin.

Hardware.

- Procesador AMD FX(tm)-8320 Eight-Core 3.50 GHz.
- Memoria RAM 4 GB.
- Disco duro de 1 TB.

Esto con el fin de soportar logs y administrar de forma adecuada y rápida el número de usuarios que será almacenado en la base de datos.

G. Selección de Software

En base al estándar ISO/IEC/IEEE 29148 que se indica en la sección II.I. se realiza la comparación entre los Softwares CentOS y Debian para seleccionar el más adecuado basados en los requerimientos ya establecidos, la Tabla 3 muestra la calificación por característica.

Las calificaciones se describen de la siguiente manera:

Para cada requerimiento se asignaron los niveles de características que se consideraron necesarios, dependiendo de

ello, se asignaron los valores: cero (0) a aquella menos apta para la implementación, uno (1) para una característica intermedia o adecuada y dos (2) a la que se consideró más adecuada para el proyecto.

Tabla 3
Calificación de parámetros para selección de software

Requerimiento	Característica	Calificación	CentOS	Debian
Interfaces de Usuario.	Entorno gráfico obligatorio	0	1	1
	Consola de comandos	1		
Interfaces de Software.	No Soporta Servidores y BDD	0	1	1
	Soporta Servidores y BDD	1		
Interfaces de Comunicación.	No Permite el protocolo EAP	0	1	1
	Permite el protocolo EAP	1		
Tipos de Información.	Tipos de información limitada	0	1	1
	Tipos de información completa	1		
Frecuencia de Uso y Acceso.	Disponibilidad baja	0	2	2
	Disponibilidad media	1		
	Disponibilidad alta	2		
Entidades de Datos y sus Relaciones.	No clasifica los usuarios	0	1	1
	Permite clasificar usuarios	1		
Restricciones de Integridad.	Administración limitada	0	1	1
	Administración completa	1		
Retención de Datos.	No es posible generar reportes	0	1	1
	Es posible generar reportes	1		
Versión.	Anterior y estable	0	2	2
	Actualizada	1		
	Actualizada y Estable	2		
Licencia.	Propietaria	0	1	1
	Libre	1		
Rendimiento.	Rendimiento bajo	0	2	2
	Rendimiento medio	1		
	Rendimiento Alto	2		
Interoperabilidad.	Limitada	0	1	2
	Dos o más Plataformas	1		
	Cualquier Plataforma	2		
Escalabilidad.	No es escalable	0	1	1
	Es escalable	1		
Seguridad y Fiabilidad.	Seguridad baja	0	2	2
	Seguridad media	1		
	Seguridad alta	2		
TOTAL			**18**	**19**

Como se puede observar en la tabla anterior la diferencia entre los softwares es mínima, sin embargo, **Debian** califica principalmente por su interoperabilidad con otras plataformas, en este caso en particular se debe integrar el sistema operativo con el Wireless LAN Controller de la institución.

IV. INTEGRACIÓN E IMPLEMENTACIÓN DE EDUROAM

Una vez que se ha seleccionado el sistema operativo sobre el cual se montaran los servicios, se procede en primera instancia a realizar las configuraciones básicas para garantizar la conectividad a la red. El siguiente paso es la instalación de los servicios.

FreeRadius, quien hace las veces de servidor AAA, realizando la Autenticación, Autorización y Auditoria de EDUROAM.

LDAP, es la base de datos donde se albergarán los usuarios de la institución.

Schema, que define la organización de los usuarios, que, en este caso, será de forma jerárquica.

phpLDAPadmin, interfaz web que permite la administración y organización de los usuarios dentro de la base de datos, todo esto una vez que se ha definido la jerarquía con schema.

En la Figura 6 se observa el proceso de una petición de conexión por parte de un usuario de la Universidad Técnica del Norte dentro de su propio campus una vez que se han configurado todos los servicios y asignado las credenciales de acceso.

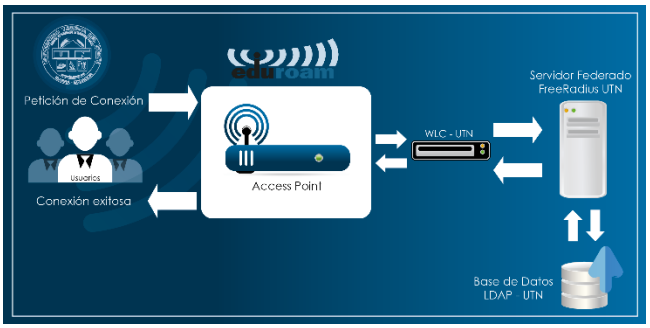

Figura 6. Diagrama de conexión local.

El proceso inicia cuando un usuario identifica el ssid "eduroam" y solicita el acceso.

El Access point (AP) entra en funcionamiento solicitando al usuario ingrese las credenciales.

Cuando el usuario ha ingresado sus credenciales el AP hace las veces de túnel, y a través del Wireless LAN Controller (WLC) se comunica con el servidor.

El servidor FreeRadius realiza el proceso de autenticación de las credenciales por medio de la base de datos LDAP realizando una comparación de datos para validar la existencia del usuario.

La base de datos responde al servidor un "Acceso aceptado" de credenciales verídicas.

El servidor asigna el certificado digital al usuario que está realizando la petición y responde nuevamente a través del WLC y del AP permitiéndole el acceso y garantizándole la conexión.

Para una conexión entre instituciones pertenecientes al convenio el proceso es similar, adicionalmente como se observa en la Figura 7, se realiza la comunicación entre los servidores de las instituciones implicadas y el servidor nacional de CEDIA, a lo que se llama federación.

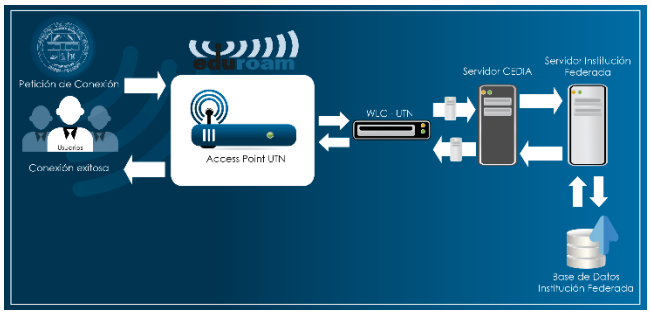

Figura 7. Diagrama de conexión Interinstitucional.

V. PRUEBAS Y RESULTADOS

A. *Prueba Local*

La prueba se realiza luego de haber configurado correctamente todo en cuanto se refiere a la conexión entre el servidor de la Universidad Técnica del Norte y CEDIA

El primer test se realiza con un usuario propio de la institución previamente registrado en la base de datos dentro del servidor y asignado las credenciales respectivas para su correcto acceso, es así que ejecutando el comando ***radtest*** junto con el usuario y credenciales ya mencionadas podemos observar en la Figura 8 la autenticación se realiza con éxito y el acceso es aceptado.

```
root@eduroam:~# radtest cpespinelr@utn.edu.ec 1003235213 127.0.0.1 1812 AdminLdap@Eduroam
Sending Access-Request of id 129 to 127.0.0.1 port 1812
        User-Name = "cpespinelr@utn.edu.ec"
        User-Password = "1003235213"
        NAS-IP-Address = 10.24.8.8
        NAS-Port = 1812
        Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=129, length=37
        Tunnel-Private-Group-Id:0 = "128"
        Tunnel-Medium-Type:0 = IEEE-802
        Tunnel-Type:0 = VLAN
```

Figura 8. Prueba Local con comando radtest.

Se concluye, de acuerdo con el resultado, que la comunicación entre el servidor y la base de datos es correcta.

B. *Prueba Interinstitucional*

La presente prueba se realiza con el fin de comprobar la correcta comunicación entre el Servidor Institucional y el Servidor de CEDIA.

Para este fin el administrador ha creado el usuario *utpl@**utn.edu.ec*** correspondiente a la Universidad Técnica del Norte y solicitando la colaboración de la Universidad Técnica Particular de Loja, perteneciente a la federación, para realizar la respectiva prueba. El colaborador realiza la conexión por medio de un dispositivo móvil con sistema operativo Android, a continuación, la Figura 9 muestra cómo se realiza la petición a través del servidor federado de CEDIA y se conecta al servidor Institucional, es así como el usuario UTN se conecta satisfactoriamente dentro del campus de la UTPL.

```
ptado :) %{User-Name} -> Usuario Aceptado :) utpl@utn.edu.ec
 (from client org-federado.cedia.org.ec port 0 via TLS tunnel) Usuario Aceptado :) utpl@utn.edu.ec
section.  Using default return values.
ith from file /etc/freeradius/sites-enabled/inner-tunnel
```

Figura 9. Prueba de conexión de un usuario UTN en una institución perteneciente a la federación.

De acuerdo a las pruebas realizadas tanto con usuarios locales como con usuarios externos a la institución se concluye que el servicio permite la conectividad en todos los campus de las instituciones que pertenezcan a la federación, de igual forma esto garantiza la correcta configuración del servidor institucional de la Universidad Técnica del Norte y la comunicación del mismo con el servidor federado de CEDIA.

VI. CONCLUSIONES

Se implementó el servicio federado EDUROAM en la Universidad Técnica del Norte que garantiza la conectividad segura de los usuarios tanto en el campus local como en los campus de instituciones pertenecientes a la federación.

La Universidad Técnica del Norte cuenta con los equipos adecuados para una administración centralizada lo que facilita la implementación del servicio federado.

Debian en su versión 6.07 es el sistema operativo adecuado para albergar los servidores necesarios, además de ser compatible con el WLC de la Institución.

La jerarquía utilizada por la base de datos LDAP en el servidor FreeRadius permite clasificar y administrar adecuadamente los usuarios de la institución.

El uso de certificados digitales proporciona a los usuarios mayor seguridad al momento de realizar su conexión con el servicio federado pues protege su navegación y mantiene a salvo sus credenciales.

Las pruebas realizadas garantizan la conexión de usuarios de la Universidad Técnica del Norte en los campus de las Instituciones pertenecientes al convenio, además demuestra la correcta federación entre servidores.

VII. RECOMENDACIONES

Previo a la implementación de un servicio inalámbrico se deben realizar un site survey en la institución para comprobar de cobertura y disponibilidad de los equipos.

En vista del inminente cambio de direccionamiento IPv4 a IPv6, se recomienda migrar el servidor para que trabaje bajo el nuevo protocolo.

Se debe realizar un análisis periódico de capacidad de usuarios de los equipos inalámbricos de la Institución, esto con el fin de dimensionar las conexiones diarias y semanales, con dichos datos se podrá solventar las peticiones de los futuros usuarios del servicio federado, además de administrar correctamente los equipos de la red inalámbrica para evitar su saturación, por lo que se recomienda crear políticas de conexión adecuadas para los usuarios.

Es recomendable reiniciar los servicios instalados durante la implementación con una frecuencia moderada, esto con el fin de garantizar el correcto funcionamiento del servidor.

Actualizar la base de datos semestralmente, esto tomando en cuenta que en cada periodo ingresan alumnos nuevos a la institución, así como algunos la abandonan.

Para brindar el servicio EDUROAM en los campus exteriores de la Universidad Técnica del Norte los equipos instalados en dichas dependencias deben cambiar su configuración de Modo Autónomo a Modo Local.

VIII. REFERENCIAS

[1] eduroam, «eduroam,» [En línea]. Available: https://www.eduroam.org. [Último acceso: 3 dic 2016].

[2] Definiciones.de, «Definiciones.de,» 2008. [En línea]. Available: http://definicion.de/red-inalambrica/.

[3] I. Bernal, «Comunicaciones Inalámbricas Generalidades de WLAN,» Quito, 2005.

[4] I. Moderna, «Informática Moderna,» 2008. [En línea]. Available: http://www.informaticamoderna.com/Acces_point.htm. [Último acceso: 19 abril 2015].

[5] GlosarioIT, «Glosario Informático,» 2003-2015. [En línea]. Available: http://www.glosarioit.com/#!FreeRadius. [Último acceso: 5 septiembre 2015].

[6] S. G. Mattew, Redes Wireless 802.11, vol. 2, Madrid: Anaya Multimedia, S.A., 2006.

[7] P. P. F. Martínez, «dns.bdst.net,» [En línea]. Available: http://www.bdat.net/seguridad_en_redes_inalambricas/x80.html. [Último acceso: 22 marzo 2016].

[8] RedHat, «Red Hat Enterprise Linux 4,» 2005. [En línea]. Available: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/index.html. [Último acceso: 21 noviembre 2015].

[9] RedIRIS, «eduroam,» 26 julio 2015. [En línea]. Available: https://www.eduroam.es/.

[10] Cisco, «Cisco,» 2016. [En línea]. Available: http://www.cisco.com/c/en/us/products/wireless/access-points/index.html. [Último acceso: 17 agosto 2016].

[11] F. Andreu, I. Pellejero y A. Lesta, Redes WLAN Fundamentos y aplicaciones de seguridad, Barcelona: Marcombo, 2006.

IX. BIOGRAFIAS

Carlos Alberto Vásquez Ayala

Nació en Quito el 19 de septiembre de 1981, ingeniero en Electrónica y Telecomunicaciones, Escuela Politécnica Nacional en 2008, actualmente docente de la Carrera de Ingeniería en Electrónica y Redes de Comunicación de la Universidad Técnica del Norte, egresado de la Maestría en Redes de Comunicación, Pontificia Universidad Católica del Ecuador.

Cristian Paúl Espinel Ramos

Nació el 6 de febrero de 1989 en la ciudad de Ibarra, culminó sus estudios secundarios en el Colegio Fisco-Misional San Francisco especialidad Físico Matemático, actualmente egresado de la carrera de Ingeniería en Electrónica y Redes de Comunicación, Presidente de la Rama Estudiantil IEEE de la Universidad Técnica del Norte periodo 2016, miembro activo de IEEE desde el 2015.