UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA DE INGENIERÍA DE SISTEMAS INFORMÁTICOS


# INTEGRACIÓN DE LA UNIVERSIDAD DE EL SALVADOR A LA RED ACADÉMICA MUNDIAL DE USUARIOS MÓVILES EDUROAM

PRESENTADO POR:

**ENZO DANILO FLORES LAGOS**

**BÁRBARA PATRICIA FUENTES SERRANO**

**ELMER OSVALDO REYES HERNÁNDEZ**

**KATYA KAROLYNA RODRÍGUEZ RIVAS**

PARA OPTAR AL TITULO DE:

## INGENIERO DE SISTEMAS INFORMÁTICOS

CIUDAD UNIVERSITARIA, AGOSTO DE 2008

**UNIVERSIDAD DE EL SALVADOR**

RECTOR :

**MSc. RUFINO ANTONIO QUEZADA SÁNCHEZ**

SECRETARIO GENERAL :

**LIC. DOUGLAS VLADIMIR ALFARO CHÁVEZ**

**FACULTAD DE INGENIERÍA Y ARQUITECTURA**

DECANO :

**ING. MARIO ROBERTO NIETO LOVO**

SECRETARIO :

**ING. OSCAR EDUARDO MARROQUÍN HERNÁNDEZ**

**ESCUELA DE INGENIERÍA DE SISTEMAS INFORMÁTICOS**

DIRECTOR :

**MSc. ING. CARLOS ERNESTO GARCÍA GARCÍA**

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA DE INGENIERÍA DE SISTEMAS INFORMÁTICOS

Trabajo de Graduación previo a la opción al Grado de:

**INGENIERO DE SISTEMAS INFORMÁTICOS**

Título :

# INTEGRACIÓN DE LA UNIVERSIDAD DE EL SALVADOR A LA RED ACADÉMICA MUNDIAL DE USUARIOS MÓVILES EDUROAM

Presentado por :

**ENZO DANILO FLORES LAGOS**
**BÁRBARA PATRICIA FUENTES SERRANO**
**ELMER OSVALDO REYES HERNÁNDEZ**
**KATYA KAROLYNA RODRÍGUEZ RIVAS**

Trabajo de Graduación Aprobado por:

Docente Director :
Lic. Guillermo Mejía Díaz

San Salvador, Agosto de 2008

Trabajo de Graduación Aprobado por:

Docente Director :

**Lic. Guillermo Mejía Díaz**

**DEDICATORIA.**

**A Dios todo poderoso**, por que a El le debo todos mis logros como estudiante y cristiano, gracias por todas las bendiciones y por que siempre me fortalecisteis cuando más lo necesité. Gracias por ayudarme a alcanzar este primer nivel en mi vida.

**A mis padres, Ricardo y Mirna,** por brindarme todo su apoyo, su amor, su paciencia, su sacrificio, su entrega; por haber creído en mí y haberme dado la oportunidad de obtener una profesión, como forma de vida.

**A mis hermanos, Ricardo e Iván** por su paciencia, compresión y su amor.

**A mi familia,** por creer en mi y por que se que comparten mi alegría en este importante paso de mi vida.

**A mis amigos, Oscar, Mario, David, Carlos, Javier, Emerson y Beatriz**; por estar conmigo en las buenas y en las malas, brindándome su apoyo y solidaridad. Por estar ahí cuando más los necesite.

**A la Universidad Nacional de El Salvador**, por ser la madre de generaciones de profesionales, cuyas raíces son la pobreza y la humildad, pero con una capacidad, una tenacidad y un estoicismo, propio de los salvadoreños y salvadoreñas.

**A mis compañeros de tesis, Katya, Bárbara y Elmer**, por su paciencia y el trabajo en equipo para desarrollar nuestro proyecto, porque con su esfuerzo cada uno hizo posible nuestro objetivo. Muchos éxitos en sus vidas personales y profesionales.

**A nuestro docente director y docente observador, Lic. Guillermo Mejia e Ingeniero Pedro Peñate**, por transmitirnos sus conocimientos, su tiempo y guiarnos a través del desarrollo del trabajo de graduación.

*Enzo Danilo Flores Lagos.*

## DEDICATORIA.

**A Dios todopoderoso**, por darme el don de la vida, por ser mi fortaleza en todo momento, por guiarme siempre en el camino, porque me ama con mis defectos, por todas las bendiciones que en cada momento recibo.

**A mi madre Milagro Serrano de Fuentes,** por su amor, su apoyo incondicional, su paciencia, sus sacrificios, sus regaños, sus enseñanzas y consejos sin los cuales no sería quien soy ahora y por brindarme la oportunidad de realizarme como profesional.

**A mi padre Oscar Ulises Fuentes,** que no alcanzó a ver los resultados pero sigue vivo en mi pensamiento; fue su estímulo para llegar al final.

**A mis hermanos, Cristian Rafael, Ligia Marcela y Gema Emperatriz,** por su amistad por su compresión, su amor y su apoyo.

**A mi novio, mi amigo, mi compañero de tesis Elmer Reyes,** por aparecer en mi vida y ayudarme a crecer como persona y como profesional.

**A mi familia,** por creer en mí y por compartir mi alegría en este importante logro de la vida, por ayudarme cuando los he necesitado y estar presente en vida.

**A mis amigas y amigos** por estar conmigo en las buenas y en las malas, brindándome su apoyo y solidaridad. Por estar ahí cuando más los necesite.

**A la Universidad de El Salvador**, por brindarme la oportunidad de ser miembro de ella y permitirme convertir en una profesional productiva para la sociedad salvadoreña.

**A mis compañeros de tesis Enzo Flores y Katya Rodríguez**, por todos los desvelos trabajar juntos en un mismo fin. Muchos éxitos en sus vidas personales y profesionales.

**A nuestro docente director y docente observador, Lic. Guillermo Mejía e Ing. Pedro Peñate,** por ser una guía durante el desarrollo del proyecto y transmitirnos su sabiduría para llevarlo a feliz término.

**A Eric López y a la Unidad de Educación a Distancia**, por confiarnos la realización del proyecto.

*Bárbara Patricia Fuentes Serrano.*

## DEDICATORIA

**A Dios** Gracias por todas las bendiciones que recibo de ti, por tu infinita misericordia y amor sin límites, por las personas que puso en mi camino. Este logro te lo debo a ti.

**A mis padres Atilio Reyes y Rosa Isabel,** gracias por su confianza y apoyo en mis años de estudio, por sus consejos y valores inculcados, por creer en mí. Sin ustedes nada de esto hubiese sido posible.

**A mis hermanos Félix, Sandra, Atilio y Jeannette**, por su comprensión, su apoyo incondicional y su voto de confianza, su cariño y especialmente por ser fuente de inspiración para mí. Los admiro mucho.

**Familia**, gracias por su apoyo y por compartir conmigo la alegría de mi primer objetivo alcanzado.

**A mis amigos,** por darme ánimo a seguir adelante, por ser tal y como son.

**A mis compañeros de tesis** por el esfuerzo, tiempo y dedicación para la realización de este proyecto. He aprendido mucho de ustedes. ¡Que Dios los bendiga!

**A mi Novia Bárbara Fuentes,** por ser la persona mas bella que he conocido en mi vida, por que con ella he aprendido mucho y he crecido profesionalmente.

**Lic. Mejía y Eric López**, gracias por creer en este proyecto, por el tiempo invertido en él y por su gran esfuerzo para llevarlo a feliz término.

*Elmer Osvaldo Reyes Hernández.*

***Agradecimientos***

Gracias **Padre Santo** por todas las bendiciones que recibo de ti, por tu infinita misericordia y amor sin límites. Este logro es obra tuya. Sin ti nada soy.

**Virgencita de Guadalupe**, me has acompañado toda mi vida. Gracias madre por tus intercesiones, tu amor incondicional y tu protección.

**A mi madre Ana Josefa,** gracias por tu confianza plena, por tus consejos, tu inagotable paciencia, por tu amor de madre, por tus oraciones, por creer en mí. Sin ti esto no hubiera sido posible. Este logro te pertenece porque más que mío es tuyo.

**A mi Padre Ernesto**, gracias por creer en mí, por sus consejos, por estar siempre pendiente de mí, por ser padre, amigo y maestro.

**A mi hermano Reynaldo**, por su comprensión, su apoyo incondicional, su cariño y especialmente por ser fuente de inspiración para mí. Te admiro mucho.

**Abuelos Elba y Frank**, que seria de mí sin sus oraciones, sin sus consejos y cariño. Gracias por su confianza en mí, porque cuando yo dudaba de alcanzar la meta, ustedes, poniendo su confianza en Dios, ya celebraban el triunfo.

**Familia**, gracias por su apoyo y por compartir conmigo la alegría de un objetivo alcanzado.

**Christian, Liche y Frankcito**, gracias por el tiempo que hemos compartido juntos, por sus risas, sus travesuras, por considerarme su amiga. Ustedes me motivan a tratar de ser mejor persona cada día.

**A mis amigos, Isa, Murillo, Nacho, Ricardo, Bea** por todo el tiempo compartido, por estar conmigo en las buenas y en las malas, por darme ánimo a seguir adelante, por ser como son.

**Portillo**, gracias por ser un amigo incondicional, estoy segura que desde el cielo estás conmigo celebrando este triunfo que comparto contigo. Te llevo en mi corazón.

**A mis hermanos de comunidad** por escucharme, por sus oraciones y apoyo.

**A mis compañeros de tesis** por el esfuerzo, tiempo y dedicación para la realización de este proyecto. He aprendido mucho de ustedes. ¡Que Dios los bendiga!

**Lic. Mejía y Eric López**, gracias por creer en este proyecto, por el tiempo invertido en él y por su gran esfuerzo para llevarlo a feliz término.

*Katya Karolyna Rodríguez Rivas*

# ÍNDICE

# *INTRODUCCIÓN*

Solo hemos empezado a descubrir el potencial que las tecnologías de la información nos ofrecen no solo en el importante campo de la investigación y la educación sino también en áreas como el comercio, la industria, las ciencias de la salud, etc. En el caso particular de las universidades, utilizar dichas tecnologías en el campo de las redes informáticas es de suma importancia ya que esto permite a largo plazo, la creación de grupos o comunidades de expertos con el fin de compartir conocimientos, experiencias e información que conlleven a que la población universitaria (estudiantes, docentes, personal administrativo) de diferentes partes del mundo se apoyen mutuamente dando como resultado mayores oportunidades en el campo de las investigaciones y la educación.

En el año 2003, TERENA pone en marcha un proyecto diseñado para proporcionar un acceso seguro a las redes informáticas de las diferentes instituciones miembros de las Redes Nacionales de Investigación y Educación de Europa. Este proyecto se conoce con el nombre de Eduroam (Education Roming). Eduroam nace con el objetivo de coordinar las iniciativas de diversas organizaciones con el fin de conseguir un espacio único de movilidad (Roaming) entre ellas. Este espacio único de movilidad consiste en un amplio grupo de organizaciones que con base en una política de uso y una serie de requerimientos tecnológicos y funcionales, permiten que sus usuarios puedan desplazarse entre ellas, disponiendo en todo momento de servicios móviles que pudiera necesitar. El objetivo último sería que estos usuarios al llegar a otra organización dispusieran, de la manera más transparente posible, de un entorno de trabajo virtual con conexión a Internet, acceso a servicios y recursos de su organización origen, así como acceso a servicios y recursos de la organización que en ese momento les acoge. Eduroam está basado en una autenticación de usuarios segura a redes por medio de los protocolos RADIUS, 802.1X y LDAP.

Integrar la Universidad de El Salvador a la red académica de usuarios móviles Eduroam involucra que la universidad cumpla los requisitos necesarios tanto técnicos como operativos. Estos requisitos involucran tanto a las facultades que integran la universidad como a la población universitaria (Personal Docente, Personal Administrativo y Estudiantes), para todo esto es necesario llevar un control de la ejecución de los requisitos técnicos y operativos.

En este documento se presenta un análisis de la situación actual de la red inalámbrica de la Universidad de El Salvador, base para la integración de la misma al proyecto mundial Eduroam, así como un inventario detallado del equipo con el que cuenta actualmente, su ubicación y la cobertura que este brinda. Además se presenta la Determinación de los Requerimientos, Diseño de la red inalámbrica de la Universidad de El Salvador para la integración a Eduroam y finalmente la configuración de los equipos de red para la integración de la universidad a Eduroam.

# OBJETIVOS

## *GENERAL*

Realizar el análisis de la situación actual, el diseño y la configuración de todos los elementos que componen el proyecto de Integrar a la Universidad de El Salvador al Proyecto Mundial de Usuarios Móviles Eduroam.

## *ESPECÍFICOS*

1. Analizar la seguridad existente en la red inalámbrica de la Universidad de El Salvador, para proponer mejoras ha dicho sistema de seguridad.
2. Elaborar un inventario detallado del equipo con el que cuenta la red inalámbrica de la universidad actualmente para proponer mejoras.
3. Determinar los requerimientos técnicos y funcionales para la integración de la universidad a Eduroam.
4. Elaborar el diseño de red inalámbrica propuesta en la Universidad de El Salvador para que pueda integrarse con éxito al programa mundial Eduroam.
5. Verificar el correcto funcionamiento de los protocolos RADIUS y LDAP.
6. Configurar el protocolo 802.1X en los dispositivos de red.
7. Configurar el programa cliente del protocolo 802.1X en los equipos móviles o estacionarios.
8. Elaborar Manual de Usuarios para el Cliente 802.1X SecureW2.
9. Elaborar Manual Técnico para administradores de Red.
10. Presentar alternativas de configuraciones de equipo.

# 1 MARCO TEÓRICO

## 1.1 PROYECTO MUNDIAL EDUROAM

### ¿Qué es Eduroam?

Es un programa al cual pertenecen muchas instituciones educativas, con el fin de permitir a los miembros de dichas instituciones navegar en Internet a través de cualquiera de sus redes inalámbricas locales, con la seguridad de contar con dicho servicio y tener la posibilidad de acceso a recursos o aplicaciones de éstas según las políticas de cada institución a través de dispositivos móviles que dispongan de tecnología WiFi.

Los miembros de cada institución pueden acceder a la red inalámbrica con las credenciales (usuario y contraseña) asignadas por su institución. En el caso de usuarios invitados (miembros que pertenecen a otra institución adscrita al proyecto Eduroam) podrán autenticarse en la red inalámbrica de la institución que se ubican y acceder a los recursos de su institución por medio del nombre de usuario y contraseña asignadas por su institución origen.

Eduroam utiliza protocolos de seguridad para evitar que usuarios no invitados tengan acceso a la red inalámbrica y por lo tanto a servicios y recursos o aplicaciones que ésta brinda. Los protocolos utilizados son el 802.1X, LDAP y RADIUS.

***Protocolo LDAP (Protocolo Ligero de Acceso a Directorios):***

Es un protocolo de tipo cliente-servidor para acceder a un servicio de directorio. Un directorio es como una base de datos, pero en general contiene información más descriptiva y basada en atributos. La información contenida en un directorio normalmente no se modifica simplemente se consulta. Los directorios no implementan normalmente los complicados procesos de transacciones (insertar, eliminar, consultar y modificar) que las bases de datos utilizan para llevar a cabo procesos de grandes volúmenes de datos. Por lo anterior, las actualizaciones en un directorio son usualmente cambios sencillos de "todo o nada", si es que se necesita hacer algún cambio.

***Protocolo (Servidor) RADIUS (Remote Authentication Dial-In User Server):***

Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones. Cuando se realiza la conexión con un proveedor de Internet (ISP) mediante módem, DSL, cablemódem, Ethernet o Wi-Fi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se

transfiere a un dispositivo NAS (Servidor de Acceso a la Red) sobre el protocolo PPP[1] (protocolo punto a punto), quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como EAP[2]. Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros como L2TP, etc. Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión.

***Protocolo 802.1X:***

Es una norma del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE por sus siglas en inglés) para Control de Admisión de Red basada en puertos. Es parte del grupo de protocolos IEEE 802 [3](IEEE 802.1). Permite la autenticación de dispositivos conectados a un puerto LAN (red de área local), estableciendo una conexión punto a punto o previniendo el acceso por ese puerto si la autenticación falla. Es utilizado en algunos puntos de acceso inalámbricos cerrados y se basa en protocolo de autenticación extensible (EAP). Algunos proveedores están implementando 802.1X en puntos de acceso inalámbricos que pueden utilizarse en ciertas situaciones en las cuales el punto de acceso necesita operarse como un punto de acceso cerrado, corrigiendo fallas de seguridad del Protocolo de Encriptación (WEP[4]). Esta autenticación es realizada normalmente por un tercero, tal como un servidor de RADIUS. Esto permite la autenticación sólo del cliente o, más apropiadamente, una autenticación mutua fuerte utilizando protocolos como EAP. *Protocolo Entendible de Autenticación* (EAP). Es uno de los elementos básicos del 802.1X y desarrollado como mejora del Protocolo Punto a Punto (PPP). PPP utiliza como Método de autenticación "username" y "password". Así fue diseñado EAP, basado en el protocolo PPP y proporcionando un marco generalizado para diversos métodos de autenticación. EAP sirve como soporte a protocolos propietarios de autenticación, gestiona las contraseñas en mecanismos de desafío-respuesta y es capaz de trabajar con tecnología de clave pública.

El ser parte de Eduroam permite a los usuarios que visitan otras instituciones conectadas con Eduroam entrar a la red inalámbrica de acceso local (WLAN[5]) usando las mismas credenciales

[1] PPP (Point-to-Point Protocol), http://en.wikipedia.org/wiki/Point-to-Point_Protocol

[2] EAP (Extensible Authentication Protocol), http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol

[3] Protocolo IEEE 802, http://es.wikipedia.org/wiki/IEEE_802

[4] WEP (*Wired Equivalent Privacy), http://es.wikipedia.org/wiki/WEP*

[5] WLAN (wireless Local-Area Network), Red de Área Local Inalámbrica.

(usuario y contraseña) que el usuario utilizaría si él estuviera en su institución sede. Dependiendo de las políticas locales de la institución visitada, los participantes de Eduroam pueden también tener recursos adicionales en su disposición. Todo esto con una administración mínima.

## *1.2 CÓMO INICIO EDUROAM*

La idea del proyecto Eduroam nace de la necesidad de desarrollar un espacio de colaboración en cuanto a movilidad entre organizaciones de la comunidad investigadora europea de tal manera que se faciliten los desplazamientos de los investigadores entre las diferentes instituciones, permitiendo que puedan disponer de forma automática de servicios de conectividad como, por ejemplo, el acceso a Internet.

La iniciativa Eduroam nació dentro del grupo de trabajo TF-Mobility Task Force de TERENA [6](Trans-European Research and Education Networking Association), cuyas actividades se basan en la promoción y la participación en el desarrollo de infraestructuras de telecomunicaciones y computación en beneficio de la investigación y la educación.

En concreto, el TF-Mobility Task Force se inició en enero del 2003 para estudiar las diferentes soluciones de movilidad existentes en Europa. Sus trabajos se centran en el desarrollo de arquitecturas de red y herramientas de autenticación y autorización que faciliten la itinerancia (roaming) a los investigadores y estudiantes y les permitan la movilidad entre las diferentes redes de investigación y educación nacionales (NREN). De entre las NREN europeas que ya se han adherido a esta iniciativa, destacan las de Alemania, Italia, Grecia, Portugal y Reino Unido, entre otras. También se está iniciando su implantación en otros países fuera de la Unión Europea, como Australia.

Los métodos de acceso a Eduroam se basan principalmente en tres tipos de tecnologías diferentes: el estándar 802.1X, el control de acceso vía web y el acceso a través de redes privadas virtuales (VPN[7]). Todas estas soluciones de movilidad son válidas y pueden interoperar en un mismo entorno.

El 802.1X es un estándar de autenticación que necesita de un software de cliente para poder establecer la sesión de autenticación. El acceso mediante la redirección web no requiere de la instalación de ningún software específico y es válido para cualquier sistema operativo. Para conectarse es necesario autenticarse a través de un navegador web cualquiera. La VPN es una red privada que se extiende a diferentes puntos remotos a través de infraestructuras públicas de

[6] TF-Mobility Task Force, http://www.terena.org/

[7] Virtual Private Networks: Red Privada Virtual

transporte, mediante el encapsulado y cifrado de los paquetes de datos. Para poder utilizarla hace falta disponer de un cliente VPN que ya se incluye por defecto en muchos sistemas operativos o que se puede instalar gratuitamente.

El acceso mediante la redirección web es muy sencillo y práctico, y es el que actualmente ofrecen las instituciones de la Anella que ya participan en Eduroam. Aunque este método presenta algunas carencias en cuanto a seguridad y por eso es recomendable que esté disponible algún otro método alternativo. Según TERENA, el más conveniente es el 802.1X, que asegura que sólo los usuarios autenticados podrán acceder a los recursos de la red.

## *1.3 OBJETIVOS DE EDUROAM*

1. Coordinar la puesta en marcha de infraestructuras de movilidad en la comunidad internacional, sirviendo de punto de encuentro de problemas y soluciones.
2. Coordinar el desarrollo de una política de uso con el fin de crear un espacio único de movilidad entre nuestras organizaciones.
3. Homologar las soluciones tecnológicas a implantar en las diferentes organizaciones con las acordadas a nivel europeo e internacional en este sentido.
4. Trabajar en soluciones que ayuden a difundir información sobre tipos de instalaciones e información a nivel de organización sobre: modos de acceso, cobertura, etc.
5. Informar de todos los temas relativos a la movilidad: guías de apoyo, estándares, soluciones (tanto propietarias como de libre distribución), etc.
6. Promocionar nuevas soluciones e iniciativas originadas en organizaciones de nuestra comunidad tanto dentro de nuestra red, como a nivel internacional.

## *1.4 CÓMO INTEGRARSE A EDUROAM*

Para poder llevar todo esto a la práctica, es necesario que las instituciones participantes cumplan con una serie de parámetros tanto tecnológicos como funcionales. Tienen que configurar el sistema de autenticación de su red para identificar a los usuarios a través de un servidor RADIUS que se enlazará con los servidores de las otras instituciones.

**PASOS PARA INTEGRARSE A EDUROAM**

Para poder integrarse a Eduroam es necesario que estén configurados y en buen funcionamiento los protocolos LDAP y RADIUS en toda la institución. A continuación se presentan los pasos a seguir:

1. Configurar el protocolo 802.1X en la LAN[8] interna de la institución.
2. Instalar en las computadoras de los usuarios el cliente 802.1X para poder establecer una comunicación con la LAN de la institución.
3. Una vez que se ha configurado correctamente 802.1X en su institución, es necesario conectar el servidor RADIUS local con el servidor RADIUS de nivel superior Europeo, los cuales son dos:
    - etlr1.Eduroam.org (192.87.106.34), por SURFnet, ubicado en Holanda
    - etlr2.Eduroam.org (130.225.242.109), por UNI-C, ubicado en Dinamarca

Las NREN[9] que quieran convertirse en miembros de Eduroam puede enviar un E-mail a la dirección siguiente: join@Eduroam.org

## *1.5 COMO TRABAJA EDUROAM*

Usted puede aprender más sobre cómo trabaja Eduroam leyendo los siguientes ejemplos:
*Ejemplo 1: Conexión usando Eduroam localmente, descripción general*
Juan estudia antropología en la Institución1. Él, como todos sus compañeros de estudio, lleva siempre su laptop con él pues la red inalámbrica ahora se ha desplegado a casi todo el campus. Cada vez que él desea utilizar la red, tiene que autenticarse con sus credenciales personales (usuarios y contraseña) en la infraestructura de Eduroam. Cuando él está conectado la red inalámbrica de la Institución 1, Juan, como usuario localmente afiliado, puede tener acceso a todos los servicios normales como si él estuviera conectado a la red normal.

<u>El procedimiento de conexión</u>

Juan encuentra la red inalámbrica llamada "Eduroam" y se conecta. El punto de acceso local inalámbrico trabaja como encargado del ingreso, pidiendo para el control del administrador de la red las credenciales de Juan. Éstos se proporcionan vía software del cliente en la computadora de Juan (mientras que el proceso de la conexión se basa en el Protocolo de seguridad 802.1X usando una

[8] Local Area Network: Red de Area Local

[9] National Research and Education Network: Red Nacional de Investigación y Educacion

disposición especial llamada TTLS[10]). El servidor de autenticación (que contiene todos los usuarios conocidos del campus) en la Institución 1 es contactado y si Juan se autentica, el estará conectado a través de la red inalámbrica. Antes de esto el no podrá conseguir una dirección IP y por lo tanto no puede acceder a otros a la red de ninguna manera.

**Autenticación en la institución Origen, usando Eduroam**

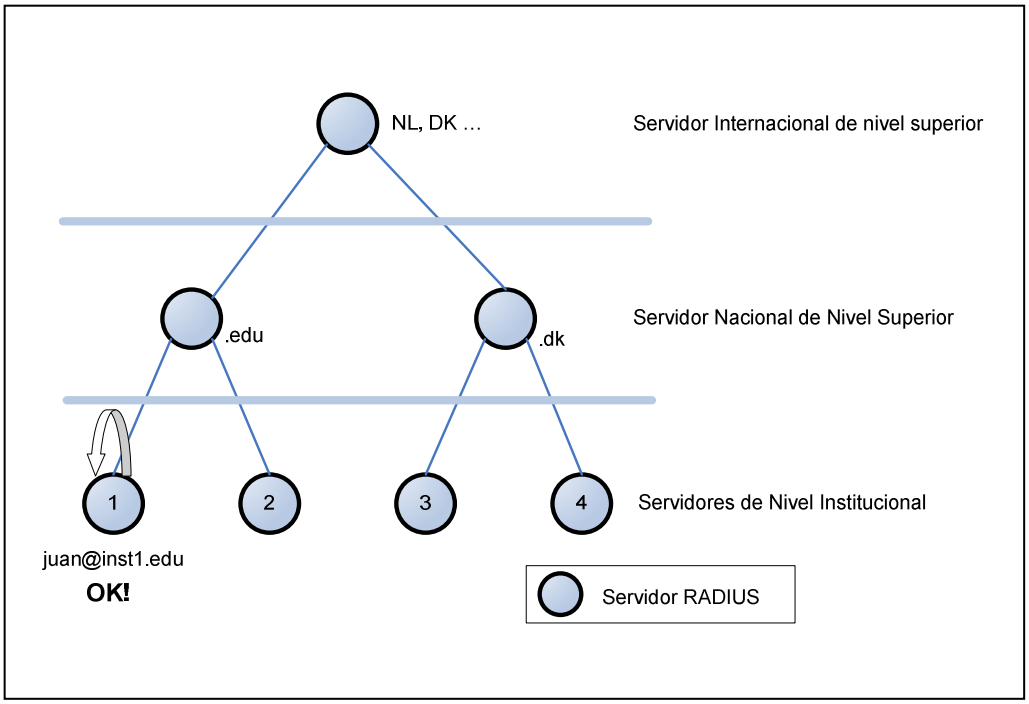



*Figura 1.5.1 Conexión a Eduroam localmente.*

Cuando el punto de acceso de la red inalámbrica ve la máquina de Juan, primero pide el dominio del usuario (inst1.edu). Esto se utiliza para crear un canal encriptado entre el usuario y el servidor de autenticación donde no puede ser interceptada una transmisión privada y para no intervenir el punto de acceso de la red inalámbrica. Entonces las credenciales son transferidas al servidor de autenticación de la institución central. En este caso solamente es necesario el nombre del usuario (Juan) que es la dirección de correo de Juan, mientras que él es reconocido localmente (por el real 'inst1.edu'). Cuando es aceptado, un mensaje es enviado a los puntos accesos de la red inalámbrica que alternadamente permite al usuario acceso a la red. De esta manera todos los punto de acceso conocerán sobre Juan es su dominio y eso es aceptable y lo deja conectarse a la red. El tráfico entre el punto de acceso y la máquina de Juan seguirá cifrado durante la sesión entera.

[10] TTLS Tunneled Transport Layer Security: Seguridad por Túnel en la Capa de Transporte, http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol

*Ejemplo 2: Conexión usando Eduroam como invitado, el mismo país*

Juan ha decidido seguir una serie de charlas que serán impartidas en otra universidad (Institución-2). Él irá allí cada semana por dos meses pero no se propone inscribirse en esa universidad, él solamente desea oír las charlas. Para Juan, el estar ausente un día entero sin la conexión de red es inconcebible, y afortunadamente su temor es infundado ya que la Institución-2 tiene por supuesto una red de conexión inalámbrica y también es miembro de Eduroam.
Una diferencia, sin embargo, es que él no podrá imprimir o usar cualquier servicio especial siendo un invitado en la Institución-2. Esto es, porque la Institución-2 decidió que estos servicios sean solamente para personas directamente relacionadas con la institución. Pero Juan podrá conectarse a la World Wide Web, revisar su correo electrónico y usar su cliente VPN para conectarse a la Institución-1, de la cual es miembro.

El procedimiento de conexión

Como siempre Juan se tiene que conectar a la red inalámbrica llamada "Eduroam", justo como lo hace en la institución a la que pertenece. Hasta el momento todo trabaja exactamente de la misma forma que en su institución: Digita sus credenciales y éstas le permiten conectarse a la red.

**Autenticación en otra institución del mismo país, usando Eduroam**

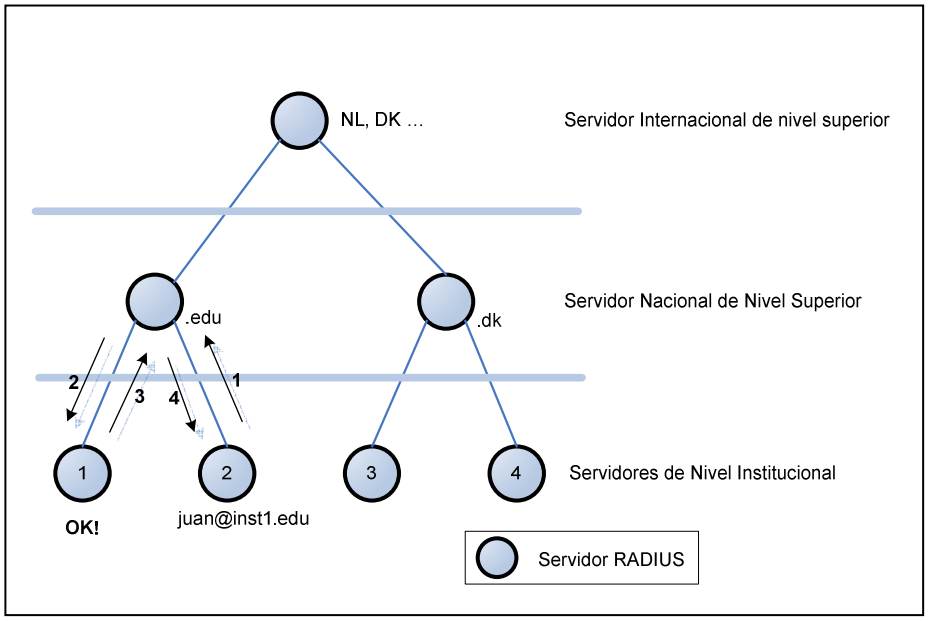



*Figura 1.5.2 Conexión a Eduroam en otra institución a nivel nacional.*

Lo que él no ve es que en lugar de solicitar su autenticación al servidor local, ésta solicitud es enviada a su institución (Institución-1) por medio del servidor de nivel superior de Eduroam. El servidor de autenticación local de la Institución-2 no sabe que hacer con la petición y por lo tanto envía la petición al servidor nacional de Eduroam de nivel superior que sabe qué hacer con ésta. El servidor nacional mantiene una lista de todos los dominios que participan de un país dado y por lo tanto sabe dónde enviar la petición. El servidor de autenticación de la Institución-1 reconoce a Juan como un usuario de la red y envía el mensaje de regreso al punto de acceso que lo solicitó siguiendo la misma ruta que siguió la petición.

El tráfico entre el punto de acceso inalámbrico y la máquina de Juan se mantendrá encriptado durante toda la sesión.

*Ejemplo 3: Conexión usando Eduroam como invitado, al exterior*

Al buen estudiante Juan le han pedido presentar su tésis en una conferencia en la Institución-3 para ser aceptado en Dinamarca, Escandinavia.

Dinamarca y la Institución-3 también se han unido a Eduroam y por lo tanto él puede conectarse como de costumbre y todavía está siendo autorizado por el servidor de su universidad. Esto por supuesto da a los organizadores de la conferencia (y a administradores de la red) mucho menos en qué pensar ya que saben que los usuarios huéspedes que usen su red serán usuarios autenticados por alguna otra Universidad o institución miembro de Eduroam.

<u>El procedimiento de conexión</u>

Como siempre Juan se tiene que conectar a la red inalámbrica llamada 'Eduroam', como si él estuviese en su país. Todo parece trabajar exactamente de la misma manera: él digita sus credenciales y esto le permite conectarse a la red.

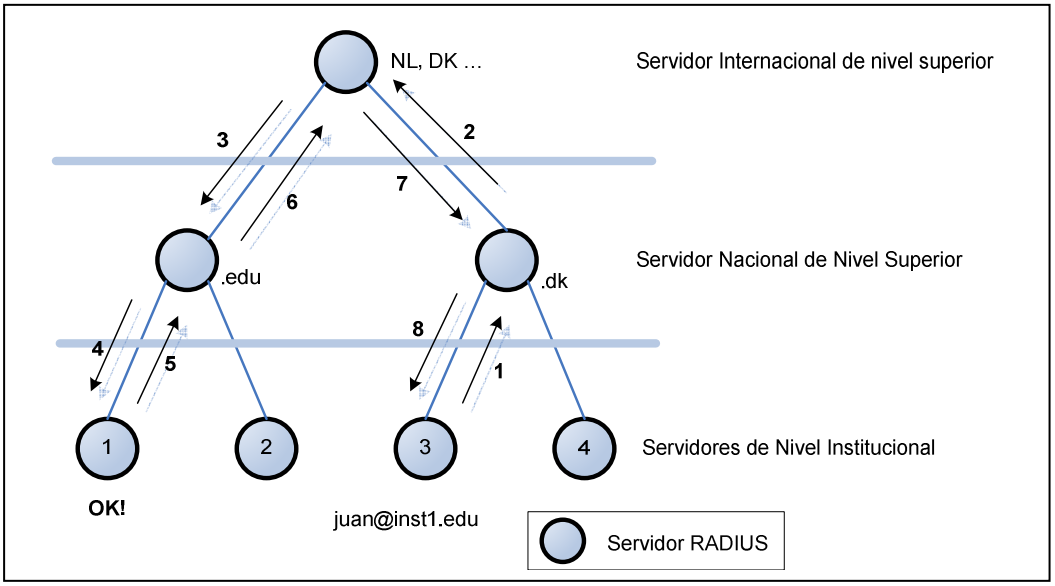



*Figura 1.5.3 Conexión a Eduroam como invitado a nivel internacional.*

Lo que él no ve es que su petición de autenticación primero está enviada al servidor local de la autenticación en Institución-3, y después al Servidor Internacional de nivel superior en Dinamarca. Sin embargo, como la institución 1 es desconocida para el servidor nacional, entonces se envía al Servidor Internacional de nivel superior que si sabe dónde enviar los pedidos para los dominios de nivel superior y por lo tanto también adonde enviar la petición que se está haciendo que para este caso es **.edu**. Éste servidor nacional sabe a qué institución debe enviarla y finalmente se autentica al usuario en la Institución-1. El mensaje del reconocimiento se envía de nuevo al punto de acceso inalámbrico donde fue solicitado, siguiendo la misma ruta de la petición.

El tráfico entre el punto de acceso inalámbrico y la máquina de Juan seguirá cifrado durante la sesión entera.

## *1.6 MAPA DE MIEMBROS DE EDUROAM*

Aunque Eduroam inicio en Europa, recolectó rápido consenso afuera de Europa. El primer país no-Europeo en unirse a Eduroam fue Australia, en diciembre de 2004.

Eduroam se ha desarrollado en una federación de las federaciones (confederación), donde una sola federación se funciona a nivel nacional y todas conectan con una región.

Hasta la fecha hay dos confederaciones: La confederación europea Eduroam y la confederación Asia-Pacifico Eduroam (APAN). En la siguiente figura se muestra el mapa que representa las confederaciones de Eduroam. Para una vista detallada de los países (federaciones nacionales) que pertenece a cada confederación (europeo y APAN).

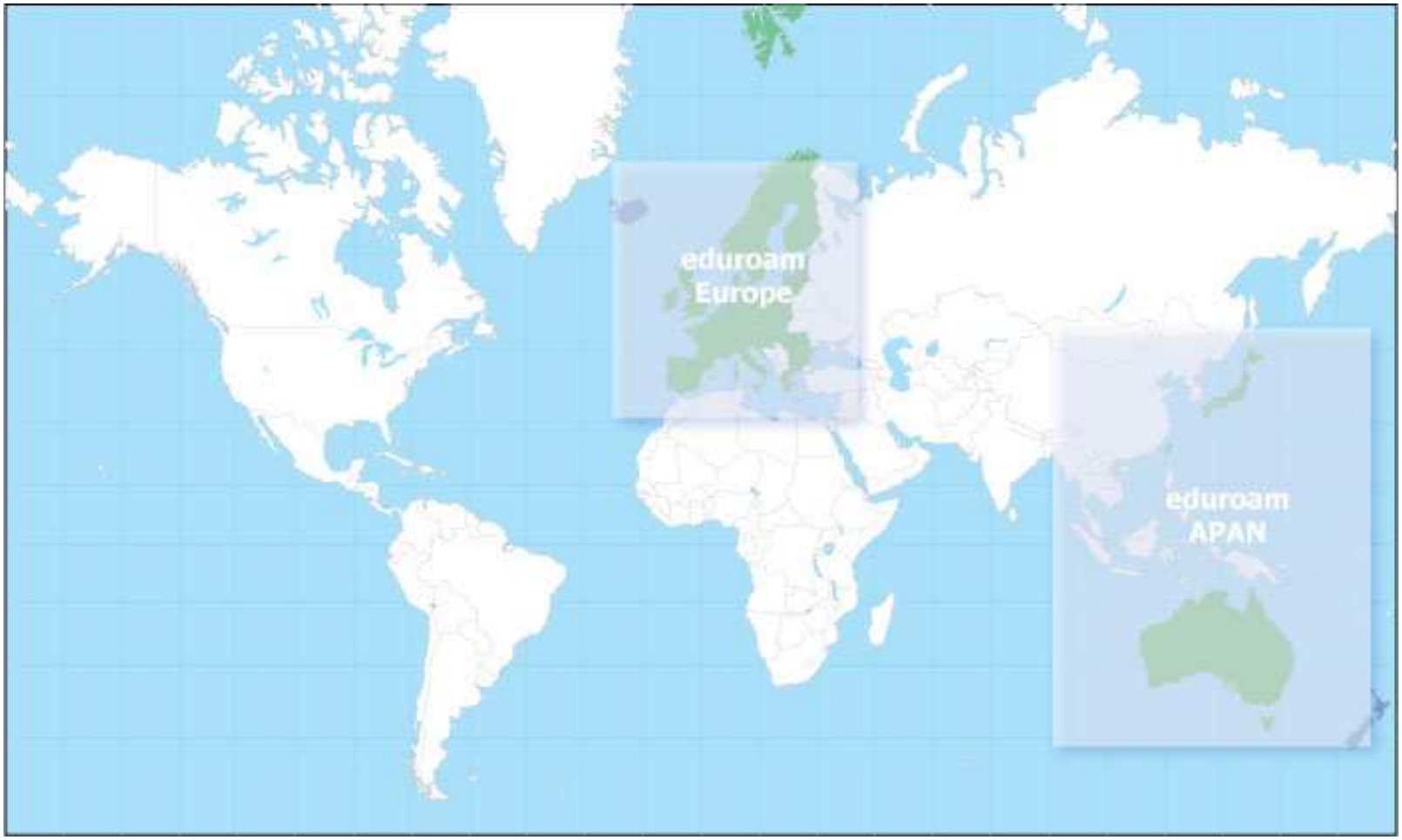



*Figura 1.6.1 Confederaciones de Eduroam.*

## CONFEDERACIÓN EUROPEA EDUROAM

En la siguiente figura se muestra los países donde hay un servidor RADIUS europeo de nivel superior funcionado por la red local educacional e investigación nacional (NREN) o la institución equivalente. TERENA proporciona la raíz europea (cuadro amarillo de la Figura 1.6.2 Países europeos miembros de Eduroam). Los dos servidores que proporcionan este servicio están funcionando por SURFnet (Holanda) y Forskningsnettet (Dinamarca).

PAÍSES CONECTADOS A EDUROAM DEL CONTINENTE EUROPEO

Los países europeos conectados actualmente con el Eduroam son:

| | |
|---|---|
| Austria (ACONet) | Lituania (LITNET) |
| Bulgaria (ISTF) | Luxemburgo (RESTENA) |
| Bélgica (BELNET) | Malta (CSC) |
| Croacia (CARNet) | Holanda (SURFnet) |
| Republica Checa (CESNET) | Noruega (UNINETT) |
| Dinamarca (UNI-C) | Polonia (PIONIER) |
| Estonia (EENet) | Portugal (FCCN) |
| Francia (RENATER) | Rumania (RoEduNet) |
| Finlandia (FUNET) | Eslovaquia (SANET) |
| Alemania (DFN) | Eslovenia (ARNES) |
| Grecia (GRNET) | España (RedIRIS) |
| Hungría (HUNGARNET) | Suiza (SUNET) |
| Italia (GARR) | Suecia (SWITCH) |
| Irlanda (HEAnet) | Reino Unido (UKERNA) |
| Latvia (LANET) | |


*Figura 1.6.2 Países Europeos Miembros de Eduroam.*

## CONFEDERACIÓN APAN EDUROAM

Los esfuerzos internacionales de implantar Eduroam en diversas regiones (Asia-Pacifico y los Estados Unidos) están en curso. Mientras que en Asia-Pacifico el avance de Eduroam está progresando absolutamente rápido ver la figura 1.6.3 países miembros a APAN Eduroam, en los Estados Unidos, el interés en el Eduroam se ha arraigado y un cierto trabajo se está haciendo para probar Eduroam.

PAÍSES CONECTADOS AL APAN EDUROAM

Los países conectados actualmente al APAN Eduroam son:

| | |
|---|---|
| Australia (AARNet) | Japón (NII) |
| China (UESTC) | Hong Kong (PolyU) |

A continuación se muestran los países interesados en hacerse miembros del APAN Eduroam: Corea, Nueva Zelanda y Singapur.

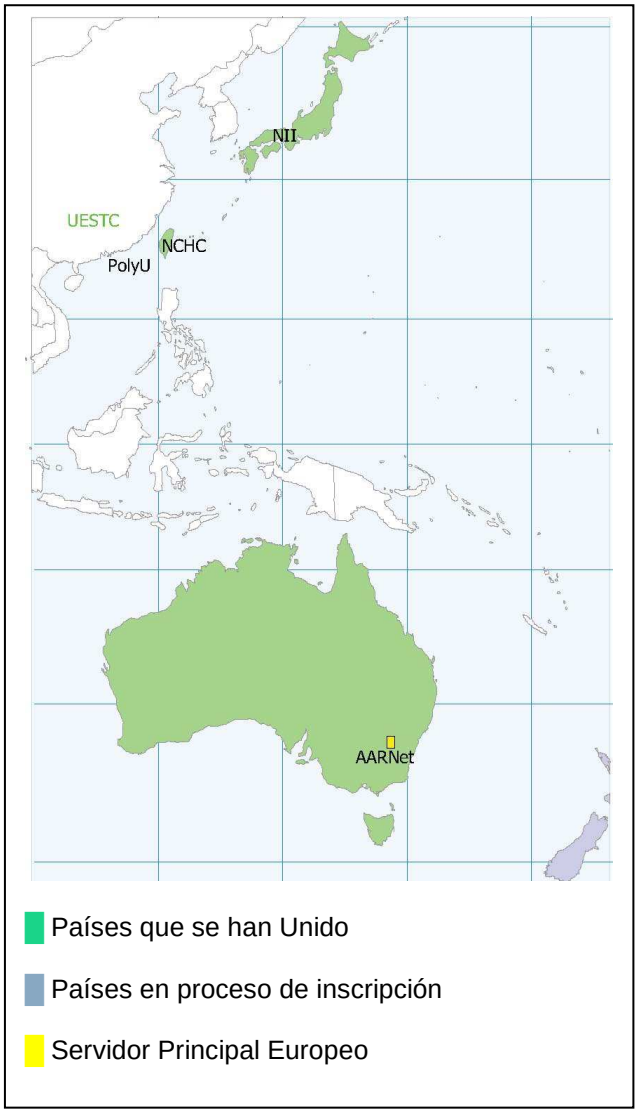



*Figura 1.6.3 Países Miembros al APAN Eduroam*

# 2 ANÁLISIS DE SITUACIÓN ACTUAL Y REQUERIMIENTOS

## 2.1 SITUACIÓN ACTUAL DE LA CONECTIVIDAD A EDUROAM EN LA UNIVERSIDAD DE EL SALVADOR

El estado actual de los elementos de la infraestructura para la conectividad de la Universidad de El Salvador al programa mundial Eduroam es la siguiente:

1. *Servidor RADIUS de nivel superior de la confederación.*

   Este está localizado en los Países Bajos y Dinamarca para la confederación europea, y en Australia y Hong Kong para las regiones del Pacífico y Asia respectivamente.

   Cada uno tiene una lista de los dominios de los países conectados y proporcionados adecuadamente por NRENs. Ellos aceptan las peticiones de dominios de la federación de los cuales son responsables y posteriormente reenvían las peticiones a los servidores RADIUS asociados de otras federaciones (y transportan las peticiones de autenticación de retorno).

2. *Servidor RADIUS de nivel superior de la Federación.*

   Tiene una lista de instituciones conectadas al servidor y realmente asociadas. Recibe peticiones de los servidores de la confederación y de las instituciones que tienen asociadas. Si están conectadas a él reenvía la petición a la institución apropiada, sino la redirecciona al servidor de la confederación.

3. *Servidor RADIUS Institucional.*

   Es el responsable de la autenticación de sus propios usuarios (tanto locales como de usuarios visitantes de otros instituciones) por medio de la verificación de sus credenciales sistema de administración local de identidades y reenvía las peticiones de los usuarios visitantes a sus respectivos servidores RADIUS de nivel superior de su Federación. Sobre la base de una autenticación apropiada este servidor asigna VLAN al usuario.

   Este servidor es el más complejo de todos ya que mientras los otros servidores RADIUS simplemente atienden peticiones de Proxy, el servidor institucional, además de resolver peticiones EAP, realiza operaciones de búsqueda en el sistema de administración de identidades.

   Actualmente la Universidad cuenta con un servidor RADIUS configurado y funcional, este funciona bajo la responsabilidad de la Unidad de Educación a Distancia, la cual es una dependencia de la Vice-Rectoría Académica.

En conjunto con el servidor RADIUS debe funcionar el sistema de Administración de Identidades, el cual contiene información de los usuarios; por ejemplo nombres de usuario y sus contraseñas. Este debe de mantenerse actualizado por la institución responsable. La Universidad de El Salvador cuenta actualmente para éste fin con la implementación del protocolo LDAP el cual permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información del entorno de red y es llamado con ese mismo nombre.

4. *Suplicantes*

   Un suplicante es un software (construido a menudo en el Sistema Operativo pero también está disponible como programa separado) que utiliza el protocolo 802.1X para enviar peticiones de información de autenticación usando EAP.

   Para este fin esta disponible el software SecureW2, el cual es un cliente de EAP-TTLS [11]de libre distribución.

5. Puntos de Acceso (AP)

   Necesita soportar el protocolo 802.1X. Deben ser capaces de reenviar peticiones de acceso provenientes de un suplicante hacia un servidor RADIUS institucional, para dar el acceso de red sobre la base de una autenticación apropiada, y posibilitar la asignación de los usuarios a VLANs específicas basados en la información recibida del servidor RADIUS. Además el punto de acceso intercambia información de las llaves (vectores de inicialización, llaves públicas y de acceso, etc) con los sistemas clientes para prevenir la contaminación de las sesiones de red establecidas.

   La mayoría de las Facultades de la Universidad cuentan con este tipo de equipo y también existe en el mercado local varias opciones a precios accesibles (ver anexo 10 ""Cotización y adquisición de equipo de red").

[11] EAP-TTLS (EAP-Tunneled Transport Layer Security), http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#EAP-TTLS

6. Switches

Deben tener la capacidad de reenviar peticiones de acceso provenientes de un suplicante hacia los servidor RADIUS institucional, todo con el fin de dar acceso a la red basada en una autenticación apropiada y con la posibilidad de asignar usuarios a una especifica VLAN basada en la información recibida del servidor RADIUS.

Se podría decir que estos tienen la misma situación que los puntos de acceso. Las diferentes facultades de la Universidad los poseen en diferentes marcas y modelos (ver anexo 9 “Inventario de Hardware de Red por Facultad de la Universidad de El Salvador”).

## 2.2 SITUACIÓN ACTUAL DE LA WLAN

La red inalámbrica de la Universidad de El Salvador actualmente no tiene un enfoque "Roaming", en el cual, las estaciones de trabajo se puedan mover de un punto de acceso (Acces Point) a otro sin perder conectividad. La red inalámbrica de la universidad consiste en la colocación de varios switches administrables en algunos de los edificios principales de cada facultad, a los cuales se vinculan los distintos puntos de acceso necesarios para dar cobertura a una zona especifica, y dentro de ésta al número posibles de usuarios finales que tenga la red.

A continuación se detalla el inventario actual de equipo de red con que cuenta la universidad y los planos de ubicación de los puntos de acceso con sus respectivos radios de cobertura.

### 2.2.1 Inventario de Hardware de red inalámbrica de la Universidad de El Salvador

A continuación se presentan los equipos de red inalámbrica que poseen cada facultad de la Universidad de El Salvador. Este inventario fue realizado entre Marzo y Abril del año 2007, con la ayuda de los administradores de la red de cada facultad de la Universidad de El Salvador.

#### 2.2.1.1FACULTAD MULTIDISCIPLINARIA OCCIDENTAL (SANTA ANA)

Edificios con la que cuenta dicha facultad:

- ✓ Usos Múltiples
- ✓ Medicina
- ✓ Instituto del Agua
- ✓ Ciencias Jurídicas
- ✓ Académica/Biología
- ✓ Economía
- ✓ Bunker

El edificio de Usos Múltiples es el nodo principal de la red en el se encuentran los siguientes equipos:

A. 2 MODEM ASMI-52 con el que provee servicio Telecom
B. 1 Router Cisco 1800 series
C. 1 Router Cisco 2800 series
D. 1 Pix Cisco 515E Firewall
E. 2 Switches Allied Telesyn modelo AT-8024GB
F. 3 Switches 3 COM modelo 3C17304
G. 2 Switches Allied Telesyn modelo AT-FS724L
H. 1 Router Lynsys Inalámbrico modelo WRT54GL
I. 2 Puntos de Acceso D-Link modelo DWL2100AP

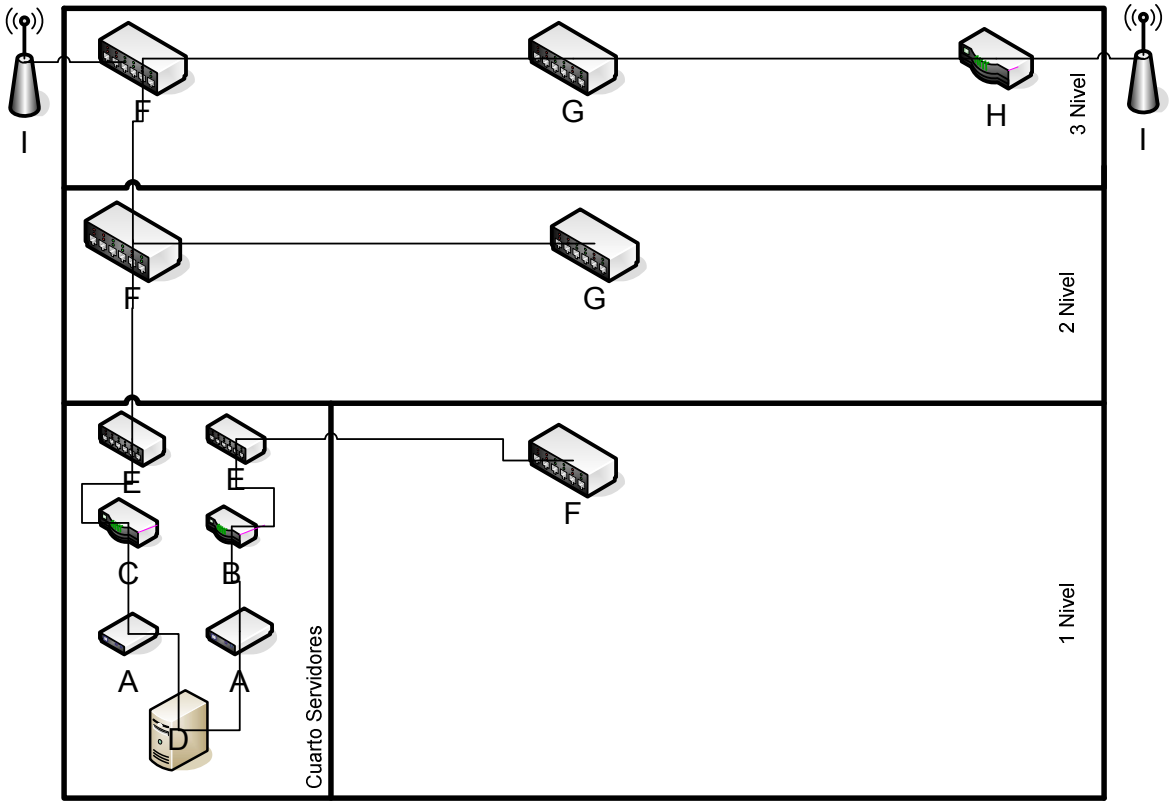



*Figura 2.2.1.1.1 Diagrama de ubicación de los equipos de red del Edificio de Usos Múltiples de la Facultad Multidisciplinaria de Occidente*

En el edificio de Medicina se encuentran los siguientes equipos de red:

A. 2 Switches Allied Telesyn modelo AT-FS724L
B. 1 Punto de Acceso D-Link modelo DWL2100AP

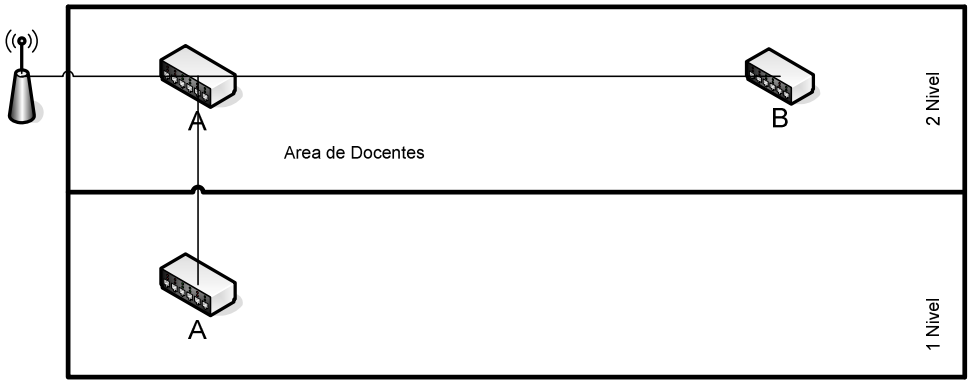



*Figura 2.2.1.1.2 Diagrama de Ubicación de los Equipos de Red del Edificio de Medicina de la Facultad Multidisciplinaria de Occidente*

En el edificio del Instituto del Agua se encuentran los siguientes equipos de red:

A. 2 Switches Allied Telesyn modelo AT-FS724L

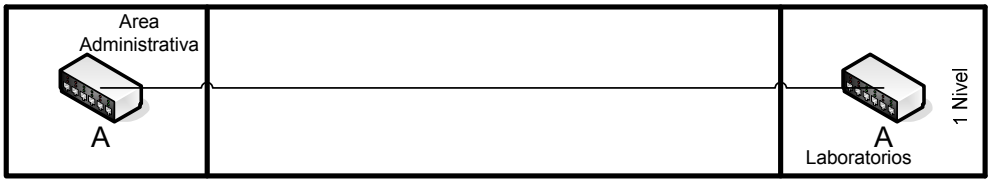



*Figura 2.2.1.1.3 Diagrama de Ubicación de los Equipos de Red del Edificio del Instituto del Agua de la Facultad Multidisciplinaria de Occidente*

En el edificio de Ciencia Jurídicas se encuentran los siguientes equipos de red:

A. 2 Switches Allied Telesyn modelo AT-FS724L


*Figura 2.2.1.1.4 Diagrama de Ubicación de los Equipos de Red del Edificio de Ciencias Jurídicas de la Facultad Multidisciplinaria de Occidente*

El edificio de Académica/biología es el nodo Secundario de la red en el se encuentran los siguientes equipos:

A. 1 Switches Allied Telesyn modelo AT-8024GB
B. 3 Switches 3 COM modelo 3C17304
C. 2 Switches Allied Telesyn modelo AT-FS724L

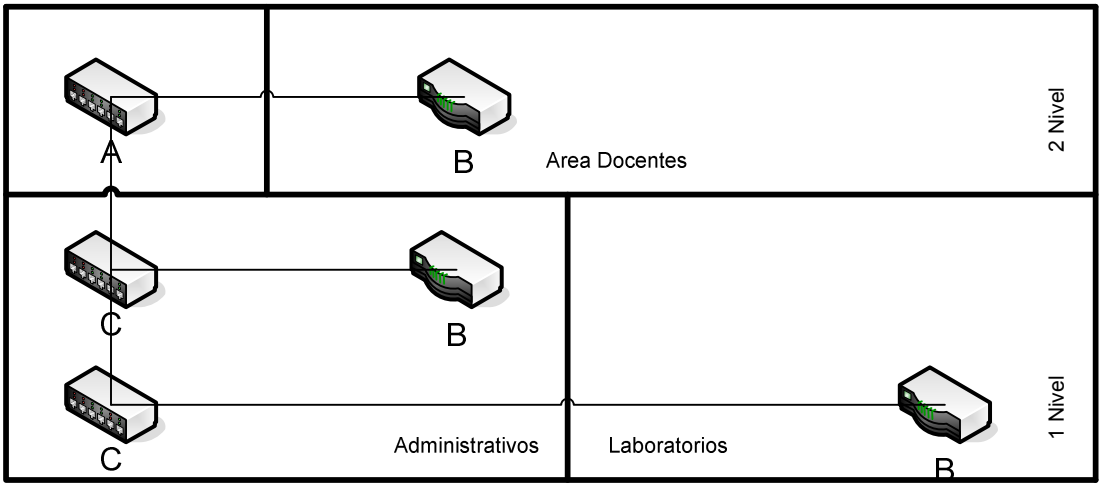



*Figura 2.2.1.1.5 Diagrama de Ubicación de los Equipos de Red del Edificio de Académica / Biología de la Facultad Multidisciplinaria de Occidente*

Por el momento los edificios de la facultad occidental se encuentran conectados por medio de fibra óptica a excepción de los edificios de economía y ciencias jurídicas que se conectan con UTP a través del nodo secundario. Además solamente el edificio de usos múltiples y medicina poseen red inalámbrica.

Contacto: Julio Damián Morales.

## 2.2.1.2 FACULTAD MULTIDISCIPLINARIA PARACENTRAL (SAN VICENTE)

Edificios con la que cuenta dicha facultad:

- ✓ Administrativo/Biblioteca/Maestros
- ✓ Aulas
- ✓ Asociación de Estudiantes
- ✓ Proyección y Servicio Social
- ✓ Postgrado
- ✓ Centro de Desarrollo Profesional Docente

El edificio de Administrativo/Biblioteca/Maestros es el nodo principal de la red en el se encuentran los siguientes equipos:

A. 2 MODEM ASMI-52 con el que provee servicio Telecom
B. 1 Router Cisco 2118 series
C. 1 Switch Allied Telesyn modelo Rapier 24i
D. 6 Switches Allied Telesyn modelo AT-FS716L
E. 3 Switches D-LINK DES-1024D

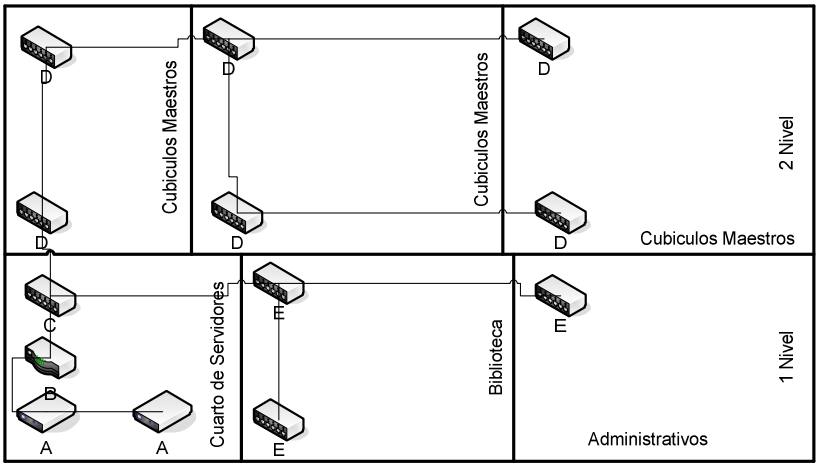



*Figura 2.2.1.2.1 Diagrama de ubicación de los equipos de red del Edificio de Administrativo / Biblioteca / Maestros de la Facultad Multidisciplinaria Paracentral*

En el edificio de Aulas se encuentran los siguientes equipos de red:

2 Switches Allied Telesyn modelo AT-FS716L.

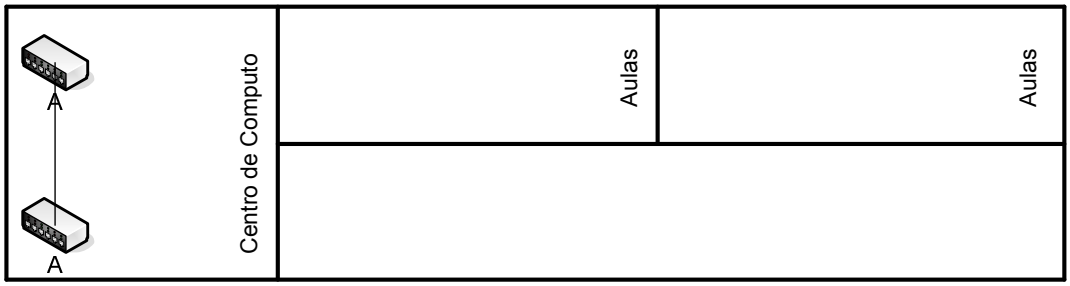



*Figura 2.2.1.2.2 Diagrama de ubicación de los equipos de red del Edificio de Aulas de la Facultad Multidisciplinaria Paracentral*

Por el momento los edificios de la facultad Paracentral se encuentran conectados por medio de cable UTP y solamente existe conexión entre dos edificios los cuales son el de Administrativo/Biblioteca/Maestros y Aulas

Además no poseen red inalámbrica.

Contacto: Víctor Castro.

## 2.2.1.3FACULTAD MULTIDISCIPLINARIA ORIENTAL (SAN MIGUEL)

Edificios con la que cuenta dicha facultad:

- ✓ Medicina
- ✓ Auditórium.
- ✓ Biblioteca
- ✓ Administrativo
- ✓ Centro de Computo
- ✓ Aulas Derecho/Economía

El edificio Administrativo es el nodo principal de la red en el se encuentran los siguientes equipos:

A. 2 MODEM ASMI-52 con el que provee servicio Telecom
B. 1 Router Cisco 1800 series
C. 1 Pix Cisco 515E Firewall
D. 1 Switch Allied Telesyn modelo Rapier 24i
E. 2 Switches Allied Telesyn modelo AT-8024GB
F. 3 Switches 3 COM modelo 3C17304
G. 2 Switches Allied Telesyn modelo AT-FS724L
H. 1 Punto de Acceso D-Link modelo DWL2100AP

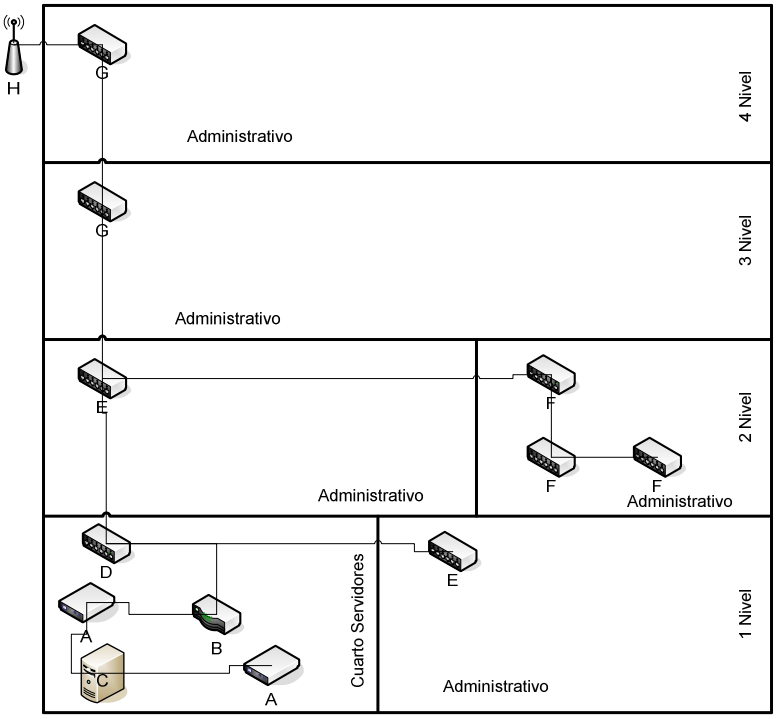



*Figura 2.2.1.3.1 Diagrama de ubicación de los equipos de red del Edificio Administrativo de la Facultad Multidisciplinaria Oriente*

En el edificio de Biblioteca se encuentran los siguientes equipos de red:

A. 1 Switch Allied Telesyn modelo Rapier 24i
B. 1 Switches Allied Telesyn modelo AT-FS724L

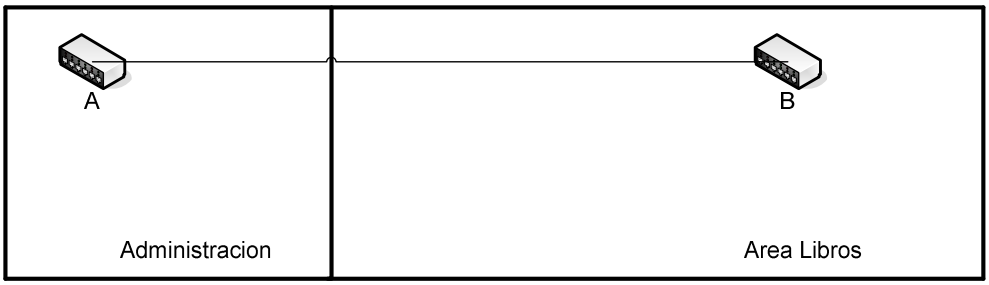



*Figura 2.2.1.3.2 Diagrama de ubicación de los equipos de red del Edificio de Biblioteca de la Facultad Multidisciplinaria Oriente*

En el edificio del Centro de Cómputo se encuentran los siguientes equipos de red:

A. 1 Switch Allied Telesyn modelo Rapier 24i
B. 3 Switches D-LINK DES-1024D

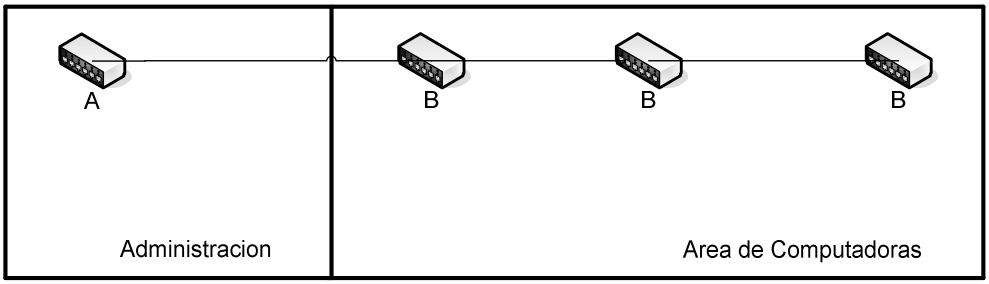



*Figura 2.2.1.3.3 Diagrama de ubicación de los equipos de red del Centro de Computo de la Facultad Multidisciplinaria Oriente*

Por el momento los edificios que se encuentran conectados de la facultad oriental son Administrativo, Biblioteca y Centro de Computo, estos lo hacen a través de cable UTP, los otros edificios como Medicina, Auditórium, Aulas Derecho/Economía no tienen conexión de red.

Además solamente el edificio Administrativo posee red inalámbrica.
Contacto: Consuelo Sandoval.

## 2.2.1.4FACULTAD DE CIENCIAS Y HUMANIDADES

Edificios con la que cuenta dicha facultad:

- ✓ Administrativo
- ✓ Idiomas/Filosofía
- ✓ Periodismo/Letras
- ✓ Intendencia
- ✓ Psicología/Educación
- ✓ Escuela de Artes
- ✓ Colecturía y CENIUS

El edificio Administrativo es el nodo principal de la red en el se encuentran los siguientes equipos:

A. 1 Switch Allied Telesyn modelo Rapier 24i
B. 1 Switch Allied Telesyn modelo AT-FS716L
C. 1 Switch D-LINK DES-1024D

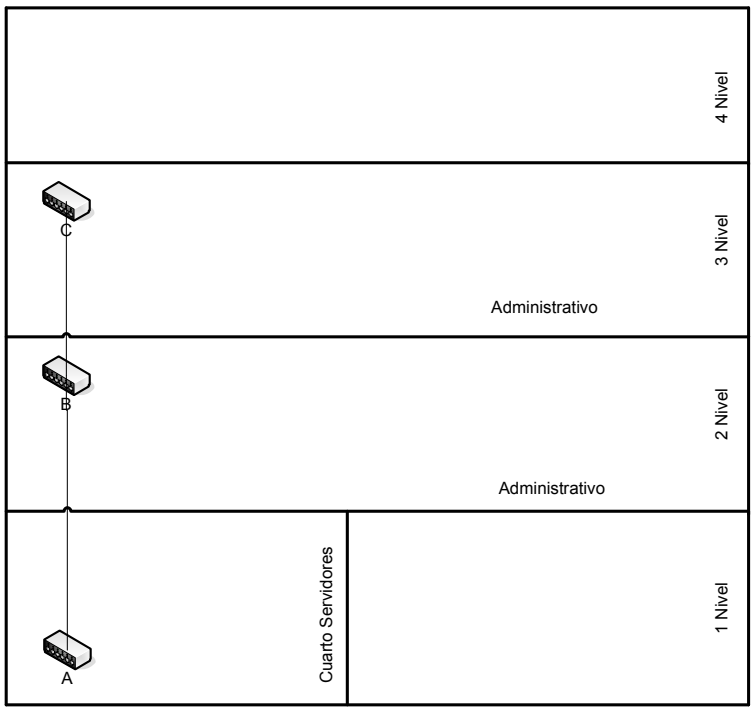



*Figura 2.2.1.4.1 Diagrama de ubicación de los equipos de red del Edificio Administrativo de la Facultad de Ciencias y Humanidades*

En el edificio de Idiomas/Filosofía se encuentran los siguientes equipos de red:

A. 1 Switch Allied Telesyn modelo Rapier 24i
B. 1 Switch Allied Telesyn modelo AT-FS716L

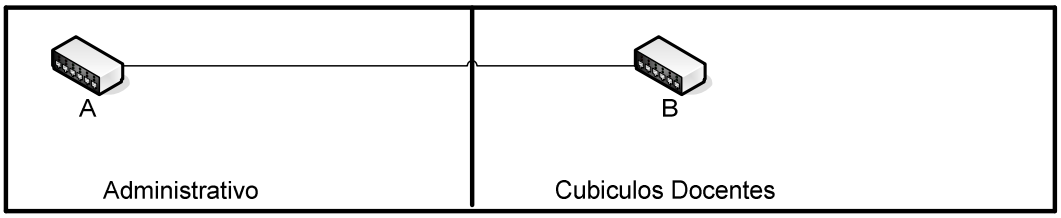



*Figura 2.2.1.4.2 Diagrama de ubicación de los equipos de red del Edificio Idiomas/Filosofía de la Facultad de Ciencias y Humanidades*

En el edificio de Periodismo/Letras se encuentran los siguientes equipos de red:

A. 1 Switch Allied Telesyn modelo Rapier 24i
B. 1 Switch Allied Telesyn modelo AT-FS716L


*Figura 2.2.1.4.3 Diagrama de ubicación de los equipos de red del Edificio Periodismo/Letras de la Facultad de Ciencias y Humanidades*

En el edificio de Psicología/Educación se encuentran los siguientes equipos de red:

- ✓ 1 Switch Allied Telesyn modelo Rapier 24i
- ✓ 1 Switch Allied Telesyn modelo AT-FS716L

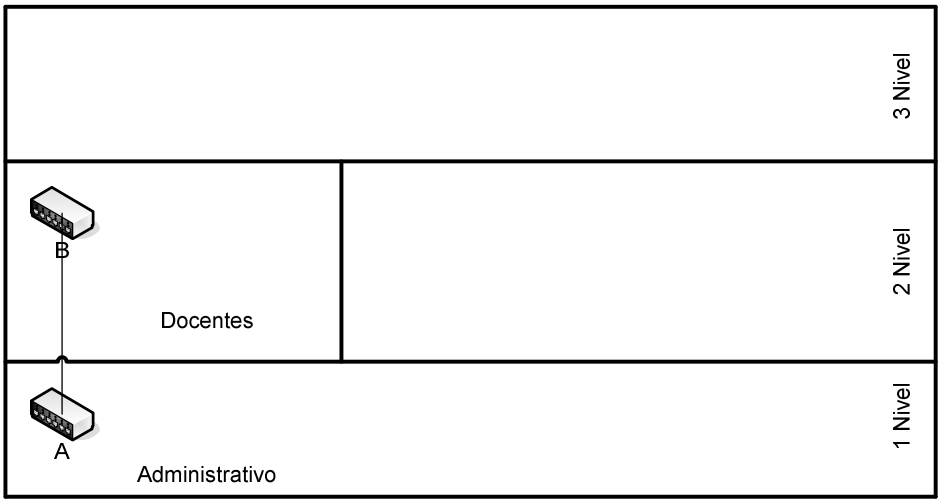



*Figura 2.2.1.4.4 Diagrama de ubicación de los equipos de red del Edificio Psicología/Educación de la Facultad de Ciencias y Humanidades*

En el edificio de Escuela de Artes se encuentran los siguientes equipos de red:

A. 1 Switch Allied Telesyn modelo Rapier 24i
B. 1 Switch Allied Telesyn modelo AT-FS716L


*Figura 2.2.1.4.5 Diagrama de ubicación de los equipos de red del Edificio Escuela de Artes de la Facultad de Ciencias y Humanidades*

En el edificio de Colecturía y CENIUS se encuentran los siguientes equipos de red:

A. 1 Switch Allied Telesyn modelo Rapier 24i
B. 1 Switch Allied Telesyn modelo AT-FS716L

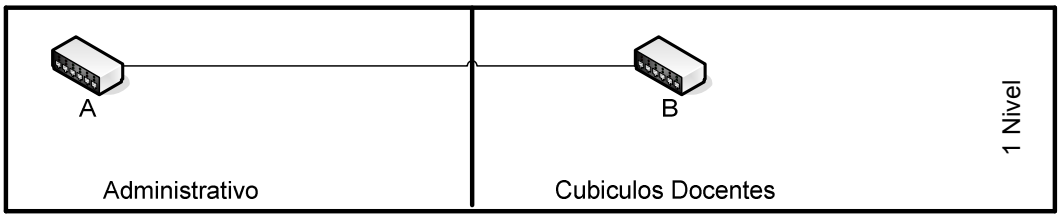



*Figura 2.2.1.4.5 Diagrama de ubicación de los equipos de red del Edificio Colecturía y CENIUS de la Facultad de Ciencias y Humanidades*

Por el momento los edificios de la facultad de Ciencias y Humanidades se encuentran conectados por medio de Fibra Óptica y dentro del mismo edificio lo hacen a través de cable UTP.

Además no poseen red inalámbrica pero están en proceso de instalación del equipo.

Contacto: José Manuel López.

## 2.2.1.5FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICAS

Edificios con la que cuenta dicha facultad:

- ✓ Física/Matemática
- ✓ Administrativo/Química
- ✓ Biología
- ✓ Auditórium.

El edificio de Física/Matemática es el nodo principal de la red en el se encuentran los siguientes equipos:

A. 1 Switch Allied Telesyn modelo Rapier 24i
B. 1 Switch Allied Telesyn modelo AT-FS724L
C. 10 Switches C-NET modelo CNSH1600
D. 2 Switches NEXXT modelo NW223NXT29
E. 2 Switches LG modelo LS3116A
F. 1 Switch D-LINK modelo DES-1016D
G. 1 Switch D-LINK modelo DES-1024D

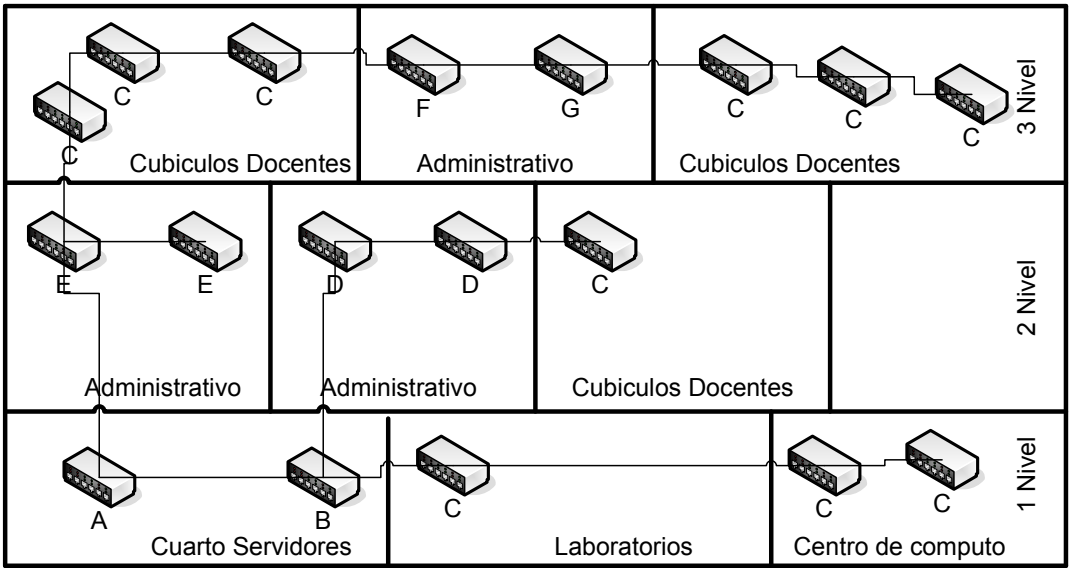



*Figura 2.2.1.5.1 Diagrama de ubicación de los equipos de red del Edificio Física/Matemática de la Facultad de Ciencias Naturales y Matemáticas*

En el edificio de Administrativo/Química se encuentran los siguientes equipos de red:

A. 1 Switch Allied Telesyn modelo AT-FS724L
B. 3 Switches C-NET modelo CNSH1600

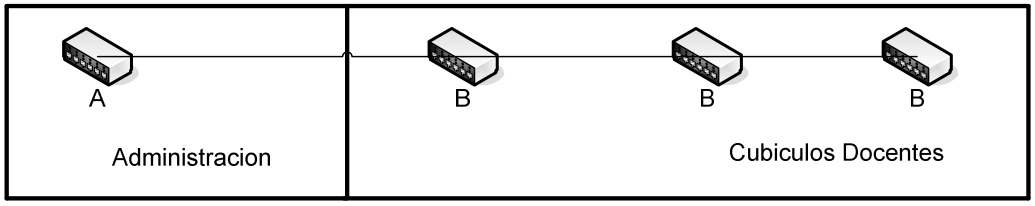



*Figura 2.2.1.5.2. Diagrama de ubicación de los equipos de red del Edificio Administrativo/Química de la Facultad de Ciencias Naturales y Matemáticas*

En el edificio de Biología se encuentran los siguientes equipos de red:

A. 2 Switches C-NET modelo CNSH1600
B. 2 Switches LG modelo LS3116A

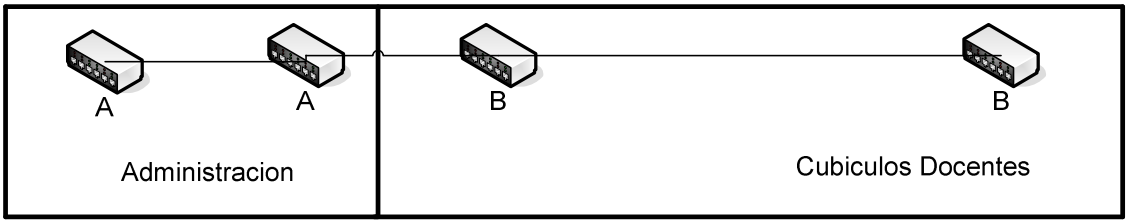



*Figura 2.2.1.5.3 Diagrama de ubicación de los equipos de red del Edificio Biología de la Facultad de Ciencias Naturales y Matemáticas*

Por el momento los edificios de la facultad de Ciencias Naturales y Matemáticas se encuentran conectados por medio de Fibra Óptica y dentro del mismo edificio lo hacen a través de cable UTP. El Auditórium no posee conexión de red.

Además no poseen red inalámbrica.

Contacto: Balmore Ulises Quintanilla Barrera.

## 2.2.1.6FACULTAD DE ECONOMÍA

Edificios con la que cuenta dicha facultad:

- ✓ Académica Central
- ✓ Administrativo
- ✓ Centro de Computo Clases/Proyección Social/ASECE
- ✓ 2 Edificios de Aulas
- ✓ Aulas de la A hasta la I

El edificio de Académica Central es el nodo principal de la red en el se encuentran los siguientes equipos:

A. 1 Switch Allied Telesyn modelo Rapier 24i
B. 1 Switch Allied Telesyn modelo AT-FS724L
C. 1 Switch D-LINK modelo DES-1024D
D. 1 Punto de Acceso D-Link modelo DWL2100AP

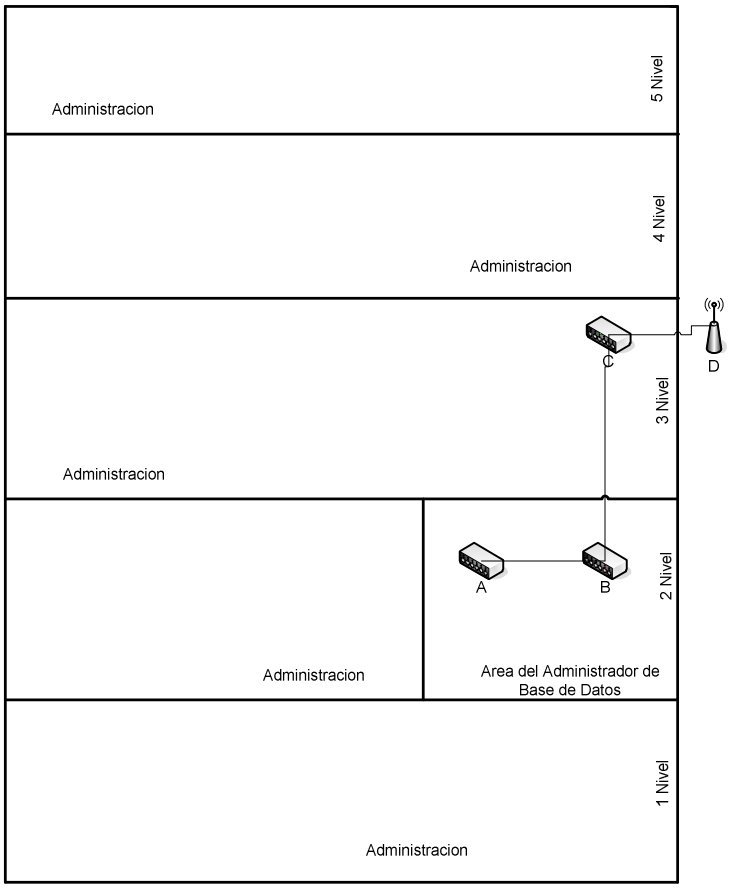



*Figura 2.2.1.6.1 Diagrama de ubicación de los equipos de red del Edificio Académica Central de la Facultad de Economía*

En el edificio de Administrativo se encuentran los siguientes equipos de red:

A. 1 Switch Allied Telesyn modelo AT-FS724L
B. 1 Switch D-LINK modelo DES-1024D
C. 1 Switch D-LINK modelo DES-1016D

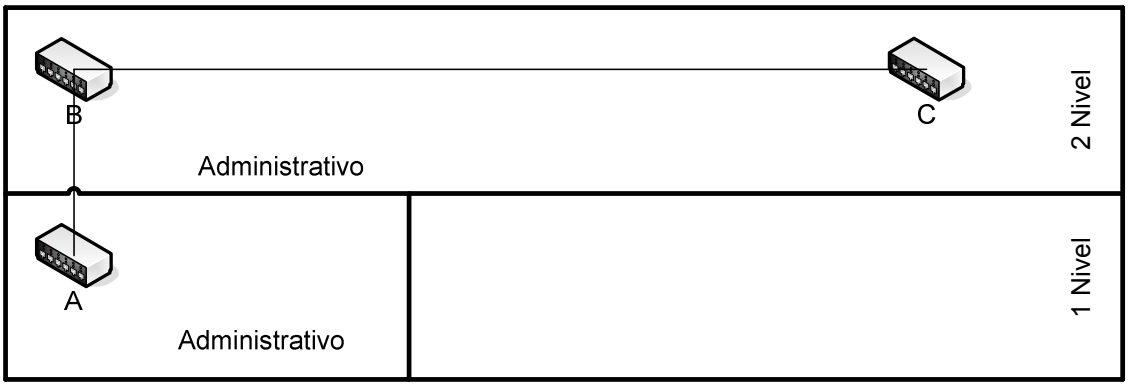



*Figura 2.2.1.6.2 Diagrama de ubicación de los equipos de red del Edificio Administrativo de la Facultad de Economía*

En el edificio de Centro de Computo Clases/Proyección Social/ASECE se encuentran los siguientes equipos de red:

A. 2 Switches D-LINK modelo DES-1024D
B. 1 Punto de Acceso D-Link modelo DWL2100AP

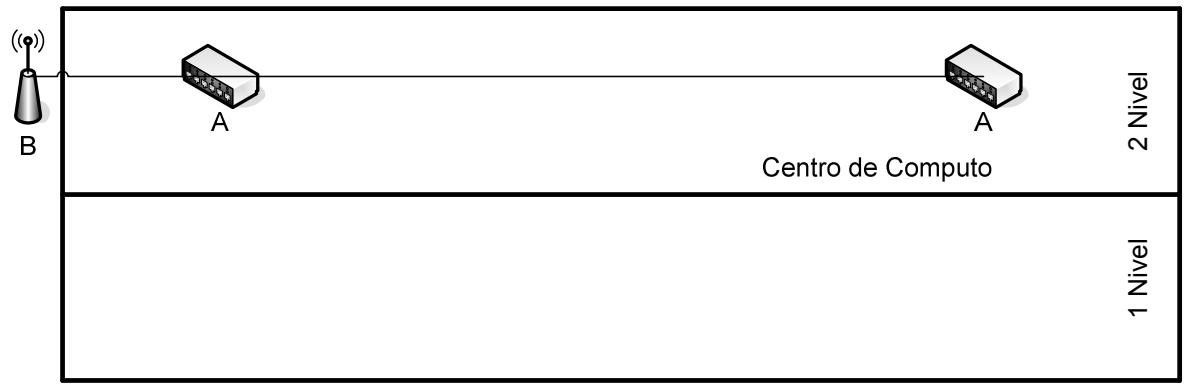



*Figura 2.2.1.6.3 Diagrama de ubicación de los equipos de red del Edificio Centro de Computo Clases/Proyección Social/ASECE de la Facultad de Economía*

Por el momento los edificios de la facultad de Ciencias Económicas se encuentran conectados por medio de Fibra Óptica y dentro del mismo edificio lo hacen a través de cable UTP. Los dos edificios de Aulas y las Aulas de la A - I no poseen conexión de red.

Además si poseen red inalámbrica.

Contacto: Licenciado Medrano.

## 2.2.1.7FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

Edificios con la que cuenta dicha facultad:

- ✓ Académica/Biblioteca/Centro de Computo
- ✓ Relaciones Internacionales
- ✓ Socorro Jurídico

El edificio de Académica/Biblioteca/Centro de Computo es el nodo principal de la red en el se encuentran los siguientes equipos:

A. 1 Switch Allied Telesyn modelo Rapier 24i
B. 2 Switches D-LINK modelo DES-1024D
C. 3 Switches LG modelo LS3116A
D. 1 Switch D-LINK modelo DES-1016D

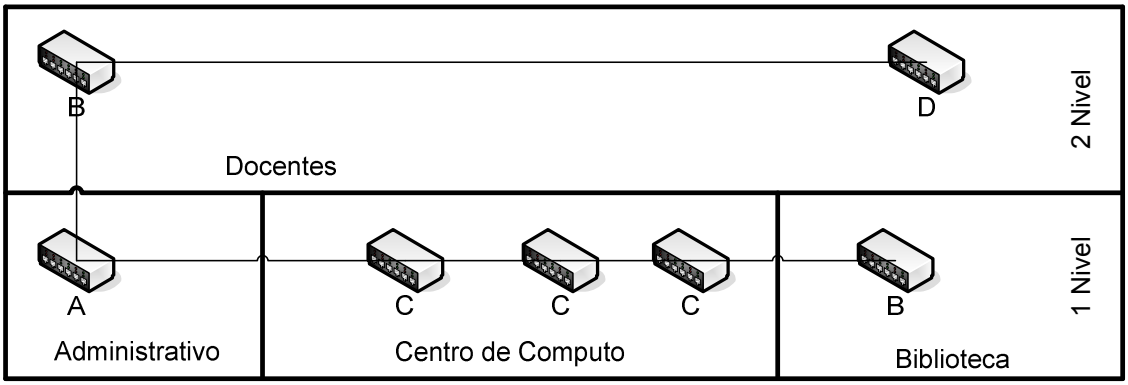



*Figura 2.2.1.7.1 Diagrama de ubicación de los equipos de red del Edificio Académica/Biblioteca/Centro de Computo de la Facultad de Jurisprudencia y Ciencias Sociales*

En el edificio de Relaciones Internacionales se encuentran los siguientes equipos de red:

A. 2 Switches D-LINK modelo DES-1016D

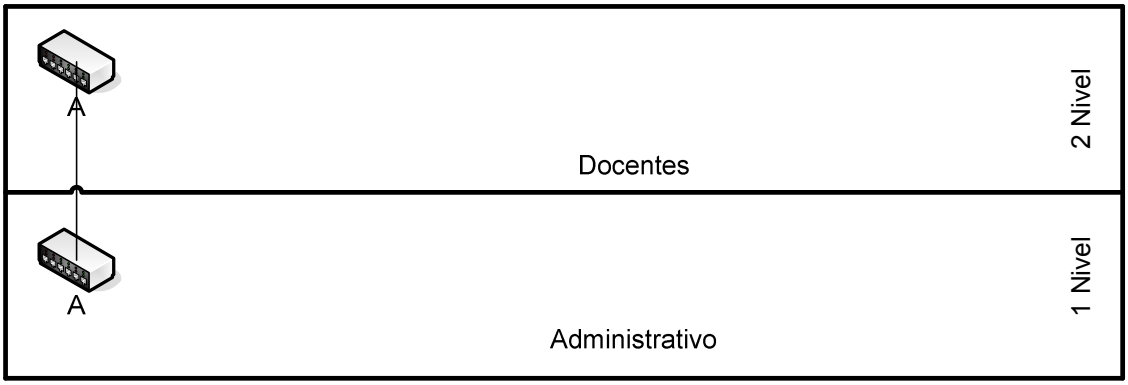



*Figura 2.2.1.7.2 Diagrama de ubicación de los equipos de red del Edificio de Relaciones Internacionales de la Facultad de Jurisprudencia y Ciencias Sociales*

Por el momento los edificios de Socorro Jurídico se encuentran conectados por medio de cable UTP al igual que dentro de los mismos edificios. El Auditórium no posee conexión de red.

Además no poseen red inalámbrica pero están en proceso de instalación del equipo.
Contacto: Mercedes Lara

## 2.2.1.8BIBLIOTECA CENTRAL

El edificio de Biblioteca Central no posee más edificios que la conforman solamente el principal y actualmente es nodo independiente que tiene una conexión hacia Internet pero además posee conexión de datos con toda la red actual de Universidad a través de fibra óptica, en el se encuentran los siguientes equipos de red:

A. 1 MODEM ASMI-52 con el que provee servicio Telecom
B. 1 Router Cisco 1721 series
C. 1 Pix Cisco 525E Firewall
D. 1 Switch Allied Telesyn modelo AT-9816GB
E. 1 Switch Allied Telesyn modelo Rapier 24i
F. 2 Switches Allied Telesyn modelo AT-FH724SW
G. 1 Switch D-LINK modelo DES-1024D.
H. 2 Puntos de Acceso D-Link modelo DWL2100AP

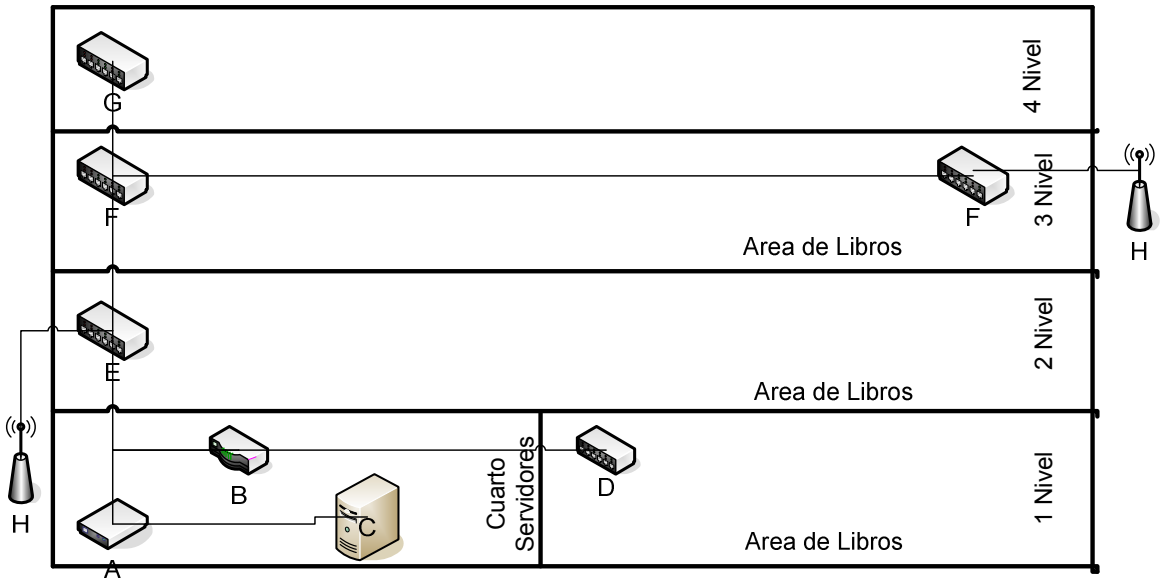



*Figura 2.2.1.8.1 Diagrama de ubicación de los equipos de red del Edificio de la Biblioteca Central*

Poseen red inalámbrica en equipo en el nivel 3 y otro en el nivel 1
Contacto: Néstor López.

## 2.2.1.9 FACULTAD DE MEDICINA

La Facultad de Medicina no posee edificios que la conformen solamente el edificio principal, este posee conexión con toda la red actual de Universidad a través de fibra óptica, las conexiones internas dentro del edificio son a través de cable UTP, en el se encuentran los siguientes equipos de red:

A. 1 Switch Allied Telesyn modelo Rapier 24i
B. 1 Switch DELL Power Conectec 3348
C. 6 Switches D-LINK modelo DES-1024D.

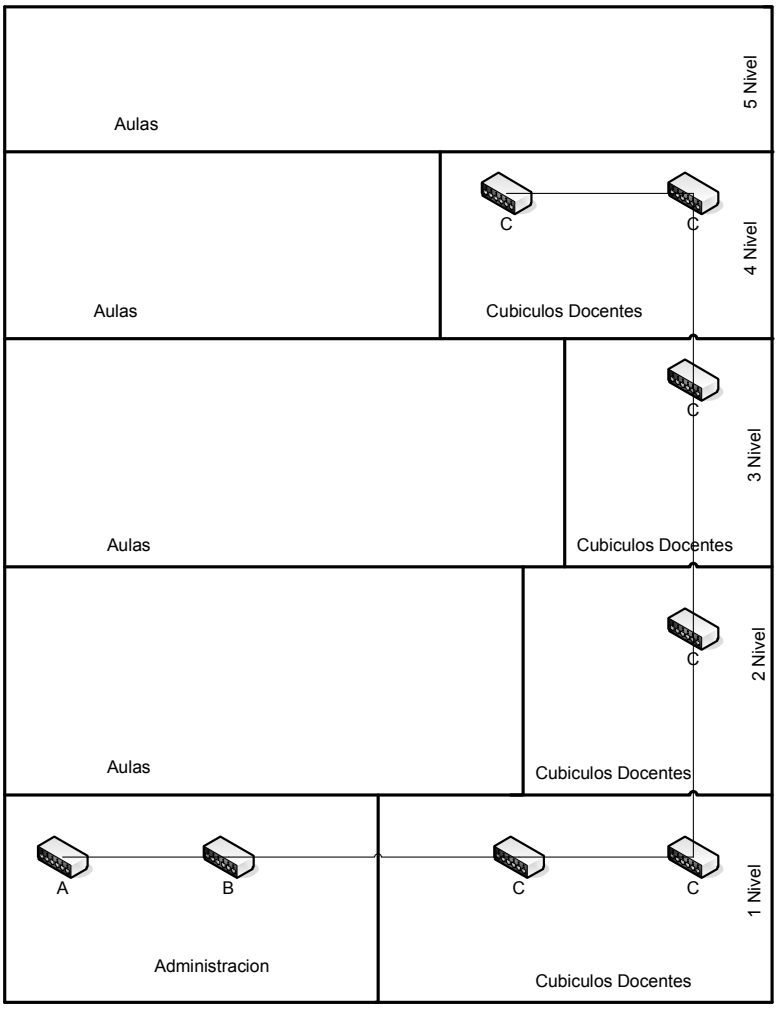



*Figura 2.2.1.9.1 Diagrama de ubicación de los equipos de red del Edificio de Medicina*

Además no poseen red inalámbrica pero están en proceso de instalación del equipo.
Contacto: Doctor Enríquez Ávila.

## 2.2.1.10 FACULTAD DE ODONTOLOGÍA

Edificios con la que cuenta dicha facultad:

- ✓ Administrativo
- ✓ Clínicas
- ✓ Aulas

El edificio Administrativo es el nodo principal de la red en el se encuentran los siguientes equipos:

A. 2 Switches Allied Telesyn modelo Rapier 24i
B. 1 Switch Allied Telesyn modelo AT-FS724i
C. 1 Switch D-LINK DES-1024D
D. 4 Switches Allied Telesyn modelo AT-FS716L
E. 2 Switches Allied Telesyn modelo AT-FS708LE
F. 1 Hub ENCORE modelo ESH-717

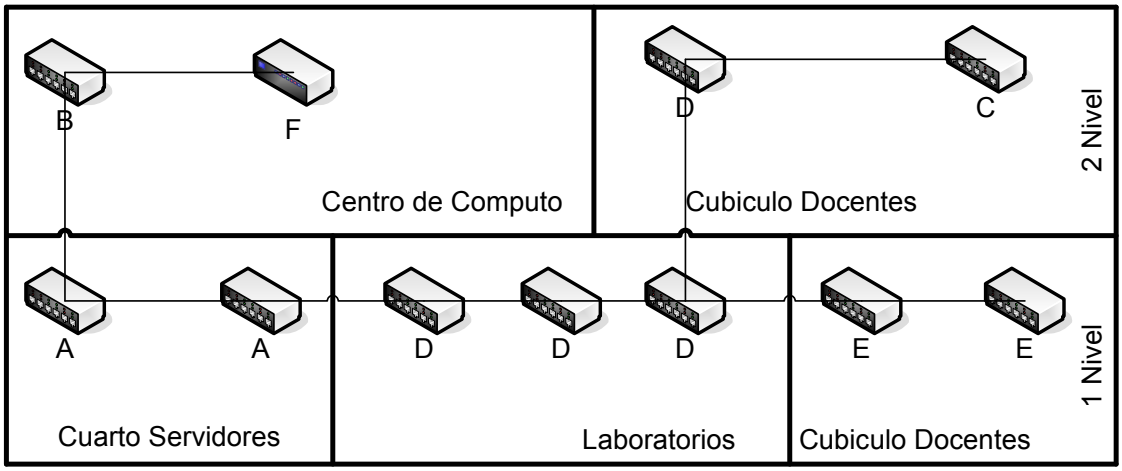



*Figura 2.2.1.10.1 Diagrama de ubicación de los equipos de red del Edificio Administrativo de la Facultad de Odontología*

En el edificio de Clínicas se encuentran los siguientes equipos de red:

A. 1 Switch Allied Telesyn modelo AT-FS724L
B. 1 Switch Allied Telesyn modelo AT-AT8000S48

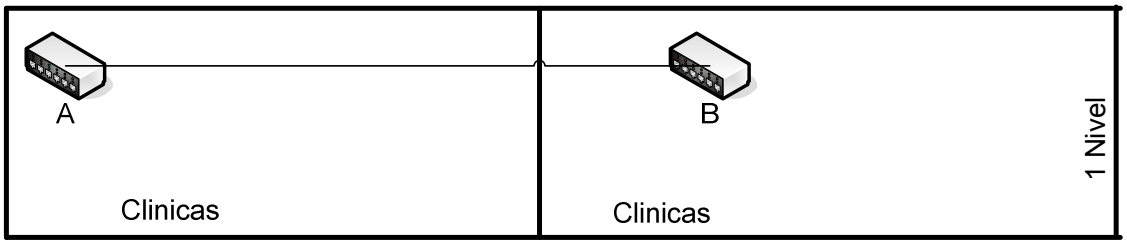



*Figura 2.2.1.10.2 Diagrama de ubicación de los equipos de red del Edificio de Clínicas de la Facultad de Odontología*

Por el momento los edificios de la facultad de Odontología se encuentran conectados por medio de cable UTP y el edificio de Aulas aun no posee conectividad.

Además no poseen red inalámbrica pero están en proceso de instalación del equipo.
Contacto: Douglas Sánchez.

## 2.2.1.11 FACULTAD DE QUÍMICA Y FARMACIA

Edificios con la que cuenta dicha facultad:

- ✓ Administrativo
- ✓ Laboratorios
- ✓ Aulas

El edificio Administrativo es el nodo principal de la red en el se encuentran los siguientes equipos:

A. 1 Switch Allied Telesyn modelo Rapier 24i
B. 3 Switches Allied Telesyn modelo AT-GS924GB
C. 4 Switches D-LINK DES-1008D
D. 2 Switches D-LINK DES-1024D
E. 1 Punto de Acceso Allied Telesyn modelo AT WA1004G
F. 1 Punto de Acceso ENCORE modelo AIR-AP1231G-A-K9

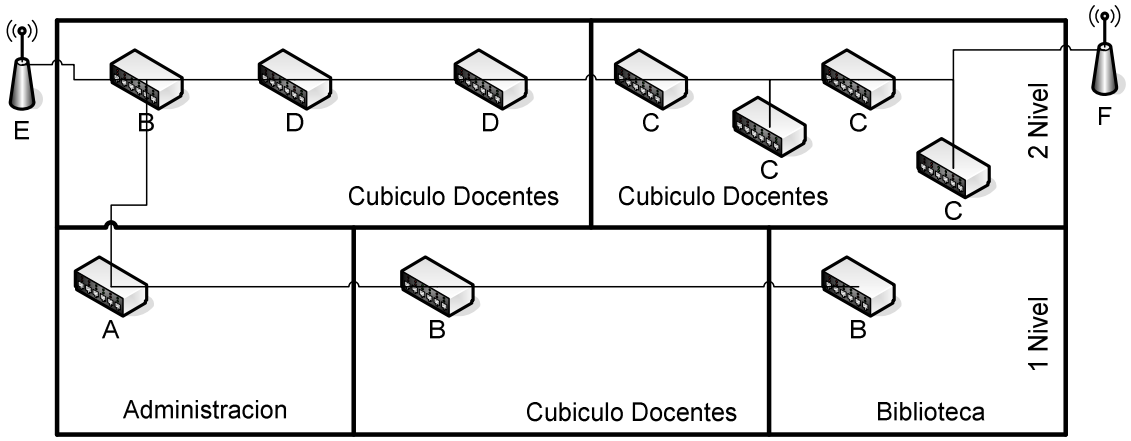



*Figura 2.2.1.11.1 Diagrama de ubicación de los equipos de red del Edificio Administrativo de la Facultad de Química y Farmacia*

En el edificio de Laboratorios se encuentran los siguientes equipos de red:

A. 1 Switches D-LINK DES-1008D


*Figura 2.2.1.11.2 Diagrama de ubicación de los equipos de red del Edificio de Laboratorios de la Facultad de Química y Farmacia*

Por el momento los edificios de la facultad de Odontología se encuentran conectados por medio de cable UTP y el edificio de Aulas aun no posee conectividad.

Poseen red inalámbrica.

Contacto: Bernardo Díaz.

## 2.2.1.12 FACULTAD DE CIENCIAS AGRONÓMICAS

Edificios con la que cuenta dicha facultad:

- ✓ Unidad de Computo.
- ✓ Planificación.
- ✓ Aulas/Postgrado
- ✓ Planta Piloto
- ✓ Profesores.

El edificio de Unidad de Computo es el nodo principal de la red en el se encuentran los siguientes equipos:

A. 1 Switch Allied Telesyn modelo Rapier 24i
B. 2 Switches Allied Telesyn modelo AT-FS724L
C. 1 Switch 3COM modelo 3C16471
D. 1 Hub ENCORE modelo ESH-717

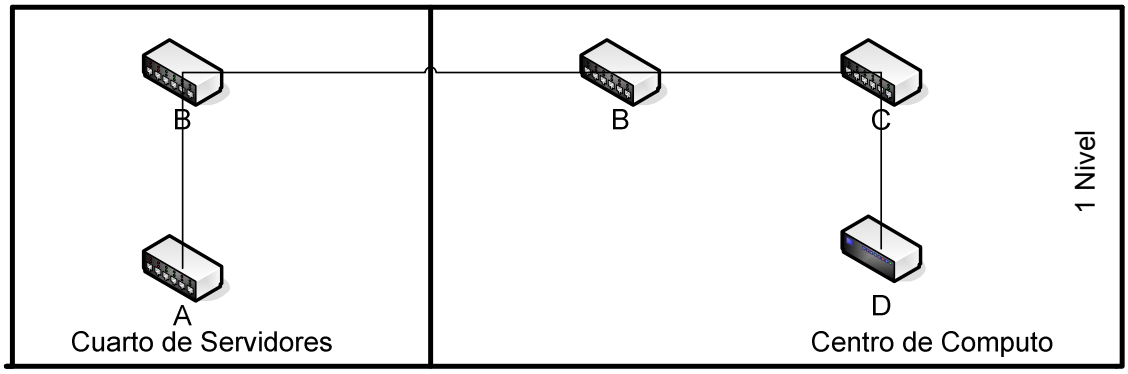



*Figura 2.2.1.12.1 Diagrama de ubicación de los equipos de red del Edificio de Unidad de Computo de la Facultad de Ciencias Agronómicas*

En el edificio de Planificación se encuentran los siguientes equipos de red:

A. 1 Switch C-NET modelo CNSH1600


*Figura 2.2.1.12.2 Diagrama de ubicación de los equipos de red del Edificio de Planificación de la Facultad de Ciencias Agronómicas*

En el edificio de Aulas/Postgrado se encuentran los siguientes equipos de red:

A. 1 Switch Allied Telesyn modelo AT-FS708LE
B. 1 Switches D-LINK DES-1008D

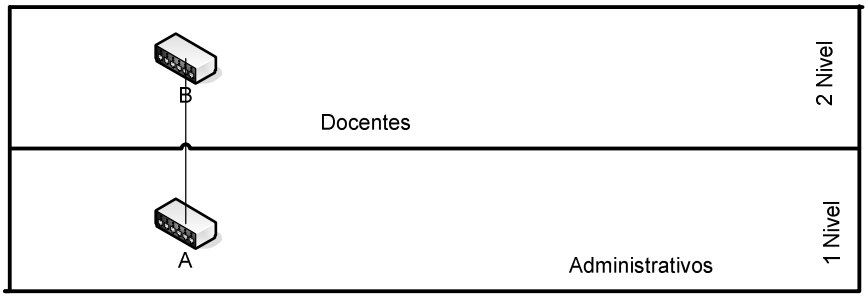



*Figura 2.2.1.12.3 Diagrama de ubicación de los equipos de red del Edificio de Aulas/Postgrado de la Facultad de Ciencias Agronómicas*

En el edificio de Planta Piloto se encuentran los siguientes equipos de red:

A. 1 Switch LG modelo LS3116A


*Figura 2.2.1.12.4 Diagrama de ubicación de los equipos de red del Edificio de Planta Piloto de la Facultad de Ciencias Agronómicas*

En el edificio de Profesores se encuentran los siguientes equipos de red:

A. 2 Switches D-LINK modelo DES-1024D.

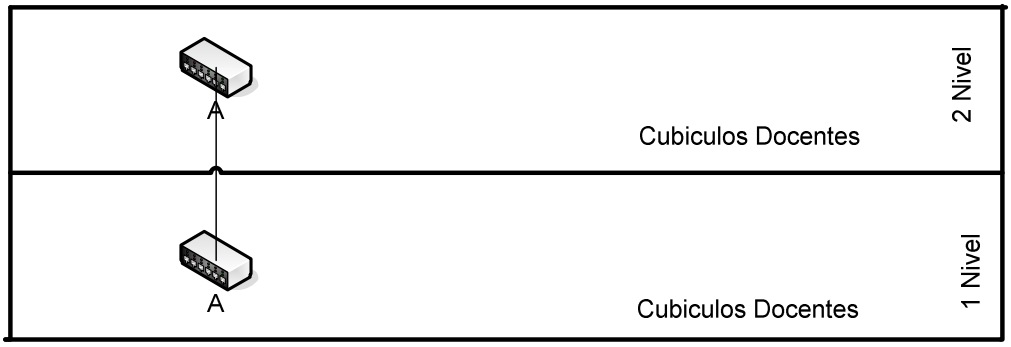



*Figura 2.2.1.12.5 Diagrama de ubicación de los equipos de red del Edificio de Profesores de la Facultad de Ciencias Agronómicas*

Por el momento los edificios de la facultad de Ciencias Agronómicas se encuentran conectados por medio de cable UTP.
Además no poseen red inalámbrica.
Contacto: Orlando Enríquez Pérez.

### 2.2.1.13 FACULTAD DE INGENIERÍA Y ARQUITECTURA

Edificios con la que cuenta dicha facultad:

- ✓ Académica
- ✓ Ingeniería de Sistemas/Ingeniería Industrial
- ✓ Ingeniería Eléctrica
- ✓ Arquitectura (Edificio D)
- ✓ Ingeniería Mecánica
- ✓ Ingeniería Civil
- ✓ Biblioteca
- ✓ Ciencias Básicas
- ✓ Edificio B
- ✓ Edificio C
- ✓ Auditórium (Mármol).

El edificio de Académica de la facultad de ingeniería se encuentran los siguientes equipos:

A. 1 Switch Allied Telesyn modelo Rapier 24i
B. 1 Switch 3Com Switch 4500 modelo 3CR17561-91
C. 1 Switch Allied Telesyn modelo AT-8326GB
D. 1 Switch Allied Telesyn modelo AT-FS724L
E. 1 Switch D-LINK modelo DES-1024D.
F. 1 Puntos de Acceso D-Link modelo DWL2100AP
G. 1 Punto de Acceso 3Com OfficeConnect Wireles 54Mbps 11g.

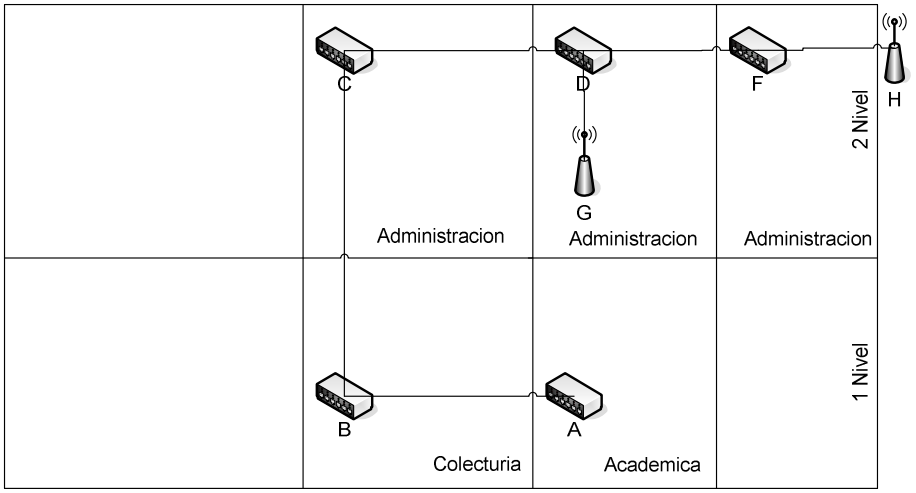



*Figura 2.2.13.1 Diagrama de ubicación de los equipos de red del Edificio de Académica de la Facultad de Ingeniería y Arquitectura*

En el edificio de Ingeniería Eléctrica se encuentran los siguientes equipos de red:

A. 1 Switch Allied Telesyn modelo Rapier 24i
B. 1 Switch 3Com Switch 4500 modelo 3CR17561-91
C. 2 Switches Allied Telesyn modelo AT-FS724L
D. 1 Switch D-LINK modelo DES-1024D.
E. 1 Puntos de Acceso D-Link modelo DWL2100AP
F. 1 Punto de Acceso 3Com OfficeConnect Wireles 54Mbps 11g.

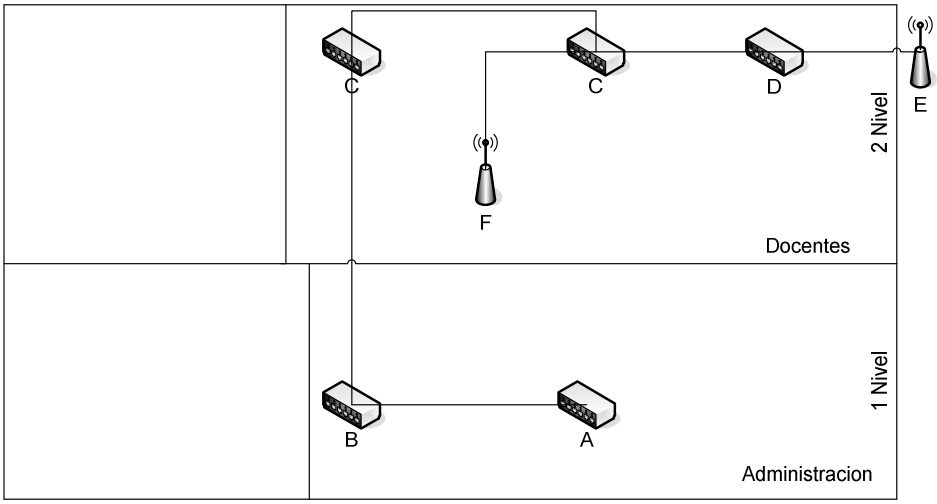



*Figura 2.2.13.2 Diagrama de ubicación de los equipos de red del Edificio de Ingeniería Eléctrica de la Facultad de Ingeniería y Arquitectura*

En el edificio de Ingeniería Civil se encuentran los siguientes equipos de red:

A. 1 Switch Allied Telesyn modelo Rapier 24i
B. 1 Switch 3Com Switch 4500 modelo 3CR17561-91
C. 2 Switches Allied Telesyn modelo AT-FS724L
D. 1 Switch D-LINK modelo DES-1024D.
E. 1 Punto de Acceso 3Com OfficeConnect Wireles 54Mbps 11g.

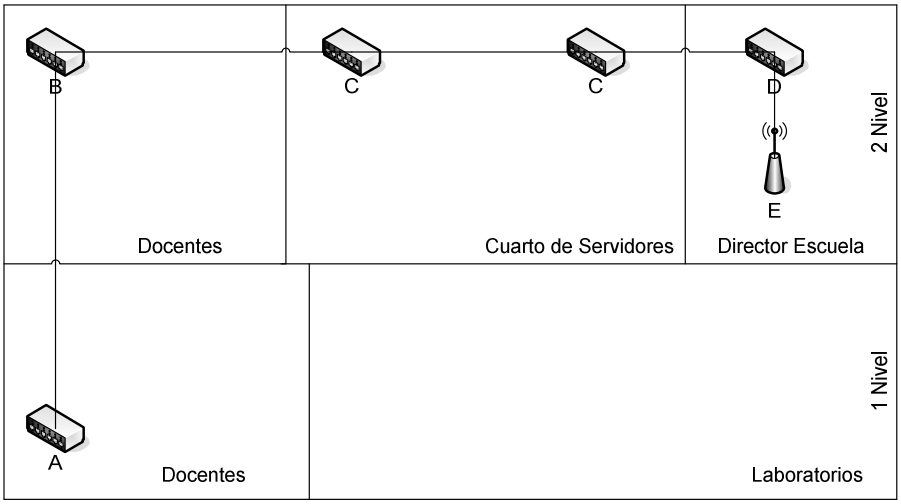



*Figura 2.2.13.3 Diagrama de ubicación de los equipos de red del Edificio de Ingeniería Civil de la Facultad de Ingeniería y Arquitectura*

En el edificio de Biblioteca se encuentran los siguientes equipos de red:

A. 1 Switch Allied Telesyn modelo Rapier 24i
B. 1 Switch 3Com Switch 4500 modelo 3CR17561-91
C. 1 Switch Allied Telesyn modelo AT-FS724L
D. 1 Punto de Acceso 3Com OfficeConnect Wireles 54Mbps 11g.

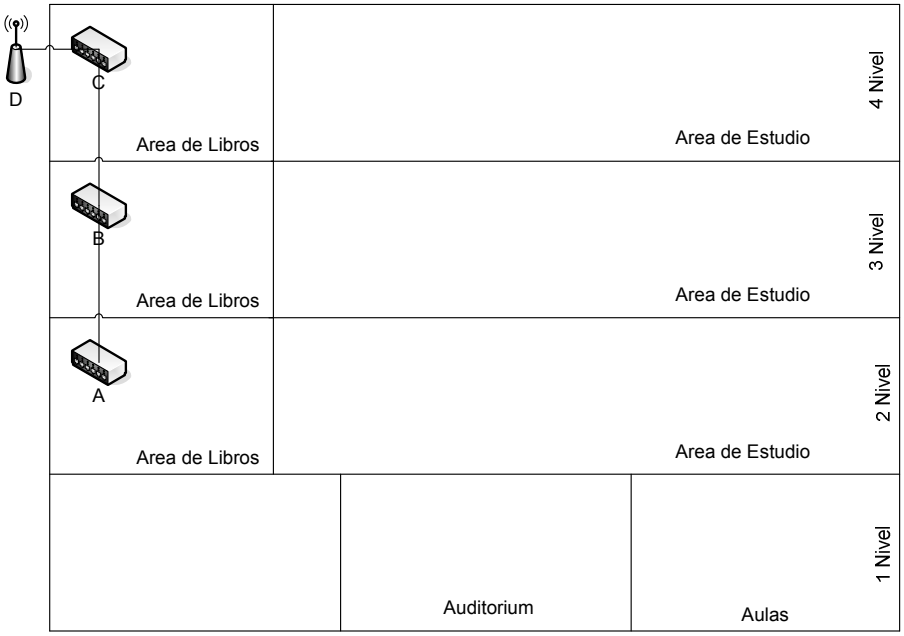



*Figura 2.2.13.4 Diagrama de ubicación de los equipos de red del Edificio de Biblioteca de la Facultad de Ingeniería y Arquitectura*

En el edificio de Ciencias Básicas se encuentran los siguientes equipos de red:

A. 1 Switch Allied Telesyn modelo Rapier 24i
B. 1 Switch 3Com Switch 4500 modelo 3CR17561-91
C. 2 Switches Allied Telesyn modelo AT-FS724L
D. 1 Switch D-LINK modelo DES-1024D.
E. 1 Punto de Acceso 3Com OfficeConnect Wireles 54Mbps 11g.

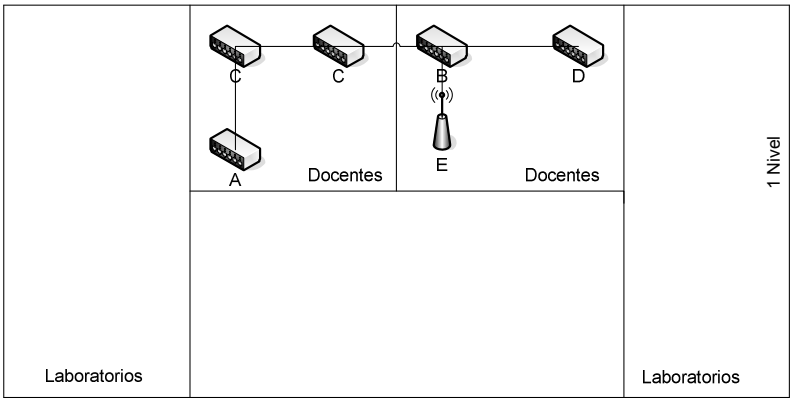



*Figura 2.2.13.5 Diagrama de ubicación de los equipos de red del Edificio de Ciencias Básicas de la Facultad de Ingeniería y Arquitectura*

En el edificio de Ingeniería de Sistemas/Ingeniería Industrial se encuentran los siguientes equipos de red:

A. 1 Switch Allied Telesyn modelo AT-8026T
B. 1 Switch 3Com Switch 4500 modelo 3CR17561-91
C. 3 Switches Allied Telesyn modelo AT-FS724L
D. 1 Puntos de Acceso D-Link modelo DWL2100AP
E. 1 Punto de Acceso 3Com OfficeConnect Wireles 54Mbps 11g.

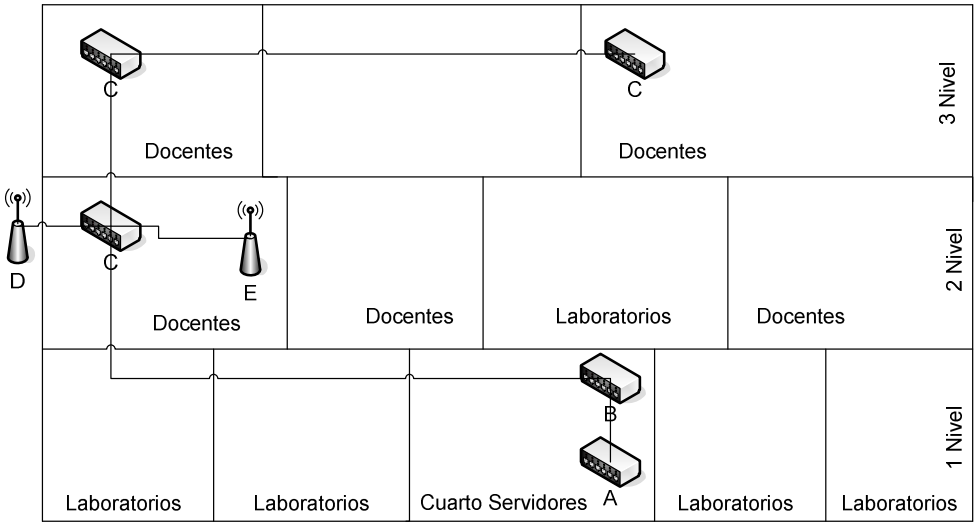



*Figura 2.2.13.6 Diagrama de ubicación de los equipos de red del Edificio de Ingeniería de Sistemas / Ingeniería Industrial de la Facultad de Ingeniería y Arquitectura*

En el edificio de Arquitectura (Edificio D) se encuentran los siguientes equipos de red:

A. 1 Switch Allied Telesyn modelo AT-FS724L
B. 1 Switch 3Com Switch 4500 modelo 3CR17561-91
C. 1 Switches D-LINK modelo DES-1024D.
D. 1 Punto de Acceso 3Com OfficeConnect Wireles 54Mbps 11g.

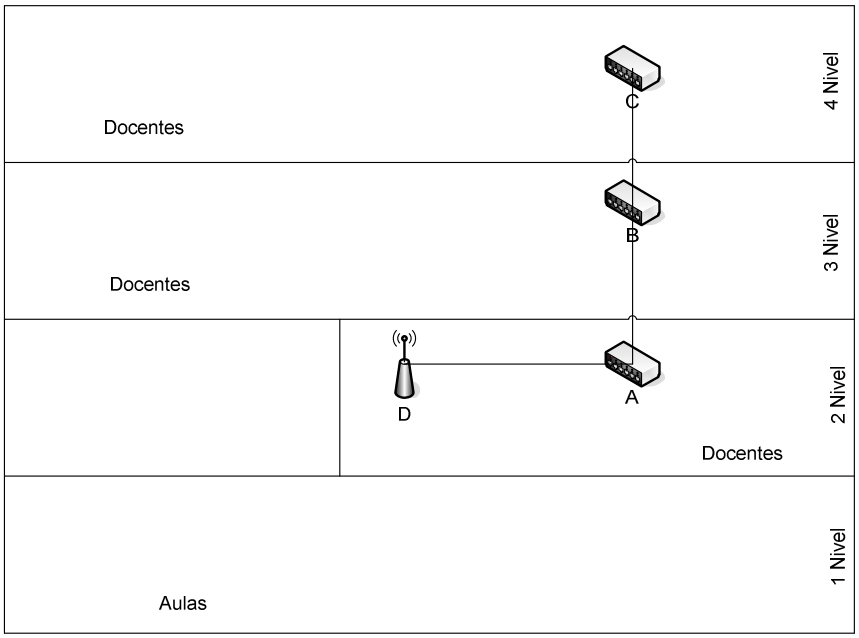



*Figura 2.2.13.7 Diagrama de ubicación de los equipos de red del Edificio de Arquitectura (D) de la Facultad de Ingeniería y Arquitectura*

## *2.2.2 Planos actuales de ubicación de puntos de acceso y radios de cobertura*

En los planos de cobertura del Campus Central, Campus Multidisciplinaria Occidental, Campus Multidisciplinaria Paracentral y Campus Multidisciplinaria Oriental los radios de cobertura de los puntos de acceso que actualmente posee el campus están señalados con círculos rellenos con líneas diagonales discontinuas. Además se ha determinado que debido a los obstáculos en el medio los puntos de acceso brindan una señal óptima en un radio de 50 metros.

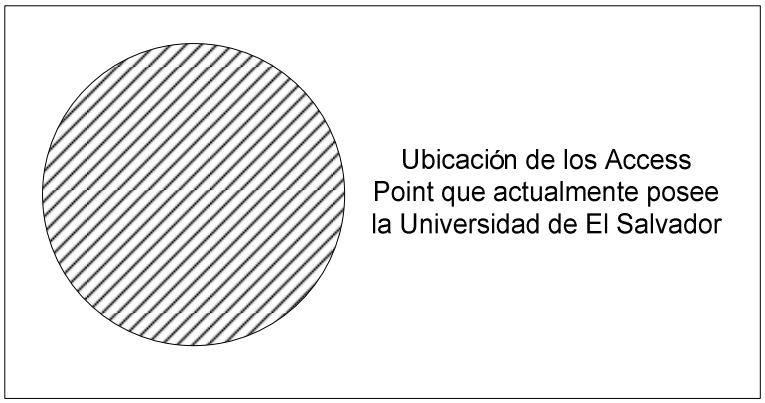



*Figura 2.2.2.1 Radios de cobertura de Access Point*

***Campus Central***

Ver anexo 1

***Multidisciplinaria Occidental***

Ver Anexo 2

***Multidisciplinaria Paracentral***

Ver Anexo 3

***Multidisciplinaria Oriental***

Ver Anexo 4

## *2.2.3 Diagnóstico de la WLAN de la Universidad de El Salvador*

La red inalámbrica de la Universidad de El Salvador posee actualmente un sistema de autenticación de protocolo abierto. Este es el protocolo de autenticación por defecto en el estándar IEEE 802.11, en el cual cualquiera que quiera entrar a la red se puede autenticar sin ningún impedimento. El tráfico va sin cifrar.

Es una forma muy básica de autenticación que consiste de una simple solicitud de autenticación que contiene la ID de la estación y una respuesta de autenticación que contiene el éxito o fracaso. En caso de éxito, se considera que ambas estaciones están mutuamente autentificadas. La seguridad que nos proporciona un Sistema Abierto es por lo tanto nula, por lo que cualquier estación de trabajo con el equipo necesario puede entrar en la red sin ningún problema.

Con este sistema de seguridad se corre el riesgo de que un intruso use la red inalámbrica para acceder de forma gratuita a Internet. Mientras esto parece en apariencia inocuo, y los activos de información no se ven afectados, es una actividad que supone un uso no aceptado de recursos de la organización por personal no autorizado. Además afecta a la calidad y disponibilidad del servicio de red de los usuarios legítimos, y puede suponer un problema legal para la organización si el intruso utiliza el acceso a Internet de la empresa para realizar acciones ilegales (*hacking*) o acceso a contenido de Internet inapropiado.

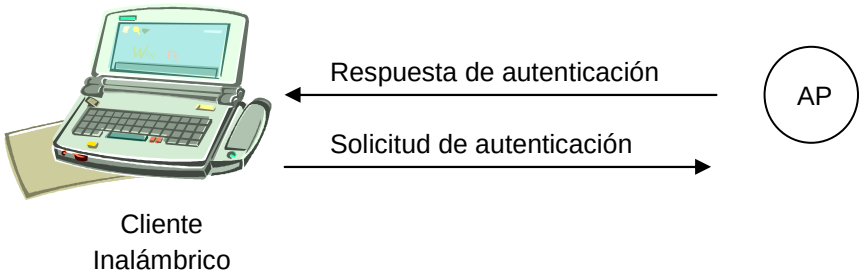



*Figura 2.2.3.1 Sistema de autenticación abierta*

La infraestructura de la seguridad que posee actualmente la red inalámbrica de la UES no cumple con los requisitos de seguridad que exige a sus miembros el proyecto Eduroam. A continuación se detallan los requerimientos necesarios para implementar una solución a este problema de seguridad y así poder lograr con éxito la integración de la Universidad de El Salvador al programa mundial Eduroam.

# *2.3 DETERMINACIÓN DE LOS REQUERIMIENTOS*

El proyecto mundial Eduroam, permite a los usuarios de las instituciones participantes obtener un acceso seguro a la red, principalmente por medios inalámbricos, utilizando la credencial de la institución origen. El requisito que las instituciones que desean unirse a Eduroam deben cumplir es: La implementación de un sistema de control de acceso centralizado con una infraestructura RADIUS basado en el estándar 802.1X. Para implementar la autenticación se configuran equipos de red como switches en los que se conectan puntos de acceso capaces de soportar IEEE 802.11 de forma que utilicen el estándar IEEE 802.1X y con la capacidad de enviar peticiones a servidores RADIUS apoyándose en una infraestructura LDAP para identificar, autenticar y autorizar a los usuarios y dispositivos mediante políticas de acceso centralizadas.

Para integrar a la Universidad de El Salvador al programa mundial Eduroam existen políticas establecidas por el proyecto Eduroam y se describen a continuación en tres grandes grupos: requerimientos técnicos, requerimientos económicos y requerimientos operativos.

## *2.3.1 Requerimientos técnicos*

Se consideran requerimientos técnicos a aquellos elementos tanto hardware como software que en conjunto hacen posible el funcionamiento y gestión del programa.

### 2.3.1.1Servidor de Autorización/Autenticación (RADIUS)

Es un protocolo que permite la autenticación, autorización y contabilización del uso, además está compuesto por un servidor propiamente dicho, un conjunto de normas de transmisión o protocolo y un cliente. Las principales características que éste componente debe tener son:

1. Compatibilidad con 802.1X
2. Soporte de diversos tipos de autenticación EAP (TLS, TTLS, PEAP)
3. Capacidad de registro (Auditoria)
4. Soporte para el control de acceso en redes inalámbricas
5. Flexibilidad para validar a los suplicantes mediante varios métodos (Base de datos de usuarios local, directorio de usuarios LDAP, certificados, entre otros).

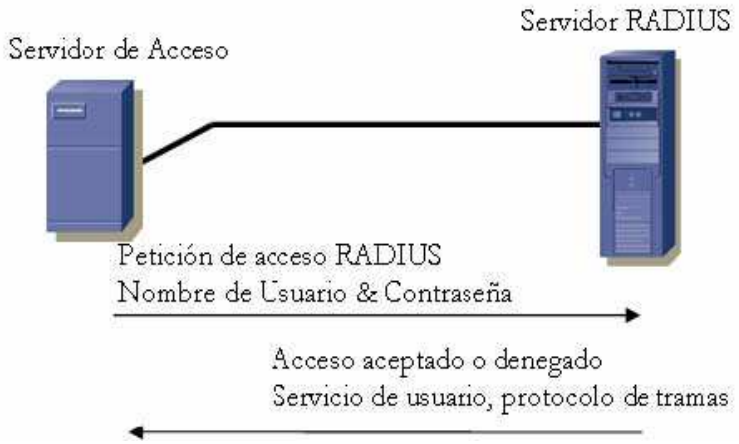



*Figura 2.3.1.1.1 Ejemplo de un servidor RADIUS*

**Características del Equipo (Hardware)**

Procesador

Mínimo: 350 Mhz velocidad del reloj

Pentium IV a 300 Mhz o superior

Memoria RAM

mínima de 128 MB

Capacidad de almacenamiento

Para la instalación se necesitan al menos 500 MB de espacio libre en la unidad C.

**Características de los programas (Software)**

*FreeRADIUS*[12]*:* el cual es un servidor RADIUS de código abierto, que además es considerado como uno de los 5 mejores del mundo y esta correctamente instalado y funcionando en la Universidad de El Salvador.[13]

*Servidor de Acceso Directo a Directorio (LDAP):*Funciona en conjunto con el servidor RADIUS. Consiste en una combinación de hardware y software que permite el acceso remoto a herramientas o información que generalmente residen en una red de dispositivos. Normalmente, almacena credenciales (usuarios y contraseñas) y es utilizado para autenticarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc.).

[12] http://freeradius.org/

[13] http://wiki.freeradius.org/FreeRADIUS

1. Almacena de forma centralizada las cuentas de usuarios con sus características y credenciales (certificados digitales, etc.)
2. Almacena políticas de control de acceso de forma centralizada.

Actualmente la Universidad de El Salvador utilizará el servidor de acceso ligero a directorios LDAP que actualmente administra el Departamento de Educación a Distancia el cual identifica de manera única a cada miembro de la universidad, a esta identificación se le denomina "credencial" la cuál consta de un nombre de usuario y una contraseña.

## 2.3.1.2Suplicante

El suplicante, o equipo del cliente, es uno de los tres participantes involucrados en la definición del protocolo 802.1X; es el que desea conectarse con la red.

Los otros participantes son el servidor de autorización/autenticación, que contiene toda la información necesaria para saber cuáles equipos y/o usuario está autorizado para acceder a la red y el autenticador, que es el equipo de red (switch, enrutador, servidor de acceso remoto) que recibe la conexión del suplicante.

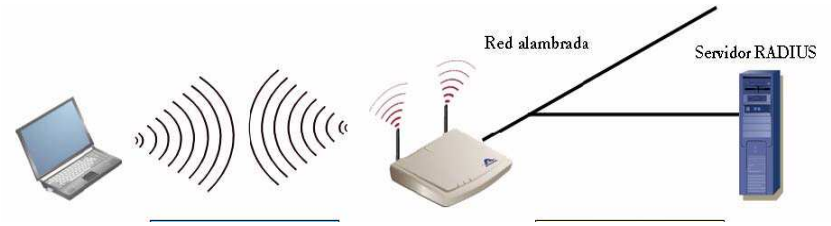



*Figura 2.3.1.2.1 Ejemplo de un suplicante*

**Características del Equipo (Hardware)**

El ordenador de los usuarios debe estar equipado con una tarjeta de red inalámbrica en cualquiera de sus presentaciones: USB, PCI, PCMCIA. La tarjeta de red inalámbrica debe ser compatible con:

1. Estándar 802.11b/g ó 802.11n
2. Protocolo WEP como mínimo

***Características de los programas (Software)***

La autenticación de los usuarios a la red Eduroam desde cualquier plataforma se realiza por medio del software gratuito SecureW2. SecureW2 es el programa que se encargará de validar el usuario y contraseña de los usuarios en la red inalámbrica.

## 2.3.1.3Puntos de Acceso

Es un aparato que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Estos proporcionan una interfaz entre el sistema de operación de red del cliente o suplicante los mismos servicios que un switch cableado. La diferencia entre ellos es el medio (aire o cable).

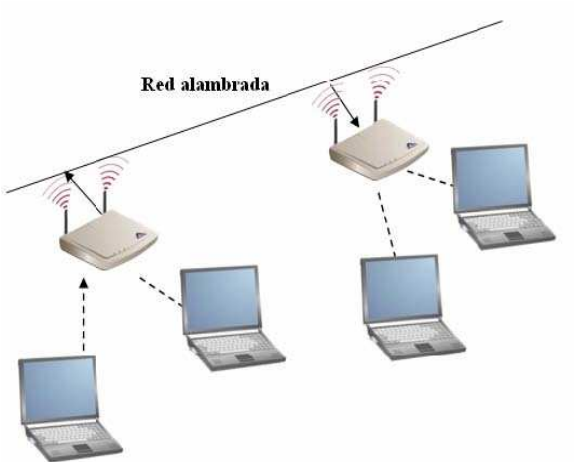



*Figura 2.3.1.3.1 Ejemplo de un punto de acceso*

**Características del Equipo (Hardware)**

1. Compatibilidad con 802.11 y soporte de cifrado (WEP al menos)
2. Capacidad de implementar el servicio de control de acceso 802.1X

## 2.3.1.4 Switches

Llamado también "conmutador", es un dispositivo electrónico de interconexión de redes de datos, transmite datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas (fragmento de paquete) en la red.

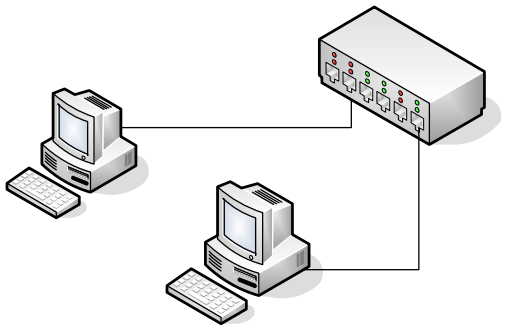


*Figura 2.3.1.4.1 Ejemplo de un switch*

**Características del Equipo (Hardware)**

1. Compatibilidad con 802.1X
2. Soporte de diversos tipos de autenticación EAP (TLS, TTLS, PEAP)

## *2.3.2 Requerimientos Económicos*

A continuación se presenta el procedimiento para adquisición de equipos a través de la UACI, estos procedimientos dependen de los montos de los equipos que se desean adquirir.

Las compras de productos o servicios que realiza la Universidad de El Salvador se rigen según la "Ley De Adquisiciones Y Contrataciones De La Administración Pública"[14]. En el artículo 39 de de dicha ley en la actualidad existen 5 formas de contratar productos o servicios

a) Licitación o concurso público
b) Licitación o concurso público por invitación
c) Libre Gestión
d) Contratación Directa
e) Mercado Bursátil

La Libre Gestión son compras por un monto inferior al equivalente a ochenta (80) salarios mínimos urbanos, realizando comparación de calidad y precios, el cual debe contener como mínimo tres ofertantes. No será necesario este requisito cuando la adquisición o contratación no exceda del equivalente a diez (10) salarios mínimos urbanos; y cuando se tratare de ofertante único o marcas específicas, en que bastará un solo ofertante, para lo cual se debe emitir una resolución razonada.

Los salarios mínimos vigentes según el Ministerio de Trabajo y Previsión Social[15] para trabajadores de comercio e industria es $5.81 diario, es decir $174.30 mensual.

Lo anterior establece que para compras menores $13,944 se deben pedir 3 cotizaciones y si es menor a $1,743 no se necesita este requisito, pero en ninguno de los casos es necesario iniciar un proceso de licitación para compras menores a éstos montos. La adquisición queda a discreción del Jefe de la Unidad de Adquisiciones y Contrataciones Institucional y a las limitantes de los presupuestos de cada facultad.

Debido al análisis realizado del hardware que poseen las distintas facultades de la Universidad de El Salvador realizado entre los meses de Marzo y Abril del año 2007, se pudo observar que la mayoría de las facultades ya posee o están en vías de instalación de la red inalámbrica, dando también como resultado que son 4 facultades que no poseen una red inalámbrica es por esto que se presenta la siguiente cotización de los equipos necesarios para tener una red inalámbrica.

Ver anexo 10 "Cotización y adquisición de equipo de red"

[14] http://www.igd.gob.sv/LeyesNormas/leyes/LAdquContr.pdf

[15] http://www.mtps.gob.sv/default.asp?id=21&mnu=21

### *2.3.3 Requerimientos Operativos*

Para que el programa Eduroam sea funcional y que los usuarios al llegar a nuestra institución o instrucciones miembros dispusieran, de la manera más transparentemente posible, de un entorno de trabajo virtual con conexión a Internet, acceso a servicios y recursos de su organización origen, así como acceso a servicios y recursos que nuestra institución o instituciones miembro que en ese momento los acogen, deben de seguir los siguientes lineamientos:

1. Las instituciones participantes deben responsabilizarse de formar a sus usuarios en el respeto a las políticas de uso de las instituciones visitadas, y ayudar en cualquier aspecto relacionado con sus usuarios.
2. Las instituciones participantes deben poseer un servidor de autenticación (AS) que en nuestro caso será el LDAP en conjunto con RADIUS para que pueda, de un modo seguro, procesar y transmitir las credenciales de usuario solicitadas, utilizando para ello paquetes Access-Accept de RADIUS, en conformidad con la sección *3.16 de la RFC3580*[16]*.*
3. Las instituciones participantes deberán disponer de mecanismos para informar a los usuarios visitantes en qué medida y cómo ofertan sus servicios de movilidad. Estos mecanismos consisten dar a conocer las instrucciones o pasos a seguir para la configuración de los sistemas operativos y programas adicionales a instalar como SecureW2 para los usuarios de la Universidad de El Salvador , tanto dentro de ella como fuera, donde estarán disponibles los sistemas operativos: Windows Vista, Windows XP, GNU/Linux, Mac OS X, Pocket PC. Toda esta información será mostrada en la página Web de la Universidad de El Salvador relacionada con el proyecto Eduroam.
4. Es obligatorio el uso del SSID "Eduroam" excepto en aquellos casos en los que exista un solapamiento de puntos de acceso de distintas instituciones físicamente muy cercanas. Para aquellos puntos de acceso en los que se de este solapamiento se recomienda el uso de SSIDs de la forma "Eduroam-[INST]", donde [INST] son una sigla descriptiva de la institución a la que pertenece cada uno de los puntos de acceso en cuestión.
5. Las instituciones participantes deberán disponer de mecanismos para informar a sus usuarios visitantes de los niveles de seguridad ofrecidos en la transmisión de credenciales. Estos mecanismos consisten en que aquellos usuarios que provengan de otras instituciones y que quieran conectarse en la Universidad de El Salvador a Internet mediante Eduroam deben seguir las instrucciones dadas por su institución de origen. Sólo han de tener en cuenta que aquí el nombre de la red será *Eduroam* y que el cifrado de datos se realiza usando

[16] http://www.ietf.org/rfc/rfc3580.txt

*WPA+TKIP*[17]. Toda esta información será mostrada en la página Web de la Universidad de El Salvador relacionada con el proyecto Eduroam.

6. Las instituciones participantes deben informar a sus usuarios del servicio de movilidad, señalando que el soporte técnico recae sobre su organización origen. Sólo cuando la organización origen determina que el problema es responsabilidad de la organización visitada, éste debe ser revisado con la organización visitada.
7. Las instituciones participantes deben guardar información relativa a sesiones de autenticación y acceso a la red. Asimismo deben ser capaces de realizar un seguimiento de un usuario por razones de seguridad o gestión de capacidad. En concreto, deberán mantener la correlación de direcciones MAC[18] y direcciones IP dadas a los visitantes mediante DHCP, junto con la hora, establecida a partir de una fuente fiable de tiempo, en la que se produjo la asignación. Las instituciones participantes deben comunicar problemas de seguridad o uso fraudulento tanto a los responsables de la iniciativa Eduroam, como a los responsables de seguridad de RedIRIS (IRIS-CERT), para solucionarlo de manera coordinada.
8. Las instituciones participantes deben disponer de mecanismos de monitorización y seguimiento que permitan conocer el estado de los servidores de autenticación, para poder analizar problemas de conexión. Para esto se utilizará el protocolo de dirección de red simple (SNMP[19]). este actúa en la Capa 7 del modelo OSI y es usado por sistemas de dirección de red para supervisar dispositivos conectados por red para las condiciones que garantizan la atención administrativa. Para que funcione se agrega una comunidad a dicho protocolo y luego se grafica a través de **STG** (SNMPTrafficGrapher), el cual es una herramienta libre.
9. De acuerdo con la política establecida para el servicio a nivel europeo, sólo podrá usarse el SSID "Eduroam" para mecanismos de control de acceso basados en el estándar IEEE 802.1X. Aquellas instituciones que usen otros métodos (notablemente, los basados en redirecciones HTTP[20]) cuentan para su adaptación con una moratoria que expira el 30 de septiembre de 2007. Ya que los métodos basados en redirecciones http es demasiado vulnerable.

[17] TKIP (***T****emporal* ***K****ey* ***I****ntegrity* ***P****rotoco), http://es.wikipedia.org/wiki/TKIP*

[18] MAC (Medium Access Control address), http://es.wikipedia.org/wiki/Direcci%C3%B3n_MAC

[19] SNMP (Simple Network Management Protocol), http://es.wikipedia.org/wiki/Simple_Network_Management_Protocol

[20] HTTP (*HyperText Transfer Protocol), http://es.wikipedia.org/wiki/HTTP*

# 3 DISEÑO DE LA WLAN DE LA UNIVERSIDAD DE EL SALVADOR PARA LA CONECTIVIDAD A EDUROAM

En este capítulo se proporciona una descripción de los elementos básicos necesarios, así como sus funciones específicas dentro de la red Eduroam. Además se presenta el diseño propuesto para mejorar la cobertura actual de la red inalámbrica de la Universidad de El Salvador.

## 3.1 COMPONENTES DEL SISTEMA DE AUTENTICACIÓN

Como se mencionó anteriormente, los componentes básicos de una implementación 802.1X son: el suplicante, el autenticador y el servidor de autenticación. Para ilustrar lo anterior a continuación se presenta un escenario donde se integra la autenticación del esquema 802.1X con la base de datos de usuarios, la cual se encuentra en un controlador tipo LDAP. Adicionalmente se presenta una segmentación en zonas de seguridad establecida por un firewall el cual únicamente habilita el tráfico permitido entre las diferentes zonas.

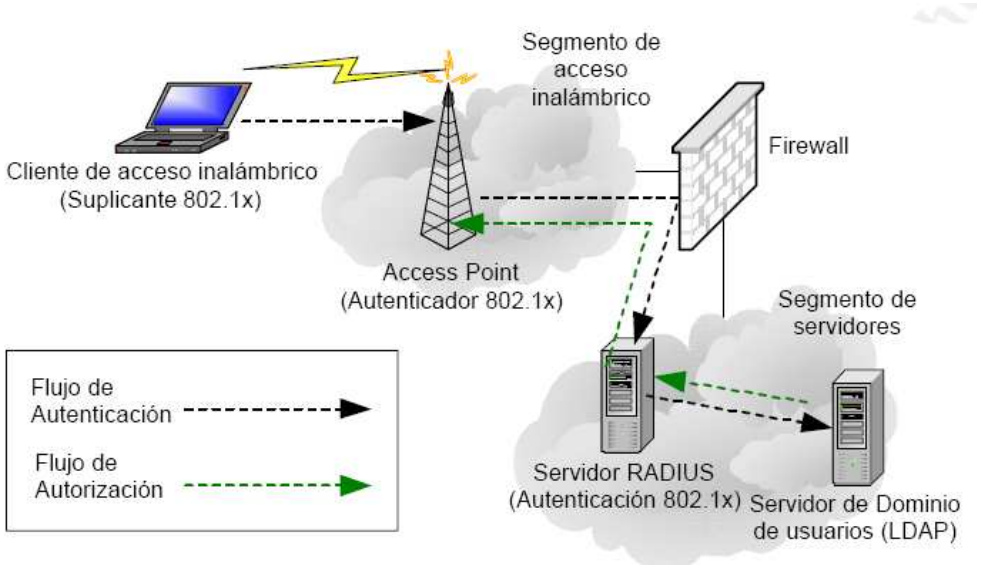



*Figura 3.1.1 Escenario de implementación de 802.1X en una Infraestructura de acceso inalámbrico.*

Es importante considerar en el diseño todos los elementos que se involucrarán con el esquema a implementar, para así considerar los requerimientos en cada uno de ellos y terminar de definir adecuadamente el plan de implementación.

## 3.2 MECANISMO DE AUTENTICACIÓN

Los usuarios deberán autenticarse para tener acceso a la red inalámbrica Eduroam. Para esta autenticación se utilizará el usuario y contraseña asignados, que serán validados por medio de un servidor RADIUS que utilizará el servicio de directorio LDAP de la Universidad de El Salvador.

Se utilizará el protocolo *WPA (Wireless Protected Access)* para cifrar todos los datos que viajan por la red inalámbrica. *WPA* mejora la forma de codificar los datos respecto a sistemas anteriores, utilizando *TKIP ("Temporal Key Integrity Protocol*") al mismo tiempo proporcionará la autenticación de usuarios mediante *802.1X* y *EAP*. Este es, actualmente, el método más seguro de acceso a una red inalámbrica y, además, *WPA* será compatible con las especificaciones de seguridad *802.11i*.

En la siguiente figura se muestran los protocolos que se utilizan en el proceso de autenticación entre los distintos elementos.

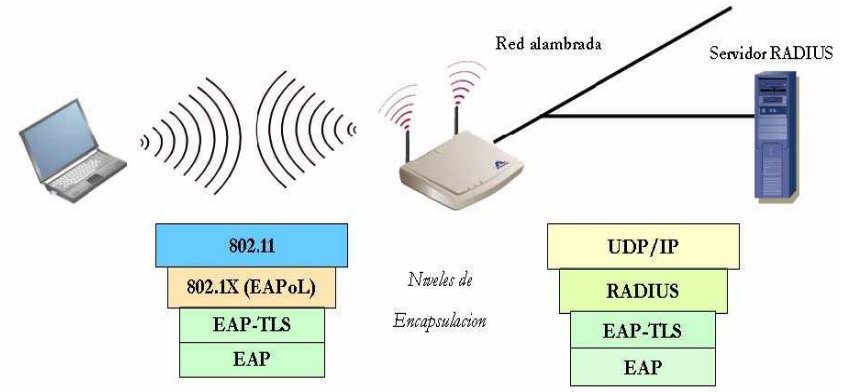



*Figura 3.2.1 Protocolos del proceso de autenticación*

En el proceso de autenticación se establece una sesión entre el servidor de acceso (AS) y la estación de trabajo (STA). En cada sesión que se establece se genera una llave compartida nueva, además de que la autenticación mutua está comprendida solamente entre el AS y la STA.

El proceso inicia con una petición de identidad por parte del AP. La STA responde la petición que es tomada por el AP, el cual la transfiere mediante RADIUS al servidor de autenticación AS. Si el AS valida la identidad de la STA ambos generan la PMK (Pairwise Master Key) y la autenticación es exitosa.

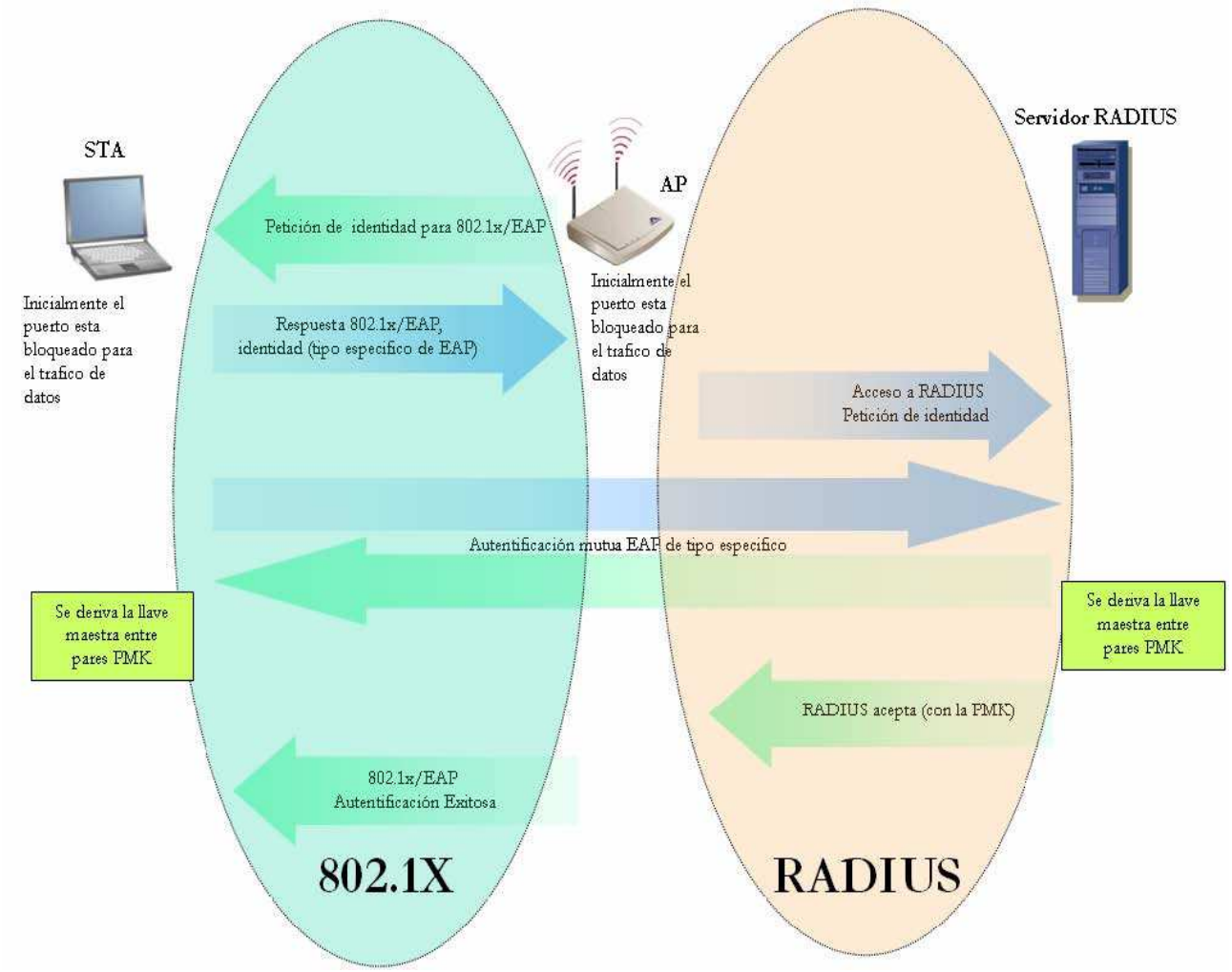



*Figura 3.2.2 Proceso de Autenticación*

## 3.3 SISTEMA DE AUTENTICACIÓN CON OTRAS INSTITUCIONES MIEMBROS DE EDUROAM

En la figura 2.4 se muestra la estructura general del proyecto mundial Eduroam. En el escenario interactúan las instituciones A y B, ambas integradas a Eduroam con sus respectivas redes inalámbricas.

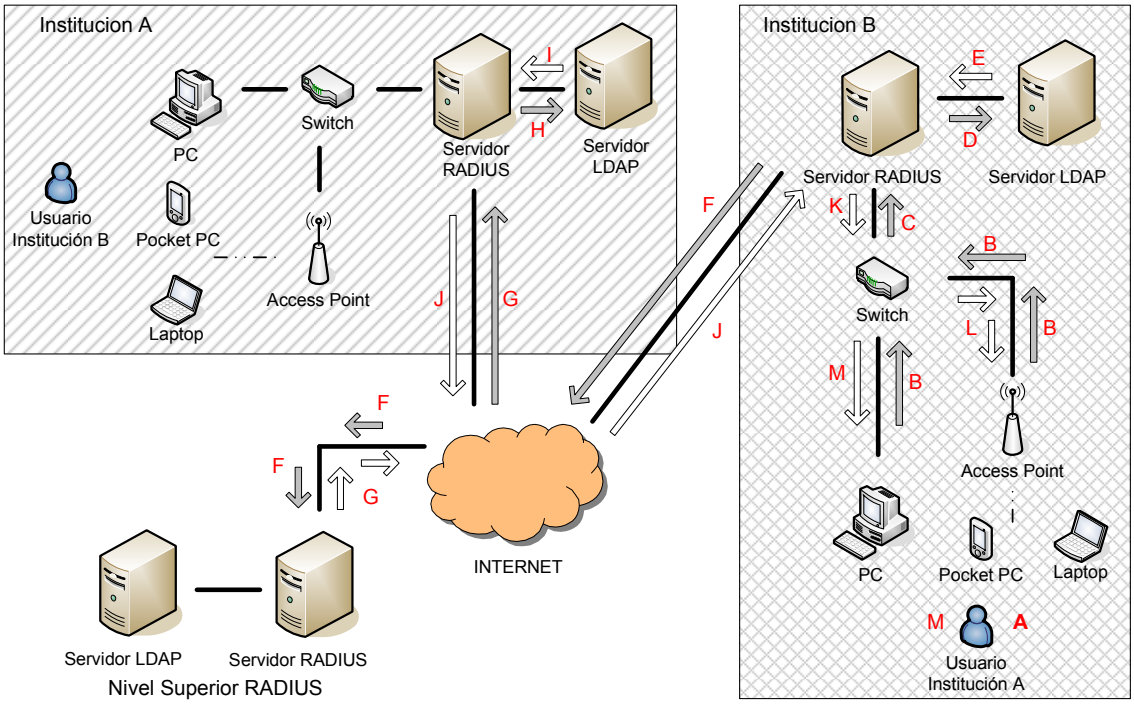



*Figura 3.3.1 Estructura General del Proyecto Mundial Eduroam*

A continuación se detalla el proceso de autenticación entre instituciones:

A. El usuario de la institución A llega de visita a la institución B, él puede conectarse de tres maneras por la PC, Laptop o una Pocket PC (Palm), para cualquiera de las tres formas de conectarse es el mismo funcionamiento. Una vez detectada la red el cliente pregunta al usuario su password y su usuario, ya ingresado el usuario y el password entra en funcionamiento la seguridad en el proyecto.

B. La petición de ingreso (usuario y password) viaja a través del punto de acceso y llega al switch.

C. El switch envía la petición de ingreso al servidor RADIUS.

D. El servidor RADIUS envía la petición al servidor LDAP, es aquí donde está la base de datos de los usuarios tanto su usuario como el password de la institución B, es aquí donde busca si

la petición enviada por el usuario de la Institución A (Usuario y Password) se encuentra en su base de datos.

E. Al no encontrar a ese usuario el servidor LDAP envía un mensaje al servidor RADIUS diciendo que no ese usuario de la institución A no pertenece a la Institución B
F. El Servidor RADIUS al recibir el mensaje del servidor LDAP envía un mensaje vía Internet al servidor RADIUS de nivel superior con el usuario y password
G. Al recibir el servidor RADIUS de nivel superior el mensaje de petición del usuario institución A este redirecciona la petición al servidor RADIUS de la institución A
H. Este recibe la petición del Usuario institución A y la envía al servidor LDAP y verifica si la petición, compara si el usuario y el password pertenecen a la institución A
I. El servidor LDAP al comparar la petición, da respuesta que el usuario institución A si pertenece a la institución A y envía la respuesta al servidor RADIUS de la institución A
J. Este reenvía la respuesta que el servidor LDAP a dado por medio Internet al servidor RADIUS de la institución B.
K. El servidor RADIUS recibe la respuesta y la reenvía al switch.
   El Switch envía la respuesta al punto de acceso para dar acceso al equipo del usuario institución A

Ya una vez autorizado por la institución B comienza la sesión en la red de la institución B, esta sesión es cifrada y el envió de paquetes y recibir paquetes esta seguro.

## *3.4 DISEÑO DE LA INTERFAZ PARA AUTENTICACIÓN DE USUARIOS*

En esta sección se presentará la interfaz que el usuario observará para poder conectarse al programa mundial de Eduroam.

### *3.4.1 Software para autenticación SecureW2*

Como se mencionó anteriormente, los usuarios de la red mundial Eduroam se autentican a la red por medio del software gratuito SecureW2. SecureW2 es el programa que se encargará de validar el usuario y el password de los usuarios en la red inalámbrica.

A continuación se muestra un ejemplo de la interfaz que posee el software SecureW2.

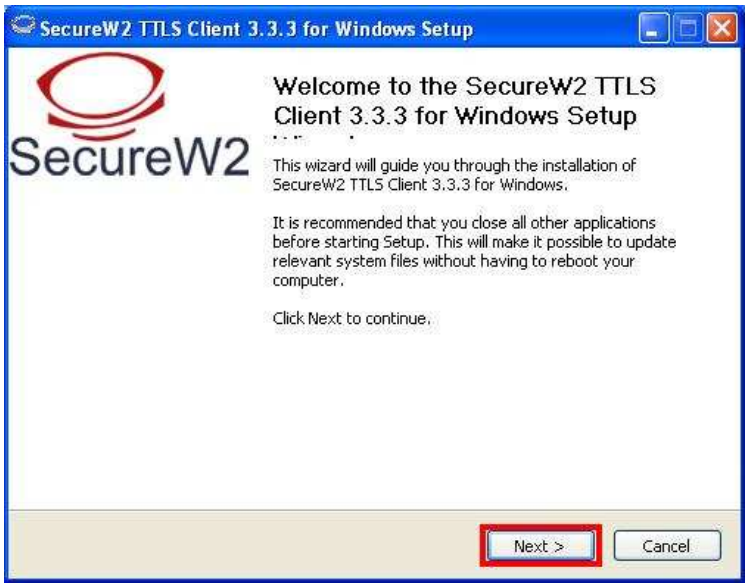



*Figura 3.4.1.1 Interfaz del software SecureW2*

## *3.4.2 Pagina Web*

Uno de los requisitos que el programa mundial Eduroam solicita es que la institución posea una página web informativa del proyecto. El diseño del sitio web se define a continuación:
En la ventana se mostrarán cuatro áreas (frames) como se muestra en la figura 3.4.2.1

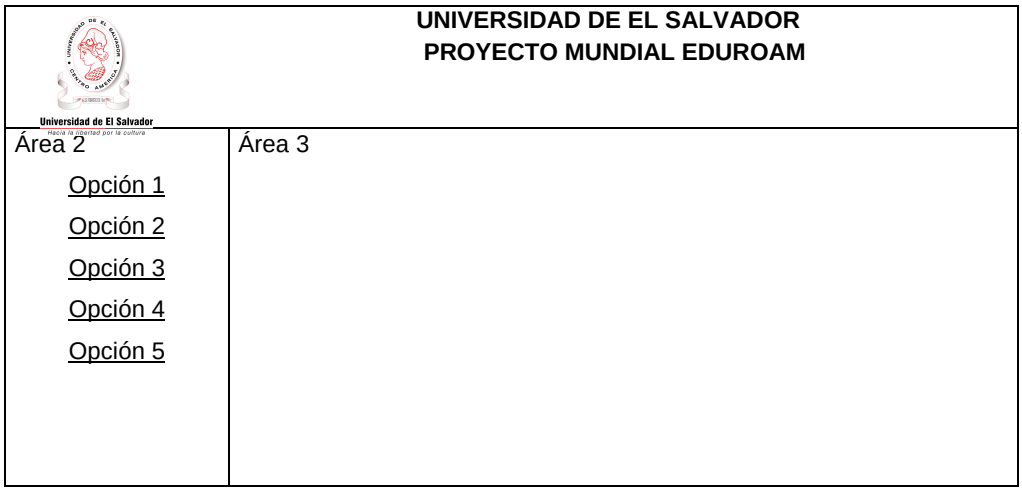



*Figura 3.4.2.1 Distribución de frames.*

Área 1: Mostrará el nombre del proyecto con los logos de la Universidad de El Salvador y de Eduroam.
Área 2: Mostrará el menú con las opciones, por ejemplo:

- ✓ Descripción del Servicio
- ✓ Que es Eduroam
- ✓ Ayuda

Área 3: Página de información

La apariencia del sitio web será como se muestra en la figura 3.4.2.2 Diseño de la página web informativa.

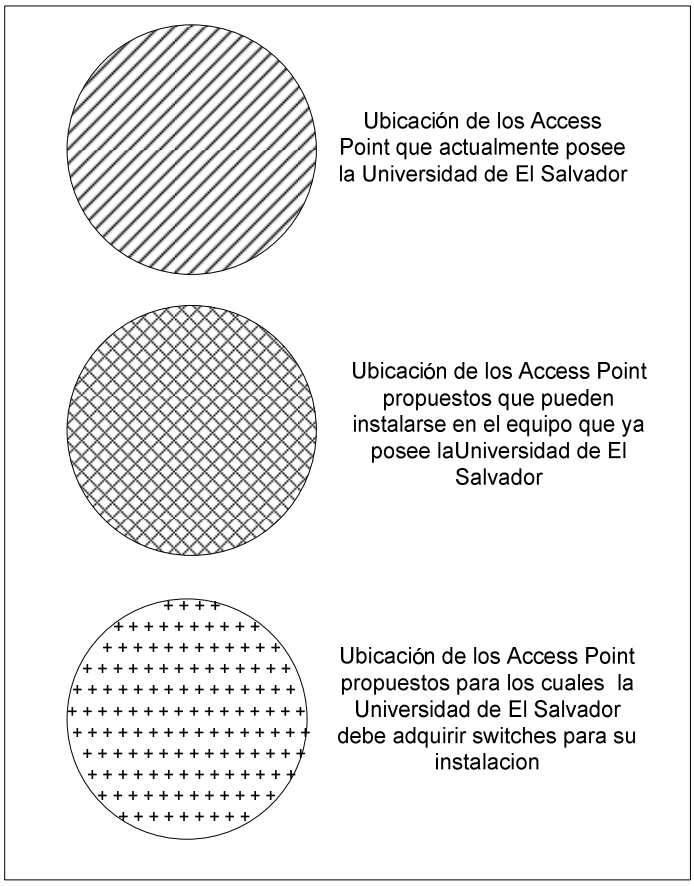

*Figura 3.4.2.2 Diseño de la pagina web informativa*

# 3.5 COBERTURA DE LA RED INALÁMBRICA PROPUESTA

Con el fin de mejorar la cobertura de la red inalámbrica de la Universidad de El Salvador y con base en el inventario del hardware de red que actualmente posee la universidad se plantea a continuación una mejora de los radios de cobertura de la WLAN y el detalle del equipo necesario para dicha mejora.

## 3.5.1 Planos propuestos de ubicación de puntos de acceso y planos de cobertura

Los puntos de acceso propuestos para una mejor cobertura los cuales pueden agregarse al equipo que actualmente posee la universidad, se muestran en círculos rellenos con cruces, y finalmente, los círculos rellenos de cuadros representan los puntos de acceso propuestos para los cuales la universidad debe adquirir switches con la características que se describieron anteriormente en el apartado 1.3.1.3 Puntos de Acceso (Autenticadores).




*3.5.1.1 Radios de Cobertura de Access Point*

***Campus Central***

Ver anexo 5

***Multidisciplinaria Occidental***

Ver Anexo 6

***Multidisciplinaria Paracentral***

Ver Anexo 7

***Multidisciplinaria Oriental***

Ver Anexo 8

### *3.5.2 Equipo propuesto*

Los puntos de acceso están situados de forma tal, que el área que cubre cada punto, se solape lo menos posible con los puntos adyacentes, a la vez que se maximice su alcance para uso de los alumnos, profesores y personal administrativo de la universidad. Los puntos de acceso propuestos son con antenas externas, ya que proporcionan servicio con un alcance óptimo en un radio de 50 metros. La distribución de los puntos de acceso propuesto es la siguiente:

***Campus Central:***

- ✓ 3 puntos en la facultad de Ingeniería y Arquitectura.
  - o Edificio de Ingeniería Eléctrica
  - o Edificio de Ingeniería Mecánica / Química
  - o Unidad de Ciencias Básicas
- ✓ 7 puntos en la facultad de Ciencias y Humanidades.
  - o Edificio de Periodismo y Letras
  - o Edificio de Idioma y Filosofía
  - o Edificio de Fondo Universitario y Protección
  - o Edificio de Biología
  - o Edificio Escuela de Química
  - o Edificio de Escuela de Física y Matemáticas
  - o Edificio del Psicología y Educación
- ✓ 1 puntos en la facultad de Ciencias Económicas.
  - o Edificio de Administración de Empresas
- ✓ 2 puntos en la facultad de Jurisprudencia y Ciencias Sociales.
  - o Edificio de Jurisprudencia y Ciencias Sociales los 2 puntos de acceso
- ✓ 2 puntos en la facultad de Medicina.
  - o Edificio de Medicina los 2 puntos de acceso
- ✓ 1 punto en la facultad de Odontología.
  - o Edificio de Odontología
- ✓ 1 punto en la facultad de Agronomía.
  - o Edificio de Ciencias Agronómicas
- ✓ 1 punto en el edificio de la Vicerrectoria.
  - o Edificio de Vicerrectoria Académica
- ✓ 1 punto en el edificio de Académica Central.
  - o Edificio de Académica Central

***Multidisciplinaria Occidental (Santa Ana):***

- ✓ 2 puntos de acceso en el edificio de Docentes y usos múltiples.
- ✓ 1 punto de acceso en el Bunker.

***Multidisciplinaria Paracentral (San Vicente):***

- ✓ 1 punto de acceso en el edificio de Post-Grado.
- ✓ 1 punto de acceso en el Centro de Desarrollo Profesional y Docente.
- ✓ 1 punto de acceso en el edificio de Biblioteca.

***Multidisciplinaria Oriental (San Miguel):***

- ✓ 1 punto de acceso en el edificio del Departamento de Economía.
- ✓ 1 punto de acceso en el Laboratorio de Química.
- ✓ 1 punto de acceso en la Biblioteca.
- ✓ 2 puntos en el edificio de administración.
- ✓ 1 punto en el Centro de Cómputo.
- ✓ 2 puntos en el Edificio de Medicina.

# 3.6 DISEÑO PROCEDIMENTAL

## *3.6.1 Integración de la Universidad de El Salvador al Programa Mundial Eduroam*

Una vez dispuestos y en correcto funcionamiento de los servidores RADIUS y LDAP, así como los equipos de red configurados con el protocolo 802.1X y finalmente instalado el software SecureW2 en los clientes o suplicantes se debe realizar las siguientes tareas administrativas de afiliación al programa:

Afiliarse a la organización RedIRIS.

La coordinación de las instituciones participantes se fundamenta en la participación en la lista **moviris**:

- Para Suscripción o borrado de la lista moviris.
- Información sobre el uso de la lista moviris.
- Archivos de la Lista MovIRIS

Las organizaciones participantes deberán además ajustarse a la política de participación de la iniciativa. (Ver anexo 15 "Políticas de participación a Eduroam")

### 3.6.2 Diseño de la metodología de prueba de conexión a la red mundial Eduroam

Para poder realizar las pruebas de conexión a la red mundial Eduroam se efectuará de la siguiente manera, con la colaboración de un contacto en España que pertenece a la RedIRIS (http://www.rediris.es/) de nombre es José Manuel Macías Luna (jmanuel.macias@rediris.es).

Pasos para las pruebas de conexión a la red mundial Eduroam:

***PRUEBA 1: Conexión usando Eduroam como invitado, al exterior***

1. Se creará una cuenta (usuario y password) con la autorización del encargado de la red de la Universidad de El Salvador (Eric López)
2. Esta nueva cuenta se le proporcionara a José Manuel Macías Luna (contacto en España).
3. José Manuel Macías Luna se conectara a la red mundial Eduroam con la cuenta (usuario y password) que se le proporcionó.
4. Una vez se pueda conectar se le pedirán pruebas de conexión que serán
    a. Logs de registro de los servidores

Ver las pruebas de conexión en el Capitulo 4.4 "Pruebas de configuración"

Ejemplo del procedimiento de conexión

El colaborador se tiene que conectar a la red inalámbrica llamada 'Eduroam', como si fuese un miembro de la Universidad de El Salvador. Todo parece trabajar exactamente de la misma manera: él digita sus credenciales y esto le permite conectarse a la red.

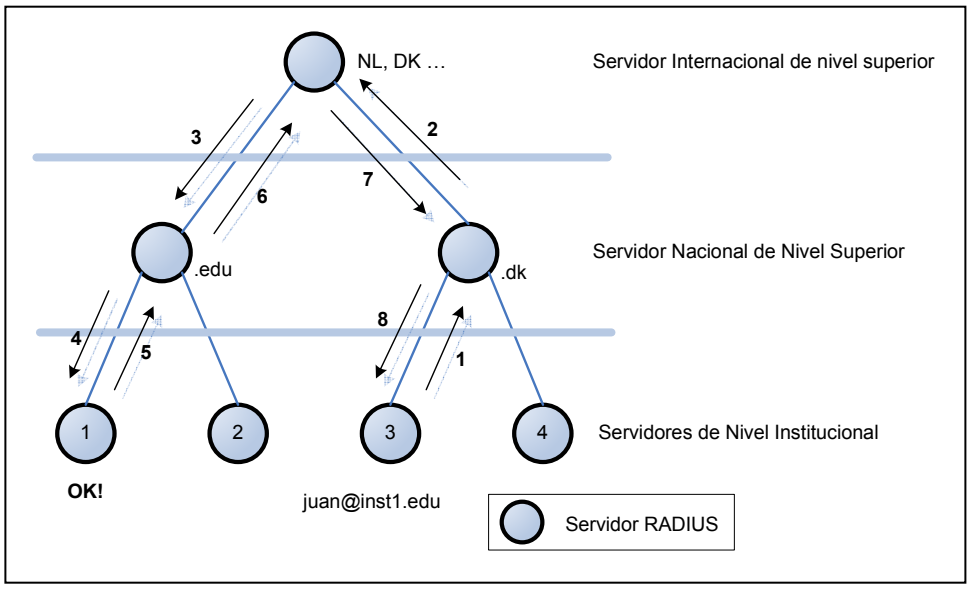



*Figura 3.6.2.1 Conexión a Eduroam como invitado a nivel internacional.*

Lo que él no ve es que su petición de autenticación primero está enviada al servidor local de la autenticación en Institución-3, y después al Servidor Internacional de nivel superior en Dinamarca. Como la institución 1 es desconocida para el servidor nacional, entonces se envía al Servidor Internacional de nivel superior que sabe dónde enviar los pedidos para los dominios de nivel superior y por lo tanto también adonde enviar la petición que se está haciendo para este caso es **.edu**. En éste servidor nacional sabe para qué institución debe enviarlo y finalmente autentican al usuario en Institución-1. El mensaje del reconocimiento es envía de nuevo al punto de acceso inalámbrico donde fue solicitado, siguiendo la misma ruta de la petición.

El tráfico entre el punto de acceso inalámbrico y la máquina del usuario seguirá cifrado durante la sesión entera.

### *PRUEBA 2: Conexión usando Eduroam como invitado, al exterior*

El procedimiento de autenticación es el mismo que el anterior, pero se realizará para comprobar que se puede hacer en dos vías.

1. José Manuel Macías Luna creará en su RedIRIS una nueva cuenta para nosotros el cual el nos la proporcionará.
2. Una vez teniendo la cuenta proporcionada por José Manuel Macías Luna y con la ayuda de Eric López (Administrador de la red de la Universidad de El Salvador) se procederá a conectarse a la red mundial Eduroam
3. Ya conectado a la red mundial Eduroam se le pedirá a Eric López, las pruebas de que dicha conexión fue exitosa. Estas pruebas sean:
    a. Logs de registro de los servidores

Ver las pruebas de conexión en el Capitulo 4.4 "Pruebas de configuración"

### *PRUEBA 3: Conexión usando Eduroam localmente*

1. Un miembro del grupo de trabajo digitará sus credenciales para conectarse a la red con el SID Eduroam.
2. Después de digitados el usuario y contraseña se verificará que se tiene acceso a la red y conexión a Internet.
3. Ya conectado a la red se solicitarán al responsable de la red las pruebas de que dicha conexión fue exitosa. Estas pruebas serán:
    a. Logs de registro de los servidores

Ver las pruebas de conexión en el Capitulo 4.4 "Pruebas de configuración"

Ejemplo del procedimiento de conexión

El usuario encuentra la red inalámbrica llamada "Eduroam", luego presiona el botón conectar, posteriormente le aparecerá un mensaje en la conexión inalámbrica o alambica donde le pedirá autenticarse con su usuario y password con el programa SecureW2 instalado posteriormente en la laptop o PC. El punto de acceso local inalámbrico trabaja como encargado del ingreso, pidiendo a favor del administrador de la red las credenciales. Éstos se proporcionan vía software del cliente en la computadora del usuario (mientras que el proceso de la conexión se basa en el Protocolo de seguridad 802.1X usando una disposición especial llamada TTLS). El servidor de autenticación (contiene todos los usuarios conocidos del campus) en la Universidad de El Salvador, es contactado y si se autentica, el estará "adentro" de la red inalámbrica. Antes de esto el no podrá conseguir una dirección IP y por lo tanto no puede molestar a otros o la red de ninguna manera.

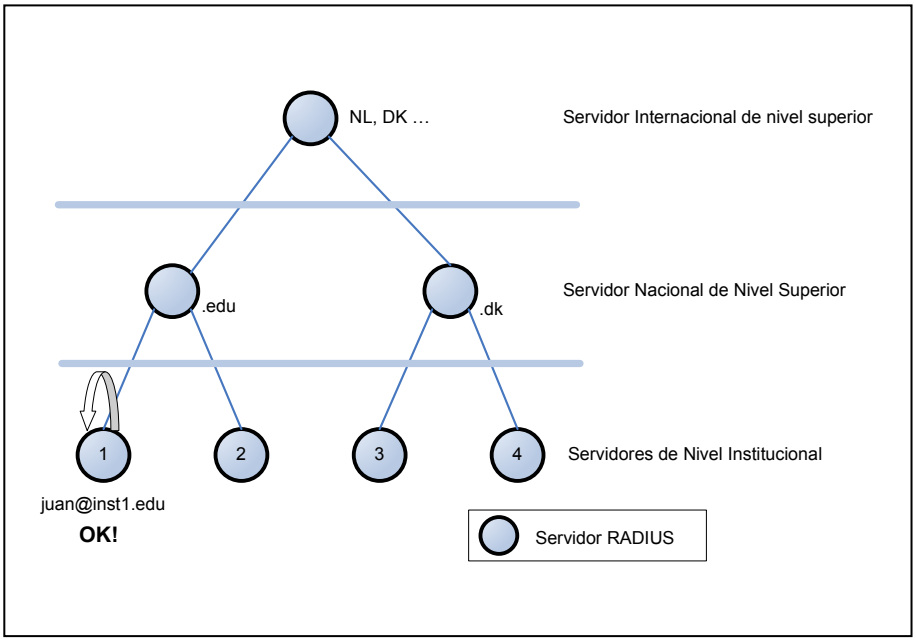



*Figura 3.6.2.2 Conexión a Eduroam localmente.*

Cuando el punto de acceso de la red inalámbrica ve la máquina, primero pide el dominio del usuario. Esto se utiliza para crear un canal encriptado entre el usuario y el servidor de autenticación donde no puede ser interceptada una transmisión privada y para no intervenir el punto de acceso de la red inalámbrica. Entonces las credenciales son transferidas al servidor de autenticación de la institución central. En este caso solamente es necesario el nombre del usuario que es la dirección de correo, mientras que él es reconocido localmente (por el realm). Cuando es aceptado, un mensaje es enviado a los puntos accesos de la red inalámbrica que alternadamente permite al usuario acceso a la red. De esta manera todos los punto de acceso reconocerán que el usuario pertenece al mismo dominio y eso

es aceptable y lo deja conectarse a la red. El tráfico entre el punto de acceso y la máquina del usuario seguirá cifrado durante la sesión entera.
Todas estas pruebas están documentadas en el Capitulo 4.4 "Pruebas de configuración"

# *4 CONFIGURACIÓN Y PRUEBAS*
## *4.1 DESCRIPCIÓN DEL AMBIENTE*

Eduroam proviene de EDUcation ROAMing. Esta ofrece a los usuarios de las instituciones académicas participantes un acceso a Internet seguro desde cualquier otra institución en la que este habilitado Eduroam. La arquitectura de Eduroam hace esto posible basado en una serie de tecnologías y acuerdos, que en conjunto proveen al usuario de Eduroam una experiencia: "abre tu laptop y estas en línea".

El acuerdo crucial en el que se fundamenta Eduroam es que la autenticación de un usuario se lleva a cabo en su institución origen usando sus propios métodos de autenticación específicos, mientras que, la decisión de autorización del uso de la red de la institución visitada la realiza el propietario de la red.
Con el fin de transportar la solicitud de autenticación de un usuario de una institución visitante hacia su institución origen y la respuesta de esa solicitud, se crea un sistema jerárquico de servidores RADIUS. Normalmente cada institución cuenta con un servidor RADIUS conectado a una base de datos de usuarios locales. Este servidor RADIUS es conectado a un servidor RADIUS a nivel nacional, que a su vez esta conectado al servidor europeo o (mundial). Porque los usuarios están usando sus nombres de usuario en el formato "usuario@dominio", donde dominio es el nombre de DNS que frecuentemente se forma como institucion.tld (tld = código de país de dominio de nivel superior), el servidor RADIUS puede usar esta información para encaminar o direccionar las solicitudes apropiadamente al siguiente salto en la jerarquía hasta que la institución origen sea hallada. Un ejemplo de la jerarquía RADIUS se muestra en la figura 4.1.1

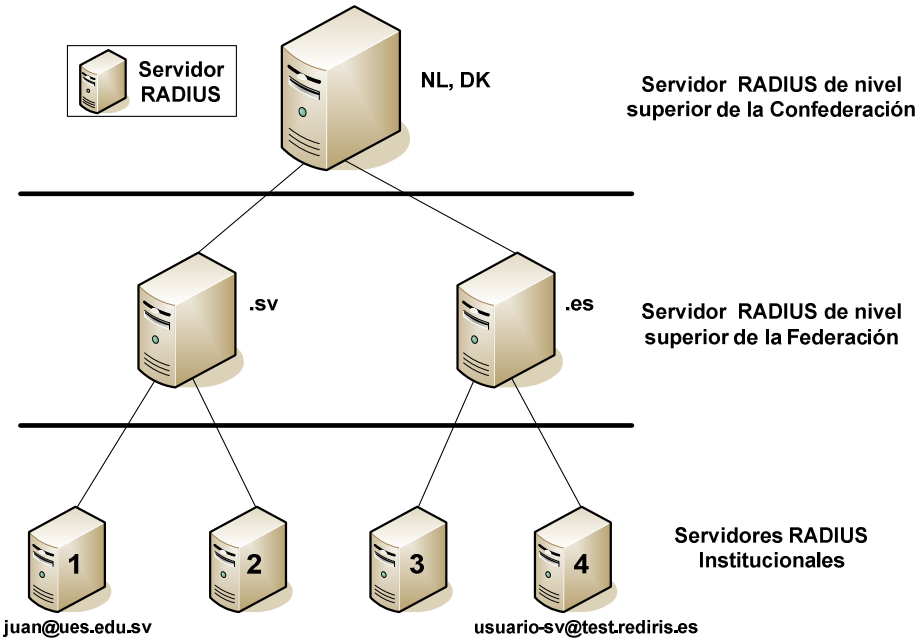



*Figura 4.1.1 Capas de la herencia de un servidor RADIUS de la red Eduroam.*

Para transferir la información de autenticación del usuario de forma segura a través de la infraestructura-RADIUS a su institución de origen, y para evitar que otros usuarios intercepten la conexión después de una autenticación exitosa, los puntos de acceso o los switches usan el estándar IEEE 802.1X que incluye el uso del Protocolo de Autenticación Extensible (EAP). El cual establecerá un túnel seguro desde la computadora del usuario a su institución de origen a través del cual la información de autenticación (nombre de usuario / contraseña) será llevada por EAP-TTLS

RADIUS transporta el nombre del usuario en el atributo User-Name, también transporta paquetes EAP, los cuales viajan cifrados y no son visibles por servidores intermedios, solamente por el servidor de autenticación de su institución origen.

Con el fin de garantizar la privacidad, el usuario deberá tener instalado el software SecureW2[21] en su equipo, el cual en la configuración de dicho software no se utilizara el nombre de un usuario real del servidor RADIUS en el atributo "User-Name" (este atributo es con el que se identifica con el "exterior"). En lugar de ello, se utilizara anonymous@dominio en este atributo. La parte dominio debe ser correcta, como el utilizado en la ruta para enviar la solicitud al respectivo servidor origen. Una vez que el servidor descifra el túnel TLS del paquete EAP, se obtiene el verdadero nombre de usuario (la identidad "interior").

[21] http://www.securew2.com/

Después de la autenticación exitosa por la institución origen y la autorización de la institución visitante, esta última da permisos de acceso al usuario visitante, posiblemente colocando al usuario en una VLAN para invitados.

A continuación se describen varios de los elementos de la arquitectura y sus funciones.

## *4.1.1 Elementos de la infraestructura Eduroam*

**Servidor RADIUS de nivel superior de la Confederación.**

Este está localizado en los Países Bajos y Dinamarca para la confederación europea, y en Australia y Hong Kong para las regiones del Pacífico y Asia respectivamente. Cada uno tiene una lista de los dominios de los países conectados y proporcionados adecuadamente por NRENs. Ellos aceptan las peticiones de dominios de la federación de los cuales son responsables y posteriormente reenvían las peticiones a los servidores RADIUS asociados de otras federaciones (y transportan las peticiones de autenticación de retorno).

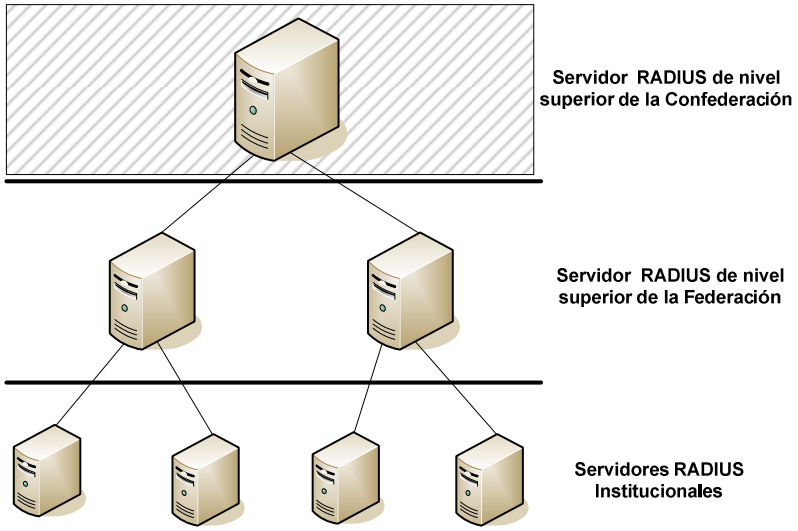



*Figura 4.1.1.1 Servidor RADIUS de nivel superior de la confederación*

**Servidor RADIUS de nivel superior de la Federación.**

Tiene una lista de instituciones conectadas al servidor y realmente asociadas. Recibe peticiones de los servidores de la confederación y de las instituciones que tienen asociadas. Si están conectadas a él reenvía la petición a la institución apropiada, sino la redirecciona al servidor de la confederación.

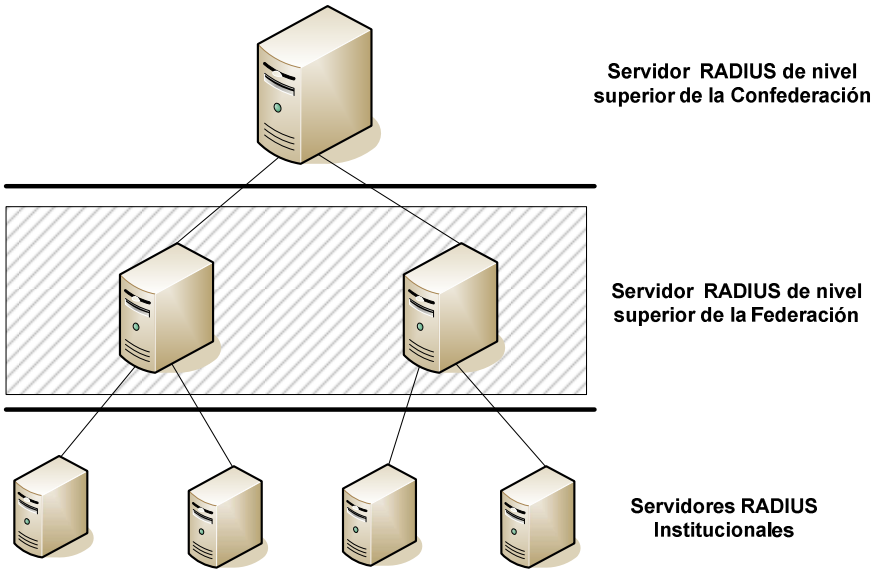



*Figura 4.1.1.2 Servidor RADIUS de nivel superior de la federación*

**Servidor RADIUS Institucional.**

Es el responsable de la autenticación de sus propios usuarios (tanto locales como de usuarios visitantes de otros instituciones) por medio de la verificación de sus credenciales en el sistema de administración local de identidades y reenvía las peticiones de los usuarios visitantes a sus respectivos servidores RADIUS de nivel superior de su federación. Sobre la base de una autenticación apropiada este servidor asigna VLAN al usuario.

Este servidor es el más complejo de todos ya que mientras los otros servidores RADIUS simplemente atienden peticiones de Proxy, el servidor institucional, además de resolver peticiones EAP, realiza operaciones de búsqueda en el sistema de administración de identidades.

Actualmente la Universidad cuenta con un servidor RADIUS configurado y funcional, este funciona bajo la responsabilidad de la Unidad de Educación a Distancia, la cual es una dependencia de la Vice-Rectoría Académica.

En conjunto con el servidor RADIUS debe funcionar el sistema de Administración de Identidades, el cual contiene información de los usuarios; por ejemplo nombres de usuario y sus contraseñas. Este debe de mantenerse actualizado por la institución responsable. La Universidad de El Salvador cuenta actualmente para éste fin con la implementación del protocolo LDAP el cual permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información del entorno de red y es llamado con ese mismo nombre.

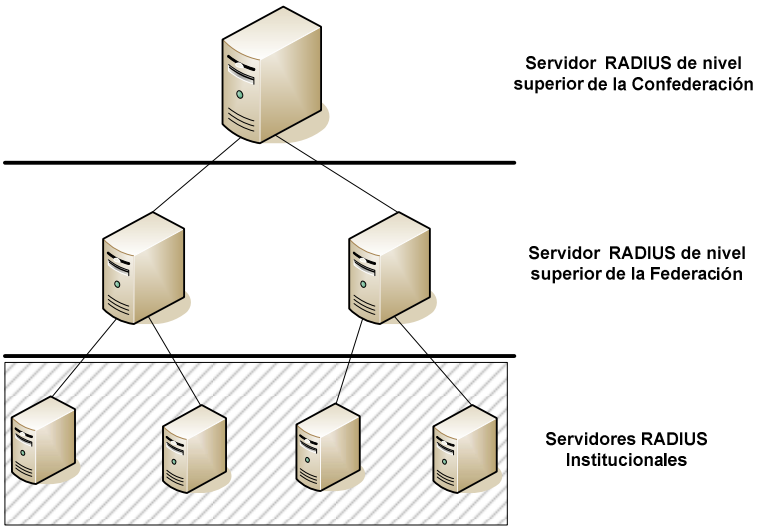



*Figura 4.1.1. Servidor RADIUS institucionales*

# *4.2 CONFIGURACIÓN DE LOS PROTOCOLOS EN LOS EQUIPOS DE RED*

En las redes institucionales o de campus varían mucho las topologías, equipo utilizado, software y otros. Con el objeto de ayudar a los administradores o la configuración de Eduroam en sus campus, esta sección presenta una instalación típica. Se espera que permita a los usuarios de diferentes topologías y equipos entender los pasos necesarios para hacerlos. Por otra parte en los anexos también se presentan ejemplos de configuración de equipos y software comunes utilizados.

Para la red de ejemplo utilizamos un típico conjunto de equipos de red que consta de:

- Un switch 3Com 4200 (o similar).
- Un Access Point 3COM 11a/b/g.
- Una laptop con Windows XP.
- Un servidor RADIUS.

## *4.2.1 Protocolo RADIUS*

RADIUS (Remote Authentication Dial-In User Service) es un protocolo de autenticación, autorización y manejo de cuentas de usuario originalmente desarrollado por Livingston Enterprises y publicado en 1997 como los RFC 2058[22] y 2059[23]. Es utilizado para administrar el acceso remoto y la movilidad IP,

[22] http://www.normes-internet.com/normes.php?rfc=rfc2058&lang=es

como ocurre en servicios de acceso por modem, DSL, servicios inalámbricos 802.11 o servicios de VoIP (Voice over IP o Voz sobre IP). Este protocolo trabaja a través del puerto 1812 por UDP.

La autenticación gestionada por este protocolo se realiza a través del ingreso de un nombre de usuario y una clave de acceso. Esta información es procesada por un dispositivo NAS (Network Access Server) a través de PPP (Point-to-Point Protocol o Protocolo Punto-a-Punto) siendo posteriormente validada por un servidor RADIUS a través del protocolo correspondiente valiéndose de diversos esquemas de autenticación, como PAP[24] (Password Authentication Protocol o Protocolo de Autenticación de Clave de acceso), CHAP[25] (Challenge-Handshake Authentication Protocol) o EAP (Extensible Authentication Protocol), y permitiendo el acceso al sistema.

La universidad de El Salvador utiliza un servidor RADIUS de código abierto, *FreeRADIUS versión 1.1.3.*

**FreeRADIUS.**

FreeRADIUS, proyecto iniciado en 1999 por Alan DeKok y Miquel van Smoorenburg (quien colaboró anteriormente en el desarrollo de Cistron RADIUS), es una alternativa libre hacia otros servidores RADIUS, siendo uno de los más completos y versátiles gracias a la variedad de módulos que le componen. Puede operar tanto en sistemas con recursos limitados así como sistemas atendiendo millones de usuarios.

FreeRADIUS inició como un proyecto de servidor RADIUS que permitiera una mayor colaboración de la comunidad y que pudiera cubrir las necesidades que otros servidores RADIUS no podían. Actualmente incluye soporte para LDAP, SQL y otras bases de datos, así como EAP, EAP-TTLS y PEAP. Actualmente incluye soporte para todos los protocolos comunes de autenticación y bases de datos.

Para ver el detalle de la configuración del servidor RADIUS para que funcione con un servicio de acceso a directorio LDAP se puede ver el anexo 12 "Manual Técnico de Configuración".

[23] http://www.normes-internet.com/normes.php?rfc=rfc2059&lang=es

[24] http://es.wikipedia.org/wiki/PAP

[25] http://es.wikipedia.org/wiki/CHAP

### *4.2.2 Protocolo LDAP*

LDAP (Lightweight Directory Access Protocol) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas.

Habitualmente, almacena la información de login (usuario y contraseña) y es utilizado para autenticarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc.).

En conclusión, LDAP es un protocolo de acceso unificado a un conjunto de información sobre una red. La Universidad de El Salvador cuenta con una versión de código abierto llamada OpenLDAP versión 2.3.3.

**Instalación Básica**

1. Una vez obtenido el archivo Tar que contiene OpenLDAP, este debe ser descomprimido en un directorio temporal ( /tmp por lo general) para poder iniciar la instalación.
2. Dentro del directorio temporal ( /tmp ) donde fue descomprimido OpenLDAP se genera un directorio por nombre openLDAP-<numero de versión>, colóquese dentro de este directorio y ejecute el comando: ./configure , este comando configura los archivos de instalación de acuerdo a su sistema.
3. Posteriormente debe ejecutar make depend seguido de make, esto genera OpenLDAP dentro del mismo directorio temporal.
4. Debe ejecutar ciertas pruebas para garantizar que OpenLDAP funcione correctamente, colóquese dentro del directorio tests y ejecute make seguido de make test.
5. Ahora si debe instalar OpenLDAP en el sistema, descienda del directorio tests y como raíz ejecute: make install
6. El comando anterior instala OpenLDAP bajo el directorio /usr/local/etc/openladp (si no cambió este parámetro al tiempo de compilar OpenLDAP).
7. Después de haber completado los pasos anteriores la instalación esta completa, ahora debe configurar los parámetros básicos.

Para ver el detalle de la configuración del servidor LDAP ver anexo 12 "Manual Técnico de Configuración".

### *4.2.3 Protocolo 802.1X*

Permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto o previniendo el acceso por ese puerto si la autenticación falla. Es utilizado en algunos puntos de acceso inalámbricos cerrados.

802.1X está disponible en ciertos switches de red y puede configurarse para autenticar nodos que están equipados con software suplicante. Esto elimina el acceso no autorizado a la red al nivel de la capa de enlace de datos.

Al implementar el 802.1X en puntos de acceso inalámbricos se pueden utilizar para corregir fallas de seguridad de WEP. Esta autenticación es realizada normalmente por un tercero, tal como un servidor de RADIUS. Esto permite la autenticación sólo del cliente o, más apropiadamente, una autenticación mutua fuerte utilizando protocolos como EAP-TTLS.
Lo anterior implica que este debe ser configurado en los equipos de red compatibles.

### *4.2.4 Equipo de Red*

**Switch 3Com 4200**
Ver anexo 12 "Manual Técnico de Configuración", tema "Switch 3Com 4200".

**Punto de Acceso 3Com 7760 11 a/b/g**
Ver anexo 12 "Manual Técnico de Configuración", tema "Acces Point 3Com 7760".

### *4.2.5 Cliente 802.1X*

EAP-TTLS se ha considerado la forma más fácil de aplicar Eduroam en grande (especialmente estudiantes). MS Windows no tiene un soporte para EAP-TTLS, pero puede ser añadido por la instalación de SecureW2, un producto de Alfa&Ariss Network Security Solution, y permitir así a una gran comunidad de usuarios para EAP-TTLS.
Las instrucciones de instalación del cliente SecureW2 se encuentran en el anexo 11 "Manual de Usuario".

# 4.3 LISTADOS DE CONFIGURACIÓN

## 4.3.1 Protocolo RADIUS

Debido a que esto archivos contienen información confidencial de la configuración del servidor RADIUS de la Universidad de El Salvador no será posible presentar los listados completos, en este sentido se colocaran listados ejemplos de configuraciones de servidor RADIUS

Los principales archivos de configuración del servidor RADIUS son 4:

**RADIUS.conf**

Archivo general de configuración de FreeRADIUS. A continuación se listan los esquemas usados en el servidor RADIUS de la Universidad de El Salvador

```
prefix = /usr/local
exec_prefix = ${prefix}
sysconfdir = ${prefix}/etc
localstatedir = ${prefix}/var
sbindir = ${exec_prefix}/sbin
logdir = ${localstatedir}/log/RADIUS
raddbdir = ${sysconfdir}/raddb
radacctdir = ${logdir}/radacct
# Location of config and logfiles.
confdir = ${raddbdir}
run_dir = ${localstatedir}/run/RADIUS
log_file = ${logdir}/RADIUS.log
libdir = ${exec_prefix}/lib
pidfile = ${run_dir}/RADIUSd.pid
max_request_time = 30
delete_blocked_requests = no
cleanup_delay = 5
max_requests = 1024
bind_address = *
port = 0
hostname_lookups = no
allow_core_dumps = no
regular_expressions = yes
extended_expressions = yes
log_stripped_names = yes
log_auth = yes
log_auth_badpass = yes
log_auth_goodpass = yes
usercollide = no
lower_user = no
lower_pass = no

nospace_user = no
nospace_pass = no
checkrad = ${sbindir}/checkrad
# SECURITY CONFIGURATION
security {
```

```
max_attributes = 200
reject_delay = 1
status_server = no
}
# PROXY CONFIGURATION
proxy_requests = no
# CLIENTS CONFIGURATION
$INCLUDE ${confdir}/clients.conf
# SNMP CONFIGURATION
snmp = no
# THREAD POOL CONFIGURATION
thread pool {
start_servers = 5
max_servers = 32
min_spare_servers = 3
max_spare_servers = 10
max_requests_per_server = 0
}
# MODULE CONFIGURATION
modules {
$INCLUDE ${confdir}/eap.conf
mschap {
authtype = MS-CHAP
}
files {
usersfile = ${confdir}/users
acctusersfile = ${confdir}/acct_users
preproxy_usersfile = ${confdir}/preproxy_users
compat = no
}
}
# Instantiation
instantiate {
}
authorize {
files
mschap
eap
}
# Authentication.
authenticate {
Auth-Type MS-CHAP {
mschap
}
```

**EAP.conf**

Archivo de configuración de las directivas EAP a utilizar. Es una librería de RADIUSd.conf. A continuación se listan los esquemas usados en el servidor RADIUS de la Universidad de El Salvador

```
eap {
default_eap_type = tls
timer_expire = 60
ignore_unknown_eap_types = no
cisco_accounting_username_bug = no
# Supported EAP-types
# EAP-TLS
tls {
private_key_password = laclave
private_key_file = ${raddbdir}/certs/servidor-prueba.key
certificate_file = ${raddbdir}/certs/servidor-prueba.crt
CA_file = ${raddbdir}/certs/demoCA/cacert.pem
dh_file = ${raddbdir}/certs/dh
random_file = ${raddbdir}/certs/random
fragment_size = 1024
include_length = yes
}
peap {
default_eap_type = mschapv2
}
mschapv2 {
}
}
```

**CLIENTS.conf**

Descripción y credenciales de los diferentes dispositivos que consultan al RADIUS. A continuación se listan los esquemas usados en el servidor RADIUS de la Universidad de El Salvador

```
client 192.168.13.91 {
secret = testing123
shortname = AP-RADIUS
}
client 192.168.13.99 {
secret = testing123
shortname = PRIMATE
}
client 200.27.70.12 {
secret = testing123
shortname = GIBBON
}
client 127.0.0.1 {
secret = testing123
shortname = localhost
nastype = other # localhost isn’t usually a NAS...
}
```

**USERS**

Archivo donde se especifican las credenciales de los usuarios de la red. Se usa este archivo si no existe otro archivo para el almacenamiento de los usuarios. A continuación se listan los esquemas usados en el servidor RADIUS de la Universidad de El Salvador

```
test Auth-Type := Local , User-Password == "test"
```

### *4.3.2 Protocolo LDAP*

A continuación se muestra el listado de los 3 archivos de configuración del protocolo LDAP implementado en la Universidad de El Salvador. Los cuales son:

- SLPAD.conf
- SYSLOG.conf
- [nombre_archivo].ldif

Debido a que esto archivos contienen información privada de la comunidad estudiantil (Estudiantes, Docentes y Administrativos) de la Universidad de El Salvador, como por ejemplo usuario, contraseña, puesto que ocupa, no será posible presentar la información de estos archivos, pero se presentan archivos ejemplos de cómo están configurados dichos archivos.

El contenido de cada uno de estos archivos es el siguiente:

**SLPAD.conf**

El archivo slapd.conf, localizado en /etc./openLDAP, contiene la información de la configuración necesaria para su servidor LDAP. A continuación se listan los esquemas usados en la instalación de configuración

```
# Schema and objectClass definitions
1. include      /etc/LDAP/schema/core.schema
2. include      /etc/LDAP/schema/cosine.schema
3. include      /etc/LDAP/schema/nis.schema
4. include      /etc/LDAP/schema/inetorgperson.schema
5. include      /etc/LDAP/schema/authLDAP.schema
6. include      /etc/LDAP/schema/perdition.schema
```

Línea 1: Esquema núcleo de cualquier árbol LDAP

Línea 2: Esquema de gestion de identidades compatibles con X.500

Línea 3: Esuema para LDAP y Network Information Service

Línea 4: Esquema genérico que describe a una persona en una Organización

Línea 5: Esquema de Courier para integración con LDAP

Línea 6: Esquema del Proxy de correo Perdition para integración con LDAP

**SYSLOG.conf**[26]

OpenLDAP por "default" envía su información de registro ("log") al Daemon syslog (syslog) bajo el canal LOCAL4. A continuación se presenta un ejemplo:

local4.* /var/log/openLDAP

Lo anterior indica enviar todo mensaje del canal LOCAL4 al archivo /var/log/openLDAP

[26] http://www.osmosislatina.com/ldap/configuracion.htm

**ARCHIVOS .ldif**[27]

El *LDAP Data Interchange Format* (LDIF) es un formato que se utiliza para la importación y exportación de datos independientemente del servidor LDAP que se está utilizando.

Cada servidor LDAP tiene una o varias maneras de almacenar físicamente sus datos en el disco duro, por esto que LDIF proveen una manera de unificar la manera de tratar los datos y así poder migrar de un servidor a otro sin importar que clase de implementación sea.

Una vez instalado el servidor LDAP será necesario poblar nuestro directorio con nuestros datos mediante el uso de archivos ldif

server:~# LDAPadd -x -D "cn=admin,dc=tes,dc=ues,dc=edu,dc=sv" -W -f misdatos.ldif

El archivo ldif es un archivo de texto que contiene los registros que serán ingresados en el directorio. Este formato es útil tanto para realizar copias de seguridad de los datos de un servidor LDAP, como para importar pequeños cambios que se necesiten realizar manualmente en los datos, siempre manteniendo la independencia de la implementación LDAP y de la plataforma donde está instalada. A continuación se muestra registro de nuestro árbol:

```
# Entry 1: uid=prueba,ou=usuarios,dc=test,dc=ues,dc=edu,dc=sv
dn:uid=prueba,ou=usuarios,dc=test,dc=ues,dc=edu,dc=sv
uid: prueba
cn: Ana Beatriz Aguirre Villalta
gidNumber: 105
homeDirectory: /var/buzones/
objectClass: CourierMailAccount
objectClass: inetLocalMailRecipient
objectClass: person
objectClass: top
objectClass: inetOrgPerson
quota: 209715200
uidNumber: 104
givenName: Ana Beatriz
displayName: Ana Beatriz Aguirre Villalta
sn: Aguirre Villalta
mail: aaguirre1@test.ues.edu.sv
title: Lic. COMPUTACION
o: PU-I ( PROFESOR UNIVERSITARIO )
l: San Salvador
mailbox: aaguirre1@ues.edu.sv/
mailHost: smtp1.ues.edu.sv
userPassword: {MD5}tjqvC0ltB4UHw5ZCgHkUCg==
```

[27] http://dns.bdat.net/documentos/ldap/#id2918899

## 4.4 PRUEBAS DE CONFIGURACIÓN

A continuación se presenta los log de las pruebas de conexión realizadas, usando la autenticación del SecureW2, el protocolo 802.1X y el servidor RADIUS. Se presentarán dos tipos de pruebas: las de conexión local y las de un invitado en la Universidad de El Salvador.

### 4.4.1 PRUEBA CONEXION LOCAL

Para la elaboración de esta prueba un miembro de la comunidad universitaria con sus credenciales se autenticará con el SecureW2, si el usuario se encuentra activo le permitirá acceder a la red.

A continuación el Log de la conexión:

```
Packet-Type = Access-Request
Fri Jul 18 12:55:48 2008
      Message-Authenticator = 0xd02ccd31c46bbc2582c4c81095da110f
      Service-Type = Framed-User
      User-Name = "rh97015"
      Framed-MTU = 1488
      State = 0xa22454ca1db2e874311bc512d6bee537
      Called-Station-Id = "00-1E-C1-33-00-40:AP2EDUROAM"
      Calling-Station-Id = "00-90-4B-99-58-46"
      NAS-Identifier = "3Com Access Point 7760"
      NAS-Port-Type = Wireless-802.11
      Connect-Info = "CONNECT 54Mbps 802.11g"
      EAP-Message =
0x020400c81580000000be160301008610000820080099fd7a1ad860e1b25dec08d93992d5d
5c6f40d400110e961cb069a2bd96c02cf194eb87a295b456d1c89a1e36bc85ae691ec2e5b1de
1d2d5d42579ebc08c9ce68e6b1a4bd42dc70839d75848505b04a5f17763516d91160ba7a698e
0b50d3ea900eccdefae1473a6c5e1128d360bd45ee4c70f864506a840e807d05a0dc6c4e1403
0100010116030100 28cb335afb09f55f789b1090aa64ce1f1750c0a6153a501e32a6b8aeb0b3
3aecf546d9d39839081ba8
      NAS-IP-Address = 192.168.0.139
      NAS-Port = 2
      NAS-Port-Id = "STA port # 2"
      Client-IP-Address = 168.243.2.247
```

### 4.4.2 PRUEBA INVITADO EN LA UNIVERSIDAD DE EL SALVADOR

Para la elaboración de esta prueba fue necesario que Eric López contactara al administrador de la RedIRIS José Manuel Macías Luna y nos proporcionara credenciales de prueba de la RedIRIS. José Manuel Macías Luna nos proporcionó las siguientes credenciales:

Usuario: usuario-sv@test.rediris.es

Contraseña: AcdypHejMi

Con las credenciales proporcionadas por RedIRis se procedió a realizar las pruebas de conexión con el SecureW2, si el usuario se encuentra activo le permitirá accesar a la red.

A continuación el Log de la conexión:

```
 #radtest usuario-sv@test.rediris.es AcdypHejMi localhost 1812 uesguest
Sending Access-Request of id 177 to 127.0.0.1 port 1812
      User-Name = "usuario-sv@test.rediris.es"
      User-Password = "AcdypHejMi"
      NAS-IP-Address = 255.255.255.255
      NAS-Port = 1812
rad_recv: Access-Accept packet from host 127.0.0.1:1812, id=177, length=48
      User-Name = "usuario-sv@test.rediris.es"
#radtest usuario-sv@test.rediris.es AcdypHejMi 168.243.7.146 1812 uesguest
Sending Access-Request of id 128 to 168.243.7.146 port 1812
      User-Name = "usuario-sv@test.rediris.es"
      User-Password = "AcdypHejMi"
      NAS-IP-Address = 255.255.255.255
      NAS-Port = 1812
rad_recv: Access-Accept packet from host 168.243.7.146:1812, id=128,
length=48
      User-Name = usuario-sv@test.rediris.es
```

## 4.5 DOCUMENTACIÓN

### 4.5.1 Manual de Usuario

Ver anexo 11 “Manual de Usuario”

### 4.5.2 Manual de Técnico

Ver anexo 12 “Manual Técnico de Configuración”

### *4.5.3 Plan de Implementación*

## 4.5.3.1 INTRODUCCIÓN

La seguridad en las redes inalámbricas está más que cuestionada hoy en día. Muchas de las redes existentes en la actualidad, basadas en el protocolo 802.11, ni siquiera se encuentran cifradas, por lo que el acceso a estas redes es tan sencillo como dejar que una computadora se conecte de manera automática o encontrar una IP válida para conectarnos a la red.

Los usuarios con algunos conocimientos cifran las redes basadas en el protocolo 802.11 mediante WEP (Wired Equivalent Privacy). Este es un procedimiento mediante el cual todas las comunicaciones establecidas por la red se encuentran cifradas con una clave compartida para todos los usuarios, que se emplea tanto para cifrar como para descifrar los mensajes enviados. En este caso, el acceso a dichas redes, se complica un poco, pero existen programas llamados "sniffer" para monitorizar la red y sacar la clave que se está empleando para cifrar los datos. Algunas claves pueden ser descubiertas con una PDA y algún programa de este tipo en menos de 2 horas.

## 4.5.3.2 OBJETIVOS

**OBJETIVO GENERAL**

Crear una guía que ilustre paso a paso la implementación de la seguridad en LANs alámbrica e inalámbricas utilizando el protocolo 802.1X

**OBJETIVOS ESPECÍFICOS**

- Dar a conocer la Vulnerabilidad de las Wlan con el protocolo **802.11**.
- Verificar la configuración en un servidor RADIUS.
- Verificar la configuración en un servidor LDAP
- Configurar un Punto de Acceso, con el protocolo 802.1X
- Configurar un Switch, con el protocolo 802.1 x

El objetivo de este plan, que trata las pautas generales de diseño de la solución de red de área local segura, reside en describir minuciosamente el diseño de la solución y las razones para hacerlo de tal forma. Asimismo, proporciona toda la información para adaptar el diseño a las necesidades particulares de cualquier institución.

El tiempo estimado para la implementación es de aproximadamente 95 dias.

Se comienza con una descripción del funcionamiento de 802.1X y del protocolo de autenticación extensible (EAP-TTLS) para proteger el acceso a la red. A continuación, se especifica la organización de destino de la solución, al tiempo que se explican algunos de los requisitos clave.

**Protocolo 802.1X – Autentificación y Manejo de Claves**

Con el fin de solucionar estos problemas surge el protocolo 802.1X, que aunque lleve ya algunos años en el mercado, pocas empresas lo utilizan, debido a su complejidad de instalación. Pero gracias a esta guía que implementamos las cosas van hacer mucho mas fáciles.

El protocolo 802.1X ofrece un marco en el que se lleva a cabo un proceso de autenticación del usuario, así como un proceso de variación dinámica de claves, todo ello ajustado a un protocolo, denominado EAP (Extensible Authentication Protocol). Mediante este procedimiento, todo usuario que esté empleando la red se encuentra autentificado y con una clave única, que se va modificando de manera automática y que es negociada por el servidor y el cliente de manera transparente para el usuario.

- El cliente, que quiere conectarse a la red, manda un mensaje de inicio de EAP-TTLS que da lugar al proceso de autentificación. Siguiendo con nuestro ejemplo.
- El punto de acceso a la red respondería con una solicitud de autentificación EAP-TTLS.
- El cliente responde al punto de acceso con un mensaje EAP-TTLS que contendrá los datos de autentificación.
- El servidor de autentificación verifica los datos suministrados por el cliente mediante algoritmos, y otorga acceso a la red en caso de validarse.
- El punto de acceso suministra un mensaje EAP-TTLS de aceptación o rechazo, dejando que el cliente se conecte o rechazándolo.
- Una vez autenticado, el servidor acepta al cliente, por lo que el punto de acceso o switch establecerá el puerto donde se auténtica el cliente en un estado autorizado.

De esta manera, el protocolo 802.1X provee una manera efectiva de autentificarse, se implementa una clave de autentificación WAP-TKIP. Pero de todas formas, la mayoría de las instalaciones 802.1X otorgan cambios automáticos de claves de encriptación usadas solo para la sesión con el cliente, no dejando el tiempo necesario para que ningún sniffer sea capaz de obtener la clave.

**Modo de funcionamiento de la seguridad de LAN inalámbrica**

Autenticación segura para WLAN a través de 802.1X y del cifrado del tráfico de red mediante el acceso protegido Wi-Fi (WPA). A continuación se detallan los puntos claves relacionados con este tema:
El uso de IEEE 802.1X proporciona un mecanismo de control de acceso seguro para la WLAN que ha de asociarse al mismo tiempo con un método de protocolo de autenticación extensible (EAP). La elección de este método de EAP define el tipo de credenciales que pueden usarse a la hora de autenticar usuarios y equipos en la WLAN.

EAP-TTLS constituye un medio de protección en el canal de seguridad. De este modo, EAP-TTLS se convierte en un elemento esencial para evitar ataques a métodos de EAP basados en contraseñas.
Una buena protección de datos del tráfico de WLAN puede conseguirse por medio de una WPA. Las claves de cifrado maestras para la protección de datos se generan como parte del proceso de autenticación 802.1X (WPA emplean estas claves de manera distinta).

EAP-TTLS**:** Define un tunel TLS encriptado para el envío seguro de datos. EAP-TTLS encapsula otro mecanismo de autenticación, de esta manera se tiene una seguridad en el envío de datos. El mecanismo de autenticación que utiliza EAP-TTLS es PAP (Password Authentication Protocol).
Para entender cómo funciona el protocolo 802.1X sigamos el siguiente esquema:

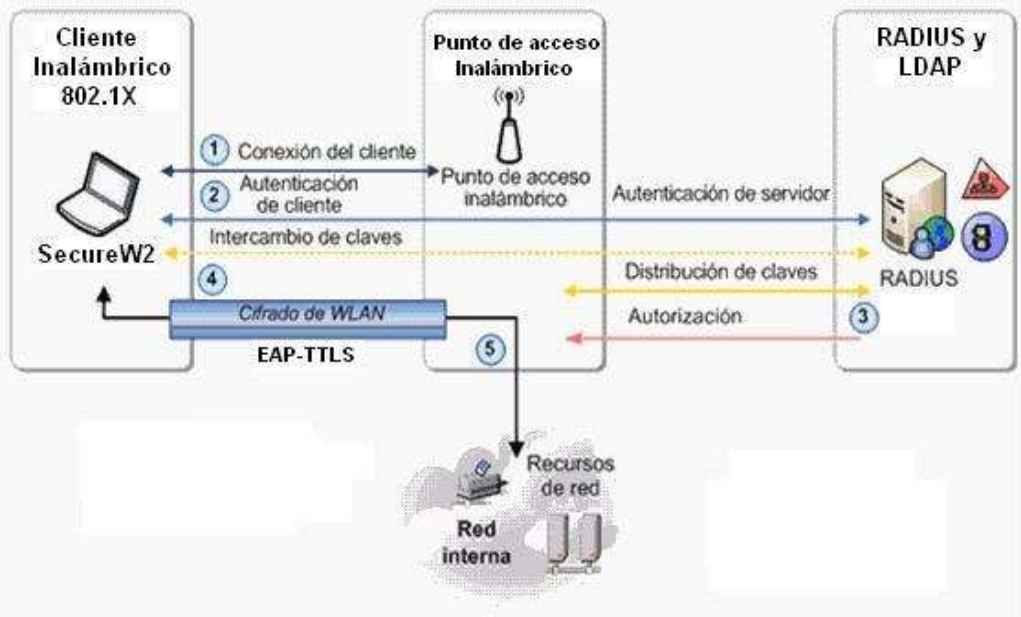



*Figura 4.5.3.1 Autenticación 802.1X para la LAN inalámbrica*

En la figura se muestran cuatro componentes principales:

**Cliente inalámbrico 802.1X:** se trata de un equipo o dispositivo que ejecuta una aplicación que requiere acceso a los recursos de red. El propietario del equipo debe de ingresar sus credenciales de correo, las cuales son utilizadas para autenticar al cliente en la red. El cliente debe tener un adaptador de red WLAN que sea compatible con 802.1X y con el cifrado de WPA. Este cliente, además, debe tener instalado el cliente SecureW2.

Antes de que el cliente pueda tener acceso a la WLAN, deberá autenticarse por medio del software SecureW2 (el servidor RADIUS y el directorio LDAP). Una vez detectada la red inalámbrica se selecciona la red que tiene por nombre Eduroam y luego se le da conectar, posteriormente nos aparecerá un cerificado (SecureW2) el cual nos pedirá nombre de usuario y contraseña, si todos los datos introducidos son correctos el puerto se abrirá y ya estaremos conectados.

**Punto de acceso inalámbrico:** el punto de acceso inalámbrico tiene como función el control del acceso a la WLAN y, al mismo tiempo, la unión de la conexión del cliente a la LAN interna. Debe ser compatible con 802.1X y con el cifrado de WPA. Asimismo, el punto de acceso inalámbrico y el servidor RADIUS comparten un secreto que les permite identificarse mutuamente sin riesgo alguno.

**El servidor RADIUS y el directorio LDAP:** el servidor RADIUS utiliza el directorio para comprobar las credenciales de los clientes WLAN, al tiempo que toma decisiones relativas a la autorización en función de una directiva de acceso a red. También puede recopilar información de responsabilidad y de auditoria sobre el acceso de los clientes a la red. Esto se conoce como servicio de autenticación.

**La red interna:** se trata de una red segura a la que la aplicación cliente inalámbrica debe obtener acceso.
Los siguientes pasos indican el modo en que el cliente realiza una solicitud y recibe permiso para tener acceso a la WLAN (y, en consecuencia, a la red interna). La numeración de estos pasos se corresponde con los números de la figura 2.1.

1. Cuando el equipo cliente se encuentra dentro del alcance del punto de acceso inalámbrico, intenta conectarse a la WLAN que se encuentre activa en este punto y que el Identificador del conjunto de servicios (SSID) haya identificado. El SSID es el nombre de la WLAN que el cliente utiliza para identificar la configuración correcta y el tipo de credencial para esta WLAN en particular.
2. Permite que el cliente autentique el servidor RADIUS; esto significa que el cliente sólo establecerá la sesión con un servidor que cuente con un certificado en el que confíe el cliente.

3. Protege el protocolo de autenticación PAP frente al rastreo de paquetes.
4. La negociación de la sesión TLS genera una clave que el cliente y el servidor RADIUS pueden utilizar a fin de establecer claves maestras comunes (que, a su vez, se usan para generar aquellas claves que van a emplearse para cifrar el tráfico de WLAN).
5. En caso de que el cliente necesitara una dirección IP, podría solicitar el alquiler de un protocolo de configuración dinámica de host (DHCP) de un servidor de la LAN. Una vez se haya asignado la dirección IP, el cliente podrá empezar a comunicarse con normalidad con los restantes sistemas de la red.

A continuación se presentan las actividades a realizar, esto incluyen recurso, responsables tiempo de duración y costo

| No. | Actividad | Recursos | Responsable | Duración | Costo $ | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | Hardware | Software | Recurso Humano | Total |
| 1 | Instalar el Servidor RADIUS | FreeRADIUS versión 1.1.3<br>Manual de instalación FreeRADIUS v. 1.1.3 | Encargado del Proyecto de Educación a Distancia | 3 días | 0 | 0 | 180 | 180 |
| 1.1 | Configurar el Protocolo RADIUS | Manual de instalación FreeRADIUS v. 1.1.3 | Encargado del Proyecto de Educación a Distancia | 2 días | 0 | 0 | 120 | 120 |
| 1.2 | Configurar protocolo 802.1X | Manual de instalación FreeRADIUS v. 1.1.3 | Encargado del Proyecto de Educación a Distancia | 1 día | 0 | | 60 | 60 |
| 2 | Instalar el Servidor LDAP | OpenLDAP versión 2.3.3<br>Manual de instalación OpenLDAP versión 2.3.3 | Encargado del Proyecto de Educación a Distancia | 6 días | 0 | 0 | 360 | 360 |
| 2.1 | Configurar protocolo LDAP | Manual de instalación OpenLDAP versión 2.3.3 | Encargado del Proyecto de Educación a Distancia | 1 día | 0 | 0 | 60 | 60 |

| No. | Actividad | Recursos | Responsable | Duración | Costo $ | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | Hardware | Software | Recurso Humano | Total |
| 2.2 | Crear lista de directorios de clientes del LDAP | Datos Generales de la comunidad universitaria de la Universidad de El Salvador | Encargado del Proyecto de Educación a Distancia | 5 días | 0 | 0 | 300 | 300 |
| 3 | Configurar el Protocolo 802.1X en equipo de Red en la Unidad Responsable del proyecto | Switch y Manual de equipo y Punto de Acceso y manual de equipo | Encargado del Proyecto de Educación a Distancia, 4 Miembros del Equipo de Integración a Eduroam | 4 días | 0 | 0 | 240+320=560 | 560 |
| 4 | Pruebas de Verificación de los Servidores RADIUS y LDAP | Servidor RADIUS, Servidor LDAP, Equipos de Red (Switch y Punto de Acceso) | Encargado del Proyecto de Educación a Distancia, 4 Miembros del Equipo de Integración a Eduroam | 1 día | 0 | 0 | 60+80=140 | 140 |
| 5 | Elaboración políticas de participación exigidas por Eduroam | Políticas de Eduroam | Encargado del Proyecto de Educación a Distancia | 5 días | 0 | 0 | 300 | 300 |

| No. | Actividad | Recursos | Responsable | Duración | Costo $ | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | Hardware | Software | Recurso Humano | Total |
| 6 | Publicación y Distribución de las políticas de participación | Políticas de Participación | Administrador de Pagina Web de la Universidad de El Salvador, 4 Miembros del Equipo de Integración a Eduroam | 10 días | 0 | 0 | 400+800=1200 | 1200 |
| 6.1 | Elaboración de Pagina web informativa | Políticas de Participación, Zonas de cobertura Servicios que brinda Datos del contacto de soporte. | 4 Miembros del Equipo de Integración a Eduroam | 10 días | 0 | 0 | 800 | 800 |
| 7 | Elaboración de manual técnico de equipos de red | Manuales de equipo de red. | 4 Miembros del Equipo de Integración a Eduroam | 6 días | 0 | 0 | 480 | 480 |
| 7.1 | Manual Técnico de Switches | Manuales de equipo de red | 4 Miembros del Equipo de Integración a Eduroam | 3 días | 0 | 0 | 240 | 240 |
| 7.2 | Manual Técnico de Puntos de Acceso | Manuales de equipo de red | 4 Miembros del Equipo de Integración a Eduroam | 3 días | 0 | 0 | 240 | 240 |

| No. | Actividad | Recursos | Responsable | Duración | Costo $ | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | Hardware | Software | Recurso Humano | Total |
| 8 | Elaboración de manual de usuario | Software SecureW2. Parámetros de configuración según sistema operativo. | 4 Miembros del Equipo de Integración a Eduroam | 3 días | 0 | 0 | 240 | 240 |
| 9 | Distribución a los administradores de red de cada facultad los manual técnico y de usuario | Manual Técnico y Manual de Usuario | Administrador de red de cada facultad, Encargado del Proyecto de Educación a Distancia | 5 días | 0 | 0 | 2400+300= 2700 | 2700 |
| 10 | Configuración del protocolo 802.1X en los equipos de red por facultad | Manual Técnico | Administrador de red de cada facultad | 8 días | 0 | 0 | 3840 | 3840 |
| 10.1 | Configuración del Protocolo 802.1X en los Switches de cada facultad | Manual Técnico de switches | Administrador de red de cada facultad | 4 días | 0 | 0 | 1920 | 1920 |

| No. | Actividad | Recursos | Responsable | Duración | Costo $ | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | Hardware | Software | Recurso Humano | Total |
| 10.2 | Configuración del Protocolo 802.1X en los Puntos de Acceso de cada facultad | Manual Técnico de Puntos de Acceso | Administrador de red de cada facultad | 4 días | 0 | 0 | 1920 | 1920 |
| 11 | Pruebas de verificación del funcionamiento de los protocolos en cada facultad | Computadora portátil o de escritorio con cliente 802.1X | Administrador de red de cada facultad, Usuarios finales (Personal Docente, Personal Administrativo y Estudiantes) | 2 días | 0 | 0 | 960 | 960 |
| 12 | Distribución a la comunidad Universitaria el manual de usuario | Pagina Web, Manual de Usuario, SecureW2, papelería | Administrador de red de cada facultad. | 5 días | 0 | | 2400 | 2400 |

| No. | Actividad | Recursos | Responsable | Duración | Costo $ | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | Hardware | Software | Recurso Humano | Total |
| 13 | Configuración de cliente 802.1X | Manual de usuario, Software SecureW2 | Administrador de red de cada facultad, Usuarios finales (Personal Docente, Personal Administrativo y Estudiantes) | 2 días | 0 | 0 | 960 | 960 |
| 14 | Solicitar el Ingreso al programa mundial de usuarios Móviles Eduroam | Solicitud de Ingreso | Encargado del Proyecto de Educación a Distancia | 3 días | 0 | 0 | 180 | 180 |
| **Total** | | | | **95 Días** | **Total** | | **20160** | |

Conclusión:

- Para realizar el plan de implementación será realizara en un periodo de 95 días hábiles, teniendo un costo solo de recurso humano por el personal involucrado de $20,160
- El costo de hardware es de cero debido a que la Universidad de El Salvador tiene al menos un equipo configurable con el protocolo 802.1X en cada una de sus facultades. Ver anexo 9 “Inventario de Hardware de red por facultad de la Universidad de El Salvador”
- El Costo de software es cero ya que el único software que se utiliza es el SecureW2 y este es gratuito.

Responsables:

- 1 Encargado del proyecto de educación a distancia. $1800 mensual - $ 60 Diarios
- 1 Encargados de red de cada facultad (12 Facultades) $1200 Mensual - $ 40 Diarios
- 4 Miembros del Equipo de Integración a Eduroam $ 600 Mensual / Miembro - $ 20 Diarios / Miembro
- 1 Administrador Pagina Web $ 1200 Mensual - $ 40 Diarios.

Los salarios son definidos por cada facultad pero los salarios mensuales mencionados fueron proporcionados por fuentes de la Vicerrectoría Académica En el "Reglamento de Escalafón de Carrera Docente en la Universidad De El Salvador" en el artículo 64 menciona que los salarios se fijarán anualmente por acuerdo de Junta Directiva de cada Facultad, sujeto a ratificación por parte del Consejo Superior Universitario, dentro de las respectivas clases y categorías conforme al artículo 8 del mismo reglamento donde se menciona que el Escalafón de la Carrera Docente comprende niveles jerárquicos, éste último es avalado por la "Ley Orgánica de la Universidad de El Salvador" en el artículo 52. Ver anexo 16 "Reglamento de Escalafón de la Carrera Docente y Ley Orgánica de la Universidad de El Salvador"

A continuación se presenta un diseño detallado de una red supuesta.

**DISEÑO PARA UN PLAN DE IMPLEMENTACIÓN DE EDUROAM.**

**Equipo mínimo necesario para construir el acceso a EDUROAM, en una institución:**

Servidores FreeRADIUS con una tarjeta de red Ethernet.

1. Servidores LDAP con una tarjeta de red Ethernet.
1. Switch Ethernet (12 puertos debería ser suficiente) con soporte 802.1Q y 802.1X.
1. Punto de acceso que soporte la autenticación 802.1X, 802.1Q y cifrado de datos con WPA / TKIP.
1. Cliente 802.1X instalado en los equipos móviles para el sistema operativo que se utilice.

**Diseño para la autenticación al Programa Mundial de Usuarios Móviles eduroam**

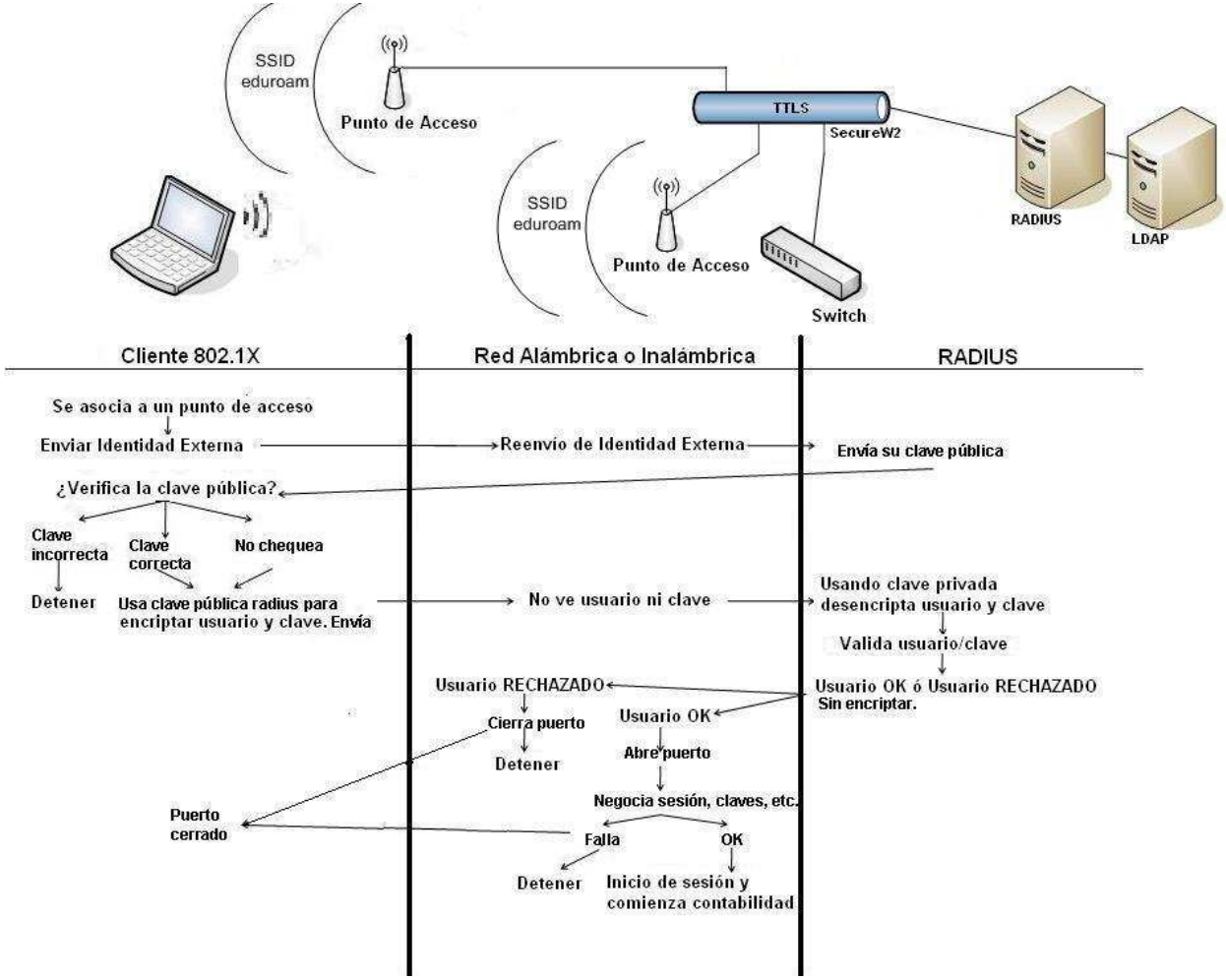



*Figura 4.5.3.2 Proceso de autenticación mostrado en diagrama de secuencia.*

**Diseño de la Red de Datos de la Universidad de El Salvador**

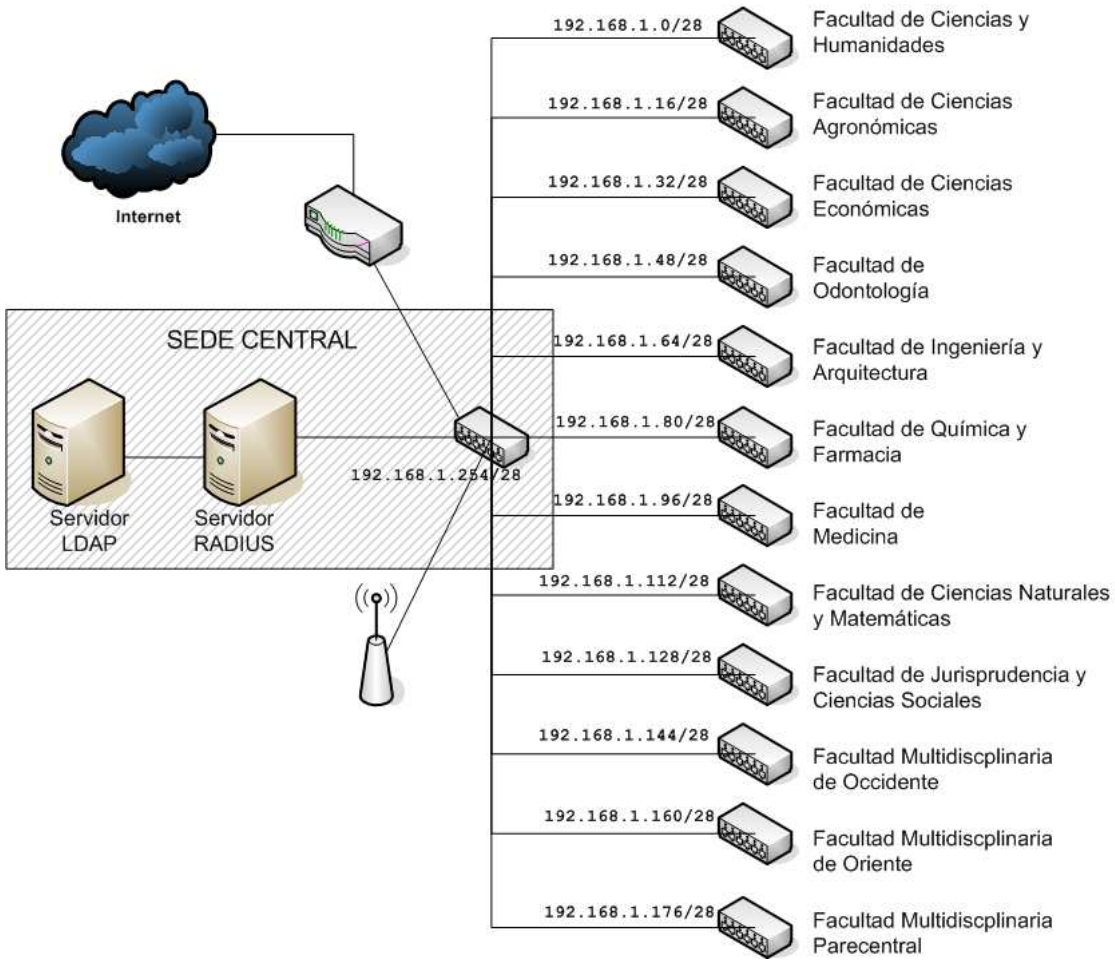



*Figura 4.5.3.3 Diagrama de red de la Universidad de El Salvador*

**Diseño de las direcciones IP por Facultades**

Para nuestro plan de implementación se ha supuesto una dirección IP clase C dicha direeción es 192.168.1.0 (/24) con una máscara de red de 255.255.255.0, ya que la Universidad de El Salvador cuenta con 12 facultades será necesario realizar un subneteo para 16 subredes en donde se abarca las 12 facultades.
A continuación se presenta el subneteo para cada una de las facultades de la Universidad de El Salvador:

| Facultad | Dirección IP | Máscara (/28) |
|---|---|---|
| Ciencias y Humanidades | 192.168.1.0 | 255.255.255.240 |
| Ciencias Agronomías | 192.168.1.16 | 255.255.255.240 |
| Ciencias Económicas | 192.168.1.32 | 255.255.255.240 |
| Odontología | 192.168.1.48 | 255.255.255.240 |
| Ingeniería y Arquitectura | 192.168.1.64 | 255.255.255.240 |
| Química y Farmacia | 192.168.1.80 | 255.255.255.240 |
| Medicina | 192.168.1.96 | 255.255.255.240 |
| Ciencias Naturales y Matemáticas | 192.168.1.112 | 255.255.255.240 |
| Jurisprudencia y Ciencias Sociales | 192.168.1.128 | 255.255.255.240 |
| Multidisciplinaria Occidente | 192.168.1.144 | 255.255.255.240 |
| Multidisciplinaria Paracentral | 192.168.1.160 | 255.255.255.240 |
| Multidisciplinaria Oriente | 192.168.1.176 | 255.255.255.240 |
| No asignadas | 192.168.1.192 | 255.255.255.240 |
| No asignadas | 192.168.1.208 | 255.255.255.240 |
| No asignadas | 192.168.1.224 | 255.255.255.240 |
| No asignadas | 192.168.1.240 | 255.255.255.240 |

*Tabla 1 Resumen de las subredes por facultades***.**

Para cada facultad se ha asignado un número de 16 direcciones IP de las cuales 14 direcciones son utilizables ya que la primera se utiliza para la red y la ultima para broadcast. También se utilizo Máscara de subred con longitud variable (VLSM) para dicho subneteo.

A continuación se detalla dicho subneteo:

Dirección IP: 192.168.1.0
Máscara de red: 255.255.255.0 = 24
Wildcard: 0.0.0.255
Dirección de Red: 192.168.1.0/24
Primera IP Utilizable: 192.168.1.1
Ultima IP Utilizable: 192.168.1.254
Dirección de Broadcast: 192.168.1.255
Cantidad de IPS Utilizables:254

Como se puede observar debido a que solamente son 12 facultades, se tuvo que realizar la transición de la máscara / 24 (255.255.255.0) a / 28 (255.255.255.240), utilizando VLSM. Posteriormente se detalla cada una de las subredes.
Máscara de red: 255.255.255.240 = 28
Wildcard: 0.0.0.15

**Ciencias y Humanidades**
Dirección de Red: 192.168.1.0/28
Primera IP Utilizable: 192.168.1.1
Ultima IP Utilizable: 192.168.1.14
Dirección de Broadcast: 192.168.1.15
Cantidad de IPS Utilizables:14

**Facultad Ciencias Agronomías**
Dirección de Red: 192.168.1.16/28
Primera IP Utilizable: 192.168.1.17
Ultima IP Utilizable: 192.168.1.30
Dirección de Broadcast: 192.168.1.31
Cantidad de IPS Utilizables:14

**Facultad Ciencias Económicas**
Dirección de Red: 192.168.1.32/28
Primera IP Utilizable: 192.168.1.33
Ultima IP Utilizable: 192.168.1.46
Dirección de Broadcast: 192.168.1.47
Cantidad de IPS Utilizables:14

**Facultad Odontología**
Dirección de Red: 192.168.1.48/28
Primera IP Utilizable: 192.168.1.49
Ultima IP Utilizable: 192.168.1.62
Dirección de Broadcast: 192.168.1.63
Cantidad de IPS Utilizables:14

**Facultad Ingeniería y Arquitectura**
Dirección de Red: 192.168.1.64/28
Primera IP Utilizable: 192.168.1.65
Ultima IP Utilizable: 192.168.1.78
Dirección de Broadcast: 192.168.1.79
Cantidad de IPS Utilizables:14

**Facultad Química y Farmacia**
Dirección de Red: 192.168.1.80/28
Primera IP Utilizable: 192.168.1.81
Ultima IP Utilizable: 192.168.1.94
Dirección de Broadcast: 192.168.1.95
Cantidad de IPS Utilizables:14

**Facultad Medicina**
Dirección de Red: 192.168.1.96/28
Primera IP Utilizable: 192.168.1.97
Ultima IP Utilizable: 192.168.1.110
Dirección de Broadcast: 192.168.1.111
Cantidad de IPS Utilizables:14

**Facultad Ciencias Naturales y Matemáticas**
Dirección de Red: 192.168.1.112/28
Primera IP Utilizable: 192.168.1.113
Ultima IP Utilizable: 192.168.1.126
Dirección de Broadcast: 192.168.1.127
Cantidad de IPS Utilizables:14

**Facultad Jurisprudencia y Ciencias Sociales**
Dirección de Red: 192.168.1.128/28
Primera IP Utilizable: 192.168.1.129
Ultima IP Utilizable: 192.168.1.142
Dirección de Broadcast: 192.168.1.143
Cantidad de IPS Utilizables:14

**Facultad Multidisciplinaria Occidente**
Dirección de Red: 192.168.1.144/28
Primera IP Utilizable: 192.168.1.145
Ultima IP Utilizable: 192.168.1.158
Dirección de Broadcast: 192.168.1.159
Cantidad de IPS Utilizables:14

**Facultad Multidisciplinaria Paracentral**
Dirección de Red: 192.168.1.160/28
Primera IP Utilizable: 192.168.1.161
Ultima IP Utilizable: 192.168.1.174
Dirección de Broadcast: 192.168.1.175
Cantidad de IPS Utilizables:14

**Facultad Multidisciplinaria Oriente**
Dirección de Red: 192.168.1.176/28
Primera IP Utilizable: 192.168.1.177
Ultima IP Utilizable: 192.168.1.190
Dirección de Broadcast: 192.168.1.191
Cantidad de IPS Utilizables:14

**No asignadas**
Dirección de Red: 192.168.1.192/28
Primera IP Utilizable: 192.168.1.193
Ultima IP Utilizable: 192.168.1.206
Dirección de Broadcast: 192.168.1.207
Cantidad de IPS Utilizables:14

**No asignadas**
Dirección de Red: 192.168.1.208/28
Primera IP Utilizable: 192.168.1.209
Ultima IP Utilizable: 192.168.1.222
Dirección de Broadcast: 192.168.1.223
Cantidad de IPS Utilizables:14

**No asignadas**
Dirección de Red: 192.168.1.224/28
Primera IP Utilizable: 192.168.1.225
Ultima IP Utilizable: 192.168.1.238
Dirección de Broadcast: 192.168.1.239
Cantidad de IPS Utilizables:14

**No asignadas**
Dirección de Red: 192.168.1.240/28
Primera IP Utilizable: 192.168.1.241
Ultima IP Utilizable: 192.168.1.254
Dirección de Broadcast: 192.168.1.255
Cantidad de IPS Utilizables:14

**Total de Subredes: 16**
Subredes Utilizadas: 12
Subredes Disponibles: 4

**Total de IPS Utilizables: 224**
IPS Utilizadas: 168
IPS Disponibles: 56

**Diseño de las VLAN para el Proyecto eduroam.**

A continuación se detalla un diagrama sobre cómo utilizar las diferentes VLAN para ser usada en eduroam, después se describen sus elementos.

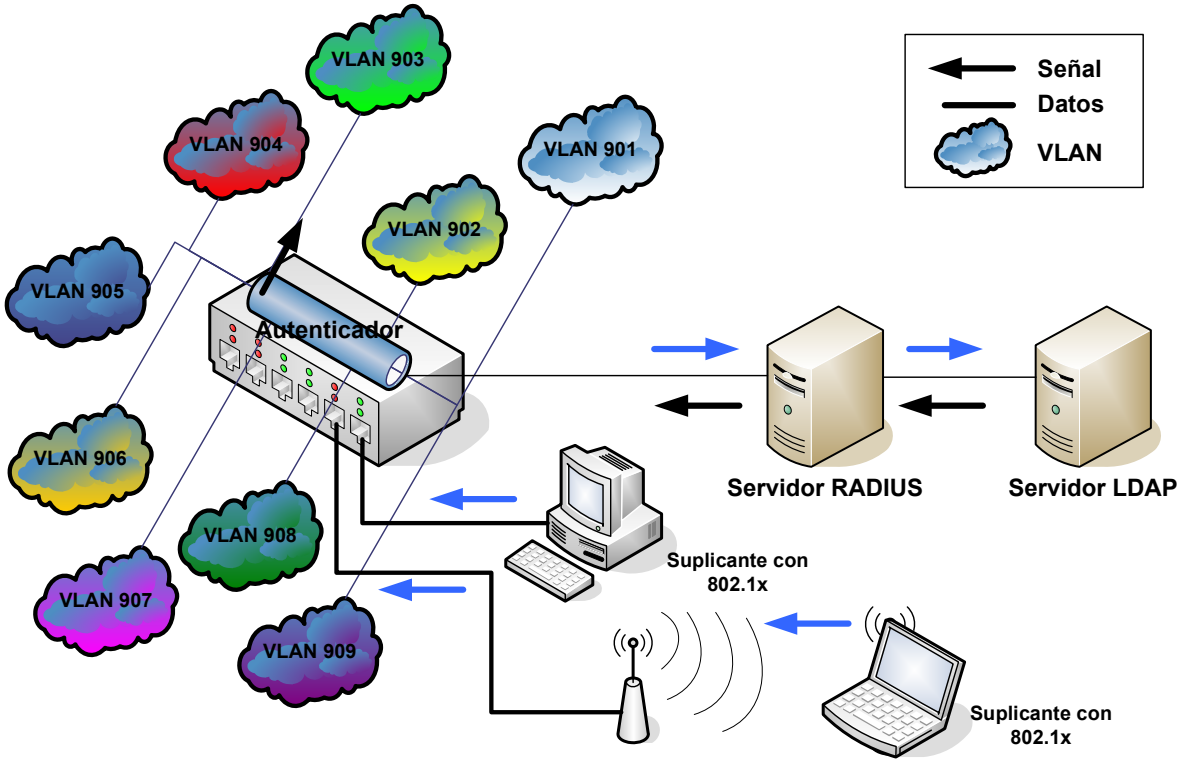



*Figura 4.5.3.4 Diagrama de VLAN*

**VLAN ID´S**

Las VLAN (Redes Virtuales) utilizadas en este documento son sólo un ejemplo y pueden ser modificadas dependiendo de cada una de las necesidades de la institución donde se implemente, si es necesario. El ID (Identificador) de VLAN a utilizar van desde la 901 hasta 909 y sus funciones se describen en el siguiente cuadro:

| VLAN ID | Proponer |
|---|---|
| 901 | VLAN para el acceso a Internet (si fuera necesario) |
| 902 | VLAN para la administración de los Puntos de Acceso |
| 903 | VLAN reservadas para los usuarios de la "eduroam" SSID |
| 904 | VLAN reservadas para los usuarios de la "eduroam-invitado" SSID |
| 905 | VLAN reservadas para los usuarios de una 3 ª (otro_ssid_1X) SSID |
| 906 | VLAN reservadas para los usuarios de un 4 º (otro_ssid _ abierto) SSID |
| 907 | VLAN utilizados para la asignación dinámica VLAN pruebas o otras pruebas |
| 908 | VLAN utilizados para la asignación dinámica VLAN pruebas o otras pruebas |
| 909 | VLAN utilizados para la asignación dinámica VLAN pruebas o otras pruebas |

*Tabla 2 Descripción de las VLAN.*

**Ethernet Switch**

El switch debe estar configurado para permitir la comunicación entre los dispositivos de los puntos de acceso y los recursos disponibles en el banco de pruebas. A continuación hay un cuadro que describe la configuración de VLAN de cada puerto Ethernet en el Switch y lo equipos deben estar conectados a él. Una vez más, el Número de puerto Ethernet es sólo un ejemplo:

| Puerto | Configuración de VLANs (T - Etiquetado; U - Sin etiquetar) | Lo que debería estar conectado a el puerto |
|---|---|---|
| 1 | T (901, 902, 903, 904, 905;906, 907, 908, 909) | Enrutador |
| 2 | U (902) | FreeRADIUS |
| 3 | U (904) | Servidor WEB / Portal WEB. |
| 4 | U (901) | Servidor WEB / Portal WEB -- Accesos autorizados a Internet para la VPN / basado en portal WEB para los usuarios (Sitios Cautivos). |
| 5 | U / T (?) | Pueden utilizarse para la depuración de cualquier VLAN? |
| 6 | T (902, 903, 904, 905, 906;907, 908, 909) | El punto de acceso puede estar configurado para que todas las VLAN's sean etiquetados |
| 7 | U (902) T (903, 904, 905, 906;907, 908, 909) | El punto de acceso puede estar configurado para que la VLAN administrativa este sin etiquetar. |

*Tabla 3 Propuesta de diseño para la configuración de un Switch Ethernet***.**

**Enrutador**

El enrutador debe tener una interfaz Ethernet donde deberá tener configurado en sus sub-interfaces a cada una de las VLAN (901 a 909), y con un servidor DHCP (con la excepción de la VLAN 901) en cada una de ellas.

Las direcciones IP de cada interfaz, con servidor DHCP tienen un rango, las configuraciones se describen en la siguiente tabla. También hay una columna con el nombre ó SSID que debe ser estáticamente asignado en el punto de acceso si aplica.

| Interfaz | 802.1Q Etiqueta | Dirección IP por Interfaz | DHCP Pool | Serán asignadas a Punto de Acceso del SSID |
|---|---|---|---|---|
| FE0.901 | 901 | Alguna dirección IP pública | N / A | |
| FE0.902 | 902 | 192.168.0.254 | 192.168.0.0/24 | |
| FE0.903 | 903 | 192.168.1.254 | 192.168.1.0/24 | eduroam |
| FE0.904 | 904 | 192.168.2.254 | 192.168.2.0/24 | eduroam-invitado |
| FE0.905 | 905 | 192.168.3.254 | 192.168.3.0/24 | otro_ssid_1X |
| FE0.906 | 906 | 192.168.4.254 | 192.168.4.0/24 | otro_ssid _ abierto |
| FE0.907 | 907 | 192.168.5.254 | 192.168.5.0/24 | |
| FE0.908 | 908 | 192.168.6.254 | 192.168.6.0/24 | |
| FE0.909 | 909 | 192.168.7.254 | 192.168.7.0/24 | |

*Tabla 4 Propuesta de diseño para la configuración de un Enrutador***.**

**Puntos de Acceso**

Los puntos de acceso deberían estar configurado con los siguientes SSID y VLAN's / IP 's

| 802.1Q Etiqueta | dirección IP de la Interfaz | SSID |
|---|---|---|
| 902 (*) | 192.168.0. <any> (**) | N / A |
| 903 | N / A | eduroam |
| 904 | N / A | eduroam-invitado |
| 905 | N / A | otro_ssid_1X (***) |
| 906 | N / A | otro_ssid _ abierto (***) |
| 907 | N / A | N / A |
| 908 | N / A | N / A |
| 909 | N / A | N / A |
| | | |

*Tabla 5 – Propuesta de diseño para la configuración de un Punto de Acceso*.

(*) - Pueden ser etiquetados o sin etiquetar dependiendo de las necesidades de Punto de Acceso (**) - Debe estar configurado como un cliente en el servidor RADIUS. (***) - No puede ser configurado si no se admite la prueba por equipos

**FreeRADIUS**

El servidor debe estar configurado para aceptar autenticación 802.1X. Los métodos de autenticación más comunes son los PEAP y TTLS por lo que es recomendable que para cada Punto de Acceso esté configurado con al menos uno de estos dos métodos.

Debe haber al menos 2 tipos diferentes de usuarios 802.1X habilitados en el Servidor RADIUS: Uno que debe estar conectado a la VLAN estática asignada para el SSID eduroam (VLAN 903) y el otro que debe ser asignado a otra VLAN (907 a 909) para la fase final que es la autenticación.

Normalmente la asignación de VLAN dinámicas se logra mediante el envío de paquetes de acceso, el cual contiene 3 atributos con la información de la VLAN para cada usuario autenticado, dicha información se muestra continuación:

***Tunnel-Type = "1: VLAN"***
***Tunnel-Medium-Type = "1:802"***
***Tunnel-Private-Group-ID = "1: VLANID"***

## ESTRUCTURA FINAL SUGERIDA PARA LA IMPLEMENTACION A EDUROAM

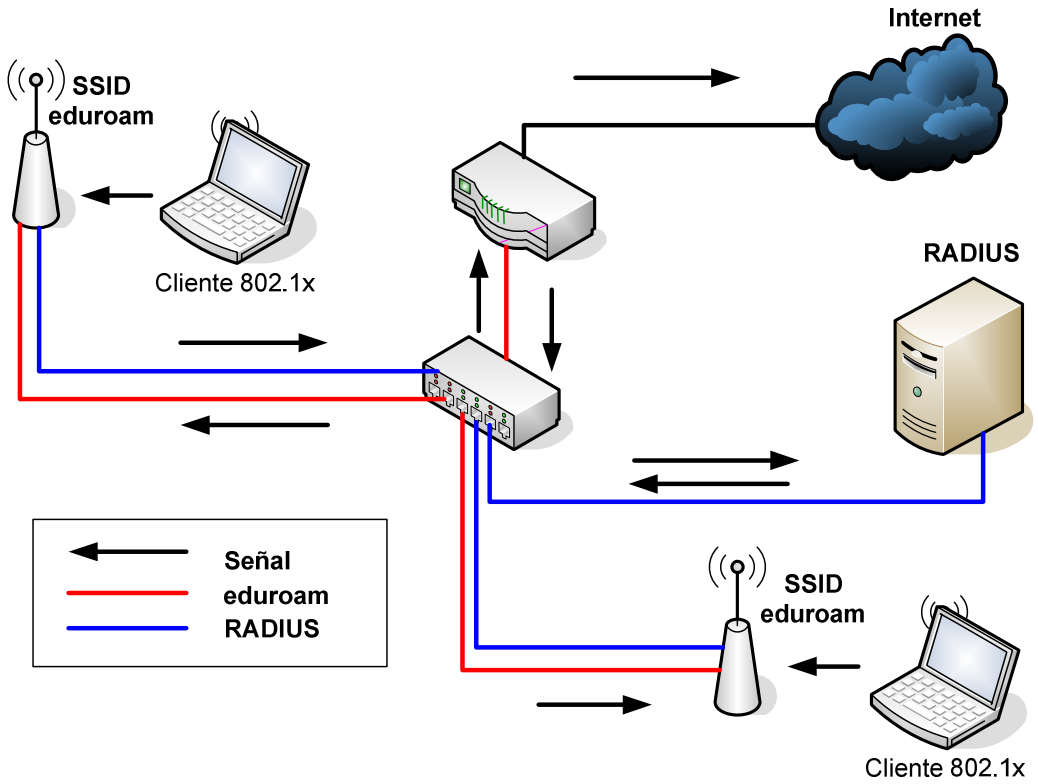



*Figura 4.5.3.5 Diagrama de conexión a eduroam*

**EDUROAM**

Para poder acceder a la red se requiere de autenticación IEEE 802.1X (TTLS, pero debería trabajar con otros métodos EAP). En esta red el usuario debe autenticarse a nivel de la capa 2 (Enlace de datos), a través de un Punto de Acceso con soporte 802.1X.

# *CONCLUSIONES*

Al finalizar nuestro proyecto podemos concluir que:

1. La seguridad de la red inalámbrica existente en la Universidad de El Salvador se considera vulnerable a ataques, debido a que se utilizan sitios cautivos para la autenticación de los usuarios.
2. Todas las facultades de la Universidad de El Salvador poseen al menos un equipo de red inalámbrico con compatibilidad con el estándar 802.1X.
3. La adquisición del equipo no representa problemas o limitantes ya que se pueden incluir como "Compras de Libre Gestión" ya que su costo no sobrepasa los 80 salarios mínimos que es una de las condiciones de la Ley de Adquisiciones y Contrataciones de la Administración Pública, LACAP
4. La Universidad cuenta con todos los elementos que requiere la arquitectura de RADIUS
    a. Servidor LDAP
    b. Equipo de red configurable del protocolo 802.1X
5. En base a la cobertura actual de la red inalámbrica se identificaron áreas en las que es conveniente la colocación de nuevos equipos para garantizar el roaming o movilidad, estás se presentan en los planos de cobertura propuestos.
6. Se presentó información para dar a los administradores las herramientas suficientes para que de una manera sencilla se pueda conectar a Eduroam. Es evidente que en cada una de las instituciones las arquitecturas de la red varían mucho, es por esto que es tarea del administrador de la red de cada institución diseñar una solución para lograr conectarse a Eduroam.
7. Se describió de una manera resumida y con ejemplos cada uno de los elementos necesarios para comprender los pasos necesarios para ser en usuario habilitado de Eduroam.
8. La solución planteada permitirá que usuarios provenientes de otras instituciones miembros del programa puedan ingresar y hacer uso de la red de la Universidad de El Salvador con las credenciales de su institución origen.
9. La solución planteada permitirá que usuarios locales al visitar otros países e instituciones miembros del programa puedan ingresar y hacer uso de la red de la institución visitada con las credenciales de su institución origen.
10. La solución planteada permitirá que la Universidad de El Salvador se convierta en la primera universidad en América en ser miembro de la red académica mundial de usuarios móviles Eduroam

# *RECOMENDACIONES*

Después de haber realizado ésta etapa del proyecto se recomienda:

Integrar a la Universidad de El Salvador al programa mundial de usuarios móviles Eduroam ya que además de darle prestigio a la misma se tendrán los siguientes beneficios:

1. Se reducirán los riesgos asociados a la interceptación del tráfico de red.
2. Se evitará el Acceso a la red de usuarios no autorizados y uso no autorizado de la red.
3. Le dará a los usuarios facilidad de uso de la red.
4. El acceso a la red no se limita a computadoras portátiles, sino también tiene compatibilidad con amplio número de dispositivos inalámbricos.
5. Es escalable ya que permitirá a los administradores de las facultades incrementar la cobertura por la sencillez y bajo costo.
6. Uso de sistemas y protocolos estándares de la industria.
7. Facilitará la administración, monitorización y auditoría de acceso a la red.

# *GLOSARIO DE TERMINOS*

- 802.11i Estándar IEEE que define la seguridad en las redes 802.11
- 802.1X Protocolo de la IEEE para asegurar las redes cableadas mediante autenticación y TLS
- AAA Servidor de Autenticación, Autorización y Auditoria (Authentication Authorization Accounting)
- AAD Datos de Autenticación Adicionales (Aditional Authentication Data)
- AP Punto de Acceso inalámbrico (Access Point)
- ARP Protocolo de Resolución de Direcciones (Address Resolution Protocol)
- AS Servidor de Acceso (Access Server)
- Back-end Programa que efectúa las acciones de fondo
- Beacon Anuncios del AP para especificar su existencia y otra informacion
- Broadcast Transmisión a todos los elementos de la red
- BSS Grupo de Servicios Básicos (Basic Service Grupo)
- CA Autoridad de Certificación (Certificate Authority)
- CBC Encadenamiento de bloques cifrados (Cipher-block chaining)
- CCM Contador con modo de encadenamiento de bloques cifrados (Counter Cipher-block chaining mode)
- CCMP Protocolo CTR con CBC-MAC
- CHAP Protocolo de Autenticación por desafío (Challenge Authentication Protocol)
- CRC Comprobación de redundancia cíclica (Cyclic Redundancy Check)
- CSMA/CD Sensor de señal de conexión para múltiple acceso con detección de colisiones (Carrier Sense Multiple Access / Colision Detection)
- CTR Registro contador (Count Register)
- DA Dirección de Destino (Destination Address)
- dB Decibeles
- DES Estándar de cifrado de datos (Data Encryption Standard)
- DHCP Protocolo de configuración dinámica de Host (Dynamic Host Configuration Protocol)
- DoS Ataques de Denegación de Servicio (Denial of Services)
- DSSS Espectro de extensión de secuencia directa (Direct Sequence Spread Spectrum)
- EAP Protocolo de Autenticación Extensible (Extensible Authentication Protocol)
- eavesdroppers Espías de información, atacantes pasivos
- EMI Interferencia Electromagnética (Electromagnetic Interference)
- ESS Grupo de Servicios Extendidos (Extended Service Group)

- ETSI Instituto Europeo de Estándares en Telecomunicaciones (European Telecommunications Standards Institute)
- FCC Comité Federal de Comunicaciones (Federal Communications Commission)
- FCS Secuencia de comprobación de trama (Frame Check Sequence)
- FHSS Modulación por saltos de frecuencia (Frequency Hopping Spread Spectrum)
- FIPS Norma de Procesamiento de la Información Federal
- GTK Llave temporal de grupo (Grup Key entre las STAs y el AP)
- HMAC Suma de chequeo para corroborar la integridad de los datos (Keyed-Hashing for Message Authentication)
- Host Servidor que provee servicios a otros ordenadores
- HUB Bifurcador de redes cableadas
- IBSS Grupo de Servicios Básicos Independiente (Independent Basic Service Grupo)
- ICV Valor de comprobación de integridad (Integrity Check Value)
- ID Identidad
- IEEE Instituto de Ingenieros Eléctricos y Electrónicos (Institute of Electrical and Electronics)
- IETF Fuerza de Trabajo de la Ingeniería de Internet (Internet Engieneering Task Force)
- IPSec Seguridad en el protocolo IP
- ISM Industrial, Científica y Médica (Industrial Scientific and Medical)
- IV Vector de Inicialización (Initialization Vector)
- KCK Llave de cifrado (Key Encription Key)
- LAN Red de Área Local (Local Area Network)
- MAC Control de Acceso al Medio (Medium Access Control)
- MAN Redes de área metropolitana (Metropolitan Area Network)
- Management frames Tramas de gestión
- man-in-the-middle Ataque de interceptar la conexión, pasandola a través de una tercera persona
- Mbps Mega-bits por segundo
- MD5 Suma de chequeo para corroborar la integridad de los datos (Message Digest 5)
- MIB Administración de la Base de Informacion (Management Information Base)
- MIC Código de integridad del mensaje (Message Integrity Code)
- MK Llave Maestra (Master Key)
- MPDUs Unidades de datos del protocolo MAC (MAC protocol data units)
- MSDUs Unidades de datos del servicio MAC (MAC service data units)
- multicast Envío de información a varios puntos

- NAT — Traducción de Direcciones de Red (Network Address Translation)
- NIC — Tarjeta para Interfaz de Red (Network Interface Card)
- NIST — Instituto Nacional de Normas y Tecnologías (National Institute of Standards and Technology)
- NTP — (Network Time Protocol) es un protocolo de internet para sincronizar los relojes de los sistemas informáticos a través de ruteo de paquetes en redes con latencia variable. NTP utiliza UDP como su capa de transporte, usando el puerto 123. Está diseñado para resistir los efectos de la latencia variable.
- OFDM — Multiplexión por División de Frecuencia Ortogonal (Orthogonal Frequency Division Multiplexing)
- OSI — Interconexión de Sistemas de Abiertos (Open Systems Interconnection)
- PAE — Entidad de acceso al puerto (Port Access Entity IEEE 802.1X)
- PAP — Protocolo de Autenticación de Claves (Password Authentication Protocol)
- payload — Datos útiles de las tramas o paquetes
- PCM — Modulación de Código de Pulso (Pulse Code Modulation)
- peer-to-peer — Conexión punto a punto
- PID — Un archivo PID contiene el número de identificación de procesos (process identification number) que se almacena en un lugar específico en la ubicación del sistema de ficheros permitiendo así que otros programas sepan el pid de un script en funcionamiento. Los daemons o demonios necesitan el PID de los scripts que se ejecutan actualmente en segundo plano para enviarles señales de llamada. Los Demonios utiliza el término señal para decirle a un script cuando ejecutarse al enviarse una orden de parada.
- PMK — Pares de llave compartida (Pairwise Master Key)
- PN — Número de paquete (Package Number)
- PPP — Protocolo Punto a Punto (Point-to-Point Protocol)
- PPTP — Protocolo de entunelamiento punto a punto (Point to Point Tuneling Protocol)
- PRNG — Generador de números pseudoaleatorios de WEP (Pseudo Random Number Generator)
- PSK — Llave precompartida (Pre-Shared Key)
- QoS — Calidad de Servicio
- RADIUS — Servicio de Autenticación de usuarios telefónicos remotos (Remote Authentication Dial-In User Service (IETF RFC 2865)
- RC4 — Código de cifrado utilizado por WEP
- Roaming — Movimiento entre APs sin perder conectividad
- RSN — Seguridad de Red Robusta (Robust Secure Network)

- RSNA — Asociación de seguridad de red robusta (Robust Security Network Association )
- SA — Dirección de Fuente (Source Address)
- sniffer — Capturador de trafico especifico en la red
- SOHO — Oficina Pequeña Oficina en Casa (Small Office Home Office)
- spoofing — Engaño
- SSID — Identificador de Grupo de Servicios Extendidos (Service Group Identifier)
- STAs — Estaciones de trabajo inalámbricas (Stations)
- TIM — Mapa de indicación de tráfico (Traffic Indication Map)
- TKIP — Protocolo de Integridad de Llave Temporal (Temporary Key Integrity Protocol)
- TKs — Llaves temporales (Temporal Keys)
- TLS — Seguridad en la Capa de Transporte (Transport Layer Security)
- TSC — Contador de Secuencia (Sequence Counter) o TKIP
- UDP — Protocolo de data gramas de usuario (User Datagram Protocol)
- unicast — Envío de información a solo un punto
- VLANs — LANs Virtuales
- VPN — Red Virtual Privada (Virtual Private Network)
- WECA — Alianza de Compatibilidad de Redes Inalámbricas (Wireless Ethernet Compatibility Alliance)
- WEP — Privacidad Equivalente con la Alambrada (Wired Equivalent Privacy)
- Wi-Fi — Fidelidad Inalámbrica (Wireless Fidelity)
- Wi-Fi Alliance — Anteriormente WECA, certifica la interoperabilidad de equipos inalámbricos
- WLAN — Red Inalámbrica de Área Local (Wireless Local Area Network)
- WPA — Acceso Protegido Wifi (Wifi Protected Access)
- WPA2 — Acceso Protegido Wifi 2 (Wifi Protected Access 2)
- write-only — Sólo escritura

# 5 BIBLIOGRAFÍA

## 5.1 Libros


1. Muller, Nathan J. "Wireless A to Z", McGraw-Hill, 2003
2. Fleck, Bob. "802.11 Security", O'Reilly, 2002
3. Matthew, Gast. "802.11 Wireless Networks: The Definitive Guide", O'Reilly, 2002
4. Flickenger, Rob. "Wireless Hacks", O'Reilly, 2003
5. Aspinwall, Jim. Installing, "Troubleshooting, and Repairing Wireless Networks", McGraw-Hill, 2003
6. Nichols, Randall K. "Wireless Security", McGraw-Hill, 2002
7. Ohrtman, Frank. "Wi-Fi Handbook: Building 802.11b Wireless Networks", McGraw-Hill, 2003
8. Miller, Stewart S. "Wi-Fi Security", McGraw-Hill, 2003.
9. Akin, Devin. "CWAP Certified Wireless Analysis Professional Official Study Guide (Exam PW0-300)", McGraw-Hill/Osborne, 2004.
10. Planet3 Wireless, Inc "Certified Wireless Network Administrator, Official Study Guide", Planet3 Wireless 2002.
11. Scott, Charlie. "Virtual Private Networks", Second Edition, O'Reilly, 1999
12. T. Kersting (DFN, main editor), P. Dekkers (SURFnet), L. Guido (FCCN), S. Papageorgiou (NTUA/GRNET), Janos Mohacsi (NIIF/HUNGARNET), R. Papez (ARNES), M. Milinovic (CARNet/Srce), D. Penezic (CARNet/Srce), J. Rauschenbach (DFN), K. Wierenga (SURFnet), S. Winter (RESTENA), T. Wolniewicz (Nicolaus Copernicus University, Torun), JRA5 group. Deliverable DJ5.1.5,2:Inter-NREN Roaming Infrastructure and Service Support Cookbook – Second Edition. 17 Agosto 2007.
13. 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 et al. Inter-NREN Roaming Architecture: Description and Development Items. GEANT2 Deliverable DJ5.1.4. September 2006.


## 5.2 Páginas web


1. ANSI/IEEE Std 802.11, 1999 Edition (R2003). "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", http://standards.ieee.org/getieee802/802.11.html
2. IEEE Std 802.1X-2001. "Port-Based Network Access Control", http://standards.ieee.org/getieee802/802.11.html
3. IEEE Std 802.11i-2004. "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications", http://standards.ieee.org/getieee802/802.11.html
4. Oliva Fora, Pau. "(In) seguridad en redes 802.11b", http://pof.eslack.org/writings/In-Seguridad%20en%20redes%20802.11b.pdf

5. Martínez Ponce, Daniel. “Seguridad en Redes WIRELESS Bajo Linux”, http://hackitectura.net/jornadas_telematicas/Charla_Seguridad_seco_baja.pdf
6. Seguridad en Eduroam http://sdi.uc3m.es/sdiario2/article.php?sid=231 http://www.alcancelibre.org/staticpages/index.php/como-freeRADIUS-basico
7. http://www.freeRADIUS.org/
8. http://tools.ietf.org/html/rfc2058
9. http://tools.ietf.org/html/rfc2059
10. http://www.osmosislatina.com/LDAP/configuracion.htm
11. http://dns.bdat.net/documentos/LDAP/#id2918899
12. http://www.Eduroam.es/politica.es.php

# *ANEXOS*

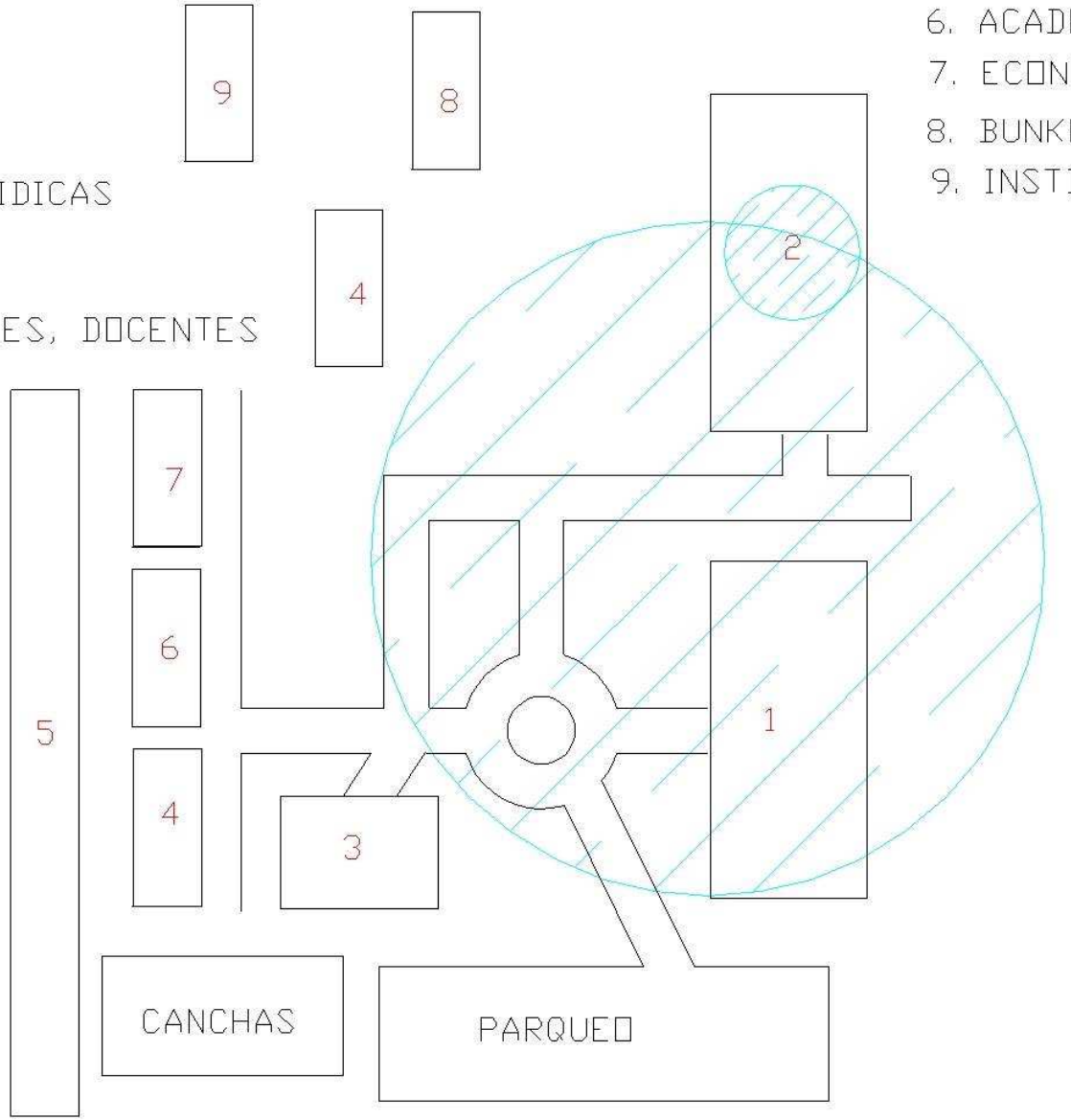
# *ANEXO 1 PLANO ACTUAL DE UBICACIÓN DE PUNTOS DE ACCESO Y RADIOS DE COBERTURA CAMPUS CENTRAL*


ESCUELA REPUBLICA
DE ESPAÑA

# *ANEXO 2 PLANO ACTUAL DE UBICACIÓN DE PUNTOS DE ACCESO Y RADIOS DE COBERTURA CAMPUS MULTIDISCIPLINARIA OCCIDENTAL*

# UNIVERSIDAD DE EL SALVADOR
# FACULTAD MULTIDISCIPLINARIA DE OCCIDENTE

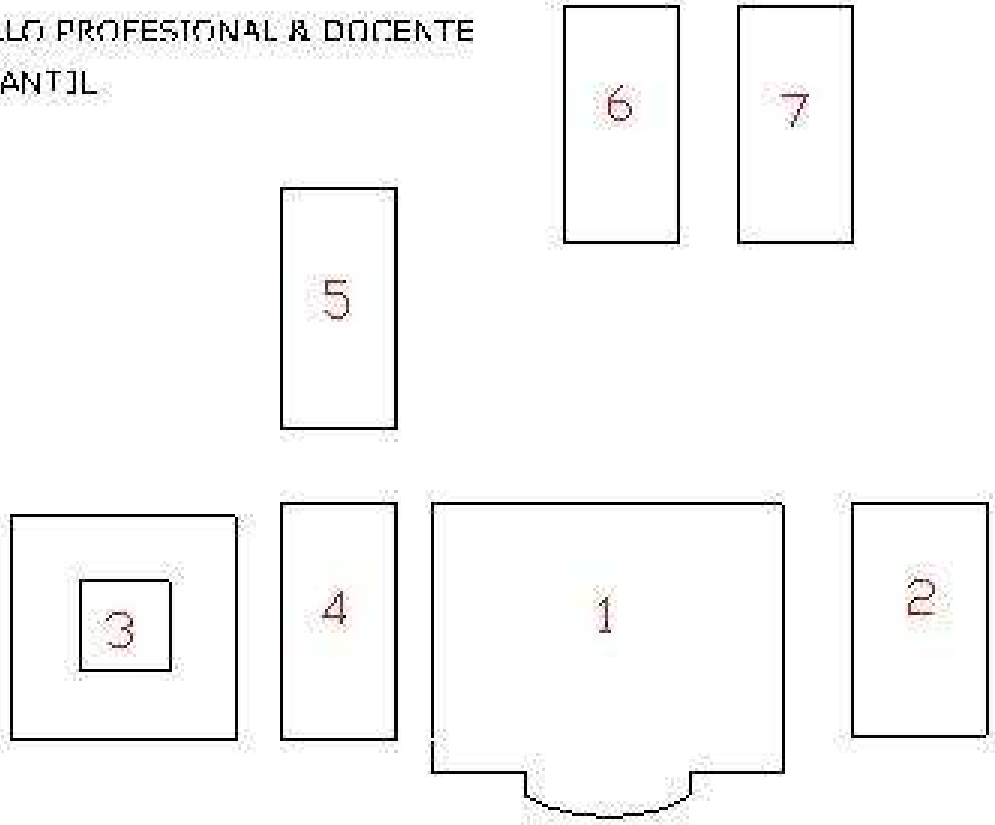
1. BIBLIOTECA
2. MEDICINA
3. CIENCIAS JURIDICAS
4. AULAS
5. USOS MULTIPLES, DOCENTES
6. ACADEMICA / BIOLOGIA
7. ECONOMIA
8. BUNKER
9. INSTITUTO DEL AGUA



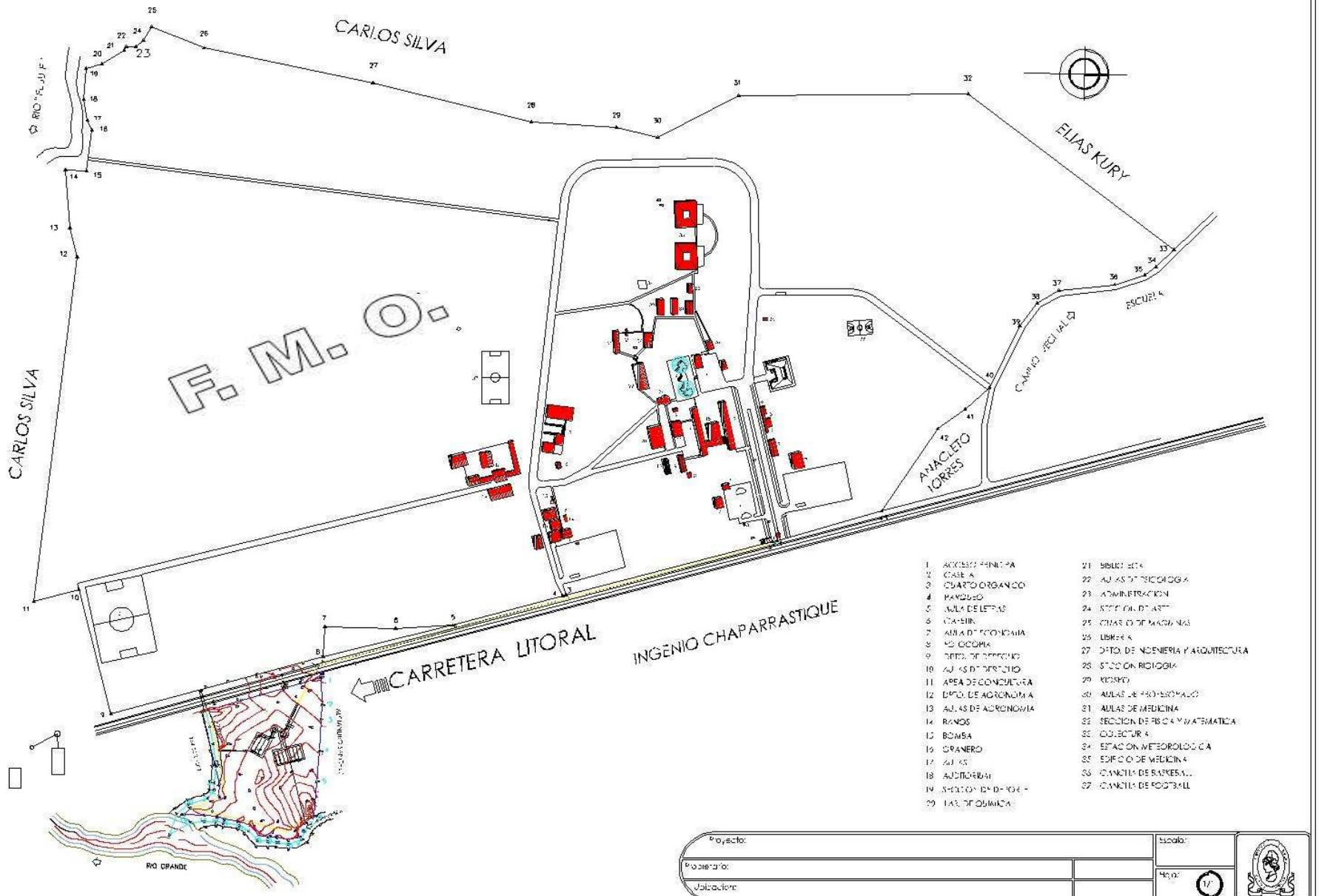
# *ANEXO 3 PLANO ACTUAL DE UBICACIÓN DE PUNTOS DE ACCESO Y RADIOS DE COBERTURA CAMPUS MULTIDISCIPLINARIA PARACENTRAL*

# UNIVERSIDAD DE EL SALVADOR
# FACULTAD MULTIDISCIPLINARIA PARACENTRAL

1. EDIFICIO AULAS
2. BIBLIOTECA, ADMINISTRATIVOS & MAESTROS
3. CENTRO DE DESARROLLO PROFESIONAL & DOCENTE
4. ASOCIACION ESTUDIANTIL
5. PROYECCION
6. SERVICIO SOCIAL
7. POST-GRADO



# *ANEXO 4 PLANO ACTUAL DE UBICACIÓN DE PUNTOS DE ACCESO Y RADIOS DE COBERTURA CAMPUS MULTIDISCIPLINARIA ORIENTAL*




| | | |
|---|---|---|
| Proyecto: | | Escala: |
| Propietario: | | Hoja: 1/ |
| Ubicacion: | | |

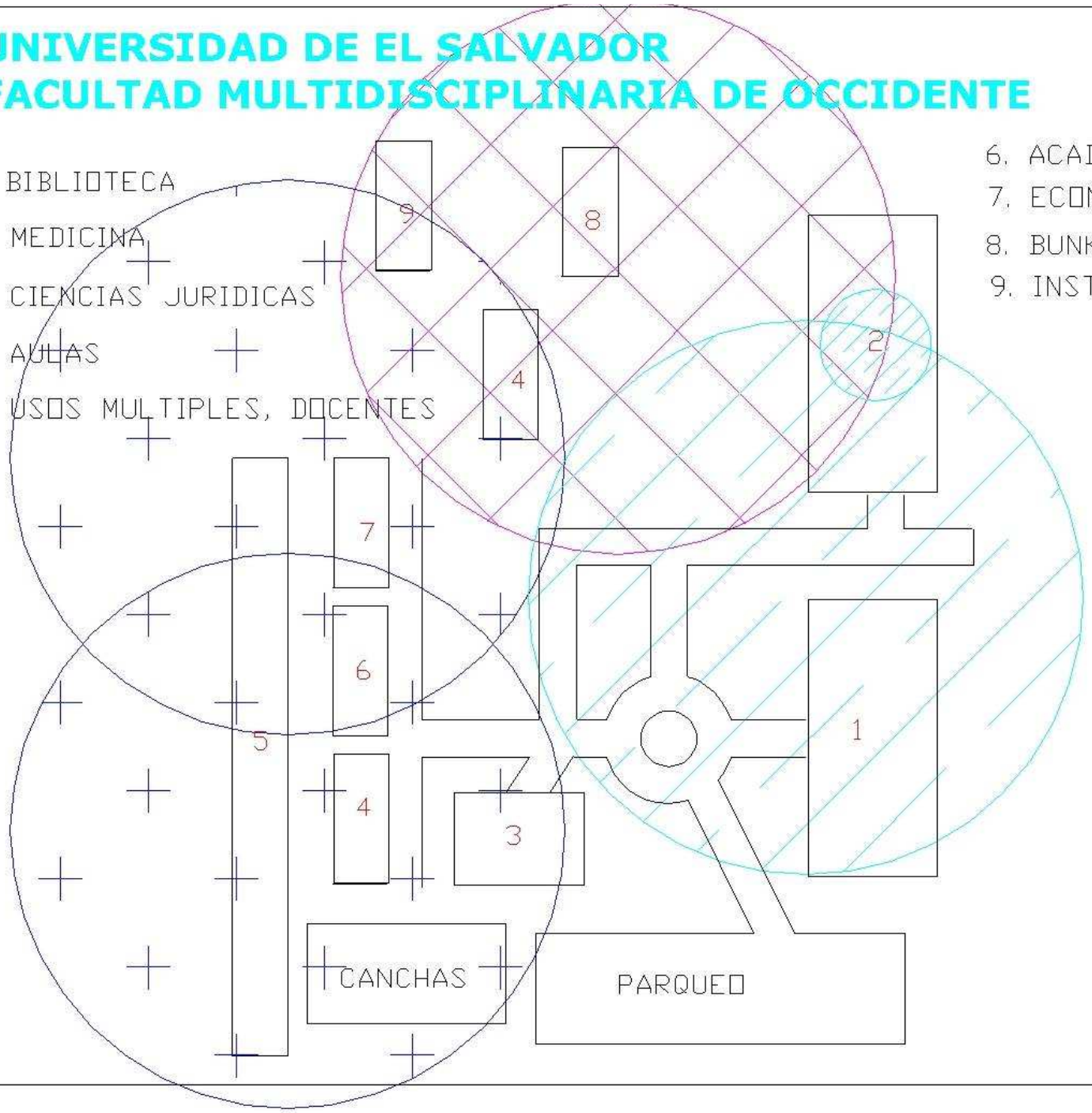
# *ANEXO 5 PLANO PROPUESTO DE UBICACIÓN DE PUNTOS DE ACCESO Y RADIOS DE COBERTURA CAMPUS CENTRAL*


ESCUELA REPUBLICA
DE ESPAÑA

# *ANEXO 6 PLANO PROPUESTO DE UBICACIÓN DE PUNTOS DE ACCESO Y RADIOS DE COBERTURA CAMPUS MULTIDISCIPLINARIA OCCIDENTAL*

# UNIVERSIDAD DE EL SALVADOR
# FACULTAD MULTIDISCIPLINARIA DE OCCIDENTE

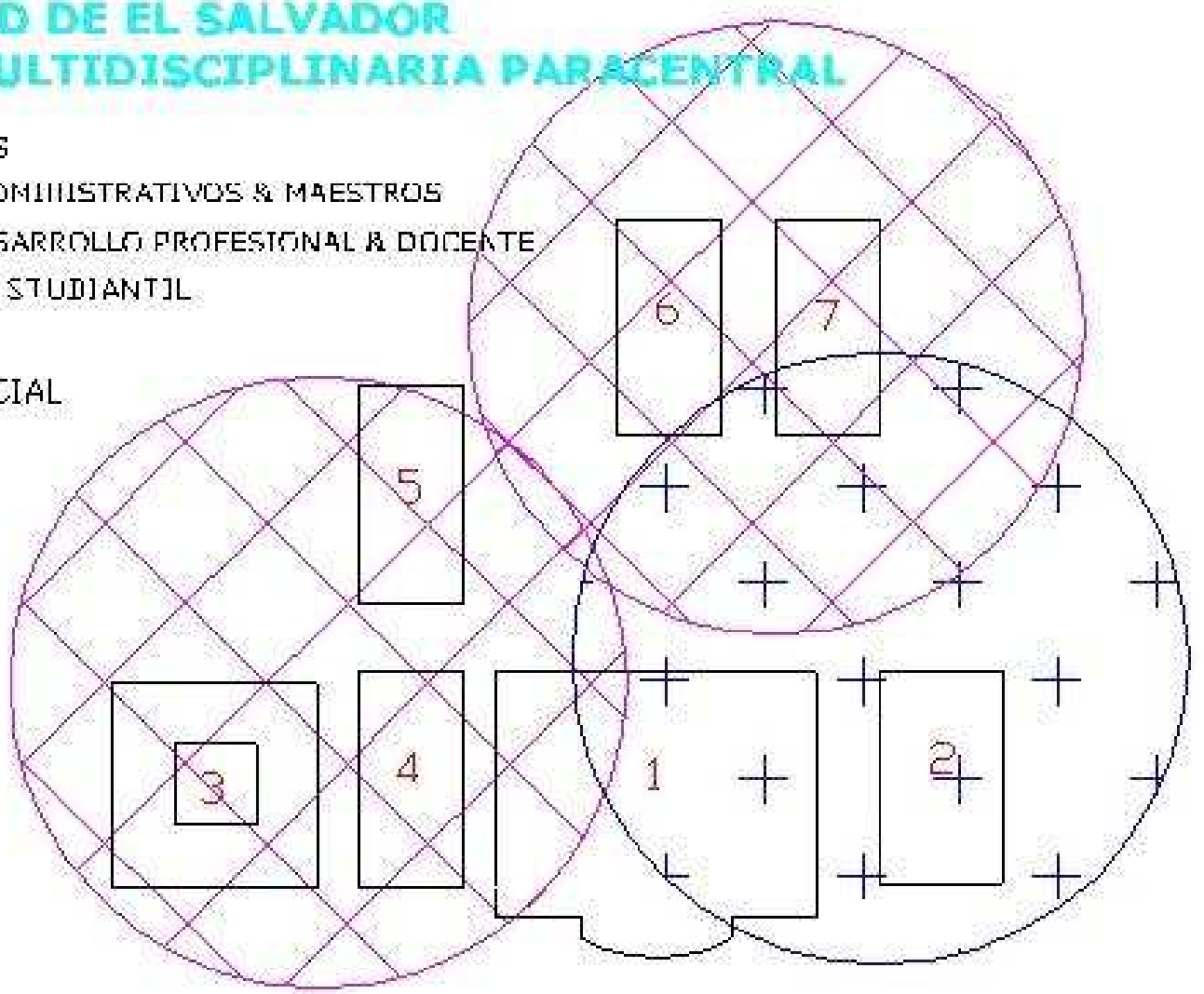
1. BIBLIOTECA
2. MEDICINA
3. CIENCIAS JURIDICAS
4. AULAS
5. USOS MULTIPLES, DOCENTES
6. ACADEMICA / BIOLOGIA
7. ECONOMIA
8. BUNKER
9. INSTITUTO DEL AGUA



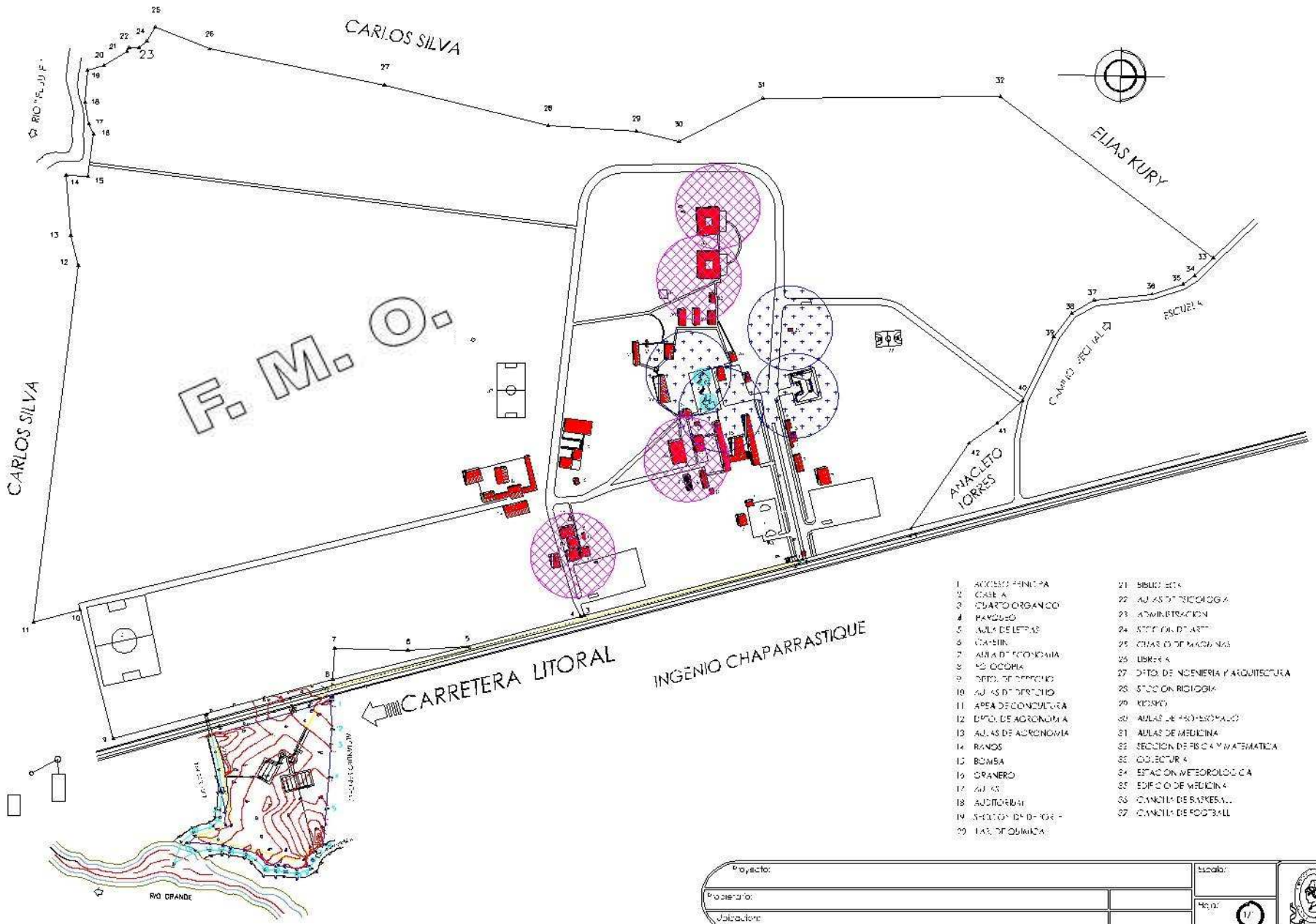
# *ANEXO 7 PLANO PROPUESTO DE UBICACIÓN DE PUNTOS DE ACCESO Y RADIOS DE COBERTURA CAMPUS MULTIDISCIPLINARIA PARACENTRAL*

# UNIVERSIDAD DE EL SALVADOR
# FACULTAD MULTIDISCIPLINARIA PARACENTRAL

1. EDIFICIO AULAS
2. BIBLIOTECA, ADMINISTRATIVOS & MAESTROS
3. CENTRO DE DESARROLLO PROFESIONAL & DOCENTE
4. ASOCIACION ESTUDIANTIL
5. PROYECCION
6. SERVICIO SOCIAL
7. POST-GRADO



# *ANEXO 8 PLANO PROPUESTO DE UBICACIÓN DE PUNTOS DE ACCESO Y RADIOS DE COBERTURA CAMPUS MULTIDISCIPLINARIA ORIENTAL*


CARLOS SILVA
ELIAS KURY
F. M. O.
CARLOS SILVA
ANACLETO TORRES
CAMINO VECINAL
ESCUELA
CARRETERA LITORAL
INGENIO CHAPARRASTIQUE
RIO GRANDE
1 ACCESO PEATONAL
2 CASETA
3 CUARTO ORGANICO
4 PARQUEO
5 AULAS DE LETRAS
6 CAFETIN
7 AULAS DE ECONOMIA
8 FOTOCOPIA
9 DEPTO. DE DERECHO
10 AULAS DE DERECHO
11 AREA DE CONCULTURA
12 DEPTO. DE AGRONOMIA
13 AULAS DE AGRONOMIA
14 BANOS
15 BOMBA
16 GRANERO
17 AULAS
18 AUDITORIUM
19 SECCION DE BIOLOGIA
20 LABS. DE QUIMICA
21 BIBLIOTECA
22 AULAS DE PSICOLOGIA
23 ADMINISTRACION
24 SECCION DE ARTE
25 CUARTO DE MAQUINAS
26 LIBRERIA
27 DEPTO. DE INGENIERIA Y ARQUITECTURA
28 SECCION BIOLOGIA
29 KIOSKO
30 AULAS DE PROFESORADO
31 AULAS DE MEDICINA
32 SECCION DE FISICA Y MATEMATICA
33 COLECTURIA
34 ESTACION METEOROLOGICA
35 EDIFICIO DE MEDICINA
36 CANCHA DE BASKETBALL
37 CANCHA DE FOOTBALL
Proyecto:
Propietario:
Ubicacion:
Escala:
Hoja:
1/

# *ANEXO 9 INVENTARIO DE HARDWARE DE RED POR FACULTAD DE LA UNIVERSIDAD DE EL SALVADOR*

A continuación se muestra un cuadro resumen del hardware por facultades

| EQUIPO DE RED | OCCIDENTAL | PARACENTRAL | ORIENTAL | CIENCIAS Y HUMANIDADES | CIENCIAS NATURALES Y MATEMÁTICAS | ECONOMÍA | JURISPRUDENCIA Y CIENCIAS SOCIALES | BIBLIOTECA CENTRAL | MEDICINA | ODONTOLOGÍA | QUÍMICA Y FARMACIA | CIENCIAS AGRONÓMICAS | INGENIERÍA Y ARQUITECTURA | TOTAL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Hub ENCORE modelo ESH-717 | | | | | | | | | | 1 | | 1 | | 2 |
| Modem ASMI-52 (Telecom) | 2 | 2 | 2 | | | | | 1 | | | | | | 7 |
| Pix Cisco 515E Firewall | 1 | | 1 | | | | | | | | | | | 2 |
| Pix Cisco 525E Firewall | | | | | | | | 1 | | | | | | 1 |
| Router Cisco 1721 series | | | | | | | | 1 | | | | | | 1 |
| Router Cisco 1800 series | 1 | | 1 | | | | | | | | | | | 2 |
| Router Cisco 2118 series | | 1 | | | | | | | | | | | | 1 |
| Router Cisco 2800 series | 1 | | | | | | | | | | | | | 1 |
| Router Lynsys Inalámbrico modelo WRT54GL | 1 | | | | | | | | | | | | | 1 |
| **SWITCHES** | | | | | | | | | | | | | | |
| Switch 3COM modelo 3C17304 | 6 | | 3 | | | | | | | | | | | 9 |
| Switch 3COM modelo 3C16471 | | | | | | | | | | | | 1 | | 1 |
| Switch 3Com Switch 4500 modelo 3CR17561-91 | | | | | | | | | | | | | 8 | 8 |
| Switch Allied Telesyn modelo AT-8024GB | 3 | | 2 | | | | | | | | | | | 5 |

| EQUIPO DE RED | OCCIDENTAL | PARACENTRAL | ORIENTAL | CIENCIAS Y HUMANIDADES | CIENCIAS NATURALES Y MATEMÁTICAS | ECONOMÍA | JURISPRUDENCIA Y CIENCIAS SOCIALES | BIBLIOTECA CENTRAL | MEDICINA | ODONTOLOGÍA | QUÍMICA Y FARMACIA | CIENCIAS AGRONÓMICAS | INGENIERÍA Y ARQUITECTURA | TOTAL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **SWITCHES** | | | | | | | | | | | | | | |
| Allied Telesyn modelo AT-8026T | | | | | | | | | | | | | 1 | 1 |
| Allied Telesyn modelo AT-8326B | | | | | | | | | | | | | 1 | 1 |
| Allied Telesyn modelo AT-9816GB | | | | | | | | 1 | | | | | | 1 |
| Allied Telesyn modelo AT-AT8000S48 | | | | | | | | | | 1 | | | | 1 |
| Allied Telesyn modelo AT-FH724SW | | | | | | | | 2 | | | | | | 2 |
| Allied Telesyn modelo AT-FS708LE | | | | | | | | | | 2 | | 1 | | 3 |
| Allied Telesyn modelo AT-FS716L | | 8 | | 6 | | | | | | 4 | | | | 18 |
| Allied Telesyn modelo AT-FS724i | | | | | | | | | | 1 | | | | 1 |
| Allied Telesyn modelo AT-FS724L | 12 | | 3 | | 2 | 2 | | | | 1 | | 2 | 14 | 36 |
| Allied Telesyn modelo AT-GS924GB | | | | | | | | | | | 3 | | | 3 |
| Allied Telesyn modelo Rapier 24i | | 1 | 3 | 6 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 1 | 5 | 24 |
| C-NET modelo CNSH1600 | | | | | 15 | | | | | | | 1 | | 16 |
| DELL Power Conectec 3348 | | | | | | | | | 1 | | | | | 1 |
| D-LINK modelo DES-1008D | | | | | | | | | | | 5 | 1 | | 6 |
| D-LINK modelo DES-1016D | | | | | 1 | 1 | 3 | | | | | | | 5 |

| EQUIPO DE RED | OCCIDENTAL | PARACENTRAL | ORIENTAL | CIENCIAS Y HUMANIDADES | CIENCIAS NATURALES Y MATEMÁTICAS | ECONOMÍA | JURISPRUDENCIA Y CIENCIAS SOCIALES | BIBLIOTECA CENTRAL | MEDICINA | ODONTOLOGÍA | QUÍMICA Y FARMACIA | CIENCIAS AGRONÓMICAS | INGENIERÍA Y ARQUITECTURA | TOTAL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **SWITCHES** | | | | | | | | | | | | | | |
| D-LINK modelo DES-1024D. | | 3 | 3 | 1 | 1 | 4 | 2 | 1 | 6 | 1 | 2 | 2 | 5 | 31 |
| LG modelo LS3116A | | | | | 4 | | 3 | | | | | 1 | 1 | 9 |
| NEXXT modelo NW223NXT29 | | | | | 2 | | | | | | | | | 2 |
| **PUNTOS DE ACCESO** | | | | | | | | | | | | | | |
| Allied Telesyn modelo AT WA1004G | | | | | | | | | | | 1 | | | 1 |
| CISCO modelo AIR-AP1231G-A-K9 | | | | | | | | | | | 1 | | 1 | 2 |
| D-Link modelo DWL2100AP | 3 | | 1 | | | 2 | | 2 | | | | | 3 | 11 |
| 3Com OfficeConnect Wireles 54Mbps 11g. | | | | | | | | | | | | | 18 | 18 |

## Características de equipo de hardware de La Universidad de El Salvador

| Facultad | Edificio | Equipo | Configurable con el Protocolo 802.1X | |
|---|---|---|---|---|
| | | | SI | NO |
| Multidisciplinaria Occidental | Usos Múltiples | MODEM ASMI-52 | | X |
| | | Router Cisco 1800 series | X | |
| | | Router Cisco 2800 series | X | |
| | | Pix Cisco 515E Firewall | | X |
| | | Switches Allied Telesyn modelo AT-8024GB | X | |
| | | Switches 3 COM modelo 3C17304 | X | |
| | | Switches Allied Telesyn modelo AT-FS724L | | X |
| | | Router Lynsys Inalámbrico modelo WRT54GL | X | |
| | | Puntos de Acceso D-Link modelo DWL2100AP | X | |
| | Medicina | Switches Allied Telesyn modelo AT-FS724L | | X |
| | | Punto de Acceso D-Link modelo DWL2100AP | X | |
| | Instituto del agua | Switches Allied Telesyn modelo AT-FS724L | | X |
| | Ciencias Jurídicas | Switches Allied Telesyn modelo AT-FS724L | | |
| | Academica / Biologia | Switches Allied Telesyn modelo AT-8024GB | X | |
| | | Switches 3 COM modelo 3C17304 | X | |
| | | Switches Allied Telesyn modelo AT-FS724L | | X |
| Multidisciplinaria Paracentral | Administrativo/ Biblioteca/ Maestros | MODEM ASMI-52 | | X |
| | | Router Cisco 2118 series | | X |
| | | Switch Allied Telesyn modelo Rapier 24i | X | |
| | | Switches Allied Telesyn modelo AT-FS716L | | X |
| | | Switches D-LINK DES-1024D | | X |
| | Aulas | Switches Allied Telesyn modelo AT-FS716L | | X |

| Facultad | Edificio | Equipo | Configurable con el Protocolo 802.1X | |
|---|---|---|---|---|
| | | | SI | NO |
| Multidisciplinaria Oriente | Administrativo | MODEM ASMI-52 | | X |
| | | Router Cisco 1800 series | X | |
| | | Pix Cisco 515E Firewall | | X |
| | | Switch Allied Telesyn modelo Rapier 24i | X | |
| | | Switches Allied Telesyn modelo AT-8024GB | X | |
| | | Switches 3 COM modelo 3C17304 | X | |
| | | Switches Allied Telesyn modelo AT-FS724L | | X |
| | | Punto de Acceso D-Link modelo DWL2100AP | X | |
| | Biblioteca | Switch Allied Telesyn modelo Rapier 24i | X | |
| | | Switches Allied Telesyn modelo AT-FS724L | | X |
| | Centro de Computo | Switch Allied Telesyn modelo Rapier 24i | X | |
| | | Switches D-LINK DES-1024D | | X |
| Ciencias Y Humanidades | Administrativo | Switch Allied Telesyn modelo Rapier 24i | X | |
| | | Switch Allied Telesyn modelo AT-FS716L | | X |
| | | Switch D-LINK DES-1024D | | X |
| | Idiomas/ Filosofía | Switch Allied Telesyn modelo Rapier 24i | X | |
| | | Switch Allied Telesyn modelo AT-FS716L | | X |
| | Periodismo/ Letras | Switch Allied Telesyn modelo Rapier 24i | | X |
| | | Switch Allied Telesyn modelo AT-FS716L | | X |
| | Psicología/ Educación | Switch Allied Telesyn modelo Rapier 24i | X | |
| | | Switch Allied Telesyn modelo AT-FS716L | | X |
| | Escuela de Artes | Switch Allied Telesyn modelo Rapier 24i | X | |
| | | Switch Allied Telesyn modelo AT-FS716L | | X |
| | Colectaría y CENIUS | Switch Allied Telesyn modelo Rapier 24i y AT-FS716L | X | |

| Facultad | Edificio | Equipo | Configurable con el Protocolo 802.1X | |
|---|---|---|---|---|
| | | | SI | NO |
| Ciencias Naturales y Matematicas | Física/ Matemática | Switch Allied Telesyn modelo Rapier 24i | X | |
| | | Switch Allied Telesyn modelo AT-FS724L | | X |
| | | Switches C-NET modelo CNSH1600 | | X |
| | | Switches NEXXT modelo NW223NXT29 | | X |
| | | Hug LG modelo LS3116A | | X |
| | | Switch D-LINK modelo DES-1016D | | X |
| | | Switch D-LINK modelo DES-1024D | | X |
| | Administrativo/ Química | Switch Allied Telesyn modelo AT-FS724L | | X |
| | | Switches C-NET modelo CNSH1600 | | X |
| | Biología | Switches C-NET modelo CNSH1600 | | X |
| | | Switches LG modelo LS3116A | | X |
| Economia | Académica Central | Switch Allied Telesyn modelo Rapier 24i | X | |
| | | Switch Allied Telesyn modelo AT-FS724L | | X |
| | | Switch D-LINK modelo DES-1024D | | X |
| | | Punto de Acceso D-Link modelo DWL2100AP | X | |
| | Administrativo | Switch Allied Telesyn modelo AT-FS724L | | X |
| | | Switch D-LINK modelo DES-1024D | | X |
| | | Switch D-LINK modelo DES-1016D | | X |
| | Centro de Computo/ Clases/ Proyección Social/ ASECE | Switches D-LINK modelo DES-1024D | | X |
| | | Punto de Acceso D-Link modelo DWL2100AP | X | |

| Facultad | Edificio | Equipo | Configurable con el Protocolo 802.1X | |
|---|---|---|---|---|
| | | | SI | NO |
| Jurisprudencia y ciencias Sociales | Académica/ Biblioteca/ Centro de Computo | Switch Allied Telesyn modelo Rapier 24i | X | |
| | | Switches D-LINK modelo DES-1024D | | X |
| | | Switches LG modelo LS3116A | | X |
| | | Switch D-LINK modelo DES-1016D | | X |
| | Relaciones Internacionales | Switches D-LINK modelo DES-1016D | | X |
| Biblioteca Central | Biblioteca Central | MODEM ASMI-52 | | X |
| | | Router Cisco 1721 series | X | |
| | | Pix Cisco 525E Firewall | | X |
| | | Switch Allied Telesyn modelo AT-9816GB | X | |
| | | Switch Allied Telesyn modelo Rapier 24i | X | |
| | | Switches Allied Telesyn modelo AT-FH724SW | | X |
| | | Switch D-LINK modelo DES-1024D | | X |
| | | Puntos de Acceso D-Link modelo DWL2100AP | X | |
| Medicina | Medicina | Switch Allied Telesyn modelo Rapier 24i | X | |
| | | Switch DELL Power Conectec 3348 | X | |
| | | Switches D-LINK modelo DES-1024D | | X |
| Odontologia | Administrativo | Switches Allied Telesyn modelo Rapier 24i | X | |
| | | Switch Allied Telesyn modelo AT-FS724i | | X |
| | | Switch D-LINK DES-1024D | | X |
| | | Switches Allied Telesyn modelo AT-FS716L | | X |
| | | Switches Allied Telesyn modelo AT-FS708LE | | X |
| | | Hub ENCORE modelo ESH-717 | | X |

| Facultad | Edificio | Equipo | Configurable con el Protocolo 802.1X | |
|---|---|---|---|---|
| | | | SI | NO |
| Odontología | Clínicas | Switch Allied Telesyn modelo AT-FS724L | | X |
| | | Switch Allied Telesyn modelo AT-AT8000S48 | X | |
| Quimica Y Farmacia | Administrativo | Switch Allied Telesyn modelo Rapier 24i | X | |
| | | Switches Allied Telesyn modelo AT-GS924GB | | X |
| | | Switches D-LINK DES-1008D | | X |
| | | Switches D-LINK DES-1024D | | X |
| | | Punto de Acceso Allied Telesyn modelo AT WA1004G | X | |
| | | Punto de Acceso ENCORE modelo AIR-AP1231G-A-K9 | X | |
| | Laboratorios | Switches D-LINK DES-1008D | | X |
| Agronomia | Unidad de Computo | Switch Allied Telesyn modelo Rapier 24i | X | |
| | | Switches Allied Telesyn modelo AT-FS724L | | X |
| | | Switch 3COM modelo 3C16471 | X | |
| | | Hub ENCORE modelo ESH-717 | | X |
| | Planificación | Switch C-NET modelo CNSH1600 | | X |
| | Aulas/ Postgrado | Switch Allied Telesyn modelo AT-FS708LE | | X |
| | | Switches D-LINK DES-1008D | | X |
| | Planta Piloto | Switch LG modelo LS3116A | | X |
| | Profesores | Switches D-LINK modelo DES-1024D | | X |
| Ingenieria y Arquitectura | Académica | Switch Allied Telesyn modelo Rapier 24i | X | |
| | | Switch Allied Telesyn modelo AT-8326B | | X |
| | | Switch Allied Telesyn modelo AT-FS724L | | X |
| | | Switch D-LINK modelo DES-1024D | | X |
| | | Punto de Acceso CISCO modelo AIR-AP1231G-A-K9 | X | |

| Facultad | Edificio | Equipo | Configurable con el Protocolo 802.1X | |
|---|---|---|---|---|
| | | | SI | NO |
| Ingenieria y Arquitectura | Electrica | Switch Allied Telesyn modelo Rapier 24i | X | |
| | | Switches Allied Telesyn modelo AT-FS724L | | X |
| | | Switch D-LINK modelo DES-1024D | | X |
| | Civil | Switch Allied Telesyn modelo Rapier 24i | X | |
| | | Switches Allied Telesyn modelo AT-FS724L | | X |
| | | Switch D-LINK modelo DES-1024D | | X |
| | Biblioteca | Switch Allied Telesyn modelo Rapier 24i | X | |
| | | Switch Allied Telesyn modelo AT-FS724L | | X |
| | Ciencias Basicas | Switch Allied Telesyn modelo Rapier 24i | X | |
| | | Switches Allied Telesyn modelo AT-FS724L | | X |
| | | Switch D-LINK modelo DES-1024D | | X |
| | Sistemas/ Industrial | Switch Allied Telesyn modelo AT-8026T | X | |
| | | Switches Allied Telesyn modelo AT-FS724L | | X |
| | | Punto de Acceso CISCO modelo AIR-AP1231G-A-K9 | X | |
| | Arquitectura | Switch Allied Telesyn modelo AT-FS724L | | X |
| | | Switches D-LINK modelo DES-1024D | | X |
| | Mecanica | Switches Allied Telesyn modelo AT-FS724L | | X |
| | | Switch LG modelo LS3116A | | X |

# *ANEXO 10 COTIZACIÓN Y ADQUISICIÓN DE EQUIPO DE RED*

| Cotización de Equipo | A | B | C |
|---|---|---|---|
| **Access Point** | | | |
| CISCO AIR-AP1231G-A-K9 Wireless Access Point | 569.99 | | |
| Punto de Acceso D-Link modelo DWL2100AP | | 99.99 | |
| Linksys WAP54G Wireless-G Access Point | | | 64.99 |
| | | | |
| **Antenas Exteriores** | | | |
| 2.4GHz Outdoor Omn Antenna | 191.37 | | |
| 8dBi Omni-Directional Outdoor Wireless Antenna | | 24.99 | |
| 7 dBi Desktop Omni Range Extender WiFi Antenna for Linksys | | | 10.95 |
| | | | |
| **Soportes de Antena** | | | |
| MOUNTING BRACKET FOR OUTDOOR ANTENNA | 49.97 | 49.97 | |
| Universal Antenna Mount | | | 12.95 |
| **Total ($)** | **811.33** | **174.95** | **88.89** |

La inversión[28] que necesitan para tener al menos un punto de acceso por facultad oscila entre $811.33 y $88.89. Esta inversión no es obligatoria ya que son las autoridades de cada facultad deben decidir si desean implementar el programa en sus respectivas facultades. Esto no representa un problema para que la Universidad de El Salvador se integre al programa Eduroam ya que necesita al menos que una facultad proporcione el servicio de autenticación de usuarios para efectuar dicha integración.
Los montos de adquisición del equipo englobarían la compra como de Libre Gestión.

[28] Precios obtenidos en Intcomex

# *ANEXO 11 MANUAL DE USUARIO*

# *MANUAL DE USUARIO*

## INDICE

# 1 Introducción

Este manual está diseñado para ayudar a los usuarios a configurar correctamente el software SecureW2. La configuración correcta de este software es indispensable para que los usuarios puedan conectarse exitosamente a Eduroam.

El manual contempla la utilización de diferentes sistemas operativos como Windows XP, Windows Vista y Windows 2000. Además, se incluyen capturas de pantallas útiles para el seguimiento de la configuración paso a paso, desde las instrucciones para la obtención de este software hasta el logro exitoso de la conexión a Eduroam.

# 2 Objetivo

Este manual tiene como objetivo guiar paso a paso en la configuración del software SecureW2 a todos los usuarios autorizados que deseen acceder a la red académica mundial de usuarios móviles Eduroam, desde la red de la Universidad de El Salvador.

# 3 Obtener el cliente para Windows.

Tiene que instalar el software cliente que se encargará de nuestra autenticación de forma segura. En nuestro caso se utilizara el SecureW2, por ser gratuito y estar suficientemente probado.

**Desde el 27 de abril del 2008 está disponible una nueva versión de SecureW2 (EapSuite 1.0.6).** Aconsejamos esta versión para los usuarios de Windows 2000, XP y Vista . Puede descargar esta versión directamente desde Internet en http://www.SecureW2.com.

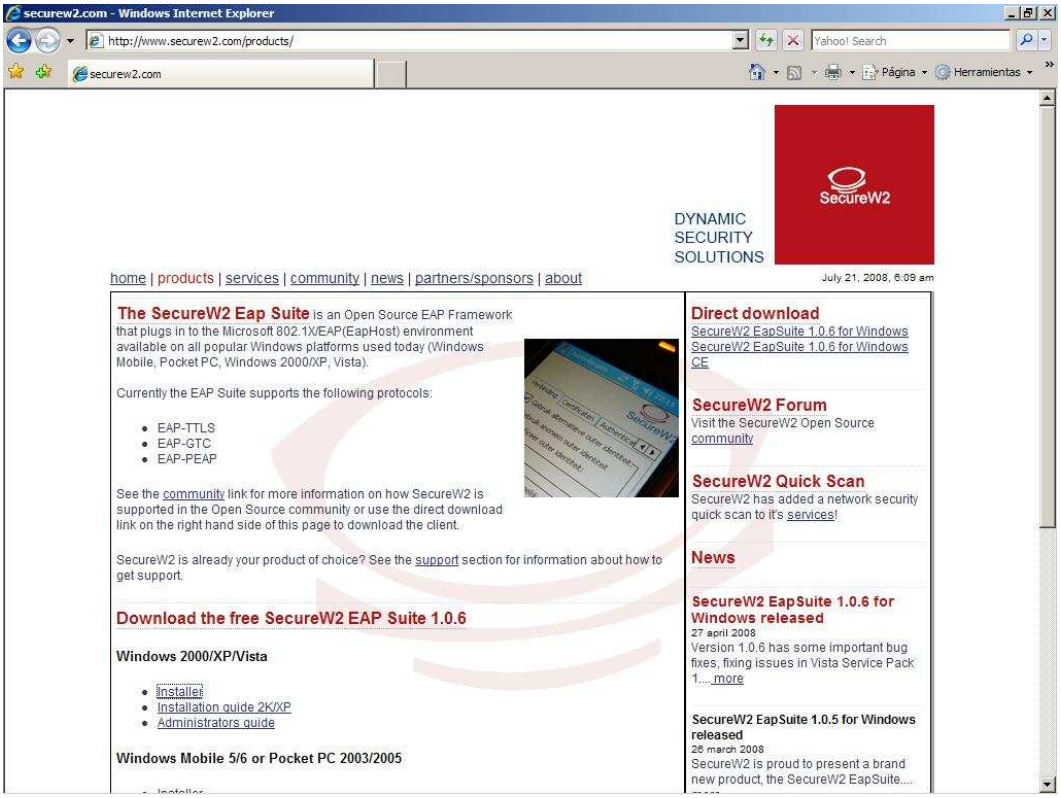



*Figura 3.1 Sitio de descarga del software SecureW2*

1. Si nos fijamos en la parte inferior esta el enlace donde dice installer, damos un click y descargaremos el SecureW2 EAP Suite 1.0.6 para Windows 2000/XP/VISTA.

2. Donde nos aparecerá la descarga la cual nos preguntara qué queremos hacer si Abrir, Guardar o Cancelar:


*Figura 3.2 Pantalla de opciones de descarga del software*

3. Si presionamos el botón cancelar este cancelara la descarga del programa

4. Si presionamos el botón Abrir el programa comenzara a descomprimir con el compresor que tengamos instalado en nuestra maquina.

5. Si presionamos el botón Guardar este nos preguntara donde queremos guardar el instalador en la maquina. Una vez descargado y guardado en una carpeta del equipo se descomprime con el compresor que tengamos instalado en nuestro equipo hasta obtener cinco ficheros como los de la imagen:


*Figura 3.3 Pantalla de confirmación de descarga del software*

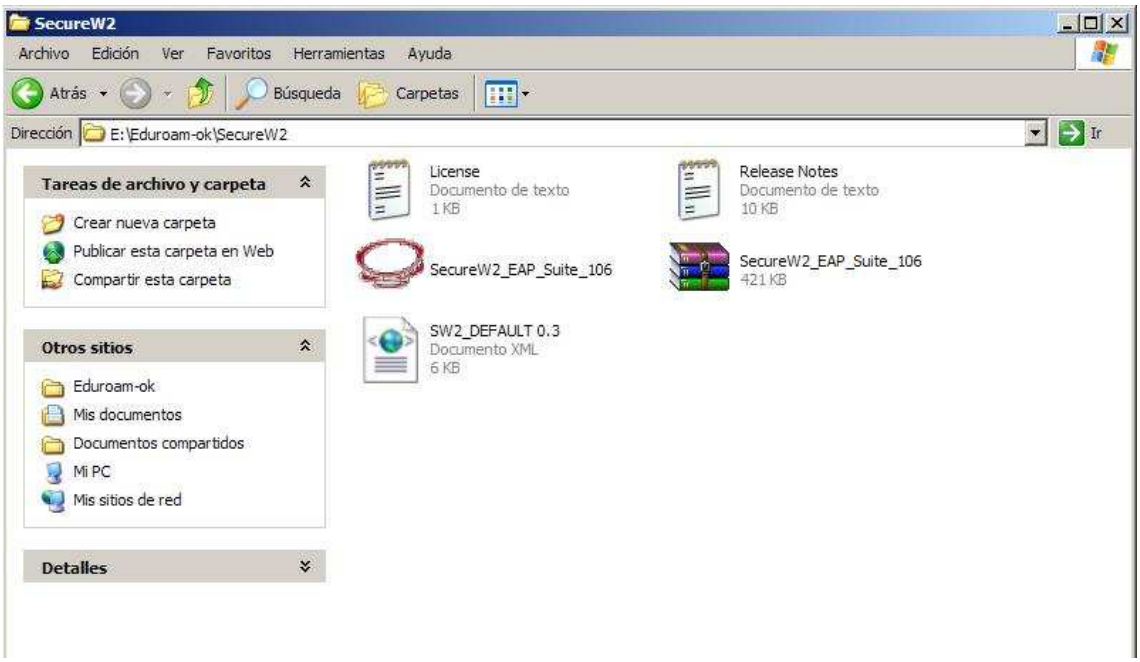



*Figura 3.4 Archivo de instalación comprimido*

# 4 Instalación y configuración del SecureW2.

## 4.1 Instalar el cliente SecureW2

1. Darle doble click al archivo ejecutable SecureW2_EAP_Suite_106. Seguiremos las instrucciones del asistente.


*Figura 4.1.1 Pantalla de selección de idioma de instalación del software*

2. Si presionamos el botón Cancel este cancelara la instalación
3. Seleccionamos el lenguaje que queremos instalar el programa
4. Presionamos el botón OK para continuar con la instalación y nos mostrara la ventana siguiente.

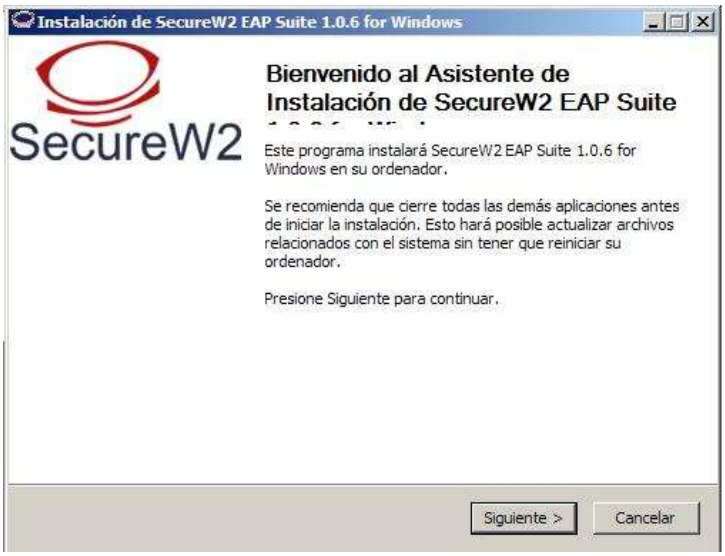



*Figura 4.1.2 Pantalla de asistente de configuración*

5. Si presionamos el botón Cancel este cancelara la instalación
6. Presionamos el botón Siguiente para continuar con la instalación este nos mostrara la ventana siguiente

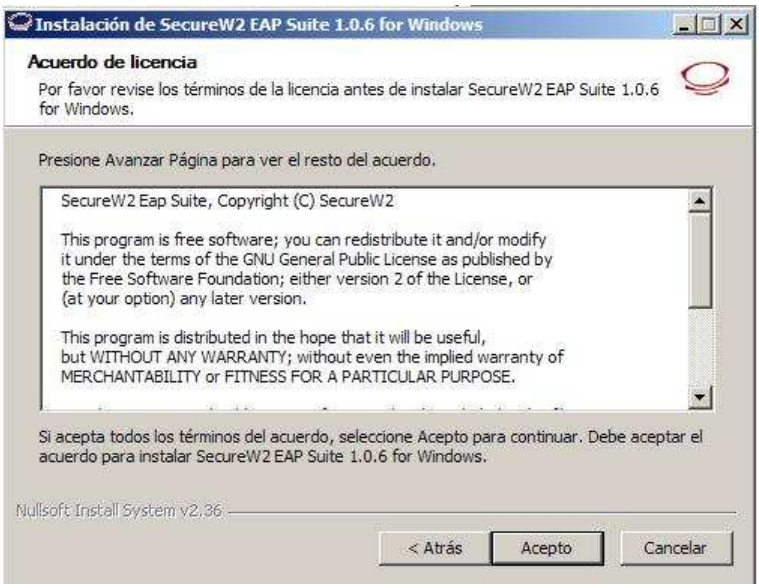



*Figura 4.1.3 Pantalla de acuerdo de licencia*

7. Si presionamos el botón Cancel este cancelara la instalación
8. Si presionamos el botón Atrás este nos regresara a la ventana anterior
9. Presionamos el botón Acepto para continuar con la instalación. Nos mostrara la ventana siguiente

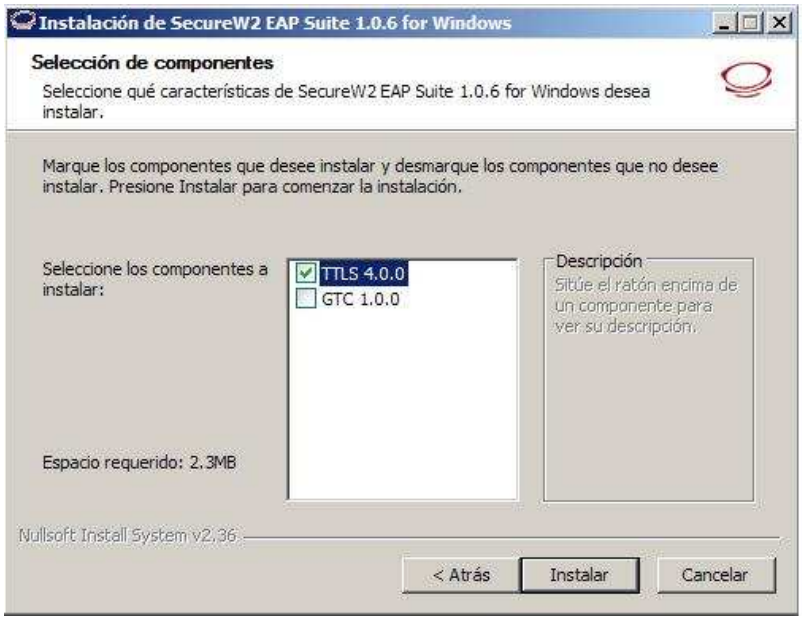



*Figura 4.1.4 Pantalla de selección de componentes a instalar*

10. Si presionamos el botón Cancel este cancelara la instalación
11. Si presionamos el botón Atrás este nos regresara a la ventana anterior
12. Verificamos que este seleccionada la opción TTLS 4.0.0 y no seleccionar la opción GTC 1.0.0

13. Presionamos el botón Instalar para continuar con la instalación

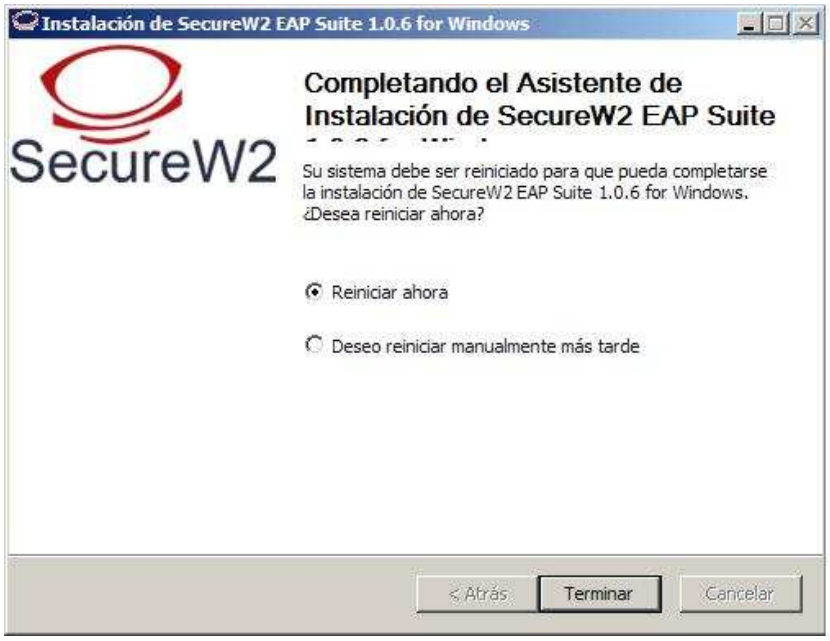



*Figura 4.1.5 Finalización del asistente de configuración del software*

14. Presionar el botón Terminar para finalizar la instalación del software SecureW2, al presionar el botón reiniciara la maquina.

## 4.2 Configurar el cliente SecureW2

Para configurar el perfil de acceso en el "SecureW2" seguiremos los siguientes pasos:

1. Presionamos el botón INICIO de Windows
2. Presionamos el botón Conexión de Área Local
3. Damos click derecho y seleccionamos Propiedades de Red nos mostrara la siguiente ventana.

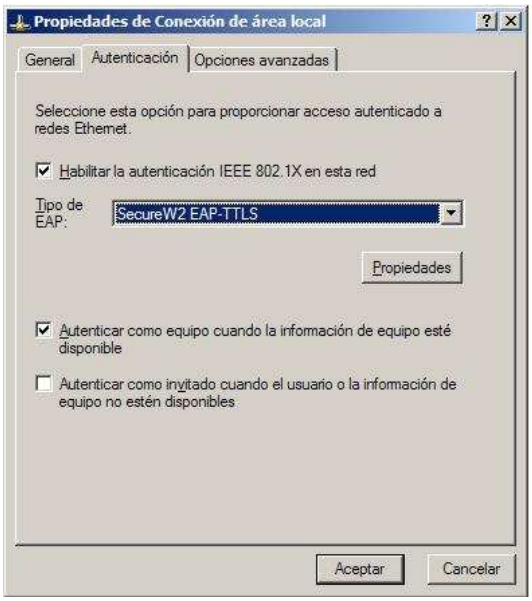



*Figura 4.2.1 Opciones en pestaña Autenticación de las propiedades de Conexión de área local*

1. Si presionamos el botón Cancelar este cerrara la ventana
2. Presionamos la pestaña autenticación
3. Verificamos si está habilitada la opción de Habilitar la autenticación IEEE 802.1X en esta red, si no lo está habilitarla dándole click en el recuadro.
4. En la opción Tipo de EAP seleccionamos SecureW2
5. Luego presionamos el botón propiedades, donde nos aparece la ventana siguiente. La cual puede usar el perfil por defecto (Default)


*Figura 4.2.2 Configuración del perfil del SecureW2*

6. Si Presionamos Nuevo este nos creara un nuevo perfil
7. Si presionamos el botón Cancelar este cerrara la ventana
8. Presionamos el botón Configurar nos mostrara la ventana de Creación del perfil de acceso, (ver tema 5 Creación del perfil de acceso).
9. Una vez configurado el perfil presionar el botón Aceptar.

## 4.3 Creación del perfil de acceso

Para la creación del perfil de acceso es necesario seguir los siguientes pasos:

1. En la pestaña "Conexión", no seleccionamos ninguna opción los campos se dejan en blanco, como se muestran en la imagen siguiente


*Figura 4.3.1 Pestaña Conexión para configuración del perfil del SecureW2*

2. En la pestaña "Certificados", no se marcar ninguna opción, tal y como se indica en la siguiente imagen.


*Figura 4.3.2 Pestaña Certificados para configuración del perfil del SecureW2*

3. En la pestaña "Autenticación" seleccionar en el Método Autenticación el método PAP.


*Figura 4.3.3 Pestaña Autenticación para configuración del perfil del SecureW2*

4. En la pestaña "Cuenta de Usuario" seleccionar "Pedir Credenciales de Usuario"


*Figura 4.3.4 Pestaña Cuenta de usuario para configuración del perfil del SecureW2*

5. Si presionamos el botón Cancelar este cancelara la configuración.
6. Presionar el botón Aceptar para finalizar la configuración.

# 5 Configuración de red según sistema operativo.

## 5.1 Configuración de acceso en Windows XP

### 5.1.1 Consideraciones Preliminares

Debe tener instalado: Windows XP con Service Pack 2. También funciona con Service Pack 1 + Revisión **Q815485** y Revisión **KB826942**.

El cliente **SecureW2** será el programa encargado de transmitir para su validación el usuario y clave en la red inalámbrica mediante el uso de EAP-TTLS. Una vez instalado y configurado automáticamente (proceso recomendado), procedemos a configurar las conexiones de red inalámbricas.

### 5.1.2 Configuración de Windows XP

1. Abra el Panel de Control y pulse sobre Conexiones de red. Seleccione Propiedades, mediante el botón derecho del ratón sobre Conexiones de red inalámbricas.
2. En primer lugar debe asegurarse que para el interfaz inalámbrico tiene definido correctamente la obtención de dirección IP por DHCP.


*Figura 5.1.2.1 Pantalla de Propiedades de Conexiones de red Inalámbricas*

3. En la opción **General** marque **Protocolo Internet TCP/IP** y pulse sobre Propiedades. Mostrara la siguiente ventana


*Figura 5.1.2.2 Pestaña General de Propiedades de Protocolo TCP/IP*

4. Compruebe que tiene establecido "Obtener una dirección IP automáticamente" y "Obtener la dirección del servidor DNS automáticamente". Presionamos el botón Aceptar para cerrar la ventana

5. A continuación seleccione la opción **Redes Inalámbricas** y en Redes preferidas seleccionamos Eduroam y luego pulsamos Propiedades.


*Figura 5.1.2.3 Pestaña Redes Inalámbricas de Propiedades de Conexiones de red Inalámbricas*

6. La opción de **Asociación** nos mostrará:

- Nombre de red (SSID): **Eduroam**
- Autenticación de red: Seleccionar **WPA**
- Cifrado de datos: Seleccionar **TKIP** (Si la tarjeta inalámbrica soporta WPA2 podemos seleccionar AES, que añade mayor seguridad que TKIP).


*Figura 5.1.2.4 Propiedades de la conexión a Eduroam*

7. En la opción de **Autenticación**: Tipo de EAP: Seleccionaremos **SecureW2 TTLS**
8. Luego pulsamos en Propiedades, veríamos la configuración del cliente SecureW2.


*Figura 5.1.2.5 Pestaña de Autenticación de las propiedades de la conexión a Eduroam*

9. Pulse aceptar hasta salir.
    - Deberá tener habilitada la conexión inalámbrica, para su funcionamiento.

### *5.1.3 Prueba de funcionamiento*

Para realizar las pruebas de configuración de la tarjeta inalámbrica seguir los pasos siguientes:

1. Se iniciará el proceso de la conexión inalámbrica, y se mostrará un mensaje emergente como el de la figura, pulsando sobre el mismo nos mostrará una lista de conexiones existentes.

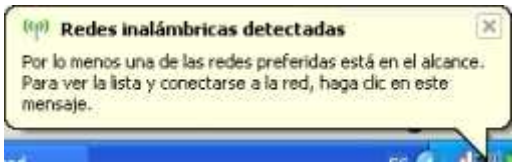



*Figura 5.1.3.1 Pantalla emergente de detección de redes existentes*

2. Si nos encontramos en una zona de cobertura, detectara la red inalámbrica de nombre (SSID) **Eduroam**. Le damos click

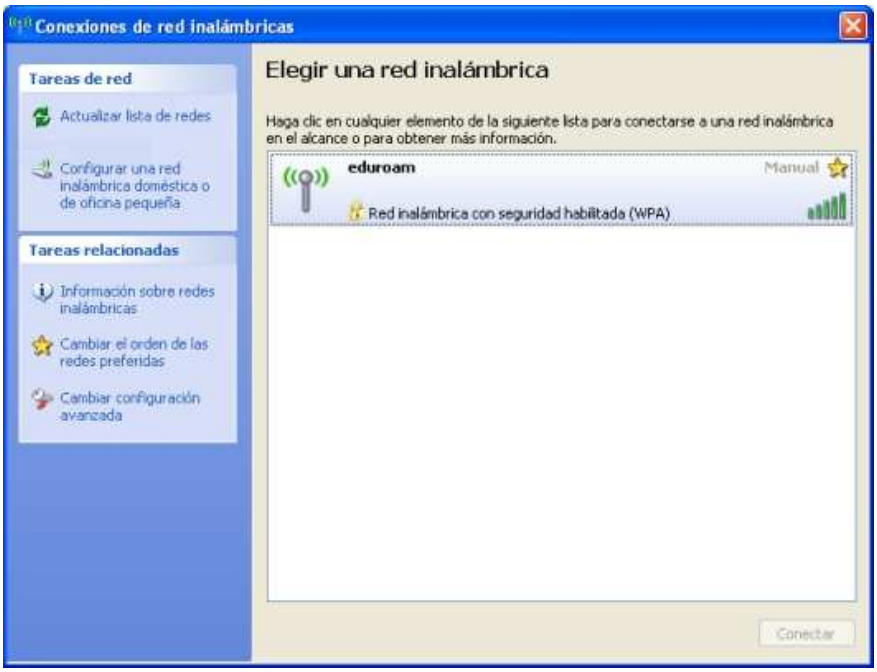



*Figura 5.1.3.2 Detección de red Eduroam*

3. Seleccionamos Conectar.
4. Nos aparece sobre el icono de red inalámbrica un mensaje que indica que se está comprobando la identidad como se muestra en la imagen siguiente


*Figura 5.1.3.3 Pantalla emergente de petición de credenciales*

5. Después le damos click al mensaje que nos aparece en la tarjeta de red y nos aparecerá el certificado SecureW2, el cual nos pedirá que nos identifiquemos mediante nuestra credencial (dirección de correo electrónico y contraseña).


*Figura 5.1.3.4 Pantalla de solicitud de credenciales*

6. Pulse OK y si todo ha ido bien estaremos conectados.

## 5.2 Configuración de acceso con cliente Intel Pro/Wireless

La mayoría de los portátiles que se venden hoy en día, vienen con la tarjeta inalámbrica Intel (centrino), que trae incluido el cliente propio de Intel, por lo que vamos a describir brevemente cuales serían los pasos para configurar dicho cliente con el fin de lograr el acceso a la red inalámbrica con SSID: **Eduroam.**

Mediante el propio cliente de Intel y el sistema operativo correctamente actualizado a SP2 se podrá configurar dicho acceso, no haciendo falta por tanto ningún software intermedio como puede ser *SecureW2*.

### 5.2.1 Instalación del cliente de Intel:

1. Deberá descargar el cliente de Intel ProSet, para ello haga clic sobre el siguiente enlace: http://support.intel.com/support/wireless/wlan/sb/cs-010623.htm
2. Una vez se haya descargado el software, hacer doble clic sobre él y siga las instrucciones de instalación que le vayan apareciendo.

### *5.2.2 Deshabilitar el cliente genérico de Windows*

Para la instalación del cliente será necesario deshabilitar el cliente genérico de Windows tal y como se muestra en los siguientes pasos:

1. Deshabilitar la casilla *"Usar Windows para establecer mi configuración de red inalámbrica".*


*Figura 5.2.2.1 Propiedades de conexión de red inalámbrica.*

### *5.2.3 Acceder al cliente que ha instalado el programa de Intel*

1. Haga doble clic sobre el icono que se haya creado en su escritorio, tras la instalación. Nos aparecerá una ventana donde procedemos a crear un nuevo perfil, para ello pulsamos el botón **Perfiles**.
2. Pulsamos el botón **Agregar** para crear el perfil;


*Figura 5.2.3.1 Agregando un nuevo perfil al cliente de Intel.*

3. En la ventana Configurar opciones inalámbricas digitar eduroam en la parte de Nombre del Perfil y Nombre de la red inalámbrica

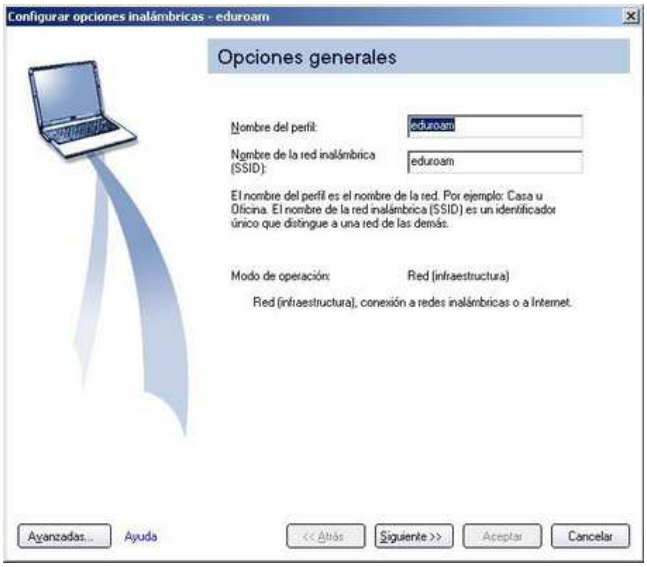



*Figura 5.2.3.2 Agregando un nuevo perfil al cliente de Intel.*

4. Presionar el botón siguiente para continuar con la instalación.

5. Si presionamos el botón Cancelar este cancelara la configuración.

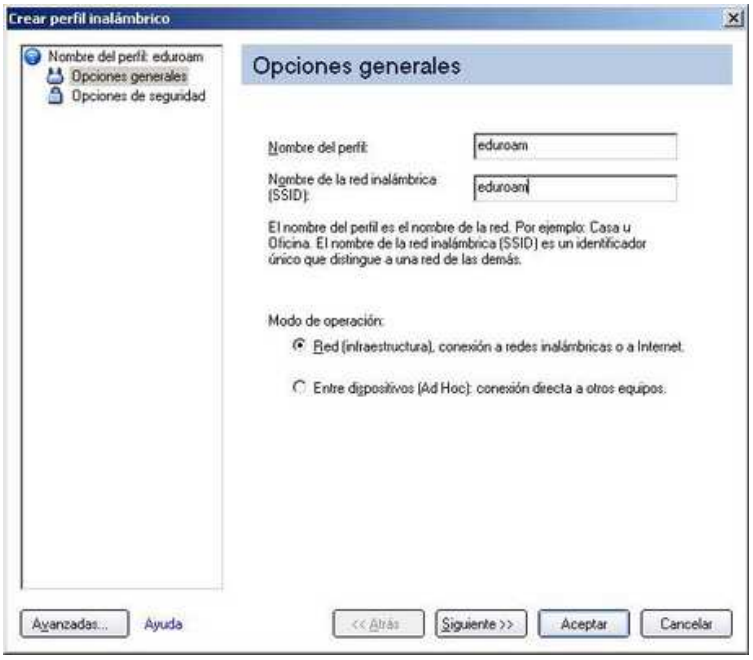



*Figura 5.2.3.3 Agregando un nuevo perfil al cliente de Intel.*

6. Seleccionar en el Modo de operación Red (infraestructura).}
7. Presionar el botón siguiente para continuar con la instalación.
8. Si presionamos el botón Cancelar este cancelara la configuración.

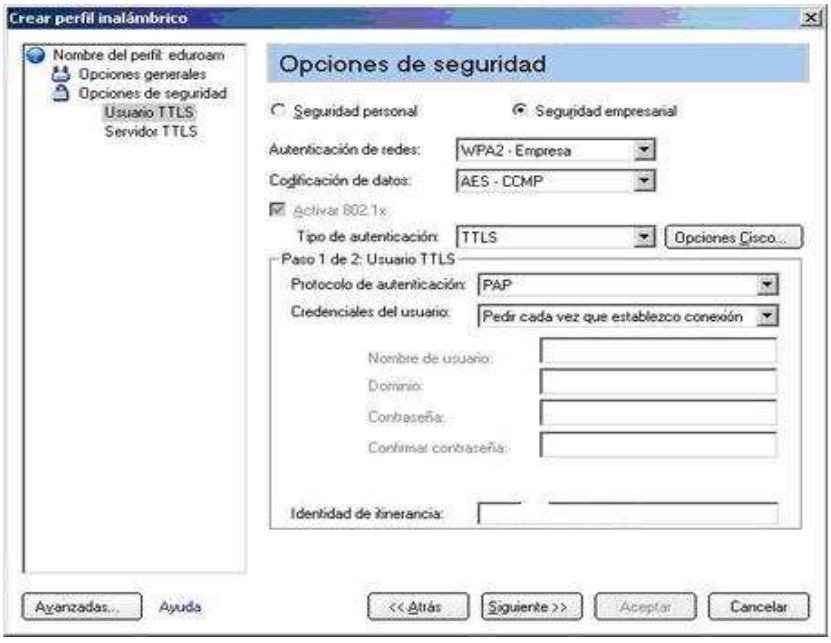



*Figura 5.2.3.4 Paso final para la configuración de nuestro nuevo perfil Eduroam.*

9. Darle click a Opciones de seguridad
10. Seleccionar Usuario TTLS

11. Seleccionar la opción de seguridad que más le conviene si Personal o empresarial, en nuestro caso seleccionaremos empresarial.
12. En la opción Autenticación de redes, seleccionar WPA2 – Empresa.
13. En la opción Codificación de datos, seleccionar AES-CCMP
14. Verificar que la opción Activar 802.1X este habilitada.
15. En la opción tipo de codificación, seleccionar TTLS
16. Seleccionar PAP en la opción protocolo de autenticación.
17. Seleccionar Pedir cada vez que establezca conexión en la opción Credenciales de usuario.
18. Presionar el botón siguiente para continuar con la instalación.
19. Presionar el botón Atrás para regresar a la pantalla anterior
20. Si presionamos el botón Cancelar este cancelara la configuración.

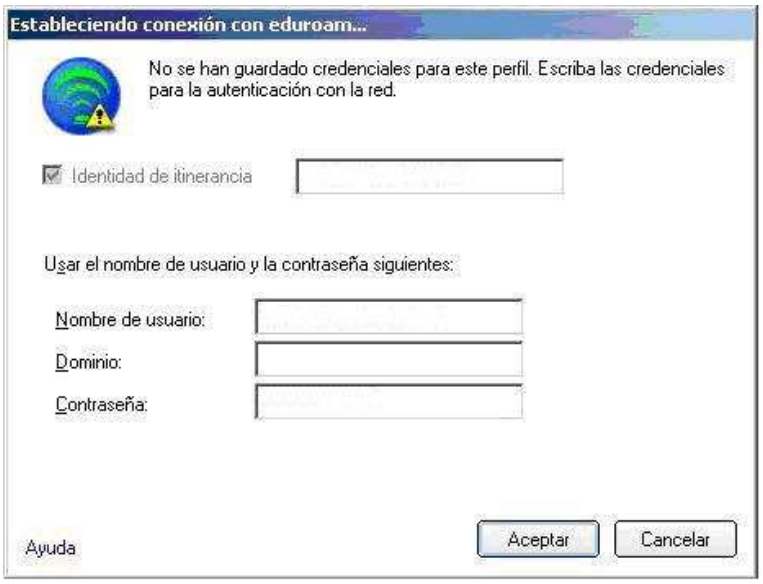



*Figura 5.2.3.5 ingreso de usuario y contraseña.*

21. Presentara la ventana de ingreso de usuario y contraseña
22. Presionar el botón Aceptar para terminar la configuración.
23. Si presionamos el botón Cancelar este cancelara la configuración.
24. Si todo se ha realizado correctamente, se deberá conectar a la nueva red inalámbrica con SSID: **Eduroam**.

# 5.3 Configuración de acceso en Windows Vista

## 5.3.1 Consideraciones Previas

1. En estas instrucciones se refleja la experiencia en la configuración de la conexión a Eduroam, utilizando la versión Business de Windows Vista.
2. El cliente SecureW2 será el programa encargado de transmitir para su validación el usuario y clave en la red inalámbrica mediante el uso de EAP-TTLS. Una vez instalado y configurado, procedemos a configurar las conexiones de red inalámbricas.

## 5.3.2 Configuración de Windows Vista

1. Configurar la conexión inalámbrica a SSID: Eduroam. Para ello abrimos el Centro de redes y recursos compartidos de Windows Vista, pulsando en Inicio - Red.
2. Seleccionamos pulsando **Administrar redes inalámbricas.**


*Figura 5.3.2.1 Ventana de centro de redes y recursos compartidos*

3. Si el proceso de instalación del cliente SecureW2 se ha hecho automáticamente, nos aparecerá el perfil "**Eduroam**" ya configurado.

4. Si optamos por configurar manualmente el cliente SecureW2, debemos añadir un nuevo perfil que llamaremos "**Eduroam**". Para ello pulsamos la opción **Agregar** que se muestra en la ventana siguiente.

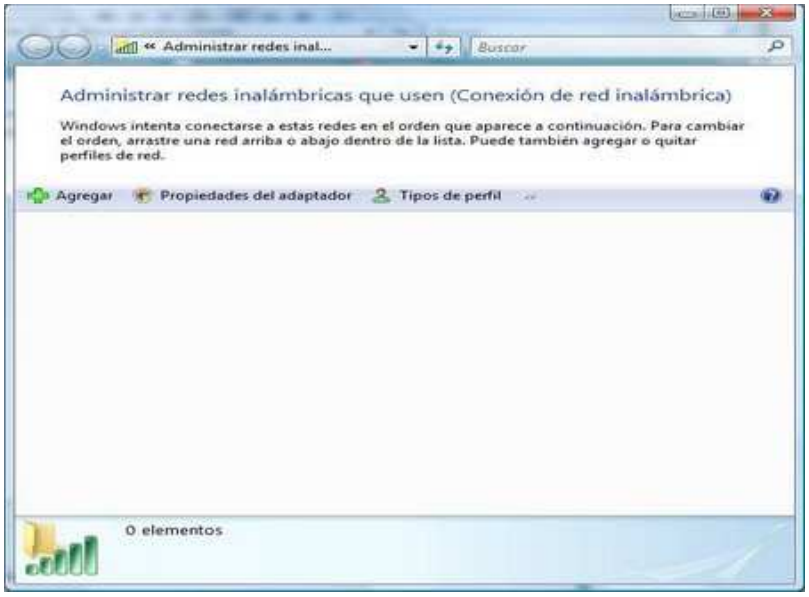



*Figura 5.3.2.2 Ventana de administrar redes inalambricas*

5. A la pregunta ¿Cómo desea agregar una red?, elegimos **Crear un perfil de red manualmente.**

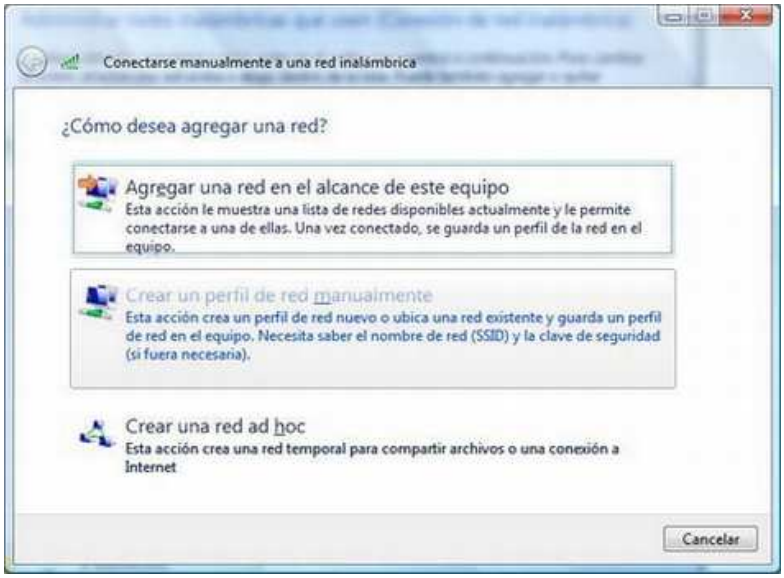



*Figura 5.3.2.3 Ventana de configuracion a una red inalambrica*

6. Si presionamos el botón Cancelar este cancelara la configuración.

7. Completamos los datos como aparecen en la siguiente imagen, seleccionando **WPA2-Enterprise** y **AES** como métodos de seguridad y cifrado.
   - En algunos modelos de tarjetas inalámbricas (como Broadcom), hemos verificado que esta elección no funciona correctamente, por lo que deberemos seleccionar **WPA-Enterprise** y **TKIP** como métodos de seguridad y cifrado.

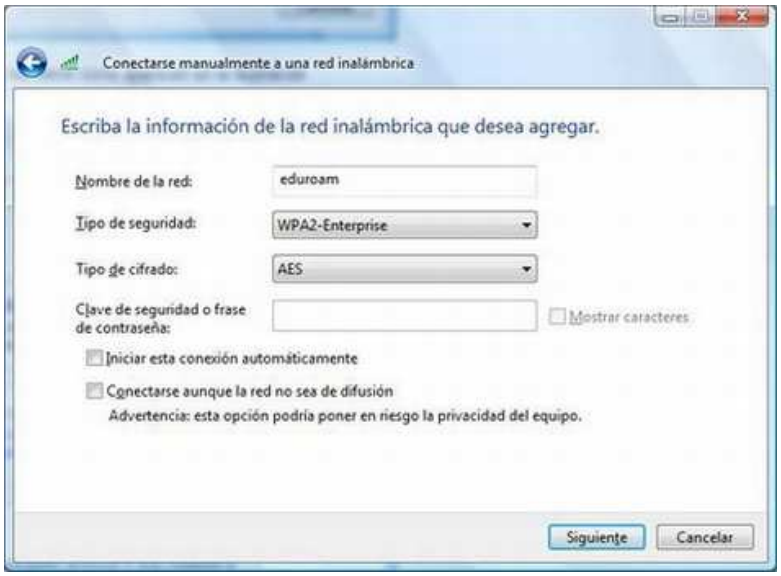



*Figura 5.3.2.4 Ventana de configuracion a una red inalambrica*

8. Y elegimos **Siguiente** para continuar con el proceso.
9. Si presionamos el botón Cancelar este cancelara la configuración.

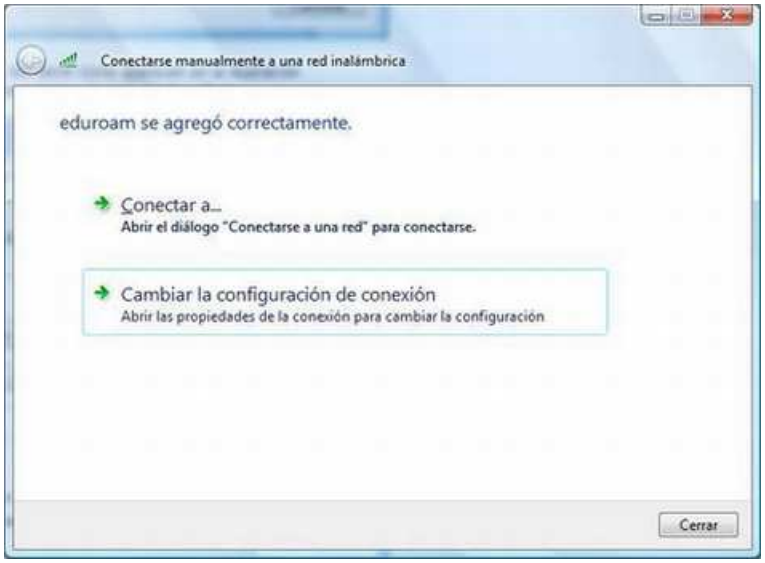



*Figura 5.3.2.5 Ventana de configuracion a una red inalambrica*

10. Seleccionamos la opción **Cambiar la configuración de conexión**

11. Si presionamos el botón Cerrar este cancelara la configuración

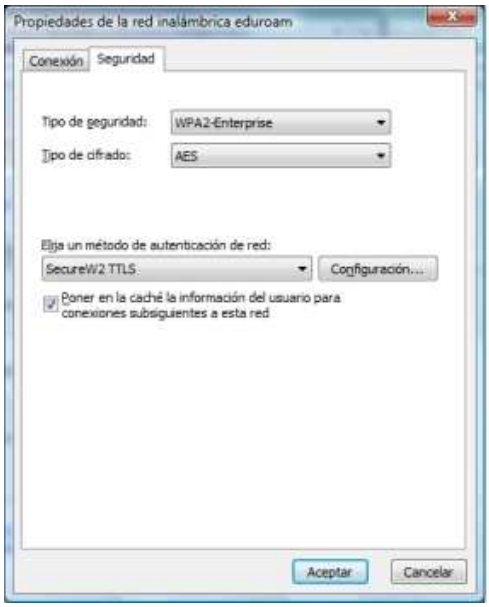



*Figura 5.3.2.6 Ventana de propiedades de la red inalambrica*

12. Seleccionamos la pestaña **Seguridad**, donde elegimos como método de autenticación de red: **SecureW2 TTLS**.
13. Pulsamos sobre **Configuración...** y se abrirá la ventana para configurar el cliente **SecureW2.**
14. Pulse **Aceptar** hasta salir.
15. Si presionamos el botón Cancelar este cancelara la configuración.

### *5.3.3 Pruebas de Funcionamiento*

Deberá tener habilitada la conexión inalámbrica, para su funcionamiento.

1. Ahora podemos comprobar el funcionamiento de la conexión, para ello accedemos de nuevo al **Centro de redes y recursos compartidos** de Windows Vista y seleccionamos la opción de **Conectarse a una red**.

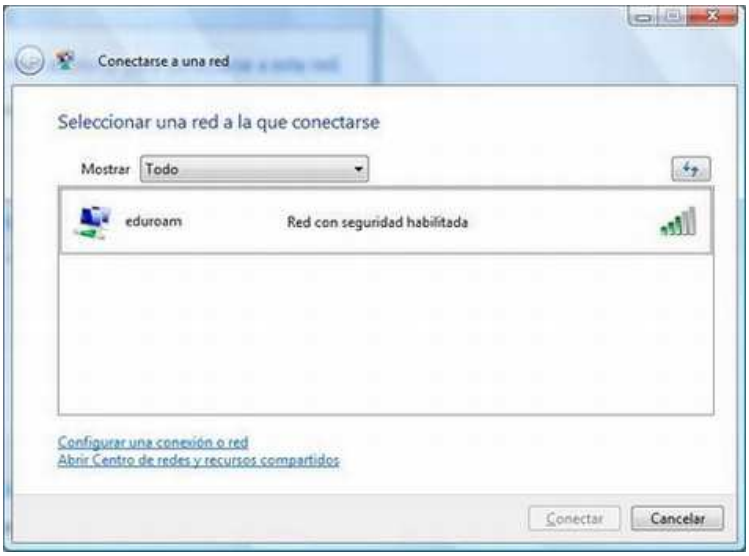



*Figura 5.3.3.1 Ventana de Selección de red inalambrica*

2. Donde nos aparecerá las redes disponibles y entre ellas "**Eduroam**", que es la que seleccionamos para conectarnos.
3. Si presionamos el botón Cancelar este cancelara la configuración

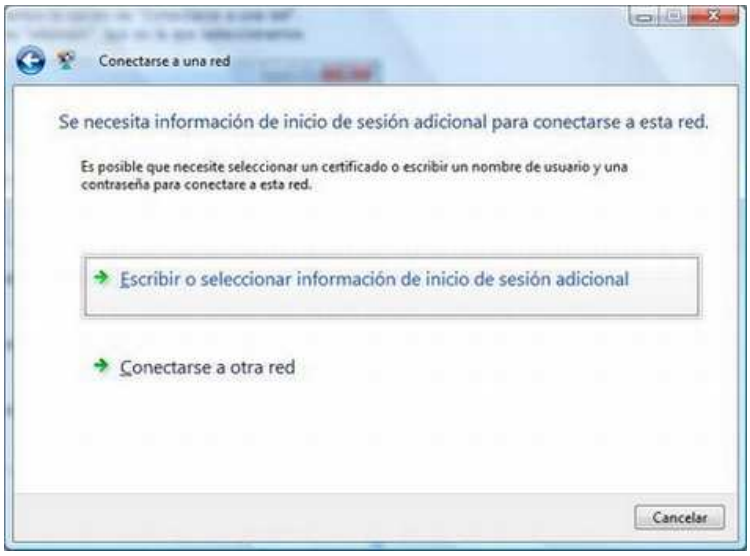



*Figura 5.3.3.2 Ventana de inicio de sesion adicional*

4. Se nos pedirá información de inicio de sesión adicional, para ello pulsamos sobre **Escribir o seleccionar información de inicio de sesión adicional**.
5. Si presionamos el botón Cancelar este cancelara la configuración


*Figura 5.3.3.3 Ventana de ingreso de usuario y contraseña del SecureW2*

6. Ingresar el usuario y la contraseña.
7. Presionar el botón ok para finalizar las pruebas de configuración.
8. Si presionamos el botón Cancelar este cancelara la configuración
9. Si todos los datos se han introducido correctamente, nos aparece la siguiente ventana:

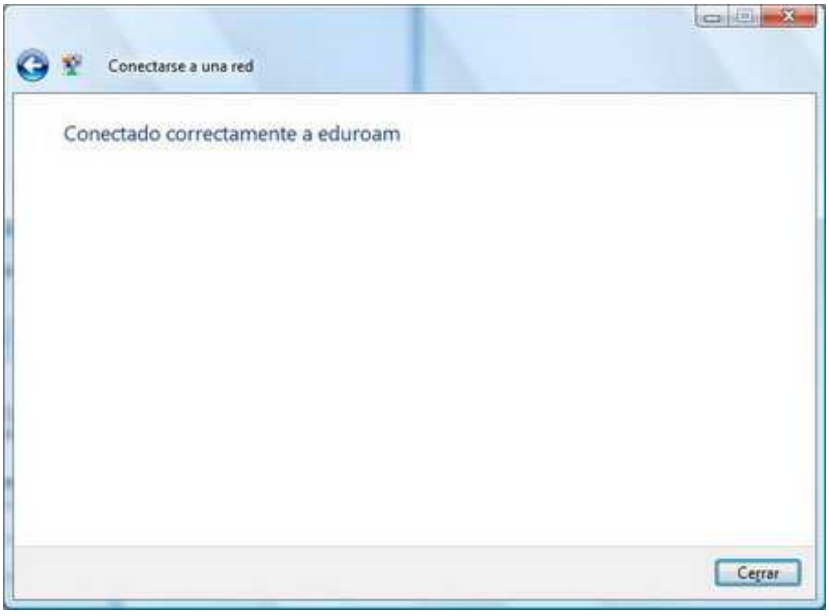



*Figura 5.3.3.4 Ventana de aviso de conexión exitosa*

10. Si presionamos el botón Cerrar este cerrara la ventana

## 5.4 Configuración de acceso con cliente Windows 2000

### 5.4.1 Consideraciones Previas

Windows 2000 no entiende las conexiones inalámbricas como tal, es mas, "cree" que los dispositivos inalámbricos son tarjetas ethernet de cable; por tanto sólo se pueden conectar a la red inalámbrica aquéllos dispositivos que, en el software del fabricante, incorporen el módulo 802.1X y que funcione en Windows 2000. Aunque el software del fabricante incorpore dicho cliente 802.1X, la configuración de opciones y los modos de activación serán diferentes en cada caso.

Recomendamos para utilizar este servicio de conexión inalámbrica, la actualización del sistema operativo a **Windows XP ó superior**. No obstante explicamos en pocos pasos como sería dicha configuración, en términos generales.

En Windows 2000 no es posible habilitar la autenticación 802.1X que es la que se necesita para conectarse de forma predeterminada. Para habilitar este protocolo, lo primero que deberemos comprobar es si el sistema operativo Windows 2000 está actualizado para soportar 802.1X; para ello comprobaremos qué versión de Service Pack tenemos instalada. Pulsamos el botón derecho del ratón en el icono Mi PC, y seleccionamos Propiedades del menú desplegable.

Si tenemos **Windows 2000 SP3**. Necesitamos tener instalada la "REVISIÓN DE WINDOWS 2000 PARA SOPORTE DE 802.1X" (Q313664). Para comprobar si está instalada, ir a: *Inicio -> Panel de Control -> Agregar o quitar programas.*

Tiene que existir un programa instalado con el número **313664**. En caso de no tenerlo instalado, podemos obtenerlo en este siguiente enlace:

**http://support.microsoft.com/default.aspx?scid=kb;en-us;313664**

Si tenemos **Windows 2000 SP4**. El equipo no necesita ninguna actualización para este método de conexión, ya que soporta 802.1X.

## *5.4.2 Configuración de la conexión inalámbrica*

Lo primero que deberemos hacer es arrancar el servicio de autenticación 802.1X de Windows 2000.

1. Para ello deberá pulsar en el botón *Inicio -> Configuración -> Panel de Control -> Herramientas administrativas y Servicios*.

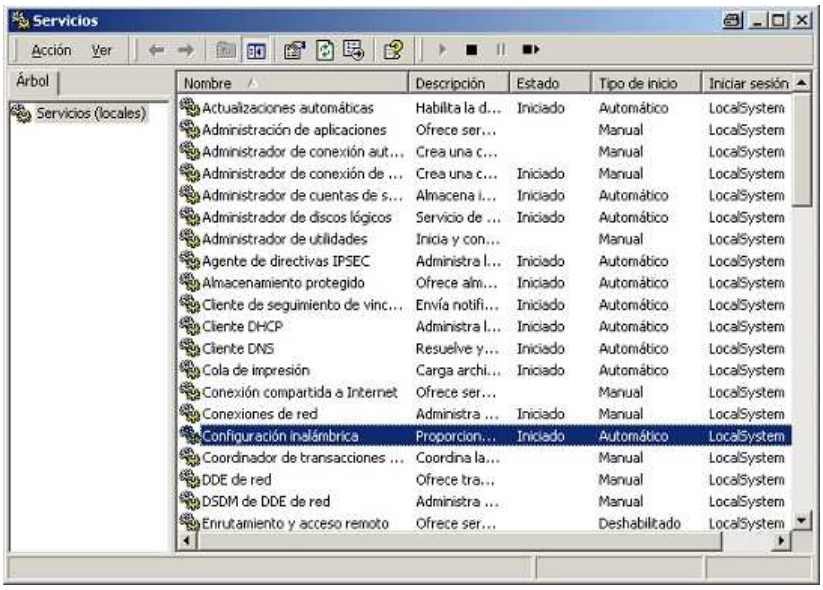



*Figura 5.4.2.1 Ventana de Servicios*

2. A continuación se abrirá una pantalla donde ha de buscar el servicio con el nombre **Configuración inalámbrica** y hacer doble clic sobre él.

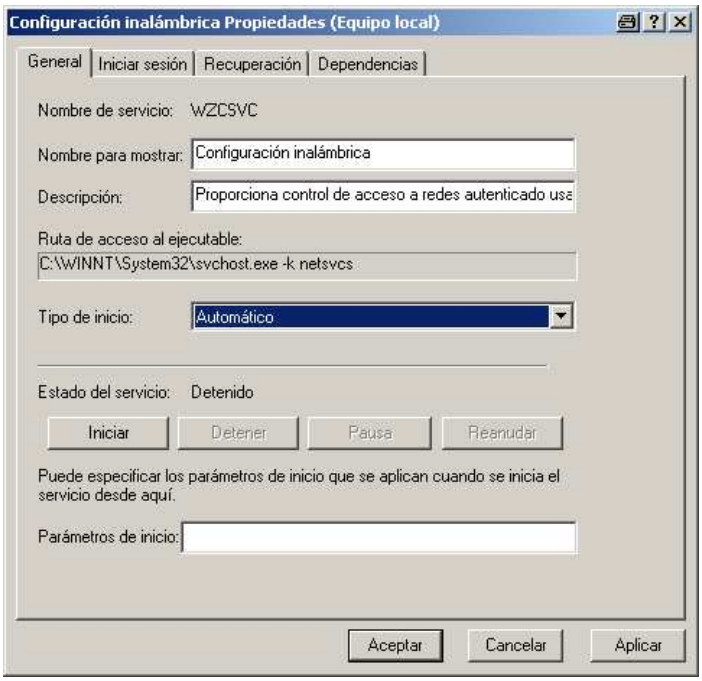



*Figura 5.4.2.2 Ventana de Configuracion inalambrica Propiedades*

3. Se abrirá la siguiente pantalla donde deberemos seleccionar como **Automático** el *Tipo de inicio*, pulsamos sobre el botón **Iniciar** para que el Estado del Servicio quede iniciado y seguidamente sobre el botón **Aceptar** para consolidar los cambios. Si presionamos el botón Cancelar este cancelara la configuración.
4. El siguiente paso será configurar los parámetros de red. Deberemos tener instalado y sino debemos hacerlo en este momento el ***software de nuestra tarjeta para conexión inalámbrica*** y el ***software de cliente SecureW2***.

## *5.4.3 Configuración de los parámetros TCP/IP*

1. Procedemos a configurar la conexión inalámbrica, para ello pulsamos sobre el botón *Inicio -> Configuración -> Conexiones de red y acceso telefónico.* Con el botón derecho pulsamos sobre la conexión de su tarjeta inalámbrica y seleccionamos **Propiedades**.


*Figura 5.4.3.1 Ventana de propiedades de conexión inalambrica*

2. En la pantalla de **Propiedades de Conexión Inalámbrica**, deberemos seleccionar el *Protocolo Internet (TCP/IP)* y pulsar sobre el botón **Propiedades**.

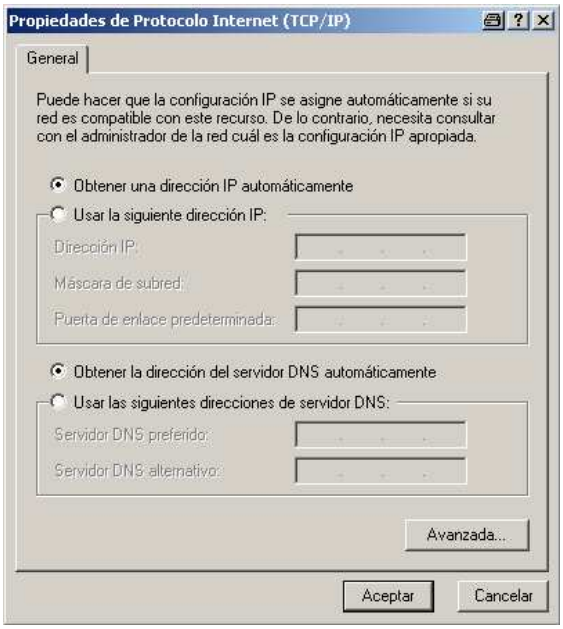



*Figura 5.4.3.2 Ventana de propiedades de protocolo internet*

3. Deberá comprobar que están marcadas las opciones **Obtener una dirección IP automáticamente** y **Obtener la dirección del servidor DNS automáticamente**, a continuación deberá pulsar en el botón **Aceptar**.
4. Si presionamos el botón Cancelar este cancelara la configuración

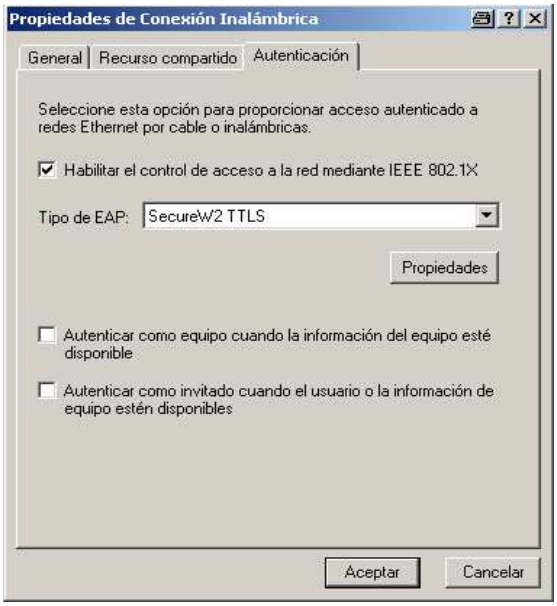



*Figura 5.4.3.3 Ventana de propiedades de conexión inalambrica*

5. Seleccionamos la pestaña **Autenticación** y marcamos **Habilitar el control de acceso a la red mediante IEEE 802.1X** y como Tipo de EAP deberemos Seleccionar **SecureW2 TTLS**.
6. Presionamos Aceptar hasta salir.
7. Si presionamos el botón Cancelar este cancelara la configuración

# *ANEXO 12 MANUAL TÉCNICO DE CONFIGURACIÓN*

# *MANUAL TÉCNICO DE CONFIGURACIÓN*

## *Índice*

# 1 Introducción

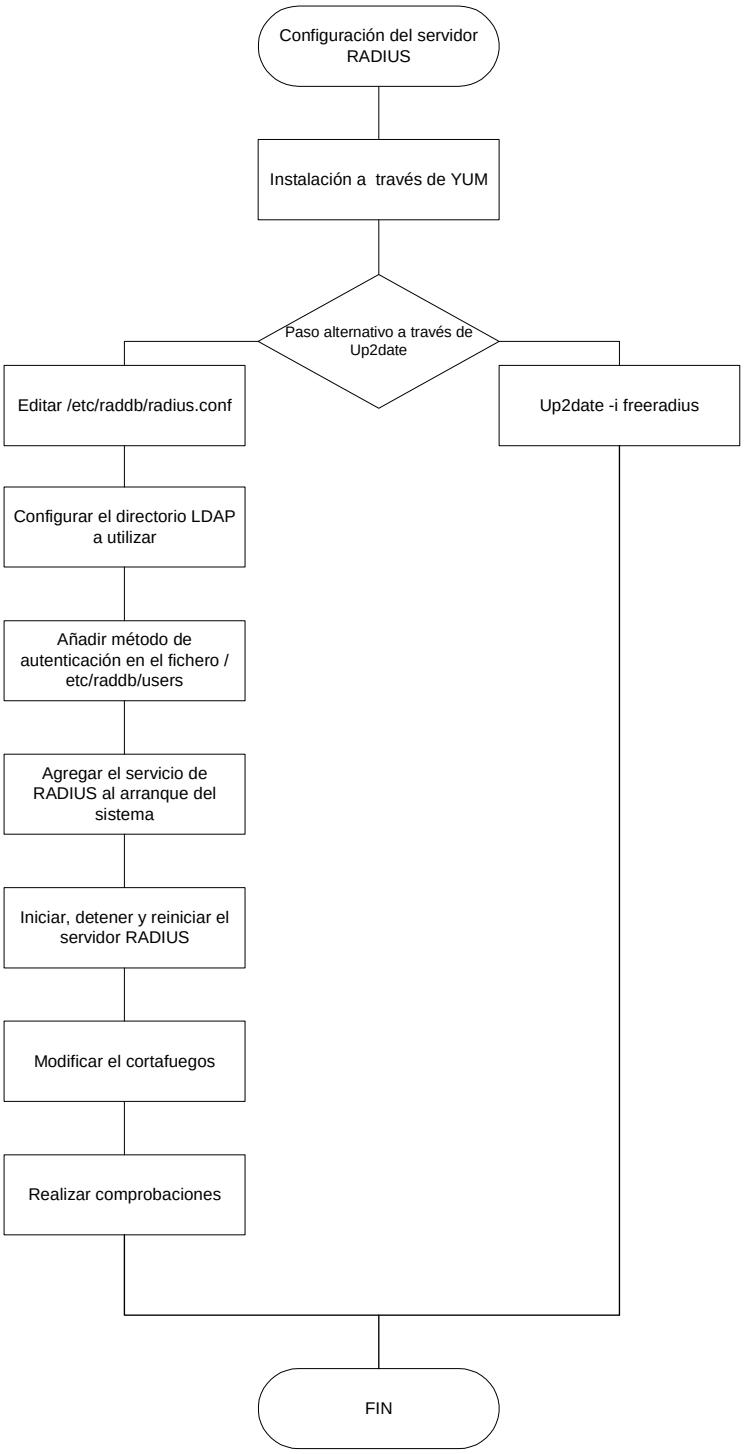
Para poder integrar a la Universidad de El Salvador a la red académica de usuarios móviles Eduroam, es necesario que la institución cuente con equipos de red, servidores y protocolos configurados conforme a las exigencias que dicho programa establece, debido a esto, en el presente manual técnico se explicaran los pasos para la configuración de los equipos de red, protocolos y servidores RADIUS y LDAP.

Este manual técnico tiene la finalidad de guiar a los administradores de red de cada facultad así como también al administrador de la red de la Universidad de El Salvador en el proceso de configuración de los equipos de red, protocolos y servidores.

El manual abarcara primero las configuraciones de los servidores RADIUS y LDAP, posteriormente se muestra la configuración del Switch 3COM 4200 y finalmente se detalla la configuración del punto de acceso 3COM.

# 2 Configuración del servidor RADIUS.

En el diagrama se muestra la secuecia a seguir para la configuración de un servidor RADIUS.




*Flujograma de la configuración del servidor RADIUS*

## 2.1 Instalación a través de yum.

Si se utiliza de CentOS 4 o White Box Enterprise Linux 4, solo se necesita utilizar lo siguiente:

```
yum -y install freeRADIUS
```

## 2.2 Instalación a través de Up2date(Alternativo)

Si se utiliza de Red Hat™ Enterprise Linux 4, solo se necesita utilizar lo siguiente:

```
up2date -i freeRADIUS
```

## 2.3 Procedimientos.

Editar /etc/raddb/RADIUSd.conf y habilitar la línea que activa el módulo de LDAP:

```
Authorize {
        # The LDAP module will set Auth-Type to LDAP if it has not
        #  already been set
        #  LDAP
```

En este mismo fichero se configura el directorio LDAP a utilizar:

```
LDAP {
                server = "tu-servidor-LDAP"
                # identity = "cn=admin,o=My Org,c=UA"
                # password = mypass
                basedn = "ou=People,dc=dominio,dc=com"
                password_attribute = "userPassword"
                filter = "(uid=%{Stripped-User-Name:-%{User-Name}})"
```

Si no se va a utilizar el acceso Dial-Up, se puede desactivar la función o de otro modo no permitirá autenticar o realizar las pruebas de verificación.

```
# access_attr = "dialupAccess"
```

## 2.4 Añadir Método de Autenticación

Se añade el método de autenticación LDAP en el fichero /etc/raddb/users del siguiente modo:

```
# First setup all accounts to be checked against the UNIX /etc/passwd.
# (Unless a password was already given earlier in this file).
DEFAULT Auth-Type = System
    Fall-Through = 1
# Defaults for LDAP
DEFAULT Auth-Type := LDAP
    Fall-Through = 1
```

Finalmente se define en el fichero /etc/raddb/clients.conf a la red o redes que se permitirá autenticar:

```
client 192.168.0.0/24 {
   secret          = clave-acceso-red
   shortname       = Nombre de la red privada
}
```

## 2.5 Agregar el servicio al arranque del sistema.

Para hacer que el servicio de RADIUS esté activo con el siguiente inicio del sistema, en todos los niveles de corrida (2, 3, 4, y 5) se utiliza lo siguiente:

```
chkconfig RADIUSd on
```

## 2.6 Iniciar, detener y reiniciar el servicio.

Para ejecutar por primera vez el servicio, utilice:

```
service RADIUSd start
```

Para hacer que los cambios hechos tras modificar la configuración surtan efecto, utilice:

```
service RADIUSd restart
```

Para detener el servicio, utilice:

```
service RADIUSd stop
```

## 2.7 Modificaciones necesarias en el muro cortafuegos.

Si se utiliza un cortafuegos con políticas estrictas, como por ejemplo Shorewall, es necesario abrir el puerto 1812 por UDP.

Las reglas para el fichero /etc/shorewall/rules de Shorewall correspondería a algo similar a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST          SOURCE
#                       PORT          PORT(S)1
ACCEPT  net     fw      udp     1812
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

## 2.8 Comprobaciones.

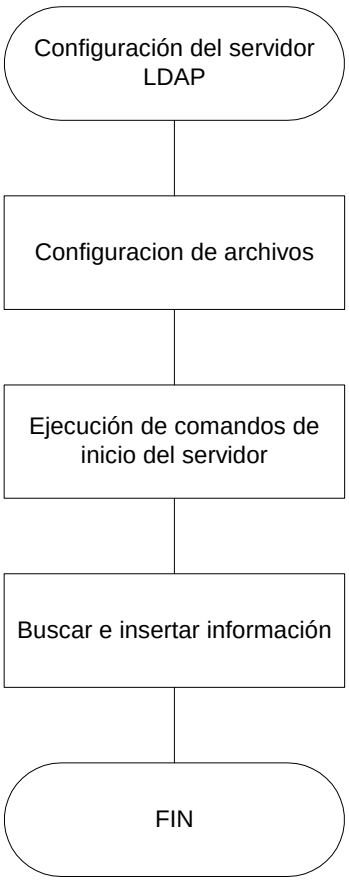
FreeRADIUS incluye una herramienta para realizar pruebas. A fin de verificar que funcione correctamente la autenticación, se utiliza el mandato radtest del siguiente modo:

```
radtest usuario-LDAP "clave-de-acceso-en-LDAP" 192.168.0.1 2 clave-acceso-red
```

Lo anterior debe devolver algo como lo siguiente:

```
Sending Access-Request of id 191 to 192.168.0.1:1812
        User-Name = "usuario-LDAP"
        User-Password = "clave-de-acceso-en-LDAP"
        NAS-IP-Address = nombre-servidor
        NAS-Port = 2
rad_recv: Access-Accept packet from host 192.168.0.1:1812, id=191, length=20
```

# 3 Configuración del servidor LDAP




*Flujograma de la configuración del servidor LDAP*

## 3.1 Configuración de archivos

**Configurar el archivo slapd.conf**

Es el archivo principal de OpenLDAP y es aquí donde se configuran todos sus parámetros, si hace una instalación de acuerdo a esta guía, slapd.conf se encuentra dentro del directorio /usr/local/etc/openLDAP

- **Parámetros Globales**

Los parámetros dentro de esta sección afectan el funcionamiento de todo el Servidor OpenLDAP, cualquier definición antes de un parámetro database es considerado global, cabe mencionarse que los valores de parámetros globales pueden ser contrarrestados al nivel de bases de datos, esto es, si se define el parámetro access globalmente, es posible alterar el valor de este parámetro en "X" base de datos y el resto de las bases de datos permanecerán con el valor global.

Los siguientes son parámetros globales básicos para slapd.conf :

```
include         /usr/local/etc/openLDAP/schema/core.schema
#referral       LDAP://root.openLDAP.org/
#access to *  by * write
pidfile         /usr/local/var/slapd.pid
argsfile /usr/local/var/slapd.args
loglevel 0
```

**include** : Este parámetro indica otros archivos de configuración utilizados por el Servidor OpenLDAP, la declaración anterior carga el archivo core.schema.

**referral**: Indica un Servidor LDAP alterno en dado caso de no poderse efectuar la búsqueda en el servidor LDAP actual.(Desactivado con comentario #).

**access to** ...: Parámetro utilizado para restringir acceso al servidor LDAP, la utilización de acceso también es un tema muy amplio descrito en otra sección de esta guia. (Desactivado con comentario #)

**pidfile** : Contiene el numero de proceso asignado al servidor LDAP al arranque. (Vea: Ejecución y Terminación del Servidor LDAP )

**argsfile** : Contiene parámetros utilizados en la línea de comandos al iniciar el servidor OpenLDAP (Vea: Ejecución y Terminación del Servidor LDAP )

**loglevel** : Indica el nivel de registros ("log") producidos por el servidor LDAP, posibles valores:

| Level | Description | Level | Description |
|---|---|---|---|
| -1 | enable all debugging | 0 | no debugging |
| 1 | trace function calls | 2 | debug packet handling |
| 4 | heavy trace debugging | 8 | connection management |
| 16 | print out packets sent and received | 32 | search filter processing |
| 64 | configuration file processing | 128 | access control list processing |
| 256 | stats log connections/operations/results | 512 | stats log entries sent |
| 1024 | print communication with shell backends | 2048 | print entry parsing debugging |

- **Parámetros por Base de Datos**

Dentro de cada servidor LDAP se pueden encontrar varias bases de datos, es dentro de estas bases de datos que residirá toda información del Servidor OpenLDAP.

> **NOTA:** En el sentido más estricto de la palabra OpenLDAP no utiliza una base de datos, la "base de datos" utilizada en OpenLDAP es un tipo de "Flat File" generalmente ldbm .

Una definición para base de datos sería la siguiente:

```
database        ldbm
suffix          "dc=osmosislatina, dc=com"
#suffix         "o=Osmosislatina, c=MX"
rootdn          "cn=Admin, dc=osmosislatina,
dc=com"
#rootdn         "cn=Admin, o=Osmosislatina,
c=MX"
rootpw          daniel
directory       /usr/local/var/openLDAP-ldbm
```

**database**: Indica el tipo de "base de datos" a utilizarse, generalmente del tipo ldbm (Otras alternativas: shell,passwd), además indica el inicio de "base de datos", esto es, cada declaración de database se considera una "base de datos" por separado, esto será descrito a mayor detalle en Insertar datos en OpenLDAP .

**suffix**: Este parámetro indica el *nodo raíz* de la base de datos, esto es, el nodo sobre el cual será derivada toda la información, en este caso dc=osmosislatina, dc=com (Nótese que este también pudo ser o=Osmosislatina, c=MX). Lo anterior indica que toda información dentro de esta "base de datos" LDAP descenderá de la jerarquía dc=osmosislatina, dc=com (Esta jerarquía fue ilustrada en LDAP). Lo anterior será descrito a mayor detalle en Insertar datos en OpenLDAP

**rootdn** : Establece el nodo ("usuario") que tiene privilegios globales para modificar la "base de datos" LDAP , en este caso cn=Admin, nótese que *desciende* del nodo raíz (suffix) dc=osmosislatina, dc=com .

**rootpw** : Indica la contraseña para el usuario rootdn.

**directory** : Define el directorio donde residirá la base de datos, este directorio debe existir antes iniciar el Servidor LDAP.

## 3.2 Ejecución de comandos de inicio del servidor

- **Ejecución**

Para iniciar OpenLDAP se ejecuta el comando slapd , ubicado en /usr/local/libexec/ , esto inicia el Daemon LDAP bajo el puerto TCP 389 por default. Al momento de ejecutar slapd también es posible indicar ciertos parámetros de arranque como el (los) puerto(s) TCP: slapd -h "LDAPs:// LDAP://127.0.0.1:978" , lo anterior inicia el servidor LDAP bajo SSL (Secure Socket Layer) bajo el puerto default 636 y bajo el puerto TCP 978 (en vez del default 389).

El indicar estos parámetros en la linea de comandos cada ocasión puede ser tedioso, por lo que se recomienda agregar estos parámetros al archivo slapd.args ubicado generalmente en /usr/local/var/ (ambos modificables de slapd.conf ).

Para cerciorarse que el servidor LDAP esta operativo realice un telnet al puerto TACA en cuestión: telnet localhost 389 , si la conexión no es aceptada verifique los registros ("logs") de OpenLDAP.

- **Terminación**

Para terminar el Daemon LDAP se debe ejecutar: kill -INT `cat /usr/local/var/slapd.pid` , lo anterior asume que el parámetro pidfile en slapd.conf se encuentra definido como: pidfile /usr/local/var/slapd.pid.

## 3.3 Buscar e Insertar la información en el servidor

El insertar información en un servidor LDAP es uno de los primeros pasos a seguir después de su instalación, pero antes de insertar información es conveniente saber cual es su estructura dentro de las bases de datos (LDBM) utilizadas por LDAP.

Todo nodo o fragmento en un servidor LDAP es un **DN Distinguished Name**

Es dentro de cada Distinguished Name que son definidos distintos atributos los cuales contienen información relevante como: Contraseñas, Apellidos, Fotografías, Nodos IP, o cualquier otro fragmento de información imaginable.

- **Distinguished Name Raíz (suffix)**

Cuando son definidos parámetros para base de datos siempre se indica un DN (Distinguished Name) raíz, éste debe ser representativo de la estructura jerárquica que se intenta captar.

| DISTINGUISHED NAME Raíz | | | | |
|---|---|---|---|---|
| méxico | méxico | brasil | brasil | venezuela |
| drubio | garaiza | lsantos | ffontes | kpiment |
| 3ffw12eg | 2emndfs | we334faf | tert232 | 4fhlzpqa |
| (52)-(6)-3422321 | (52)-(5)-2353312 | (55)-(11)-8696446 | (55)-(21)-7453242 | (58)-(2)-4943421 |

La jerarquía anterior representa una organización, por lo que el Distinguished Name Raíz puede ser:

"dc=osmosislatina, dc=com"

o

"o=Osmosislatina, c=MX"

La composición de cada distinguished name puede variar, en este caso se utilizaron los vocablos dc de "Domain Component", c de "Country", o de "Object", sin embargo también hubiera sido posible utilizar p de "País",cd de "Componente Dominio". Los vocablos son solo descriptivos y su única restricción (si existiese) es llevada acabo en la definición de Schemas .

- **Distinguished Name Administrativo (rootdn)**

Además del DN distinguished name raíz, previa inserción de datos también existe un DN el cual posee acceso global sobre la base de datos (LDBM) en cuestión. Este DN es derivado del DN raíz, por lo que puede ser: "cn=Admin, dc=osmosislatina, dc=com", donde se utiliza cn como vocablo y Admin como valor, sin embargo, al igual que el DN raíz, este vocablo y valor pueden variar.

Para accesar la base de datos (LDBM) utilizando el DN administrativo se emplea la contraseña también definida en slapd.conf mediante el parámetro rootpw.

- **Archivos LDIF**

Estas estructuras o DN distinguished names generalmente se definen en archivos denominados LDIF. El siguiente archivo LDIF contiene los DN's mencionados anteriormente ( raíz y administrativo ):

```
dn: dc=osmosislatina,dc=com
objectClass: dcObject
objectClass: organization
o: Osmosislatina
description: Desarrollos Open-Source en Español

# Rol para administrador de la Red

dn: cn=Admin,dc=osmosislatina,dc=com
objectClass: organizationalRole
cn: Admin
description: Administrador del Servidor LDAP
```

El primer elemento de cada estructura es casi obvio dn de distinguished name. Los elementos en itálicas objectclass están directamente relacionados con Schemas y definen el tipo de objeto para el DN,esto es: cuales y cuantos atributos puede contener.

Posteriormente se definen los Atributos para cada DN:

- description para el primer DN.
- cn y description para el segundo DN.

Nótese que no necesariamente existe correlación directa entre el DN y sus atributos, y como fue mencionado anteriormente la única restricción para atributos (si existiese) es llevada acabo mediante Schemas

- **Insertar DN's raíz y administrativo**

Aunque los DN's raíz y administrativos se encuentran definidos para una base de datos (LDBM) es necesario insertarlos antes de realizar cualquier tipo de operación, el siguiente ejemplo asume que los parámetros para base de datos definidos en la sección de configuración serán utilizados.

Una vez definido un archivo LDIF con los DN's raíz y administrativos.( Como el definido anteriormente )

Ejecute el comando:

LDAPadd -f osmo.ldif -D "cn=Admin,dc=osmosislatina,d=com" -w daniel
Donde osmo.ldif es el archivo LDIF.

Si aparece adding new entry dc=smosislatina,dc=com fue exitosa la inserción, de otra manera deberá revisar Registros ("logs") de OpenLDAP para observar el error ocurrido.

- **DN's Generales**

Una vez definidos los DN's raíz y administrativo es posible insertar otros DN's que conformaron parte de la jerarquía. A continuación tres DN's estructurados como un archivo LDIF:

```
dn: cn=Daniel
```

**Robledo,dc=osmosislatina,dc=com**
cn: Daniel Robledo
p=Mexico
mail: drobledo@yahoo.com
telefono: (52)-(6)-3422321

**dn: cn=Fernanda Fontes,dc=osmosislatina,dc=com**
cn: Fernanda Fontes
p=Brazil
mail: fontes@yahoo.com
telefono: (55)-(11)-8696446

**dn: cn=Luis Arano,dc=osmosislatina,dc=com**
cn: Luis Arano
p=Argentina
mail: larano@slb.com
teléfono: (58)-(2)-4943421

Para agregar estos DN's a la base de datos (LDBM) se debe ejecutar:

```
LDAPadd -f personal.ldif -D "cn=Admin,dc=osmosislatina,dc=com" -w daniel
```

Donde personal.ldif es el archivo LDIF definido en la parte superior.

- **Mas DN's**

Los DN's y sus atributos declarados anteriormente son solo básicos, ya que es posible definir una extensa jerarquía así como atributos; DN's por países, oficinas, hardware...., así como atributos relacionados con: nodos IP, contraseñas, fotografías JPEG o GIF

- **Búsquedas**

Con los DN's que ya han sido insertados en la base de datos (LDBM) del servidor LDAP, ya es posible realizar búsquedas de información:

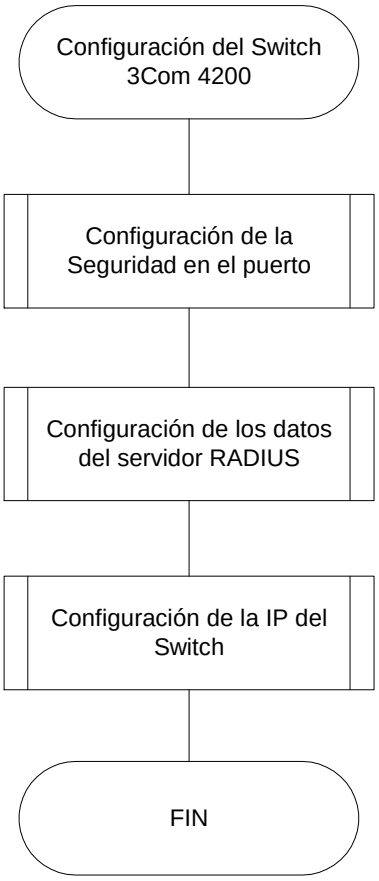
- LDAPsearch -bdc=osmosislatina,dc=com telefono=*52* : Busca los DN's bajo el DN raíz dc=osmosislatina,dc=com que contengan el atributo teléfono con las cifras 52.
- LDAPsearch -bdc=osmosislatina,dc=com mail=* : Busca los DN's bajo el DN raíz dc=osmosislatina, dc=com que contengan el atributo email.

La instalación del servidor OpenLDAP que ha sido llevada acabo permite que cualquier tipo de búsqueda sea llevada acabo, sin embargo, en un ambiente de producción es un hecho que deben ser agregados diversos filtros y restricciones en base al usuario que este realizando la búsqueda.

# 4 Configuración de equipo de red.

## 4.1 Switch 3Com 4200

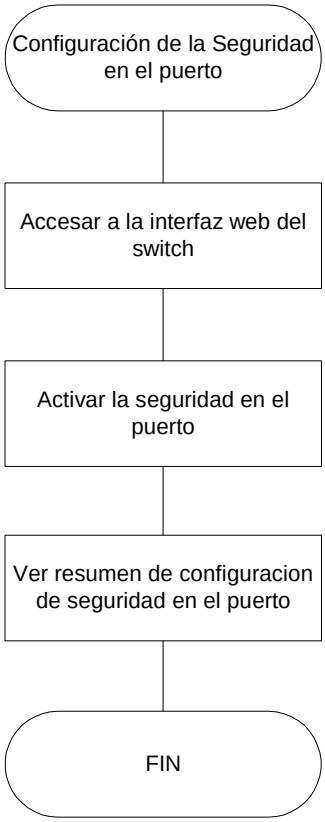
El siguiente diagrama muestra la secuencia lógica a seguir para la configuración del switch.




*Flujograma de la configuración del Switch 3Com 4200*

### *4.1.1 Configuración de la Seguridad en el puerto*

En el diagrama se muestran los pasos necesarios para configurar la seguridad en un puerto del switch, posteriormente se detalla en que consiste cada uno de ellos.




*Flujograma de la seguridad en el puerto del Switch 3Com 4200*

A continuación se presenta la configuración de la seguridad en el puerto en el Switch 3Com 4200. Para realizar esta configuración es necesario acceder a la interfaz web.

## 4.1.1.1 ACCESO A LA INTERFAZ WEB

Para acceder a la interfaz web a través de la red, adoptar las siguientes medidas:

1. Asegúrese de que su red está correctamente configurado para la gestión mediante la interfaz web.
2. Abra su navegador Web.

3. En el campo Ubicación del navegador, introduzca la dirección URL. Esto debe ser en el formato: http://999.999.999.999/ donde 999.999.999.999 es la dirección IP. Cuando el navegador ha cargado, aparecerá un cuadro de dialogo que contiene nombre de usuario y contraseña.

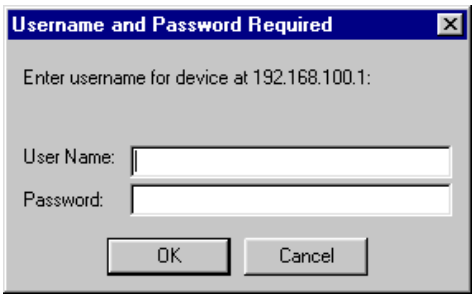



*Figura 5.1.1.1.1 Ventana de ingreso de usuario y password a la interfaz Web*

4. Introduzca el nombre de usuario y su contraseña de administrador del switch.
5. Presionar el botón ok
6. Para cancelar todo presionar el botón Cancel

## 4.1.1.2 ACTIVAR Y DESACTIVAR LA SEGURIDAD EN EL PUERTO

Puede activar y desactivar la seguridad y establecer el modo de funcionamiento en un puerto usando el asistente de seguridad portuaria.

Para acceder al asistente:

1. Haga clic en Device View en la barra de herramientas.
2. Seleccione Security -> Network -> Access -> Port Security en el árbol de navegación

Forma alternativa:

1. Si usted ya sabe que puerto quiere habilitar la seguridad presione click izquierdo en el puerto.
2. Le aparecerá un menú y selecciones Port Security

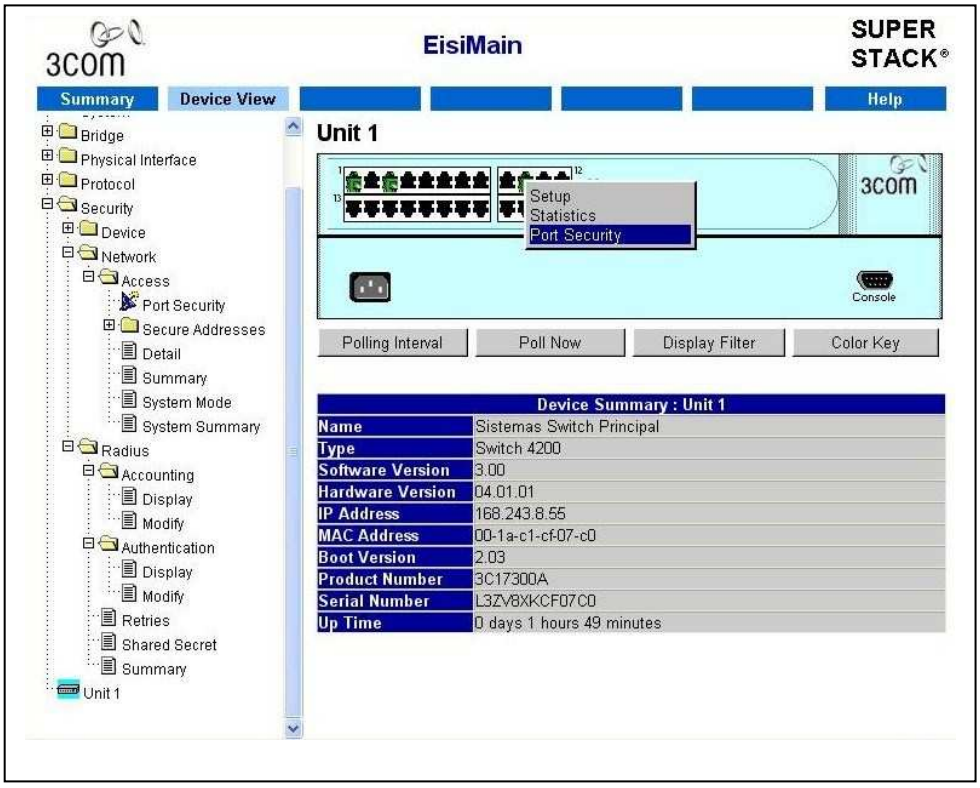



*Figura 5.1.1.2.1 Ventana principal de la Interfaz Web del Switch 3COM 4200*

3. La primera página del Port Security se muestra

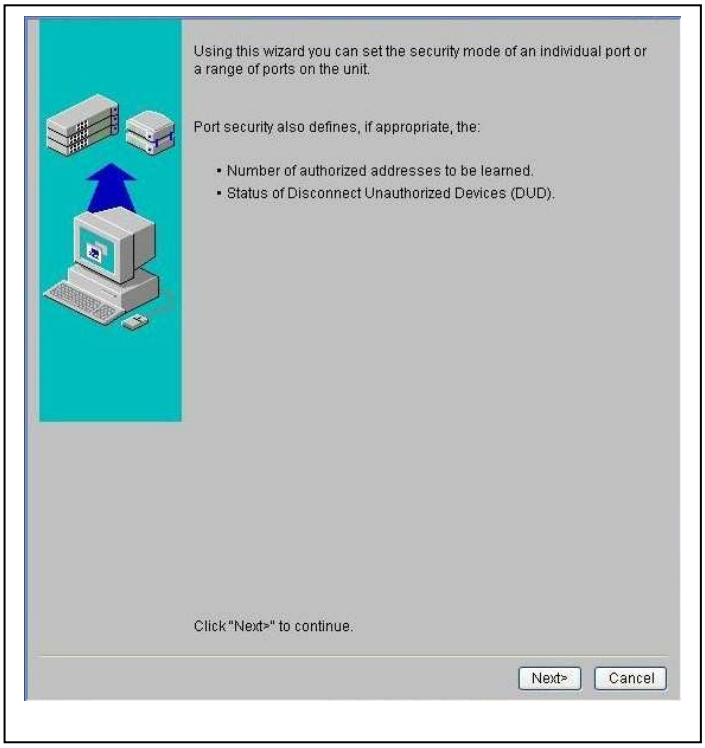



*Figura 5.1.1.2.2 Ventana principal de la configuración en seguridad en el puerto*

4. Darle click al botón Next
5. Al presionar el botón Cancel este cancelara la configuración de la seguridad en el puerto

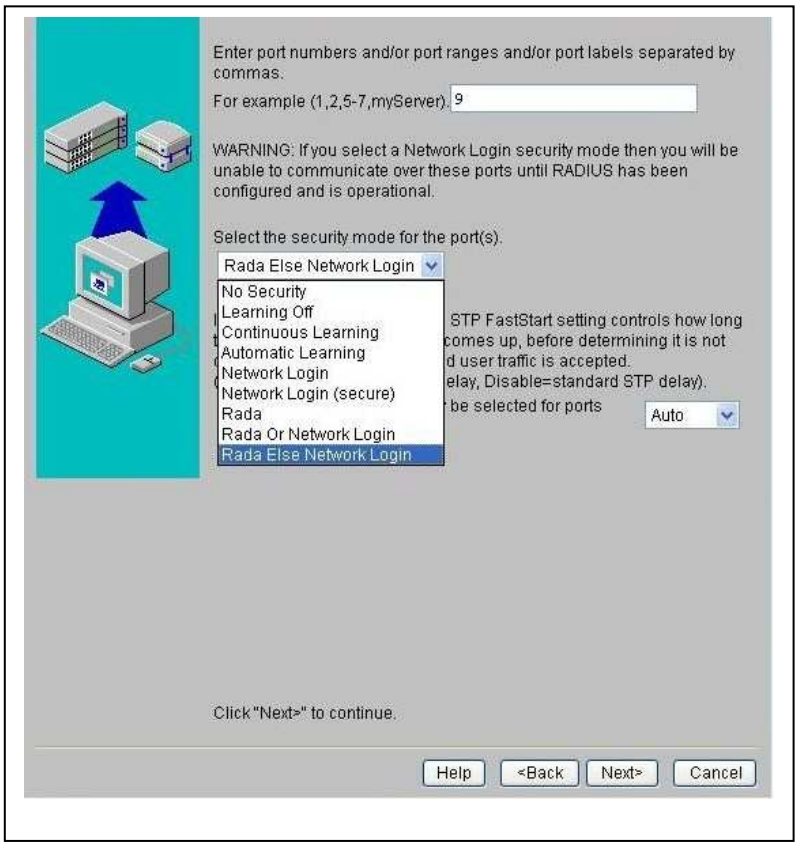



*Figura 5.1.1.2.3 Ventana de configuración del puerto y método de seguridad*

6. Introducir el número de puerto o los números de los puertos que usted desea agregarle seguridad.
7. Seleccionar Rada Else Network Login en el Modo Security
8. Presionar el botón Next para continuar
9. Presionar el botón Back para regresar a la ventana principal de la seguridad en el puerto.
10. Presionar el botón Cancel si se desea cancelar la configuración.

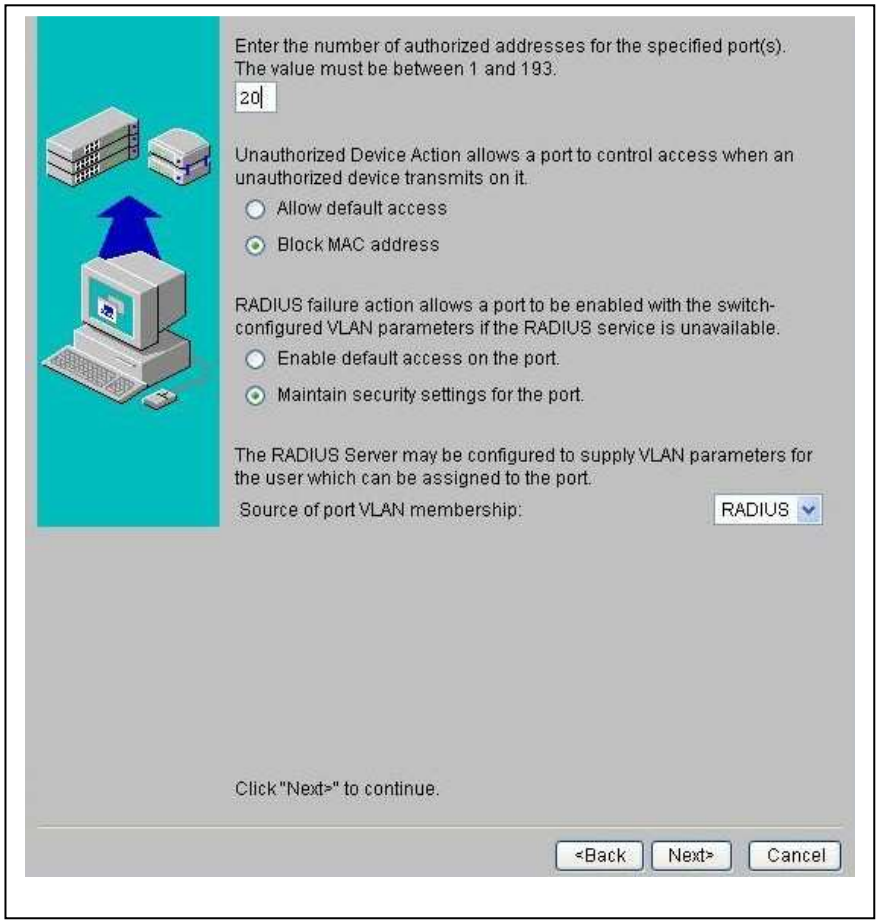



*Figura 5.1.1.2.4 Ventana de configuración de números de equipos autorizados por puertos se conectaran*

11. Introducir el numero de maquinas autorizadas a por puerto. El valor es entre 1 y 193.
12. Seleccionar la opción Block Mac Address.
13. Seleccionar la opción Maintain security settings for the port.
14. En la opción Source of port VLAN membership, seleccionar la opción RADIUS.
15. Presionar el botón Next
16. Presionar el botón Back para regresar a la ventana de configuración de números de equipos autorizados por puertos.
17. Presionar el botón Cancel si se desea cancelar la configuración.

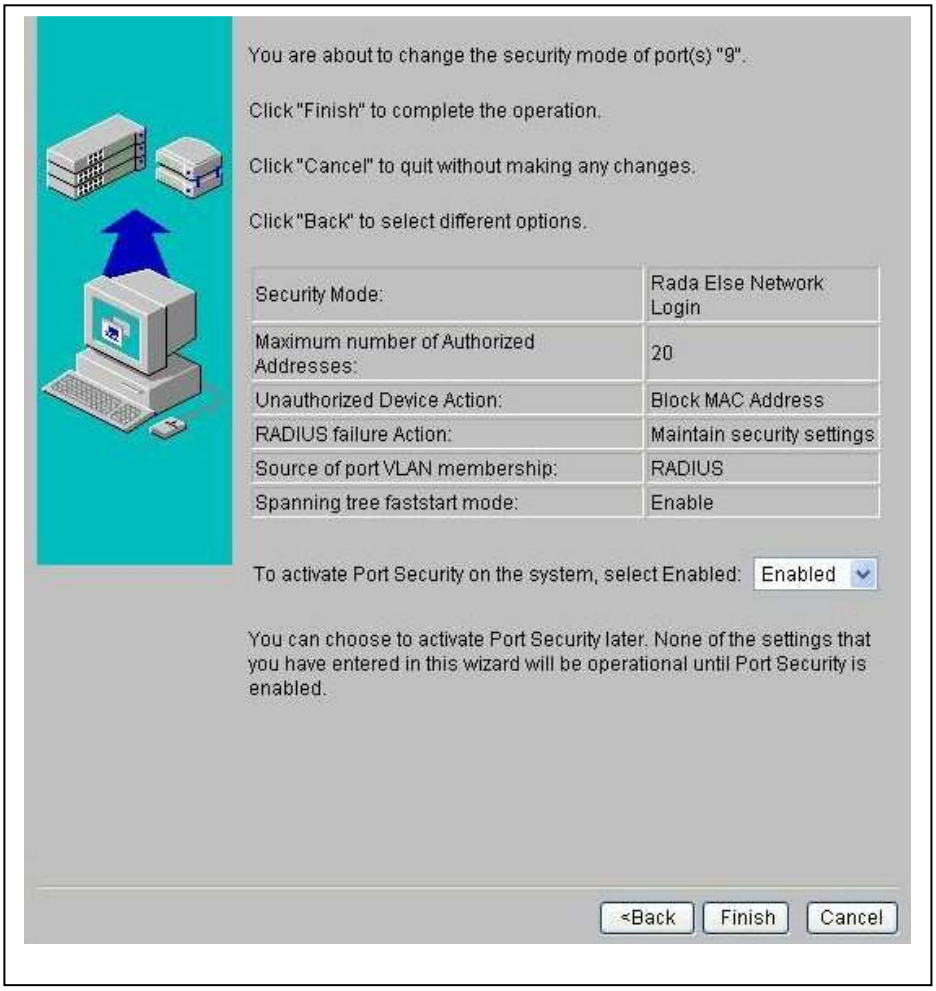



*Figura 5.1.1.2.5 Ventana de finalización de la configuración en seguridad en el puerto*

18. A continuación nos muestra un resumen de las opciones que hemos seleccionado.
19. En la opción To active Port Security on the system, Select Enable, seleccionar la opción Enabled.
20. Presionar el botón Finish para terminar la configuracion.
21. Presionar el botón Back para regresar a la ventana de finalización de la configuración en seguridad en el puerto.
22. Presionar el botón Cancel si se desea cancelar la configuración.

## 4.1.1.3 RESUMEN SEGURIDAD EN EL PUERTO

Puede ver la información resumida acerca de la seguridad en puerto del switch mediante la ventana de resumen del puerto.

Para acceder a la ventana:

1. Haga clic en Ver dispositivos a la barra de herramientas.
2. Seleccione Security -> Network -> Access -> Summary en el árbol de navegación.

El Puerto Resumen ventana.

| Port | Mode | Max Addresses | DUD Mode | Authorized |
|---|---|---|---|---|
| 1 | No Security | 1 (NA) | N/A | 0 (NA) |
| 2 | No Security | 1 (NA) | N/A | 0 (NA) |
| 3 | No Security | 1 (NA) | N/A | 0 (NA) |
| 4 | No Security | 1 (NA) | N/A | 0 (NA) |
| 5 | No Security | 1 (NA) | N/A | 0 (NA) |
| 6 | No Security | 1 (NA) | N/A | 0 (NA) |
| 7 | No Security | 1 (NA) | N/A | 0 (NA) |
| 8 | No Security | 1 (NA) | N/A | 0 (NA) |
| 9 | No Security | 1 (NA) | N/A | 0 (NA) |
| 10 | Rada Else Network Login | 10 | blockMacAddress | 0 |
| 11 | Rada Else Network Login | 10 | blockMacAddress | 1 |
| 12 | No Security | 1 (NA) | N/A | 0 (NA) |
| 13 | No Security | 1 (NA) | N/A | 0 (NA) |
| 14 | No Security | 1 (NA) | N/A | 0 (NA) |
| 15 | No Security | 1 (NA) | N/A | 0 (NA) |
| 16 | No Security | 1 (NA) | N/A | 0 (NA) |
| 17 | No Security | 1 (NA) | N/A | 0 (NA) |
| 18 | No Security | 1 (NA) | N/A | 0 (NA) |
| 19 | No Security | 1 (NA) | N/A | 0 (NA) |

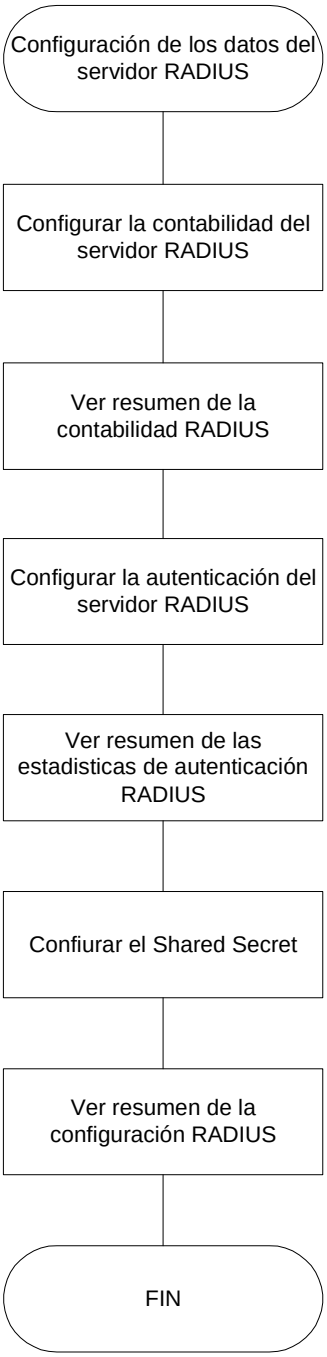
OK

*Figura 5.1.1.3.1 Ventana Resumen de la Seguridad en el puerto*

3. Presionar el botón Ok para cerrar la Ventana resumen de la seguridad en el puerto.

### *4.1.2 Configuración de los datos del servidor RADIUS*

En el siguiente diagrama se muestra los pasos necesarios para configurar los datos del servidor RADIUS en el switch




*Flujograma de la configuración de los datos del servidor RADIUS en el Switch 3Com 4200*

A continuación se detallan los pasos para configurar RADIUS en el switch, es necesario configurar la Contabilidad y la Autenticación.

## 4.1.2.1 CONTABILIDAD

Para poder modificar la configuración de contabilidad RADIUS para el Switch, será necesario utilizar la ventana Modify.

Para acceder a la ventana:

1. Haga clic en View Device en la barra de herramientas.
2. Seleccione Security -> RADIUS -> Accounting -> Modify en el árbol de navegación.
3. Mostrara la ventana Modify.

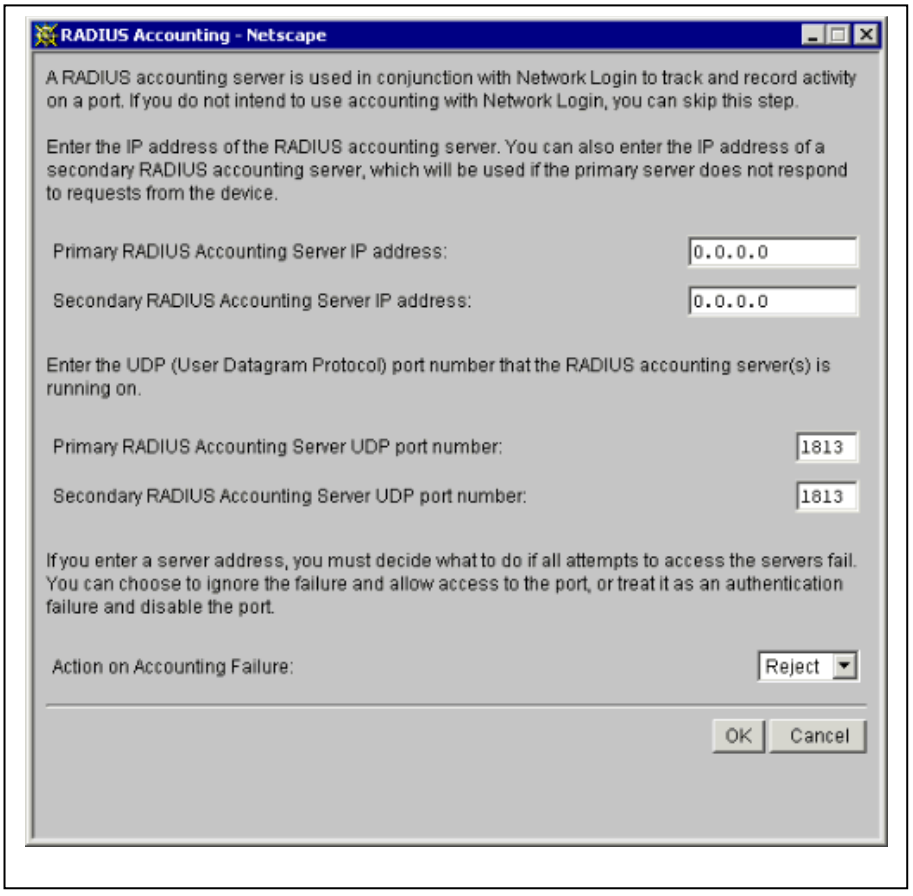



*Figura 5.1.2.1.1 Ventana de configuración de la contabilidad del RADIUS*

4. Introduzca la dirección IP de los servidores RADIUS que usted desea que sea la Primaria y Secundaria de los servidores de Contabilidad.
5. Introduzca el número de puerto UDP del servidor RADIUS Primario y Secundario de los servidores de Contabilidad, por defecto el puerto es el 1813
6. Seleccione las medidas que deben adoptarse si el acceso a los servidores falla. Puede seleccionar Ignorar para permitir el acceso al puerto, o Rechazar para desactivar el puerto.
7. Haga clic en OK.
8. Presionar el botón Cancel si desea cancelar la configuración.

## 4.1.2.2 RESUMEN DE LA CONTABILIDAD RADIUS PARA EL SWITCH

Puede mostrar las estadísticas de contabilidad RADIUS para el Switch utilizando la ventana de Display. Estas estadísticas se pueden utilizar para la vigilancia y solución de problemas de su sistema. Para acceder a la ventana de Display:

1. Haga clic en View Device en la barra de herramientas.
2. Seleccione Security -> RADIUS -> Accounting -> Display en el árbol de navegación.

Mostrara un resumen de las estadísticas de contabilidad RADIUS para el Switch.

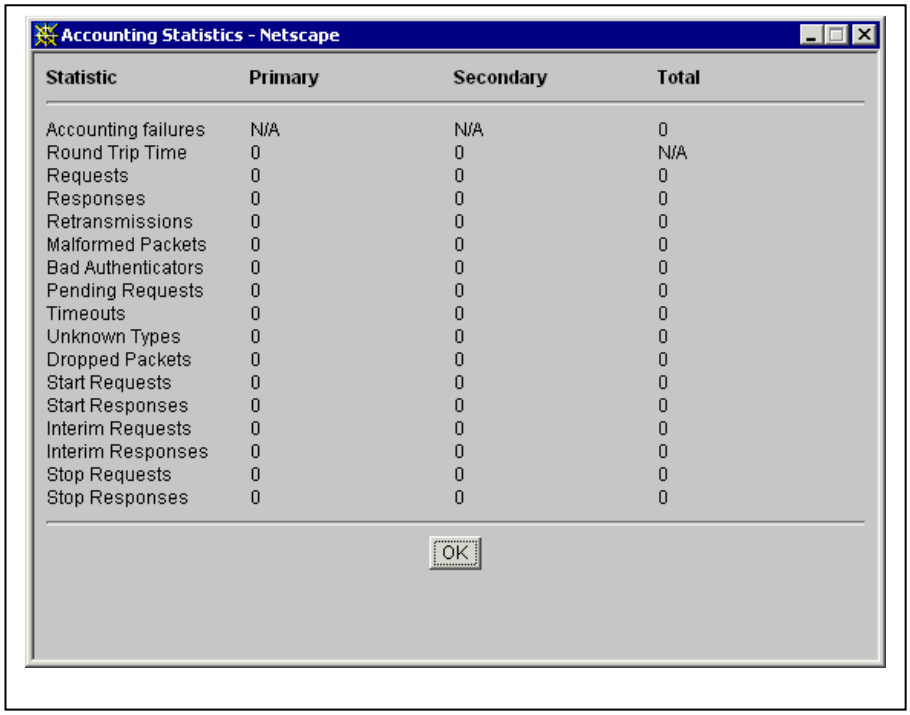



*Figura 5.1.2.2.1 Ventana Resumen de la contabilidad de RADIUS*

3. Presionar Ok para cerrar la ventana Resumen.

### 4.1.2.3 AUTENTICACIÓN

Usted puede modificar la configuración de autenticación RADIUS para el Switch utilizando la ventana Modify.

Para acceder a la ventana:

1. Haga clic en View Device en la barra de herramientas.
2. Seleccione Security -> RADIUS -> Authentication -> Modify en el árbol de navegación.
3. Mostrara la ventana de Modify.

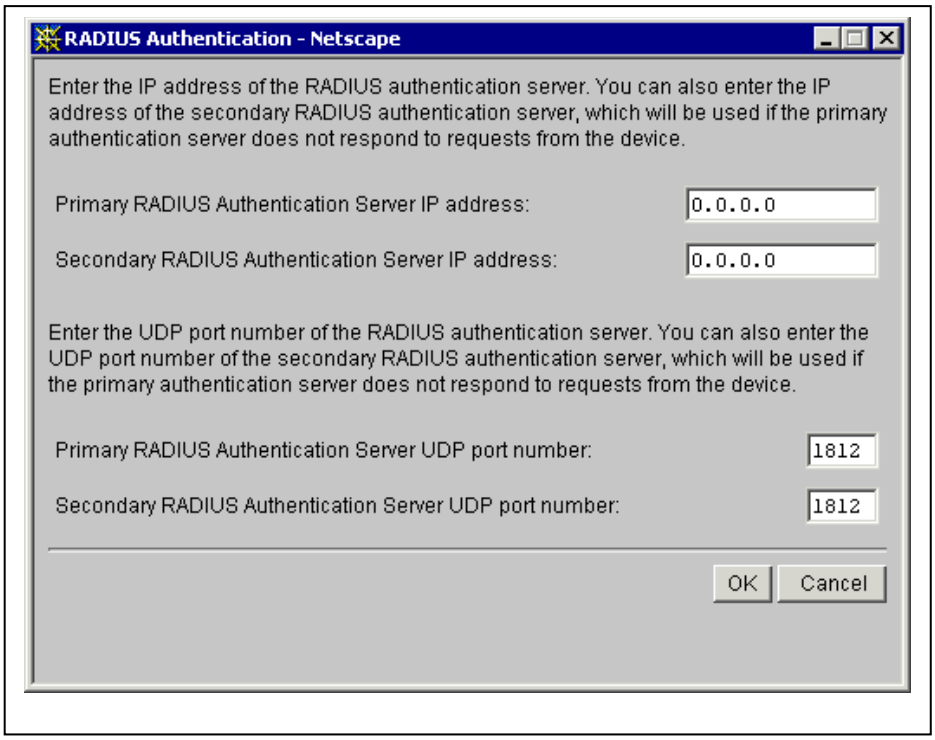



*Figura 5.1.2.3.1 Ventana de configuración de Autenticación RADIUS*

4. Introduzca la dirección IP de los servidores RADIUS primario y secundario de los servidores de autenticación.
5. Introduzca el número de puerto UDP del servidor RADIUS primario y secundario de los servidores de autenticación.
6. Haga clic en Ok.
7. Presionar el botón Cancel si desea cancelar la configuración

## 4.1.2.4 RESUMEN DE LAS ESTADÍSTICAS DE AUTENTICACIÓN RADIUS

Puede mostrar las estadísticas de autenticación RADIUS para el Switch utilizando la ventana de Display.

Estas estadísticas se pueden utilizar para la vigilancia y solución de problemas de su sistema.

Para acceder a la ventana de Display:

1. Haga clic en View Device a la barra de herramientas.
2. Seleccione Security -> RADIUS -> Authentication -> Display en el árbol de navegación.

Un resumen de las estadísticas de autenticación RADIUS para el Switch se muestra.

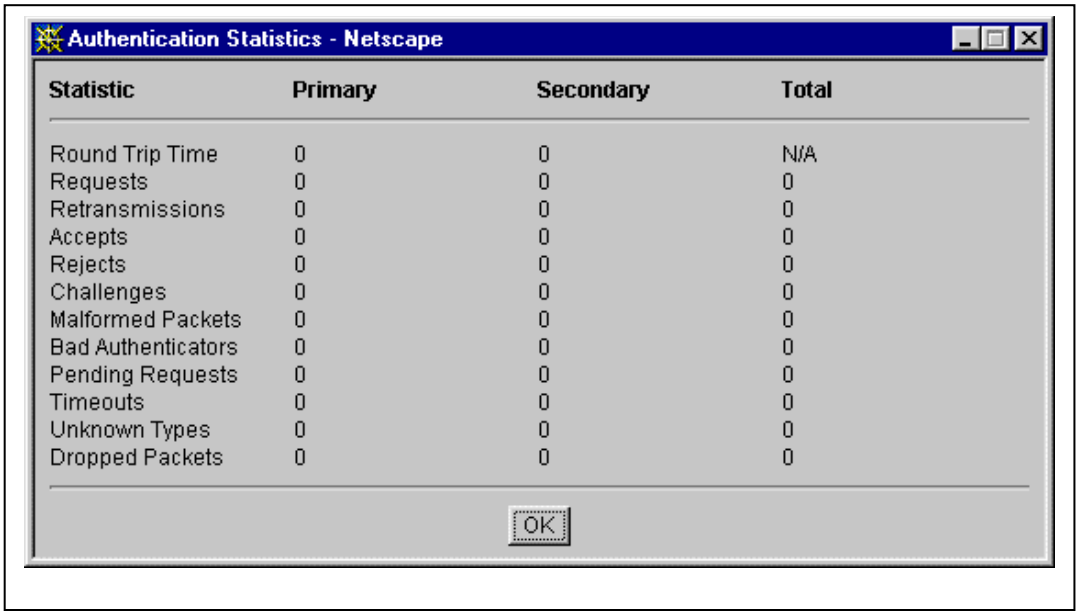



*Figura 5.1.2.4.1 Ventana Resumen de la Autenticación RADIUS*

3. Presionar Ok para cerrar la ventana Resumen.

## 4.1.2.5 SHARED SECRET

Usted puede modificar la clave de seguridad, que es el valor secreto compartido que el Switch y el servidor RADIUS usan, utilizando la ventana Shared secret.

Para acceder a la ventana:

1. Haga clic en View Device en la barra de herramientas.
2. Seleccione Security -> RADIUS -> Shared Secret en el árbol de navegación.
3. Mostrar la ventana Shared Secret en la pantalla.

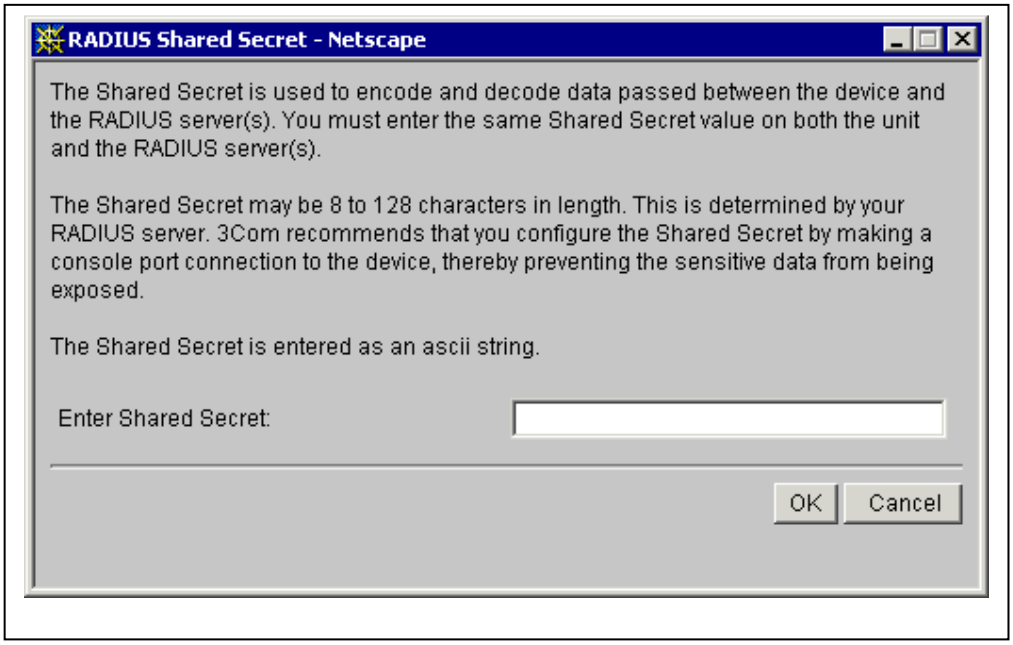



*Figura 5.1.2.5.1 Ventana de configuración de la Clave Compartida*

4. Introduzca el Shared Secret.
5. Haga clic en Aceptar.
6. Presionar el botón Cancel si desea cancelar la configuración

## 4.1.2.6 RESUMEN RADIUS

Puede mostrar un resumen de los ajustes de configuración RADIUS de los Switch en la sección Summary.

Para acceder a la ventana:

1. Haga clic en View Device a la barra de herramientas.
2. Seleccione Security -> RADIUS -> Summary en el árbol de navegación.
3. Mostrara la ventana Summary.

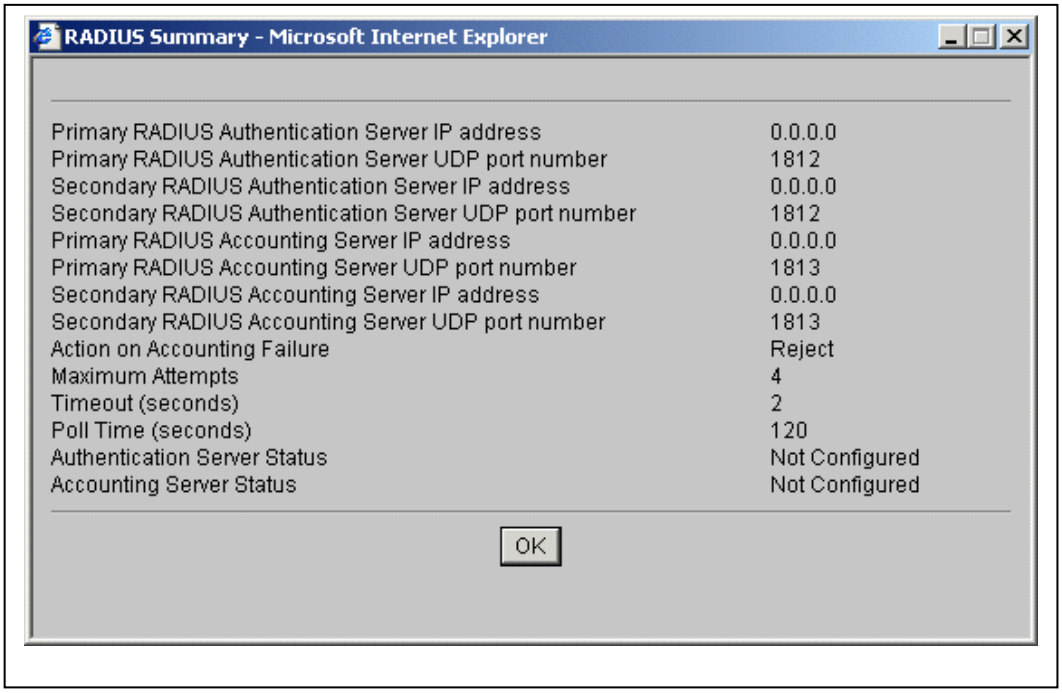



*Figura 5.1.2.6.1 Ventana Resumen de las configuraciones RADIUS*

4. Presionar Ok para cerrar la ventana Resumen.

### *4.1.3 Configuración de una IP al switch 3com 4200*

Se muestra el diagrama de la secuencia lógica de pasos para configurar una dirección IP en el switch.


*Flujograma de la configuración de una IP en el Switch 3Com 4200*

Para acceder a la interfaz web por primera vez o tras una inicialización se muestran los primeros pasos del asistente, le permite introducir la configuración básica de información para la el Switch.
Para acceder al asistente:

1. Haga clic en View Device en la barra de herramientas.
2. Seleccione System -> Primeros pasos en el árbol de navegación.

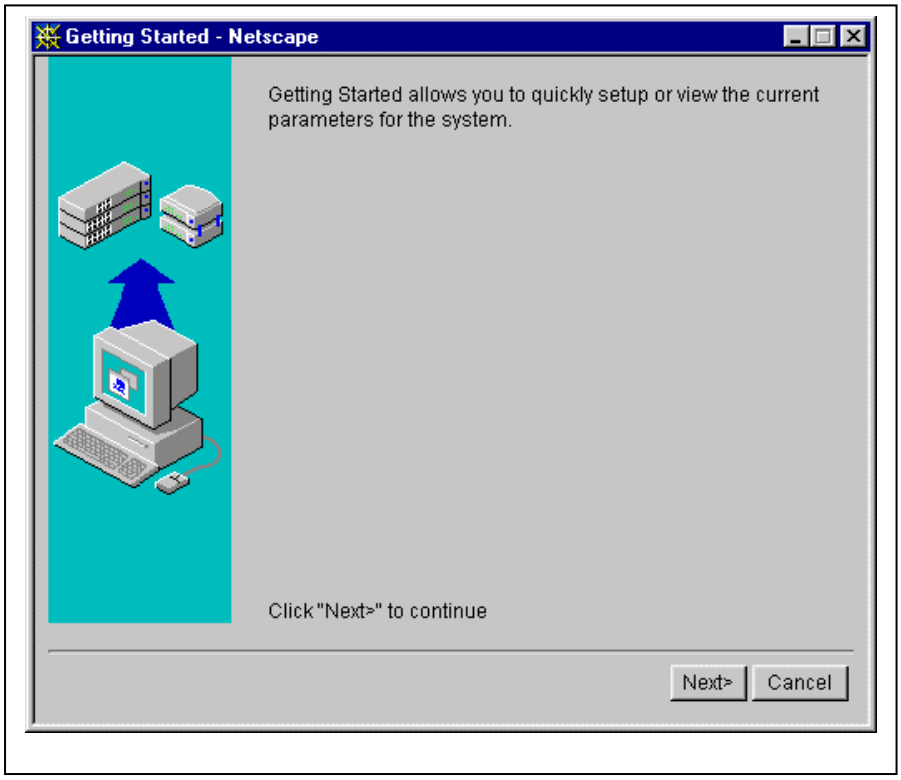



*Figura 5.1.3.1 Ventana principal de configuración de IP al switch 3com 4200*

3. A medida que pasan por el asistente, es necesario que usted escriba:
    - Un nombre descriptivo para el Switch.
    - La ubicación física de del Switch.
    - El nombre de la persona a contactar acerca del Switch.

También se tiene otras opciones:

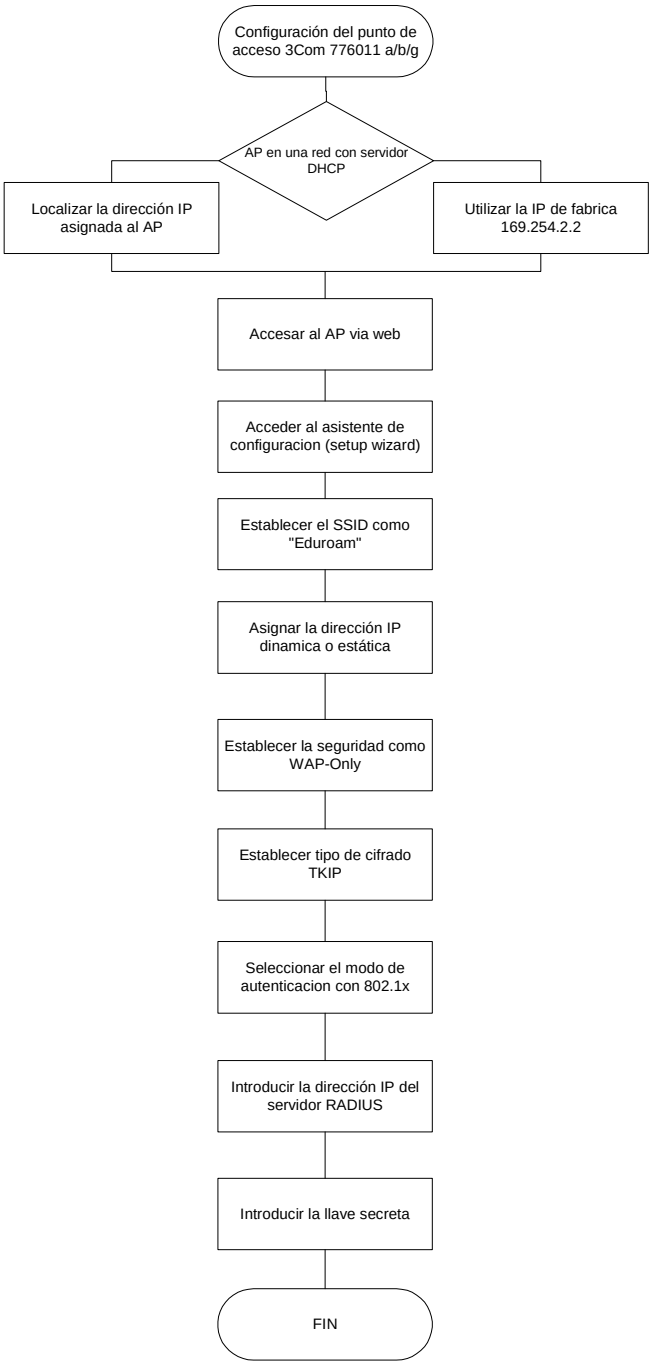
- Configurar manualmente la información IP para el Switch
    - Dirección IP: Le permite entrar en una única dirección IP para el Switch
    - Máscara de subred: Le permite entrar en una máscara de subred para el Switch.
    - Puerta de enlace predeterminada (enrutador): Si la red contiene una o varias puertas de entrada, este campo le permite introducir la dirección IP de la puerta de enlace por defecto.
- Configurar automáticamente la información IP para el Switch
    - El interruptor automático tiene tres métodos de configuración IP que intenta a su vez, estos son: DHCP, Auto-IP y BOOTP.
- Desactivar la interfaz LAN

4. Si selecciona Ninguno, no seguir las instrucciones que se muestran.
5. Una nueva contraseña para el usuario actual (introduce la contraseña existente si desea dejar la contraseña sin cambios).

## 4.2 Puntos de Acceso 3Com 7760 11 a/b/g

### 4.2.1 Configuración del Access Point 3Com 11a/b/g

El diagrama siguiente muestra el proceso de configuración del punto de acceso:




*Flujograma de la configuración del acces point 3Com 776011 a/b/g*

Si la configuración por defecto del AP[29] no cumple con los requisitos de la red, o si quiere personalizar la configuración de su propia red, puede usar estas herramientas para cambiar la configuración:

1. Inicie el 3Com Wireless Infraestructura Administrador de dispositivos (Widman) utilidad.
2. Conectar directamente al dispositivo a través de su puerto Ethernet o puerto de consola.

### 4.2.1.1Redes con un servidor DHCP

Si la red tiene un servidor DHCP, una dirección IP se asigna automáticamente al AP. Se tarda entre uno y dos minutos para que el Punto de Acceso determine si hay un servidor DHCP en la red. Utilice el 3Com Wireless Infraestructura Administrador de dispositivos (Widman) incluido en el CD de instalación de 3Com para localizar el punto de acceso sobre la red y ver su dirección IP.

Después de determinar la direccion IP del AP, puede introducir la dirección IP en un navegador web en su ordenador en la misma subred para ver el estado del sistema o cambiar su configuración en el AP.

### 4.2.1.2Redes sin un servidor DHCP

Si la red no tiene un servidor DHCP, el AP utiliza una dirección IP de fábrica (169.254.2.2). Puede utilizar esa dirección IP para configurar el AP, o bien puede asignar una nueva dirección IP al AP.
Para verificar que el punto de acceso está utilizando la dirección IP por defecto:

1. Conecte un ordenador directamente al AP utilizando el estándar suministrado Categoría 5 UTP cable Ethernet.
2. Introduzca la dirección IP por defecto (169.254.2.2) en el ordenador a través del navegador web. Si el Sistema de Gestión de Configuración arranca, el punto de acceso está utilizando la dirección IP asignada de fábrica. Usted puede configurar el AP con la siguiente información de acceso:
    - Usuario: admin
    - Contraseña: password

Si el Sistema de Gestión de configuración no se inicia, el Punto de Acceso se encuentra en una subred diferente de la computadora. Instalar e iniciar el 3Com Wireless Infraestructura Administrador de dispositivos para descubrir el punto de acceso de la dirección IP.

[29] AP: Punto de Acceso ( Access Point)

## 4.2.1.3Estado del sistema (SYSTEM STATUS)

La interfaz Web ha sido diseñada para que pueda realizar fácilmente las tareas de configuración avanzada y ver información acerca de la AP

### *4.2.1.3.1 RESUMEN DEL SISTEMA (SYSTEM SUMMARY)*

Después de hacer clic en Logon al iniciar la sesión en la pantalla, verá la página de estado del sistema en la pantalla. La página de resumen del sistema es la página por defecto que aparecerá una vez que consiga entrar satisfactoriamente. La página de resumen del sistema muestra todos los datos sobre la configuración de tu AP.

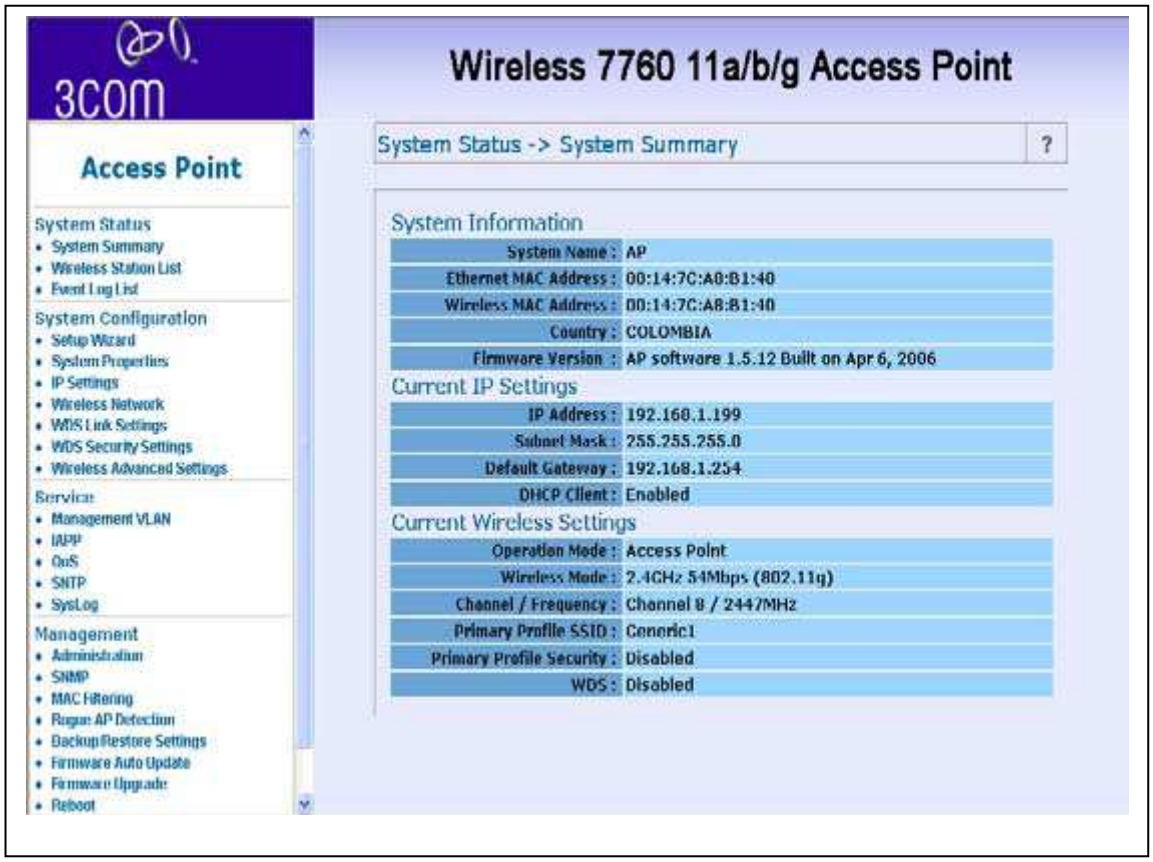



*Figura 521311 Ventana resumen de configuración del Punto de Acceso*

### *4.2.1.3.2 CONFIGURACION DEL SISTEMA (SYSTEM CONFIGURATION)*

En esta parte, se mostrara cómo configurar las funciones básicas de su red inalámbrica en el AP.

#### 4.2.1.3.2.1 ASISTENTE DE CONFIGURACION (SETUP WIZARD)

El asistente de configuración lo guiará para la configuración AP. A continuación se presentan los pasos a realizar dicha configuración:

1. Darle clic a la opción Setup Wizard
2. Mostrara la ventana de Redes Inalámbricas (Wireless Network)

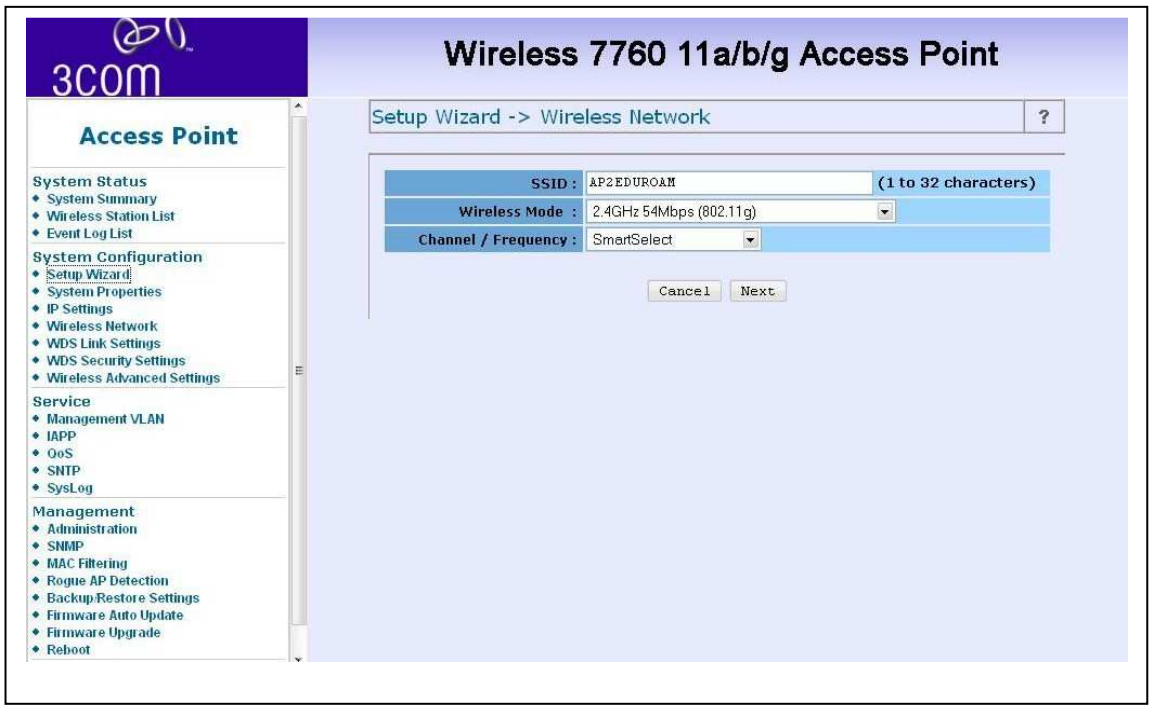



*Figura 5.2.1.3.2.1.1 Ventana de configuración de la red inalámbrica*

3. En la sección SSID colocar el nombre de la Red Inalámbrica a mostrar, en este caso Eduroam
4. Seleccionar el botón Next
5. Mostrara la ventana Configuración IP (IP SETTINGS)
6. Si desea cancelar la configuración presionar el botón Cancel

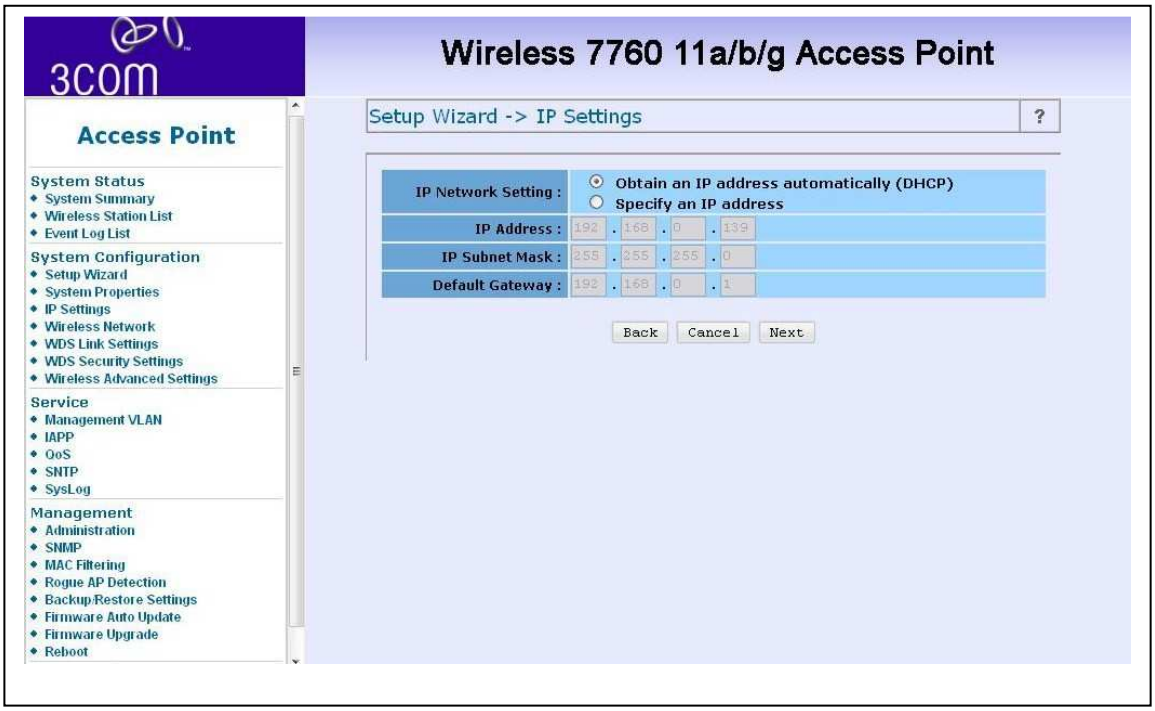



*Figura 5.2.1.3.2.1.2 Ventana de configuración de la dirección IP*

7. Seleccionar la opción Obtain an IP address automatically (DHCP)
8. O si ya tiene una ip designada para el AP seleccionar Specify an IP address
    a. Introducir la dirección IP en IP Address
    b. Introducir la máscara de subred en IP Subnet Mask
    c. Introducir la Puerta de enlace predeterminada en Default Gateway
9. Presionar el botón Next
10. Mostrara la ventana Configuración de la seguridad inalámbrica (Wireless Security Settings), es aquí donde configuraremos el protocolo 802.1X con RADIUS.


*Figura 5.2.1.3.2.1.3 Ventana de configuración de la seguridad inalambrica*

11. En la opción Security seleccionar WPA-Only
12. En la opción Cipher Type: seleccionar TKIP
13. En la opción de Authentication Mode seleccionar 802.1X
14. Introducir la dirección IP del Servidor RADIUS
15. Por defecto el puerto de RADIUS es 1812
16. Introducir la llave secreta de RADIUS
17. Presionamos el botón Finish.

El AP 3COM 7760 11a/b/g se reiniciara para guardar las modificaciones hechas y estará listo y configurado con los protocolos RADIUS y 802.1X

# *ANEXO 13 SITIO CAUTIVO*

Eduroam llama Sitio Cautivo a las paginas HTML que sirven para autenticar a los usuarios y poder asi dejarlos ingresar en la red de la institución.

Para el Proyecto Mundial Eduroam dentro de sus políticas hace referencia al NO utilizar este tipo de sitios cautivos para autenticar a los usuarios de las instituciones debido a que soy muy vulnerables a ataques. A continuación se presenta el texto donde Eduroam hace mención a este tema: "*Las organizaciones participantes deben disponer de mecanismos de monitorización y seguimiento que permitan conocer el estado de los servidores de autenticación, para poder analizar problemas de conexión. De acuerdo con la política establecida para el servicio a nivel europeo, sólo podrá usarse el SSID "Eduroam" para mecanismos de control de acceso basados en el* ***estándar IEEE 802.1X****. Aquellas organizaciones que usen otros métodos (notablemente,* ***los basados en redirecciones HTTP****) cuentan para su adaptación con una moratoria que expira* ***el 30 de septiembre de 2007***."[30]

A continuación se presenta un ejemplo de una pantalla de un Sitio Cautivo que se utiliza al ingresar en la red FIA.

1. Al conectar el cable de red a la tarjeta de red, este resuelve y asigna una dirección IP a la maquina.
2. Al abrir un navegador web, este direcciona al sitio cautivo, donde aparece una ventana de alerta de seguridad.

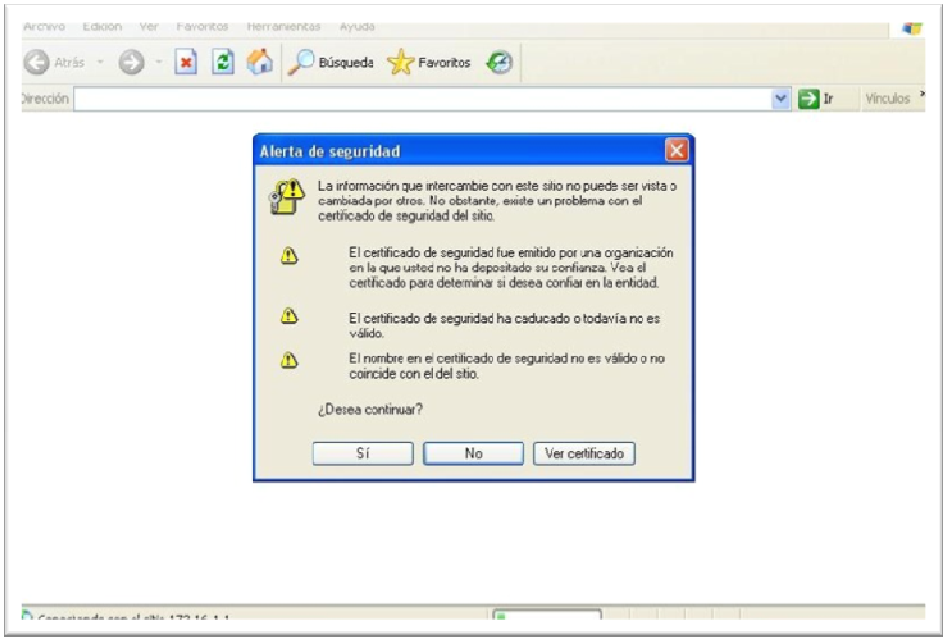



*Figura 13.1 Ventana de alerta de seguridad*

3. Presionar el Botón Si

[30] http://www.eduroam.es/politica.es.php

4. Mostrara la ventana donde pide Usuario y Contraseña

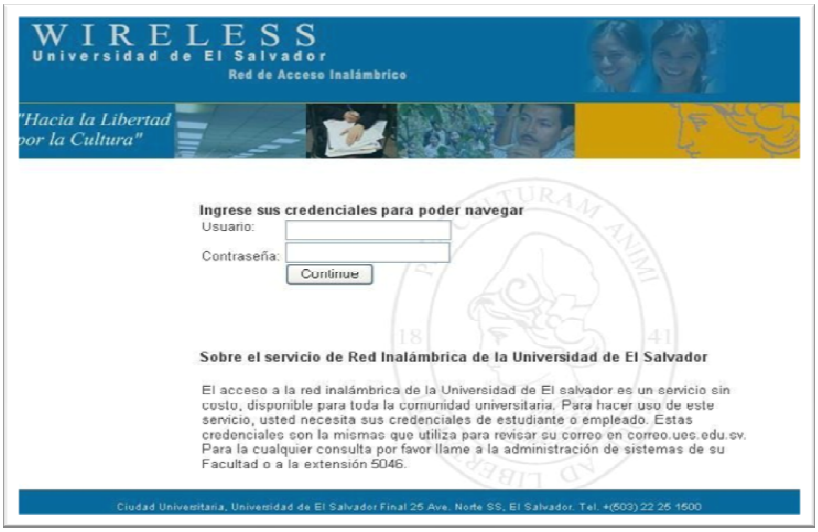



Figura 13.2 Pagina web del sitio cautivo

5. Ingresar el Usuario y Contraseña


Figura 13.3 Pagina web del sitio cautivo

6. Presionar el botón Continúe
7. Si nos encuentra nos dará permiso para ingresar a la red y cargara la pantalla de inicio en el navegador web.

# *ANEXO 14 DIRECTORIO*

**E-LEARNING**

Por definición, el e-Learning es el suministro de programas educacionales y sistemas de aprendizaje a través de medios electrónicos. El e-Learning se basa en el uso de una computadora u otro dispositivo electrónico (por ejemplo, un teléfono móvil) para proveer a las personas de material educativo. La educación a distancia creó las bases para el desarrollo del e-Learning, el cual viene a resolver algunas dificultades en cuanto a tiempos, sincronización de agendas, asistencia y viajes, problemas típicos de la educación tradicional.

Así mismo, el e-Learning puede involucrar una mayor variedad de equipo que la educación en línea. El término de e-Learning o educación electrónica abarca un amplio paquete de aplicaciones y procesos, como el aprendizaje basado en Web, capacitación basada en computadoras, salones de clases virtuales y colaboración digital (trabajo en grupo).

**Ventajas de los programas de e-Learning**

En seguida presentamos lo que los expertos en esta materia consideran como las ventajas más importantes de la educación electrónica:

- **Mayor productividad**: Las soluciones de aprendizaje electrónico como la capacitación basada en Web (WBT, web-based training) y la capacitación basada en computadora (CBT computer-based training) permite a los alumnos estudiar desde su propio escritorio. La entrega directa de los cursos puede disminuir los tiempos muertos que implican una escasa productividad y ayuda a eliminar costos de viajes.
- **Entrega oportuna**: Durante la puesta en marcha de un nuevo producto o servicio, el e-Learning puede proveer entrenamiento simultáneo a muchos participantes acerca de los procesos y aplicaciones del nuevo producto. Un buen programa de e-Learning puede proveer la capacitación necesaria justo a tiempo para cumplir con una fecha específica de inicio de operaciones.
- **Capacitación flexible**: Un sistema e-Learning cuenta por lo general con un diseño modular. En algunos casos, los participantes pueden escoger su propia ruta de aprendizaje. Adicionalmente, los usuarios pueden marcar ciertas fuentes de información como referencia, facilitando de este modo el proceso de cambio y aumentando los beneficios del programa.
- **Ahorros en los costos por participante**: Tal vez el mayor beneficio del e-Learning es que el costo total de la capacitación por participante es menor que en un sistema tradicional guiado por un instructor. Sin embargo, los programas de e-Learning diseñados a la medida pueden

de entrada ser más costosos debido al diseño y desarrollo de los mismos. Se recomienda llevar a cabo un análisis minucioso para determinar si el e-Learning es la mejor solución para sus necesidades de capacitación y adiestramiento antes de invertir en el proyecto.

**¿Qué detiene al e-Learning?**

Entre las principales barreras que han impedido la integración de estas tecnologías del e-Learning en los programas de capacitación de las empresas, se encuentran:

1. Estructura organizacional y tradicionalismo.
2. La falta de ejemplos de mejores prácticas.
3. La falta de soporte y experiencia.
4. La falta de comprensión y visión acerca del e-Learning.
5. La falta de recurso humano y aceptación por parte del usuario.
6. Organizaciones y procesos tradicionales.
7. La falta de de habilidad por parte de profesores e instructores, aunada a una actitud negativa.
8. Falta de acciones estratégicas.
9. Falta de entrenamiento y soporte a los profesores e instructores.
10. El tiempo requerido para la preparación del material.

**Los errores más comunes**

Como toda tecnología emergente, la educación electrónica requiere de la participación de consultores expertos que puedan implementar un programa que conduzca a las organizaciones a buenos resultados. En seguida se presentan los diez errores más comunes al definir una estrategia de e-Learning:

1. No tener visión.
2. Confundir la estrategia con la tecnología.
3. Colocar el Sistema de Administración de Aprendizaje (LMS, learning management system) como eje central de la estrategia.
4. Concentrarse en el desarrollo y en la entrega más que en el propio negocio.
5. Enfocarse en transformar un programa de capacitación convencional en un programa de educación en línea.
6. No lograr un consenso entre los asociados.
7. No diagnosticar a tiempo la falta de soporte por parte de la alta dirección.
8. Pensar que esta nueva función es una labor de tiempo parcial o de corta duración.
9. Ignorar las debilidades y los peligros.
10. Fallar en la administración del cambio.

**Señales de una implementación exitosa**

Una forma de poder diagnosticar que el proyecto cuenta con una apropiada identidad y dirección es a través de la identificación de los siguientes elementos:

- **Soporte**: "Deseamos que esto se logre".
- **Patrocinio**: "Estamos proveyendo los recursos para que los objetivos del proyecto se cumplan".
- **Integración**: "Deseamos que nuestros esfuerzos se enfoquen en las necesidades reales del negocio".
- **Supervisión**: "Estaré observando personal y continuamente los avances para asegurarme que los objetivos se cumplan".
- **Participación**: "Me estoy conectando en este momento a la red para experimentar esto por mí mismo"

De hecho, estos últimos cinco puntos son comunes a proyectos de implementación de otras tecnologías, como pueden ser los sistemas de información y la mercadotecnia en Internet.

**Diseñando la educación del mañana**

A pesar de que en México ya existen empresas que ofrecen soluciones de e-Learning, que involucran contenido desarrollado por expertos, plataformas de administración e infraestructura y otros servicios, la aceptación de estas tecnologías todavía no es la que esta industria desearía tener. Afirman expertos que la adopción de e-learning en México ha sido lenta, pues existen barreras culturales.

Al igual que otras iniciativas como e-México, las instituciones públicas y privadas están obligadas a diseñar e implementar programas específicos para impulsar la educación electrónica en América Latina. Es imprescindible movilizar a las comunidades educacionales y culturales, así como a los actores económicos y sociales, para acelerar los cambios en los sistemas de educación y capacitación para que nuestros países se muevan hacia una sociedad basada en conocimientos.

Una iniciativa de e-Learning podría ser un camino más para modernizar nuestra economía. Al mismo tiempo, a través de los componentes de la educación electrónica, se pueden proveer a toda la comunidad, pero particularmente a nuestros jóvenes, de las habilidades y herramientas que ellos necesitan para tener éxito en una economía globalizada y basada en el conocimiento. Quienes se encuentran más interesados en este tipo de proyectos son desde luego las instituciones educativas, que por la reducción de costos tanto para el alumno como para la propia institución, significan un gran incentivo.

Mientras que las empresas continúen contratando egresados de las universidades que demanden recursos de Internet y acceso a información basada en tecnologías Web, es cuestión de tiempo que las mismas organizaciones se den cuenta de que la adopción de esta nueva generación de tecnologías es inminente.

**Información de personal que trabaja para e-learning**

- MELCOE: http://www.melcoe.mq.edu.au/index.htm
    - Contacto: James Daziel
    - Correo: jdaziel@melcoe.mq.edu.au
    - Contacto: MELCOE
    - Correo: rvance@melcoe.mq.edu.au
- Cursos de Español en Internet: http://ave.cervantes.es/
    - Contacto: infoave@cervantes.es

**E-CIENCIA**

Se trata de un concepto sencillo, que trata de aprovechar la maraña de redes informáticas de alta velocidad que recubre el planeta para crear la más potente herramienta de investigación imaginable, al servicio de disciplinas tan variadas como la Física, Medicina, Biogenética, Humanidades y en general todos los ámbitos del saber.

Por ejemplo, los científicos e ingenieros necesitan ordenadores de mayor capacidad computacional para afrontar investigaciones y desarrollos más y más complejos, desde modelos climáticos hasta el diseño de nuevos aviones. ¿Se imaginan que a través de Internet se pudieran unir los computadores más rápidos para que funcionaran como uno solo, independientemente de cuál sea su situación geográfica? Este es uno de los objetivos de la e-Ciencia.

Por otro lado, vivimos en la época de la información. Se ha generado en los últimos cinco años más cantidad de datos que en toda la historia de la humanidad. La e-Ciencia permite acceder, contrastar y analizar, es decir, extraer conocimiento de una manera eficiente de todo este volumen de información compartido en miles de bases de datos a lo largo y ancho de la Tierra.

Incluso la tradicional imagen de un científico encerrado en su laboratorio está cambiando. Gracias a la e-Ciencia, el investigador podrá controlar telescopios, microscopios electrónicos, estaciones sísmicas, etc., así como asistir a reuniones, impartir conferencias, dar clases... todo ello sentando cómodamente en la silla de su despacho, aunque éste se encuentre a kilómetros de distancia.

**Información de personal que trabaja para e-ciencia**

- Proyecto e-Ciencia de Madrid: http://www.madrimasd.org/informacionIDI/e-ciencia/
    - Contacto: e-ciencia@madrimasd.org.
- Proyecto E-e-Ciencia de la Universidad rey Juan Carlos: http://www.urjc.es/z_files/ac_biblio/nuevaweb/eciencia/eciencia.htm

    - Contacto: Fernando Silva Sánchez
    - Correo: fernando.silva@urjc.es
- Red Española de e-Ciencia: http://www.e-ciencia.es/iniciativas.jsp
    - Contacto: oficina.e-ciencia@upv.es
- Centro de Supercomputacion de Cataluya: http://www.cesca.es/es/novetats/2005/octubre.html
    - Contacto: info@cesca.es

# *ANEXO 15 POLITICAS DE PARTICIPACION A EDUROAM*

**Introducción**

La creación de un espacio común de movilidad entre todas las instituciones académicas y de investigación englobadas en las redes europeas de investigación, requiere la adopción de una política común de uso de la tecnología.

Este documento pretende ser una guía de uso de la infraestructura eduroam para España, que está basado y es compatible con la política desarrollada dentro de la actividad JRA5 de GÉANT2.

**Objetivo**

El objetivo principal de este documento es formalizar la relación entre organizaciones que configuran **"eduroam ES"**, aportando procedimientos compatibles con la misma iniciativa a nivel europeo y que faciliten la gestión de la movilidad entre organizaciones a nivel nacional.

**La idea**

El proyecto eduroam ES consiste en el desarrollo de un espacio de colaboración para facilitar la movilidad en el acceso a la red entre organizaciones de la comunidad RedIRIS, de tal forma que cuando sus usuarios viajen a otras organizaciones, éstos puedan disponer de una manera automática de servicios de conectividad u otros que en un futuro se vayan considerando como necesarios.

Esta política esta desarrollada en concordancia con la desarrollada a nivel de las redes de investigación europeas. Es responsabilidad del usuario móvil respetar las políticas de uso tanto de la institución visitada, como de su organización origen.

**Servicio de movilidad - Principios generales**

El servicio de movilidad común debe ser prestado únicamente a usuarios que pertenezcan a organizaciones afiliadas a redes de investigación que pertenecen al proyecto de espacio común de movilidad a nivel internacional.

A todos los usuarios móviles se les requerirá autenticarse frente a su organización origen, con el fin de obtener servicios de acceso en la organización visitada.

Todos los usuarios móviles son responsables de sus credenciales y deben respetar la política de uso aceptada por su organización origen.

Las organizaciones visitadas deben ofertar servicios de acceso, y además, los usuarios móviles podrán reconocerlos y hacer uso de ellos.

La organización visitada debe garantizar la transmisión segura de las credenciales de los usuarios móviles.

La organización visitada tiene potestad de bloquear el acceso a cualquier usuario móvil, institución o red europea de investigación, si no cumpla con la política de uso de la organización visitada.
Las organizaciones visitadas establecerán la autorización para el acceso a los servicios prestado a los usuarios móviles.
La organización origen será responsable de dar soporte a sus usuarios, incluyendo formación en tecnologías de acceso y aceptación de políticas de uso.

**Requisitos a cumplir por las organizaciones participantes en eduroam ES**
Las organizaciones participantes deben responsabilizarse de formar a sus usuarios en el respeto a las políticas de uso de las organizaciones visitadas, y ayudar en cualquier aspecto relacionado con sus usuarios.

Las organizaciones participantes deben poseer un servidor de autenticación (NAS) que pueda, de un modo seguro, procesar y transmitir las credenciales de usuario solicitadas, utilizando para ello paquetes Access-Accept de RADIUS, en conformidad con la sección 3.16 de la RFC3580.
Las organizaciones participantes deberían disponer de mecanismos para informar a los usuarios visitantes de en qué medida y cómo ofertan sus servicios de movilidad.

Es obligatorio el uso del SSID "eduroam" excepto en aquellos casos en los que exista un solapamiento de puntos de acceso de distintas organizaciones físicamente muy cercanas. Para aquellos puntos de acceso en los que se de este solapamiento se recomienda el uso de SSIDs de la forma "eduroam-[INST]", donde [INST] son una sigla descriptiva de la institución a la que pertenece cada uno de los puntos de acceso en cuestión.

Las organizaciones participantes deberían disponer de mecanismos para informar a sus usuarios visitantes de los niveles de seguridad ofrecidos en la transmisión de credenciales.
Las organizaciones participantes deben informar a sus usuarios del servicio de movilidad, señalando que el soporte técnico recae sobre su organización origen. Sólo cuando la organización origen determina que el problema es responsabilidad de la organización visitada, éste debe ser revisado con la organización visitada.

Las organizaciones participantes deben guardar información relativa a sesiones de autenticación y acceso a la red. Asimismo deben ser capaces de capaces de realizar un seguimiento de un usuario por razones de seguridad o gestión de capacidad. En concreto, deberán mantener la correlación de direcciones MAC y direcciones IP dadas a los visitantes mediante DHCP, junto con la hora, establecida a partir de una fuente fiable de tiempo, en la que se produjo la asignación. Las organizaciones participantes deben comunicar problemas de seguridad o uso fraudulento tanto a los responsables de la iniciativa eduroam ES, como a los responsables de seguridad de RedIRIS (IRIS-CERT), para solucionarlo de manera coordinada.

Las organizaciones participantes deben disponer de mecanismos de monitorización y seguimiento que permitan conocer el estado de los servidores de autenticación, para poder analizar problemas de conexión.

De acuerdo con la política establecida para el servicio a nivel europeo, sólo podrá usarse el SSID "eduroam" para mecanismos de control de acceso basados en el estándar IEEE 802.1X. Aquellas organizaciones que usen otros métodos (notablemente, los basados en redirecciones HTTP) cuentan para su adaptación con una moratoria que expira **el 30 de septiembre de 2007**.

# *ANEXO 16 REGLAMENTO DE ESCALAFON DE LA CARRERA DOCENTE Y LEY ORGANIGA DE LA UNIVERSIDAD DE EL SALVADOR*

Articulo 64 del Capitulo VIII del Reglamento de Escalafón de la Carrera Docente de la Universidad de El Salvador:

CAPITULO VIII

De la Escala de Salarios

Art. 64.- Las escalas e incrementos de salarios correspondientes a las diferentes clases y categorías establecidas en el presente Reglamento, se fijarán anualmente por acuerdo de Junta Directiva de cada Facultad, sujeto a ratificación por parte del Consejo Superior Universitario, tomando como base las disponibilidades presupuestarias y las exigencias del costo de vida adecuadamente ponderadas por una sana y realista política de salarios y desarrollo de recursos humanos, en lo posible con criterio de uniformidad dentro de las respectivas clases y categorías conforme al Art. 8 para todas las Unidades de la Universidad de El Salvador.

Articulo 52 de la Sección Cuarta de la Ley Orgánica de la Universidad de El Salvador:

**Sección Cuarta**
**DEL ESCALAFÓN DEL PERSONAL**

**Funcionamiento**

Art. 52.- La Universidad contará con un sistema de escalafón para su personal académico y administrativo no docente, que contendrá la respectiva clasificación de los cargos, así como los criterios básicos para la aprobación de ascensos y estímulos por merecimientos del personal y los mecanismos para la promoción social y salarial del mismo. Regulará además los deberes y derechos del personal, especialmente los relacionados con la capacitación constante y con el régimen disciplinario aplicable al mismo.

El sistema de escalafón de la Universidad será aprobado o reformado, con los dos tercios de los votos de la Asamblea General Universitaria, a propuesta del Consejo Superior Universitario. Sus disposiciones deberán ajustarse periódicamente al presupuesto ordinario de la Universidad, en la respectiva Ley de Salarios.