REVISIÓN DE LOS CONCEPTOS Y TECNOLOGÍAS UTILIZADAS EN LA IMPLEMENTACIÓN DE UN SISTEMA FEDERATIVO TIPO EDUROAM

ARNOL ALBERTO HERNANDEZ SERNA
ANDRES JULIAN GRAJALES MARIN

UNIVERSIDAD CATÓLICA DE PEREIRA
FACULTAD DE CIENCIAS BÁSICAS E INGENIERÍA
PROGRAMA DE INGENIERIA DE SISTEMAS Y TELECOMUNICACIONES
PEREIRA
2011

REVISIÓN DE LOS CONCEPTOS Y TECNOLOGÍAS UTILIZADAS EN LA IMPLEMENTACIÓN DE UN SISTEMA FEDERATIVO TIPO EDUROAM

ARNOL ALBERTO HERNANDEZ SERNA
CODIGO: 9861572
ANDRES JULIAN GRAJALES MARIN
CODIGO: 4516529

Asesor

Magister. Luis Alejandro Fletcsher Bocanegra

UNIVERSIDAD CATÓLICA DE PEREIRA
FACULTAD DE CIENCIAS BÁSICAS E INGENIERÍA
PROGRAMA DE INGENIERIA DE SISTEMAS Y TELECOMUNICACIONES
PEREIRA2011

TABLA DE CONTENIDO

LISTADO DE FIGURAS

DECLARACIÓN DE DERECHOS DE AUTOR

El presente trabajo de grado incluye ideas de sus autores y asesores, por lo tanto, se dará el crédito correspondiente cuando así se haga necesario, además de esto en este trabajo se expresan debidamente los conceptos o ideas que son tomadas de otras fuentes.

Se deja claro que este proyecto y su contenido podrá ser consultado como material de cursos o trabajos posteriores realizados en la Universidad Católica de Pereira, por lo tanto se deberá dar el crédito correspondiente y utilizar este material de acuerdo con las normas de derechos de autor.

SÍNTESIS

EDUROAM es un servicio que inició en España y se extendió a Europa, Asia-Pacifico, Estados Unidos y Canadá, para brindar conectividad y facilitar el trabajo en equipo, esto en procura de estimular la actividad de investigación y desarrollo.

Utiliza protocolos de seguridad y carga administrativa de competencia exclusiva en la red origen del usuario itinerante. Esto garantiza que la red a la cual se accede sea conocida y confiable, ya que la información del usuario en la autenticación, solo será de dominio del servidor de la institución a la cual el usuario pertenece.

RADAR por su naturaleza de red académica tiene la infraestructura necesaria para soportar ese servicio, de ahí que este trabajo pretenda conceptualizar su posible configuración.

DESCRIPTORES: EDUROAM, RADAR, Itinerancia, RADIUS, RedIris

EDUROAM is a service that began in Spain and spread to Europe, Asia-Pacific, U.S.and Canada, to provide connectivity and facilitate teamwork, this in an attempt to stimulate research and development activity.

Uses security protocols and administrative burden of exclusive jurisdiction in the home network of the roaming user. This ensures that the network which is known and reliable access as user information for authentication, single server domain is the institution towhich the user belongs.

RADAR nature of academic network has the infrastructure necessary to support thisservice, hence this paper intends Conceptualize its possible configuration.

DESCRIPTORS EDUROAM, RADAR, Roaming, RADIUS, RedIris

INTRODUCCIÓN

Desde todos los tiempos se ha evidenciado que la practicidad acompañada de seguridad se muestra como uno de los retos más inmediatos en la tecnología. Cada día los sistemas de información[*] y la manera de acceder a ellos forman parte de problemas laborales tanto como académicos.

Es ahora normal, decir que el concepto de movilidad en estos sistemas, cumple con el tiempo que demanda el día a día. Las mejores prácticas demuestran que tener la información de primera mano, de forma simple y sobe todo segura, hace más productivo cualquier sector llámese social, económico o académico.

La tecnología **EDUROAM** 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 (2006) .

Por esto, es que la implementación de una infraestructura móvil de conectividad, puede ser la solución a la problemática que genera la diversidad de conexiones dependientes de la posición geográfica que se tenga. El proyecto busca hacer una revisión de los sistemas ya implementados en Europa, Canadá y Asia, analizando minuciosamente sus inicios, tecnologías utilizadas, proyecciones y sobre todo, bondades que sostiene.

[*] Entiéndase "sistema de información", como el conjunto de elementos relacionados entre sí, que se encarga de procesar manual y/o automáticamente datos, en función de determinados objetos. Disponible en: www.alegsa.com.ar/Dic/sistema%20de%20informacion.php

1. OBJETIVO GENERAL

Revisar los conceptos necesarios en la implementación de tecnologías que brinden una solución a la itinerancia estudiantil en las instituciones de educación superior en Pereira.

1.1. OBJETIVOS ESPECÍFICOS

- Conocer cuáles son los componentes más relevantes en un sistema tipo EDUROAM
- Identificar proyectos similares que puedan aportar en el diseño de una solución para la región.
- Plantear una solución que ayude a definir modos de acceso y cobertura en la itinerancia educativa.
- Generar una propuesta como solución en la itinerancia educativa en Pereira.

2. ITINERANCIA ACADÉMICA COMO CONSTRUCCIÓN COLECTIVA DEL CONOCIMIENTO

La movilidad dentro de un mundo globalizado toma importancia en la medida en que las herramientas tecnológicas logran proporcionar un lazo permanente con los medios de comunicación sin desligar los afanes propios. Los sistemas educativos han sido cuna de soluciones que buscan desarrollar estos mecanismos.

Poder moverse dentro del sistema educativo sin perder conexión con lo que se encuentra a fuera de este y viceversa, ha dado pie a que la itinerancia sea tomada como un elemento presente en la cotidianidad del estudiante-usuario. Berlanga, Bosom, Hernández (2008)

Tener a mano herramientas que faciliten acceso a los recursos académicos sin importar la ubicación, posibilitan un trabajo en equipo, pues la distancia no es un factor decisivo en el cumplimiento de objetivos comunes. El trabajo en equipo puede permitir la construcción de conceptos con mejor argumentación dando la posibilidad de recibir aportes desde diversos enfoques.

Si la itinerancia corresponde a un proceso natural de un estudiante-usuario es posible llegar al concepto de convergencia académica pues el complemento disciplinar es motivada a raíz de este mismo campo, por lo que es válido plantear un sistema de itinerancia académica que integre sus fortalezas para crear una plataforma confiable de concurrencia, donde la movilidad no sea obstáculo.

2.1. PRESENTACIÓN DE LA INICIATIVA EDUROAM

2.1.1. Filosofía de funcionamiento:

> *"El objetivo es 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…"Servicio de informática y comunicaciones, universidad de Zaragoza (2011)*

EDU referente a educación y ROAM que viene de la palabra en inglés ROAMING que significa "*capacidad de un dispositivo de moverse de una zona de cobertura a otra, sin pérdida de la conectividad*" diccionario de informática (2009).

EDUROAM es más que una iniciativa, es una red con funcionamiento pleno y cobertura en países como Canadá y Estados unidos y continentes como Asia-Pacifico y Europa.

EDUROAM consiste en el desarrollo de un espacio de colaboración entre organizaciones dedicadas a procesos de investigación, de tal forma, que cuando sus usuarios (estudiantes, docentes, empleados) se trasladen a otras organizaciones puedan disponer de una manera inmediata de servicios de conectividad y recursos de su propia institución. La red inalámbrica EDUROAM en las universidades puede ser utilizada por usuarios de otras organizaciones participantes en el proyecto, para conectarse a Internet.

De otro lado EDUROAM hace parte de la iniciativa internacional que agrupa a varias redes de carácter académico europeas y TERENA (Organización que acoge un grupo importante de instituciones de investigación y desarrollo de diferentes disciplinas) que actúan como operadoras financiadas por GEANT3[*].

EDUROAM ofrece una base técnica suficiente y confiable para el uso de protocolos como:

- Protocolos básicos de Internet: HTTP, HTTPS, DNS, FTP, SSH, TELNET, NTP y RTMP
- Protocolos de correo electrónico: IMAP, IMAP3, IMAPS, POP3, POP3S, SMTPs, SMTP con STARTTTLS
- Protocolos de creación de túneles VPNs: IPSEC, OpenVPN, IPv6TunnelBroker, Cisco IPSec over TCP, PPTP
- Otros protocolos: MSN, JABBER, RDP, TCP_8080, TCP_8083, TCP_8081, TCP_7778

2.1.2 Redes académicas que pertenecen a esta iniciativa:

Las principales redes que integran la iniciativa EDUROAM son:

RedIris: **(**red para **I**nterconexión de los **R**ecursos **I**nformáticos**)** de las universidades y centros de investigación. Esta red se encarga de proveer servicios de conexión a Internet a diferentes instituciones en España, dentro de las que se encuentran departamentos del

[*] infraestructura de Internet avanzada que interconecta las diferentes redes académicas europeas

gobierno, el ministerio de turismo y comercio y el ministerio de ciencia e innovación de este mismo país.

RedIris se encarga de hacer la conexión de las instituciones pertenecientes a EDUROAM mediante su red troncal de telecomunicaciones llamada RedIris-10 y esta a su vez se conecta a la red PAM-Europea GEANT2 proporcionando la conexión con 33 países en este continente.

Por otra parte se encuentra **TERENA** que es un organismo que sirve como punto de convergencia para las comunidades dedicadas a la investigación y desarrollo de las tecnologías en Internet.

Tiene tres pilares fundamentales:

- Proporcionar un entorno para el fomento de nuevas iniciativas en la comunidad de redes de investigación en Europa.
- Apoyar el trabajo europeo de desarrollo, evaluación, pruebas, integración y promoción de nuevas redes, middleware y tecnologías de aplicación a través del Programa Técnico de TERENA.
- Organizar conferencias, talleres y seminarios para el intercambio de información en la comunidad de redes de investigación europeas, y buscar la transferencia de conocimientos a las organizaciones menos avanzadas de red.

Las redes académicas y de investigación y desarrollo más importantes asociadas a TERENA se relacionan en la siguiente tabla:

Austria (ACOnet) Belarús (BASNET) Bélgica (BELNET) Bulgaria (BREN) Croacia (carnet) Chipre (CYNET) República Checa (CESNET) Dinamarca (UNI-C) Estonia (EENET) Finlandia (Funet) Francia (RENATER) Alemania (DFN) Grecia (GRNET SA) Hungría (NIIF / HUNGARNET) Islandia (RHnet)	Irlanda (HEAnet) Israel (IUCC) Italia (GARR) Letonia (SigmaNet) Lituania (LitNet) Luxemburgo (Restena) República Yugoslava de (Marnet) Malta (UM / RicerkaNet) Montenegro (Mren) Países Bajos (SURFnet) Noruega (UNINETT) Polonia (PIONIER) Portugal (FCCN) Rumania (RoEduNet) Serbia (AMRES)	Eslovaquia (República Eslovaca) (SANET) Eslovenia (ARNES) España (RedIRIS) Suecia (SUNET) Suiza (SWITCH) Turquía (ULAKBIM) Reino Unido (JANET (Reino Unido))

Figura 1 Tabla: Redes académicas y desarrollo, vinculadas con TERENA

Fuente: Pagina oficial de TERENA disponible en http://www.terena.org/about/members_nat.php

3. UN EJEMPLO EN EL MUNDO

3.1. EDUROAM EUROPA

Es una organización mundial de servidores RADIUS* que facilita el acceso a la red utilizando 802.1x IEEE como vehículo conectando a una serie de afiliados académicos. El uso de EDUROAM 802.1x con RADIUS se basa en entender las normas establecidas en la infraestructura de red de las instituciones educativas.

Estas normas están compuestas por lo que se conoce como credenciales de usuario, que no es otra cosa diferente que una identificación ya instalada en el dispositivo que se usa para establecer la conexión. El certificado digital es expedido por el servidor local ubicado en la institución de origen. Toda vez que el usuario itinerante desea conectarse, el servidor crea un certificado digital y lo envía a una única cuenta de correo; el usuario deberá descargar e instalar dicho envío en el dispositivo con el que se va a conectar. EDUROAM EUROPA (2010)

Las credenciales no se revelan a la institución a la que el usuario se une, proporcionando una medida adicional de seguridad. La red EDUROAM también realiza una evaluación simple del sistema, ofreciendo calidad de servicio (aprovisionamiento de recursos). En lugar de proporcionar una red al visitante por separado, con la sobrecarga administrativa que esto supone si se mantuviera listas de usuarios, que además pueden tener fechas de vencimiento manual, una institución participante puede confiar en la institución de origen del visitante para autenticar las credenciales durante su estancia.

Otra de las ventajas de EDUROAM, que además estimula su uso, es que los fabricantes y desarrolladores de tecnología como Microsoft, Apple, Google y GNU/Linux incluyen el protocolo 802.1x suplicante†, por lo que unirse a EDUROAM es mucho más simple para los usuarios. El no tener este protocolo por defecto en el dispositivo de conexión no representa un problema, pues existen una serie de herramientas de control como Open1x y Securew2 que lo permiten. Alianza OPenSEA (2007).

---

* Remote Authentication Dial In User Service, servidor para autenticación

† El software del cliente en el equipo

3.1.1 Aspectos técnicos de EDUROAM Europa.

Fundamentalmente EDUROAM se basa en los protocolos estándar de autenticación inalámbrica como 802.11, 802.1x, y RADIUS.

Cuando un usuario se asocia con el SSID EDUROAM* (802.1x protegidas o cualquier SSID† o cable de conexión para el caso) el equipo cliente no es capaz de pasar todo el tráfico que no sea 802.1x hasta que concede el acceso por el punto o interruptor del cable de acceso. FILIP Y VASQUEZ (2010)

El software del cliente en el equipo se llama el *suplicante* (aunque es posible que se refieran a la computadora del cliente así mismo como el suplicante también); El hardware de red a la que el equipo esté asociado o conectado físicamente se llama el *autenticador*, y el autenticador dirige la comunicación con la infraestructura de autenticación, conocido como el " *servidor de autenticación* ". El servidor de autenticación puede ser en realidad múltiples servidores y / o componentes de autenticación tales como LDAP (Protocolo Ligero de Acceso a Directorios), (o Samba actuando como un controlador de dominio principal y la interacción con LDAP detrás de las escenas). El esquema de autenticación básica se describe a continuación (fig. 2). FILIP Y VÁSQUEZ (2010)

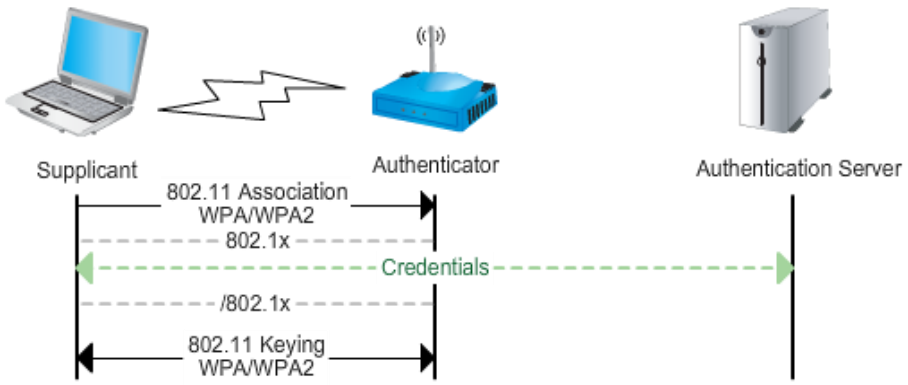


Figura 2 Gráfica: Basic Authentication with 802.1x over 802.11

Fuente: http://www.EDUROAMus.org/technical_overview

* Service Set IDentifier: se puede definir como un identificador de conjunto de servicios.

† †SSID (Service Set IDentifier) es un nombre incluido en todos los paquetes de una red inalámbrica (Wii-Flow) para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres que la mayoría de las veces son alfanuméricos (aunque el estándar no lo especifica, así que puede consistir en cualquier carácter). Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID

El proceso de autenticación 802.1x es más complejo que simplemente "el intercambio de credenciales". El intercambio real entre el suplicante y el autenticador implica un Protocolo de Autenticación Extensible (EAP) de conversación. La solicitud de EAP se envía al servidor de autenticación, generalmente en forma de una solicitud RADIUS. La seguridad real de la PEA proviene del uso de SSL (Secure Socket Layer)* con uno de los muchos sub protocolos EAP, los más comunes son:

- EAP-TLS - requiere el cliente y el servidor de certificados SSL / TLS.

- EAP-PEAP - requiere un certificado de servidor, también un ActiveDirectory o Samba servidor de autenticación de PDC. Este es el valor predeterminado para la parte solicitante de Windows, no requiere ningún software externo, es compatible de forma nativa en OSX de Apple y algunos suplicantes Linux.

- EAP-TTLS - este sub-protocolo también requiere sólo un certificado de servidor y es compatible de forma nativa en OSX de Apple, el iPhone OS, Linux y la mayoría de los suplicantes. Para utilizar EAP-TTLS en Windows requiere de un solicitante externo, como seguro-W2. FILIP Y VÁSQUEZ (2010)

3.2 MÉTODOS EAP Y COMPARACIÓN DE SUS FUNCIONES EN OTROS LUGARES DEL MUNDO.

La siguiente es una comparación de los métodos EAP más comunes desplegado en el sistema EDUROAM-Estados Unidos.

EAP-Type	Soporte nativo suplicante	Ventaja	Desventaja
EAP-TLS	Windows (XP, Vista, 7), Mac OS X, Linux, el IOS (iPhone, iPod Touch, IPAD), Android (v1.6 +)	Valida cliente, así como la infraestructura	Se requiere Infraestructura de PKI

Figura 3 Tabla: Comparación EAP común en EDUROAM EE.UU

Fuente: Referencia de Mitchell, Segurity for mobility (2004) elaboración propia

* El protocolo SSL es un sistema diseñado y propuesto por Netscape Communications Corporation. Se encuentra en el nivel de la capa OSI entre los niveles de TCP/IP y de los protocolos HTTP, FTP, SMTP, etc. Proporciona sus servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico.

- Los certificados pueden ser mitigados mediante herramientas de configuración, tales como el iPhone Configuration Utility para iOS dispositivos (iPhone, iPod Touch, IPAD), Active Directory para dispositivos de Windows (XP , Vista), etc.

- Ataques Man-in-the-Middle (es un ataque en el que se adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado.)

Durante la autenticación a través de cualquiera de los protocolos EAP que se describen anteriormente, un túnel SSL se crea entre el solicitante y el servidor de autenticación, dentro del cual los procesos se intercambian. Esto protege al usuario en el intercambio de credenciales por parte de terceros durante la autenticación. En el caso de RADIUS, el túnel SSL es construido por el uso de atributos RADIUS que consiste en llevar los datos cifrados como puede evidenciarse en la Figura (4). HASSELL (2002)

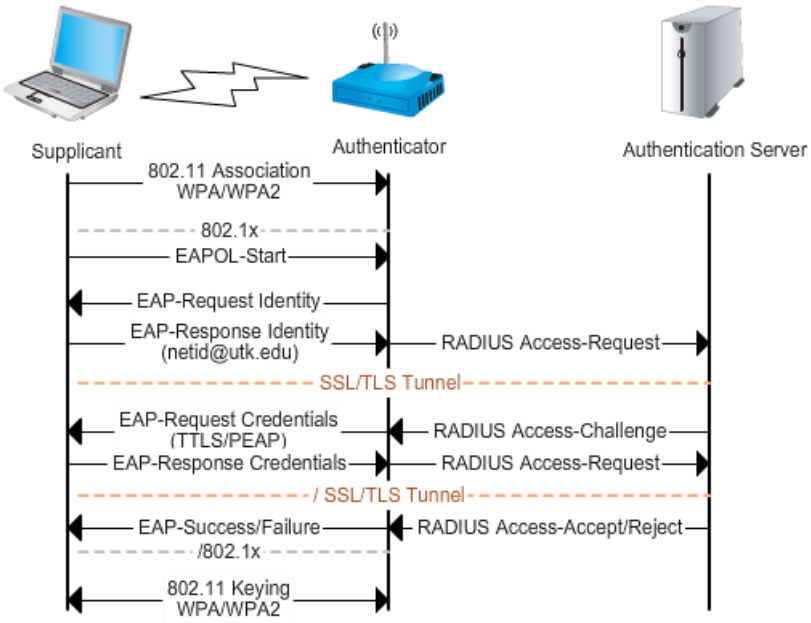


Figura 4 Gráfica: Autenticación 802.1x con más de 802.11 con detalles EAP

Fuente: http://www.EDUROAMus.org/technical_overview

Una opción adicional que los usuarios pueden configurar en su suplicante es utilizar el llamado "exterior de la identidad", que se usa fuera del túnel cifrado en los servidores de autentificación. Por defecto esta identidad no es más que el nombre de usuario, o en el caso de EDUROAM nombre de usuario@dominio (por ejemplo, julian@example.edu donde "Julián" es el nombre de usuario o "identificador de red" y "example.com" es el llamado dominio).PAGINA WEB MICROSOFT (2011).

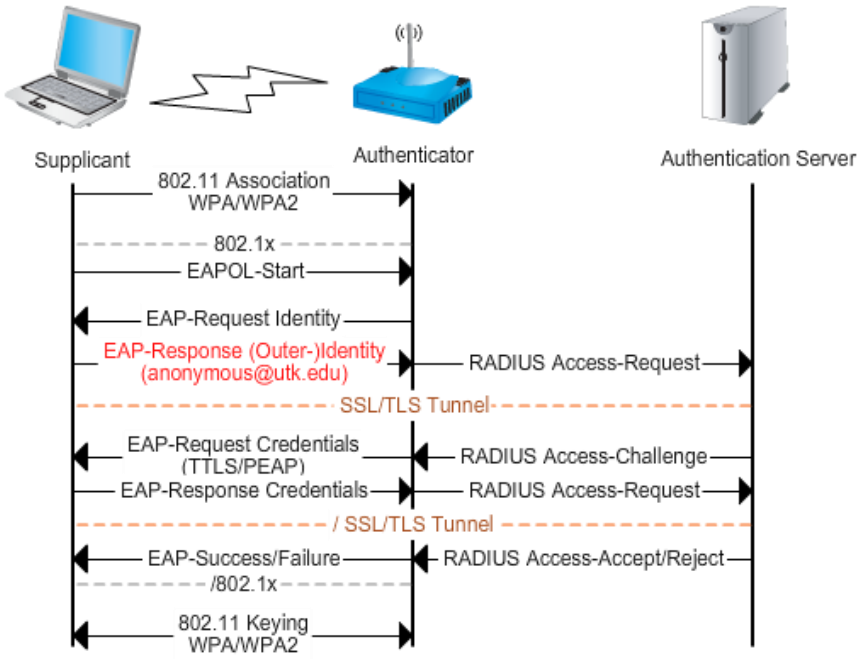


Figura 5 Gráfica: Autenticación 802.1x con más de 802.11 con un anónimo externo-la identidad

Fuente: http://www.EDUROAMus.org/technical_overview

El servidor de autenticación local no debe ser el destino final de una solicitud de autenticación cualquiera. Cuando el usuario no está en el ámbito local, la solicitud puede ser enviada a un servidor RADIUS remoto que tenga autoridad en ese dominio.

RADIUS puede admitir dicha solicitud. Cuando una petición es transmitida se crea un túnel SSL que protege la privacidad de quien solicita para que la información no se propague por la infraestructura de RADIUS eliminando la responsabilidad del administrador en la transmisión, por lo que la solicitud no es interceptada ni mucho menos, manipulado su contenido en el intercambio de EAP.

El servidor RADIUS intermedio solo tendrá la información exterior de la identidad del solicitante, el estado de la solicitud de EAP (solicitud de aceptar, el reto de acceso, aceptarlo o rechazarlo) y todos los atributos RADIUS que se pase fuera del túnel. HASSELL (2002)

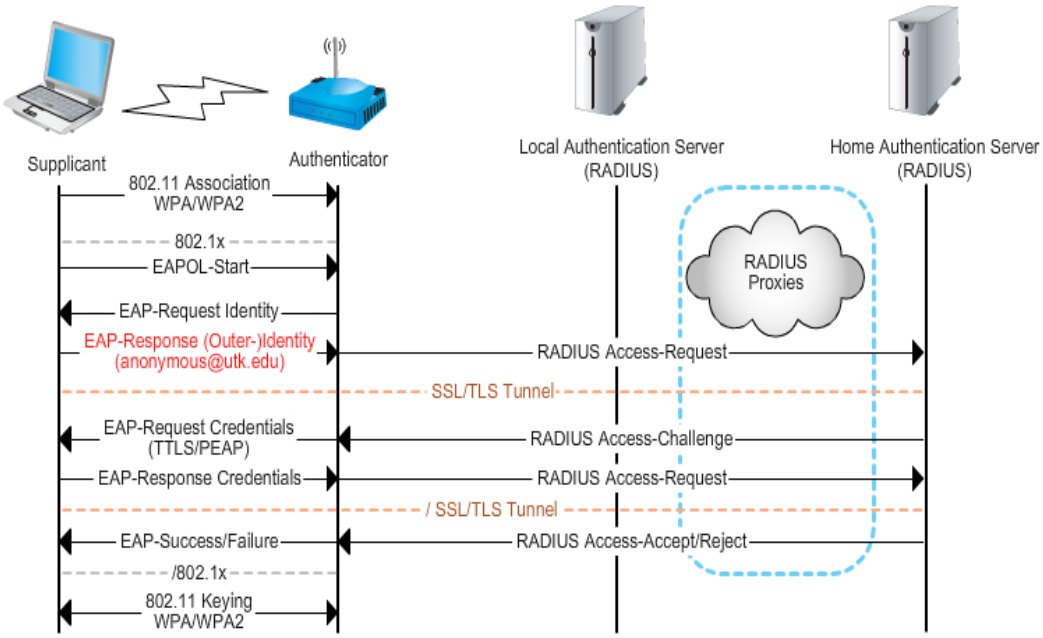


Figura 6 Gráfica: Authentication with 802.1x over 802.11 with RADIUS proxing

Fuente: http://www.EDUROAMus.org/technical_overview

EDUROAM-Estados Unidos está autorizado para la educación TLD, y se ocupa del enrutamiento a otros dominios de nivel superior incluyendo aquellos manejados por EDUROAM en Europa (para todos los miembros europeos de la federación), EDUROAM en la región de Asia-Pacífico (incluyendo Australia, China, Hong Kong, Japón, Nueva Zelanda, y Taiwán), y Canadá, Dentro de los EE.UU. EDUROAM-Estados Unidos el nivel superior del servidor RADIUS (TLRS) se encarga de enrutamiento.

3.3 SERVICIO DE MOVILIDAD

En este servicio se distingue la responsabilidad del usuario para respetar las políticas de uso, tanto de la institución visitada como de la de origen. Algunas de las políticas para este servicio son. EDUROAM (2006):

- El servicio de movilidad será prestado solamente al personal y a las organizaciones dedicadas a proyectos de investigación que pertenezcan al espacio de movilidad internacional.

- Los usuarios móviles deberán autenticarse en su organización de origen con el fin de tener acceso a la organización visitada.

- Los usuarios móviles son responsables de sus claves y deben respetar las políticas de uso de la organización de origen.

- Las organizaciones visitadas deberán ofrecer servicios de acceso, los usuarios podrán aceptarlas y hacer uso de ellas.

- La organización visitada debe garantizar la transferencia segura de las claves de los usuarios móviles.

- La organización visitada tiene la autoridad de impedir el acceso a cualquier usuario móvil, institución o red de investigación que no cumpla con las políticas de uso de la organización visitada.

- Las organizaciones visitadas establecerán el permiso para el acceso de servicios prestados a los usuarios móviles.

- La organización de origen será la encargada de brindar soporte a sus usuarios, incluyendo información en tecnologías de acceso y políticas de uso.

3.4 POLÍTICAS DE SEGURIDAD

Las políticas de seguridad definen la manera en que los usuarios deben comportarse dentro de un sistema informático. De esta forma, para la utilización de EDUROAM se han definido las siguientes políticas:

- Las organizaciones participantes deben responsabilizarse de enseñar a sus usuarios el respeto y cumplimiento de las políticas de uso de las organizaciones visitadas, y brindar asesoramiento en cualquier aspecto relacionado con sus usuarios.

- Las organizaciones participantes deben contar con un servidor de autenticación que de modo seguro, pueda procesar y transmitir las credenciales de usuario solicitadas,

utilizando para ello paquetes (Acceso-Aceptación de RADIUS), utilizados para cifrar y autenticar de forma remota.

- Las organizaciones participantes deberían difundir mecanismos para informar a los usuarios visitantes cómo son afectados 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 deberán disponer de elementos para informar a los usuarios visitantes de los niveles de seguridad ofrecidos en la transmisión de claves.

- Las organizaciones participantes deben informar a sus usuarios del servicio de movilidad, señalando que fallas de soporte técnico son responsabilidad en primera instancia de la organización origen. Sólo cuando la organización origen determina que el problema es responsabilidad de la organización visitada, éste debe ser revisado por la misma.

- Las organizaciones 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 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 procesos de monitorización y seguimiento que permitan conocer el estado de los servidores de autenticación, para poder analizar problemas de conexión.

- 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.

3.5 USUARIOS

En una red son los usuarios quienes deben tener mayor importancia, dado que son ellos quienes se benefician en EDUROAM, buscando crear un único espacio Wi-Fi donde se posibilite el acceso inalámbrico a Internet de forma sencilla cuando se requiera desplazamiento a una institución asociada al proyecto.

En el momento que un usuario se encuentre en una zona Wi-Fi de la Universidad o institución asociada y desea conectarse a la Red, podrá hacerlo básicamente de tres formas. PAGINA WEB UPV (UNIVERSIDA DEL PAIS VASCO 2011):

1. Como usuario Corporativo: Este servicio está dirigido principalmente al alumnado y personal PDI, PAS (Personal Docente e Investigador, Personal Administrativo y Servicios) de la Universidad. De esta forma se consigue acceder de manera personalizada (cuenta y contraseña) y segura a la red corporativa de datos de la Universidad y a Internet. Usuarios de otras instituciones adheridas al programa de movilidad EDUROAM podrán utilizar también este método de conexión.
   En el momento de establecer el SSID para esta forma de servicio debe elegirse EDUROAM.

   A la hora de configurar el *"suplicante",* los usuarios deberán proporcionar el nombre del SSID, la cuenta y el password, teniendo en cuenta que se utilizará el método EAP (método de autenticación) para autenticarse y WPA con TKIP para cifrar los datos.

2. Como usuario Asistente a Eventos Universitarios: Este servicio está pensado para dar conectividad a usuarios ajenos a la Universidad que se encuentran asistiendo a algún evento oficial de la misma, tal como cursos, congresos, conferencias o cualquier otro evento temporal con necesidad de una conexión WI-FI. En este caso no se utiliza autenticación y se cifra con una palabra clave que se proporciona en cada evento de forma puntual.

   El usuario debe configurar su Wi-Fi en la forma de autenticación abierta y cifrado WEP.

3. Como usuario foráneo. Debe disponer de un ticket para poder navegar en Internet. De no disponer de él, solamente podrá navegar por la WEB pública de la Universidad. En este servicio no se realiza ningún tipo de cifrado del tráfico. El usuario debe especificar comunicación *"Abierta" y "Sin Encriptación"* a la hora de configurar su "suplicante" o programa de conexión inalámbrica. Este servicio va dirigido a personas no vinculadas con la Universidad y que encontrándose en la misma deseen acceder a Internet.

3.6 CAMPO DE APLICACIÓN

La infraestructura EDUROAM se desprende de la carencia de movilidad en los grupos encargados de la investigación y la educación en la universidad politécnica de Madrid, siendo allí donde se conceptualiza y empieza a expandirse a las demás ciudades de España, su funcionalidad ha permitido que esta infraestructura tecnológica haya podido implementarse en Europa, Asia, África y parte de Norte América.

Sirve como punto de convergencia para varias de las más renombradas entidades encargadas de la investigación y desarrollo de varios países.

A pesar de haber surgido como una herramienta con fines académicos, cabe resaltar que gracias a los niveles de seguridad y funcionalidad que EDUROAM ofrece, su estructura puede catalogarse apta para otras aplicaciones como: Comercio electrónico, aplicaciones en bolsa de valores o prestación de cualquier otro tipo de servicios electrónicos, logrando que su campo de aplicación pueda ser reconocido en instancias diferentes a la labor académica.

4. TECNOLOGÍAS

4.1 PROTOCOLO

El estándar 802.1x es una solución de seguridad ratificada por el IEEE en junio de 2001 que puede identificar a un usuario que quiere acceder a la red (cable o inalámbrica). Esto se hace a través del uso de un servidor de autenticación.kioskea.net (2008)

El 802.1x se basa en el protocolo EAP (*Protocolo de autenticación extensible*), definido por el IETF. Este protocolo se usa para transportar la información de identificación del usuario. Liu (2009)

La forma en que opera el protocolo EAP se basa en el uso de un controlador de acceso llamado autenticador, que le otorga o no al usuario el acceso a la red. El usuario en este sistema se llama solicitante. El controlador de acceso es un firewall básico que actúa como intermediario entre el usuario y el servidor de autenticación, y que necesita muy pocos recursos para funcionar. Cuando se trata de una red inalámbrica, el punto de acceso actúa como autenticador. Pellejero (2006)

El servidor de autenticación (*NAS*)* puede aprobar la identidad del usuario transmitida por el controlador de la red y otorgarle acceso según sus credenciales. Además, este tipo de servidor puede almacenar y hacer un seguimiento de la información relacionada con los usuarios. En el caso de un proveedor de servicio, por ejemplo, estas características le permiten al servidor facturarles con base en cuánto tiempo estuvieron conectados o cuántos datos transfirieron.

Generalmente el servidor de autenticación es un servidor RADIUS (*Servicio de usuario de acceso telefónico de autenticación remota*), un servidor de autenticación estándar definido por la RFC 2865 y 2866, pero puede utilizar cualquier otro servicio de autenticación en su lugar. A continuación se presenta la figura (6) donde puede identificarse el proceso de autenticación entre dominios con el estándar 802.1X: MATHON (2004)

* *Servicio de autenticación de red* o *Servicio de acceso a la red*

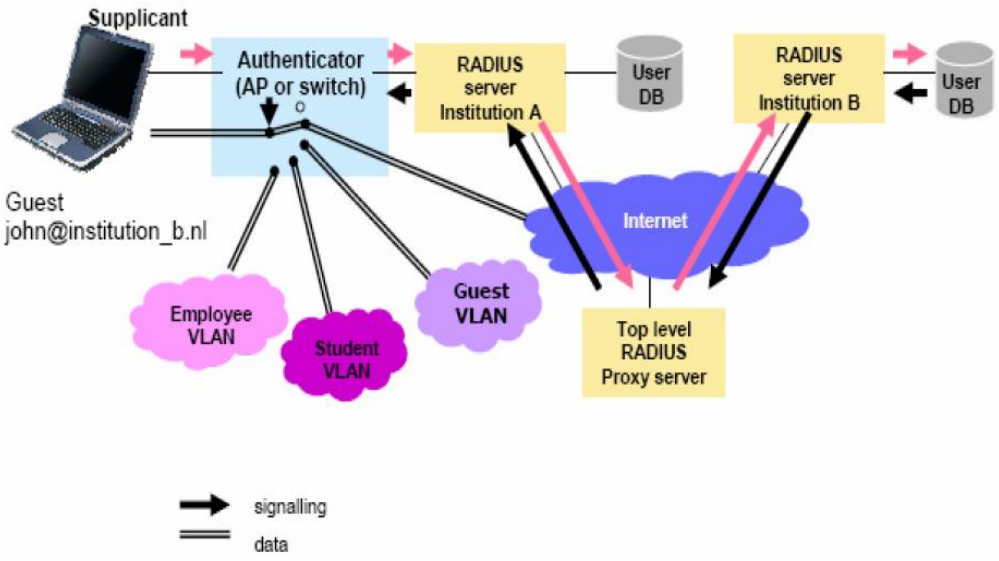


Figura 7 Gráfica: Infraestructura de autenticación entre dominios mediante el estándar 802.1x

Fuente: página principal de TERENA (http://www.terena.org/activities/tf-mobility/deliverables/delD/DelD_v1.2-f.pdf)

4.2 ARQUITECTURA

El marco 802.1X añade funcionalidad a los componentes existentes en una red. Por lo tanto, existen componentes adicionales que se hacen necesarios.

En una red fija, el terminal (PC o portátil, por ejemplo) tiene que tener una tarjeta de red (NIC), y el sistema operativo debe tener una funcionalidad llamada suplicante 802.1X a bordo.

El puerto al que se conectará la terminal se encuentra en un interruptor que está activado 802.1X. El interruptor es llamado autenticador en el marco. Sobre la base de comandos 802.1X, el interruptor puede abrir y cerrar una conexión en el puerto. El tercer componente de la arquitectura es el de autenticación del servidor. En general, un interruptor interroga a un servidor RADIUS para verificar si al usuario se le es permitido el uso de una VLAN y qué tráfico debe ir.
Cuando 802.1X se aplica a una red inalámbrica, un dispositivo de control de acceso inalámbrico sustituye el switch como el autenticador. No es relevante que el protocolo de

transporte inalámbrico (802.11b ó protocolo próximo 802.11g) se utilice en la infraestructura.

Cuando un usuario se conecta a la red que utiliza credenciales para su autenticación (el acceso al control de dispositivos) se verifica usando el backend RADIUS. Las credenciales deben siempre incluir un nombre de usuario y un dominio que se traduce en una credencial que se parece a un E-Mail (User@realm.topleveldomain).

Si un usuario utiliza la red, el servidor RADIUS local se dará cuenta que el dominio del usuario no es el dominio que le sirve. Ahí es donde el mecanismo de RADIUS proxy entra y se asegura de que la EAP ha encapsulando las credenciales, se transporta hacia la casa del servidor RADIUS. De hecho, RADIUS sólo tiene que remitir la petición a un RADIUS de más alto nivel o servidor proxy. Hassell (2002)

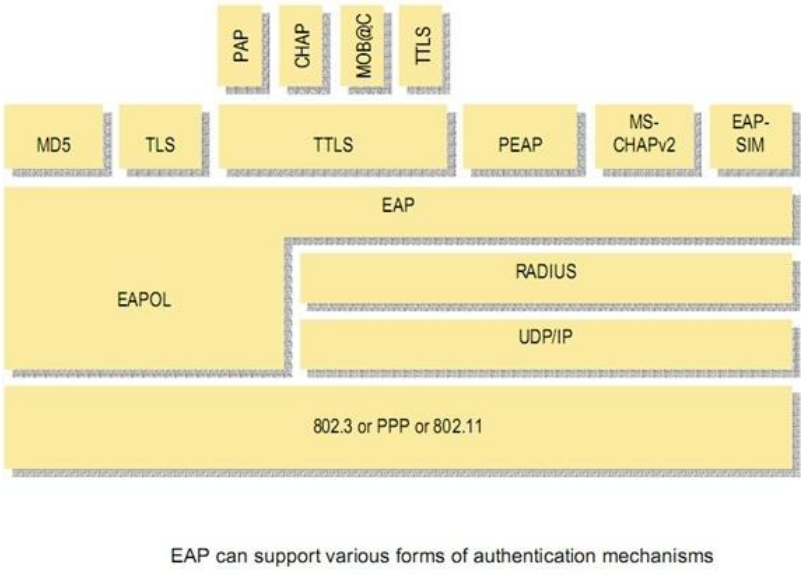
El servidor proxy conoce los demás servidores RADIUS en la constelación de roaming y reenvía la solicitud al servidor que se sabe puede controlar el reino. El servidor RADIUS "casa" se instala en la red de origen del visitante, ya sea en el mismo país o en el extranjero, donde el usuario se autentica contra una base de datos de usuarios locales. El servidor RADIUS local sólo tiene que saber que peticiones de usuario deben ser enviadas.

En la figura posterior muestra la fila de protocolos del marco 802.1X. La información de autenticación se realiza sobre el protocolo de autenticación extensible (EAP, RFC 2284), un protocolo que permite el uso de cualquier método de autenticación, como nombre de usuario / contraseña, certificados, OTP (One Time Password, música a través de SMS) o credenciales en Simcard uno de los operadores móviles. Estos mecanismos se aplican en los tipos de EAP MD5, TLS, TTLS, MS-CHAPv2, PEAP, Móvil @ c, y EAP-SIM. ESPAÑA (2003)

Tanto el solicitante y el servidor principal RADIUS debe utilizar el mismo tipo de EAP. El acceso al control del dispositivo, conmutador o proxy servidores RADIUS no tienen que ser conscientes del tipo de EAP.

En la actualidad, TLS (Transport Layer Security), TTLS (Túnel Transport Layer Security) y PEAP (EAP protegido) son los candidatos más serios para su aplicación inmediata. Pruebas adicionales se realizaron con la autenticación basada en contraseñas una vez enviado por SMS. STALLINGS (2004)

TLS, TTLS y PEAP configuran una conexión TLS entre el cliente y el dispositivo de control de acceso basado en un certificado de servidor RADIUS. Este mecanismo de autenticación mutua puede impedir que el hombre intente ataques contra el Medio. TLS a continuación, utiliza un certificado de cliente para autenticar al usuario, mientras que TTLS es generalmente utilizado para el transporte nombre de usuario / contraseña. Dado que tanto TTLS y PEAP son protocolos de túnel, cualquier otro protocolo se puede utilizar en la parte superior de ellos. Mobac es un ejemplo.



EAP can support various forms of authentication mechanisms

Figura 8 Gráfica: Mecanismos de autenticación con EAP

Fuente: http://www.EDUROAM.es(tecnología sobre 802.1x).

Si el usuario está verificado apropiadamente con el backend de autenticación de origen (que puede ser LDAP, por ejemplo) serán autenticados y el servidor principal RADIUS pasa un acuse de recibo el dispositivo de control de acceso. Cuando un usuario se encuentra en su red de origen, el servidor RADIUS puede decir al Autenticador en el que el tráfico de VLAN de los usuarios debe residir.

El dispositivo de control de acceso pasa el tráfico de usuarios en esta VLAN hasta que sea autenticado. La VLAN de conmutación se basa en la Estándar 802.1Q. Consiste en que un visitante se pondrá en una VLAN huésped, determinada por la red visitante del Servidor RADIUS.

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

Cuando el usuario retira el cable o sale del área de cobertura de un dispositivo de control de acceso inalámbrico, el dispositivo de control de acceso detecta la interrupción de la conexión y el puerto se cierra. Los Suplicantes también tienen un built-in con la posibilidad de desconectarse gracias a la red, permitiéndoles volver a conectarse con credenciales diferentes para acceder a otras VLAN. EDUROAM (2006)

4.3 ESCALABILIDAD

Como se mencionó antes, el servidor RADIUS local sólo tiene que saber a qué usuario proxy desconocido se deben enviar las solicitudes. Cuando una nueva red entra en este acuerdo de itinerancia, sólo el primero tiene que ser actualizado.

Para ampliar esta infraestructura de itinerancia a escala europea, en una organización de nivel internacional, un proxy RADIUS es el único componente que hay que añadir, como se muestra en la figura.

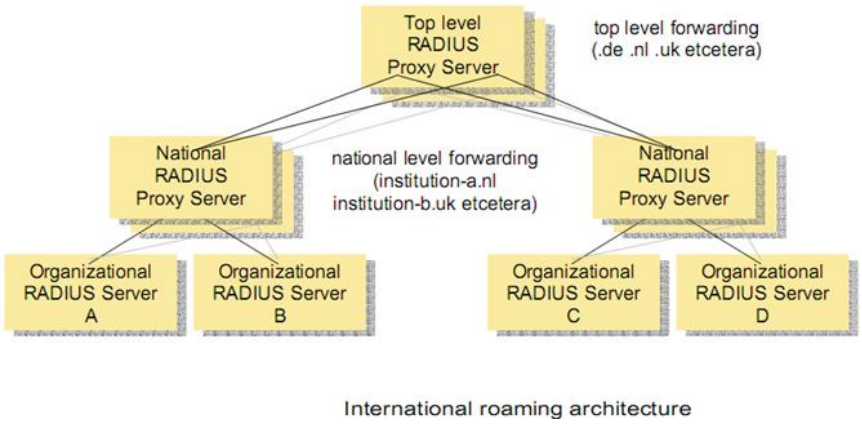


Figura 9 Gráfica: International roaming architecture

Fuente: http://www.EDUROAM.es(tecnología sobre 802.1x).

Cuando una nueva institución ingresa a la organización, su dominio sólo tiene que introducirlo en la Fase Nacional RADIUS Proxy Server, no en los servidores de otras instituciones. Lo mismo ocurre con la adición de un grupo de instituciones en un país que entra en la constelación: el nivel superior RADIUS Proxy Servidor debe estar actualizado con el nuevo dominio de alto nivel (por ejemplo ". Nl"), tras lo cual el mecanismo de reenvío de las obras de cada institución en la constelación. Siempre es posible que cuente las relaciones bilaterales entre los servidores de intercambio de tráfico, o el tráfico pertinente a nivel local.

El uso de RADIUS también hace que sea fácil de conectar la infraestructura móvil existente a un móvil de operadores de red (WiFi, GPRS o UMTS).

La infraestructura de RADIUS como se presenta aquí puede introducir bucles en el flujo de mensajes, que puede conducir a la falta de servidores RADIUS. Para evitar esto, cada servidor RADIUS puede ser obligado a no reenviar mensajes destinados a la esfera que se maneja. Además, el proxy puede filtrar estos eventos y observar la cantidad de saltos en los mensajes.

Sobreponerse es posible en todos los niveles en la arquitectura. Los dispositivos de control de acceso se pueden instalar en pares, aunque esto no suele hacerse debido a los altos costos. Además, cada dispositivo de control de acceso se puede configurar para interrogar a dos (o más) servidores RADIUS. Cuando un servidor RADIUS falla, el otro puede hacerse cargo. El mismo mecanismo se puede utilizar entre Servidores RADIUS en la infraestructura proxy.

Puesto que el software promedio del servidor RADIUS no consume muchos recursos de hardware, un PC contemporáneo ya podría servir decenas de solicitudes de autenticación, o incluso cientos de solicitudes de expedición por segundo.

La autenticación es sólo necesario en el comienzo de la sesión y cuando un usuario se mueve entre los dispositivos de control de acceso, por lo tanto un servidor RADIUS servidor proxy a nivel nacional puede servir potencialmente miles de sesiones de usuarios al mismo tiempo. Escalabilidad en términos de rendimiento de procesamiento es implícitamente logrado por el hecho de que cada dispositivo de control de acceso se encarga del cifrado de datos en el nivel dos de la capa a velocidad de cable. EDUROAM (2006)

4.4 SEGURIDAD

Mientras un fuerte protocolo EAP TLS se utiliza, 802.1X proporciona un marco que da un nivel de seguridad suficiente para los fines previstos, es decir, el control de acceso a la red. En los protocolos de túnel como PEAP y TTLS se puede configurar para evitar los tipos de ataques actualmente conocidos por el hombre.

Para la integridad de los datos o la privacidad, una serie de extensiones de seguridad inalámbrica (WPA, TKIP, 802.11i etc.) han sido propuestas y se basará también en el marco 802.1X. Sin embargo, al momento de ingresar las claves, WEP proporciona un nivel muy alto de encriptación cuando las teclas se actualizan periódicamente (normalmente cada 20 minutos o menos cuando se utiliza claves de 64 bits). Se recomienda el uso de claves de 64 bits, debido a la compatibilidad con adaptadores de red.

La seguridad en la infraestructura de RADIUS es proporcionada por el uso de claves compartidas entre servidores RADIUS y mediante la instalación de estos servidores se hace segura la red.

Todos los RADIUS de interconexión deben tener su propia llave compartida. Sin embargo, algunos mensajes pueden ser alterados en el camino, por lo que además los caminos entre los servidores RADIUS se pueden proteger mediante la creación de Túneles IPSec. Esto se ha hecho con éxito, tanto por lo menos en los Países Bajos y Finlandia.

Aquí está un breve resumen de los temas de seguridad y el abuso con los mecanismos correspondientes previstos por 802.1X para hacerles frente:

4.4.1 La identidad pública de adquisición.

Es difícil detectar el abuso en cualquier proceso de autenticación cuando el abusador tiene el conjunto de credenciales de otra persona. RADIUS permite el registro detallado de las sesiones de usuario, por lo que las denuncias de una víctima en cuyo nombre se llevó a cabo el abuso pueden estar relacionadas con las sesiones reales de que el abusador haya iniciado.

4.4.2 La pérdida de las credenciales.

Tan pronto como un usuario reporta la pérdida de credenciales a la mesa de ayuda, la mesa de ayuda puede desactivar la cuenta (ya sea en la base de datos de usuario o la organización servidor RADIUS). No es posible seguir abusando después de ese instante.

4.4.3 Abuso de ancho de banda.

Detección y prevención del uso indebido de ancho de banda en la capa 2 es un problema en cualquier red. Las acciones que se pueden tomar para dar forma al tráfico basado en VLAN o limitar los parámetros subida/bajada de la capacidad en VPN concentradores o Web pasarelas, pero esto no impide que los usuarios inunden el medio con un gran número de paquetes en caso de una red inalámbrica.

Al utilizar 802.1X, el usuario puede ser dado marcha atrás en cualquier caso. En la capa 1, el administrador de la red no puede hacer nada. La interferencia de 2,4 GHz con un horno de microondas, simplemente apaga todos los datos.

4.4.4 Contenidos de pornografía.

Cualquier abuso puede ser dado marcha atrás a una cuenta de usuario en el momento en que los huéspedes de registro relacionen la asignación de dirección IP en la red visitante. Para ello es necesario el registro de la relación entre el ID de usuario y la dirección IP asignada para una sesión determinada.

Las cuentas sospechosas o incluso dominios completos, puede ser bloqueado en cualquier nivel de la arquitectura, evitando así que el usuario sospechoso de la institución pueda iniciar sesión en la red.

4.4.5 Clientes.

Para la autenticación de contraseña de usuario, EAP-TTLS se prueba ampliamente. Es fácil de instalar ya que no requiere de una PKI con certificados de usuario final. Sólo el servidor

RADIUS tiene que tener un certificado. Cuando una PKI está en su lugar, EAP-TLS se puede utilizar como una forma de autenticación fuerte.

Para que el cliente (suplicante 802.1X en la terminología) utilice la autenticación basada en 802.1X, ya sea el sistema operativo de cliente, debe apoyar EAP y el método de autenticación requerido de forma nativa o pieza de software deberá ser instalado.

Actualmente, el MS Windows XP y Windows 2000 del sistema operativo de apoyo EAP y TLS. Por versiones de Windows anteriores EAP se apoya en SURFnet distribuye un módulo para TTLS en estas plataformas.

Además de este módulo, los clientes comerciales existentes incluyen EAP con TTLS y TLS. Ambos Funk y los clientes de Meetinghouse han sido probados. Para los sistemas de Apple clientes comerciales existentes y para diversos sabores de Unix, tanto una aplicación de dominio público (open1X), así como un comercial producto está disponible. El número de implementaciones crece rápidamente.

4.4.6 Acceder a los dispositivos de control.

La mayoría de los dispositivos modernos de control de acceso son compatibles con la autenticación 802.1X.

En los productos piloto de Cisco (350 y 1200) y el Orinoco (AP2000) se han probado con éxito. Estos fabricantes actualmente manejan la asignación de SSID a VLAN. Cisco es compatible actualmente con la mayoría de las VLAN en un dispositivo de control de acceso, mientras que el producto de Cisco sólo emite un SSID. El producto del Orinoco puede emitir dos SSID, cada uno asignado a un VLAN correspondiente.

4.4.7 Interoperabilidad

El mecanismo 802.1X proporciona acceso a la red en la capa 2 del modelo OSI. Abrir Ethernet y conectividad IP sólo vendrá después de una autenticación exitosa. Esto asegura la compatibilidad con todas las aplicaciones habilitadas para IP. Es posible establecer una conexión VPN hacia un concentrador que da acceso a los recursos protegidos, o de inicio de sesión a una puerta de entrada basada en web. Nota imposible que un usuario puede conectarse a una red 802.1X extranjera si no tiene el software suplicante y cuenta con

credenciales válidas. Para hacer la red más amigable para los visitantes 802.1X permitió una VLAN por defecto para estos visitantes con conectividad limitada.

El marco 802.1X se ha normalizado totalmente, así como EAP sobre LAN (EAPOL). Lo mismo vale para EAP-MD5 y EAP-TLS. Otros subcomponentes son en algunos casos, aún en el desarrollo. TTLS y PEAP están en proyecto en el proceso de normalización del IETF, así como EAP-SIM. TTLS está disponible en muchas implementaciones de software, PEAP en dos (y en expansión).

El uso de claves WEP en 802.1X es también estándar. En primer lugar WPA y TKIP hará un seguimiento de WEP. WPA estandarizados, pero no está ampliamente disponible todavía. Finalmente, 802.1X incluyendo TKIP y AES formará 802.11i, un estándar específico para la seguridad de WLAN.

4.5 TECNOLOGÍA RADIUS

Fundamenta su servicio en el concepto (AAA) Autenticación, Autorización y registro (Auditoria) de donde se desprende la necesidad de utilizar credenciales de usuario, validación de servicios autorizados y registro en el consumo de ellos, así se genera la necesidad de tener disponible un servidor donde la concurrencia de solicitudes de servicio sea suplida de manera idónea y veraz por cada uno de los servidores encargados de la validación de las credenciales. Hassell (2002)

Después de tener la concentración de usuarios en cada uno de los servidores pertenecientes a cada institución, se hace la autenticación en un servidor RADIUS de nivel superior el cual en algunas ocasiones es utilizado como servidor proxy y se encarga de la comunicación entre servidores RADIUS institucionales.

A continuación presenta un resumen sobre cómo funciona una red segura que usa el estándar 802.1x. PAGINA WEB KIOSKEA.NET (2011):

1. El controlador de acceso, después de recibir la solicitud de conexión del usuario, envía una solicitud de autenticación.
2. El usuario envía una respuesta al controlador de acceso, quien enruta la respuesta al servidor de autenticación.

3. El servidor de autenticación envía un "challenge" al controlador de acceso, quien lo transmite al usuario. El challenge es un método para establecer la identificación. Si

el cliente no puede evaluar el challenge, el servidor prueba con otro y así sucesivamente.

4. El usuario responde al challenge. Si la identidad del usuario es correcta, el servidor de autenticación envía la aprobación al controlador de acceso, quien le permite al usuario ingresar a la red o a parte de ella, según los derechos otorgados. Si no se pudo verificar la identidad del usuario, el servidor de autenticación envía un mensaje de denegación y el controlador de acceso le deniega al usuario el acceso a la red.

Para su ilustración a continuación se presenta como alternativa la figura (10) donde se explica el funcionamiento:

4.5.1 Funcionamiento.

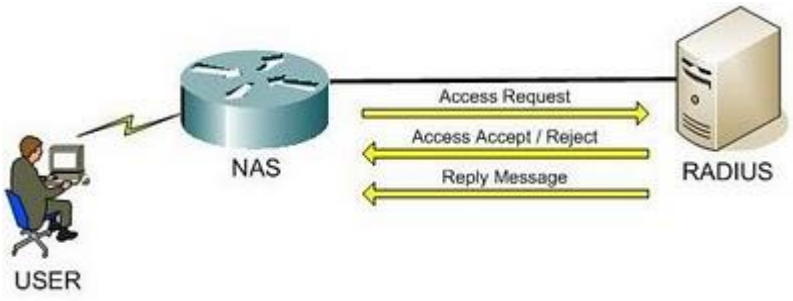


Figura 10 Gráfica: Arquitectura general de RADIUS

Fuente**:**
http://books.google.com.co/books?id=k3JuVG2D9lMC&printsec=frontcover&dq=pellejero&hl=es&ei=C0HhTbvJJI7egQfgk7HABg&sa=X&oi=book_result&ct=book-thumbnail&resnum=1&ved=0CCcQ6wEwAA#v=onepage&q&f=false

- El usuario inicia sesión en el NAS.
- El NAS le pide usuario y password.
- El usuario responde con sus credenciales.
- El NAS envía usuarios y password encriptadas al servidor RADIUS.
- RADIUS responde aceptando, rechazando o interactuando con el usuario.

4.6 PROTOCOLO (AAA)

En seguridad informática, el acrónimo AAA corresponde a un tipo de protocolos que realizan tres funciones: Autenticación, Autorización y Auditoría (Authentication, Authorization and Accounting en inglés). La expresión *protocolo AAA* no se refiere pues a un protocolo en particular, sino a una familia de protocolos que ofrecen los tres servicios citados. (AAA) se combina a veces con auditoria, convirtiéndose entonces en (AAAA). CISCO (2011)

4.6.1 Autenticación

La Autenticación es el proceso por el que una entidad prueba su identidad ante otra. Normalmente la primera entidad es un cliente (usuario, ordenador, etc.) y la segunda un servidor (ordenador). La Autenticación se consigue mediante la presentación de una propuesta de identidad (nombre de usuario) y la demostración de estar en posesión de las credenciales que permiten comprobarla. Hassell (2002)

Ejemplos posibles de estas credenciales son las contraseñas, los testigos de un sólo uso (one-time tokens), los Certificados Digitales, ó los números de teléfono en la identificación de llamadas. Viene al caso mencionar que los protocolos de autenticación digital modernos permiten demostrar la posesión de las credenciales requeridas sin necesidad de transmitirlas por la red.

4.6.2 Autorización

Se refiere a la concesión de privilegios específicos (incluyendo "ninguno") a una entidad o usuario basándose en su identidad (autenticada), los privilegios que solicita, y el estado actual del sistema. Las autorizaciones pueden también estar basadas en restricciones, tales como restricciones horarias, sobre la localización de la entidad solicitante, la prohibición de realizar logins múltiples simultáneos del mismo usuario, etc.

La mayor parte de las veces el privilegio concedido consiste en el uso de un determinado tipo de servicio. Ejemplos de tipos de servicio son, pero sin estar limitado a: filtrado de direcciones IP, asignación de direcciones, asignación de rutas, asignación de parámetros de Calidad de Servicio, asignación de Ancho de banda, y Cifrado.

4.6.3 Auditoría

La Contabilización se refiere al seguimiento del consumo de los recursos de red por los usuarios. Esta información puede usarse posteriormente para la administración, planificación, facturación u otros propósitos.

La contabilización en tiempo real es aquella en la que los datos generados se entregan al mismo tiempo que se produce el consumo de los recursos. En contraposición la contabilización por lotes (en inglés "batch accounting") consiste en la grabación de los datos de consumo para su entrega en algún momento posterior.

La información típica que un proceso de contabilización registra es la identidad del usuario, el tipo de servicio que se le proporciona, cuando comenzó a usarlo, y cuando terminó.

4.7 DIAMETER

Es un protocolo de red para la autenticación de los usuarios que se conectan remotamente a Internet a través de la conexión por línea conmutada o TLC, también provee de servicios de autorización y auditoría para aplicaciones tales como acceso de red o movilidad IP.

El concepto básico del protocolo DIAMETER, cuyo desarrollo se ha basado en el protocolo RADIUS, es de proporcionar un protocolo base que pueda ser extendido para proporcionar servicios de autenticación, autorización y auditoría, (denominados por los expertos por sus siglas AAA) a nuevas tecnologías de acceso. DIAMETER está diseñado para trabajar tanto de una manera local como en un estado de alerta, sondeo y captura, que en inglés se le denomina *roaming* de AAA, que le permite ofrecer servicios sumamente móviles, dinámicos, flexibles y versátiles.

4.8 SISTEMA DE SEGURIDAD WPA

Denomina por la sigla (Wi-Fi Protected Access o Acceso Protegido Wi-Fi) es un sistema diseñado para proteger las redes inalámbricas (Wi-Fi); también creado para corregir las

deficiencias del sistema previo WEP (Wired Equivalent Privacy o Privacidad Equivalente a Cableado).

Los investigadores han encontrado varias debilidades en el algoritmo WEP tales como la reutilización del vector de inicialización (IV)[*], del cual se derivan ataques estadísticos que permiten recuperar la clave WEP, entre otros. WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado. WPA fue creado por "The Wi-Fi Alliance".

WPA adopta la autenticación de usuarios mediante el uso de un servidor, donde se almacenan las credenciales y contraseñas de los usuarios de la red, en el caso de no verse obligado a utilizar un servidor para el despliegue de redes, WPA permite la autenticación mediante clave compartida ([PSK], Pre-Shared Key), donde se requiere introducir la misma clave en todos los equipos de la red.

[*] Vector de iniciación (VI): Bloque de bits que es requerido para permitir un cifrado en flujo.

5. FUNCIONAMIENTO EDUROAM

5.1 MÉTODOS DE AUTENTICACIÓN

5.1.1 Transport Layer Security (TLS)

Secure Sockets Layer (SSL), son protocolos criptográficos que proporcionan comunicación de seguridad en Internet. TLS y SSL cifran los segmentos de conexiones de red por encima de la capa de transporte, utilizando criptografía simétrica y una clave de mensaje código de autenticación para la fiabilidad del mensaje. MICROSOFT (2011)

- **Descripción**

El protocolo TLS permite al servidor de aplicaciones del cliente poder comunicarse a través de una red de una forma segura para prevenir escuchas ilegales y la manipulación de la misma.

Un cliente TLS y el servidor negocian una conexión de estado mediante un procedimiento llamado handshake. Durante este handshake, el cliente y el servidor se ponen de acuerdo sobre los distintos parámetros utilizados para establecer una conexión segura como se muestra en la figura (11).

- El handshake se inicia cuando un cliente se conecta a un servidor habilitado para TLS solicita una conexión segura y presenta una lista de los conjuntos de cifrado y funciones de hash que es tomar un bloque de datos arbitrarios y devolver un tamaño fijo.

- De esta lista, el servidor elige el cifrado más fuerte y la función hash que apoya y notifica al cliente de la decisión.

- El servidor devuelve su identificación en forma de un certificado digital. El certificado contiene usualmente el nombre del servidor, la entidad emisora de certificados (CA) y el servidor de clave de cifrado público.

- El cliente puede comunicarse con el servidor que emitió el certificado (CA) y confirmar que el certificado es válido antes de continuar.

- Con el fin de generar las claves de sesión utilizadas para la conexión segura, el cliente encripta un número aleatorio con la clave pública del servidor y envía el resultado al servidor. Sólo el servidor debe ser capaz de descifrar.

- A partir del número al azar, las dos partes generan material clave para el cifrado y descifrado.

Con esto concluye el handshake y comienza la conexión segura, que se cifra y descifra con el material de clave hasta que la conexión se cierra. Si alguno de los pasos anteriores no se da, el protocolo de enlace TLS falla y la conexión no se crea.

Figura 11 Gráfica: intercambio de datos utilizando TLS/SSL

Fuente:
http://www.google.com.co/search?hl=es&tbo=1&tbm=bks&q=tls%2Fssl&oq=tls%2Fssl&aq=f&aqi=&aql=&gs_sm=e&gs_upl=953057l961434l0l15l15l0l4l0l1l259l1617l0.7.2

En el diseño de aplicaciones, TLS se implementa normalmente en la parte superior de cualquiera de la capa de protocolos de transporte, encapsulando los protocolos específicos de aplicación como HTTP, FTP, SMTP, NNTP y XMPP. Históricamente se ha utilizado principalmente con protocolos de transporte confiables, tales como el Protocolo de Control

de Transmisión (TCP). Sin embargo, también se ha implementado con el transporte de protocolos orientados a datagramas, como el Protocolo de datagramas de usuario (UDP) y el de datagramas de Protocolo de control de congestión (DCCP), el uso se ha normalizado de forma independiente utilizando el término de datagramas de Transport Layer Security (DTLS).

Un uso prominente de TLS es para asegurar la World Wide Web realizado por el tráfico HTTP para formar HTTPS. Aplicaciones más importantes son el comercio electrónico y gestión de activos. Cada vez más, el Simple Mail Transfer Protocol (SMTP) también está protegido por TLS. Estas aplicaciones utilizan certificados de clave pública para verificar la identidad de los extremos.

TLS también se puede utilizar para hacer un túnel de una red de toda la pila que es una estructura de datos usando la forma LIFO (último en entrar, primero en salir para crear una VPN) , como es el caso de OpenVPN.

Muchos proveedores ahora utilizan el cifrado TLS y las capacidades de autenticación con autorización. También ha habido un desarrollo importante desde finales de 1990 en la creación de la tecnología de cliente fuera del navegador para habilitar el soporte para aplicaciones cliente / servidor. Cuando se compara contra el tradicional IPsec VPN tecnologías, TLS tiene algunas ventajas inherentes en el firewall y NAT transversal que hacen que sea más fácil de administrar para el acceso remoto a grandes poblaciones.

TLS es un método estándar para proteger Sesion Initiation Protocol (SIP) de señalización de la aplicación. TLS se puede utilizar para proporcionar la autenticación y el cifrado de la SIP de señalización asociada con VoIP y otras aplicaciones basadas en SIP. MICROSOFT (2011)

- **Seguridad**

TLS cuenta con una variedad de medidas de seguridad:

- Protección contra una versión del protocolo anterior (menos seguro) versión o una suite de cifrado más débil.
- Numeración de los registros posteriores de aplicaciones con un número de secuencia y el uso de este número de secuencia en la autenticación de los códigos de mensajes (MAC).

- El uso de un resumen de mensaje mejorado con una clave (por lo que sólo una clave-titular puede comprobar la MAC).
- El mensaje que termina el handshake "final" envía un hash de todos los mensajes intercambiados handshake visto por ambas partes.

- **TLS en detalle**

“El protocolo TLS intercambia registros, que encapsulan los datos que se intercambian. Cada registro puede ser comprimido, con un código de autenticación de mensajes (MAC), o cifrado, todo dependiendo del estado de la conexión. Cada registro tiene un campo de tipo de contenido que especifica el registro, un campo de longitud y un campo de versión TLS. PAGINA WEB MICROSOFT (2011)

- **TTLS y PEAP**

En términos generales, la historia de la seguridad 802.11 es un intento para hacer frente a dos problemas principales.

El primer problema es que los protocolos utilizados para autenticar a los usuarios de la red no eran fuertes, por lo que los usuarios no autorizados podrían acceder fácilmente a los recursos de la red.

En segundo lugar, la Wired Equivalent Privacy (WEP) resultó insuficiente. "¿Qué hay de malo en WEP?" En respuesta al usuario hay preocupaciones sobre la seguridad débil, la industria comenzó a desarrollar una serie de protocolos más fuertes para el uso con la tecnología inalámbrica LAN. La norma fundamental es IEEE 802.1X, que proporciona la autenticación más fuerte y mecanismos para la distribución de protocolos más fuertes para reforzar WEP.

5.1.2 Autenticación Protocolo de Requisitos

La exigencia de cifrado fuerte para evitar la intercepción y la autenticación mutua para garantizar que la información sensible se transmite sólo a través de redes legítimas, deberá conducir una estrategia de autenticación inalámbrica.

La Intercepción es mucho más fácil. Los atacantes necesitan tener acceso físico a la red para interceptar las transmisiones, pero las ondas de radio no pueden limitarse a una instalación física sin la seguridad física directa, las garantías de cifrado deben ser incorporadas en los protocolos por dos razones:

En primer lugar es para evitar que los atacantes recuperen las credenciales de usuario a medida que viajan a través del enlace de radio. En segundo lugar, puntos de acceso no autorizados pueden ser creados en un intento de recopilar las credenciales de los usuarios desprevenidos. La Criptografía puede ofrecer las garantías necesarias de que los usuarios se conectan a una red autorizada y asegurada.

802.1X se basa en el protocolo de autenticación extensible (EAP), por lo que ofrece la opción de varios métodos para proteger el intercambio de autenticación. En la práctica, los métodos de autenticación basados en el IETF y el más conocido Transport Layer Security (TLS) estándar de cifrado puede satisfacer estrictos requisitos de autenticación. TLS protocolos basados se han desarrollado para su uso con EAP y son adecuados para instalaciones con redes LAN inalámbricas:

EAP-Seguridad de la capa de transporte (EAP-TLS), seguridad de transporte Capa de túnel (TTLS), EAP protegido (PEAP).

- **EAP-TLS**

EAP-TLS utiliza el protocolo de enlace TLS como base para la autenticación. TLS tiene muchos atributos que lo hacen Atractivo en el uso relacionado con seguridad. Está bien documentado y ha sido ampliamente analizado, y el criptoanálisis del protocolo aún no ha puesto de manifiesto deficiencias significativas en el protocolo.

TLS realiza la autenticación por el intercambio de certificados digitales. El servidor presenta un certificado al cliente. Después de validar el servidor de certificado, el cliente presenta un certificado de cliente. Naturalmente, el certificado debe ser protegido en el

cliente por una contraseña, PIN, o almacenado en una tarjeta inteligente, en función de la aplicación.

El papel central de los certificados es el talón de Aquiles de la EAP-TLS. Si no existe PKI, se debe implementar antes de EAP- TLS se puede utilizar en una red.

Gestión de certificados es un proceso largo y engorroso es una labor administrativa, sobre todo porque los certificados deben ser renovados ya que los usuarios perderán el acceso a la red inalámbrica. Además de expedición de certificados, en línea, validos son obligatorios.

Por otra parte, una PKI existente puede ser insuficiente porque la mayoría de las implementaciones de EAP-TLS requiere la presencia de ciertos atributos que no se definen cuando los primeros sistemas PKI se extendieron. Un riesgo final es que EAP-TLS protege el material de autenticación del usuario, pero no la identidad del usuario.

La conclusión es que EAP-TLS es seguro, pero el requisito para el cliente es un certificado de gran seguridad que hace TTLS y PEAP atractivo.

- **TLS de túnel con TTLS y PEAP**

Ambos TTLS y PEAP utiliza la privacidad inherente al túnel de TLS para extender de forma segura los antiguos métodos de autenticación, tales como nombre de usuario / contraseña o token de autenticación de la tarjeta a la red inalámbrica.

Ambos están en fase dos protocolos que establecen un fuerte cifrado "exterior" túnel TLS en la primera fase y luego las credenciales de autenticación de cambio a través de un "interior" método en dos etapas. Ambos-TTLS y servidores RADIUS-PEAP se pueden utilizar con los sistemas de autenticación con capacidades de proxy RADIUS para ampliar las bases de datos existentes, directorios, o de una sola vez sistemas de contraseñas para su uso con redes LAN inalámbricas.

TTLS utiliza el canal TLS para el intercambio "valor pares de atributos" (TVA), al igual que RADIUS. La flexibilidad de la AVP* mecanismo que permite a los servidores TTLS validar credenciales de usuario en casi cualquier tipo de Mecanismos de autenticación.

* AVP Attribute Value Pairs. (Valor de Atributos Pares)

La implementación TTLS admite todos los métodos definidos por EAP, así como varios métodos antiguos (CHAP, PAP, MS-CHAP y MS-CHAPv2). PEAP utiliza el canal TLS para proteger a un segundo intercambio de EAP, llamado el "interior" de cambio de EAP. La mayoría de los suplicantes se apoyan en EAP-MS-CHAPv2 para el intercambio interno, que PEAP permite al usuario utilizar bases de datos externas.

Otros métodos comunes de EAP con el apoyo de los suplicantes PEAP EAP-TLS y la tarjeta símbolo genérico (EAP-GTC). Importante ventaja de PEAP es el apoyo de Microsoft, y por lo tanto, una función de apoyo del sistema operativo. Apoyo PEAP es una característica estándar en Windows XP y está disponible como un paquete de características de Microsoft para Windows 2000. PAGINA WEB MICROSOFT (2011)

Microsoft suplicantes (clientes inalámbricos) están estrechamente integrados con el sistema operativo base y puede por lo tanto proporcionar capacidades de inicio de sesión único mediante el uso de la mismas credenciales de usuario para la autenticación en Windows y redes inalámbricas LAN. Suplicantes Microsoft, sin embargo, no apoyan el uso de las tarjetas de token. Cisco PEAP suplicantes son compatibles con EAP-GTC, pero Cisco y Microsoft han puesto en marcha PEAP de diferentes maneras que no son compatibles).

6. DISEÑO DE UNA PROPUESTA TIPO EDUROAM USANDO LA INFRAESTRUCTURA DE RADAR

6.1. SOFTWARE PARA EDUROAM

Para utilizar EDUROAM se debe asegurar que el equipo tiene bien configuradas las propiedades del Protocolo de Internet (TCP/IP) del dispositivo inalámbrico. Éste debe estar configurado para "Obtener una dirección IP automáticamente" y "Obtener la dirección del Servidor DNS automáticamente".

La conexión a EDUROAM se realiza con la tecnología de conexión segura WPA (cliente 802.1x). La autenticación de los usuarios se realiza mediante el establecimiento de túneles EAP-TTLS (mecanismo especial de autenticación que permite la fragmentación de mensajes) entre el usuario y el servicio de autenticación. Todas las comunicaciones entre el usuario y los puntos de acceso van cifradas utilizando el sistema de cifrado TKIP[*]. EDUROAM (2006)

El software SecureW2 es un cliente de EAP-TTLS de libre distribución que permite varios métodos de autenticación. Para poder conectarse al Campus Inalámbrico (EDUROAM), es necesario tener instalado este software, si el Sistema Operativo que se tiene en el ordenador es Windows 2000/XP/Vista; teniendo en cuenta que para sistemas operativos de libre distribución no se requiere dicho software.

6.2 REQUISITOS BÁSICOS

El sistema operativo debe soportar al menos WPA. Es posible que tenga que actualizar los drivers para ello.

Las credenciales utilizadas para EDUROAM, son las mismas que las de la intranet. Por ello, es imprescindible haber entrado alguna vez en la Intranet para poder hacer uso de la red EDUROAM.

[*] TKIP (Temporal Key Integrity Protocol) es también llamado hashing de clave WEP WPA, incluye mecanismos del estándar emergente 802.11i para mejorar el cifrado de datos inalámbricos. WPA tiene TKIP, que utiliza el mismo algoritmo que WEP, pero construye claves en una forma diferente.

Debe tener configurado su adaptador inalámbrico como cliente DHCP para que el sistema le pueda asignar una dirección IP.

Se debe eliminar el uso de cualquier tipo de servidor proxy en su navegador.

6.3 HARDWARE

- Ordenador portátil, PDA o dispositivo portátil que soporte las normas de la IEEE 802.11a, 802.11b o 802.11g. (como equipo suplicante)

- Capacidad inalámbrica, o un plug-in de la tarjeta inalámbrica (por ejemplo, PCMCIA, Firewire o USB).(tarjeta de red inalámbrica-cableada) para el servidor de aplicaciones

- Router que soporte los protocolos de autenticación: WPA2 ENTERPRISE, TKIP y AES

6.4 IMPLEMENTACIÓN DE LA SOLUCIÓN

El procedimiento de configuración corresponde a la simulación de la interacción entre servidores que prestan el servicio de conexión en una configuración tipo EDUROAM. Un Servidor Radius Institucional conectado (Servidor Institucional EXAMPLE.COM) que a través de un AP (Access Point) puede conectarse a otro (Servidor Institucional ucpr.edu.co), haciendo un ejemplo del servicio, además se crea un cliente en el servidor institucional EXAMPLE.COM., con el fin de verificar que el primero valide las credenciales del usuario que realiza la solicitud y proporcione y aprovisione los recursos necesarios.

6.4.1 Procedimiento en la instalación de un sistema RADIUS con dos servidores

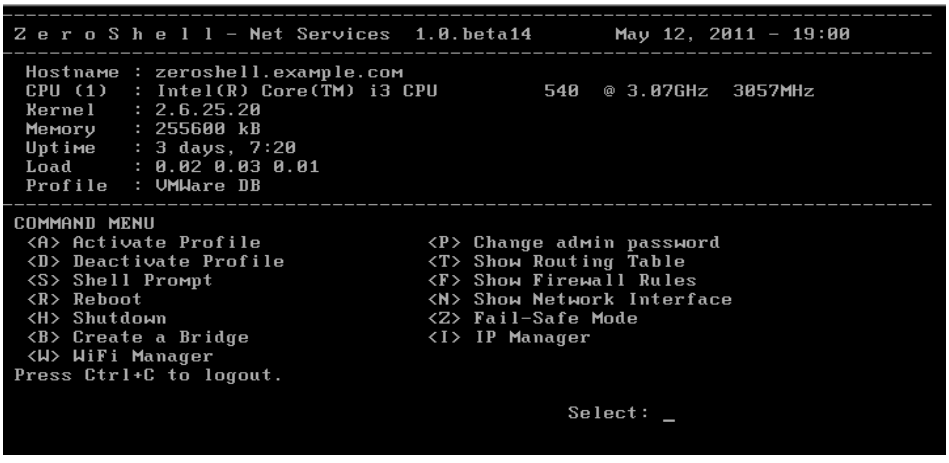


Figura 12 Gráfica: Inicio Zeroshell-Net Services 1.0.beta14 (Menú Inicial)

Fuente: Propia

La distribución utilizada para esta demostración es Zeroshell-Net services 1.0.beta14 la cual es una distribución libre y acorde a las circunstancias razón por la cual se utilizo, con dos portátiles HP Pavilion dv 6000, LENOVO G450 los cuales se utilizaron como servidores y se iniciaron con una imagen (Live CD) de la distribución zeroshell de Linux como se muestra en la figura (12) para el servidor institucional HP Pavilion dv 6000. Además se utilizo un Linksys (cisco) WRT54G2 como Access Point y como equipo certificado un portátil COMPAQ el cual demostró el proceso de conexión. Al iniciar la distribución zeroshell en los equipos servidores Institucionales se encuentra con la siguiente imagen inicial figura (12) que arroja la distribución zeroshell en ella se evidencia las características principales del equipo como memoria, procesador y cuanto tiempo lleva encendido el servidor parte superior figura (12), además los comandos principales de configuración que se visualizan al inferior figura (13).

.

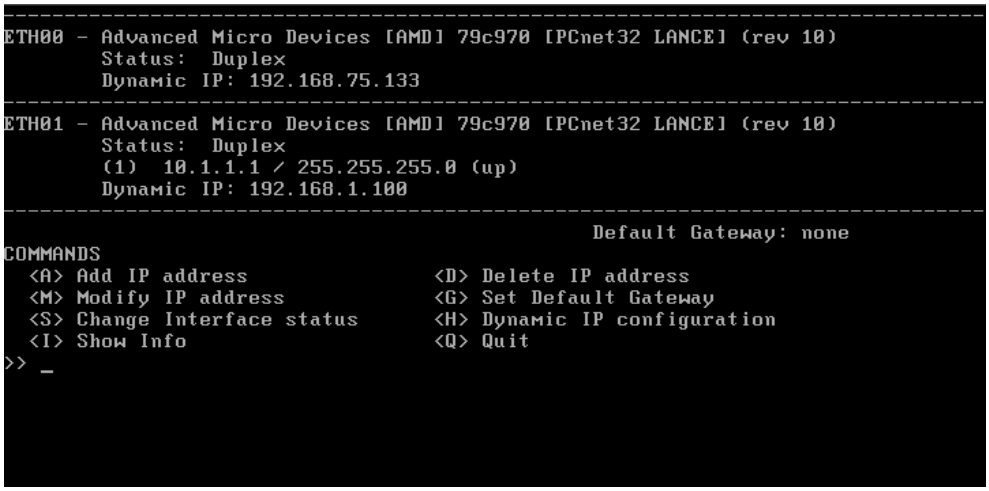


Figura 13 Gráfica: (IP Manager del Menú Inicial opción (I))

Fuente: Propia

En este imagen se puede evidenciar la configuración de las tarjetas de red del mismo, a esta función se accede a través de la opción (I) en el menú inicial figura (12); en él se configura las direcciones de red que se le asignan al servidor institucional para este caso la dirección es (10.1.1.1) con la opción (A) **Add IP address** como se ilustra en la figura (13); para volver al menú principal presionamos (Q).

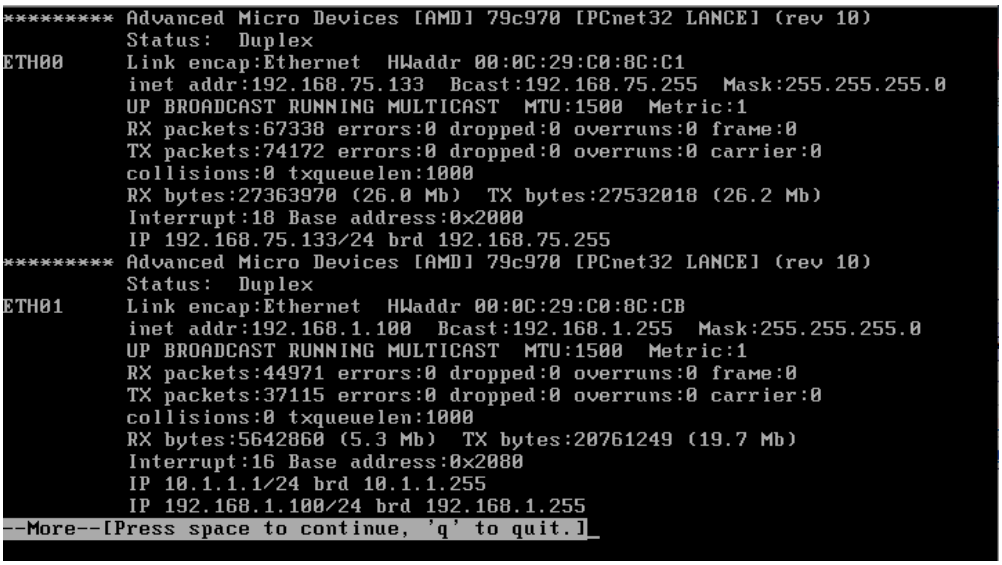


Figura 14 Gráfica: (Show Network Interface de Menú Inicial opción (N))

Fuente: Propia.

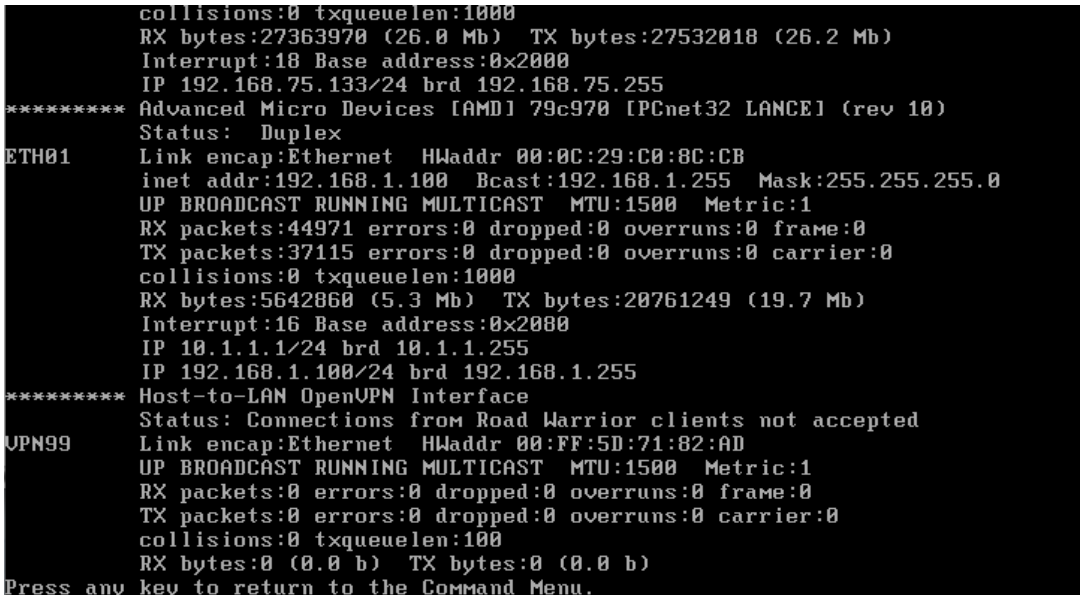


Figura 15 Gráfica: (Show Network Interface de Menú Inicial opción (N))

Fuente: Propia.

Con (N) se verifica que la dirección (IP) que se le otorgó al servidor Institucional (10.1.1.1) se encuentre correctamente configurada como se muestra en la figura (15) (ETH01 línea 8) para ingresar posteriormente vía web.

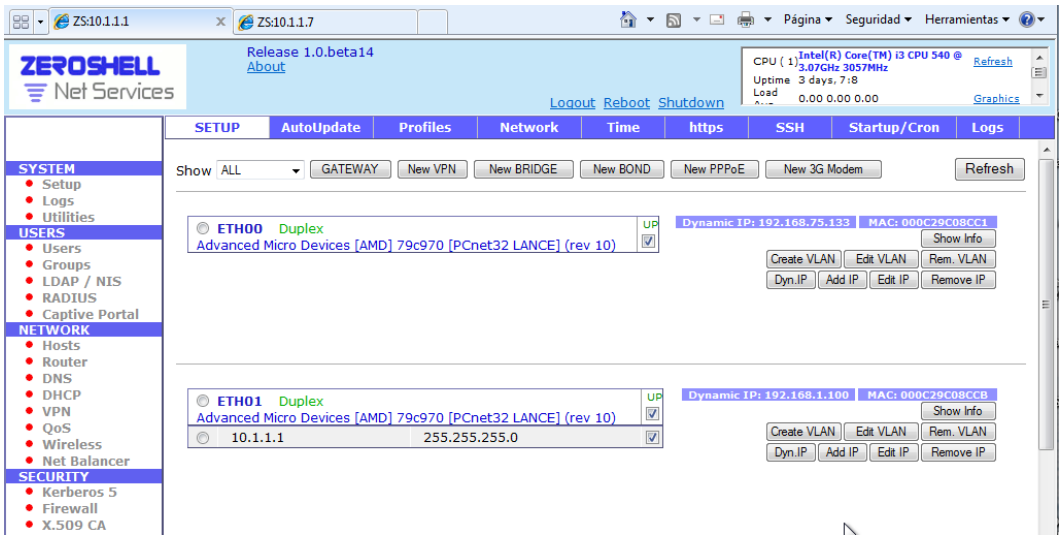


Figura 16 Gráfica: (Menú SYSTEM opción SETUP)

Fuente: Propia

A través de un navegador web se ingresa a la dirección (10.1.1.1) anteriormente configurada digitando usuario (**admin**) y contraseña (**1234**) para ingresar al sistema. Como se ilustra en la figura (16) se evidencia que la dirección ya fue asignada.

Figura 17 Gráfica: (Menú USERS opción RADIUS)

Fuente: Propia

Se ingresa a la opción RADIUS del menú para activar el servicio RADIUS (**Status:** ACTIVE) y verificar que la autoridad certificadora (CA) se encuentre activa como puede notarse en la figura (17).

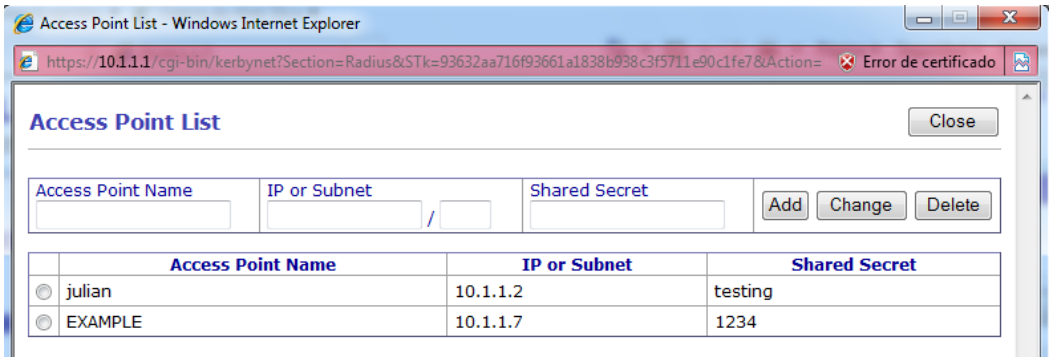


Figura 18 Gráfica: (Menu USERS/RADIUS opción Access Points)

Fuente: Propia.

Paso siguiente, se ingresa los clientes autorizados a conectarse a este servidor, en esta imagen se muestra ésta lista para el servidor (Institucional) con la dirección 10.1.1.1 entiéndase por clientes: Access Point (AP) y servidores proxy. Los cliente fueron ingresados como se ilustra en la figura (18), **Access Point Name** (julian), **IP or Subnet** (10.1.1.2) **Shared Secret** (testing), luego se presiona la tecla **ADD** y posteriormente son visualizados en la parte inferior como ilustra la misma figura.

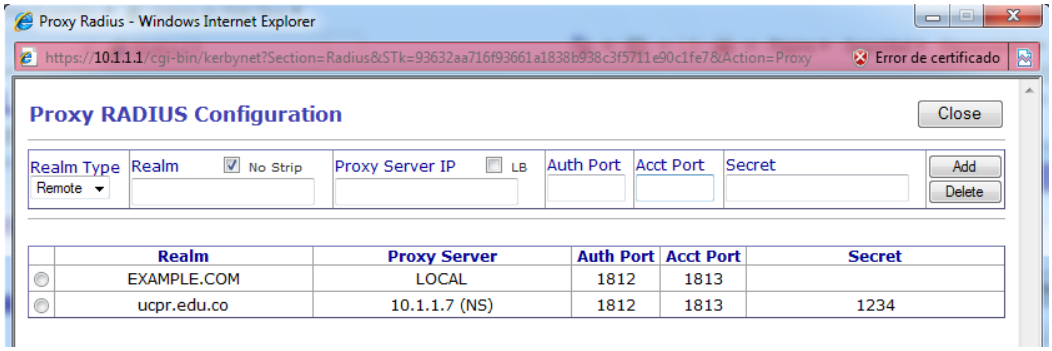


Figura 19 Gráfica: (Menú USERS/RADIUS opción Proxy)

Fuente: Propia.

A continuación se realiza la configuración de los dominios figura (19) los cuales se agregan de la siguiente forma: en la parte posterior se visualizan casillas, las cuales se complementan para el ejemplo así: **Realm** (EXAMPLE.COM), **Proxy Server IP** (LOCAL) **Auth Port** (1812) **Acct Port** (1813) **Secret** (clave que se asigna) luego se presiona la tecla **ADD** y puede observarse la creación en la parte inferior figura (19), que pueden ser autenticados de forma local o el siguiente salto que se debe dar para autenticar los dominios externos en otras maquinas, para este ejercicio se percibe que los usuarios de EXAMPLE.COM se autentican localmente mientras los de ucpr.edu.co los envía al servidor (Institucional) 10.1.1.7. Lo que nos quiere decir es que si los usuarios certificados se encuentran en este servidor (10.1.1.1) se autentican localmente, mientras si son usuarios

del servidor Institucional 10.1.1.7 y se quieren autenticar ante el servidor 10.1.1.1 los envía a verificación al servidor Institucional ucpr.edu.co 10.1.1.7.

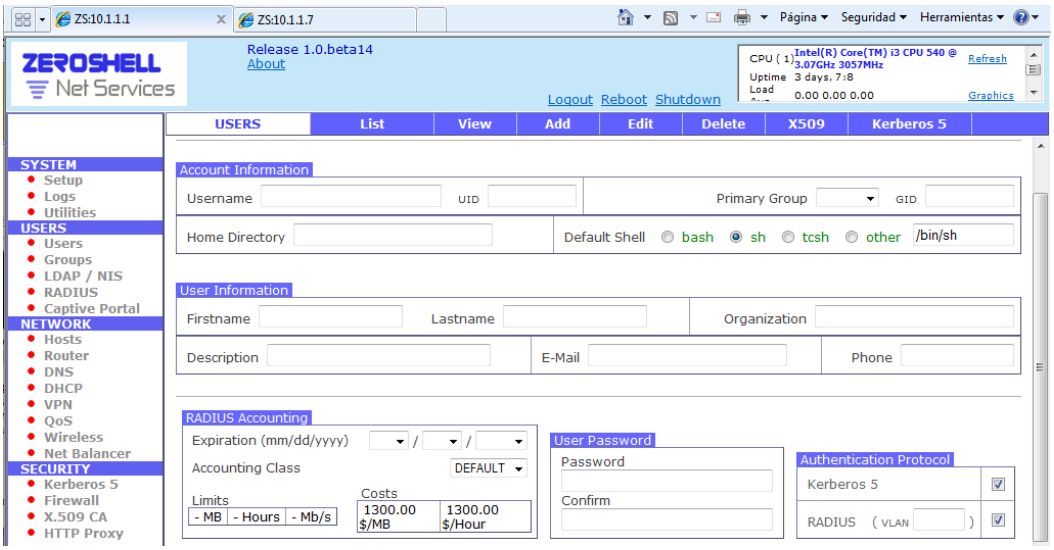


Figura 20 Gráfica: (Menú USERS /Users opción Add)

Fuente: Propia.

En la opción (Menú USERS/Users opción Add) figura (20) se ingresa la información personal de los nuevos usuarios. Estos usuarios son los que serán autenticados ante este servidor Institucional (10.1.1.1).

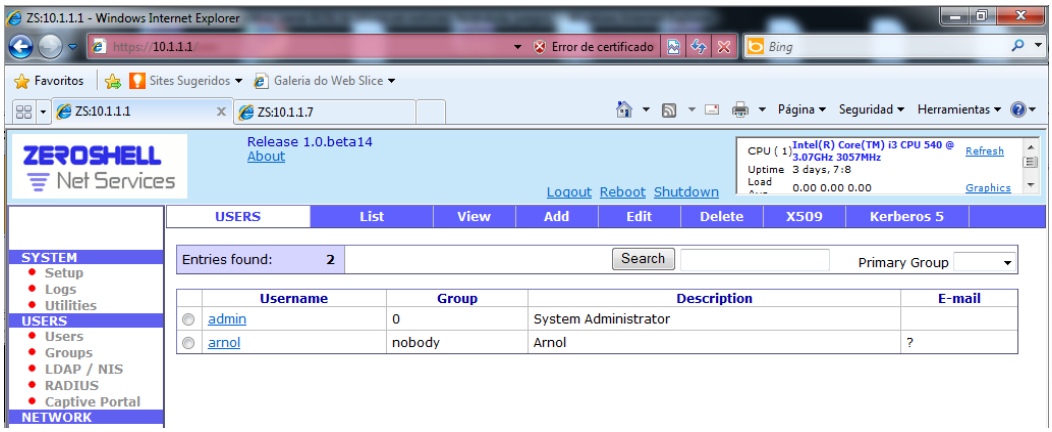


Figura 21 Gráfica: (Menú USERS opción Users)

Fuente: Propia.

En la opción USERS/Users figura (21) es donde se visualiza los usuarios que están autorizados para conectarse a este servidor (Institucional) 10.1.1.1 que fueron creados anteriormente como se ilustro en la figura (20).

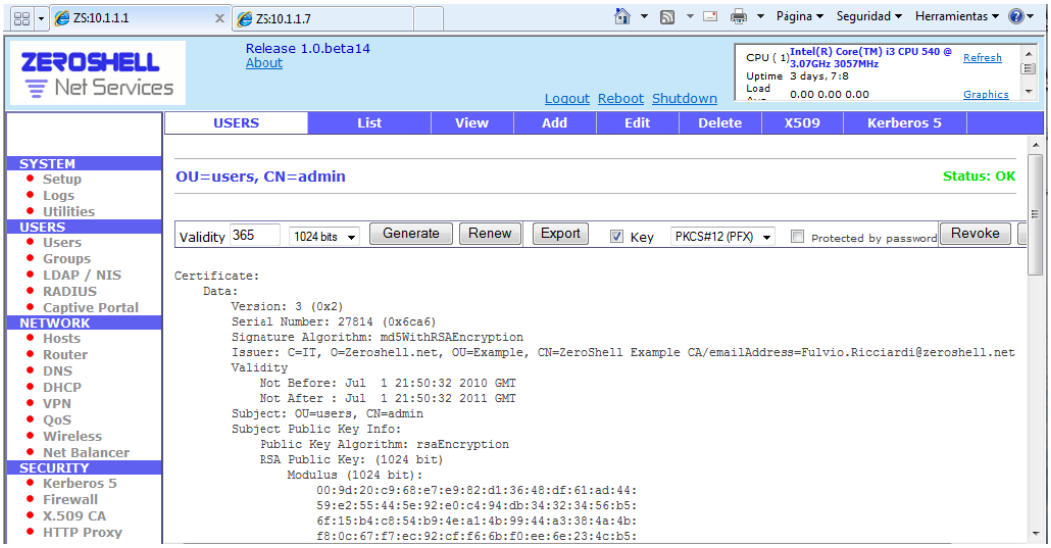


Figura 22 Gráfica: (Menú USERS /Users opción X509)

Fuente: Propia

En el (Menú USERS /Users opción X509) es donde se generan y se exportan los certificados de usuario se crean señalando el usuario para nuestro ejemplo **admin** y luego se presiona la tecla **Generate** figura (22) para su posterior instalación en el equipo cliente. Son los certificados que son utilizados para poder autenticarse ante el servidor Institucional como prueba de seguridad y de registro.

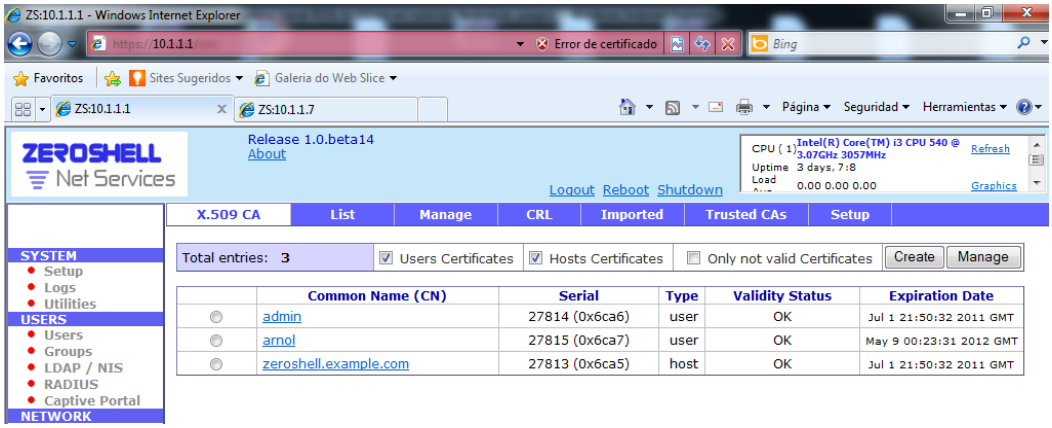


Figura 23 Gráfica: (Menú USERS /Users opción X509)

Fuente: Propia.

Figura (23) lista de los usuarios ya certificados según procedimiento de la figura (22) que pueden hacer uso de la red con sus credenciales y datos de expiración.

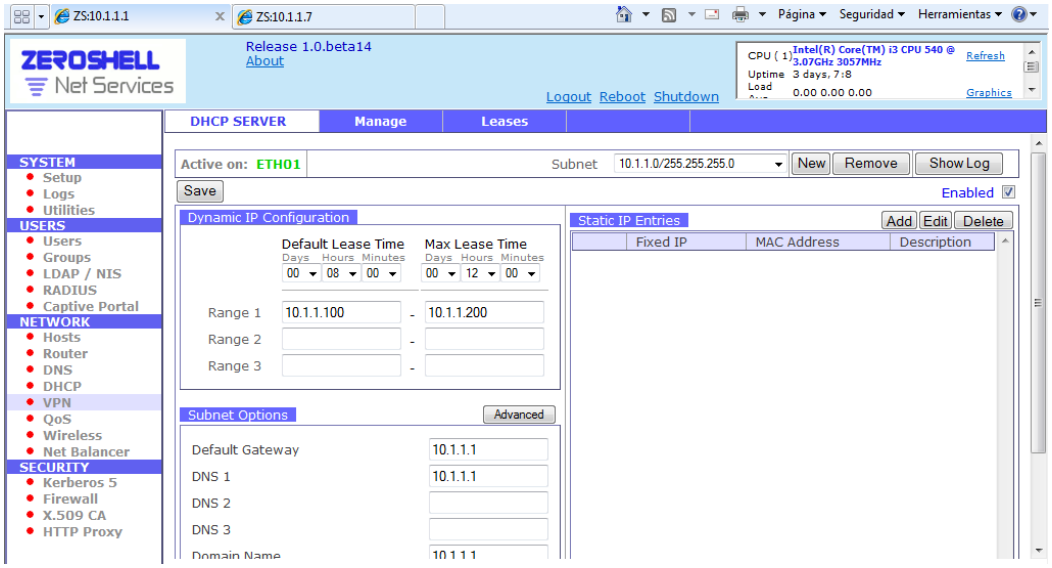


Figura 24 Gráfica: (Menú Network opción DCHP)

Fuente: Propia.

Para este caso específico figura (24) se configura en la misma máquina el servidor DCHP.

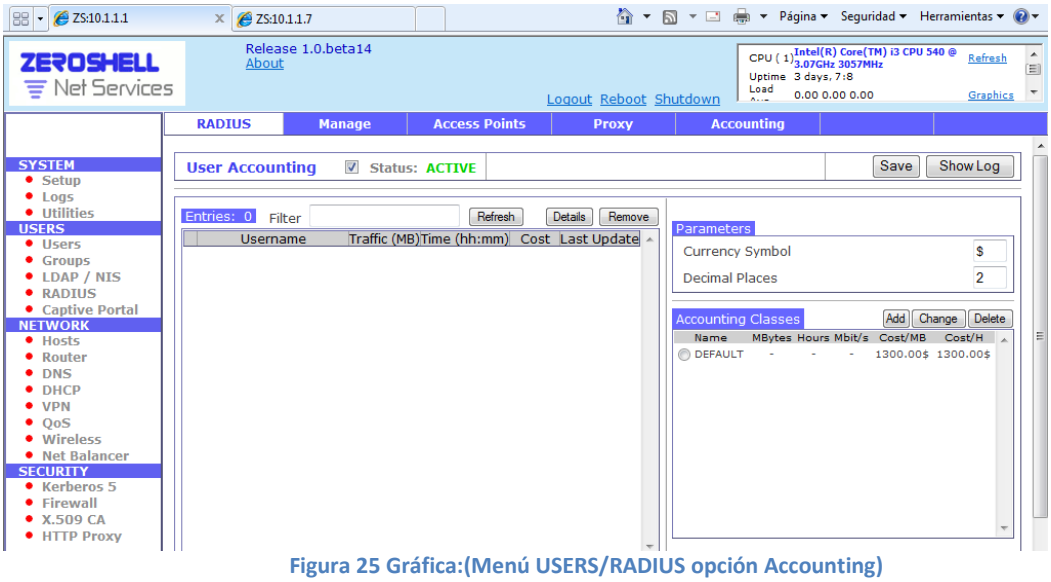


Figura 25 Gráfica:(Menú USERS/RADIUS opción Accounting)

Fuente: Propia.

Servicio de Auditoría figura (25) este servicio nos permite llevar un registro de los equipos que se encuentran conectados a la red y las actividades que realizan además de las horas de actividad que tienen los clientes.

Figura 26 Gráfica: (Menú USERS opción RADIUS)

Fuente: Propia.

Figura (26) En esta imagen se observa la configuración del servidor Institucional (10.1.1.7), en la cual se evidencia que el servicio de RADIUS este activo como se especificó en la figura (17).

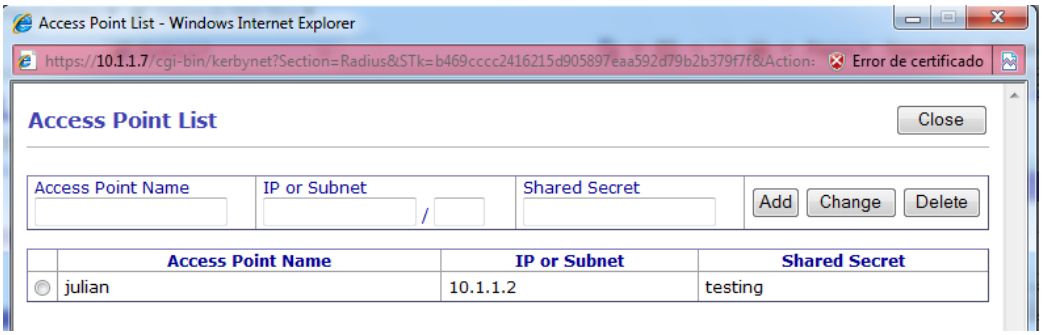


Figura 27 Gráfica: (Menú USERS/RADIUS opción Access Points)

Lista de clientes en el servidor (Institucional) 10.1.1.7, procedimiento similar al practicado en la figura (17).

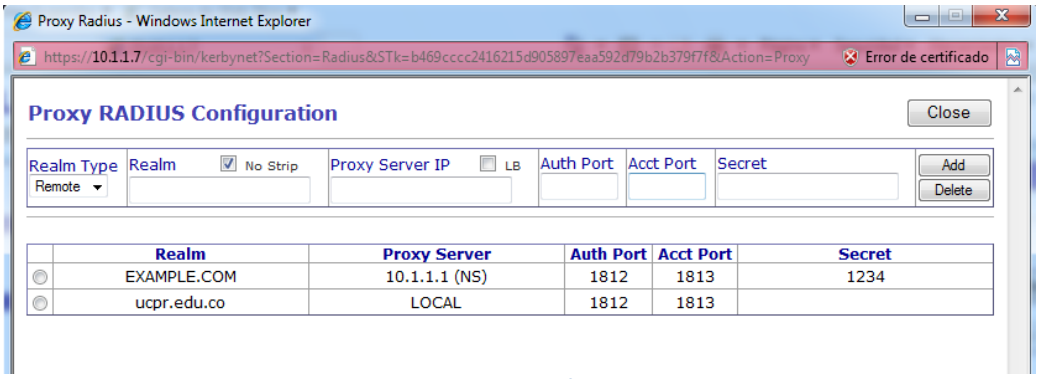


Figura 28 Gráfica: (Menú USERS/RADIUS opción Proxy)

Fuente: Propia.

Se evidencia en la figura (28) que en el servidor (Institucional) 10.1.1.7 los usuarios de EXAMPLE.COM se autentican en el servidor (Institucional) 10.1.1.1 mientras los de ucpr.edu.co lo hacen localmente. El procedimiento de agregar los dominios es igual al practicado en la figura (19). Lo que nos quiere decir es que si los usuarios certificados se encuentran en este servidor Institucional (10.1.1.7) se autentican localmente, mientras si son usuarios del servidor Institucional (10.1.1.1) y se quieren autenticar ante el servidor (10.1.1.7) los envía a verificación al servidor Institucional EXAMPLE.COM (10.1.1.1).

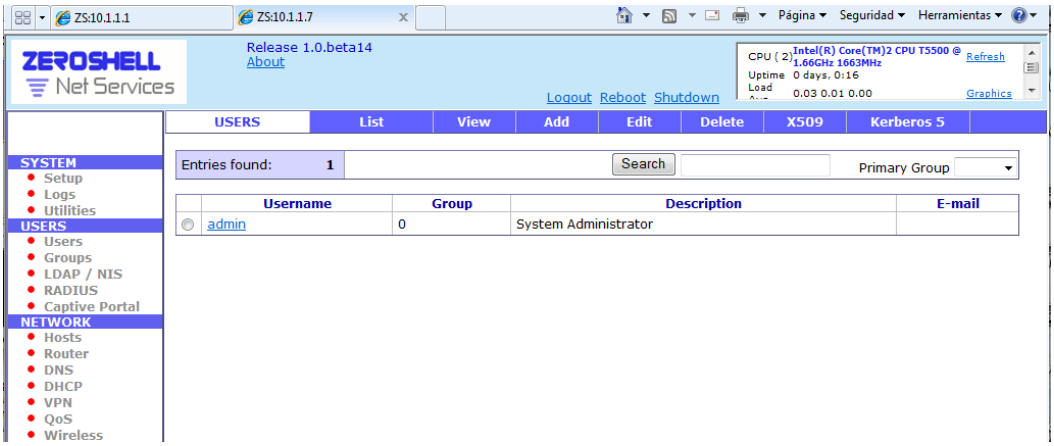


Figura 29 Gráfica: (Menú USERS opción Users)

Fuente: Propia.

Figura (29) usuario configurado para el servidor (institucional) 10.1.1.7, después de haberse seguido los pasos explicados en la configuración del servidor Institucional (10.1.1.1) en las figuras (20) y (22). Tal método de configuración aplica para este servidor.

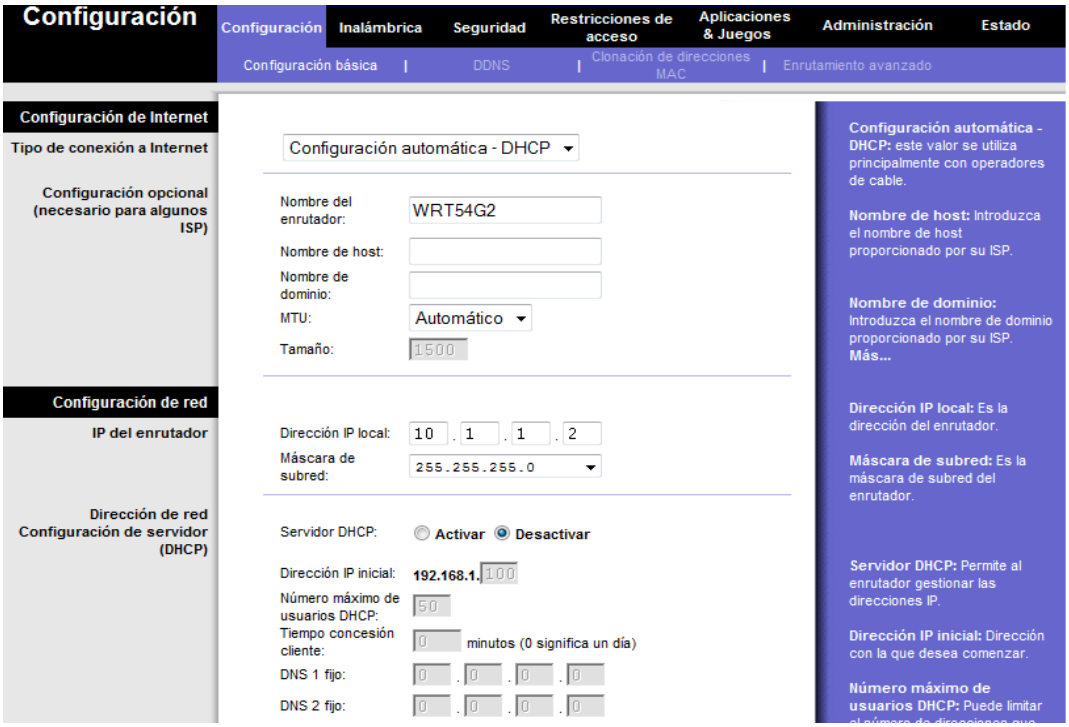


Figura 30 Gráfica: (Configuración AP/Configuración básica)

Fuente: Propia.

Configuración interna del AP (LINKSYS) figura (30) al cual se ingresa digitando en el navegador web la dirección IP 192.168.1.1, luego se desactiva la opción DHCP y se configura la Dirección IP para nuestro caso la 10.1.1.2

Figura 31 Gráfica: (Configuración AP/Inalámbrica/Configuración Inalámbrica básica)

Fuente: Propia.

Ingresamos la configuración básica como se muestra en la figura (31).

Figura 32 Gráfica (Configuración AP/Inalámbrica/Seguridad Inalámbrica)

Fuente: Propia.

Ingresamos el modo de seguridad WPA2 Enterprise, el algoritmo de cifrado TKIP+AES, la dirección del servidor RADIUS para nuestro ejemplo la 10.1.1.7 con su respectiva clave (testing) según figura (32).

- Configuración Básica para el Equipo Cliente en este caso en especial, el sistema operativo es Windows 7. Esta configuración se realiza en el equipo para poder acceder a la red sin inconvenientes**.**

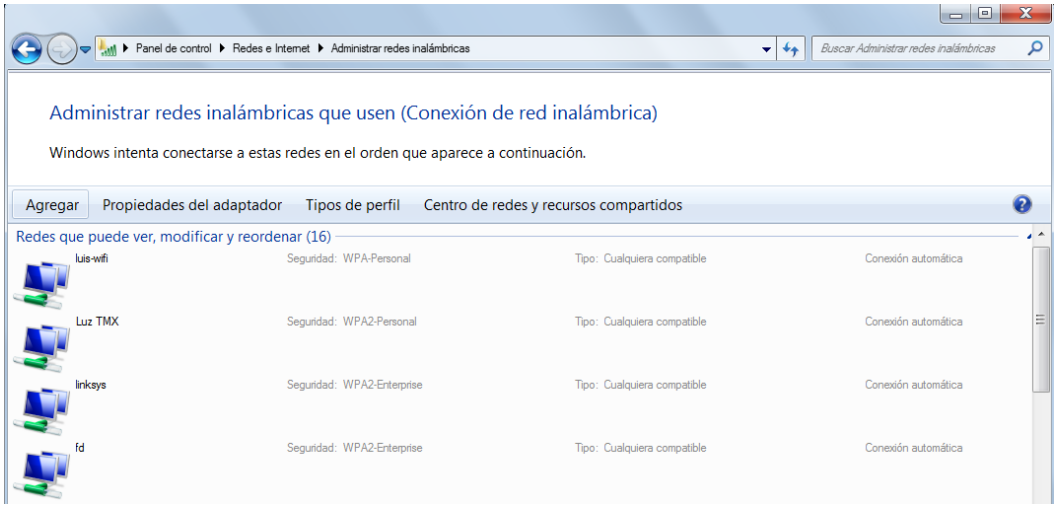


Figura 33 Gráfica: (Administrador redes Inalámbricas Windows 7)

Fuente: Propia

Para proceder con la configuración se debe crear una red nueva en el menú AGREGAR de la venta administrador redes inalámbricas como se muestra en la figura (33). Esta configuración se hace manual.

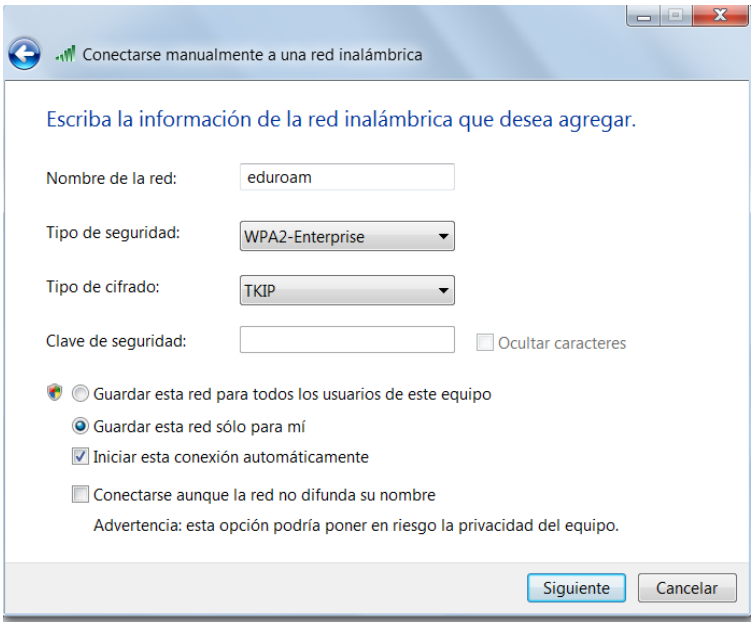


Figura 34 Gráfica: (Cuadro de Dialogo después de presionar AGREGAR (figura 33))

Fuente: Propia.

En el momento de presionar agregar una nueva red figura (33) aparece este cuadro de dialogo figura (34) en el cual se Configura **Nombre de la Red**, **Tipo de Seguridad y Cifrado** como se evidencia en la figura (34) Luego se presiona siguiente.

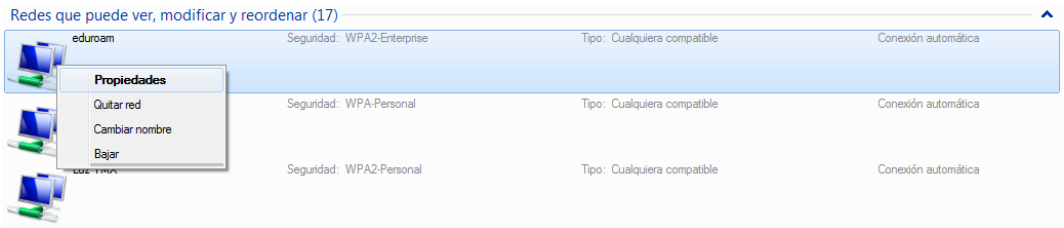


Figura 35 Gráfica: (Administrador redes Inalámbricas Windows 7)

Fuente: Propia.

Después de ser presionado el botón “siguiente” se visualiza la posterior pantalla figura (35) donde se puede observar la red creada y a la cual damos clic derecho sobre ella para configurar sus propiedades figura (35).

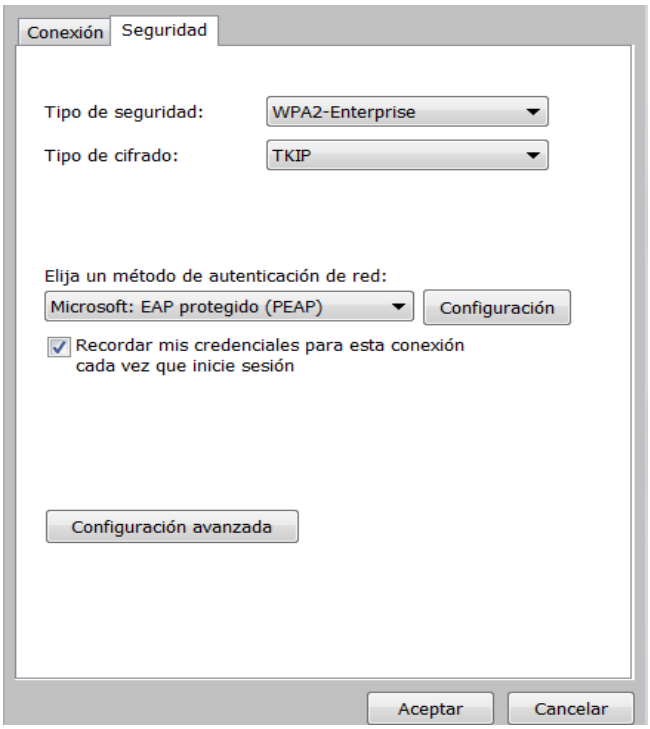


Figura 36 Gráfica: (Menú de propiedades de la red creada)

Fuente: Propia.

Al momento de dar clic en propiedades del menú figura (35) aparece la siguiente ventana figura (36) en la cual en la parte posterior hay un menú donde ubicamos la opción seguridad luego se presiona la opción configuración de la cual se despliega la ventana siguiente figura (37).

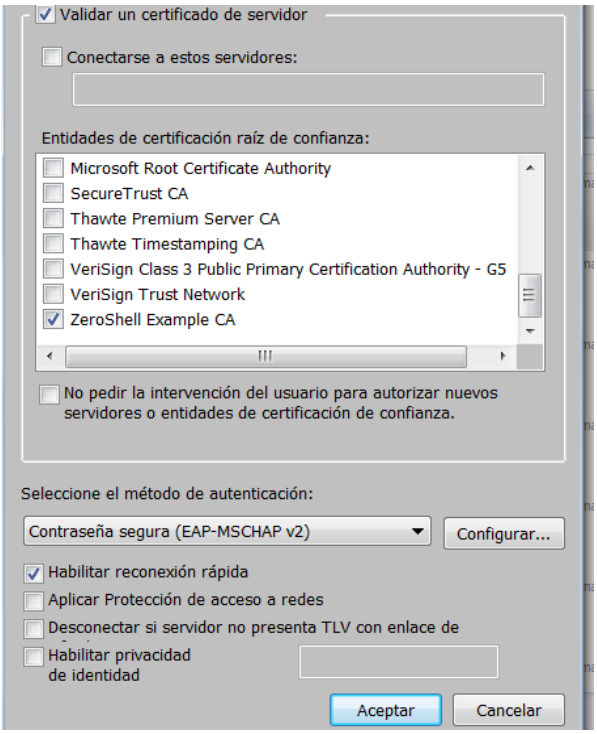


Figura 37 Gráfica: (Validación del certificado)

Fuente: Propia.

Esta ventana es la que nos valida el uso de los certificados seleccionando la opción que se muestra en la figura (37). (ZeroShell Example. CA). Luego se pasa a la opción configurar en la cual se quita la selección que tiene la casilla como se muestra en la siguiente figura (38) para que no genere conflicto con las claves de inicio de sesión de Windows.

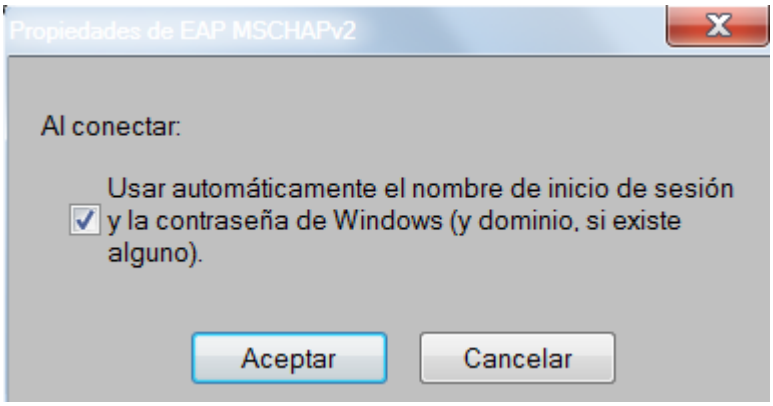


Figura 38 Gráfica: (Opción Configurar figura (36))

Fuente: Propia.

Se Presiona ACEPTAR y la configuración del equipo ha culminado correctamente.

Después de haber realizado todas las configuraciones pertinentes tantos en los servidores como en los (AP) y los equipos cliente se realiza la prueba de conexión desde un equipo que se encuentra certificado por el servidor (Institucional) 10.1.1.1 figura (23) pero que se va a conectar a través de un (AP) que se encuentra registrado en el servidor (Institucional) 10.1.1.7 figura (27).

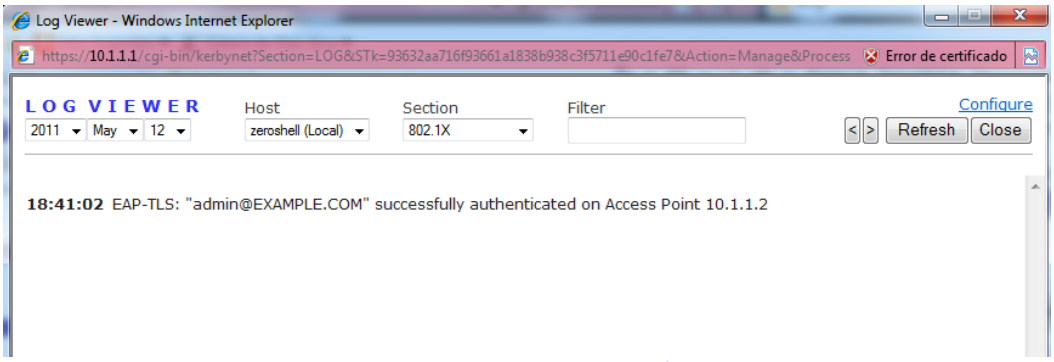


Figura 39 Gráfica: (Menú SYSTEM/Logs)

Fuente: Propia.

En el (Menú SYSTEM/Logs) ingresamos a **Section** 802.1x figura (39) del servidor (Institucional) 10.1.1.1 para verificar que el usuario identificado con el REALM admin@example.com se halla autenticado correctamente lo cual se ilustra en esta figura (39). (18:41:02 EAP-TLS: admin@EXAMPLE.COM successfully authenticated on Access Point 10.1.1.2).

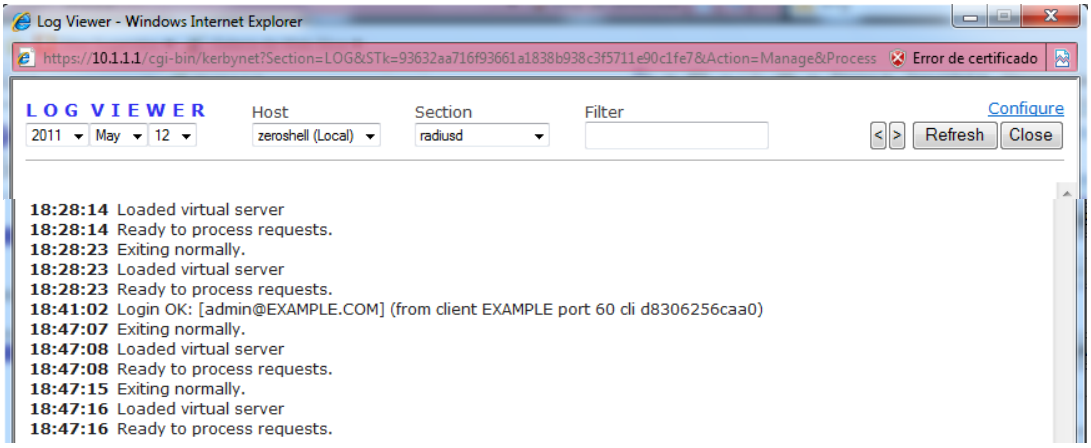


Figura 40 Gráfica: (Menú SYSTEM/Logs)

Fuente: Propia.

En el (Menú SYSTEM/Logs) se ingresa a **Section** radiusd figura (40); en esta imagen se observa como a la **18:41:02** se envía un Login ok para el REALM admin@example.com el

cual se encuentra autenticando desde el cliente "EXAMPLE" (nombre dado al servidor 10.1.1.7 en la configuración que se encuentra en la figura (19). Este paso lo que nos evidencia es que el equipo se conecto correctamente a red y el proceso de certificación se cumplió con éxito.

6.5 RADAR (Red Académica de alta Velocidad Regional)

Es una red que busca la convergencia de servicios entre las ciudades de: Caldas, Huila, Quindío, Risaralda y Tolima**.** Contando con una conexión de alta velocidad entre la región centro occidental del país (Eje Cafetero) teniendo como objetivo la promoción del trabajo en colaboración entre las instituciones educativas de la región con las del resto del país y los centros de investigación más prestigiosos del mundo.

Trabaja con un ancho de banda de 100 Mbps y 40Mbps entre regiones, Su funcionamiento está dirigido por la Universidad Tecnológica de Pereira y estas son las instituciones que hasta ahora hacen parte de RADAR:

Institución	*Tipo de institución*	*Ciudad*	*Red Académica Regional*
ACUAPEZ (Corporación Centro de Desarrollo Tecnológico Piscícola Surcolombiano)	Centro de I+D	Neiva	RADAR
CENICAFE	Centro de I+D	Chinchiná	RADAR
Corporación Instituto de Administración y Finanzas, CIAF	IES	Pereira	RADAR
Corporación Universitaria de Santa Rosa de Cabal, UNISARC	IES	Chinchiná	RADAR
Corporación Universitaria del Huila, Corhuila	IES	Neiva	RADAR
Fundación Cardiovascular de Colombia Instituto Corazón (Ibagué)	Salud	Ibagué	RADAR
Fundación Cardiovascular de Colombia Instituto Corazón (Manizales)	Salud	Manizales	RADAR
Fundación Universitaria del Área Andina (Pereira)	IES	Pereira	RADAR

Hospital Departamental Santa Sofía de Caldas	Salud	Manizales	RADAR
Hospital Universitario San Jorge	Salud	Pereira	RADAR
Universidad Autónoma de Manizales	IES	Manizales	RADAR
Universidad Católica de Manizales	IES	Manizales	RADAR
Universidad Católica Popular del Risaralda	IES	Pereira	RADAR
Universidad Cooperativa de Colombia (Pereira)	IES	Pereira	RADAR
Universidad de Caldas	IES	Manizales	RADAR
Universidad de Ibagué	IES	Ibagué	RADAR
Universidad de Manizales	IES	Manizales	RADAR
Universidad del Quindío	IES	Armenia	RADAR
Universidad del Tolima	IES	Ibagué	RADAR
Universidad Libre (Pereira)	IES	Pereira	RADAR
Universidad Nacional de Colombia (Manizales)	IES	Manizales	RADAR
Universidad Sur Colombiana	IES	Neiva	RADAR
Universidad Tecnológica de Pereira	IES	Pereira	RADAR
Centros de I + D	IES: Instituciones de Educación Superior	Salud	Cultura

Figura 41 Tabla: instituciones adscritas RADAR

Fuente: página oficial de RENATA, http://www.renata.edu.co/index.php/component/content/article/3-que-es-renata/449-radar-red-academica-de-alta-velocidad-regional-logotipo-de-la-red-regional-radar.html

6.6 PROPUESTA TIPO EDUROAM SOBRE LA INFRAESTRUCTURA RADAR

Dentro de las características de la propuesta se encuentra la independencia de la infraestructura en la que desee implementarse:

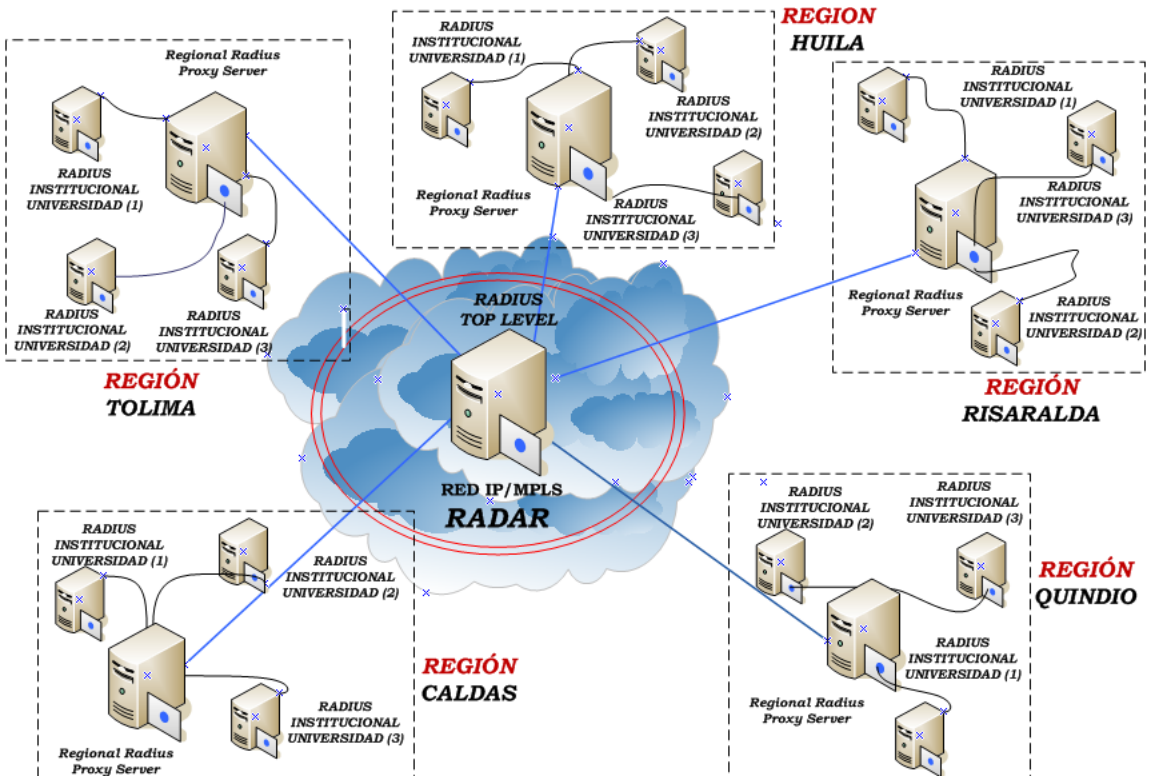


Figura 42 Gráfica: Propuesta de Implementación

Fuente: propia

Se plantea hacer uso de la infraestructura ofrecida por la red RADAR para la conexión de servicios EDUROAM. Tener un equipo ofreciendo un servidor RADIUS en cada dependencia académica puede garantizar la itinerancia de cada suplicante, quien debida a sus necesidades intente acceder a su red nativa aprovechando la conexión en la institución visitante.

Los servidores RADIUS (Institucionales) se encargan de redireccionar a un RADIUS de nivel superior (TOP LEVEL) para que este a su vez pueda determinar a qué institución pertenece el usuario que está tratando de ser autenticado en una institución visitante. Las credenciales son originadas en la institución origen para cada uno de sus clientes. Estas

credenciales las genera el servidor Institucional y luego se envía vía web para su posterior instalación en los equipos "clientes". Los clientes de una institución origen en el momento de querer conectarse a una institución destino, inician un proceso que lleva acabo el servidor Regional (Proxy Server) pues él tiene configurado los Servidores Proxy y los clientes (base de datos) de su región, además gestiona y validar el procedimiento. Si el proceso es de una región a otra el servidor (TOP LEVEL) que tiene asignado los clientes (base de datos) y los Servidores proxy de todas las regiones, es quien realiza el proceso. Todo esto usando el protocolo 802.1x y los métodos de cifrado con claves a través de EAP-TLS, TTLS y PEAP entre otros.

JERARQUÍA DE SERVIDORES RADIUS

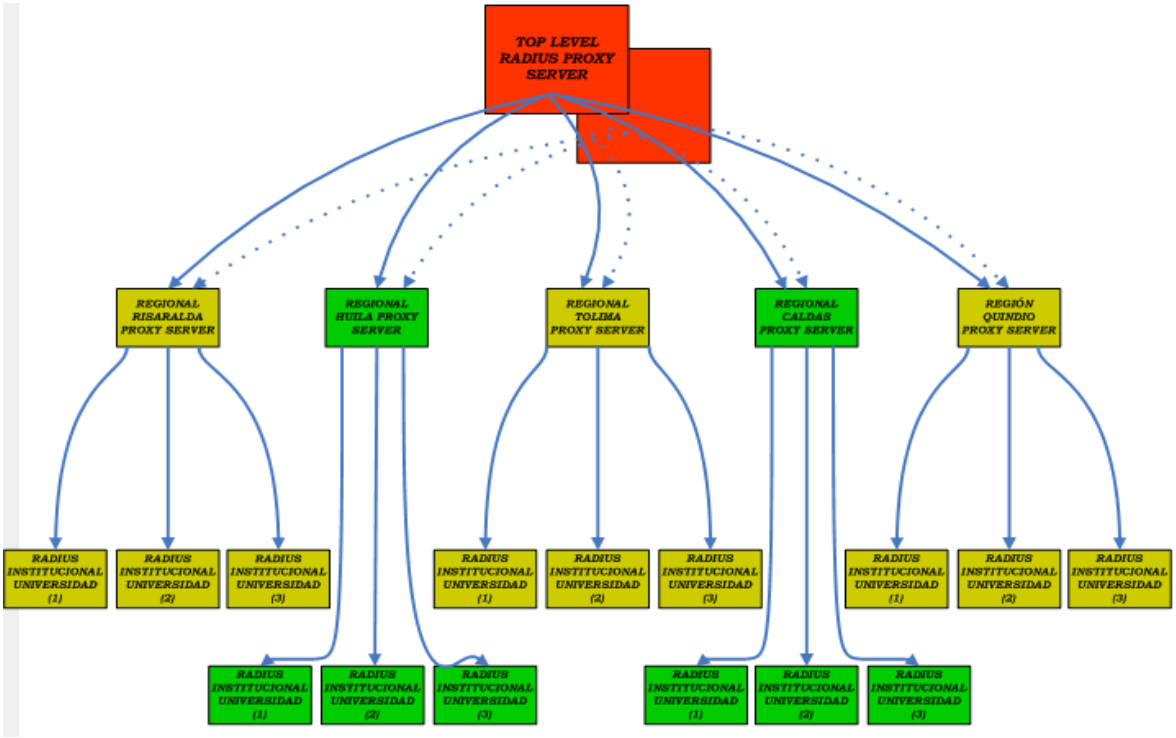


Figura 43 Gráfica: Jerarquía de servidores RADIUS

Fuente: Propia

Se establece la jerarquía de servidores, permitiendo que el RADIUS de nivel superior genere redundancia al contar con un servidor de respaldo para la comunicación entre los RADIUS institucionales. Garantizando que los usuarios no dependan de una sola conexión.

CONCLUSIONES

La itinerancia es un componente de la cotidianidad actual de los usuarios del sistema académico y de investigación por lo que el concepto de movilidad toma relevancia en la medida en que las herramientas tecnológicas prestan facilidad de conexión independiente de la ubicación geográfica. En Colombia se ha venido impulsando soluciones que buscan facilitar el trabajo colaborativo. Las redes académicas son el ejemplo más cercano además de constituir el núcleo más pequeño en un esquema que busca incluir a todos los agentes que intervienen, desde lo académico y la investigación y desarrollo en el esquema Estado-Universidad-Sector productivo.

La infraestructura de red configurada en el eje cafetero (RADAR); proyecto gestionado desde los centros educativos, soporta una multiplicidad de servicios dentro de los que puede ubicarse fácilmente EDUROAM. Este consiste en proporcionar y gestionar una conexión desde una institución usando una infraestructura diferente de la propia, con el fin de tener control sobre la itinerancia de sus usuarios y no adicionar carga en la administración a la red que es visitada.

Los componentes más relevantes dentro de un sistema EDUROAM corresponden a sus pilares fundamentales:

La información del usuario solo se revela a la red a la que pertenece, identificando su nivel de acceso y los recursos que requiere. Esto proporciona un nivel de seguridad suficiente tanto para el usuario itinerante como para la red visitada. EDUROAM no hace una sobre carga administrativa a la red visitada, pues los recursos que proporciona y aprovisiona para su uso dependen de la información que valida en la red de origen. La red visitada confía en los permisos que otorga la red de origen, pues esta última garantiza una gestión integral (Seguridad y uso de recursos).

En el mundo se destacan proyectos similares a EDUROAM, no en su funcionamiento, pero si en su filosofía, pues las redes académicas locales aparecen en el escenario como soluciones que buscan dar una alternativa de conexión a los agentes que componen los sistemas educativos.

EDUROAM en España inició en el 2002 prestando el servicio en la Universidad Politécnica de Madrid. Fue tan buena la experiencia que se tuvo que al poco tiempo se extendió a nivel nacional, incluyendo además de las universidades, a los centros de

investigación y desarrollo. España fue el piloto en esta iniciativa que se encuentra extendida en Europa, Asia-Pacífico, Estados Unidos y Canadá siendo una solución y servicio importante en el trabajo colaborativo.

En América latina más allá de las redes académicas que generalmente son de ciudades, no existe antecedente de un servicio similar. Esto llama la atención pues significa una oportunidad importante en la ampliación de soluciones que impacten a las comunidades académicas en Colombia. La red RADAR y especialmente su infraestructura, permite el desarrollo de una solución tipo EDUROAM, pues se encuentra presente en cinco departamentos por lo que puede proporcionar acceso y cobertura; factores relacionados con la itinerancia de los usuarios del sistema educativo.

La infraestructura de RADAR puede ser utilizada de forma fácil, diseñando una configuración de servicio tipo EDUROAM que aproveche los recursos de conexión ofrecidos por ella y se transforme en una red capaz de ofrecer servicios a los usuarios itinerantes de las comunidades académicas de 5 departamentos (Huila, Tolima, Risaralda, Caldas y Quindío). Además preste gestión integral de recursos de acuerdo a permisos establecidos desde cada una de las instituciones que participen en el proyecto, una seguridad en el uso de infraestructura, eficiencia en el uso de recursos compartidos, con lo cual pueda fomentarse el trabajo colaborativo al facilitar el uso de recursos de conexión en el desarrollo de dinámicas grupales entre distintos equipos o centros de investigación de instituciones diferentes en ciudades con esta misma característica.

Para una solución tipo EDUROAM en el eje cafetero aprovechando la infraestructura de RADAR se requiere de un servidor RADIUS en cada institución o centro participante que se encargue de realizar la gestión de credenciales de los agentes itinerantes del servicio, además de proveer los recursos necesarios de acuerdo a las sus características y definido por políticas individuales (cada institución será autónoma en ese sentido). Esto no necesariamente supone una adquisición de dicho servidor. Como la solución corresponde a la implementación de ciertos protocolos a través de software, se podría aprovechar un servidor existente en la institución y mediante técnicas de virtualización o segmentación, se podría ofrecer fácilmente el servicio.

Por otra parte se requiere también de otro servidor RADIUS de mayor nivel que se encargue de agrupar y gestionar las solicitudes de los servidores menores. Este servidor puede ser establecido por ciudad y/o en la medida de la posibilidad y de la necesidad su función consistirá en agrupar servidores RADIUS por zonas. En este punto la labor de direccionar y gestionar todas las conexiones y solicitudes deberá hacerlas un servidor diferente cuyas prestaciones sean adecuadas y coherentes. Esto está muy relacionado con la cantidad de conexiones a gestionar (número de instituciones participantes y estimación de la cantidad de usuarios del servicio).

La inversión en infraestructura es casi ninguna por lo que se puede dedicar una pequeña partida presupuestal en la adquisición de equipos servidores, por un lado que favorezcan el servicio y por el otro, que puedan dar ciertas garantías a los usuarios del mismo. Las instituciones pueden realizar convenios de cooperación en donde se acuerde el diseño de la solución, sobre todo en el aspecto de su administración, en este sentido el órgano asesor debe ser RADAR.

Tener un servicio como estos funcionando en RADAR amplia la cobertura y mejora las prestaciones de conexión que cualquier institución podría ofrecer por si sola, favoreciendo grandemente a los procesos sociales en los que las universidades juegan un papel relevante, pues ayudando a generar espacios en donde se pueda realizar trabajos colaborativos, los productos que se tengan a partir de dicha labor, contendrán mayores elementos de inclusión que favorecerán a la región.

Es oportuno decir que EDUROAM es un muy buen ejemplo de un servicio cuyo fin resulta en proporcionar los medios necesarios y suficientes en la conectividad de agentes académicos, con el objeto de propiciar espacios en donde la colaboración de integrantes de distintas disciplinas no encuentre en la distancia, incluso en la misma itinerancia de sus usuarios, inconvenientes al disponer de sus recursos.

RECOMENDACIONES

Una de las ventajas principales de un servicio cuya configuración sea del tipo EDUROAM resulta ser la independencia que se tiene sobre la infraestructura, entendiendo dicha autonomía no como un "sin importar" sino como "el aprovechamiento de", de ahí que su implementación sobre RADAR signifique el uso en mayor medida, de una infraestructura establecida plenamente y la disminución del costo de la inversión inicial.

De otro lado y, en la misma medida, se puede aprovechar la infraestructura actual de las instituciones o por lo menos de las universidades, pues sus equipos servidores estarían en la capacidad de soportar la configuración del servicio, esto como solución al inicio mientras se pasa la etapa de pruebas y se comience a incrementar la demanda, sin embargo también es necesario realizar proyecciones que busquen dar ciertas garantías al proyecto, por lo que es recomendable definir aspectos futuros como la administración.

Cualquier sistema o solución requerirá de un administrador y de un soporte técnico efectivo. De ahí que el establecimiento de normas de uso, administración y soporte, deban ser temas de discusión en cada una de las instituciones y/o convenios que se establezcan con cada parte. Estaría muy bien incluir un presupuesto que busque garantizar dichos elementos como parte integral de la solución.

Todo esto en lo posible debería estar enmarcado en unas políticas definidas ampliamente por las instituciones que conformen el proyecto con el fin de que se clarifique la manera como se entiende y se debe usar el servicio, además el estimulo al trabajo en equipo estaría relacionado más con los convenios de colaboración y cooperación entre las instituciones, por lo que es relevante desarrollar servicios adicionales como la movilidad estudiantil y docente, los servicios de consulta y referencia de información y demás herramientas que ayuden a que los usuarios no encuentren mayores inconvenientes con la itinerancia.

REFERENCIAS BIBLIOGRÁFICAS

PELLEJERO, Izaskun Fundamentos y aplicaciones de seguridad en redes WLan, 2006- 160p.

STALLINGS, William. Data and computer communications, 2004- 868p. Disponible en La Biblioteca Dario Castrillon Hoyos, UCP, Ref 004.68 S18 ej. 2.

OTRAS FUENTES

Adriana Berlanga, Ángeles Bosom, Maria José Hernández,http://www.slideshare.net/sandravc/e-learning-presentation-57822.

Andra filip, Estefania Vásquez Torres. Seguridad en redes WIFI: EDUROM, http://trajano.us.es/~fornes/RSR/2010/Seguridad%20en%20redes%20Wifi20Eduroam.pdf.

Dale Liu, Cisco Router and Switch Forensics: Investigating and Analyzing Malicious Network Activity (2009) 504p. consultado en http://books.google.com.co/books?id=wgSzJ737rHsC&pg=RA1-A11&dq=eap&hl=es&ei=fnndTZ2F9CftwfDmpjADw&sa=X&oi=book_result&ct=result&resnum=7&ved=0CFIQ6AEwBg#v=onepage&q=eap&f=false.

Diámetro http://translate.google.com/translate?hl=es&langpair=en%7Ces&u=http://www.javvin.com/protocolDIAMETERProtocol.html

EDUROMA (2010), http://www.eduroam.org/index.php?p=europe. Consultado marzo de 2011. Consultado Mayo 2011

Hassell, RADIUS-2002, 190p. Disponible en: http://www.google.com.co/search?hl=es&tbo=1&tbm=bks&q=radius&oq=radius&aq=f&aqi=&aql=&gs_sm=e&gs_upl=4327l7244l0l8l8l0l0l0l1l93l134l2.

Maria Carmen Españana Boquera, Servicios avanzados de telecomunicaciones. 2003-816p consultado en: http://books.google.com.co/books?id=yTSoYCiXYAAC&pg=PA297&dq=RFC+2284&hl=es&ei=m5Xh

TeveCqaN0AG_97CxBw&sa=X&oi=book_result&ct=result&resnum=1&ved=0CCUQ6AEwAA#v=onepage&q=RFC%202284&f=false.

Nakhjiri, Nakhjiri- AAA and network security for mobile access: radius, diameter, EAP 2005 - 295p. consultado en http://books.google.com.co/books?id=Qb_hFQ6QBdsC&pg=PA250&dq=ttls&hl=es&ei=p4DdTeuIIszAtgeJj-WmDw&sa=X&oi=book_result&ct=result&resnum=4&ved=0CDkQ6AEwAw#v=onepage&q=ttls&f=false.

Philippe Mathon- Windows Server 2003: Servicios de Red TCP/IP. 2004-524p.Consultado en:http://books.google.com.co/books?id=AzsPbQURXVsC&pg=PA503&dq=RFC+2865+y+2866&hl=es&ei=7ZHhTcSwLIjL0QG1vJC9Bw&sa=X&oi=book_result&ct=result&resnum=1&ved=0CCgQ6AEwAA#v=onepage&q=RFC%202865%20y%202866&f=false.

PROTOCOLO (AAA) www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-1/101_aaa-part1.html.

PROTOCOLO (AAA) www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-1/101_aaa-part1.htm, Consultado Mayo 2011.

REALM NAME http://technet.microsoft.com/en-us/library/cc779938 (WS.10).aspx, consultado mayo 2011.

Seguridad de la capa de transporte (TLS) http://technet.microsoft.com/es-es/library/ff715256.aspx.consultado Mayo 2011

Servicio de informática y comunicaciones, universidad de Zaragoza (2011).http://sicuz.unizar.es/red/wifi/EDUROAM.htm. Consultada Mayo de 2011.

.TLS Y PEAP http://technet.microsoft.com/es-es/library/cc757996(WS.10).aspx.

Usuarios EDUROAM, http://www.tic.ehu.es/p265-shintrct/es/contenidos/informacion/wifi/es_wifi/acceso.html, consultado Mayo 2011

802.1X/EAP. Consultado en http://es.kioskea.net/contents/wifi/wifi-802.1x.php3.

DICCIONARIOS

Diccionario de informática http://www.alegsa.com.ar/Dic/roaming.php.