PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO Y VALIDACIÓN DE UN MÉTODO DE ROAMING RÁPIDO EN CAPA 2 PARA UNA RED WI-FI CON AUTENTICACIÓN 802.1X

Tesis para optar el Título de Ingeniero Electrónico, presentado por:

JESÚS GARCÍA MARTÍNEZ

JOEL TEJADA LATORRE

ASESOR: César Augusto Santiváñez Guarniz, Ph. D.

Lima, octubre del 2018

A Dios, por darme la vida y
sostenerme hasta este día.

A mis padres, Simón y Milda, por
su amor, apoyo y enseñanzas. Gracias
por acompañarme en mi preparación
profesional y confiar siempre en mis decisiones.

A mis hermanos, Gilda, Orlando y
Gisella, por ser el apoyo de la familia
durante mi preparación universitaria.

A mi compañera de vida, Pamela,
por impulsarme a ser mejor siempre.
A sus padres, por el apoyo incondicional
que me mostraron desde que los conozco.

A mi asesor, Cesar Santiváñez, por su instrucción
y enseñanzas durante el desarrollo de este trabajo.

A mi amigo Joel, por siempre recordarme
el camino que recorrí hasta llegar al V.
Por todos los ratos viendo letras blancas en
una pantalla negra. Fue un gusto trabajar en equipo.

Jesús García Martínez

A Dios por darme el don de la vida.

A mis padres, Jorge y Elsa, por su infinito amor y apoyo incondicional. Gracias por su arduo trabajo y dedicación que permitieron convertirme en profesional.

A mis hermanos, Jorge Luis y Marycris, mi ahijado Felipe y familiares por ser fuente de alegría y orgullo en mi vida.

A mi asesor, Cesar Santiváñez, por su paciencia y guía durante el desarrollo de la tesis.

A mi compañero de tesis y amigo Jesús, por todas las amanecidas y nunca tirar la toalla con el código hostapd. ¡Lo logramos!

Joel Tejada Latorre

RESUMEN

El trabajo desarrollado en la presente tesis consiste en el diseño y validación de un método que garantice un roaming rápido, menor a 150 ms, para una red Wi-Fi con el nivel más alto de seguridad recomendado en el estándar 802.11 (WPA2-Enterprise) el cual utiliza un esquema de autenticación por usuario (802.1X).

En el primer capítulo, se recorre brevemente la historia de las redes Wi-Fi y se describe cómo el roaming termina siendo determinante para brindar calidad de servicio a diversas aplicaciones de tiempo real. Asimismo, se presentan los objetivos y el alcance del presente trabajo.

En el segundo capítulo, se explica brevemente conceptos básicos de redes Wi-Fi. Además, se presenta la enmienda 802.11i la cual indica el nivel de seguridad de una red Wi-Fi y se explica el proceso de asociación a una Red de Seguridad Robusta.

En el tercer capítulo, se describe el proceso de roaming, tipos y fases. Además, se explica el impacto del nivel de seguridad en un proceso de roaming. Luego, se presentan los mecanismos y métodos de roaming rápido introducidos por el estándar IEEE 802.11 además del método OKC. En la última sección de este capítulo, se brindan observaciones a los métodos de roaming rápido actuales.

En el cuarto capítulo, se indican los requerimientos de diseño que se han considerado para el sistema de roaming rápido. En la segunda parte de este capítulo, se explica el diseño cada etapa del sistema, además de detallarse la implementación de la arquitectura y el método de key Caching seleccionado.

En el capítulo final, se presentan las diferentes pruebas que se llevaron a cabo para verificar el funcionamiento del sistema. Por último, se presentan las conclusiones obtenidas de la implementación y las pruebas realizadas sobre el sistema, basadas en los objetivos de la tesis y trabajos que podrían complementar el diseño desarrollado.

DEPARTAMENTO DE
INGENIERÍA
SECCIÓN ELECTRICIDAD Y ELECTRÓNICA

PONTIFICIA
UNIVERSIDAD
CATÓLICA
DEL PERÚ

TEMA DE TESIS PARA OPTAR EL TÍTULO DE INGENIERO ELECTRÓNICO

Título : Diseño y Validación de un Método de Roaming Rápido en Capa 2 para una red Wi-Fi con Autenticación 802.1X

Área : Telecomunicaciones

Asesor : César Augusto Santiváñez Guarniz, Ph.D.

Alumnos : Jesús García Martínez / Joel Tejada Latorre

Códigos : 20104678 / 20110091

Fecha : 02-10-2018

#1431

Descripción y Objetivos

Desplegar una red Wi-Fi (IEEE 802.11) empresarial conlleva a enfrentar una serie de retos como protección ante intrusos, interferencia de canales, mantener calidad de servicio ante movimientos de usuario, entre otros. Al proceso que involucra mantener la conexión a la red de un usuario cuando se desplaza entre puntos de acceso se le conoce como *Roaming*.

En una red que utiliza el estándar 802.1X, con autenticación por usuario para proveer un nivel de seguridad alto, el roaming puede tardar hasta más de 700 milisegundos ya que requieren comunicación adicional con servidores de autenticación. Esta demora impacta negativamente en el rendimiento de aplicaciones sensibles como voz y video. Existen métodos y arquitecturas de red que pretenden mitigar la demora del roaming (por ejemplo, el estándar IEEE 802.11r para roaming rápido en redes Wi-Fi) pero requiere que todos los dispositivos usuarios en la red sean compatibles. De esta manera se evidencia que garantizar un roaming rápido con un nivel de seguridad alto (802.1X), resulta en un verdadero reto de ingeniería y aún más en redes heterogéneas (usuarios con dispositivos de distintos fabricante y distintitos sistemas operativos).

La presente tesis busca desarrollar un método de roaming rápido que funcione en una arquitectura con puntos de acceso autónomos trabajando de manera inteligente formando un clúster escalable a decenas de Puntos de Acceso Inalámbricos (Access Points, o APs), sin requerir modificación alguna en los terminales clientes y que garantice un tiempo de roaming menor a 150 milisegundos en un despliegue de alta seguridad con 802.1X.

El desarrollo de esta tesis implica (i) realizar un profundo análisis del estándar 802.11 y las técnicas de roaming rápido existentes, (ii) diseñar el método de roaming con los requerimientos descritos anteriormente, (iii) implementar un prototipo del sistema en Access Points (APs) comerciales soportando el sistema operativo OpenWRT (POSIX-compliant), (iv) validar los tiempos de roaming en un testbed formado por los APs que corren nuestra solución.

MÁXIMO 50 PÁGINAS

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
FACULTAD DE CIENCIAS E INGENIERÍA
M. Sc. Ing. WILLY CARRERA SORIA
Coordinador de la Especialidad de Ingeniería Electrónica

DEPARTAMENTO DE
INGENIERÍA
SECCIÒN ELECTRICIDAD Y ELECTRÒNICA

PONTIFICIA
UNIVERSIDAD
CATÓLICA
DEL PERÚ

TEMA DE TESIS PARA OPTAR EL TÍTULO DE INGENIERO ELECTRÓNICO

Título : Diseño y Validación de un Método de Roaming Rápido en Capa 2 para una red Wi-Fi con Autenticación 802.1X

Índice

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
FACULTAD DE CIENCIAS E INGENIERÍA

M. Sc. Ing. WILLY CARRERA SORIA
Coordinador de la Especialidad de Ingeniería Electrónica

MÁXIMO 50 PÁGINAS

DEPARTAMENTO DE
INGENIERÍA
SECCIÒN ELECTRICIDAD Y ELECTRÒNICA

PONTIFICIA
UNIVERSIDAD CATÓLICA
DEL PERÚ

JUSTIFICACIÓN TEMA DOBLE

Título : Diseño y Validación de un Método de Roaming Rápido en Capa 2 para una red Wifi con Autenticación 802.1X

Alumnos : Joel Tejada Latorre
Jesús García Martínez

Códigos : 20110091
20104678

Dada la extensión y dificultad del tema, el desarrollo del trabajo de tesis comprende dos personas. La tarea por llevar a cabo se divide como sigue:

TEMA	HORAS	
	Joel Tejada Latorre	Jesús García Martínez
Redes Wifi Enterprise	50	40
IEEE802.11i	50	30
IEEE802.1X / EAP	40	40
Métodos de Roaming	40	50
OpenWRT	40	60
Pruebas de concepto - Legacy	80	80
Diseño Método de FSR	50	50
Hostapd (Coding)	10	130
Diseño Gestor Llaves	80	30
Implementación Gestor de Llaves	90	10
Integración	30	30
Pruebas de concepto	30	30
Pruebas funcionales / Pruebas de Esfuerzo	60	60
Análisis	40	40
PROMEDIO	**690**	**680**

En total se tienen 1370 horas, con un promedio de más de 600 horas por tesista.

iii

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
FACULTAD DE CIENCIAS E INGENIERÍA

M. Sc. Ing. WILLY CARRERA SORIA
Coordinador de la Especialidad de Ingeniería Electrónica

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ECUACIONES

LISTA DE ANEXOS

(CD ADJUNTO)

INTRODUCCIÓN

Desplegar una red Wi-Fi (IEEE 802.11) empresarial conlleva a enfrentar una serie de retos como protección ante intrusos, interferencia de canales, mantener calidad de servicio ante movimientos de usuario, entre otros. Al proceso que involucra mantener la conexión a la red de un usuario cuando se desplaza entre puntos de acceso se le conoce como *Roaming*.

En una red que utiliza el estándar 802.1X, con autenticación por usuario para proveer un nivel de seguridad alto, el roaming puede tardar hasta más de 700 milisegundos ya que requieren comunicación adicional con servidores de autenticación. Esta demora impacta negativamente en el rendimiento de aplicaciones sensibles como voz y video. Existen métodos y arquitecturas de red que pretenden mitigar la demora del roaming (por ejemplo, el estándar IEEE 802.11r para roaming rápido en redes Wi-Fi) pero requiere que todos los dispositivos usuarios en la red sean compatibles. De esta manera se evidencia que garantizar un roaming rápido con un nivel de seguridad alto (802.1X), resulta en un verdadero reto de ingeniería y aún más en redes heterogéneas (usuarios con dispositivos de distintos fabricante y distintitos sistemas operativos).

La presente tesis busca desarrollar un método de roaming rápido que funcione en una arquitectura con puntos de acceso autónomos trabajando de manera inteligente formando un clúster escalable a decenas de Puntos de Acceso Inalámbricos (Access Points, o APs), sin requerir modificación alguna en los terminales clientes y que garantice un tiempo de roaming menor a 150 milisegundos en un despliegue de alta seguridad con 802.1X.

El desarrollo de esta tesis implica (i) realizar un profundo análisis del estándar 802.11 y las técnicas de roaming rápido existentes, (ii) diseñar el método de roaming con los requerimientos descritos anteriormente, (iii) implementar un prototipo del sistema en Access Points (APs) comerciales soportando el sistema operativo OpenWRT (POSIX-compliant), (iv) validar los tiempos de roaming en un testbed formado por los APs que corren nuestra solución.

CAPITULO 1

PROBLEMÁTICA Y OBJETIVOS

El presente capítulo contiene una breve introducción a las redes Wi-Fi, su evolución, los requerimientos que tiene una red empresarial y el impacto del roaming en las aplicaciones de tiempo real. Finalmente, se presenta el *Roaming* como uno de los más críticos a resolver dentro de una red de acceso inalámbrico Wi-Fi con alto nivel de seguridad.

1.1 Redes Wi-Fi

Las redes de área local inalámbricas (*WLANs* por sus siglas en inglés) son sistemas de comunicación de datos que utilizan técnicas de modulación en ondas de radio para transmitir información de un punto a otro sin necesidad de un medio físico dedicado. Estas WLANs son usadas en áreas limitadas como oficinas, edificios, campus típicamente como extensiones de sus redes fijas o cableadas para ofrecer la posibilidad de usar equipos móviles y mejorar los niveles de producción.

Las tecnologías WLAN surgieron a fines de 1990 con productos que operaban en la banda libre de 900 MHz. Estos equipos brindaban velocidades de transferencia de datos cerca a los 1Mbps lo cual era mucho más lento que lo ofrecido por las redes cableadas de la época que alcanzaban los 10Mbps. Luego, para el año 1992 los proveedores

empezaron a comercializar equipos que operaban en la banda libre de 2.4 GHz [1]. A pesar de que estos equipos alcanzaron velocidades mayores a los anteriores, tenían un problema común: la no interoperabilidad entre equipos de distintos proveedores. Esta necesidad de interoperabilidad llevó a distintas organizaciones a trabajar en la elaboración de un estándar para el desarrollo de tecnologías WLAN y garantizar interoperabilidad.

Dos organizaciones importantes que siguen contribuyen con el desarrollo de la estandarización de tecnologías WLAN son la IEEE (*Institute of Electric and Electronics Engineers*) y la *Wi-Fi Alliance.* A continuación, se explicarán sus contribuciones históricas.

1.1.1 IEEE 802.11: Historia y Evolución

La IEEE es una organización mundial sin fines de lucro de ingenieros y científicos que tiene como misión fomentar la innovación tecnológica y excelencia en beneficio de la humanidad. Trabaja en función a proyectos como el IEEE 802, que se creó en 1980 con el propósito de desarrollar estándares para las redes de área local y metropolitana (LAN y MAN), principalmente en las dos primeras capas del modelo OSI. Los proyectos se dividen en grupos de trabajos que desarrollan una tecnología específica dentro del proyecto. Por ejemplo, el estándar *ethernet* proviene del grupo de trabajo 802.3.

En el año 1990 se creó el grupo de trabajo IEEE 802.11 con el propósito de proponer un estándar abierto que defina los protocolos que garanticen interoperabilidad de los equipos inalámbricos en los dos niveles más bajos del modelo OSI, es decir las técnicas de transmisión y métodos de acceso al medio entre otras cosas.

Para el año 1997 se tuvo la primera versión del estándar para WLANs IEEE 802.11 y tanta fue la demanda de los servicios inalámbricos que incluso muchos fabricantes ya vendían equipos 802.11 antes de oficializarse formalmente el estándar. No mucho tiempo después, el rápido desarrollo de

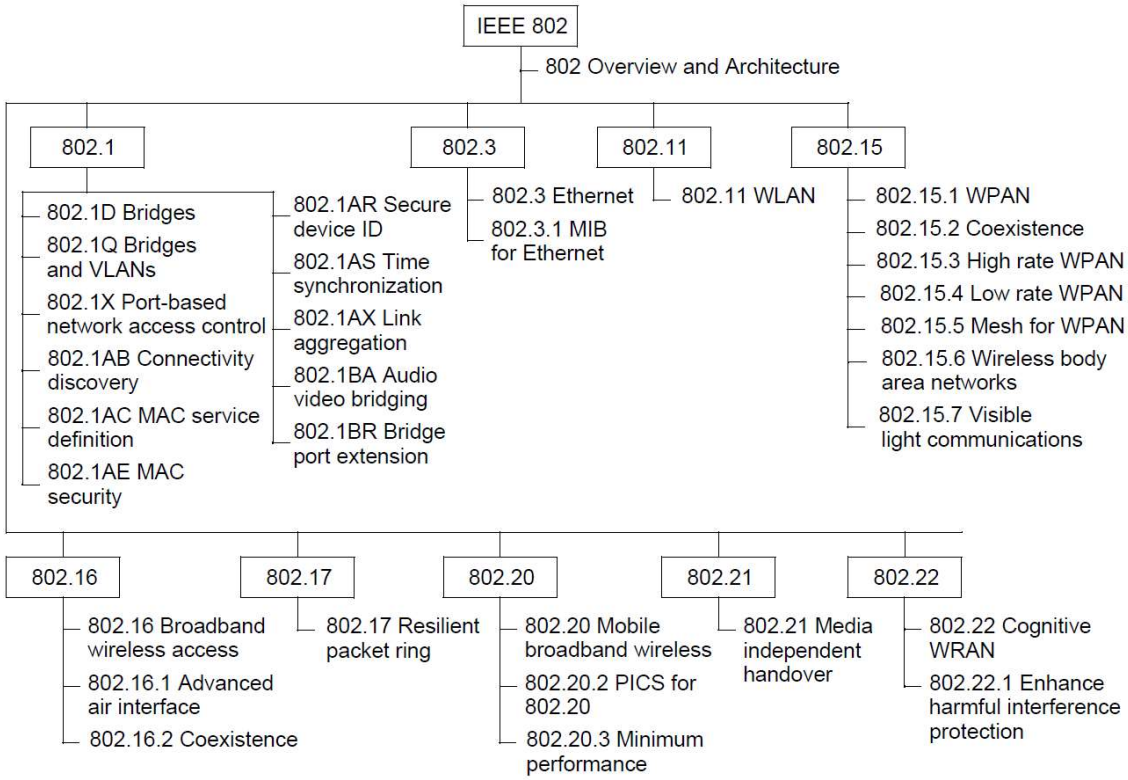


Figura 1-1 IEEE 802 – Grupos de Trabajo (2014) *[2]*

Estandar IEEE WLAN	Velocidad Over-the-Air (OTA)	Velocidad Media Access Control Layer, Service Access (MAC SAP)
IEEE 802.11b	11 Mbps	5 Mbps
IEEE 802.11g	54 Mbps	25 Mbps (cuando .11b no esta presente)
IEEE 802.11a	54 Mbps	25 Mbps
IEEE 802.11n	Hasta 600 Mbps	Hasta 400 Mbps
IEEE 802.11ac	Hasta 867 Mbps con 2 antenas y 80 MHz; Hasta 1.3 Gbps con 3 antenas y 80 MHz	Hasta 600 Mbps hasta 2 antenas y 80 MHz; Hasta 900 Mbps con 3 antenas y 80 MHz
IEEE 802.11ad	Por lo menos 1.1 Gbps (hasta 4.6 Gbps en algunos dispositivos de primera generación)	Hasta 700 Mbps para 1.1 Gbps OTA (hasta 3 Gbps para 4.6 Gbps OTA)

Tabla 1-1 Rendimiento de los Estándares IEEE 802.11 *[2]*

terminales móviles con aplicaciones que demandaban más ancho de banda puso en evidencia las deficiencias iniciales del estándar, el cual no contemplaba consideraciones importantes en cuanto a la seguridad o la calidad de servicio. Por este motivo, el grupo de trabajo 802.11 creó subgrupos de trabajos identificados con letras del abecedario, los cuales tenían el objetivo de desarrollar enmiendas técnicas para complementar y continuar mejorando el estándar completo.

1.1.2 *Wi-Fi Alliance*

La *Wi-Fi Alliance,* originalmente llamada *Wireless Ethernet Compatibility Alliance* (WECA), fue fundada en agosto de 1999. Su nombre cambió a *Wi-Fi Alliance* en el año 2001. Se trata de una organización mundial sin fines de lucro conformada por más de 300 compañías interesadas en promover el crecimiento y desarrollo de las tecnologías *WLANs*. Mientras que la IEEE es responsable de desarrollar los estándares técnicos, es la *Wi-Fi Alliance* quien

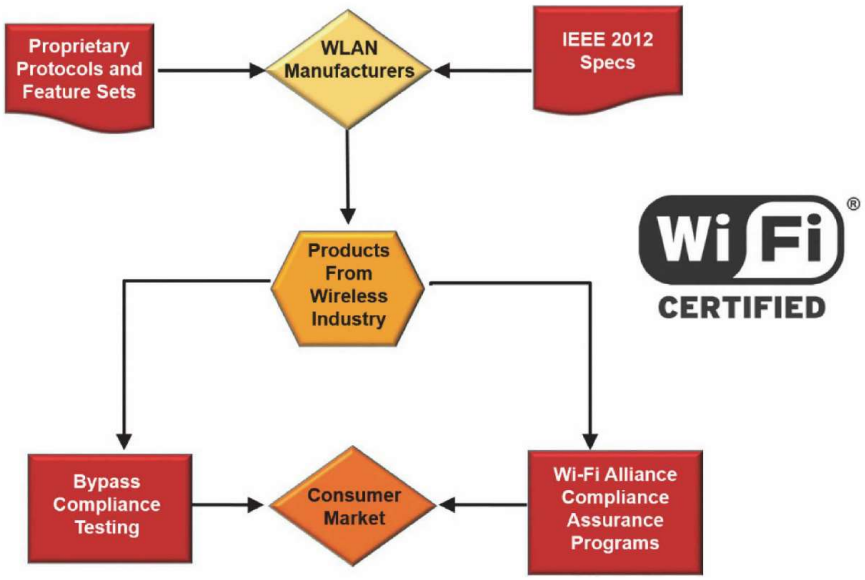


Figura 1-2 Flujo de Certificación y Logo de Wi-Fi *[1]*

se encarga de garantizar la interoperabilidad de los equipos comerciales mediante pruebas de certificación. Esto les da garantía a los usuarios finales que los equipos certificados de diferentes marcas o proveedores pueden funcionar en un ambiente común.

Esta certificación Wi-Fi no sólo incluye la radio interoperabilidad definida en los estándares 802.11 a, b, g, n, ac, ad, etc. Sino además incluye certificación de tecnologías de seguridad, multimedia, convergencia y algunas características especiales. Por dar un ejemplo, *Wi-Fi Protected Access* (WPA) es un conjunto de protocolos/tecnología desarrollado por la Wi-fi

Figura 1-3 Certificados Wi-Fi - iPhone 5s *[3]*

Alliance (motivado por presión del mercado) para proteger la confidencialidad de las comunicaciones en las WLAN las cuales eran vulnerables en los inicios del estándar IEEE 802.11.

Luego, el grupo de trabajo IEEE802.11i se encargó de mejorarlo e integrarlo formalmente al estándar llamando a su versión final WPA2. Para consultar las certificaciones Wi-Fi de un equipo dado, basta con buscar el modelo en [3]. Un ejemplo de la información que se puede encontrar a través de la interfaz web se muestra en la ***Figura 1-3***.

1.2 Redes Wi-Fi Empresariales

En los últimos 60 años, las empresas han logrado mejorar los niveles de productividad y la ventaja competitiva mediante el uso de la tecnología de la comunicación y la informática. La red de campus empresarial ha evolucionado en los últimos 30 años para convertirse en un elemento clave en esta infraestructura de computación y comunicación empresarial. Ante todo, ello, la experiencia del usuario en la red se ha convertido en un componente crítico y determinante del éxito o fracaso de los sistemas de tecnologías de información en todo campo.

Una red empresarial, corporativa o campus [4] se entiende como la parte de la infraestructura informática que proporciona acceso a los servicios y recursos de comunicación de red para usuarios finales y dispositivos distribuidos en una ubicación geográfica que puede abarcar un piso, edificio o un gran grupo de edificios distribuidos.

La red del campus consta de los elementos integrados que conforman el conjunto de servicios utilizados por un grupo de usuarios y dispositivos finales que comparten la misma infraestructura de comunicaciones de alta velocidad. Estos incluyen los servicios de transporte de paquetes (tanto cableados como inalámbricos), identificación y control de tráfico (seguridad y optimización de aplicaciones), monitoreo y gestión de tráfico, y administración y aprovisionamiento de sistemas en general.

Estas funciones básicas se implementan de manera tal que brinden y apoyen directamente los servicios de alto nivel proporcionados por la organización de TI para que los utilice la comunidad de usuarios finales. Estas funciones incluyen:

- Alta disponibilidad e ininterrupción de los servicios
- Servicios de acceso y movilidad
- Optimización de aplicaciones y protección de los servicios
- Virtualización
- Servicios de Seguridad
- Servicios de Gestión y soporte de las operaciones

Las redes Wi-Fi empresariales, por tanto, son la parte de la infraestructura responsable de brindar los servicios de acceso y movilidad a la organización. De hecho, es una de las principales razones por las que las redes Wi-Fi se han propagado como una epidemia tecnológica. Además, las corporaciones pueden aumentar la productividad si brindan a sus empleados la posibilidad de acceder a los recursos de la red de forma inalámbrica. [5]

1.2.1 Requerimientos de una red Wi-Fi Empresarial

Los fabricantes de tecnología inalámbrica líderes en el mercado mundial [5] coinciden en que las siguientes son algunas de las tareas claves que una red de clase empresarial debe manejar para poder garantizar un servicio de este nivel:

- Protección del acceso a la red: Identificación de puntos de acceso intrusos y usuarios no autorizados.

- Capacidad para extender servicios claves de la red fija como la telefonía o videoconferencia usando calidad de servicio para priorizar tráfico y garantizando una experiencia de movilidad transparente al usuario dentro de toda la zona de cobertura.

- Gestión del espectro de modo que la red tenga la inteligencia para seleccionar bandas de frecuencias menos congestionadas.

- Escalabilidad. Capacidad de gestión y administración centralizada de cientos o miles de puntos de acceso para facilitar el despliegue y mantenimiento de las redes.

- Seguridad Avanzada. Sistemas de prevención y detección de intrusiones.

1.2.2 Tráfico en tiempo real en una red empresarial

Las distintas aplicaciones de tiempo real que existen hoy en día y que son entregadas a través de una red Wi-Fi empresarial tienen una serie de beneficios [6] como:

- **Elimina la necesidad de utilizar la red celular:** Las llamadas de voz o video sobre IP pueden funcionar en una parte o en la totalidad de las organizaciones permitiendo el ahorro de costos al no usar los minutos de voz de la red celular.

- **Reduce la dependencia de cobertura de los proveedores de comunicación celular:** Las organizaciones pueden brindar una buena cobertura Wi-Fi en sus instalaciones para dar servicios de comunicación IP eliminando la necesidad de contar con cobertura móvil de los proveedores en lugares complicados (Sótanos, pisos elevados, almacenes, etc.)

- **Habilitación de dispositivos personales de los empleados o invitados:** Con el crecimiento en el mercado de celulares inteligentes y dispositivos inteligentes, aumenta también su presencia en las redes de las organizaciones. Este tipo de políticas se conocen como *Bring your own device (BYOD)* y una red preparada para recibir estos equipos personales tiene beneficios como:

    - Incrementar la satisfacción del empleado o invitado.
    - Incrementar la productividad cuando los dispositivos se habilitan para el uso de aplicaciones colaborativas.

- **Maximiza la disponibilidad y accesibilidad de los empleados móviles:** Al habilitar a los dispositivos móviles para la colaboración empresarial, se permite la comunicación con cualquier empleado en cualquier parte de la organización de manera instantánea y flexible logrando una mejor experiencia de trabajo.

En suma, las aplicaciones de tiempo real pueden ayudar a las empresas en lo siguiente:

- Reducir gastos en servicios de voz y datos de los proveedores móviles.
- Mejorar la productividad, accesibilidad y disponibilidad de los empleados.
- Aprovechar la mayor presencia de dispositivos móviles personales dentro de la empresa para colaboración y comunicación a menor costo o sin costo con las soluciones BYOD.
- Mejorar la satisfacción de los empleados cuando se involucran con herramientas de colaboración y otras aplicaciones comerciales de una manera flexible llevando a una experiencia de usuario de calidad.

1.3 Problemática del Roaming en las redes Wi-Fi

La capacidad de los dispositivos usuarios finales en una red Wi-Fi de hacer la transición de un punto de acceso a otro mientras mantiene la conectividad de la red para las aplicaciones de capa superior es conocida como roaming o itinerancia. Una analogía perfecta es la que se produce al utilizar un teléfono celular. Cuando se realiza una comunicación telefónica celular durante un viaje en automóvil, el teléfono celular se desplazará entre las torres de telefonía celular para permitir comunicaciones sin problemas y, con suerte, una conversación ininterrumpida. El roaming ininterrumpido entre los puntos de acceso permite la movilidad WLAN, que es el objetivo de la verdadera conexión y la red inalámbrica.

Como ya se revisó en el punto 1.2.2 garantizar un proceso de itinerancia transparente es fundamental para que las aplicaciones de tiempo real funcionen de manera óptima y no se degrade la experiencia de usuario. Sin embargo, los problemas empiezan a aparecer cuando el nivel de seguridad aumenta en la red. Las redes empresariales demandan niveles de seguridad altos [1] para dar protección a las aplicaciones e información que manejan en la organización y por ello muchas veces se implementan soluciones de autenticación por usuario. Esto introduce retraso en la comunicación ya que para acceder a la red se tiene que pasar por un protocolo de verificación de credenciales lo cual puede incluir en el proceso hacer consultas a un servidor centralizado en la red.

Los fabricantes en la actualidad ofrecen soluciones centralizadas que involucran un controlador como ente que gobierna los puntos de acceso de manera que esas consultas a los servidores de autenticación se tengan que realizar cada vez que ocurre un desplazamiento del usuario entre puntos de acceso distintos, sin embargo, a nivel de arquitectura esto representa un punto de falla total de la red inalámbrica en caso caiga el controlador [1]. Del mismo modo, también existen arquitecturas que trabajan con un punto de acceso como controlador de la red, sin embargo, esto eleva los requerimientos de hardware de los puntos de acceso. Por otro lado, la misma IEEE ha desarrollado un estándar para la itinerancia rápida en redes Wi-Fi, sin embargo, no es compatible con equipos que no cuenten con dicha actualización por lo que no ha sido desplegada universalmente como solución final al problema.

Por todo ello, garantizar el roaming en una red Wi-Fi empresarial, la cual demanda contar con protocolos de seguridad avanzados y heterogeneidad en los dispositivos, resulta en todo un reto de ingeniería ya que muchos de los componentes que intervienen en el proceso no están estandarizados [1].

1.4 Objetivos Generales

La presente tesis tiene por objetivo principal diseñar y validar un método que garantice un tiempo de roaming en capa 2 menor a 150 milisegundos de manera que no interrumpa las sesiones de datos de los usuarios.

Además, se diseñará un módulo de respaldo ante posibles pérdidas de paquetes durante el proceso de roaming y otro módulo de reconfiguración de la LAN al terminar el proceso de roaming.

1.5 Objetivos Específicos

- Comparar las técnicas de roaming rápido que se utilizan actualmente y evaluar sus puntos técnicos a favor y en contra en el despliegue de redes empresariales.

- Diseñar un método de roaming rápido que permita una reasociación en un tiempo menor a 150 ms y que permita una interoperabilidad entre terminales de distintos fabricantes sin necesidad de software adicional en dispositivos usuarios. Adicionalmente, integrar al diseño un módulo de respaldo para minimizar la pérdida de paquetes durante el roaming. *(UIT-T G114 - Anexo 1)*

- Implementar una red de prueba basada en APs TP-LINK WDR3600 con el firmware OpenWRT (*POSIX-compliant*) y un servidor de autenticación de código abierto (*FreeRadius)*. *(Mayor detalle del firmware OpenWRT se encontrará en el Anexo 7)*

- Validar los tiempos de roaming y la operatividad del método diseñado mediante pruebas de captura de paquetes en la red.

- Demostrar la escalabilidad del método mediante un análisis de consumo de recursos a nivel de hardware.

CAPITULO 2

SEGURIDAD EN REDES WI-FI EMPRESARIALES

En el presente capítulo se detallarán los componentes y requerimientos principales con los que debe contar una red Wi-Fi para garantizar seguridad a los usuarios o recursos con los que dispone. Luego se presentará un resumen histórico de cómo han ido evolucionando los protocolos y tecnologías de seguridad estandarizados, sus características, diferencias y qué requerimientos cubren. Finalmente, se analizan las fases de asociación a una red Wi-Fi con el estándar de seguridad vigente.

2.1 Amenazas de Seguridad en redes inalámbricas

Es conocido que las redes inalámbricas son más vulnerables que sus pares cableadas. Para poder transmitir y recibir información en una red cableada es necesario estar físicamente conectado a ella, lo cual provee un cierto grado de privacidad al limitar la recepción de la información solo a los equipos conectados a la red. Por el contrario, en una red inalámbrica basta con estar dentro del rango de cobertura para poder recibir y transmitir información. En [7] se mencionan algunos factores que contribuyen a los problemas de seguridad en las redes inalámbricas:

- **Canal:** Las transmisiones inalámbricas (A excepción del infrarrojo o laser) usualmente implican una comunicación *broadcast* lo cual facilita el espionaje e interferencias.

- **Movilidad:** En las comunicaciones inalámbricas las conexiones físicas se reemplazan por conexiones lógicas. Estas conexiones pueden ser interrumpidas cuando los dispositivos móviles se desplazan entre zonas de cobertura. Dada la naturaleza móvil de los dispositivos en este tipo de redes, garantizar procesos de asociación seguros es todo un reto.

- **Recursos:** Algunos dispositivos móviles como teléfonos inteligentes o tabletas tienen sistemas operativos sofisticados, pero memoria y recursos de procesamiento limitados para poder responder ante distintas amenazas como *DoS* y *malwares*.

- **Accesibilidad:** Algunos dispositivos inalámbricos como sensores o robots podrían ser desplegados en lugares remotos sin atención en los cuales se incrementa su vulnerabilidad a ataques físicos.

CATEGORÍA	DESCRIPCIÓN
Denial of Service (DoS)	Interrupción del acceso a la red. Se puede dar a nivel físico (DoS capa 1) con técnicas de *jamming* o a nivel de enlace (DoS capa 2) explotando las tramas de administración como la desasociación.
Eavesdropping / Traffic Analysis	Monitoreo pasivo de paquetes. Uso de criptología para descifrar información.
Man in the middle	Intercepción de la comunicación entre dos entes legítimos para obtener credenciales e información. En las WLANs se pueden lograr con Access Points intrusos que se hacen pasar por legítimos.
Masquerading / Spoofing	Acceso a recursos privilegiados suplantando identidad de usuarios legítimos

Tabla 2-1 Amenazas de Seguridad en una WLAN

Elaboración Propia

En la **Tabla 2-1** se resumen las distintas categorías en las que se agrupan las amenazas a las que una WLAN está expuesta. La mayoría de estas típicamente involucra a un atacante con acceso a la zona de cobertura del radioenlace entre un equipo usuario de la red y un punto de acceso o entre dos usuarios. La mayoría de estos ataques dependen de la habilidad del atacante de interceptar los mensajes e inyectar nuevos mensajes en la red. Esto se posibilita gracias a las diferencias entre las redes inalámbricas y cableas que se mencionaron al inicio del capítulo.

2.2 Requerimientos de Seguridad en WLAN Empresarial

Asegurar una red Wi-Fi Empresarial requiere típicamente de 5 componentes que se muestran en la ***Figura 2-1***. En primer lugar, ya que los datos son transmitidos a través de un medio no dedicado es necesario protegerlos con algún método de encriptación y así asegurar la ***confidencialidad*** de la información. Asimismo, dado que la red Wi-Fi sirve como portal de acceso a la infraestructura fija de la red, se requiere la ***autenticación, autorización y contabilización*** de accesos para que solo los usuarios legítimos puedan conectarse. Una vez autenticados los usuarios, se deben aplicar mecanismos de ***segmentación*** para limitar el uso de los recursos de la red en función a sus identidades y privilegios. Adicionalmente, los sistemas de detección/prevención de intrusos colaboran con la necesidad de ***monitorear*** constantemente la red para garantizar la disponibilidad de los recursos y protección frente a ataques. Finalmente, todos estos requerimientos deben ir acompañados de una política de seguridad clara y difundida en toda la organización, la cual es desarrollada por el equipo del oficial de seguridad de la información o director de seguridad de la información (En inglés CISO: Chief Information Security Officer) en organizaciones que desarrollan las buenas prácticas de estándares internacionales como la norma ISO 27001.

Figura 2-1 Requerimientos de una Red Wi-Fi Segura

Elaboración Propia

2.2.1 Confidencialidad

Dada las características de transmisión ya mencionadas de las redes inalámbricas, se hace obligatorio proteger la información y hacer que sea ilegible para algún tercero que pueda capturarla. Esto se logra utilizando alguna técnica de encriptación en las comunicaciones.

En la actualidad, los equipos certificados con Wi-Fi soportan el protocolo WPA2 el cual es el protocolo más seguro estandarizado por la IEEE. Este protocolo utiliza el algoritmo AES para cifrar los datos con claves temporales para hacer difícil romperlas. Adicionalmente, define dos métodos de autenticación: *Personal* (clave compartida) y *Enterprise* (credenciales por usuario), los cuales son explicados a detalle en la sección 2.5.3. En un entorno empresarial no se recomienda usar WPA2 Personal ya que puede comprometer la confidencialidad de las comunicaciones a pesar de utilizar AES como algoritmo de cifrado.

2.2.2 AAA

La "Autenticación, Autorización y Contabilidad" *(Authentication, Authorization and Accounting* – AAA, por sus iniciales en inglés) son una serie de servicios ejecutados por protocolos de seguridad para brindar protección a la red en distintos niveles explicados a continuación.

La **autenticación** es el proceso de validación de credenciales de los usuarios para poder hacer uso de la red. Algunos sistemas usan autenticación en varios pasos para aumentar el nivel de seguridad. Algunos ejemplos comunes de credenciales de autenticación presentes en las WLANs modernas son:

- Usuarios y contraseñas
- Certificados Digitales
- Claves Dinámicas (Por ejemplo, RSA SecurID)
- Tarjetas Inteligentes o credenciales almacenadas en dispositivos USB
- Claves Compartidas

Es importante mencionar que utilizar un método de autenticación robusto y muy seguro usualmente demanda un esfuerzo considerable de gestión que se traduce en mayores costos y finalmente incomoda más a los usuarios.

La **autorización** tiene que ver con la protección de los recursos de la red. Una vez que los usuarios han sido autenticados, se pueden definir distintos roles o tipos de usuarios para los cuales se tengan distintos privilegios y se use de manera más eficiente y segura la red.

La **contabilidad** hace referencia a la capacidad de la red de poder rastrear el trabajo de los usuarios dentro de la red ya sea por motivos de monitorear consumos o de seguridad (Hora de conexión y desconexión de usuarios).

En las WLANs, un servidor RADIUS es comúnmente la entidad responsable de las tareas descritas anteriormente. *Remote Authentication Dial - In User Service* (RADIUS) es un protocolo de red que provee capacidades de AAA para que las computadoras se conecten y hagan uso de los servicios de red.

Los mecanismos de autenticación y autorización del protocolo RADIUS son definidos en la RFC 2865 mientras que la contabilidad está definida en el RFC 2866. Es común encontrar que los fabricantes implementan servidores RADIUS directamente en sus APs autónomos y controladores WLAN. Esta característica es muy provechosa para las redes pequeñas y medianas que requieren un nivel de seguridad alto con infraestructura mínima.

El estándar IEEE 802.11 no obliga o especifica el usa de un servidor RADIUS. Sin embargo, especifica el uso del estándar IEEE 802.1X cuando para habilitar el nivel de seguridad Empresarial. Los servidores RADIUS en la práctica son uno de los principales componentes en el esquema de trabajo del 802.1X. La sección 2.5.2 describe con mayor profundidad las características del estándar IEEE 802.1X.

2.2.3 Segmentación

Una buena práctica de las redes fijas o cableadas es la de dividir o segmentar la red por grupos de usuarios con características o privilegios similares. Esto aplica también para las WLANs que sirven como portal de acceso a la red cableada. Existen APs en el mercado que pueden asociar distintos SSID a diferentes VLANs existentes en la red, así por ejemplo de puede tener en un campus una red Wi-Fi para invitados y otra para personal autorizado.

2.2.4 Monitoreo

Una vez diseñada y desplegada una red WLAN, es necesario monitorearla tanto para asegurar que tiene el rendimiento que se espera como para detectar ataques e intrusiones constantemente. Para monitorear las potenciales actividades maliciosas en la red se deben instalar equipos conocidos como *Wireless intrusión detection system* (WIDS) y *Wireless intrusión prevention system* (WIPS). Ambos son capaces de distinguir equipos legítimos e ilegítimos dentro de la red. Los WIPS adicionalmente permiten mitigar ataques de APs intrusos en la red impidiéndoles la transmisión dentro del área de la red.

2.2.5 Políticas

Asegurar una WLAN y monitorearla para contener amenazas es totalmente necesario en los ambientes empresariales. Sin embargo, ambos resultan no tan útiles si no se cuenta con una política clara y difundida en la organización. Educar a la organización en temas de seguridad previene que la red se vuelva vulnerable a ataques de hackers que utilizan la ingeniería social como arma. Por otro lado, existen también políticas de infraestructura TI en las empresas que pueden ser unas más complicadas de asegurar que otras. Por ejemplo, las políticas *Bring Your Own Device* (BYOD), implican que los usuarios empleen sus propios dispositivos para trabajar en la red (Por ejemplo, servicio de Wi-Fi a alumnos en una universidad). Desplegar mecanismos de autenticación robustos en un ambiente BYOD es un trabajo engorroso por el alto nivel de gestión de credenciales que ello conllevaría. Por otro lado, en un ambiente en donde solo se permita usar equipos propios de la empresa permite tener control sobre los mismos simplificando la labor de gestión y por ende aumentando la seguridad de la red.

2.3 Revisión del Estándar IEEE 802.11

Antes de continuar con el detalle de los mecanismos de seguridad definidos en el estándar, se hará una breve revisión de la arquitectura y el funcionamiento del IEEE 802.11.

2.3.1 Arquitectura del Protocolo 802.11

Como se había adelantado en el capítulo 1, el estándar IEEE 802.11 define mecanismos de comunicación inalámbrica en las dos capas inferiores del modelo OSI: Física (Capa 1) y enlace de datos (Capa 2).

A continuación, se revisará lo estipulado por el estándar con respecto a la capa 2 para las WLANs ya que es en donde se centra toda la investigación de la presente tesis.

La capa de enlace de datos del modelo OSI se divide en dos subcapas:

- *Logical Link Control* (LLC): Es la subcapa superior encargada del control de flujo de los paquetes de capa superiores hacia la subcapa inferior. Esta subcapa es idéntica para todas las tecnologías de redes LAN, aunque no todas la usan.

- *Medium Access Control* (MAC): Es la subcapa inferior que sirve de interfaz entre la capa física y la LLC. Es aquí donde el estándar agrega información relevante.

Cuando la red envía datos a la capa 2, la red es manipulada por la subcapa LLC y se convierte en lo que se conoce como *MAC Service Data Unit* **(MSDU).**
Una manera simple de definir una MSDU es la porción de datos que contiene el paquete IP (Capa 3) más algunos datos LLC.

Cuando la subcapa LLC envía el MSDU a la subcapa MAC, ésta le agrega cabeceras de información para poder identificarla. La MSDU entonces es encapsulada en lo que se conoce como *MAC Protocol Data Unit* **(MPDU).** A este nivel y de manera simple, un MPDU es lo que se conoce como trama 802.11 (*802.11 Frame*). La figura muestra un formato general de las tramas 802.11 o MPDU.

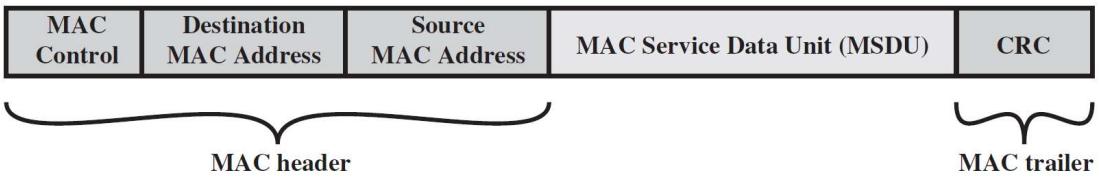


Figura 2-2 Trama 802.11 genérica - MPDU *[1]*

2.3.2 Arquitecturas de Red

El estándar 802.11 permite es despliegue de dos tipos de arquitecturas de red o dos modos de operación:

- **Ad-hoc**: En esta arquitectura se tienen estaciones (STA) capaces de comunicarse con otras basadas en un modelo de comunicación punto a punto (P2P). Un grupo de estaciones trabajando en modo Ad-hoc forma lo que se conoce como una *Independent Basic Service Set* **(IBSS).** La presente tesis no se enfoca en este tipo de arquitectura.

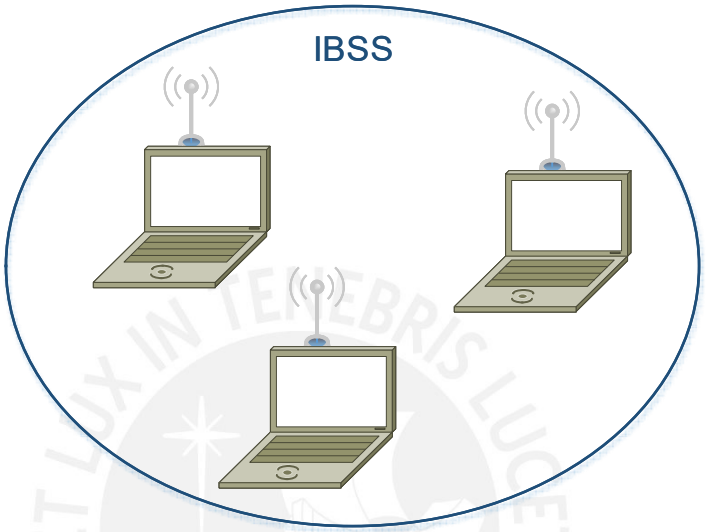


Figura 2-3 Modo Ad-Hoc

Elaboración Propia

- **Infraestructura:** En esta arquitectura las estaciones se comunican a través de puntos de acceso (APs). Los APs funcionan como puentes entre el medio inalámbrico y el cableado. Como tales, tienen al menos 2 interfaces de red: una inalámbrica que trabaja con IEEE802.11 y una segunda que conecta a la red cableada. Un grupo de estaciones asociadas a un AP específico forman lo que se conoce como un *Basic Service Set* **(BSS).** Por otro lado, un grupo de BSS conectados a través de un sistema de distribución **(DS)** forman un *Extended Service Set* **(ESS).** La presente tesis se enfoca en este tipo de arquitectura.

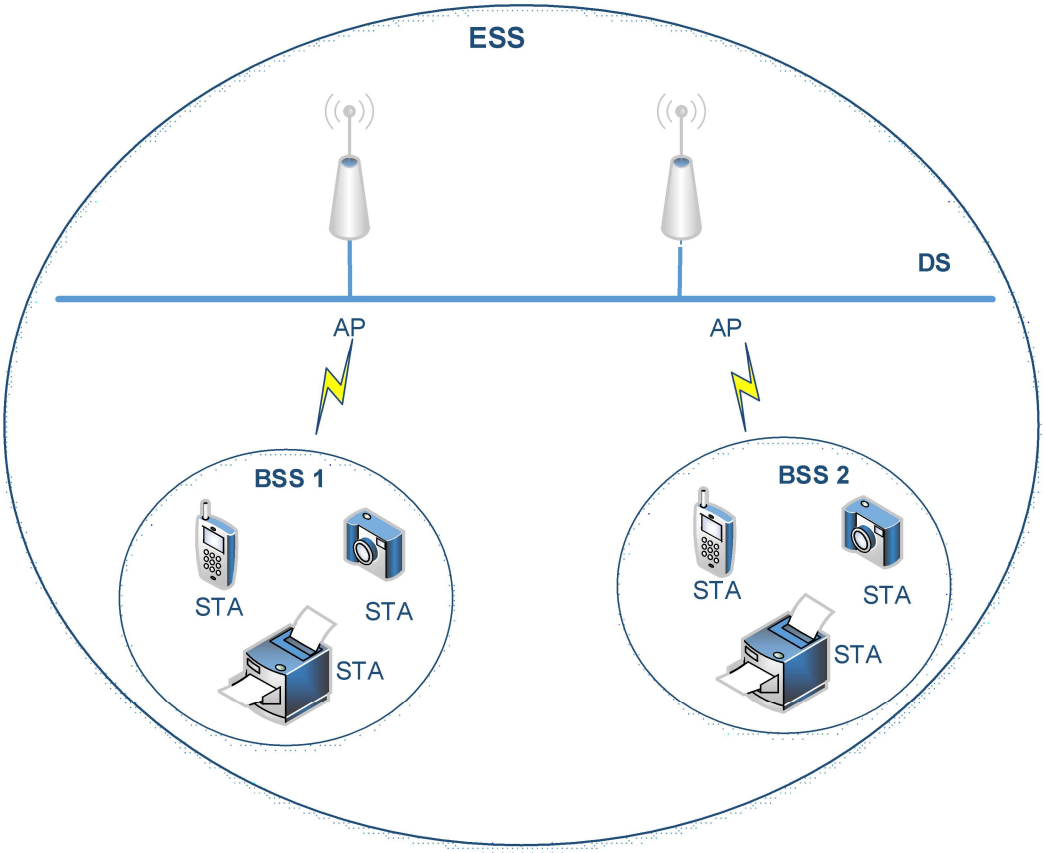


Figura 2-4 Modo Infraestructura

Elaboración Propia

2.3.3 Tipos de tramas 802.11

Las tramas 802.11 son distintas a las tramas utilizadas en los estándares para redes cableadas como el 802.3 (Ethernet), el cual solo usa un tipo de trama.

El estándar IEEE 802.11 define 3 tipos de tramas:

- **Tramas de Gestión *(Management frames)***

  Son usados por las estaciones inalámbricas para conectarse y desconectarse de un BSS. Estas tramas no son necesarias en una red cableada puesto que el conectar o desconectar físicamente el cable de red realiza esta función. Sin embargo, ya que las redes inalámbricas trabajan en un medio abierto, es necesario que las

estaciones primero encuentren una WLAN compatible para luego autenticarse a ella y finalmente asociarse para ganar acceso a la red cableada (DS).

Las tramas de gestión no llevan información de capas superiores, es decir, no existe MSDU encapsulado en el cuerpo de la MPDU. Lo único que transporta son *information fields* and *information elements.* Los primeros son campos de tamaño fijo obligatorios en el cuerpo de la trama mientras que los segundos son de tamaño variable y opcionales.

- **Tramas de Control *(Control frames)***

Ayudan con la entrega de las tramas de datos. Sirven para administrar y gestionar el uso del medio en la BSS según el mecanismo CSMA/CA definido en el estándar. Este mecanismo permite que solo una estación transmita a la vez compartiendo una serie de tramas de control con todas las estaciones para lograrlo, es por ello por lo que estas tramas deben transmitirse con la tasa de transmisión de bits más bajo soportado por la BSS. Al igual que las tramas de gestión no transportan información de capas superiores.

- **Trama de Datos *(Data Tramas)***

La mayoría de estas tramas transportan el MSDU que se recibe de los protocolos de capas superiores, es decir, la información relevante en sí. La MSDU normalmente se encripta por motivos de privacidad. Los otros dos tipos de tramas no se encriptan ya que no llevan MSDU, lo cual hace vulnerable al sistema a distintos ataques como denegación de servicio (DoS).

La ***Tabla 2-2*** muestra los subtipos que tienen cada uno de los 3 tipos de tramas del IEEE 802.11 [8]:

Management Frames	Control Frames	Data Frames
- Association request	- Power Save Poll (PS-Poll)	- Data (simple data frame)
- Association response	- Request to send (RTS)	- Null function (no MSDU payload)
- Reassociation request	- Clear to send (CTS)	- Data + CF-ACK
- Reassociation response	- Acknowledgment (ACK)	- Data + CF-Poll
- Probe request	- Contention Free-End (CF-End)	- Data + CF-ACK + CF-Poll
- Probe response	- CF-End + CF+ACK	- CF-ACK (no MSDU payload)
- Beacon	- Block ACK Request (BlockAckReq)	- CF-Poll (no MSDU payload)
- Disassociation	- Block ACK (BlockAck)	- CF-ACK + CF-Poll (no MSDU payload)
- Authentication		- QoS data
- Deauthentication		- QoS Null (no MSDU payload)
- Action		- QoS data + CF-ACK
- Announcement traffic indication message (ATIM)		- QoS data + CF-Poll
		- QoS data + CF-ACK + CF-Poll
		- QoS CF-Poll (no MSDU payload)
		- QoS CF-ACK + CF-Poll (no MSDU payload)

Tabla 2-2 Tipos de tramas 802.11 y subtipos

Elaboración Propia

2.4 IEEE 802.11i: La enmienda de seguridad

2.4.1 La necesidad de una red 802.11 más segura

Las diferencias entre las redes inalámbricas y las cableadas que se mencionaron en 2.1 sugieren la necesidad de mecanismos y servicios de seguridad robustos para las WLANs. El estándar 802.11 original ofrecía algunos mecanismos de seguridad que desafortunadamente contenían muchas vulnerabilidades que podían ser explotadas para perjudicar la autenticación, confidencialidad, integridad de datos y la disponibilidad de la WLAN. A continuación, algunos ejemplos de lo anterior:

- **Autenticación:** El estándar 802.11 original permitía el control de acceso mediante dos mecanismos: *Open System Authentication* y *Shared Key Authentication.* El primero no verificaba ninguna credencial por parte de los usuarios de modo que generalmente se usa en WLANs públicas. El segundo usaba un esquema de *challenge-*

response, pero presenta una serie de vulnerabilidades que permite ataques del tipo *man-in-the-middle.*

- **Confidencialidad:** El protocolo de encriptación que el 802.11 legacy usó se llama *Wired Equivalent Privacy* (WEP). Este protocolo fue "roto" en poco tiempo ya que usaba el mecanismo de cifrado RC4 y un vector de inicialización (IV) de 24 bits que resultaba muy pequeño para prevenir que se repitan en las tramas de datos de una WLAN ocupada. Esto permitía a los atacantes poder conseguir las claves de encriptación en minutos capturando el tráfico con herramientas de software no muy complejas.

- **Integridad de datos:** WEP usaba un algoritmo de comprobación de integridad de datos (*checksum)* simple para detectar errores en las transmisiones y lo protegía con un cifrado en cadena (*stream cipher)*. Desafortunadamente, este tipo de mecanismos de cifrado no ofrecen protección contra ataques de alteración de bits (*bit-flipping),* lo cual implicaba que en muchos casos un atacante podía alterar tanto la data como el correspondiente al algoritmo de comprobación de integridad de datos sin ser detectado.

- **Disponibilidad:** Los individuos sin acceso a una WLAN pueden afectar su disponibilidad mediante dos tipos de ataque: interferencia (*jamming)* e inundación *(flooding)*. El primero es un ataque de interferencia electromagnética al canal de transmisión de la WLAN para dejarla inutilizable. El segundo consiste en sobrecargar un AP enviándole un gran número de paquetes a altas velocidades de manera que se le impida procesar tráfico. El estándar IEEE 802.11 no ofrece defensa alguna ante estos tipos de ataques.

En el año 2001 se creó un grupo de trabajo dentro del 802.11 para estandarizar un mecanismo de seguridad robusto que resuelva las vulnerabilidades que tenía WEP. Sin embargo, el mercado no podía esperar

a la versión oficial de la IEEE por lo que la *Wi-Fi Alliance* en colaboración con distintas compañías desarrollaron el protocolo TKIP que contenía mejoras en la confidencialidad usando el mismo chip de cifrado que WEP (RC4) para evitar que los consumidores tuvieran que cambiar sus equipos. Este protocolo fue certificado por la *Wi-Fi Alliance* como WPA (*Wi-Fi protected Access*).

Finalmente, en el año 2004 se publica la versión oficial de la enmienda de seguridad del estándar llamada 802.11i la cual sigue vigente hasta la actualidad como mecanismo de seguridad robusta y es certificada por la *Wi-Fi Alliance* como WPA2.

Las especificaciones de la enmienda de seguridad son bastante complejas y ocupan 145 páginas del estándar IEEE 802.11 en su versión del 2012. En la siguiente sección se presentará una visión general de lo más importante.

2.4.2 Red de Seguridad Robusta (*Robust Security Network*)

El estándar IEEE 802.11i define los mecanismos y protocolos que debe usar una red para estar debidamente asegurada. Define una *Robust Security Network* (RSN) como una WLAN que permite la creación de únicamente asociaciones RSN (RSNA). Estas son relaciones de seguridad establecidas por el proceso conocido como *IEEE 802.11i 4-way Handshake*, el cual es detallado en 2.5.3.

Las bondades que brinda las RSNAs son las siguientes:

- Mecanismo de autenticación de usuarios mejorado
- Gestión de llaves de encriptación
- Confidencialidad de la información
- Autenticación de origen de la data e integridad
- Protección contra ataques de suplantación de identidad (*Replay Attack*)

La ***Figura 2-5*** muestra los protocolos y mecanismos que introduce la enmienda de seguridad en el estándar.

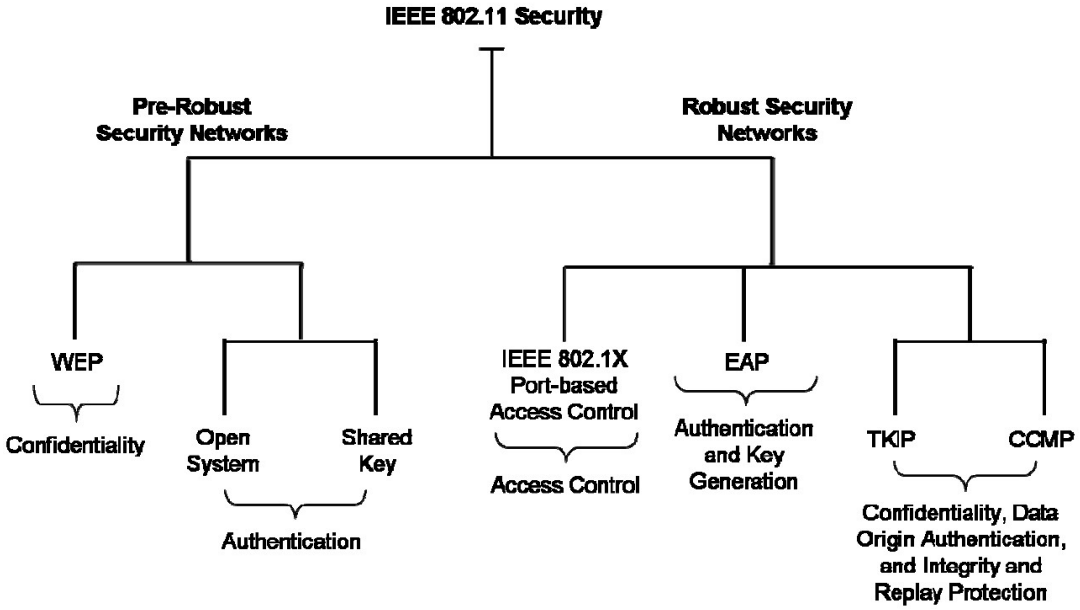


Figura 2-5 Protocolos y Mecanismos - 802.11i *[9]*

Las RSNAs usan varias llaves criptográficas para la encriptación, autenticación e integridad de datos. El estándar IEEE 802.11i define dos jerarquías de llave para las RSNAs: La *Pairwise Key Hierarchy,* diseñada para proteger el tráfico unicast y la *Group Key Hierarchy* para proteger tráfico multicast/broadcast.

Como se puede ver en la ***Figura 2-6*** las llaves raíces que encabezan la jerarquía representan las dos maneras en que dichas claves son instaladas en los equipos que soportan 802.11i.

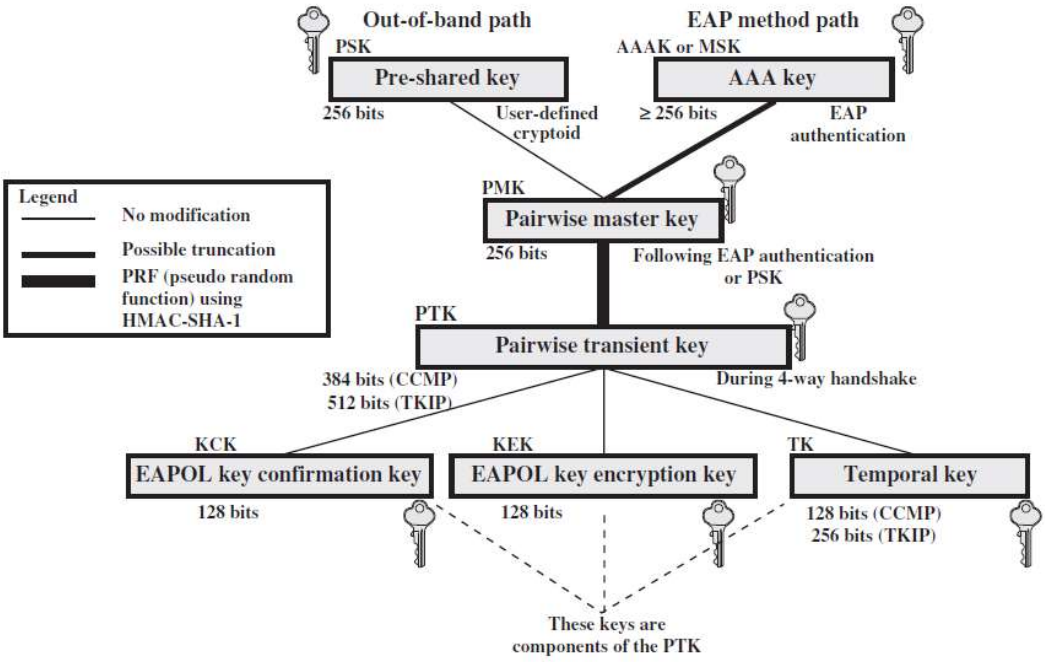


Figura 2-6 Pairwise Key Hierarchy - 802.11i *[10]*

- **Pre-Shared Key (PSK):** Es una llave estática que comparten todos los usuarios de la WLAN y que debe ser configurada en los equipos a través de un mecanismo fuera de banda. El estándar no especifica como las PSK tienen que ser generadas o distribuidas. En caso se use una PSK en hexadecimal, esta debe ser de 64 dígitos, lo cual es difícil de recordar para un usuario. Por ello, típicamente se usan frases secretas que deben ser de 6 a 63 dígitos alfanuméricos que con ayuda de una función HMAC-SHA1 se convierten en la llave *Pairwise Master Key* (PMK).

- **Authentication, Authorization, and Accounting Key:** La *AAA key* también conocida como *Master Session Key* (MSK) es entregada al usuario mediante el protocolo EAP de un servidor de autenticación cuando se trabaja con 802.1X lo cual implica que el sistema trabaja con una autenticación por usuario a diferencia de la PSK. Esto se detallará más profundamente en la sección 2.5.2.

Ya sea que se trabaje con una *PSK* o una llave *AAA*, ambas generan lo que se conoce como una *Pairwise Master Key* (PMK) la cual es una llave semilla que sirve de entrada al proceso de *4-way-handshake* para generar las llaves de encriptación (TK) finalmente. Este proceso se explica a detalle en la sección 2.5.3.

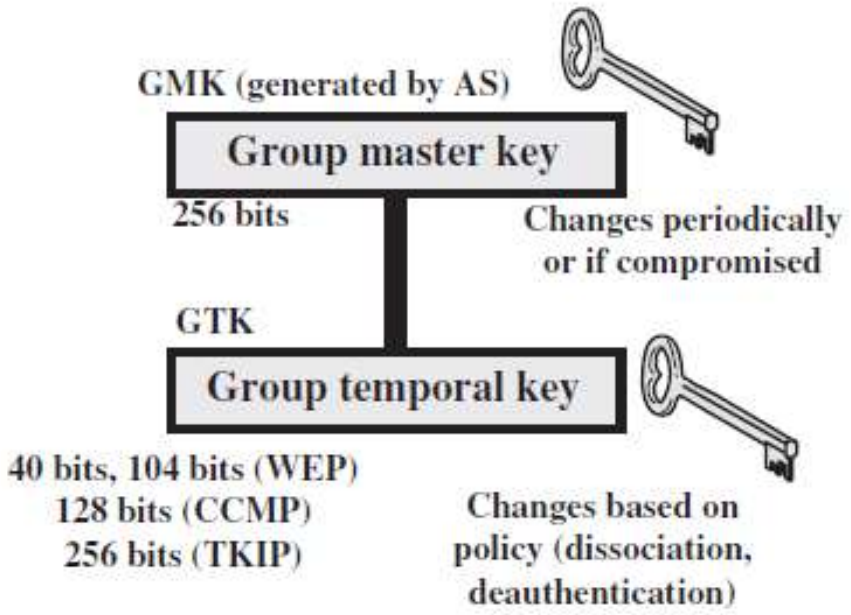


Figura 2-7 Group Key Hierarchy *[10]*

Por su parte, la *Group Key Hierarchy* consiste en una única llave de encriptación de tráfico multicast/broadcast llamado *Group Temporal Key (GTK).* A diferencia de la PMK que es generada con información tanto del suplicante como del autenticador, la GTK es generada directamente por el autenticador y derivada a las estaciones asociadas. El estándar no define un método para generar las GTK.

La tabla siguiente resume las llaves definidas en el estándar usadas por los protocolos de encriptación para la confidencialidad e integridad de datos.

Abbre-viation	Name	Description / Purpose	Size (bits)	Type
AAA Key	Authentication, Accounting, and Authorization Key	Used to derive the PMK. Used with the IEEE 802.1X authentication and key management approach. Same as MSK.	≥ 256	Key generation key, root key
PSK	Pre-Shared Key	Becomes the PMK in pre-shared key environments.	256	Key generation key, root key
PMK	Pairwise Master Key	Used with other inputs to derive the PTK.	256	Key generation key
GMK	Group Master Key	Used with other inputs to derive the GTK.	128	Key generation key
PTK	Pairwise Transient Key	Derived from the PMK. Comprises the EAPOL-KCK, EAPOL-KEK, and TK and (for TKIP) the MIC key.	512 (TKIP) 384 (CCMP)	Composite key
TK	Temporal Key	Used with TKIP or CCMP to provide confidentiality and integrity protection for unicast user traffic.	256 (TKIP) 128 (CCMP)	Traffic key
GTK	Group Temporal Key	Derived from the GMK. Used to provide confidentiality and integrity protection for multicast/broadcast user traffic.	256 (TKIP) 128 (CCMP) 40, 104 (WEP)	Traffic key
MIC Key	Message Integrity Code Key	Used by TKIP's Michael MIC to provide integrity protection of messages.	64	Message integrity key
EAPOL-KCK	EAPOL-Key Confirmation Key	Used to provide integrity protection for key material distributed during the 4-Way Handshake.	128	Message integrity key
EAPOL-KEK	EAPOL-Key Encryption Key	Used to ensure the confidentiality of the GTK and other key material in the 4-Way Handshake.	128	Traffic key / key encryption key
WEP Key	Wired Equivalent Privacy Key	Used with WEP.	40, 104	Traffic key

Tabla 2-3 Definiciones - Llaves de Encriptación según IEEE 802.11i *[9]*

El estándar IEEE 802.11i define dos protocolos para asegurar la confidencialidad e integridad de la información: *Temporal Key Integrity Protocol* (TKIP) y *Counter Mode with Cipher Block Chaining MAC Protocol* (CCMP).

TKIP fue desarrollado para permitir a los equipos del estándar 802.11 original resolver las numerosas vulnerabilidades que tenían con WEP. Su implementación requería una actualización del software de los equipos mas no algún cambio en hardware. Sin embargo, ya que TKIP usa RC4 y *Michael Message Integrity Code* (MIC), los cuales tienen vulnerabilidades conocidas, no se recomienda su uso en ambientes que requieran un alto nivel de seguridad.

Por otro lado, CCMP fue desarrollado sin la restricción de usar el hardware anterior (RC4). Es considerado la solución a largo plazo para la seguridad en WLANs. Es obligatorio su uso en un despliegue de RSN. CCMP está basado en CCM ([11]), un modo de cifrado por bloques autenticado genérico de AES [12]. CCM combina dos conocidas y comprobadas técnicas para lograr una seguridad robusta. Usa CTR para la confidencialidad y Cipher Block Chaining MAC (CBC-MAC) para proteger la autenticación e integridad de la información. CCMP protege la integridad tanto de las tramas de datos, así como de algunas partes de las cabeceras de las tramas 802.11.

2.4.3 Wi-Fi Personal vs Empresarial

La Wi-Fi Alliance certifica los mecanismos de seguridad de acuerdo con la ***Tabla 2-4 Certificaciones de Seguridad Wi-Fi Alliance*** . Como se puede observar WPA es el nombre con que se reconoce al mecanismo de TKIP/RC4 mientras que WPA 2 identifica a CCMP/AES. Ambos mecanismos tienen dos métodos de operación: Personal y Enterprise. Estos dos modos

Certificación Wi-Fi Alliance	802.11 Legacy	WPA		WPA 2	
		Personal	Enterprise	Personal	Enterprise
Método de Autenticación	Open System / Shared Key	PSK	802.1X /EAP	PSK	802.1X/EAP
Algoritmo Confidencialidad	WEP	TKIP	TKIP	CCMP	CCMP
Mecanismo de Cifrado	RC4	RC4	RC4	AES	AES
Tamaño de llaves	40 o 104 bits	128 bits (Encriptación)		128 bits (Encriptación e Integridad)	
		64 bits (Integridad)			
Mecanismo de Integridad	CRC -32	Michael MIC		CCM	
Protección de cabeceras	-	Direcciones MAC de origen y destino protegidas con MIC		Direcciones MAC de origen y destino protegidas con CCM	
Detección de *Replay*	-	Secuenciamiento de IV		Secuenciamiento de IV	

Tabla 2-4 Certificaciones de Seguridad Wi-Fi Alliance *[9]*

de operación hacen referencia al modo de autenticación. WPA/WPA2 Personal utilizan PSK como método de autenticación mientras que

WPA/WPA2 Enterprise utilizan 802.1X/EAP (Servidor de Autenticación). Es en este último método en el que la presente tesis se enfoca ya que es el más alto nivel de seguridad recomendado por el estándar.

2.5 Asociación a Red de Seguridad Robusta *(Robust Secure Network Association - RSNA)*

El proceso de asociación a una RSN es el primer objetivo de estudio de la presente tesis ya que, al proveer un alto nivel de seguridad, estos mecanismos tienen un impacto en el tiempo de asociación. Esto se explicará en el siguiente capítulo, sin embargo, una revisión profunda de los procesos involucrados es pertinente para poder sustentar el diseño de la solución que se busca en el presente trabajo de tesis.

En la ***Figura 2-8*** se puede observar un esquema genérico del proceso de RSNA en el cual se pueden observar las 3 etapas el proceso.

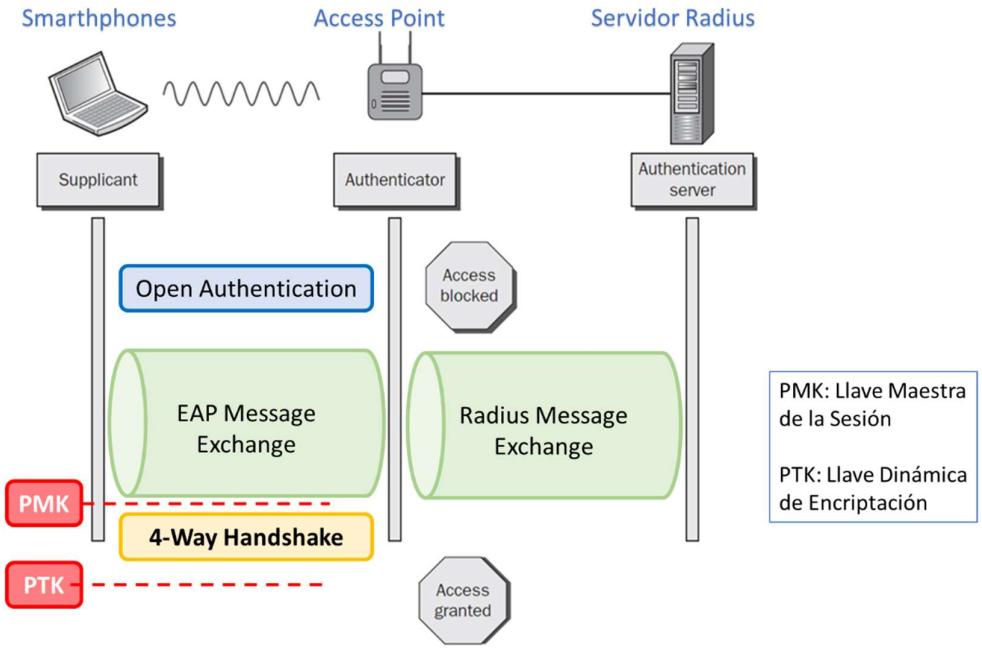


Figura 2-8 Autenticación a una RSN

Elaboración Propia

2.5.1 Sistema de Autenticación Abierta (*Open System Authentication*)

Una vez que una estación ha identificado una WLAN compatible con sus capacidades y cuenta con credenciales para acceder a ella empieza realizando un proceso que se llama *Open System Authentication*. Este proceso hereda su nombre porque fue definido como método default en el IEEE 802.11, sin embargo, tiene un nombre contradictorio ya que en verdad no realiza autenticación alguna. Este proceso sirve para establecer el radioenlace entre la estación y el punto de acceso (Equivalente a enchufar el cable a la red fija). Cuenta con 4 tramas que se muestran en la figura, las cuales llevan información sensible y relevante cuando se realizan los procesos de iteración que se explicarán en el próximo capítulo.

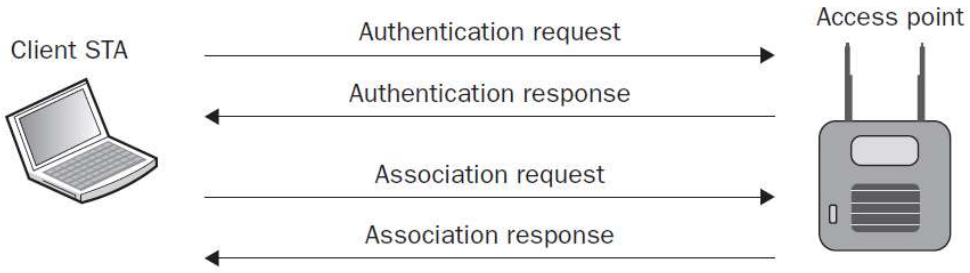


Figura 2-9 Open System Authentication *[8]*

2.5.2 802.1X / EAP

El IEEE 802.1X es un estándar anterior a las redes inalámbricas que define un control de acceso basado en puertos. Fue diseñado para usarse como marco de referencia *(framework)* de autenticación de las redes cableadas para bloquear todo tráfico de los puertos de acceso hasta que el usuario se autenticará contra un servidor especial. Este marco de referencia se halló completamente compatible con las WLANs ya que se cumple la misma lógica de que los usuarios solo pueden acceder a la red por un punto (Un puerto de un conmutador en redes cableadas y un puerto lógico en un AP en redes inalámbricas) y por lo tanto se propuso como método de autenticación en el estándar IEEE 802.11i.

A continuación, se presentan los elementos presentes en este marco de referencia *(framework)*.

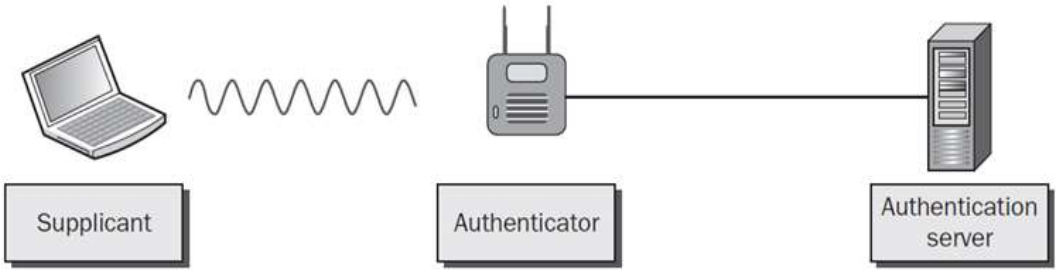


Figura 2-10 Dispositivos Participantes - 802.1X *[1]*

El suplicante viene a ser el usuario o cliente que quiere hacer uso de los recursos de la red. El autenticador tiene el rol de ser intermediario entre el suplicante y el servidor de autenticación. El autenticador bloquea toda comunicación de capa 3-7 de los usuarios que intenten asociarse a la red hasta que logren autenticarse con el servidor de autenticación. Finalmente,

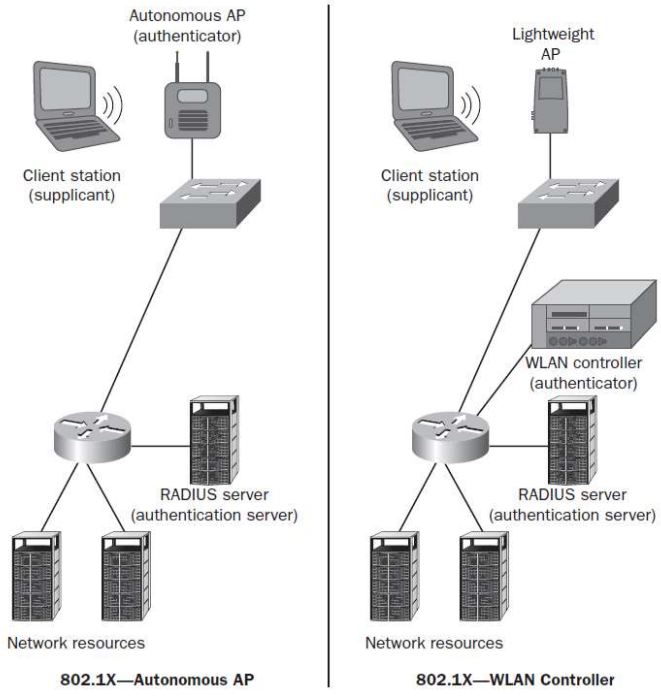


Figura 2-11 Arquitecturas 802.1X *[1]*

el servidor de autenticación es el responsable de validar las credenciales de los usuarios y comunicar al autenticador si debe o no darle el acceso a la red. El marco de referencia *(framework)* IEEE 802.1X define roles y no equipos directamente ya que por ejemplo en una arquitectura empresarial, un controlador WLAN puede comportarse como único autenticador de la red, como se observa en la ***Figura 2-11***.

IEEE 802.1X trabaja en conjunto con el protocolo EAP (RFC 2284) el cual es un protocolo de capa 2 que permite encapsular a los diversos mecanismos de autenticación que pueden ser usados con este marco de referencia *(framework)*. Adicionalmente, el servidor de autenticación típicamente usado es el RADIUS.

El protocolo EAP es muy flexible y permite transportar distintos mecanismos de autenticación con sus respectivas ventajas y desventajas. En la figura se presenta un cuadro comparativo de los distintos "sabores" de EAP. Dado que la presente tesis se enfoca en un entorno BYOD una restricción importante

	EAP-MD5	EAP-LEAP	EAP-TLS	EAP-TTLS	PEAPv0 (EAP-MSCHAPv2)	PEAPv0 (EAP-TLS)	PEAPv1 (EAP-GTC)	EAP-FAST
Security Solution	RFC-2284	Cisco proprietary	RFC-2716	IETF draft	IETF draft	IETF draft	IETF draft	IETF draft
Digital Certificates—Client	No	No	Yes	Optional	No	Yes	Optional	No
Digital Certificates—Server	No	No	Yes	Yes	Yes	Yes	Yes	No
Client Password Authentication	Yes	Yes	N/A	Yes	Yes	No	Yes	Yes
PACs—Client	No	No	No	No	No	No	No	Yes
PACs—Server	No	No	No	No	No	No	No	Yes
Credential Security	Weak	Weak (depends on password strength)	Strong	Strong	Strong	Strong	Strong	Strong (if Phase 0 is secure)
Encryption Key Management	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mutual Authentication	No	Debatable	Yes	Yes	Yes	Yes	Yes	Yes
Tunneled Authentication	No	No	Optional	Yes	Yes	Yes	Yes	Yes
Wi-Fi Alliance supported	No	No	Yes	Yes	Yes	No	Yes	Yes
Man-in-the-Middle Protection	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Dictionary Attack Resistance	No	No	Yes	Yes	Yes	N/A	Yes	Yes
Token support	No	No	Yes	Yes	No	Yes	Yes	Yes

Figura 2-12 Tipos de EAP *[1]*

es que se complica la posibilidad de usar certificados digitales en los suplicantes como credencial. Uno de los sabores que se encuentran ampliamente implementados en equipos móviles multipropósito como los teléfonos inteligentes o tabletas es el PEAP MSCHAPv2.

Tomando como referencia el método EAP/PEAP el suplicante, luego de haber realizado el proceso de *Open Authentication* pasará por los mensajes 3-17 de ***Figura 2-13 Proceso de Autenticación PEAP*** . En este método el servidor autenticador envía al suplicante un certificado digital con una llave pública con la cual se entabla un túnel TLS para asegurar el proceso de autenticación. PEAP MsCHAPv2 utiliza credenciales de usuario y contraseña las cuales se verifican a través de un proceso de *challenge reponse* dentro del túnel TLS. Si la autenticación resulta exitosa, el servidor de autenticación le envía la *AAA key* o MSK al suplicante a través de un *EAP success* (13) y una copia al autenticador mediante un paquete *RADIUS Access Accept* (16). Es en este momento que

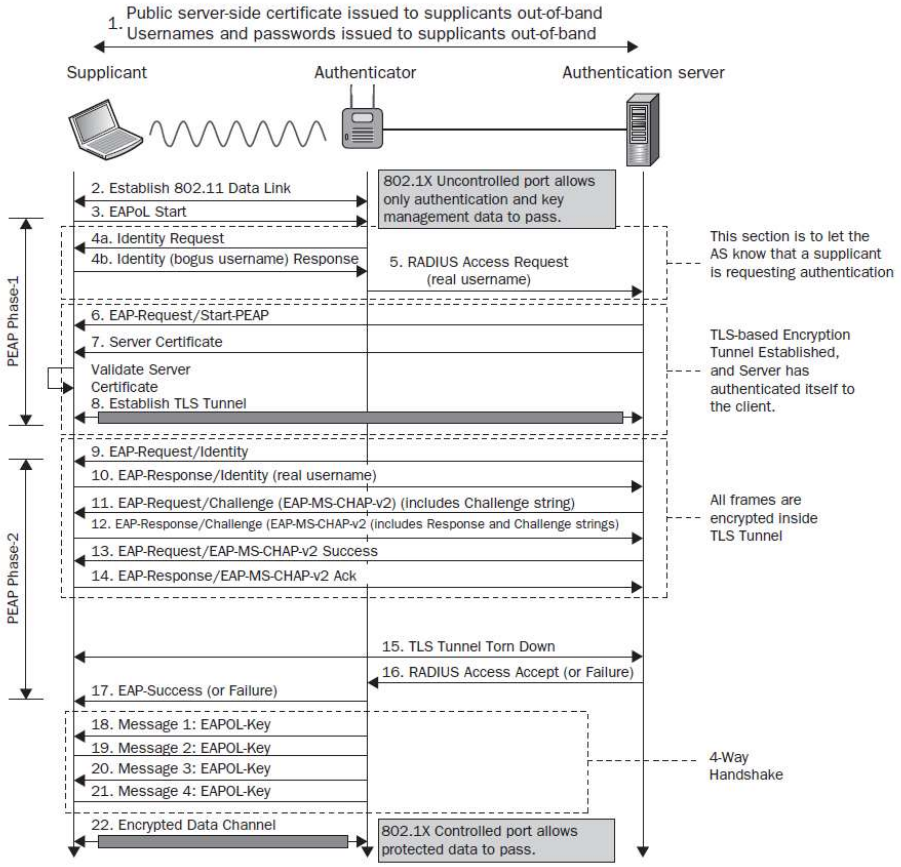


Figura 2-13 Proceso de Autenticación PEAP *[1]*

el suplicante y el autenticador tienen cada uno la PMK de la sesión que servirá para generar las llaves de encriptación en el siguiente proceso 4 way handshake.

2.5.3 4-Way Handshake

Una vez que el suplicante validó sus credenciales exitosamente frente al servidor de autenticación, tanto él como el autenticador tienen la PMK que servirá como semilla para generar las llaves de encriptación dinámicas. Esto se logra mediante un proceso llamado *4 way handshake* que implica una comunicación de 4 mensajes sin considerar los ACKs.

El objetivo final de este proceso es generar la PTK que servirá para encriptar la información. Esta PTK se obtiene con la fórmula indicada en la figura.

$$PTK = PRF\ (PMK + ANonce + SNonce + AA + SPA)$$

Ecuación 2-1 Función Pseudoaleatoria para generar la PTK

Se observa que la PTK es resultado de una función pseudoaleatoria que tiene 4 parámetros de entrada:

- **PMK:** Pairwise Master Key – Llave maestra de la sesión del suplicante.
- **ANonce:** Authenticator Nonce
- **SNonce:** Suplicant Nonce
- **AA:** Dirección MAC del Autenticador
- **SPA:** Dirección MAC del Suplicante

Los *Nonce* son números aleatorios generados por única vez en cada proceso de *4 way handshake*.

La figura muestra el proceso de *4 way handshake* que involucra los siguientes mensajes:

- **Mensaje 1:** El autenticador genera su *ANonce* y se lo envía al suplicante.

En este momento el suplicante genera su *SNonce* y ya tiene todos los parámetros necesarios para generar la PTK.

- **Mensaje 2:** El suplicante envía su *SNonce* en una trama en el que incluye un código MIC de integridad usando la llave KCK derivada de la PTK (***Figura 2-6 Pairwise Key Hierarchy - 802.11i***).

En este momento el autenticador cuenta con todos los parámetros necesarios para generar la misma PTK que el suplicante. Revisa el MIC con su propia llave KCK para verificar la integridad del mensaje 2.

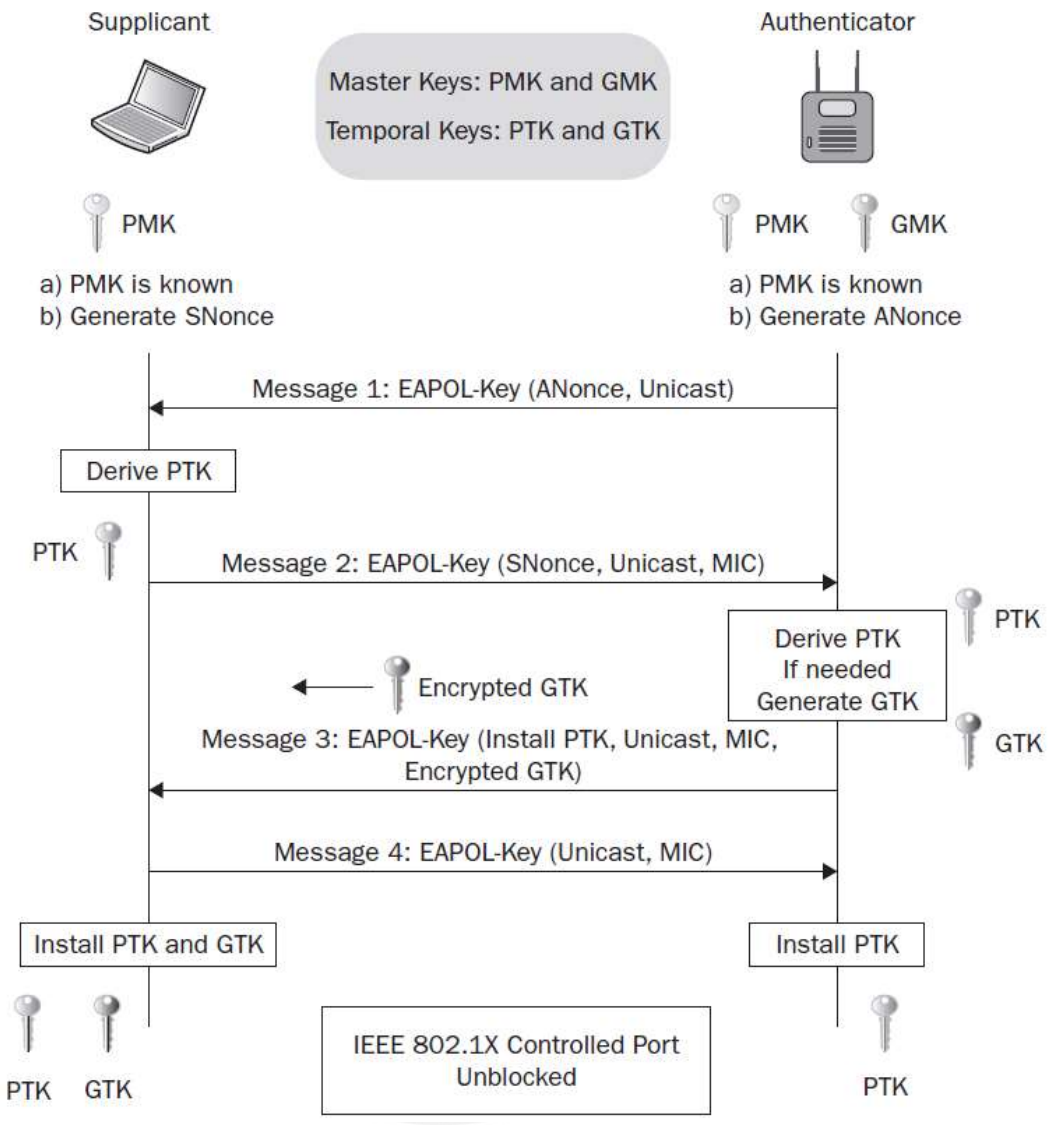


Figura 2-14 Proceso 4-Way Handshake *[8]*

- **Mensaje 3:** El Autenticador genera la GTK (***Figura 2-6 Pairwise Key Hierarchy - 802.11i***) y se la envía encriptada al suplicante usando la llave KEK (***Figura 2-7 Group Key Hierarchy***) de la misma manera incluye un MIC para la integridad.

El suplicante desencripta la GTK y la instala y se prepara para encriptar todo el tráfico con la llave TK.

- **Mensaje 4:** El suplicante confirma al Autenticador que ha instalado correctamente las llaves de encriptación y se prepara para transmitir sus tramas de datos.

Mayor detalle de la enmienda de seguridad 802.11i se encuentra en el Anexo 3.

CAPITULO 3

ROAMING EN REDES WI-FI EMPRESARIALES

Se han desarrollado mecanismos de rápida Roaming (*roaming rápido)*, como la PMKSA en Caché y la Preautenticación, estandarizados en el IEEE 802.11 que han dado como resultado la ratificación e inclusión de la enmienda 802.11r en el estándar IEEE 802.11-2012 acerca del *Fast BSS Transition*, que permite minimizar el delay ocasionado por el roaming. Además, existen otros métodos no estandarizados, pero de gran aceptación en el mercado, como el *Opportunistic Key Caching*. Sin embargo, los diferentes esfuerzos por presentar un esquema en el que se garantice una Roaming transparente se ven mermado por el software suplicante.

En el presente capítulo se describirá el proceso de Roaming de Capa 2, centrándose en la fase de ejecución, en el despliegue de una Red Robusta de Seguridad, así como también los entornos que buscan garantizar una Roaming transparente (*seamless roaming)*. Además, se realiza una comparativa entre los actuales métodos de Roaming Rápida y Segura (*Fast Secure Roaming - FSR*).

3.1 Proceso de Roaming

Las primeras versiones del estándar 802.11 reconocían al proceso de Roaming, también llamado *Roaming*, *Handoff* o *Handover, como* un proceso

de Capa 2 conocido como *servicio de reasociación*. Este servicio habilitaba la capacidad de transferir la asociación entre un *punto de acceso* (AP) y una estación móvil (*mobile station* - MS) de un AP a otro. Es decir, la reasociación permitía que un MS transite del área de cobertura de un AP, llamado *Basic Service Set* (BSS), a otro. Es por ello por lo que un nombre técnico que recibe el roaming es *BSS Transition* [8]. Sin embargo, hoy en día, el proceso de Roaming es más complejo con la inclusión de las subredes dentro de un entorno empresarial, se explica a continuación.

Una Roaming en capa 2 ocurre cuando el MS se mueve de un AP a otro AP que forma parte de la misma subred que el AP original [8]. La ***Figura 3-1 Tipos de*** muestra la transición que realiza el MS desde el AP A.1 al AP A.2 en la subred A. Este roaming de capa 2 también es conocido como Roaming Suave (*Soft Roaming).*

Un roaming en capa 3 ocurre cuando el MS migra del área de cobertura de una AP a otro que se encuentra fuera de la subred del primer AP. La ***Figura 3-1 Tipos de*** muestra la transición del MS desde el AP A.1 al AP B.1. A pesar de que el roaming es transparente en capa 2, estos APs se encuentran en subredes diferentes conectadas a través del router (subred A y subred B). En otras palabras, el MS perderá la conexión de capa 3 y deberá solicitar una nueva dirección IP a un servidor DHCP. En este punto, toda aplicación orientada a la conexión deberá ser reiniciada una vez restablecida la conectividad en capa 3 [8]. Este roaming de capa 3 es conocido también como Roaming Fuerte (*Hard Roaming).*

Para referencias posteriores en el presente documento, cuando se haga mención del roaming se debe entender que se trata de Roaming en capa 2.

El estándar 802.11 establece que un MS puede asociarse solo a un AP a la vez. Por lo que el MS, al momento de reasociarse entre los APs, debe atravesar tres fases: Fase de Detección, Fase de Selección y Fase de Ejecución [13]. La ***Figura 3-2*** muestra las diferentes fases que atraviesa el MS al realizar una Roaming a través de una *BSS*. Cada fase es definida por procedimientos independientes que introducen retardos en el proceso.

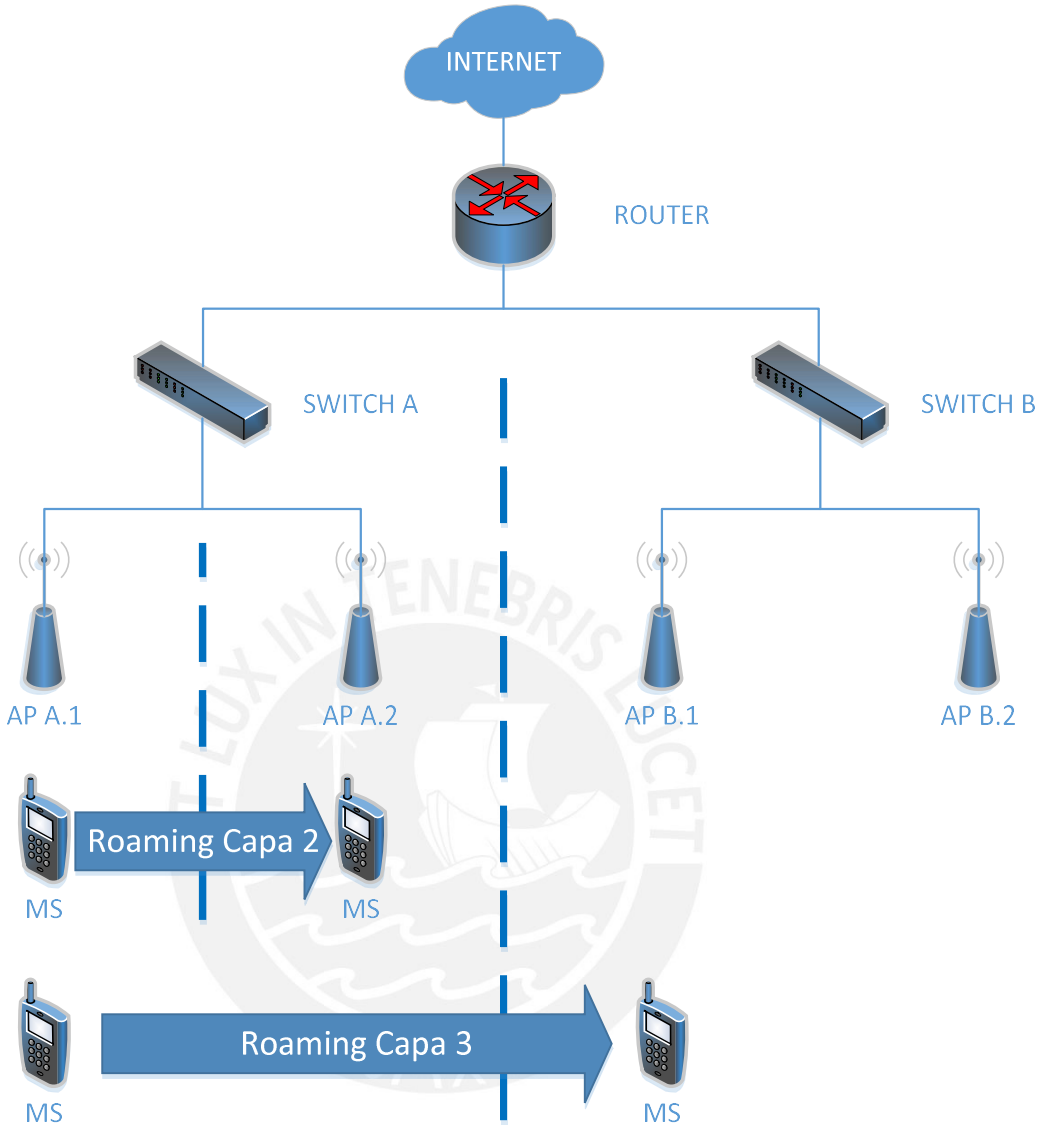


Figura 3-1 Tipos de Roaming

Elaboración Propia

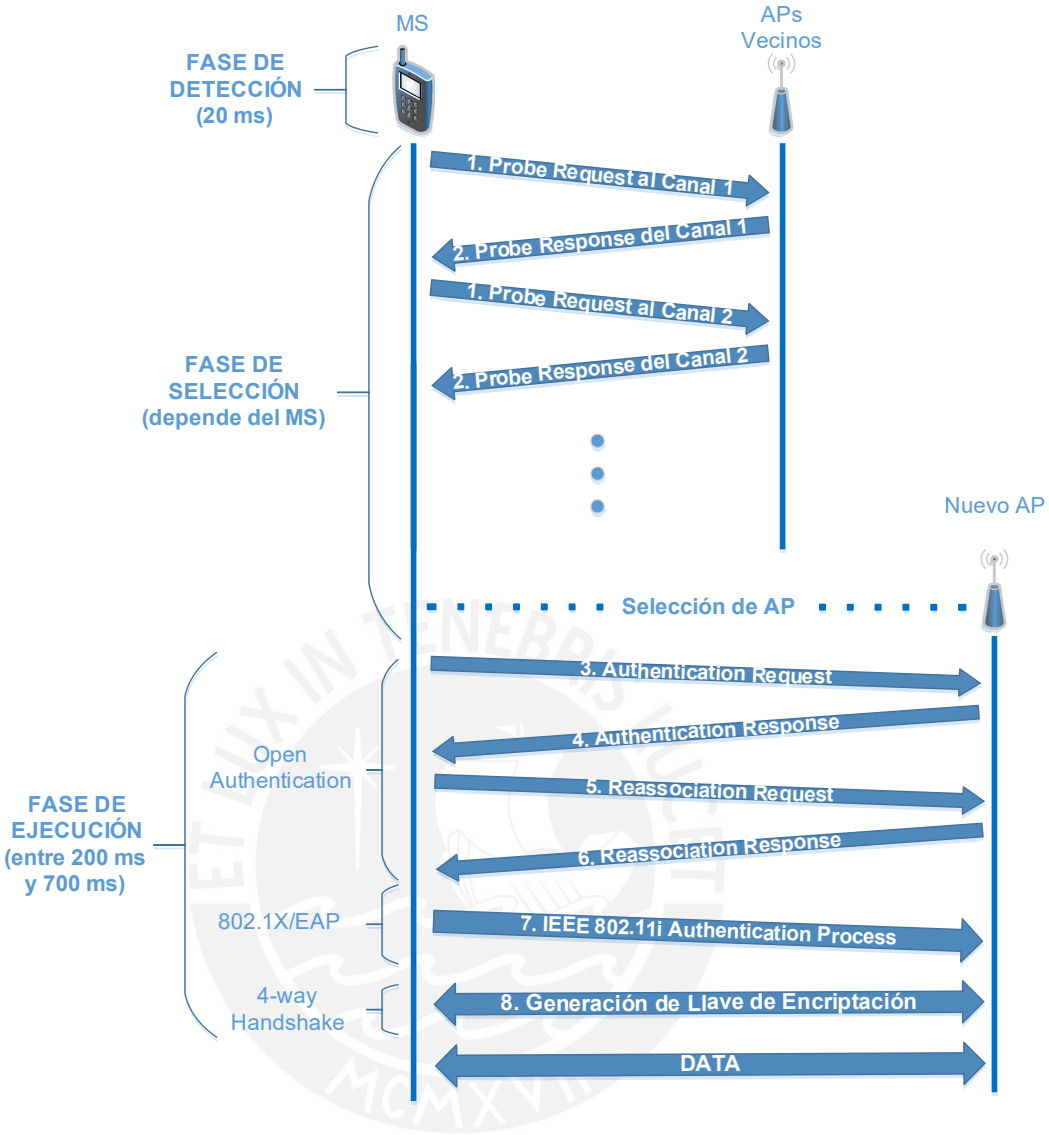


Figura 3-2 Proceso de Roaming en Capa 2

Elaboración Propia

3.1.1 Fase de Detección

El roaming inicia cuando el MS detecta, a través de diferentes técnicas, que la calidad de enlace esta debajo del umbral permitido. Esta etapa se conoce como Fase de Detección y no está estandarizada por la IEEE 802.11, sino que depende de los algoritmos de detección de Roaming que los propietarios coloquen en sus dispositivos [14]. Por ejemplo, el MS puede considerar como referencia un número consecutivo de *beacons* perdidos, número fallido de

retransmisiones, nivel de potencia, entre otros. Al finalizar esta fase, el MS se desasocia del antiguo AP.

3.1.2 Fase de Selección

Una vez que el MS decide que es momento de realizar un roaming, se inicia la Fase de Selección. En esta fase el MS escanea el medio en busca de APs candidatos a los cuales migrar. El MS escanea todos los canales 802.11 enviando mensajes *broadcast probe-request* y esperando los *probe-response* (***Figura 3-2 Proceso de Roaming en Capa 2***, mensajes 1 y 2). Durante el tiempo que toma el escaneo, no puede haber transmisión de datos. Una vez finalizado el escaneo, se debe escoger el AP óptimo al cual migrar. La selección se puede basar en la Relación Señal a Ruido (SNR por sus siglas en inglés) asociado a los *probe-response* de cada AP [15]. Se asume que la SNR del AP seleccionado debe estar, al menos, por encima del SNR del antiguo AP para evitar procesos innecesarios. Nuevamente, los algoritmos aplicados para seleccionar el AP óptimo no están estandarizados y son propios de cada *fabricante*. Por lo general, el MS intentará mantenerse en la misma red buscando un AP con el mismo *Service Set Identifier (SSID).* Si hay más de un AP identificado con el mismo *Basic Service Set Identifier* (BSSID), el MS tomará la decisión dependiendo del QoS, configuración de seguridad, etc. [1]

Se ha indicado, tanto en la fase de detección como en la de selección, que existen algoritmos que cada fabricante implementa en sus dispositivos móviles para dar inicio a el roaming y elegir un AP óptimo. A estos algoritmos se les llamará políticas o métricas.

En [16] se mencionan seis métricas que el MS puede utilizar. A continuación, se describen cuatro de esas métricas, ya que las otras son teóricas y no se ponen en práctica hoy en día:

- RSSI (*Received Signal Strength Indication*): El cliente se asocia al AP con mayor intensidad de señal, medida como el promedio exponencial de los RSSIs de los *beacon* recibidos.

- BRR (*Beacon Reception Ratio*): El MS se asocia al AP con la tasa de recepción de beacon más alta.
- *Sticky*: El MS no se desvincula del AP actual hasta la ausencia de conectividad durante un periodo de tiempo predefinido. Después de la disociación, el MS selecciona el AP con la intensidad de señal más alta.
- *History:* El MS se asocia con el AP que históricamente ha proporcionado el mejor rendimiento promedio en ese lugar. Este rendimiento se mide como la suma de las relaciones de recepción y el promedio se calcula con los datos recogidos en un tiempo previo (día anterior) en ese lugar.

En [17] se definen otras tres métricas para la decisión de realizar Roaming y la elección del mejor AP:

- MUB (*Maintain Until Broken*): Selecciona la señal del AP más fuerte y no realiza el roaming hasta que la actual conexión se pierde.
- ASS (*Always Strongest Signal*): Siempre se conecta al AP con la señal más fuerte.
- AWH (*Averaged with Hysteresis*): Utiliza una medida de tiempo de la intensidad de la señal y la histéresis para proteger la métrica anterior de las fluctuaciones del canal, lo que podría incurrir en Roaming frecuentes.

En general, existen diversos algoritmos que implementan los fabricantes en sus diferentes dispositivos móviles y al no estar estandarizados, escapan de la propuesta en el presente trabajo.

3.1.3 Fase de Ejecución

Una vez finalizada la Fase de Selección, se procede con la Fase de Ejecución, la cual consiste en tres etapas. La primera etapa es el *Open Authentication* (***Figura 3-2*** **Proceso de** , mensajes 3 y 4), la segunda es la autenticación *802.1X/EAP* (***Figura 3-2*** **Proceso de** , mensaje 7) y la tercera es el proceso *4-way Handshake* (***Figura 3-2*** **Proceso de** , mensaje 8). Estas tres etapas han sido explicadas en el capítulo previo de seguridad. Al finalizar

esta fase, el MS se ha asociado al nuevo AP y ambos han generado la llave de encriptación de la sesión (PTK) por lo que se puede retomar la transferencia de datos.

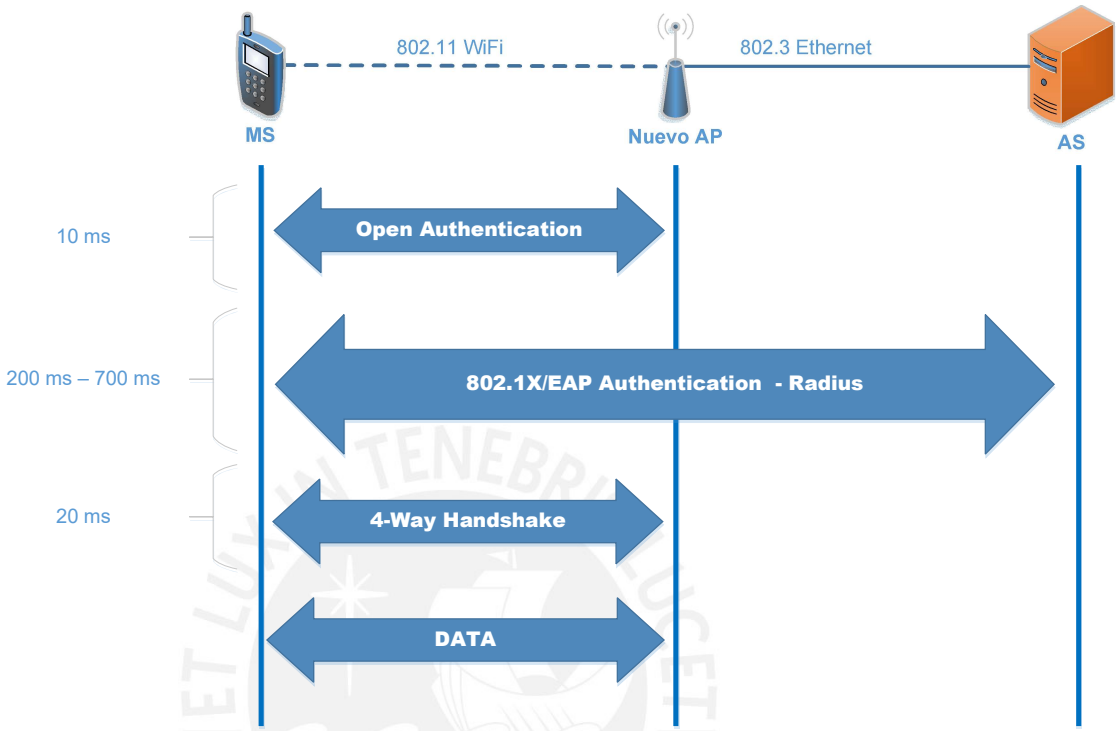


Figura 3-3 Retardos - Fase de Ejecución

Elaboración Propia

La ***Figura 3-3*** muestra las etapas de la fase de ejecución, por las que atraviesa el MS al realizar Roaming al nuevo AP, y los retardos que involucra cada una de ellas. La etapa que aporta con mayor retardo a esta fase es la Autenticación con el Servidor Autenticador. Dependiendo del método EAP, este retardo puede variar entre los 200 ms y los 700 ms [8], lo cual es inadmisible si se busca una Roaming transparente.

El presente trabajo solo se enfocará en disminuir el retardo producido por la fase de ejecución del proceso de Roaming. Por lo tanto, en posteriores menciones del término Roaming, se debe entender que se trata de la fase de ejecución de una Roaming en capa 2.

3.2 Arquitecturas para Implementaciones de Métodos de Roaming Rápidos

Considerando el estándar IEEE 802.11, en el proceso de Roaming en un entorno de seguridad alto, existen tres participantes: Suplicante, Autenticador y Servidor Autenticador. El Suplicante es el cliente móvil que se asocia a la red para utilizar sus recursos. El Autenticador es el ente con el que se comunica el Suplicante para solicitar autorización a acceder a los recursos de la red. Por último, el Servidor Autenticador es aquel dispositivo que verifica las credenciales del suplicante y garantiza su pertenencia o no a la red (servidor RADIUS).

El comportamiento del autenticador no está ligado a un dispositivo en concreto, sino que es aquel equipo que presente la inteligencia computacional para gestionar la sesión del suplicante. En este sentido, se presentan las arquitecturas que permiten la implementación de algún método

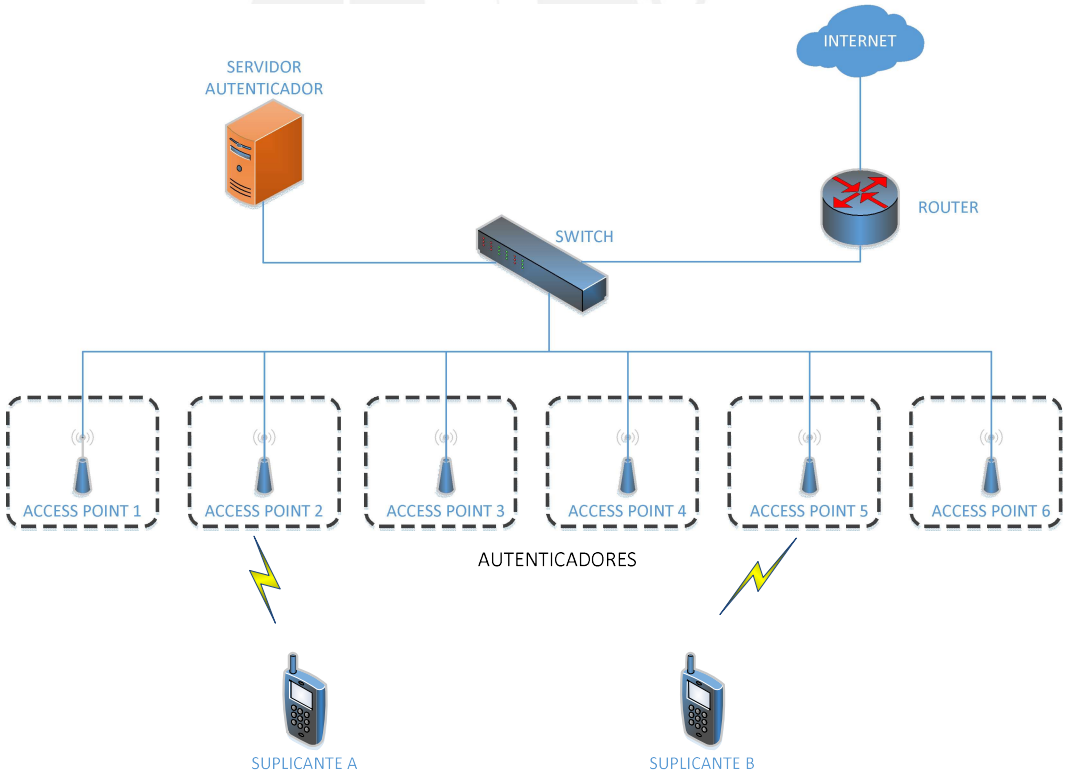


Figura 3-4 APs Autónomos como Autenticadores

Elaboración Propia

de FSR dependiendo de la ubicación del autenticador.

En la ***Figura 3-4*** se considera la arquitectura tradicional de APs autónomos. Cada AP es un ente independiente y cumple el rol de autenticador de la red. No existe comunicación entre APs para compartir información de los clientes por lo que cada vez que el cliente realice un roaming deberá autenticarse a la red. Es un esquema que no considera algún método de FSR en su solución, la cual es desplegada en un entorno empresarial mediano con equipos SOHO y no cubre las necesidades de movilidad de los usuarios dentro de su despliegue geográfico.

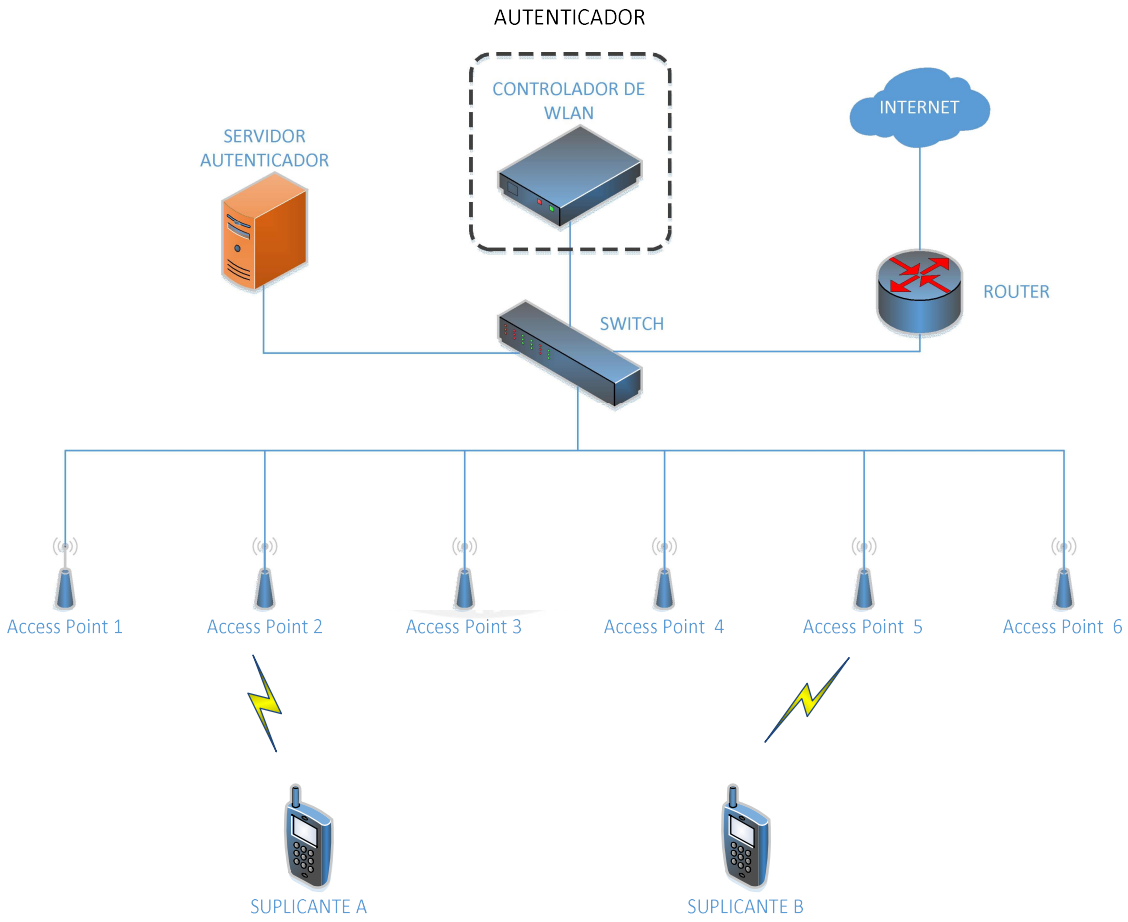


Figura 3-5 Controlador de APs como Autenticador

Elaboración Propia

La ***Figura 3-5*** muestra la arquitectura que considerable un Controlador de WLAN el cual brinda una gestión centralizada de los servicios de la capa de acceso inalámbrico. El controlador de WLAN también cumple el papel de autenticador y, bajo este esquema, la información de la sesión de cada cliente es almacenada y reenviada a criterio de este equipo. Esta arquitectura es la que más se adecúa al implementar una solución de FSR debido a que el autenticador tiene una visión general de la red y los puede gestionar de manera eficiente. Además, casi todas las soluciones FSR actuales son adaptables a esta arquitectura. Sin embargo, el controlador de WLAN es un equipo potente tanto en hardware como en software por las diferentes gestiones que maneja y los distintos algoritmos que resuelve, lo cual encarece el costo de su solución.

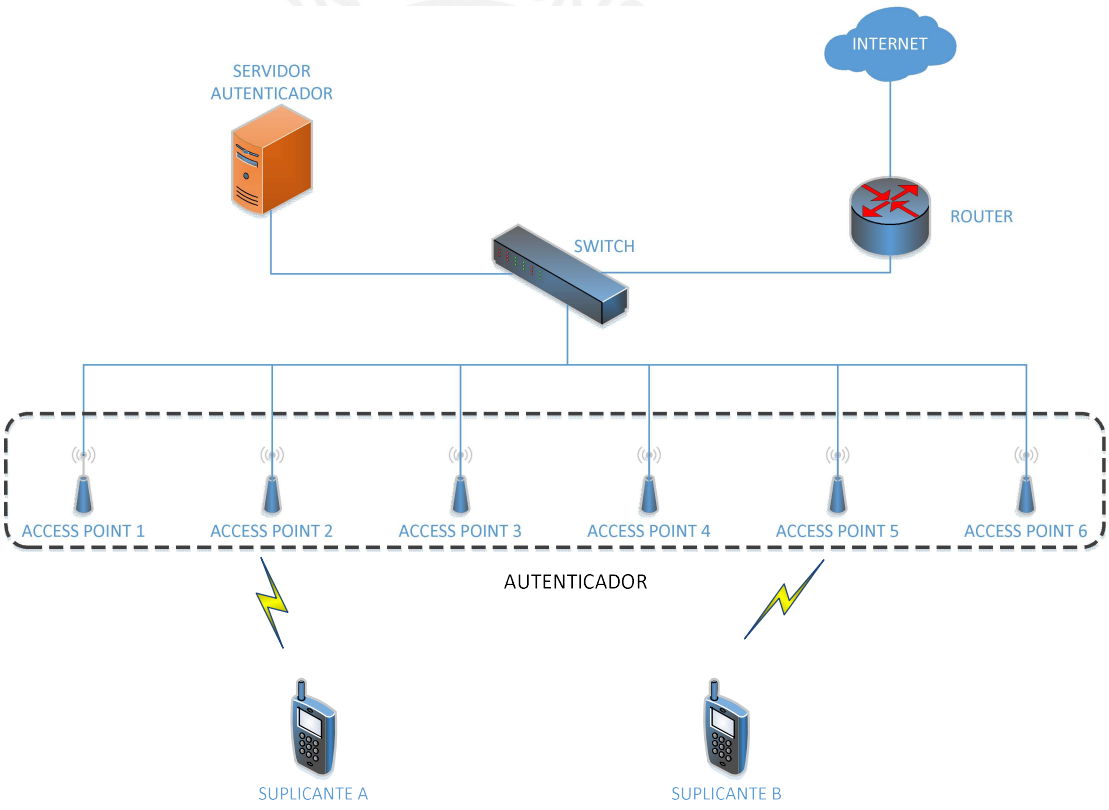


Figura 3-6 Clúster de APs como Autenticador (Sistema Distribuido)

Elaboración Propia

La ***Figura 3-6*** muestra un sistema distribuido en el cual el conjunto de APs funciona como un *clúster* autenticador. Bajo este esquema, un AP, a través de protocolos definidos, comunica la información de los usuarios de manera proactiva a los demás. De esta manera todos los APs comparten la misma información y se consideran un solo autenticador.

En la siguiente tabla, se muestra la comparación de las arquitecturas mencionadas:

	APs Autónomos	Controlador de WLAN	Cluster de APs (Sistema Distribuido)	Cluster de APs (Sistema Híbrido)
Capacidad de SW y HW en APs	ALTO	BAJO	ALTO	BAJO
Capacidad de SW y HW en Ente Externo	---	ALTO	---	BAJO
Control de la Red de Acceso	NINGUNO	CENTRALIZADO	NINGUNO	CENTRALIZADA LA GESTION DE LLAVES
Complejidad de Implementación	ALTO	BAJO	ALTO	INTERMEDIO
Costo de Implementación	BAJO	ALTO	INTERMEDIO	BAJO

Tabla 3-1 Comparación Arquitecturas de Sistemas de Roaming

Elaboración Propia

3.3 Autenticación Segura a través de la PMK

Al finalizar exitosamente la Autenticación 802.1X/EAP - Radius, se crea la *Pairwise Master Key* (PMK). Tanto la estación móvil, **suplicante**, como al *punto de acceso*, conocido como **autenticador**, se les hace llegar la PMK y se genera una asociación bidireccional de seguridad conocida como *Pairwise Master Key Security Association* (PMKSA) [8]. Como se ha explicado en el capítulo previo, la PMK es la semilla para generar la llave de encriptación dinámica (PTK), la cual es utilizada para encriptar y desencriptar el tráfico de un solo sentido (*unicast)* de la sesión.

En el Capítulo 2 se explicó que la enmienda 802.11i introduce el concepto de Red Robusta de Seguridad (RSN por sus siglas en inglés) para identificar una red que cumple con ciertos criterios de seguridad. La información del

RSN puede ser identificado en los campos de una trama de gestión 802.11 conocidos como *robust security network information element* (RSNIE). Esta información es compartida en cuatro diferentes tramas de gestión 802.11: *beacon management frames, probe response frames, Association request frames y reassociation request frames* [8]. En estas tramas se introduce un valor llamado *pairwise master key identifier* (PMKID) que es un único identificador para cada PMKSA que se haya establecido entre Suplicante y Autenticador.

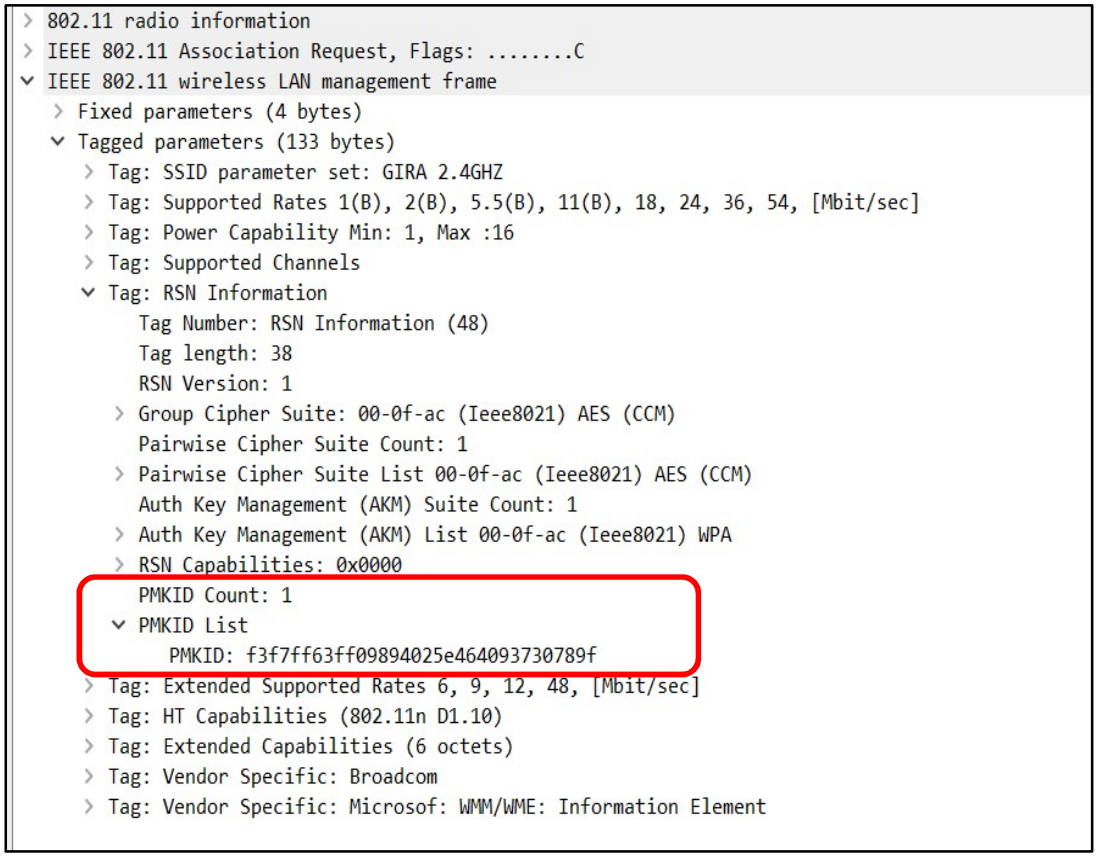


Figura 3-7 Información RSN y PMKID

Elaboración Propia

La PMKID solo se encuentra en el RSNIE en las tramas de *association request* y *reassociation request* que son enviadas desde el Suplicante al Autenticador. Se debe resaltar que, aun cuando la PMKID es un único identificador para una PMKSA, un suplicante puede establecer varios PMKSA. Es por ello que existe un campo “PMKID Count” que especifica el

número de PMKIDs que tiene guardado el suplicante. En la ***Figura 3-7 Información RSN y PMKID*** se observa que el suplicante ha guardado solo una PMKID.

Un error común es utilizar los términos de PMK y PMKSA como si denotasen la misma información. La PMK es la semilla para generar la PTK a través del 4-Way Handshake. La PMKSA está conformada por un conjunto de componentes, incluyendo la PMK, que se listan a continuación [8]:

- PMK – La llave maestra de la sesión
- PMKID – Identificador único de la sesión
- MAC Autenticador – La dirección MAC del Autenticador
- Tiempo de Sesión – Tiempo de vida de la PMK. Si no está predefinido, es infinito
- AKMP – Protocolos de autenticación y gestión de llaves

El estándar 802.11-2007 indica que el suplicante establece una PMKSA a través de una Reautenticación completa 802.1X/EAP-Radius. Además, el estándar define dos mecanismos de Roaming Rápida y Segura (*Fast Secure Roaming)* que son PMK en Caché y Preautenticación [8].

3.3.1 Reautenticación 802.1X/EAP Completa

La ***Figura 3-8*** muestra la creación de una PMKSA durante una reasociación utilizando la Autenticación 802.1X/EAP-Radius completa. En un primer momento, el suplicante se asocia a la red a través del AP Origen. La PMK 1 es enviada tanto al AP Origen como al suplicante para proceder con el 4-Way Handshake y generar la llave dinámica de encriptación (PTK).

Cuando el cliente decide realizar el roaming, se reautentica con el Servidor Autenticador a través del AP Destino. A través de esta nueva verificación de las credenciales del cliente, se genera una PMK 2 que es enviada al AP Destino y al suplicante. Esta PMK 2 es utilizada para generar una nueva PTK.

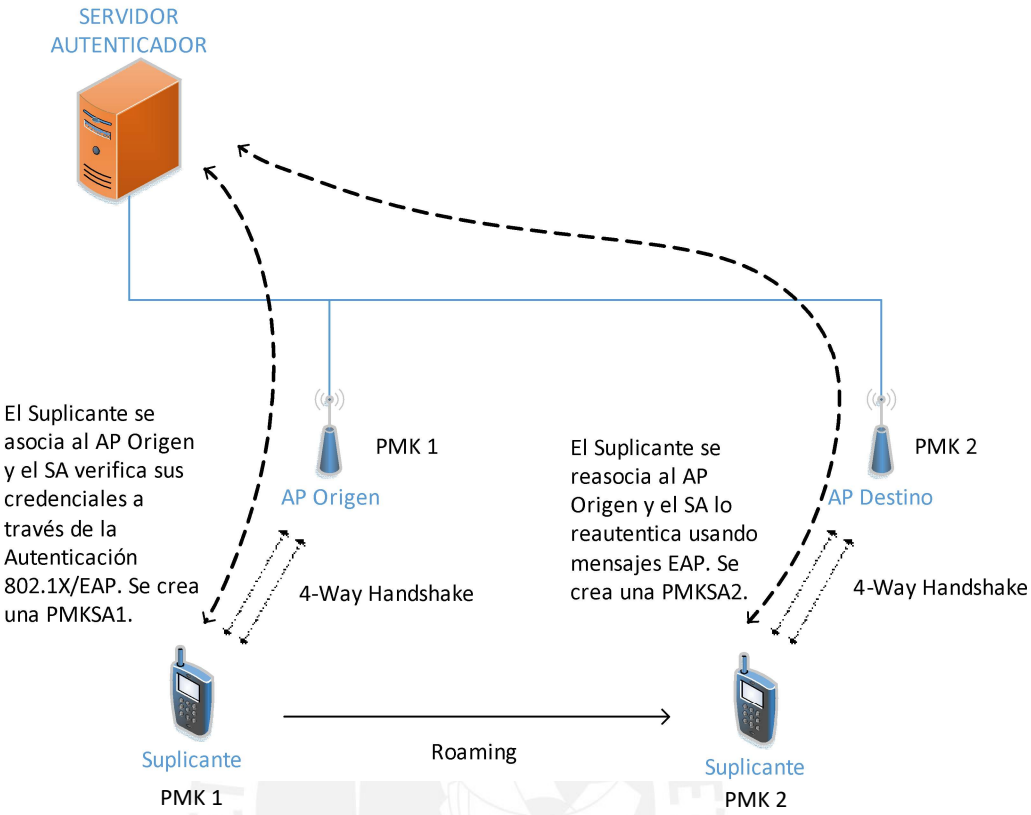


Figura 3-8 Roaming con Autenticación 802.1X/EAP - Radius Completa

Elaboración Propia

Bajo este esquema, en cada momento que el cliente decide realizar una Roaming será necesaria la intervención del Servidor Autenticador para verificar las credenciales del cliente a través de los mensajes EAP. A pesar de que se genera una asociación segura, PMKSA, el tiempo que conlleva la reasociación es significante. Es por ello por lo que el estándar define los mecanismos de FSR que se describen a continuación.

3.3.2 PMK en Caché

Este método permite a los APs y clientes mantener las PMKSAs por un periodo de tiempo mientras el cliente realiza el roaming y establece una nueva PMKSA con el AP Destino. Además, tanto el AP como el cliente

pueden guardar en caché varias PMK [8]. La ***Figura 3-9*** muestra un cliente que se ha asociado al AP Origen, por lo tanto, se ha generado una PMK 1. El cliente decidió realizar un roaming al AP Destino y se crea una PMK 2. Sin embargo, el AP Origen y el cliente han guardado la PMK 1. Por lo tanto, el cliente tiene en caché PMK 1 y PMK 2.

En cualquier momento que el cliente decide realizar el roaming al AP Origen, enviará en el mensaje *reassociation request* la lista de PMKIDs, informando al AP acerca de todas las PMKs que tiene guardadas en caché [8]. El estándar 802.11-2007 indica que se omite la autenticación 802.1X/EAP-Radius cuando un cliente realiza un roaming de retorno (*Roam Back*) al AP Origen, ya que ambos han guardado en caché la PMK 1 [8].

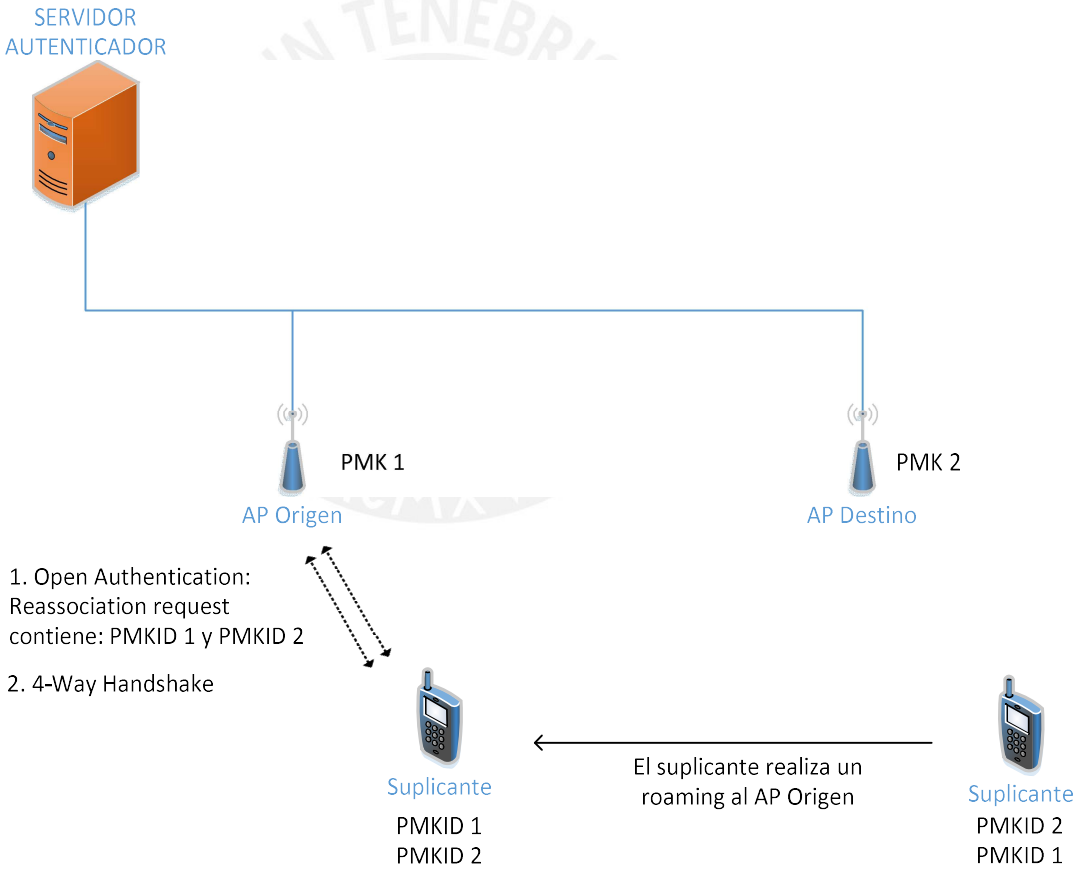


Figura 3-9 PMK en Caché

Elaboración Propia

El método PMK en Caché es también llamado el método de *Fast Roam Back*, ya que permite agilizar el proceso de roaming, pero solo con APs a los que se haya asociado previamente. En este sentido, cuando el cliente itera hacia un AP nuevo, tendrá que realizar una autenticación 802.1X/EAP completa.

3.3.3 Preautenticación

El mecanismo de Preautenticación permite al cliente establecer una nueva PMKSA previo a realizar el roaming al AP Destino. Es decir, permite al cliente iniciar una autenticación 802.1X/EAP-Radius con el AP Destino estando aun asociado al AP Origen [8]. La autenticación 802.1X/EAP completa es llevada a cabo a través del medio cableado con el propósito de mantener la sesión con el AP original mientras se prepara la conectividad con el AP destino.

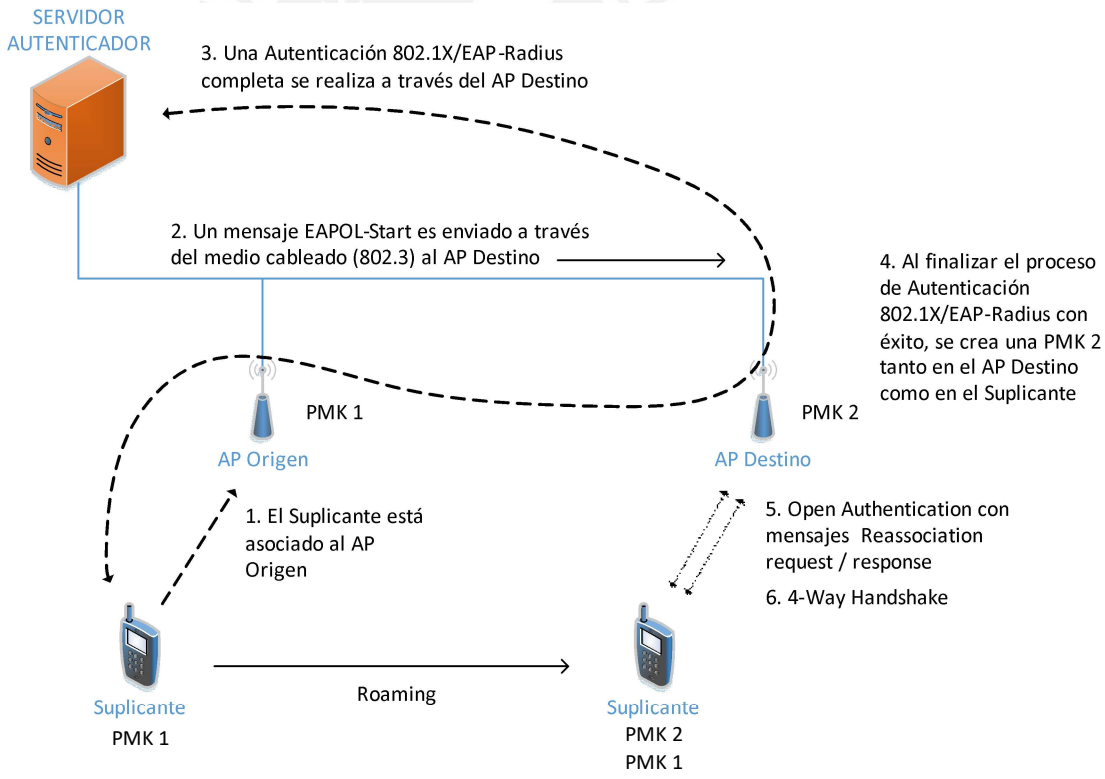


Figura 3-10 Preautenticación

Elaboración Propia

La ***Figura 3-10*** a un cliente asociado al AP Origen. El cliente envía un mensaje EAPOL-Start a través del primer AP al servidor autenticador y se inicia el de autenticación 802.1X/EAP-Radius. Una vez finalizado el proceso con éxito, se envía la PMK 2 al AP Destino como al suplicante. Si el cliente decide realizar el roaming al AP Destino, ya no será necesario reautenticarse y crear una nueva PMK ya que los dispositivos ya lo tienen guardado en caché, solo será necesario el 4-Way Handshake.

La información de a cuáles APs un cliente puede preautenticarse se encuentran en el RSN Information Element de los mensajes que envían los AP *probe response* o *beacon frames* [8].

A continuación, se presenta una comparación de los mecanismos de Roaming Rápida [8]. Como requisito primario por parte de los clientes, es necesario que soporten el estándar 802.11-2007 en el que incluyen el RSNIE.

	PMK en Caché	**Preautenticación**
Arquitectura WLAN	APs Autónomos	APs Autónomos / Controlador de WLAN
Retardo en Roaming	≈100 ms	≈ 20 ms
Modificación en Suplicante	Guarda en caché la PMKIDs de los APs a los que se	*Selección proactiva del AP Destino
Desventajas	Solo es útil en un roaming de retorno	Carga extra en el Servidor Autenticador por las

Tabla 3-2 Comparación de Mecanismos de Roaming rápido

Elaboración Propia

3.4 Métodos de Roaming Rápido y Seguro

Debido a que los mecanismos de Roaming Rápida definidos por la enmienda 802.11i, considerado dentro del estándar 802.11-2007, no cubrían completamente el requerimiento de escalabilidad en Roaming, se propusieron dos métodos integrales que son los vigentes a la fecha.

El primero es el Opportunistic Key Caching (OKC) que no es un método definido por la IEEE 802.11, sino que fue introducido al mercado debido a la ausencia de un método por parte del estándar. Posteriormente, el grupo de trabajo 802.11r presenta el método *Fast BSS Transition* el cual es ratificado y considerado parte del estándar desde el 2012.

Además, existen otros métodos de FSR como el *Cisco Centralized Key Management* (CCKM). Sin embargo, al ser soluciones propietarias patentadas, no se consideran en el presente documento.

3.4.1 Opportunistic Key Caching

Este método utiliza una arquitectura con Controlador de WLAN para la gestión de los APs. En este método se toma ventaja de una sola PMK compartida entre múltiples APs [1]. Bajo este esquema, el rol de autenticador lo cumple el Controlador de WLAN.

En la ***Figura 3-11*** se muestra el comportamiento de este método [1]:

(1) El cliente realiza una autenticación 802.1X/EAP-Radius para acceder a la red. La PMK 1 es enviada al cliente y al AP 1 y se genera la PTK a partir de esta llave maestra de sesión. Además, tanto AP 1 como cliente, generan la PMKID1 y la guardan en caché.

(2) A pesar de que la PMK fue creada a través del AP 1, el Controlador de WLAN la guarda en caché ya que este cumplirá el rol de autenticador. Es por ello por lo que, cuando el cliente decida realizar una Roaming al AP 2, el controlador de WLAN reenviará la PMK a ese AP.

(3) Cuando el cliente realice el roaming, calculará la nueva PMKID2. El cliente envía un mensaje de *reassociation request* al AP 2 con la PMKID2 en el RSNIE.

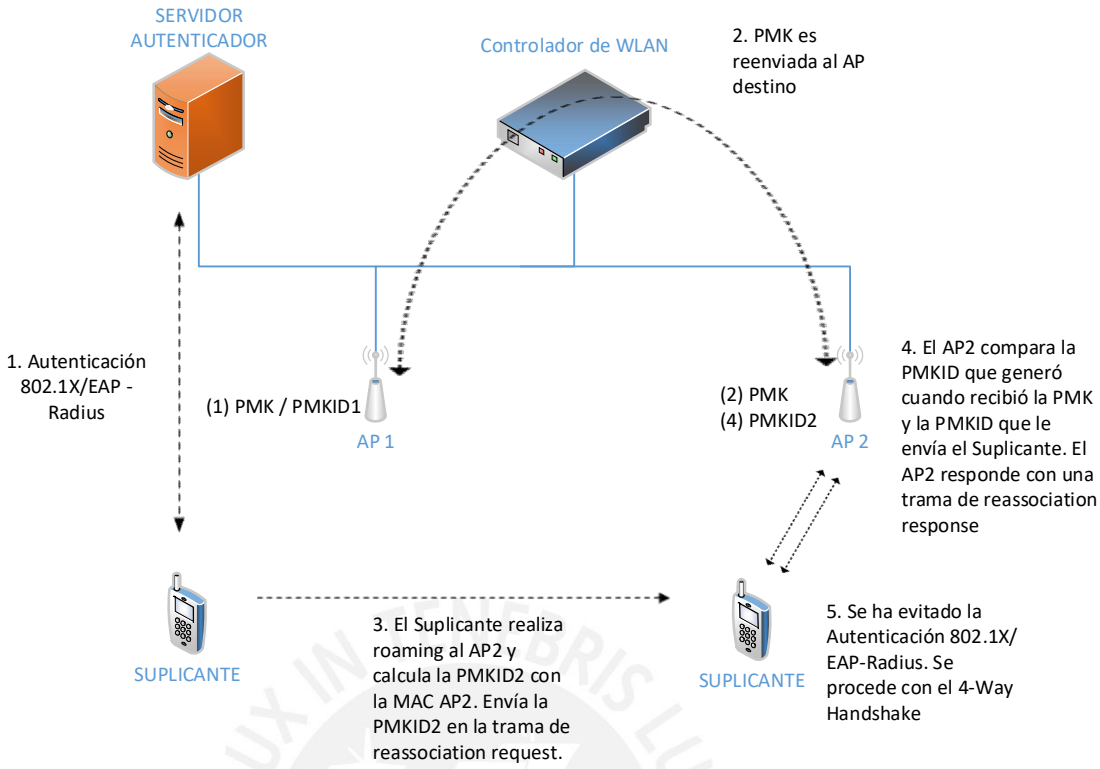


Figura 3-11 Opportunistic Key Caching

Elaboración Propia

(4) El AP 2 busca la dirección MAC del cliente al recibir el mensaje de *reassociation request* y calcula la PMKID2. En este momento, el AP 2 compara la PMKID2 que ha calculado y la enviada por el cliente. Si es una comparación exitosa, se procede con el paso (5). Caso contrario, se deberá realizar una autenticación completa. Tanto AP 2 como cliente siguen utilizando la PMK original.

(5) El proceso de autenticación 802.1X/EAP-Radius se ha omitido y se procede con el 4-Way Handshake.

El método OKC aprovecha la arquitectura centralizada con el Controlador de WLAN el cual permite gestionar los APs y la información de los usuarios de la red. Sin embargo, al no estar estandarizado, no hay una sola metodología de implementación. Es por ello por lo que este método podría ser implementado bajo la arquitectura de APs autónomos, considerando los

protocolos de comunicación entre ellos para compartir las llaves de sesión de los usuarios.

El estándar 802.11-2016 define la PMKID de la siguiente manera:

$$PMKID = Truncate\text{-}128(HMAC\text{-}SHA\text{-}1(PMK, \text{"PMK Name"} \,||\, AA \,||\, SPA))$$

Ecuación 3-1 Definición del Identificador de PMK (Anexo 2)

Donde AA es la dirección MAC del Autenticador. SPA es la dirección MAC del suplicante y PMK es la llave maestra de la sesión. Esta fórmula muestra que la PMKID es el resultado de una función hash donde se combina la PMK y las direcciones MAC del AP y del cliente [18].

3.4.2 Fast BSS Transition – 802.11r

La enmienda IEEE 802.11r-2008 fue ratificada el 15 de julio del 2008 como una extensión al estándar del 2007 y considerada parte del estándar 802.11-2012. Esta enmienda utiliza los mecanismos de Roaming rápida presentados en el estándar del 2007 (donde se considera al grupo de trabajo 802.11i como parte del estándar) para establecer un método conocido como *Fast BSS Transition* [1].

Esta enmienda establece al *Fast BSS Transition* como el movimiento de un *Station* (STA – cliente móvil) de un *Basic Service Set* (BSS – área de cobertura de un punto de acceso) a otro BSS dentro de un mismo *Extended Service Set* (ESS – el conjunto de varios BSS y sus correspondientes LAN) que minimiza el tiempo de conectividad que se pierde entre el STA y el *Distribution System* (DS – red que interconecta los BSS) [1].

El método propuesto por el grupo de trabajo 11r, cambia el esquema de autenticación establecida hasta ese momento por la fase de ejecución en el proceso de Roaming. Se reduce el número de mensajes compartidos en la última fase del proceso de Roaming con el objetivo de aminorar el tiempo que conlleva el proceso. Esta renovación de los mensajes de la fase de ejecución (protocolo IEEE 802.11r) se realiza sin perder el nivel de seguridad

robusto de la red. Se propone, a través de este método, una combinación eficiente entre los mensajes de *Open System Authentication* y *Reassociation* con los mensajes del proceso de *4-Way Handshake* [8]. La ***Figura 3-12*** muestra la secuencia de mensajes intercambiados entre el Suplicante y el Autenticador Destino, durante el proceso de Roaming, en el método de Transición Rápida (Fast Transition).

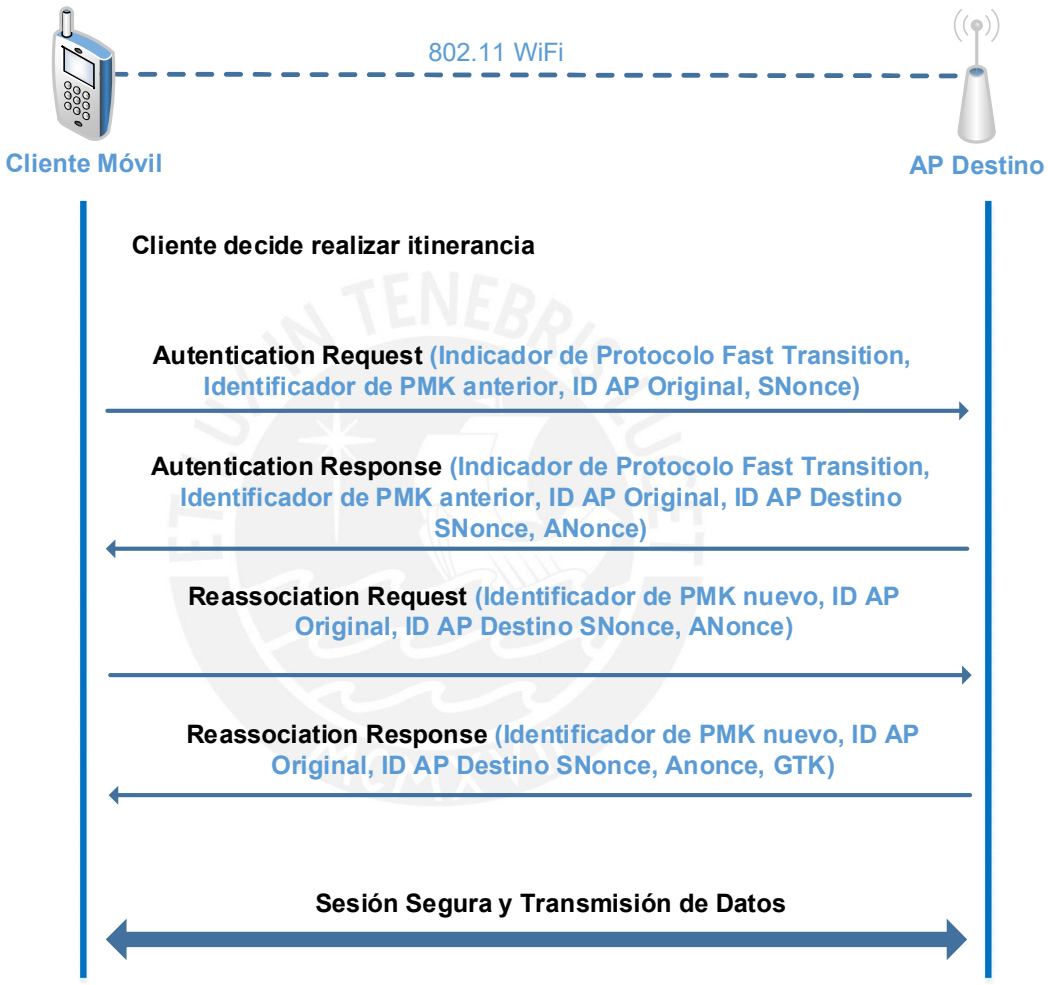


Figura 3-12 Mensajes de Autenticación y Reasociación Transición Rápida (*Fast Transition)* *[1]*

En el protocolo IEEE 802.11r, bajo la arquitectura de APs autónomos, el primer AP al que se autentica un STA almacenará en caché su PMK y lo utilizará para derivar claves de sesión para otros APs en el mismo *Mobility Domain* (Conjunto de BSS dentro de un mismo ESS). Este AP se denomina

titular de la clave R0 (R0KH) ya que contiene el PMK-R0, que simboliza el nivel 0 de la jerarquía de modificación PMK [19]. Este AP R0 bien podría ser un controlador de WLAN dentro del esquema de arquitectura centralizada.

Cuando una STA transita a un AP diferente, el R0KH derivará una PMK-R1, que es una nueva clave de sesión, de la PMK-R0, y la reenvía al nuevo AP. El nuevo AP se denomina el titular de la llave R1 (R1KH). El protocolo entre el STA y APs es un nuevo protocolo de nivel MAC definido por IEEE 802.11r [1]. El intercambio consiste en mensajes entre el AP Original y el STA, indicando el deseo de realizar el roaming, seguido de otro conjunto de mensajes entre el STA y el AP Destino para confirmar que se derivó la clave apropiada (PMK-R1) y que ha sido entregada satisfactoriamente. Este último grupo de mensajes sirve también para derivar la llave dinámica de encriptación. Con IEEE 802.11r, el AP inicial o controlador de WLAN actúa como autenticador, comunicándose con el servidor AAA. Después de eso, cada AP interactúa con el AP inicial o controlador de WLAN en lugar de hacerlo directamente con el servidor AAA [19].

La ***Figura 3-13*** detalla el proceso de roaming bajo el método Fast BSS Transition.

(1) Autenticación 802.1X/EAP – Radius completo entre el Suplicante y el Servidor Autenticador.
(2) Distribución de la llave maestra de la sesión (PMK) desde el servidor autenticador hacia el AP 1, llamado contenedor de la llave R0 (R0 Key Holder - R0KH), y al Suplicante.
(3) Proceso 4-Way Handshake ejecutado entre el Suplicante y el AP 1.
(4) El Suplicante decide realizar una Roaming hacia el AP 2. Solicita el proceso desde el AP 1 al AP 2 según el protocolo 802.11r.
(5) El AP 1 genera las llaves de sesión para el AP 2, llamado R1KH, y se las envía.
(6) El Suplicante completa el proceso de Roaming enviando los mensajes de reasociación según el protocolo 802.11r al AP 2 y generando las llaves dinámicas de encriptación.
(7) El Suplicante decide realizar un Roaming hacia el AP 2. Solicita el proceso desde el AP 2 al AP 3 según el protocolo 802.11r.

(8) El AP 2 solicita al AP 1 la generación de las llaves de sesión para el AP 3.

(9) El AP 1 envía las llaves de sesión al AP 3, llamado también R1KH.

(10) El Suplicante completa el proceso de Roaming enviando los mensajes de reasociación según el protocolo 802.11r al AP 3 y generando las llaves dinámicas de encriptación.

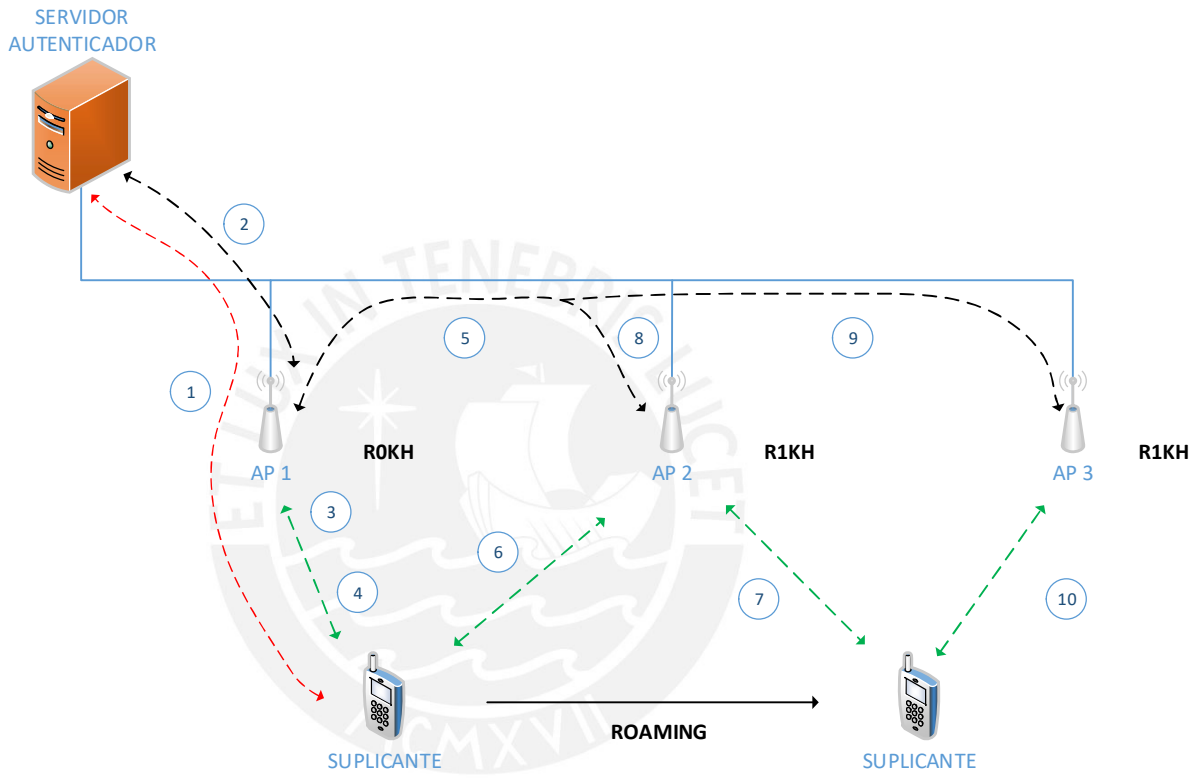


Figura 3-13 Fast BSS Transition

Elaboración Propia

El esquema mostrado en la ***Figura 3-13*** se desarrolla bajo una arquitectura distribuida, es decir APs autónomos. Al conectarse un cliente móvil a la red, el primer AP al que se asocia cumple la función de ente centralizado para gestionar las llaves de sesión del cliente con respecto a la red. Sin embargo, este método no restringe su implementación a una arquitectura distribuida, sino que puede ser implementada en un escenario con controlador de WLAN. En este caso, es el controlador quien gestionará las llaves de sesión de los clientes con cada AP de la red [8].

Además, el método *Fast BSS Transition* cuenta con dos modos de operación: *Over the Air* y *Over the DS*. El primer modo de operación, *Over the Air*, es en el cual la comunicación, durante la fase de ejecución del proceso de Roaming, Suplicante – AP Destino se desarrolla en su totalidad a través del medio inalámbrico. Por otro lado, el modo de operación *Over the DS* envía los mensajes de *Authentication request – response* a través del AP 1 y la LAN al AP 2, para realizar una Preautenticación en este último, mientras que los mensajes de Reassociation *request – response* son enviados a través del medio inalámbrico.

La ***Tabla 3-3*** muestra una comparación entre los métodos de Roaming Rápida y Segura mencionados. Se abarcan puntos como el retardo del proceso, promedio de pérdida de paquetes, impacto comercial del método y la complejidad de la implementación.

	OKC	Fast BSS Transition
Arquitectura WLAN	APs Autónomos / Controlador de WLAN	Controlador de WLAN
Retardo en Roaming	≈ 50 ms	Over the Air ≈ 50 ms Over the DS ≈ 20 ms
Pérdida de Paquetes Prom.	Sin data	0.2% (Over the Air)
Modificación en Suplicante	Implementación del método OKC	Implementación del estandar 802.11r
Aceptación Comercial	Ampliamente acogido por los fabricantes de dispositivos móviles	Muy pocos clientes soportan el método, de los cuales no soportan todos las técnicas del método
Soporte Clientes Legacy	Se conectan a la red pero sin la reducción de los retardos en el roaming	No soporta clientes legacy. Debe implementarse otra red alterna para su acceso
Implementación	Método no estandarizado. No hay un solo metodo de implementación y depende de cada vendor cómo lo haga. APs Autónomos - Complejidad ALTA Controlador de WLAN - Complejidad MEDIA	Método estandarizado por la IEEE. El estandar solo menciona roles de funcionamiento pero no cómo implementarse. Complejidad ALTA

Tabla 3-3 Comparación de los Métodos de Fast Secure Roaming

Elaboración Propia

3.5 Observaciones a los Métodos de Roaming Actuales

Luego de haber explicado el proceso de Roaming y los métodos actuales que pretenden disminuir su impacto en las sesiones de los clientes, se analizan factores que faltan resolver para lograr una Roaming transparente y las intenciones por resolverlos.

3.5.1 Dispositivos Clientes

Como se mencionó en la primera sección del presente capítulo, el comportamiento de los dispositivos clientes (teléfonos inteligentes, tabletas, laptops, etc.) no está estandarizado tanto en el umbral de decisión para realizar el roaming como en los algoritmos utilizados para seleccionar el próximo AP. Este factor es una barrera con la que los métodos de FSR actuales deben lidiar. Al no haber una homologación en este factor, no puede haber un método o sistema de FSR que considere todas las opciones de los dispositivos clientes.

La enmienda 802.11k define mecanismos de medición de recursos de radio (RRM por sus siglas en inglés) que permite que las radios compatibles con 802.11k comprendan mejor el entorno RF en el que existen [8]. Si una radio 802.11 no está transmitiendo, puede evaluar el entorno RF y el rendimiento del enlace de radio mientras está escuchando. Las mediciones de recursos de radio pueden ser realizadas por un AP o un dispositivo cliente. Las mediciones pueden tomarse localmente o pueden solicitarse y obtenerse de otro cliente o AP. Los datos de RRM se pueden poner a disposición de las capas superiores del protocolo, donde pueden utilizarse para una serie de aplicaciones, como VoIP [8]. Los dispositivos clientes aún seguirán tomando la decisión realizar o no el roaming. Sin embargo, los informes de dispositivos vecinos proporcionarán información adicional para que puedan tomar mejores decisiones de Roaming.

Así como el grupo de trabajo “k”, el grupo de trabajo “v” pretende permitir a los dispositivos clientes intercambiar información sobre la topología de la red, incluida la información sobre el entorno RF, haciendo que cada cliente sea tenga más información de su medio, facilitando la gestión general de la red inalámbrica.

3.5.2 Interoperabilidad

Una consecuencia de no conseguir una homologación de comportamiento por parte de los dispositivos clientes es que estos no puedan operar de manera eficaz, en cuanto a roaming se trate, entre soluciones de diferentes vendors. La certificación *Wi-Fi Voice-Enterprise* pretende otorgar esa compatibilidad tanto en dispositivos clientes como en la infraestructura de la red con APs [8]. Este certificado es opcional al certificado básico 802.11 y brinda el marco de trabajo (*framework)* adecuado para que los dispositivos clientes puedan operar de manera adecuada entre diferentes soluciones WLAN.

La certificación *Wi-Fi Voice-Enterprise* en conjunto con el estándar 802.11r formarían el escenario adecuado para lograr un roaming transparente. Sin embargo, no ha habido una aceptación masiva por parte de los fabricantes como se esperaba. Luego de cinco años que ambas certificaciones se hagan oficiales la penetración en el mercado es muy baja. Algunas empresas, como Cisco por parte de equipos de redes y Samsung por parte de equipos clientes, han decidido realizar alianzas estratégicas para apostar por estos estándares. No obstante, por parte de los dispositivos clientes, estos estándares no están presentes en todo su catálogo de productos, sino solo en sus equipos insignia, gama alta.

Según Cisco [20], hasta el momento no se ha reconocido la importancia de certificaciones de este tipo. Sin embargo, asegura que para el 2018 el volumen de tráfico de voz sobre Wi-Fi superará al volumen que presente sobre LTE y que para el 2019 el tráfico de voz sobre Wi-Fi supondrá el 53% de llamadas sobre IP. De igual manera, la cantidad de dispositivos móviles será 3.5 veces el volumen del 2015 que representaría 1.9 billones de dispositivos móviles en uso. Por lo que certificaciones que permitan interoperabilidad entre soluciones WLAN, en particular resolviendo el reto de roaming, serán necesarios.

3.5.3 Tipos de Soluciones De Roaming

Según el RFC 3753 [21], define las terminologías para los diferentes tipos de Roaming:

- **Roaming Rápido (Fast Roaming)**: Un roaming que tiene como objetivo minimizar la latencia del roaming, sin ningún interés explícito en la pérdida de paquetes.
- **Roaming Fluida (Smooth Roaming)**: Una Roaming que apunta principalmente a minimizar la pérdida de paquetes, sin preocuparse explícitamente por retrasos adicionales en el reenvío de paquetes.
- **Itinerancia Transparente (Seamless Roaming):** Una Roaming sin una degradación considerable de la calidad de servicio requerida por la aplicación.

Por lo general, los métodos que resuelven el tema de Roaming se enfocan en minimizar el tema del retardo generado en el proceso, por eso se mencionó que son métodos de Roaming rápida. Sin embargo, hay detalles importantes que no se resuelven solo con minimizar el retardo, como es la pérdida de paquetes.

El trabajo presentado en el siguiente capítulo considera los últimos dos factores como parte del diseño. No solo se pretende diseñar un sistema que minimice el retardo generado por el proceso, sino que además se incluirá un módulo de protección ante pérdida de paquetes. Además, en cuanto a interoperabilidad, al usar software de código abierto para la implementación de parte del diseño, el software utilizado es compatible con un gran número de dispositivos. En este sentido, se trata el tema de interoperabilidad hasta cierto punto debido a que no se realizan modificaciones en el cliente.

CAPITULO 4

DISEÑO E INTEGRACIÓN

En capítulos previos se ha revisado la teoría referente a seguridad e Roaming según el estándar 802.11. Primero se introdujo el concepto de una Red Robusta de Seguridad en entorno Empresarial y el proceso que atraviesa un cliente para asociarse a una. Luego, se explicó el proceso de Roaming, el impacto en tiempos en un entorno de seguridad Empresarial y los métodos para lograr una Roaming transparente.

Antes de empezar con el diseño del método de Reasociación Rápida y Segura propuesto, es necesario plantear los requerimientos de este. Estos requerimientos se basan en los objetivos establecidos al final del capítulo 1, uno de los cuales indica que no se realice modificaciones al equipo cliente. En este sentido, la solución a diseñar será compatible con un gran número de dispositivos móviles. Además, se delimita el tamaño de la red, la fase del proceso de Roaming en la que realizarán las modificaciones y la seguridad que se empleará.

En la segunda parte del capítulo, se presenta el diseño de la solución de FSR. Se analiza la arquitectura, el método de Captura de Llave (Key Caching), el redescubrimiento de la red y el módulo de respaldo ante pérdida de paquetes.

4.1 Requerimientos de Diseño

En la presente sección se indican los requerimientos del sistema a diseñar. Si bien es cierto el diseño se enfoca en reducir el tiempo de Roaming, se debe tener en cuenta el entorno en el que este diseño será implementado. En el Capítulo 1 se presenta el entorno empresarial mediano el cual es un espacio no atendido correctamente por las soluciones que los fabricantes ofrecen actualmente.

Los requerimientos detallados a continuación se centran en definir las bondades y limites que el diseño del sistema de *Roaming Rápida y Segura* en un entorno empresarial mediano debe considerar.

4.1.1 Compatibilidad

En cuanto a compatibilidad, es necesario considerar no modificar el comportamiento de los dispositivos clientes.

- **Clientes**: Uno de los mayores retos al momento de realizar el diseño de un sistema de FSR es el comportamiento de los equipos clientes. Este tema se explicó en el Capítulo 3 al definir las fases del proceso de Roaming. Debido a que no están estandarizados los diferentes algoritmos referentes a el roaming por parte de los equipos móviles clientes que hay en el mercado, no existe una solución absoluta que sea compatible con estos dispositivos. Aun cuando es lo esperado por la IEEE al ratificar el Fast BSS Transition como método de FSR, el tema de la compatibilidad es un factor en su contra aun hoy cinco años después de haberse incluido en el estándar [22]. Sin embargo, es un requerimiento que la solución a diseñar sea compatible con un número considerable de equipos móviles.

  En este sentido, se delimita el diseño de la solución de FSR a ser compatible con todo dispositivo móvil que soporte el estándar 802.11-2007, ya que es a partir de este estándar que se introduce el campo RSNIE [18]. Dentro de la información que comparte el cliente dentro

de este campo se encuentra la PMKID la cual se aprovechará para el desarrollo del sistema de FSR.

- **Puntos de acceso:** Como requerimiento de diseño, es necesario considerar equipos básicos en cuanto a Software y Hardware para lograr la reducción del tiempo de Roaming.

4.1.2 Roaming

De acuerdo con lo explicado en el Capítulo 3 al definir las fases del proceso de Roaming, el comportamiento del equipo cliente es una variable que no se puede controlar. Es por ello por lo que se hace referencia al roaming en el presente documento, se entiende por fase de ejecución de Roaming. Principalmente, se trabajará en un sistema que evite la comunicación suplicante – servidor autenticador, que es la etapa que mayor retardo agrega a la fase.

Adicionalmente, el diseño del sistema de FSR solo considera un método de solución de Roaming en capa 2. Debido a que se intenta implementar este sistema en un despliegue empresarial mediano, se asume que la capa de acceso inalámbrico se encuentre bajo el dominio de un solo servidor DHCP. Sin embargo, se debe entender que a trabajos futuros este diseño puede ser parte de un sistema mayor donde sea parte de una de una solución que considere a el roaming de capa 3.

4.1.3 Nivel de Seguridad

Se considera un nivel de seguridad alto debido a que el problema de roaming se intensifica bajo este requerimiento. Si una red no considera una seguridad alta, el tiempo que requiere la etapa de autenticación 802.1X/EAP-Radius no existiría y el roaming no sería un problema a ese nivel.

Sin embargo, debido a que se considera una red mediana para empresas como hoteles medianos, institutos, hospitales, entre otros, es necesario

indicar si estas instituciones requieren un nivel de seguridad elevado para su operación. Desde el punto de vista del usuario final,

4.2 Diseño de la Solución de Fast Secure Roaming

La fase de realización del proceso de roaming puede ser dividido en 3 etapas: (i) *Open Authentication*, (ii) Autenticación 802.1X/EAP – Radius y (iii) *4-Way Handshake* para la generación de llaves dinámicas de encriptación. De estas 3 etapas, es la segunda - que requiere un proceso de "*challenge-response*" - la que consume mayor tiempo.

Con la finalidad de reducir el tiempo que conlleva la fase de realización del proceso de roaming en una red con autenticación por identidad de usuario (WPA2 Enterprise / RADIUS), se debe intentar eliminar la comunicación suplicante – servidor autenticador en el proceso de reasociación.

4.2.1 Arquitectura

Para el diseño del sistema de FSR se ha tenido en cuenta las arquitecturas WLAN para implementaciones de métodos de Roaming rápida explicados en el Capítulo 3. La ***Figura 4-1*** muestra una arquitectura híbrida entre una arquitectura de APs autónomos y una con controlador de WLAN. Bajo este esquema, se abstrae solo la gestión de llaves de un controlador WLAN para gestionar las credenciales de los clientes móviles hacia un *clúster* de APs que trabajan como un solo autenticador.

Se optó por tomar como base de diseño una arquitectura centralizada debido a que libera de carga computacional a los APs. Entonces, se pueden utilizar APs ligeros para la implementación de esta arquitectura. La ***Tabla 4-1*** muestra una comparativa de arquitecturas comparándola con la que se propone en el presente trabajo. La arquitectura de clúster de APs (sistema híbrido) permite el uso de APs de bajo costo y al solo centralizar la gestión de llaves, el equipo de control no debe ser tan complejo.

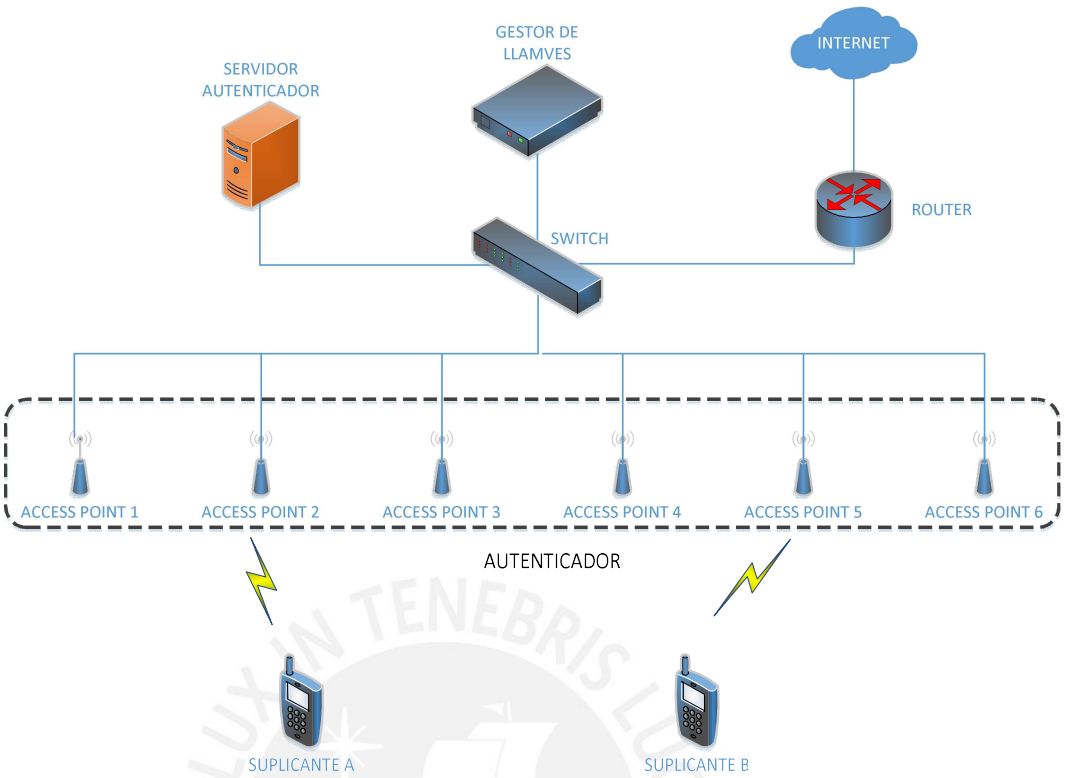


Figura 4-1 Clúster de APs como Autenticador (Sistema Híbrido)

Elaboración Propia

	APs Autónomos	Controlador de WLAN	Cluster de APs (Sistema Distribuido)	Cluster de APs (Sistema Híbrido)
Capacidad de SW y HW en APs	ALTO	BAJO	ALTO	BAJO
Capacidad de SW y HW en Ente Externo	---	ALTO	---	BAJO
Control de la Red de Acceso	NINGUNO	CENTRALIZADO	NINGUNO	CENTRALIZADA LA GESTION DE LLAVES
Complejidad de Implementación	ALTO	BAJO	ALTO	INTERMEDIO
Costo de Implementación	BAJO	ALTO	INTERMEDIO	BAJO

Tabla 4-1 Comparación de las Arquitecturas de Roaming rápido

Elaboración Propia

Para la implementación de esta arquitectura, se deben considerar tres bloques: el clúster de puntos de acceso, el gestor de llaves y el servidor autenticador.

(1) Clúster de Puntos de acceso:

Para la implementación, se utilizó puntos de acceso TP-Link WDR-3600 *(Anexo 5 – Hoja Técnica del dispositivo TP-Link)*. La **Tabla 4-2 Especificaciones** *Punto* **de acceso TP-Link WDR3600** muestra las características de hardware de estos equipos. Estos puntos de acceso han sido modificados a nivel de firmware para una mejor gestión del hardware. El firmware utilizado es el OpenWrt, el cual es POSIX-compliant, en su versión Chaos Calmer 15.05.1. Al cambiar de firmware se obtuvo mayor flexibilidad en configuración de los APs, por ejemplo, se configuraron con el protocolo de seguridad WPA2- Enterprise el cual no estaba habilitado en el firmware instalado por defecto. Además, el uso del firmware OpenWrt permite que las modificaciones realizadas en software no sean exclusivas para el TP-Link WDR3600. Esto se debe a la gran cantidad de equipos que soportan este firmware y que pueden ser considerados para este tipo de implementaciones. Esta característica resuelve el tema de compatibilidad en equipos punto de acceso. En el *Anexo 9* se muestra el listado de dispositivos que soportan OpenWrt.

	Especificaciones
Tipo de Dispositivo	WiFi Router
Marca	TP-Link
Modelo	TL-WDR3600
Plataforma	Atheros AR9344
CPU MHz	560
Memoria ROM (MB)	8
Memoria RAM (MB)	128
Puertos de Red	1 WAN + 4 LAN
WLAN 2.4GHz	b/g/n
WLAN 5.0GHz	a/n
Puertos USB	2 x 2.0
Fuente de Energía	12 VDC, 1.5 A
URL Dispositivo	http://www.tp-link.com/en/products/details/cat-9_TL-WDR3600.html

Tabla 4-2 Especificaciones Punto de acceso TP-Link WDR3600 *[23]*

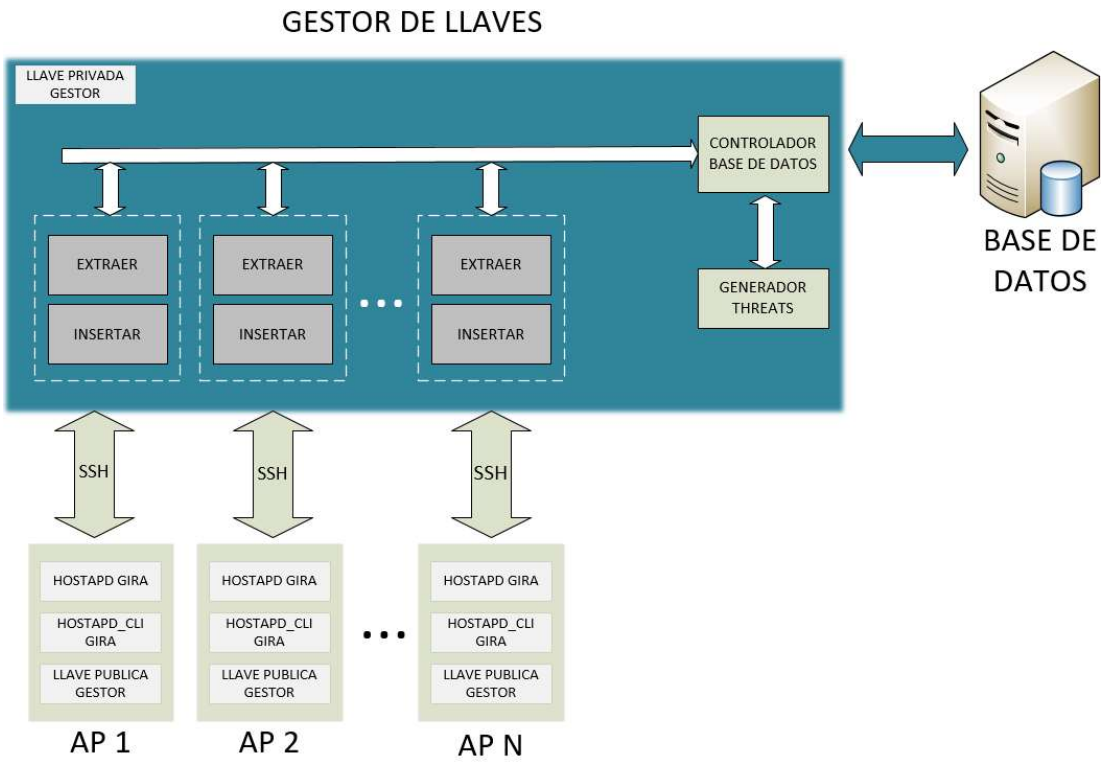


Figura 4-2 Diagrama de Bloques del Gestor de Llaves

Elaboración Propia

(2) Gestor de Llaves:

Es el responsable de la distribución de las llaves de sesión de los clientes a todos los Puntos de acceso del sistema.

La ***Figura 4-2*** muestra el diagrama de bloques que comprende el gestor de llaves y en la ***Figura 4-3*** muestra el diseño relacional de la base de datos.

El gestor de llaves se conecta a una base de datos (Habilitada en PostgreSQL) la cual consta de 3 tablas. Una tabla “ACCESS_POINTS” la cual contiene las direcciones IP de los APs pertenecientes al sistema. El llenado de esta tabla se hace de manera manual a través de la interfaz de comando del programa principal. Otra tabla llamada “USUARIOS” es la tabla general en donde serán registradas las credenciales (PMK, PMKID) de los usuarios que ingresen a la red. Finalmente, la tabla “USUARIOS_X_AP” en la cual se registran los clientes y en qué Puntos de acceso ya han sido registradas sus credenciales.

El programa principal fue desarrollado en Python 2.7 *(Anexo 11)* y operó en una laptop con procesador Intel Core i7 6ta Gen, 16 GB de RAM y SO Linux - Ubuntu. Para que la comunicación sea segura se utilizó el protocolo SSH entre APs y Gestor instalando para ello la llave pública RSA del gestor en cada uno de los APs dejando la llave privada del lado del gestor. Por cada AP registrado se crean dos subprocesos, uno (extraer) encargado de revisar si existen nuevos clientes asociados para registrar sus credenciales en la base de datos y otro (insertar) encargado de revisar la tabla "usuarios_x_ap" constantemente para verificar si existen clientes registrados en el sistema cuyas credenciales no hayan sido insertadas en el AP en cuestión. De esta manera todos los Puntos de acceso compartirán de manera automatizada las credenciales de todos los usuarios que se registren exitosamente en el sistema a través del servidor RADIUS.

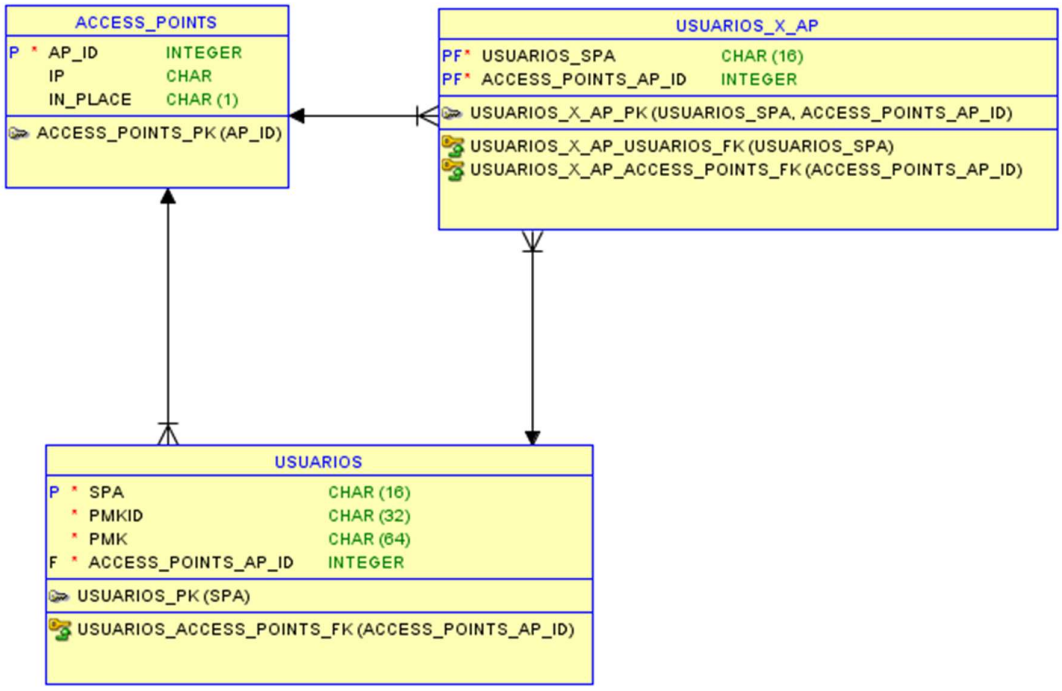


Figura 4-3 Bases de Datos Relacionales

Elaboración Propia

(3) Servidor Autenticador:

El servidor autenticador utilizado es el FreeRadius 3.0. La instalación del FreeRadius se realizó sobre un computador portátil corriendo Ubuntu 16.04. Se realizaron las configuraciones del servidor autenticador en los siguientes archivos [24]:

- **radiusd.conf**: Define los parámetros de configuración para el servidor RADIUS. Incluye referencias a todos los demás archivos de configuración.
- **clients.conf**: Define la información necesaria para configurar el cliente RADIUS, incluyendo direcciones IP y secretos compartidos. Este archivo se hace referencia desde el archivo radiusd.conf.
- **users**: El archivo de configuración RADIUS tradicional para los usuarios. Este formato de archivo es similar al formato definido en 1993. El archivo de archivos hace referencia al archivo de usuarios.

Además, se configuró el FreeRadius con el protocolo de seguridad PEAP el cual es ampliamente utilizado en WLAN, lo que permite una gestión limpia frente a los dispositivos clientes. La configuración del protocolo EAP se realiza en el archivo **eap.conf**.

4.2.2 Técnica de Captura de Llave (Key Caching)

Para la elaboración del método de Captura de Llave (*Key Caching),* se tuvo como base el comportamiento del método OKC, el cual es propietario. Al no estar estandarizado este método, no hay una regla a seguir para su implementación.

La ***Figura 4-4*** muestra el proceso de roaming el proceso de roaming utilizando la técnica de Key Caching basado en el método OKC.

(1) Al asociarse por primera vez a la red, el suplicante deberá realizar la autenticación 802.1X/EAP-Radius completa. De esta manera, el AP 1

y cliente reciben la llave maestra de la sesión (PMK) a partir de la cual generan la llave de encriptación (PTK). Además, tanto AP 1 como suplicante generan y guardan en caché la PMKID 1.

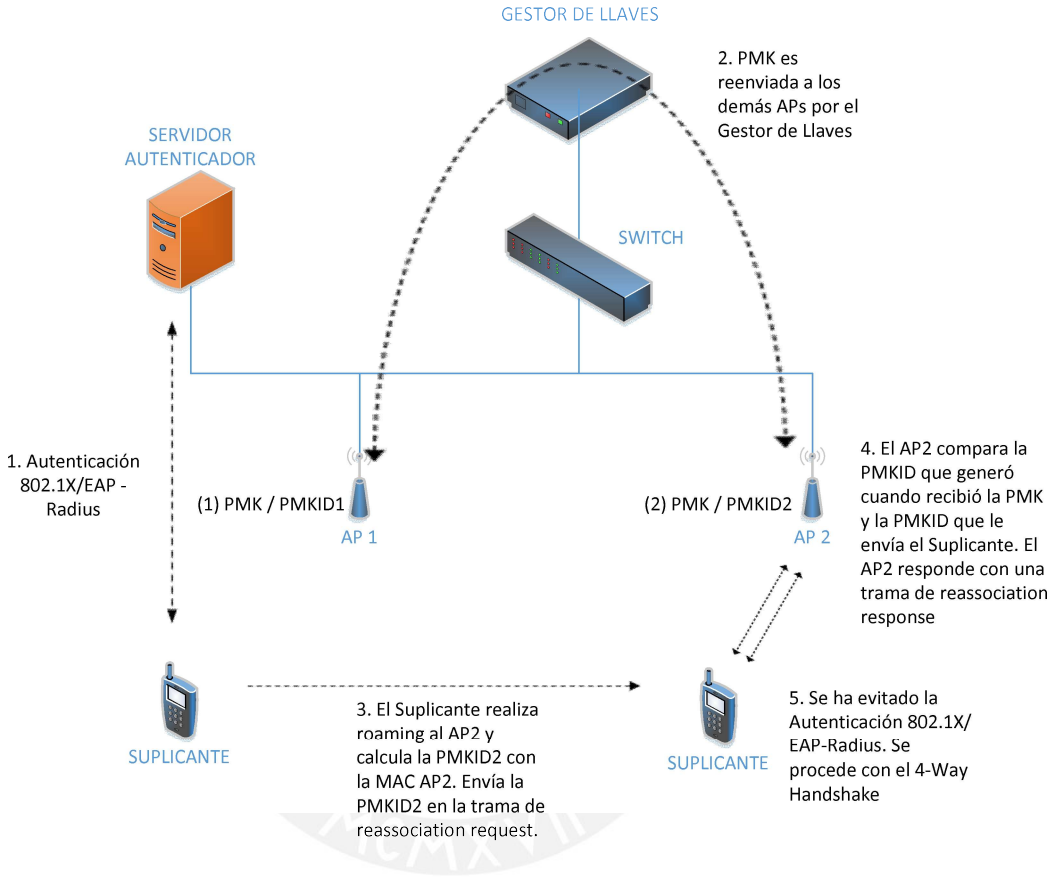


Figura 4-4 Técnica de Captura de Llave (Key Caching) basado en el Método OKC

Elaboración Propia

(2) El Gestor de Llaves extrae la PMK que recibió el AP 1 y la reenvía al AP 2 junto con la dirección MAC del cliente. Entonces, el AP 2 puede generar la PMKID 2 de manera que el suplicante este preregistrado en este AP. Observación: El cliente está preregistrado y no preautenticado ya que se ha reutilizado la PMK generada por el servidor autenticador para el AP 1 y no una debido a un proceso de autenticación 802.1X/EAP-Radius.

(3) El suplicante realiza un roaming del AP 1 al AP 2. Calcula la PMKID 2 con la información de la PMK y las direcciones MAC del AP 2 y suplicante. Esta PMKID 2 se envía en la trama de reassociation request.
(4) El AP 2 compara la PMKID 2, que generó cuando recibió la PMK de parte del gestor de llaves, y la que le envía el suplicante. Si es correcta, envía un reassociation response. De lo contrario, se procede con una autenticación 8021.1X/EAP-Radius completa.
(5) Se ha omitido la comunicación suplicante – servidor autenticador y se procede a generar la nueva llave de encriptación a través del proceso de 4-Way Handshake.

La técnica de Captura de Llave (Key Caching) antes mencionada requiere de modificación en el comportamiento del kernel del punto de acceso. Como se muestra en la ***Figura 4-5***, hay diferentes subsistemas en el código del kernel que están involucrados en la implementación del estándar IEEE 802.11 y el soporte de los controladores [25]:

- mac80211: Subsistema del kernel responsable de implementar el código compartido para dispositivos inalámbricos soft-MAC / half-MAC. Contiene la entidad de administración de capa MAC (MLME).
- cfg80211: Capa entre el espacio de usuario y los flujos mac80211. Principalmente realiza la verificación de integridad y las traducciones del protocolo.
- nl80211: Acceso por parte usuario a las operaciones de cfg80211. Utilizado por wpa_supplicant y hostapd.
- wpa_supplicant: Módulo que soporta cfg80211. Administrado por el usuario para otorgar características de suplicante al equipo.
- hostapd: Módulo que implementa el MLME de AP. Relacionado con nl80211. Administrado por el usuario para otorgar características de autenticador al equipo-
- Entidad de gestión de estaciones (SME): Soporte de comandos de autenticación / asociación independiente.

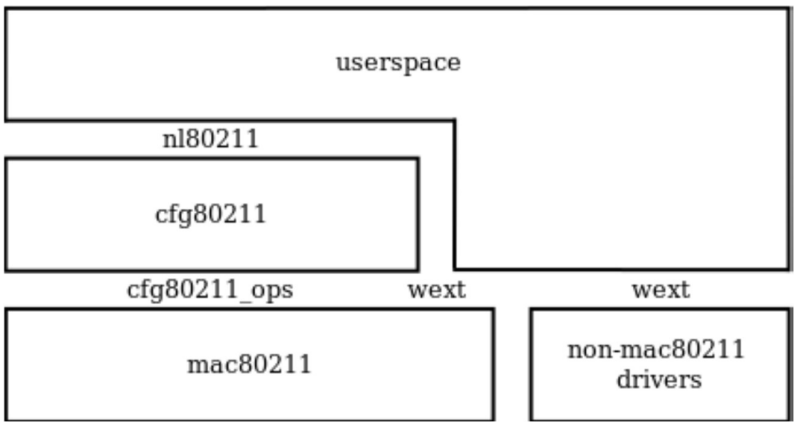


Figura 4-5 Arquitectura del Kernel en un Subsistema Wireless *[26]*

El módulo, dentro de este esquema, que se modificará es el hostapd. Se agregarán rutinas en el código hostapd para extraer e ingresar información a la memoria cache del equipo. De esta manera, el gestor de llaves podrá copiar y reenviar las credenciales de los usuarios a todos los APs de la red.

El proceso daemon hostapd es una implementación del estándar IEEE 802.11 para equipos puntos de acceso. Existen tres implementaciones de este proceso: hostapd de Jouni Malinen, hostapd de OpenBSD y hostapd de Devicescape. El proceso hostapd que se utilizó es la implementación para sistemas operativos basado en Linux de Jouni Malinen en su versión estable, para el firmware OpenWrt, 2.5 / 27-09-2015.

El hostapd cuenta con una interfaz de línea de comandos (CLI, por sus siglas en inglés) que permite a los usuarios ingresar instrucciones por medio de una línea de texto simple. La ***Figura 4-6*** muestra el diagrama de bloques del proceso hostapd. En esta figura se muestra el módulo en el que se realizaron las modificaciones.

Con el fin que el gestor de llaves realice consultas al hostapd se agregaron los siguientes comandos al CLI del hostapd (***Figura 4-7***):

- ***all_sta:*** muestra los clientes asociados al AP al momento de la consulta.

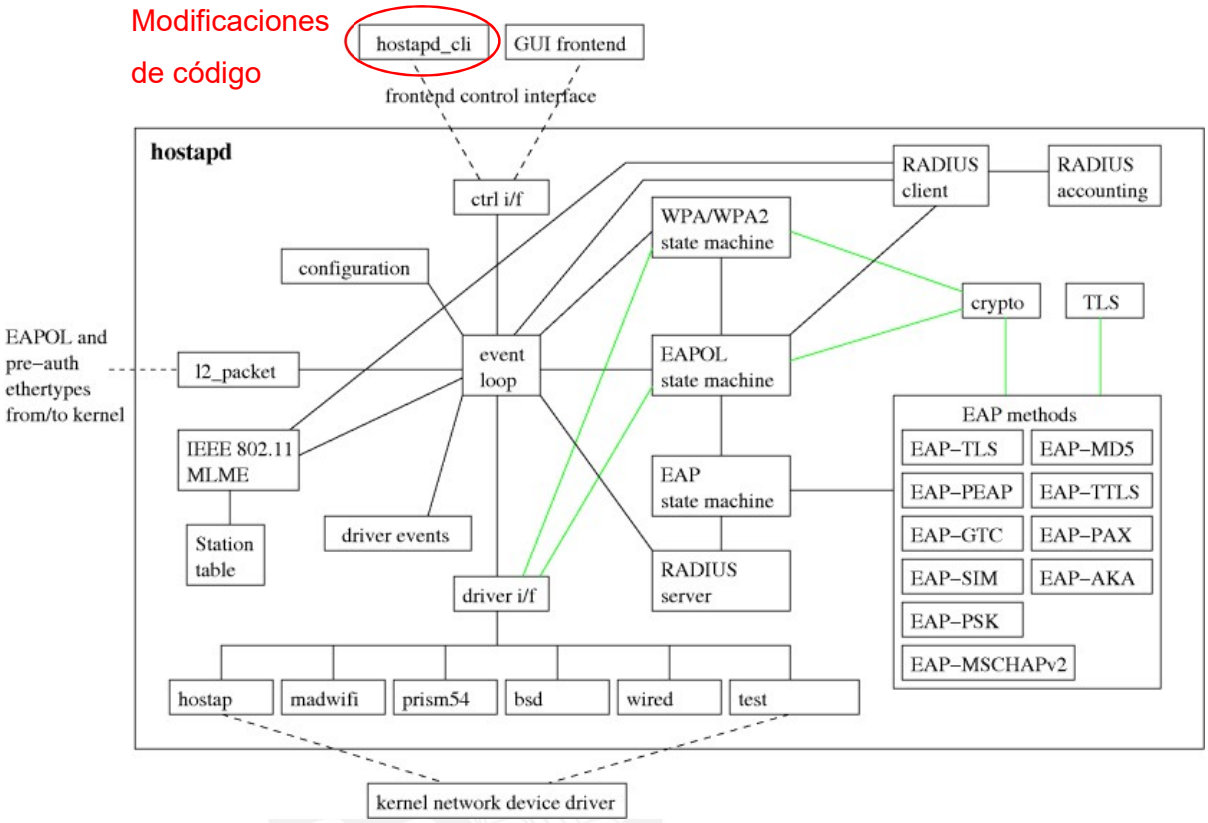


Figura 4-6 Módulos hostapd *[27]*

- ***pmksa:*** muestra las entradas PMKSA guardadas en caché en el formato: <ID><MAC Cliente><PMKID><Tiempo de expiración de la sesión>.
- ***pmksa_list:*** muestra las entradas PMKSA guardadas en caché en el formato: <ID><MAC Cliente><PMKID><PMK><Tiempo de expiración de la sesión>.
- ***pmksa_create:*** guarda en caché las entradas PMKSA ingresadas en el formato: <ID><MAC Cliente><PMKID><PMK><Tiempo de expiración de la sesión>.
- ***pmksa_flush:*** borra todas las entradas PMKSA guardadas en caché.

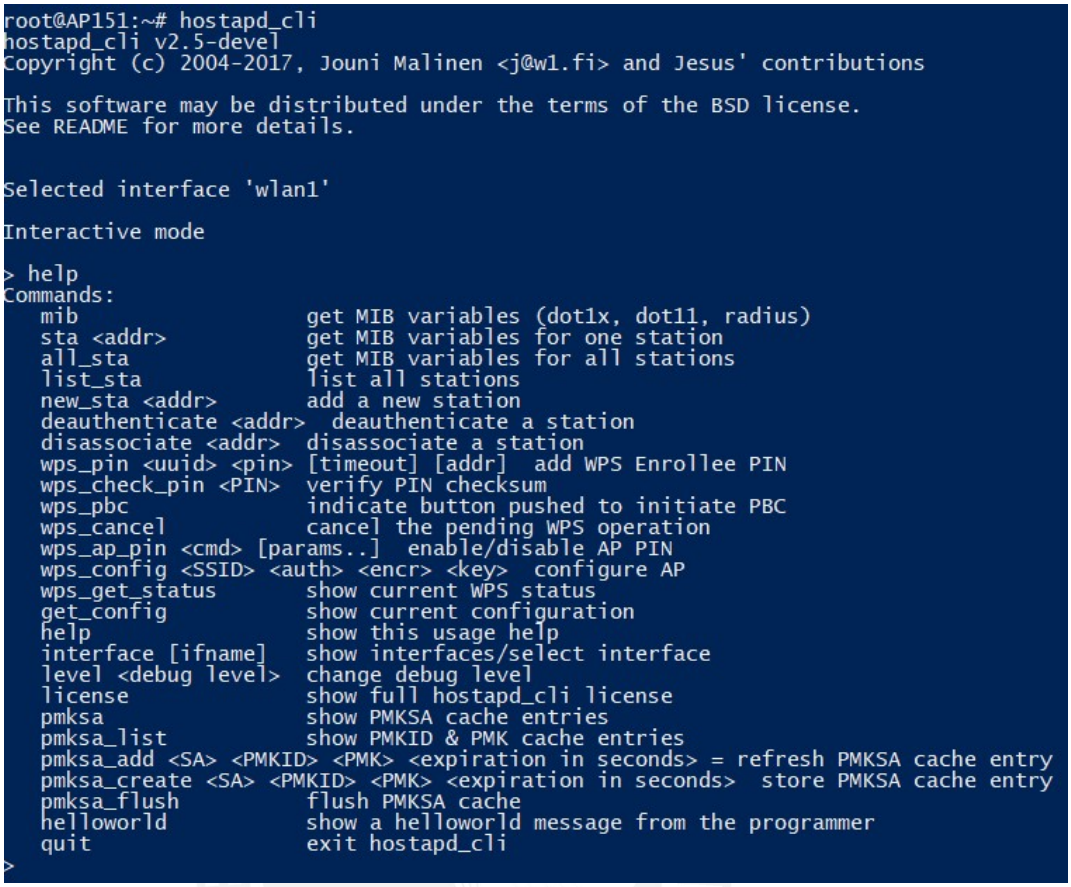


Figura 4-7 Menú CLI hostapd v. 2.5 Personalizado

Elaboración Propia

La ***Figura 4-8*** muestra las funciones que se modificaron y el flujo dentro de diferentes instancias del código hostapd para obtener la información requerida a través de la interfaz CLI. De esta manera el gestor de llaves puede consultar la información de los clientes en memoria caché. *(Anexo 10)*

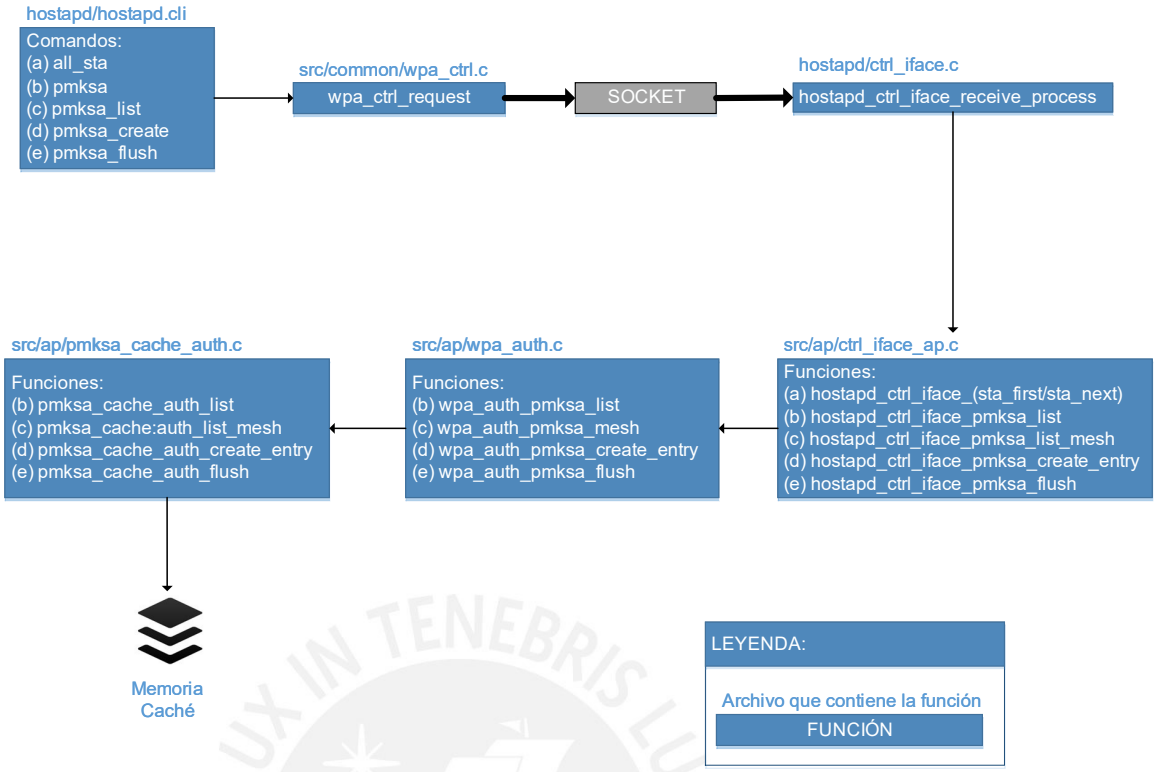


Figura 4-8 Funciones Personalizadas – hostapd

Elaboración Propia

4.2.3 Reconfiguración de la LAN

Cuando el cliente móvil culmina el proceso de Roaming y está listo para utilizar los recursos de la red a través del nuevo AP, la red aún no está preparada ya que tiene información desactualizada. La reconfiguración de la LAN implica actualizar las tablas MAC de los diferentes equipos de capa 2 con el objetivo que reconozcan que el cliente utiliza el nuevo AP para comunicarse con la red.

Para lograr este objetivo se pretende modificar el comportamiento del autenticador, de manera que, proactivamente, envíe un mensaje de reconocimiento a la red.

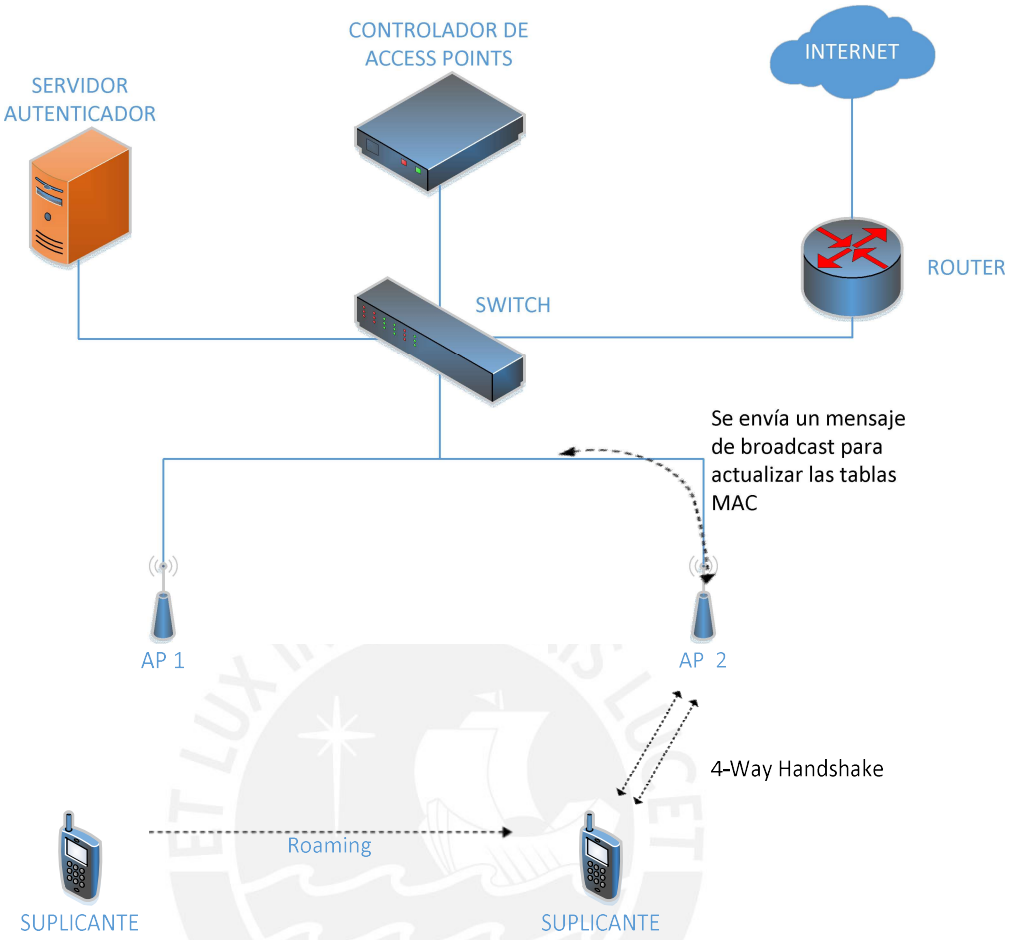


Figura 4-9 Envío de *Broadcast* para reconfiguración de la Red

Elaboración Propia

La ***Figura 4-9*** muestra el momento en que la verificación de la información del cliente ya ha finalizado de manera exitosa. Se omite la autenticación 802.1X/EAP-Radius y se procede con la generación de llaves dinámicas de encriptación. En el momento que el proceso de 4-Way Handshake da inicio, el AP 2 debe enviar un mensaje de *broadcast* con la información de la dirección MAC del cliente. De esta manera, durante el tiempo que toma la generación de la PTK (≈20 ms), las tablas MAC del *conmutador (switch)* y los demás APs de la red se actualizan y entienden que el cliente se comunica a través del AP 2. Entonces, al finalizar la generación de las llaves dinámicas

de encriptación, tanto cliente como demás equipos de capa 2 de la red estarán en condición de intercambiar flujo de datos.

4.2.4 Mínima Pérdida de Paquetes

El retardo ocasionado por el proceso roaming, aun cuando minimizado por la técnica de Captura de Llave (Key Caching), aún tiende a permitir pérdida de paquetes. Mientras que el cliente migra del AP 1 al AP 2, los servicios en capas superiores aun le continúan enviando tráfico de datos. Es por este motivo, que es necesario considerar un módulo que permita conseguir una mínima pérdida de paquetes durante el proceso de Roaming.

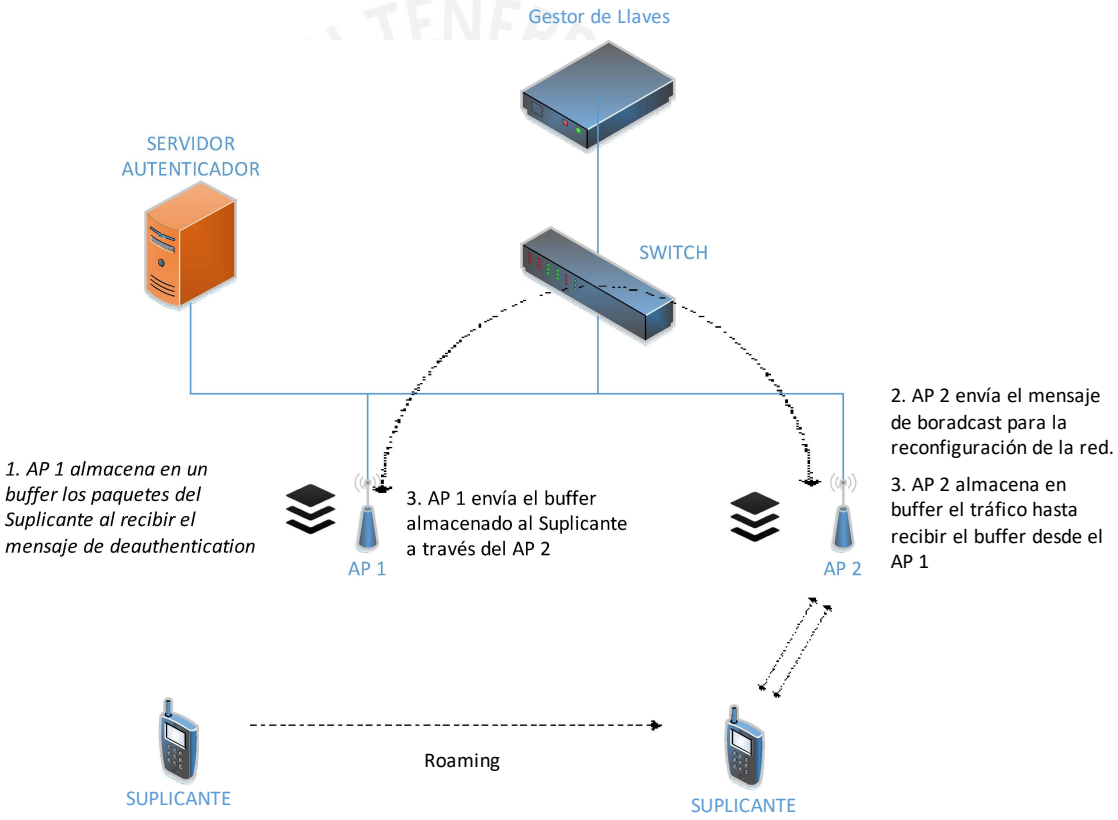


Figura 4-10 Respaldo ante Pérdida de Paquetes

Elaboración Propia

La ***Figura 4-10*** se muestra el comportamiento del diseño módulo de mínima perdida de paquetes.

(1) Cuando el cliente inicia el proceso de roaming, envía un mensaje de *deauthentication* al AP 1. En este momento, el AP 1 inicia el proceso de almacenar el tráfico dirigido hacia el suplicante en un buffer temporal.

(2) El AP 2 reconoce al suplicante como usuario de la red. Inicia el proceso de 4-Way Handshake y, proactivamente, envía un mensaje de *broadcast* para la actualización de las tablas MAC de los *conmutadores*. El tráfico de datos se direcciona hacia el suplicante a través del AP 2.

Observación: En caso de que el AP 1 no reciba el mensaje de *broadcast* dentro de los 150 ms (retardo máximo de Roaming considerado) deja de guardar en buffer los paquetes recibidos y borra el buffer temporal.

(3) Al recibir el mensaje de *broadcast*, el AP 1 entiende que el cliente se ha reasociado exitosamente a un nuevo AP de la red. El AP 1 inicia el proceso de redirigir el tráfico en *broadcast* hacia el suplicante a través del AP 2. El AP 2 almacena en un buffer temporal el tráfico redireccionado de la red, mientras termina de recibir los paquetes enviados por el AP 1. Una vez que el AP 2 envía los datos recibido del AP 1, continúa el reenvío del tráfico de datos de la red hacia el cliente.

Cabe resaltar que los dispositivos, herramientas y código desarrollado en el presente trabajo representan una manera de probar el concepto mas no se debe entender como una solución definitiva. Podría darse el caso de encontrar mejores y más eficientes herramientas, lenguajes de programación e incluso hardware que permita desarrollar el sistema de Roaming rápido tomando como referencia el diseño presentado.

CAPITULO 5

PRUEBAS Y ANÁLISIS

En el presente capítulo, se muestran las distintas pruebas de concepto utilizadas para comprobar la funcionalidad del sistema propuesto. Se realizaron pruebas de concepto de las funciones del módulo *de Roaming Rápido y Seguro*, en un entorno Linux en computadores portátiles emulando el comportamiento de autenticadores, para luego realizar las pruebas funcionales del sistema en un entorno de prueba con puntos de acceso reales.

En las últimas secciones del capítulo se presenta un análisis de la capacidad de la implementación realizada y de los equipos que se utilizaron. Se muestra la capacidad máxima de usuarios utilizando los puntos de acceso TP Link WDR3600 y el impacto en los equipos debido a las modificaciones en software realizadas.

5.1 Pruebas de Concepto

El software desarrollado para el objetivo de la tesis inicialmente fue instalado en laptops con sistema operativo Linux Ubuntu 17.04 para realizar las pruebas de concepto. Este entorno de pruebas contó con los siguientes elementos:

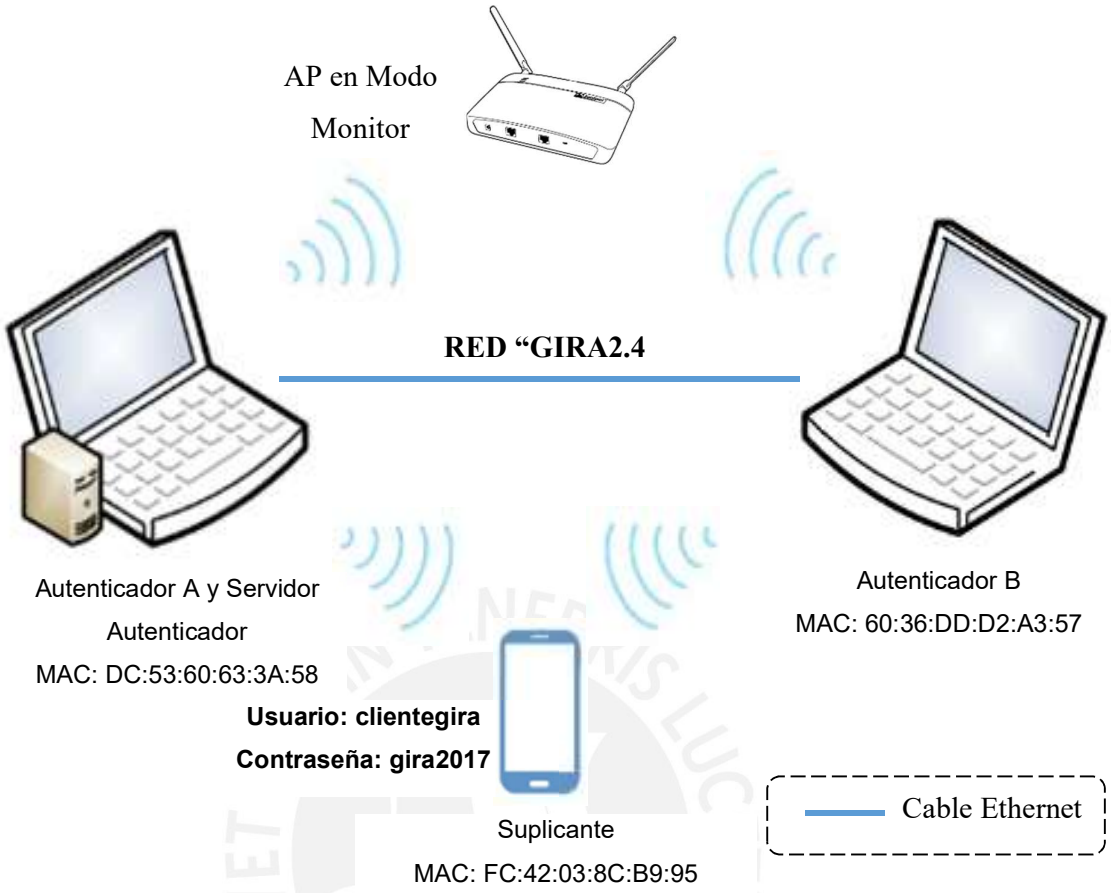


Figura 5-1 Entorno de Prueba - Ubuntu 16.04

ELABORACIÓN PROPIA

- Suplicante: Smartphone con Android 6.0.1
- Autenticadores: 2 Laptops con Ubuntu 17.04. Configurados para operar en el canal 1 y con el mismo SSID. *Hostapd* con módulo Fast Secure Roaming implementado.
- Servidor de Autenticación: *FreeRadius* 3.0 corriendo sobre una de las laptops
- Monitor: Punto de acceso con firmware OpenWrt, en modo monitor para capturar paquetes con herramienta tcpdump.

5.1.1 Reasociación del Cliente

En esta prueba se revisan, haciendo uso de la herramienta Wireshark, las tramas de gestión que captura el AP en modo monitor, utilizando la herramienta tcpdump, para confirmar la reasociación del Suplicante en el Autenticador B.

Secuencia de eventos:

(1) La interfaz inalámbrica del Autenticador A se enciende y se apaga la interfaz inalámbrica del Autenticador B.
(2) El Suplicante se asocia a la red a través del Autenticador A, de modo que este último almacena la PMK del cliente en su memoria caché y genera un PMKID.
(3) Se extraen las credenciales (MAC, PMK, PMKID y Tiempo de Expiración de la sesión) del Suplicante mediante línea de comandos del proceso “hostapd” del Autenticador A.
(4) Se enciende la interfaz inalámbrica del Autenticador B.
(5) Se registra al Suplicante y sus datos (MAC, PMK, PMKID y Tiempo de Expiración de la sesión) en la memoria caché del Autenticador B mediante línea de comandos del proceso “hostapd”.
(6) Se apaga la interfaz inalámbrica del Autenticador A y el Suplicante inicia el proceso de roaming hacia el Autenticador B.
(7) Se verifica, a través del Autenticador B, la reasociación del Suplicante a la red. ***Figura 5-2 Autenticación de Cliente en Entorno Linux - Wireshark***.

Durante todo el proceso el AP Monitor ha estado capturando las tramas del medio inalámbrico. Bajo esta secuencia de eventos, solo se realizó la prueba de concepto en un mismo canal de frecuencia.

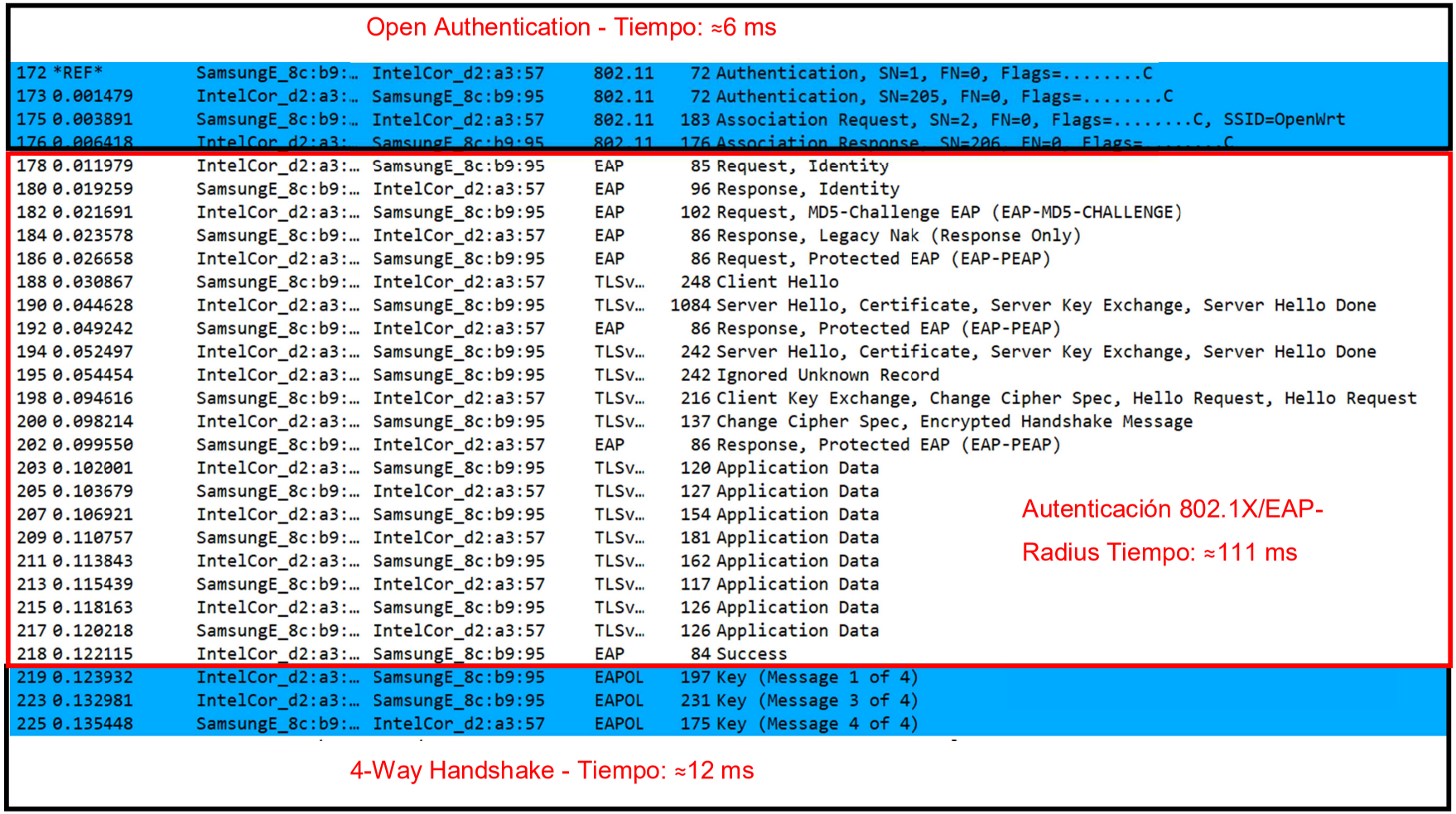
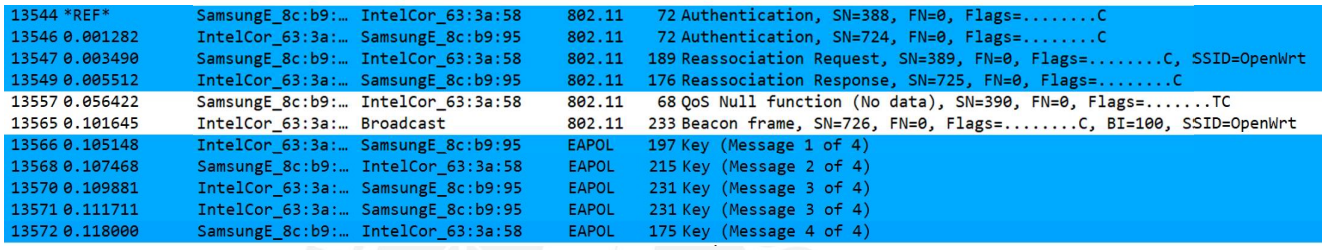


Figura 5-2 Autenticación de Cliente en Entorno Linux - Wireshark

Elaboración Propia

Se verificó que, durante el proceso de Roaming, el cliente evita la autenticación con el Servidor de autenticación. El Autenticador B, al cual el Suplicante migra, ya cuenta con sus credenciales registradas de modo que se procede con el proceso de 4 way handshake directamente. La muestra la información de Asociación del cliente a la red (número 2 en la secuencia de eventos) analizada a través de la herramienta Wireshark. Se observa los tiempos promedios de cada etapa de la asociación. En la ***Figura 5-3*** se muestra la reasociación del cliente (número 7 en la secuencia de eventos) y se confirma que se omite la autenticación 802.1X/EAP-Radius.

Autenticación 802.1X/EAP-Radius omitida - Tiempo: ≈118 ms



13544	*REF*	SamsungE_8c:b9:…	IntelCor_63:3a:58	802.11	72 Authentication, SN=388, FN=0, Flags=........C
13546	0.001282	IntelCor_63:3a:…	SamsungE_8c:b9:95	802.11	72 Authentication, SN=724, FN=0, Flags=........C
13547	0.003490	SamsungE_8c:b9:…	IntelCor_63:3a:58	802.11	189 Reassociation Request, SN=389, FN=0, Flags=........C, SSID=OpenWrt
13549	0.005512	IntelCor_63:3a:…	SamsungE_8c:b9:95	802.11	176 Reassociation Response, SN=725, FN=0, Flags=........C
13557	0.056422	SamsungE_8c:b9:…	IntelCor_63:3a:58	802.11	68 QoS Null function (No data), SN=390, FN=0, Flags=.......TC
13565	0.101645	IntelCor_63:3a:…	Broadcast	802.11	233 Beacon frame, SN=726, FN=0, Flags=........C, BI=100, SSID=OpenWrt
13566	0.105148	IntelCor_63:3a:…	SamsungE_8c:b9:95	EAPOL	197 Key (Message 1 of 4)
13568	0.107468	SamsungE_8c:b9:…	IntelCor_63:3a:58	EAPOL	215 Key (Message 2 of 4)
13570	0.109881	IntelCor_63:3a:…	SamsungE_8c:b9:95	EAPOL	231 Key (Message 3 of 4)
13571	0.111711	IntelCor_63:3a:…	SamsungE_8c:b9:95	EAPOL	231 Key (Message 3 of 4)
13572	0.118000	SamsungE_8c:b9:…	IntelCor_63:3a:58	EAPOL	175 Key (Message 4 of 4)

Figura 5-3 Reasociación del Cliente – Wireshark

Elaboración Propia

Las siguientes Tablas presentan los resultados de las pruebas de roaming en el canal de frecuencia 1 – 2412 MHz. La ***Tabla 5-1*** ***Roaming en mismo Canal de Frecuencia - Entorno Linux*** muestra los tiempos promedios del proceso de roaming completo, mientras que la ***Tabla 5-2*** muestra los tiempos promedios de la fase de ejecución del roaming.

Fase	Tiempo de Roaming - Sin Método FSR (ms)	Tiempo de Roaming - Método FSR Propuesto (ms)
Selección	**213**	**213**
Ejecución	**151**	**21**
TOTAL	**364**	**234**

Tabla 5-1 Roaming en mismo Canal de Frecuencia - Entorno Linux

Etapa de la Fase de Ejecución	Tiempo de Roaming - Sin Método FSR (ms)	Tiempo de Roaming - Método FSR Propuesto (ms)
Open Authentication	6	6
Autenticación 802.1X-Radius	130	-
4-Way Handshake	15	21
TOTAL	151	21

Tabla 5-2 Roaming en mismo Canal de Frecuencia - Fase de Ejecución - Entorno Linux

5.2 Pruebas de Funcionalidad

Se instaló y configuró el proceso "*hostapd*" con el módulo de FSR en los Puntos de acceso. Este entorno de pruebas contó con los siguientes elementos:

- Suplicantes: Dispositivos móviles con sistemas operativos Android 4, Android 6.0.1
- Autenticadores: 2 Puntos de acceso TP-LINK WDR3600 con firmware OpenWrt Chaos Calmer 15.1.1 y *hostapd* con módulo de FSR instalado.
- Servidor de Autenticación: *FreeRadius* 3.0 instalado en laptop-servidor con sistema operativo Linux Ubuntu 16.04.
- Software de Gestión de llaves: Instalado en laptop-servidor con sistema operativo Linux Ubuntu 16.04.
- Monitor: Punto de acceso con firmware OpenWrt, configurado en modo monitor para capturar paquetes con herramienta tcpdump.

Figura 5-4 Entorno de Prueba - OpenWRT

ELABORACIÓN PROPIA

5.2.1 Prueba de Roaming Rápida

En esta prueba se revisan, haciendo uso de la herramienta Wireshark, las tramas de gestión que captura el AP en modo monitor, utilizando la herramienta tcpdump, para confirmar que el Suplicante ha realizado una Roaming Rápida entre el Autenticador A al Autenticador B.

Secuencia de eventos:

(1) La interfaz inalámbrica del Autenticador A se enciende y se apaga la interfaz inalámbrica del Autenticador B.
(2) El Suplicante Android se asocia a la red a través del Autenticador A, de modo que este último almacena la PMK del cliente en su memoria caché y genera un PMKID.
(3) El Gestor de Llaves extrae la información de sesión del Suplicante Android (MAC, PMK, PMKID y Tiempo de Expiración de la sesión) a través de una comunicación SSH.
(4) El Gestor de Llaves envía los datos del Suplicante Android al Autenticador B y lo registra en su memoria caché.
(5) Se apaga la interfaz inalámbrica del Autenticador A y el Suplicante Android inicia el proceso de roaming hacia el Autenticador B.
(6) Se verifica, a través de línea de comandos del Autenticador B, la reasociación del cliente a la red.

Durante todo el proceso el AP Monitor ha estado capturando las tramas del medio inalámbrico. Bajo esta secuencia de eventos, se realizaron dos pruebas: Roaming en un mismo canal de frecuencia e Roaming en canales de frecuencia diferente.

Se verificó que el cliente realiza una Roaming rápida. El Autenticador B, al cual el Suplicante migra, ya cuenta con sus credenciales registradas por lo que procede a generar las llaves dinámicas de encriptación. En la ***Figura 5-5*** se muestra la reasociación del cliente (número 6 en la secuencia de eventos) y se confirma que se omite la autenticación 802.1X/EAP-Radius y el tiempo de roaming fue de 24 ms.

9081	*REF*	SamsungE_8c:b9:…	Tp-LinkT_ba:7c:6f	802.11	72	Authentication, SN=169, FN=0, Flags=........C
9083	0.001399	Tp-LinkT_ba:7c:…	SamsungE_8c:b9:95	802.11	72	Authentication, SN=2138, FN=0, Flags=........C
9085	0.003602	SamsungE_8c:b9:…	Tp-LinkT_ba:7c:6f	802.11	189	Reassociation Request, SN=170, FN=0, Flags=........C, SSID=OpenWrt
9087	0.005894	Tp-LinkT_ba:7c:…	SamsungE_8c:b9:95	802.11	176	Reassociation Response, SN=2139, FN=0, Flags=........C
9089	0.011174	Tp-LinkT_ba:7c:…	SamsungE_8c:b9:95	EAPOL	197	Key (Message 1 of 4)
9091	0.013438	SamsungE_8c:b9:…	Tp-LinkT_ba:7c:6f	EAPOL	215	Key (Message 2 of 4)
9092	0.016552	Tp-LinkT_ba:7c:…	SamsungE_8c:b9:95	EAPOL	231	Key (Message 3 of 4)
9095	0.024649	SamsungE_8c:b9:…	Tp-LinkT_ba:7c:6f	EAPOL	175	Key (Message 4 of 4)

Las siguientes Tablas presentan los resultados de las pruebas de Roaming en el canal de frecuencia 1 – 2412 MHz. La ***Tabla 5-3*** muestra los tiempos

Figura 5-5 Reasociación del Cliente Prueba de Roaming rápido - Wireshark

muestra los tiempos promedios de la fase de ejecución del roaming.

Fase	Tiempo de Roaming - Sin Método FSR (ms)	Tiempo de Roaming - Método FSR Propuesto (ms)
Selección	213	213
Ejecución	161	19
TOTAL	374	232

Tabla 5-3 Roaming en mismo Canal de Frecuencia – Testbed Real

Etapa de la Fase de Ejecución	Tiempo de Roaming - Sin Método FSR (ms)	Tiempo de Roaming - Método FSR Propuesto (ms)
Open Authentication	6	6
Autenticación 802.1X/EAP-Radius	140	0
4-Way Handshake	15	13
TOTAL	161	19

Tabla 5-4 Roaming en mismo Canal de Frecuencia - Fase de Ejecución – Testbed Real

5.2.2 Prueba de Funcionamiento del Gestor de Llaves

En esta prueba se verifica las tablas de información del Gestor de Llaves y su correcta distribución en los APs asociados a la red. La ***Figura 5-6*** muestra las tres tablas con las que trabaja el gestor de llaves para la administración de las credenciales de sesión de los usuarios a través de la red.

```
postgres=# \d aps
                    Table "public.aps"
      Column       |         Type          |     Modifiers
-------------------+-----------------------+--------------------
 ap_id             | integer               | not null
 ip                | character varying(15) | not null
 located           | boolean               | not null
 tried_connections | integer               | not null default 0
Indexes:
    "aps_pkey" PRIMARY KEY, btree (ap_id)
Referenced by:
    TABLE "usuarios" CONSTRAINT "usuarios_origin_ap_id_fkey" FOREIGN KEY (origin_ap_id) REFERENCES aps(ap_id) ON DELETE CASCADE
    TABLE "usuarios_x_ap" CONSTRAINT "usuarios_x_ap_ap_id_fkey" FOREIGN KEY (ap_id) REFERENCES aps(ap_id) ON DELETE CASCADE

postgres=# \d usuarios
             Table "public.usuarios"
    Column    |         Type          | Modifiers
--------------+-----------------------+-----------
 mac          | character varying(17) | not null
 pmk          | character varying(64) | not null
 pmkid        | character varying(32) | not null
 tiempo       | integer               | not null
 origin_ap_id | integer               | not null
Indexes:
    "usuarios_pkey" PRIMARY KEY, btree (mac)
Foreign-key constraints:
    "usuarios_origin_ap_id_fkey" FOREIGN KEY (origin_ap_id) REFERENCES aps(ap_id) ON DELETE CASCADE
Referenced by:
    TABLE "usuarios_x_ap" CONSTRAINT "usuarios_x_ap_mac_fkey" FOREIGN KEY (mac) REFERENCES usuarios(mac) ON DELETE CASCADE
Triggers:
    ins_usuarios_x_ap_trg AFTER INSERT ON usuarios FOR EACH ROW EXECUTE PROCEDURE ins_usuarios_x_ap_fn()
    upd_usuarios_x_ap_trg AFTER UPDATE ON usuarios FOR EACH ROW EXECUTE PROCEDURE upd_usuarios_x_ap_fn()

postgres=# \d usuarios_x_ap
        Table "public.usuarios_x_ap"
 Column |         Type          | Modifiers
--------+-----------------------+-----------
 mac    | character varying(17) | not null
 ap_id  | integer               | not null
Foreign-key constraints:
    "usuarios_x_ap_ap_id_fkey" FOREIGN KEY (ap_id) REFERENCES aps(ap_id) ON DELETE CASCADE
    "usuarios_x_ap_mac_fkey" FOREIGN KEY (mac) REFERENCES usuarios(mac) ON DELETE CASCADE
```

Tabla “aps”

Tabla “usuarios”

Tabla “usuarios_x_ap”

Figura 5-6 Tablas Relacionales - Gestor de Llaves

Elaboración Propia

Secuencia de eventos:

(1) En un momento inicial, el gestor de llaves no tiene información de los APs en la red. Se debe ingresar la dirección IP y el nombre de usuario del sistema OpenWRT en el AP a través del comando “add_ap” a través de la interfaz por línea de comandos del gestor de llaves (***Figura 5-7***).

(2) Una vez se han ingresado los datos de los APs, estos aún no han sido reconocidos por el gestor de llaves. Se debe ingresar el comando “start” con este fin. Se observa en la tabla “aps” que la columna “located” cambia de false a true cuando se ingresa el comando “start” (***Figura 5-7***). Esto indica que el gestor de llaves ha generado un enlace ssh hacia el AP de manera exitosa.

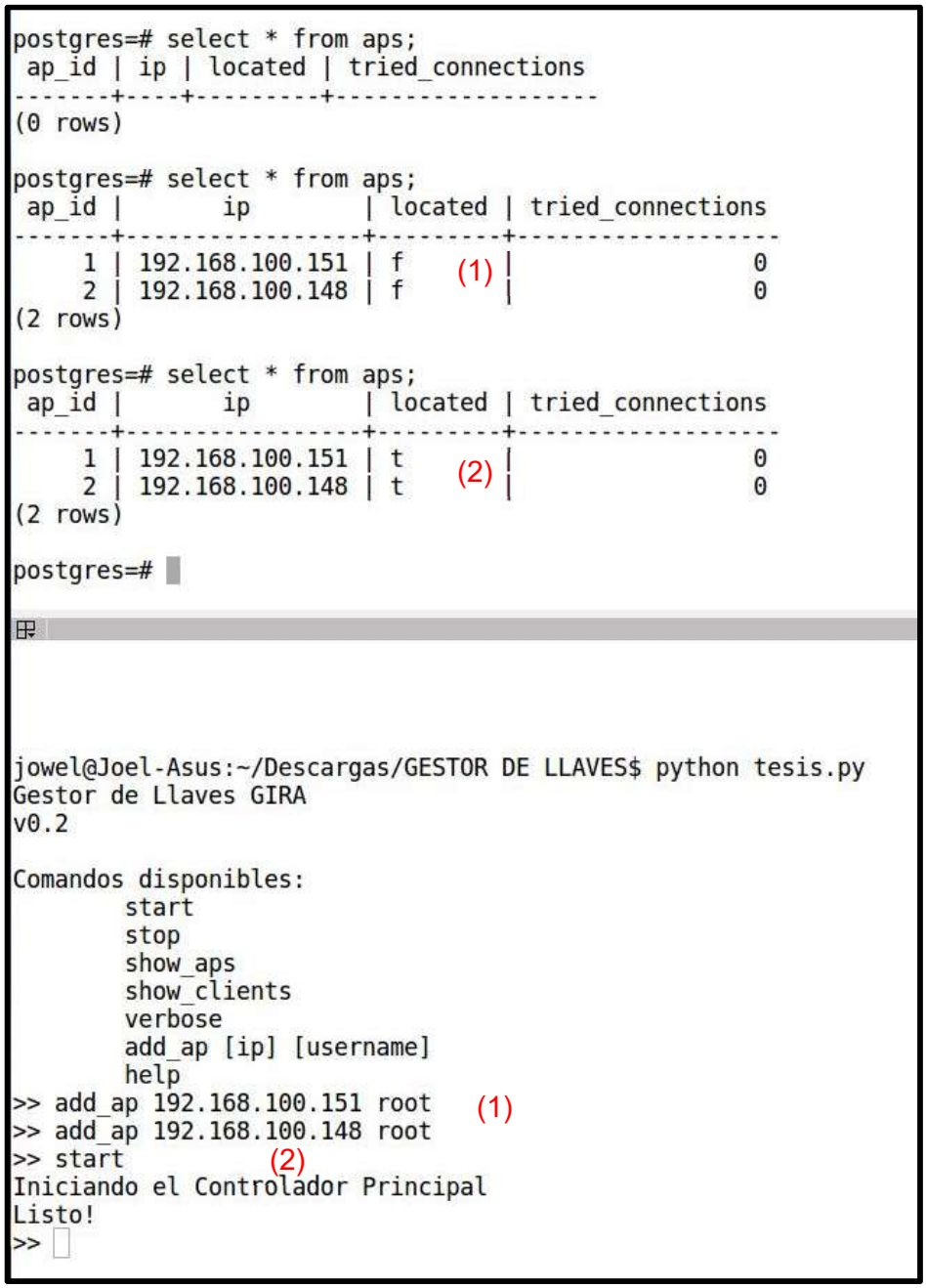


Figura 5-7 Inicialización de los APs en el Gestor de Llaves

Elaboración Propia

(3) La interfaz inalámbrica del Autenticador A se enciende y se apaga la interfaz inalámbrica del Autenticador B.

(4) El Suplicante Android se asocia a la red a través del Autenticador A, de modo que este último almacena la PMK del cliente en su memoria caché y genera un PMKID (***Figura 5-8***).

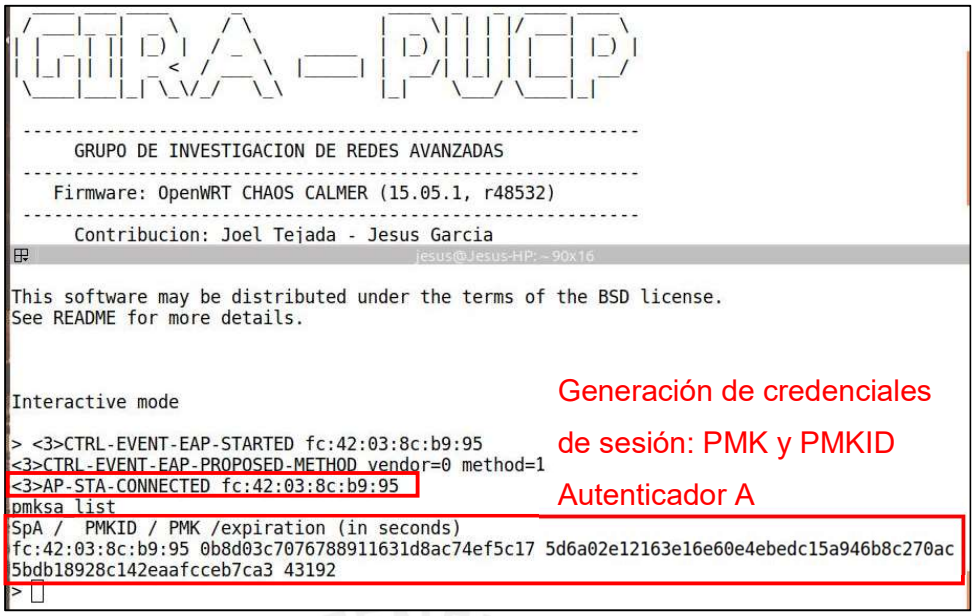


Figura 5-8 Asociación del Suplicante Android a la Red

(5) Se extraen la (MAC, PMK, PMKID y Tiempo de Expiración de la sesión) del cliente a través de una comunicación SSH realizada por el Gestor de Llaves (***Figura 5-9***).

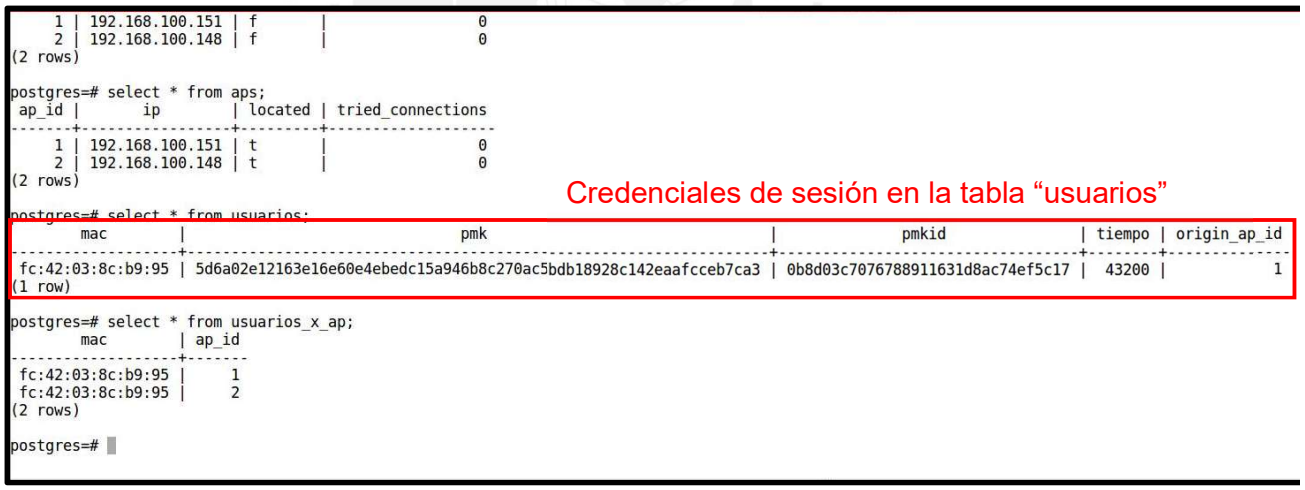


Figura 5-9 Gestión de las Credenciales de Sesión de Suplicante Android

(6) El Gestor de Llaves envía los datos del Suplicante Android (MAC, PMK, PMKID y Tiempo de Expiración de la sesión) y lo registra en la memoria caché del Autenticador B.

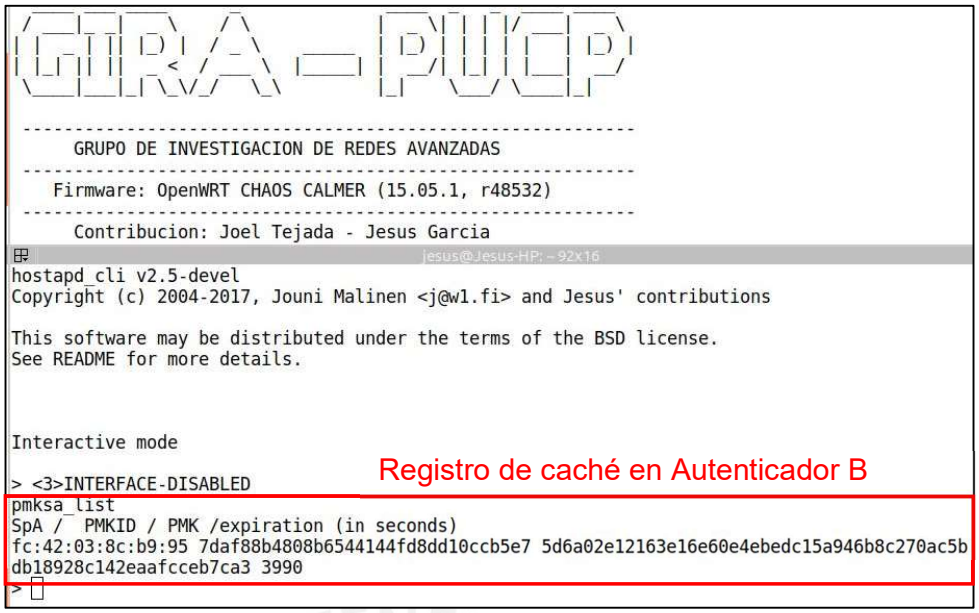


Figura 5-10 Distribución de Credenciales de Sesión del Suplicante Android

(7) Se apaga la interfaz inalámbrica del Autenticador A y el Suplicante Android inicia el proceso de Roaming hacia el Autenticador B.

(8) Se verifica, a través de línea de comandos del Autenticador B, la reasociación del cliente a la red (***Figura 5-11***).

De esta manera se comprueba el funcionamiento del gestor de llaves en la distribución de credenciales de sesión del usuario a través de los APs. Además, la ***Figura 5-11*** muestra la efectividad de la técnica de captura de llave. Una vez guardada en caché la PMK, es considerada información suficiente para el autenticador B para reconocer al suplicante como participante de la red y omitir el proceso de autenticación 802.1X/EAP-Radius.

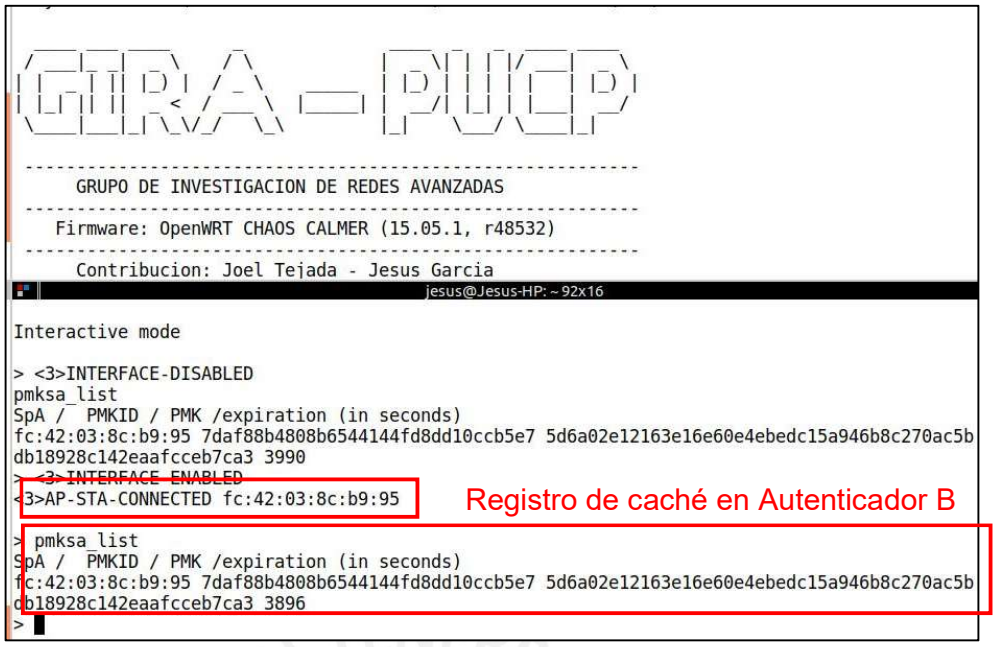


Figura 5-11 Roaming al Autenticador B – Uso del Capturador de Llave (Key Caching)

5.3 Análisis

En este apartado, se presenta el análisis de la implementación realizada. Se analiza, primero, la capacidad computacional de los puntos de acceso TP Link WDR3600 en cuanto a capacidad de usuarios que soporta. Luego, el impacto en hardware de las modificaciones de software que se realizaron en el punto de acceso.

5.3.1 Capacidad Computacional de los Puntos de acceso

Se realizaron pruebas de esfuerzo de la capacidad computacional del punto de acceso TP-Link WDR3600. Se asociaron dispositivos móviles y se procedió a producir trafico de internet, reproducción de videos en alta calidad (1080p) en Youtube, durante un periodo de 20 minutos. Para realizar esta prueba se utilizó el programa “htop” en su versión portada para el SO OpenWrt.

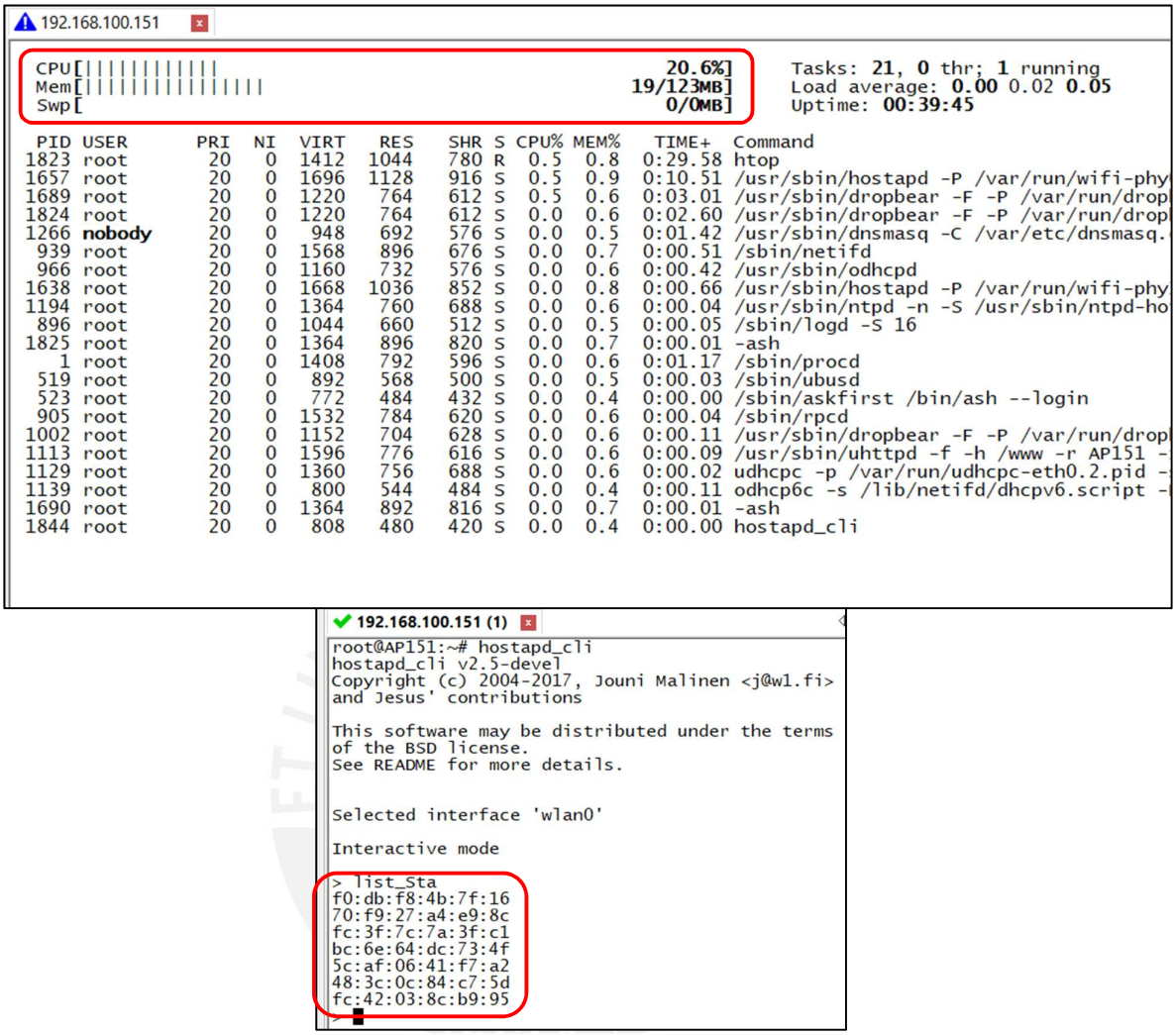


Figura 5-12 Análisis Capacidad Computacional del AP

Elaboración Propia

de 20.6% de la CPU, aunque se visualizaron picos de 33%. Estos picos de procesamiento, se asume, se deben a la generación de llaves dinámicas de encriptación que está definido a recalcularse cada 600 segundos. Entonces, si promedio de consumo de CPU es 20.6%, para utilizar el 100% de la capacidad del AP se deben asociar 33 dispositivos aproximadamente.

Sin embargo, utilizar la máxima capacidad del dispositivo generaría problemas en los momentos que el AP tenga que recalcular las llaves de encriptación. Por lo que el cálculo del número máximo de usuarios debe

realizarse con el 33% de consumo de AP. Con este valor, se calcula que, como máximo, se deben asociar 21 clientes al AP.

5.3.2 Memoria Caché Puntos de acceso

El espacio de memoria RAM disponible en los puntos de acceso TP-Link WDR3600 es de 90MB.

Cada entrada en caché de los usuarios cuenta con la siguiente información:

Detalle	Costo en bits
ID (considerando una buena practica de 20 usuarios max.)	6
MAC del Cliente	48
PMKID	128
PMK	256
Tiempo de Expiración de la sesión	19
TOTAL	**457**

Tabla 5-5 Costo en bits de entrada PMKSA por usuario

Elaboración Propia

Según la ***Tabla 5-5 Costo en bits de entrada PMKSA por usuario***, la información de la PMKSA de cada usuario tiene un costo en memoria de 457 bits. Considerando 21 usuarios conectados a cada AP en una red de 100 APs (máximo número de APs considerado dentro de una red intermedia [28]) se obtiene un total de 119.96 KB. Esto significa que, aún en el caso límite de acuerdo con los requerimientos de diseño, el impacto en memoria del almacenamiento de PMKSAs en caché es casi nulo (90MB >> 0.12 MB).

CONCLUSIONES

- Se cumplió con el objetivo principal de la tesis, se diseñó un sistema de *Roaming Rápida y Segura* y se implementó una prueba de concepto utilizando software de código abierto.

- El sistema diseñado logra minimizar el tiempo de Roaming, en su fase de ejecución, a menos de 150 ms, en la fase de ejecución. A través de pruebas, se logra medir que el tiempo promedio de Roaming es 19 ms. Este tiempo es menor al retardo de Roaming cuando se utiliza un entorno *legado*.

- El diseño propuesto cumple con el objetivo de minimizar el tiempo de Roaming sin modificación alguna en el cliente. Los dispositivos clientes que pueden beneficiarse del diseño propuesto son aquellos que soporten el método OKC, el cual es bien aceptado comercialmente.

- La implementación realizada permite lograr una solución interoperable entre equipos de distintos proveedores con distintas arquitecturas ya que se trabajó sobre un sistema POSIX.

TRABAJO A FUTURO

- Implementación de módulos complementarios. La implementación realizada se enfocó en modificar y elaborar código para minimizar el tiempo de iteración. Sin embargo, se tuvo en cuenta las implicancias de la iteración y se diseñaron los módulos de redescubrimiento de la LAN y respaldo ante pérdida de paquetes, los cuales queda pendientes de implementar.

- Desarrollo de interfaz gráfica para monitoreo de APs. Se implementó un gestor de llaves centralizado en Python, el cual puede monitorear la cantidad y ubicación de los usuarios dentro de la red. A este desarrollo se le puede agregar una interfaz gráfica que sea amigable al administrador de la red.

- Integrar el gestor de llaves en un entorno distribuido. Se propuso una arquitectura centralizada para la gestión de las credenciales de sesión de los dispositivos clientes. Sin embargo, se puede diseñar un sistema, bajo el mismo concepto del capturador de llave (*key Caching)*, en un entorno distribuido. Para este diseño se debe tener en cuenta los protocolos de comunicación entre APs y los recursos en hardware que se requerirían.

- Integración de requerimientos al sistema. La implementación realizada resuelve el reto del roaming dentro de una red WLAN mediana. Sin embargo, no es el único reto presente en estas implementaciones. Se puede trabajar en módulos de software que resuelvan problemas como protección contra intrusos, interferencia de canales, entre otros e integrarlos al sistema implementado.

REFERENCIAS

[1] L. Badman y R. Bartz, CWSP - Certified Wireless Security Professional - Official Study Guide, Segunda Edición ed., CertiTrek Publishing, 2016.

[2] D. A. Westcott, D. D. Coleman, P. Mackenzie y B. Miller, Certified Wireless Analysis Professional - Official Study Guide, Indianapolis, Indiana: Wiley Publishing, Inc., 2011.

[3] W. Alliance, «WiFi Alliance,» [En línea]. Available: http://www.wi-fi.org/product-finder. [Último acceso: 26 Junio 2017].

[4] I. Cisco Systems, Enterprise Campus 3.0 Arquitecture: Overview and Framework, 2008.

[5] S. M. Jackman, M. Swartz, M. Burton y T. W. Head, CWDP Certified Wireless Design Professional, 2011.

[6] I. Cisco Systems, Real-Time Traffic over Wireless LAN Solution Reference Network Design Guide, 2013.

[7] J. M. Luaces Novoa, Seguridad en Redes Inalámbricas de Área Local (WLAN), Cataluña: Tesis, Especialidad en Telemática, Universitat Oberta de Cataluña, 2012.

[8] D. Coleman, D. Westcott, B. Harkins y S. Jackman, CWSP - Certified Wireless Security Professional, Primera Edición ed., S. Coyl y M. Burton, Edits., Indiana: Wiley Publishing, Inc., 2010.

[9] S. Frankel, B. Eydt, L. Owens y K. Scarfone, «Establishing Wireless Establishing Wireless - A Guide to IEEE 802.11i,» National Institute of Standards and Technology, Gaithersburg, 2007.

[10] W. Stalling, Cryptography and Network Security: Principles, 6ta ed., Pearson Education, Inc., 2014.

[11] D. Whiting, R. Housely y N. Ferguson, «RFC 3610 - Counter with CBC-MAC (CCM),» Network Working Group, 2003.

[12] N. I. o. S. a. Technology, «ADVANCED ENCRYPTION STANDARD (AES),» Federal Information Processing Standards Publications (FIPS PUBS), 2001.

[13] K. Nizam Khan y J. Rehana, «Wireless Handoff Optimization: A Comparison of IEEE 802.11r and HOKEY,» de *Lecture Notes in Computer Science, págs. 118 -131*, Springer, Berlin, Heidelberg, 2010.

[14] J. W. Przemysław Machań, «On the fast BSS transition algorithms in the IEEE 802.11r local area wireless networks,» *Telecommunication Systems,* vol. 52, nº 4, pp. 2713 - 2720, Abril 2013.

[15] M. S. Bargh, R. J. Hulsebosh, E. H. Eertink, A. Prasad, H. Wang y P. Schoo, «Fast Authentication Methods for Handovers between IEEE 802.11 Wireless Lans,» de *WMASH '04: Proceedings of the 2nd ACM international workshop on Wireless mobile applications and services on WLAN hotspots*, Nueva York, 2004.

[16] A. Balasubramanian, R. Mahajan, A. Venkataramani, B. N. Levine y J. Zahorjan, «Interactive WiFi Connectivity For Moving Vehicles,» *Computer Communication Review,* vol. 38, nº 4, pp. 427 - 438, 2008.

[17] A. Giannoulis, M. Fiore y E. W. Knightly, «Supporting Vehicular Mobility in Urban Multi-hop Wireless Networks,» de *Proceedings of the 6th international conference on Mobile systems, applications, and services, págs. 54-66*, 2008.

[18] I. The Institute of Electrical and Electronics Engineers, IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, New York: IEEE, 2012.

[19] T. Charles Clancy, «Secure handover in enterprise WLANs: capwap, hokey, and IEEE 802.11R,» *IEEE Wireless Communications,* vol. 15, nº 5, pp. 80-85, 17 Octubre 2008.

[20] W. Alliance, «Wi-Fi® calling in the spotlight: Consumer, enterprise, and service provider benefits,» WiFi Alliance, 2015.

[21] J. Manner y M. Koji, «Mobility Related Terminology,» IETF RFC 3753, 2004.

[22] M. I. Sanchez y A. Boukerche, «On IEEE 802.11k/r/v Amendments: Do They Have a Rea l Impact?,» *IEEE Wireless Communications,* vol. 23, nº 1, pp. 48 - 55, 02 Marzo 2016.

[23] TP-Link, «TP-Link,» [En línea]. Available: http://www.tp-link.es/products/details/TL-WDR3600.html#specifications. [Último acceso: 18 Junio 2017].

[24] FreeRadius, «FreeRADIUS Technical Guide,» [En línea]. Available: http://freeradius.org/. [Último acceso: 22 Junio 2017].

[25] J. Berg, «Linux Wireless,» [En línea]. Available: http://linuxwireless.org/en/developers/Documentation/. [Último acceso: 17 Junio 2017].

[26] K. Georgantas, Fast Initial Authentication, a New Mechanism to Enable Fast WLAN Mobility, Estocolmo: Tesis, School of ICT, Royal Institute of Technology, 2011.

[27] D. Community, «w1.fi,» [En línea]. Available: http://w1.fi/hostapd/devel/index.html. [Último acceso: 10 Junio 2017].

[28] Cisco, «Cisco,» [En línea]. Available: http://www.cisco.com/c/dam/assets/prod/wireless/cisco-wireless-selector-tool/index.html#/wireless. [Último acceso: 23 Mayo 2017].

[29] D. Hucaby, CCNA Wireless 640-722 Official Cert Guide, Indiana: Cisco Press, 2014.

[30] R. López Barnés, Red Basada en Acceso Inalámbrico (WiFi & WiMAX), Madrid: Universidad Autónoma de Madrid - Escuela Politécnica Superior, 2008.

[31] R. Amado Gimenez, Análisis De La Seguridad En Redes 802.11, Valencia: Universitat de València - Escola Tècnica Superior D'enginyeria, 2008.

[32] P. Machan y J. Wozniak, «Performance Evaluation of IEEE 802.11 Fast BSS Transition Algorithms,» de *Wireless and Mobile Networking Conference (WMNC), 2010 Third Joint IFIP*, Budapest, 2010.

[33] H. Dolorico Balbi, F. Rolim e Souza, R. Campanha Carrano, C. Schara Magalhães, C. V. Neves de Albuquerque, D. C. Muchaluat Saade, L. Ribas do Nascimento y C. Cagliano, «SciFi – Sistema de Controle Inteligente para Redes sem Fio - Manual do Controlador V2,» Rede Nacional de Ensino e Pesquisa - RNP, Niterói, 2013.

[34] L. C. Schara Magalhães, «SCIFI2 – Sistema de Controle Inteligente para Redes sem Fio 2,» Rede Nacional de Ensino e Pesquisa, Niterói , 2011.

[35] C.-I. Fan, Y.-H. Lin y R.-H. Hsu, «Complete EAP Method: User Efficient and Forward Secure Authentication Protocol for IEEE 802.11 Wireless LANs,» *IEEE Transactions on Parallel and Distributed Systems,* vol. 24, nº 4, pp. 672 - 680, Abril 2013.

[36] R. A. De Araujo Marques, Security and Mobility in 802.11 Structured Networks, Aveiro: Tesis, Departamento de Electrónica, Telecomunicaciones e Informática, Universidad de Aveiro, 2008.

[37] S. Bangolae, C. Bell y E. Qi, «Performance study of fast BSS transition using IEEE 802.11r,» de *IWCMC '06 Proceedings of the 2006 international conference on Wireless communications and mobile computing, págs. 737-742*, Vancouver, 2006.