UNIVERSIDAD CARLOS III DE MADRID

ESCUELA POLITÉCNICA SUPERIOR

GRADO EN INGENIERíA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

ANÁLISIS DEL EFECTO DE LA ALEATORIZACIÓN DE LAS DIRECCIONES MAC DE LAS ESTACIONES EN IEEE 802.11R

PROYECTO FIN DE GRADO

Autor: Carlota Villasante Marcos
Tutor: Antonio de la Oliva Delgado

27 de septiembre de 2015

Agradecimientos

Me gustaría dedicar esta sección para dar las gracias a todas las personas que han hecho posible la realización de este proyecto y me han apoyado desde el principio.

A Carlos, por creer en mí en todo momento, por el tiempo robado leyendo y releyendo la memoria y por haberme animado en los momentos más difíciles.

A los compañeros que me han apoyado dando ánimos para realizar este trabajo.

A Carlos Donato, que posiblemente haya sido un elemento clave, por haberme enseñado a pegarme con los dispositivos y no tener miedo a manejarlos. Y también a Alberto Gordillo, por haberme socorrido en los momentos de crisis.

A mi tutor, Antonio, que ha sabido guiarme durante el proyecto a pesar de su alta carga de trabajo. Siempre ha estado dispuesto para atenderme y animarme a terminar el proyecto.

Y un especial agradecimiento a mis padres, que me han enseñado a dar lo mejor de mí y a esforzarme para conseguir los objetivos propuestos. Por haber estado presentes en las buenas y malas situaciones, por haber estado presentes siempre.

A todos vosotros, gracias.

Abstract

Nowadays, many devices incorporate wireless technology such as laptops, cellular phones, VoIP phones and MP3 players. Each of these portable devices have a unique hardware identifier called Media Access Control (MAC) address. Several organizations noticed these identifiers are trackable, therefore, the user could be followed. The discovery of this possible threat, has resulted in an urgent need to search for a solution which somehow could avoid this situation. The purpose of this paper is to present the analysis of an on-going solution proposed by the Institute of Electrical and Electronics Engineers (IEEE) 802 EC Privacy Recommendation Study Group in a wireless network with IEEE 802.11r support.

Listado de acrónimos

AA Access point Address.

AAD Additional Authentication Data.

ACK Acknowledgement.

AES Advanced Encryption Standard.

AIEE American Institute of Electrical Engineers.

AKM Authentication Key Management.

AMD Advanced Micro Devices, Inc.

ANonce Authenticator Nonce.

AP Access Point.

ARC4 Alleged Rivest Cipher 4.

AS Authentication Server.

ASCII American Standard Code for Information Interchange.

BSD Berkeley Software Distribution.

BSS Basic Service Set.

CBC Cipher-Block Chaining.

CBC-MAC Cipher-Block Chaining Message Authentication Code.

CCMP Counter Mode with Cipher-Block Chaining Message Authentication Code Protocol.

CRC Cyclic Redundancy Check.

CSD Criteria for Standards Development.

CSMA/CA Carrier Sense Multiple Access with Collision Avoidance.

CSMA/CD Carrier Sense Multiple Access network with Collision Detection.

CTR CounterMode.

CTS Clear-To-Send.

DA Destination Address.

DCF Distributed Coordination Function.

DS Distribution System.

DSS Distribution System Service.

DSSS Direct-Sequence Spread-Spectrum.

EAP Extensible Authentication Protocol.

EAP-PEAP EAP-Protected Extensible Authentication Protocol.

EAPOL EAP over LAN.

EC Executive Committee.

ESS Extended Service Set.

FCS Frame Check Sequence.

FDDI Fiber Distributed Data Interconnect.

FHSS Frequency-Hopping Spread-Spectrum.

FT Fast Basic Service Set Transition.

FTAA FT Authentication Algorithm.

FTIE Fast BSS Transition Information Element.

GTK Group Temporal Key.

GUI Graphical User Interface.

HR/DSSS High-Rate Direct-Sequence.

IAB Internet Architecture Board.

IBSS Independent BSS.

ICV Integrity Check Value.

IEEE Institute of Electrical and Electronics Engineers.

IETF Internet Engineering Task Force.

IFS InterFrame Spaces.

IRE Institute of Radio Engineers.

ISO International Organization for Standardization.

IV Initialization Vector.

LAN Local Area Networks.

LLC Logical Link Contro.

LMSC 802 LAN/MAN IEEE Standards Committe.

MAC Media Access Control.

MAN Metropolitan Area Networks.

MDC Mobility Domain Controller.

MDI Mobility Domain Identifier.

MDIE Mobility Domain Information Element.

MIB Management Information Base.

MIC Message Integrity Code.

MMPDU Management MAC Protocol Data Unit.

MPDU MAC Protocol Data Unit.

MSDU MAC Service Data Unit.

MSK Master Session Key.

NIST National Institute of Standards and Technology.

OFDM Orthogonal Frequency Division Multiplexing.

OSI Open System Interconnection.

PAR Project Authorization Request.

PCF Point Coordination Function.

PEAP Protected Extensible Authentication Protocol.

PING Packet InterNet Groper.

PLCP Physical Layer Convergence Procedure.

PMD Physical Medium Dependent.

PMK-R1 Pairwise Master Key R1.

PMK-R0 Pairwise Master Key R0.

PN Packet Number.

PPDU PLCP Protocol Data Unit.

PRF Pseudorandom Function.

PSDU PLCP Service Data Unit.

PSK Pre-Shared Key.

PTK Pairwise Transient Key.

QoS Quality of Service.

RADIUS Remote Authentication Dial-In User Service.

RSN Robust Security Network.

RSNA Robust Security Network Associations.

RTS Request-To-Send.

SA Source Address.

SBC Session Border Controller.

SG Study Group.

SNMP Simple Network Management Protocol.

SNonce Supplicant Nonce.

SQL Structured Query Language.

SS Station Service.

SSID Service Set Identifier.

STA Station.

TA Transmit Address.

TKIP Temporal Key Integrity Protocol.

TLS Transport Layer Security.

TSC TKIP Sequence Counter.

TTAK TKIP-Mixed Transmit Address and Key.

UDP User Datagram Protocol.

VPN Virtual Private Network.

WECA Wireless Ethernet Compatibility Alliance.

WEP Wired Equivalent Privacy.

WG Working Group.

Wi-Fi Wireless Fidelity.

WLAN Wireless Local Area Networks.

WPA Wi-Fi Protected Access.

WPS Wi-Fi Protected Setup.

Índice general

Índice de figuras

Índice de cuadros

Capítulo 1

Introduction

In this chapter, the main aspects of this project are discussed, such as aims, scope and the motivation to perform it. Additionally, an overview about the socioeconomic impact and the regulatory framework is provided. Afterwards, the dissertation structure is detailed in order to let the reader know each chapter's content.

1.1. Motivation of the project

The mass deployment of IEEE 802.11 [30] based Wireless Local Area Networks (WLAN), and increased sales in portable devices, has heightened the risk of being attacked or having threatened our privacy. Two major threats to our privacy are due to correlation, combinations of certain user data; and identification, register in a WLAN with particular individual information.

The security methods that are available nowadays, protect the inside data with ciphers and keys but it is the outside data which is in danger, this is Metadata. Metadata contains information like where the client is sending his details from, who he is sending it to and, more importantly, who he is .

Each mobile device has an identifier and an address that is being registered everywhere the device goes with the wireless interface turned on. A request message, defined in the standard IEEE 802.11, contains this information that is required to be sent to each Access Point (AP) in an area to try to associate it with. It is not necessary to establish a full wireless connection, even though, if a device is associated with an access point, a tracker could know how long you have been there and guess where you are heading to next.

1.1.1. IEEE 802 Study Group

These type of privacy issues raised the interest within the IEEE 802 community. On 18 July 2014, the IEEE 802 Executive Committee (EC) created an IEEE 802 EC Privacy Recommendation Study Group (SG) [53]. The SG studies privacy issues related to IEEE 802 technologies and the need for changes or amendments in IEEE 802 protocols. The standards drawback is that they require unanimity, consensus, and could take years for a

solution to settle. The principal lines of work that the SG is working on are:

1. **IEEE 802 Project Authorization Request (PAR)/Criteria for Standards Development (CSD) Text on Scope and Purpose**
2. **Threat Model for Privacy at Link Layer**
3. **Privacy Issues at Link Layer**
4. **Proposals regarding functionalities in IEEE 802 protocols to improve Privacy**
5. **Proposals regarding measuring levels of Privacy on Internet protocols**
6. **Implications of MAC address changes**
7. **Other privacy-related topics**

This paper focuses on the sixth line of work, Implications of MAC address changes. To minimize the likelihood of being tracked, the main target is that the device producers develop random identifiers for their own products. In the meantime, there exists some softwares that while you are not connected to a wireless network, the MAC address will constantly be pseudo-randomized, preventing trackers to encounter your real MAC address. Some examples are, Pry-Fi for Android, IOS 8 operating system and Windows 10.

These softwares send a message request to the available Service Set Identifier (SSID), when the Wi-Fi connection is not established yet, to let them know the client wants to authenticate it. Each message request has a new random MAC address. Also, they spoof their MAC address when changing from one wireless network connection to another.

Randomizing the MAC address without having established a full wireless connection does not cause any difficulty or problem facing connectivity, as the device is associating after changing its identifier. Therefore, an analysis of the network's behaviour and possible errors that could be originated performing a MAC address spoofing during a wireless connection, when the client is associated to an AP, was an important phenomenon to study.

1.2. Aims and Project scope

The main purpose of this project is the effects analysis, during a wireless connection, of a MAC address randomization. The more that is known about the possible behaviour and process, the easier it would be to get to a solution, a consensus. Therefore, this project was intended with the next objetives in mind:

- In order to accomplish this study, the development of an IEEE 802.11 wireless network is required.
- Concerning user's mobility and roaming, implement support for IEEE 802.11r [35] or also called Fast BSS Transition.
- Perform MAC address spoofing.
- Test the network and the possible scalability issues that may arise.

1.3. Societal and economic impact analysis and Regulatory framework

Every day, people are connecting and sending more data through WLANs, also, are traveling with their Wi-Fi connection on, therefore, having systems that protect all that information in a reliable way is becoming more and more relevant.

IEEE 802 Privacy Recommendation SG is working with other organizations to take a closer look at potential threats that expose or threaten privacy. Internet Engineering Task Force (IETF) [14], Internet Architecture Board (IAB) [13], National Institute of Standards and Technology (NIST) [17], Cisco [4] and IntelDigital members made IEEE 802 aware of the situation with a worldwide conference, since then all of them are working to reach a solution.

Changing a whole standard could seem a little drastic so the Study Group is working on new amendments that could minimize the danger. Setting random identifiers could be used as a commercial plus by the vendors, because clients do not want to be tracked. Although, many applications work with the physical device identifier and would get obsolete if the implementation changes.

Multiple things have to be under consideration before making any changes, but first a wide study and analysis has to be done.

1.4. Dissertation structure

The current document is organized into seven chapters and several appendices. In this section there will be a brief explanation of each chapter in order to guide the reader. At the beginning, a list of acronyms is defined and they will appear in the following chapters:

- **Chapter 1.** The reader will find an introduction concerning the motivations and the project's origin, as well as, the project scope and goals. Moreover, some information about social, economic and regulatory framework context surrounding this project is provided.
- **Chapter 2.** A State of the art covering the important parts from IEEE 802.11r [35] and security is provided, in order to explain the most relevant information so that the reader can understand the project.
- **Chapter 3.** Concerning the project's design, software tools and hardware equipment are defined.
- **Chapter 4.** The configurations to be implemented in each device are also provided.
- **Chapter 5.** Scalability Tests and their explanations are documented in this section, in order to check that the network works properly and to perform the analysis.
- **Chapter 6.** This chapter presents the time planning followed during the development of the project, as well as an economic analysis presenting the budget required to perform this study.

- **Chapter 7.** Provides an overall evaluation of the project, that gathers the author's conclusions, difficulties suffered during the deployment and possible future lines of work.

Furthermore, a list of appendices are provided. An extended summary is located first, a deep introduction to IEEE 802.11 networks is provided next, as it would be useful for those who barely know about them; the organization Wi-Fi Alliance is defined and some configurations and explanations for softwares used on the project are pointed out.

Later on, the reader can find a glossary, to clarify some technical terms; and a bibliography, that provides the list of resources used during the writing of this paper.

Capítulo 2

Estado del Arte

2.1. IEEE 802.11

Las redes basadas en el estándar IEEE 802.11 WLAN han sufrido un crecimiento importante a lo largo de los años y se han convertido en el método preferido por los usuarios para acceder a Internet. El estándar 802.11 original se publicó en Junio de 1997, llamado IEEE Std. 802.11-1997 [30], y fue el primer estándar WLAN.
El Institute of Electrical and Electronics Engineers (IEEE) define las tecnologías 802.11 en el Nivel Físico y en la subcapa Media Access Control (MAC) del Nivel de Enlace del modelo Open System Interconnection (OSI). La introducción del estándar IEEE 802.11 supuso un gran impacto para la cobertura de red en hogares, oficinas y áreas públicos.

Para realizar un análisis de una red inalámbrica, es necesario un amplio conocimiento de la arquitectura de redes 802.11, servicios ofrecidos y tipos de tramas. En el Apéndice B se proporciona una visión general de estos temas, mientras que aquí sólo se incluye la información más relevante para este trabajo.

2.2. Movilidad a Nivel 2 en IEEE 802.11

La movilidad es la mayor motivación para crear una red IEEE 802.11 [30], las estaciones pueden mantenerse conectadas a la red mientras se mueven por ella. Hay tres formas de transición existentes:

Sin transición
Si una estación no sale del área de cobertura de su punto de acceso, no hace falta realizar una transición. Esto ocurre si una estación no se mueve o se está moviendo dentro del Basic Service Set (BSS) del punto de acceso asociado.

Transición BSS
Las estaciones están constantemente evaluando la fuerza y calidad de la señal de los puntos de acceso asignados para cubrir una Extended Service Set (ESS). IEEE 802.11 [30] provee de movilidad de enlace MAC, las estaciones enganchadas al Distribution System (DS) pueden enviar direcciones de tramas a direcciones MAC de estaciones móviles y

dejar que el punto de acceso asociado se encargue del paso final de la transmisión. El DS no tiene por qué saber la localización exacta de una estación móvil mientras se encuentre dentro de una misma ESS.

BSS transition requiere la cooperación entre los puntos de acceso, el nuevo punto de acceso asociado debe informar al anterior que la estación se encuentra en su área. IEEE 802.11 [30] no especifica los detalles de la comunicación entre los puntos de acceso cuando se realiza una BSS transition.

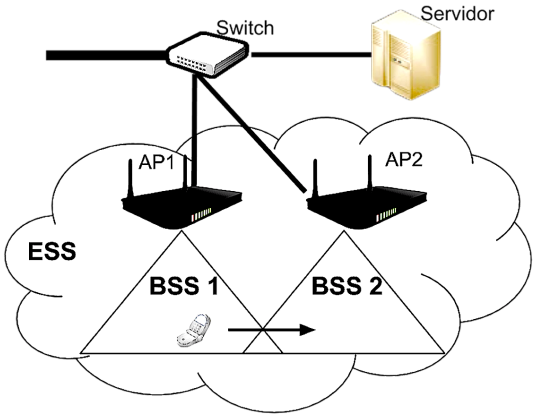

Figura 2.1: Representación de una Transición BSS.

***Transición* ESS**

Este proceso se refiere al movimiento de una estación móvil de una ESS a otra ESS diferente. IEEE 802.11 [30] no soporta este tipo de movimiento, excepto la asociación con un punto de acceso de otro ESS cuando ha dejado de estar asociado previamente del anterior. Los movimientos que se realizan en capas superiores del Modelo OSI se interrumpen antes de llevarse a cabo, necesitan un soporte adicional de los protocolos de esos niveles.

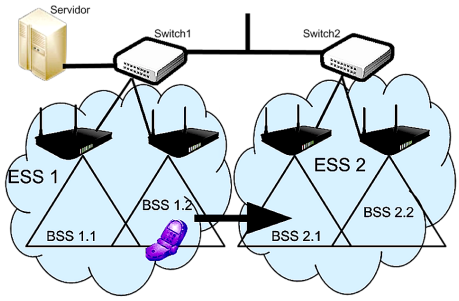

Figura 2.2: Representación de una Transición ESS.

2.2.1. Características

La movilidad es la cualidad de poder moverse con libertad de un punto a otro, en las redes IEEE 802.11 [30] la movilidad se define como el movimiento de una estación, Station (STA), o cliente de un punto de acceso (Access Point (AP)) a otro dentro de una misma ESS, llamado también *roaming* o itinerancia.

El roaming en una red IEEE 802.11 [30] es conocido como "break before make" ya que debe romper la asociación con un AP para poder asociarse a otro. Esto facilita tener un protocolo MAC y de radio más sencillo.

Los puntos de acceso que se encuentran en el mismo dominio broadcast y tienen por ello el mismo *Service Set Identifier (*SSID*)*, pertenecen al mismo dominio roaming denominado dominio Layer-2 o dominio de Capa-2. Este dominio abarca el espacio de una ESS y dónde se puede realizar la transición BSS. Para dar por completado el roaming deben suceder cuatro estados:

- **El cliente decide realizar el movimiento**: El mecanismo para saber cuándo se debe hacer roaming no está en las especificaciones del IEEE 802.11 y por ello cada fabricante decide como implementarlo. Aunque al principio supuso un fuerte problema de escalabilidad e interoperabilidad, estos han trabajado unidos para asegurar compatibilidad entre los productos IEEE 802.11. El hecho de que se deje la implementación a los fabricantes, les otorga la posibilidad para diferenciarse, crear nuevos y mejores algoritmos que sus competidores. Suelen regirse por factores como la calidad de la señal, las tramas Acknowledgement (ACK) recibidas, *beacons*, etc.
- **El cliente decide a dónde se va a mover**: Tampoco está especificado cómo se decide dónde debe asociarse una estación cuando realiza un movimiento, el vendedor decide la implementación de este proceso. La estación debe decidir a que punto de acceso es correcto asociarse, se realiza mediante el escáner del medio. Puede realizarse antes de tomar la decisión de moverse, de forma preventiva; *preemptive* AP *discovery*, o después de tomar la decisión; *roam-time* AP *discovery*. Este proceso utiliza uno o los dos medios de escáner:
  - Activo – El cliente busca activamente un nuevo punto de acceso, siendo el método más rápido. Este proceso conlleva que el cliente mande *probe requests* y espere a que los APs contesten con *Probe Response*. Cuando recibe contestación, el cliente decide que AP es el correcto.

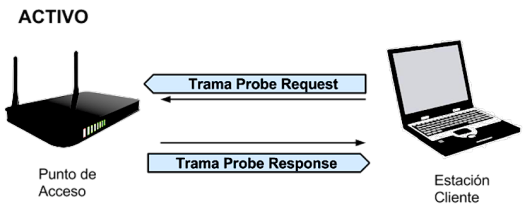

Figura 2.3: Representación método escáner Activo.

- Pasivo – El cliente escucha durante un tiempo los diferentes canales y recibe los *beacons* que envían los diferentes puntos de acceso. Una vez recibidos las tramas *beacon*, el cliente decide cual es el punto de acceso más optimo.

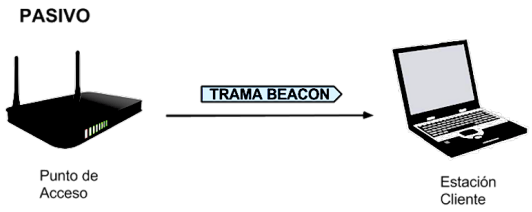

Figura 2.4: Representación método escáner Pasivo.

No hay ninguna forma ideal de realizar el escáner. El modo pasivo tiene la ventaja de no requerir el envío de mensajes por parte del cliente, como pasa en el modo activo, pero se puede dar la pérdida de un AP porque no haya mandado un *beacon* durante el tiempo de escáner.

- **Se inicia el movimiento**: La estación utiliza los servicios de red authentication y reassociation para asociarse al nuevo punto de acceso.
- **El cliente retoma las sesiones**.

2.2.2. Proceso roaming

El acto de roaming incluye más procesos que buscar un nuevo punto de acceso con el que comunicarse, algunas de las tareas son:

1. El AP anterior (AP1) debe cerciorarse que la estación móvil (STA) se ha movido a otra área.
2. El AP1 debe guardar la información que vaya dirigida a la STA que se haya movido.
3. El nuevo punto de acceso (AP2) debe informar al AP1 que la STA ha realizado con éxito el roaming. Este paso suele realizarse mediante un paquete unicast o multicast enviado desde AP1 a AP2 con la dirección MAC de la STA.
4. AP1 debe mandar la información guardada a AP2.
5. AP2 debe actualizar las tablas de dirección MAC en los switches de la infraestructura para evitar la pérdida de paquetes.

Ya que el estándar IEEE 802.11 no define la comunicación AP-a-AP mediante el DS, se deja que los fabricantes de AP creen sus propias implementaciones. Dependiendo del fabricante, el mecanismo puede enviar una trama unicast o multicast con la dirección MAC del origen del cliente y la dirección MAC destino del AP, informando al AP1 del movimiento y actualizando las tablas MAC de los conmutadores.

2.3. IEEE 802.11r

La regulación IEEE 802.11r [35] es conocida como Fast Basic Service Set Transition (FT), el nombre técnico para un roaming rápido y seguro (fast secure roaming). El mecanismo IEEE 802.11r [35] opera en un dominio de movilidad; en el mismo ESS; con mayor seguridad y rapidez. Algunos fabricantes se refieren a sus controladores Wireless Local Area Networks (WLAN) como controladores del dominio de movilidad , *Mobility Domain Controller (*MDC*).*

La primera vez que la estación cliente entre en el dominio, se asociará con un AP y comenzará una autenticación 802.1X [37]. Desde ese punto en adelante, cuando la estación se mueva por los puntos de acceso, el cliente estará usando transiciones FT BSS.

Para conseguir realizar este roaming, los mecanismos FT necesitan los elementos de información Robust Security Network (RSN) para indicar la clave de autenticación especifica, *Authentication Key Management (*AKM*)*, y el cifrado por pares, *pairwise cipher*, que se están intercambiando entre el punto de acceso y la estación. La regulación añade cuatro elementos de información nuevos, los dos más importantes son:

- El elemento de información del dominio, Mobility Domain Information Element (MDIE), se usa para indicar la existencia del dominio al igual que el método FT. El campo del identificador del dominio, Mobility Domain Identifier (MDI), es el identificador único de los APs que constituyen un dominio. La capacidad FT y el campo de política se usan para indicar de que tipo es el FT que se va a realizar.

- El elemento de información del FT, Fast BSS Transition Information Element (FTIE), incluye la información necesaria para realizar una autenticación FT durante el roaming.

En la asociación inicial FT (FT initial mobility domain association) la estación cliente intercambia con el punto de acceso las tramas request/response de la autenticación IEEE 802.11 Open System. Después, intercambian la información MDIE y FTIE en las tramas request/response de la asociación para indicar la utilización del proceso FT en un futuro.

Un intercambio 802.1X/Extensible Authentication Protocol (EAP) [37]/[39] original entre una estación y el servidor Remote Authentication Dial-In User Service (RADIUS)[45] debe ocurrir para que el FT 4-Way Handshake pueda realizarse y así crearse las claves de encriptación Pairwise Transient Key (PTK) y Group Temporal Key (GTK). También se crea la clave de sesión, Master Session Key (MSK), que se usa para la jerarquía de la clave FT. El proceso inicial de asociación FT no es muy diferente al proceso inicial de los clientes pre-802.11r, la principal diferencia es la información extra que se intercambia, como el MDIE y FTIE.

Un pequeño resumen del proceso de jerarquía de la clave sería el siguiente:

- La MSK se crea en el intercambio inicial entre el cliente y el autenticador en la fase de autenticación, es el principio del proceso de jerarquía de la clave FT. Cuando se

usa WPA2-Pre-Shared Key (PSK) [43] en vez de una autenticación EAP [39], el PSK es básicamente la MSK.

- Se desarrolla una clave Pairwise Master Key R0 (PMK-R0) que proviene de la MSK, es la clave del primer nivel del proceso FT.
- Una clave de segundo nivel Pairwise Master Key R1 (PMK-R1), se deriva de la PMK-R0.
- El tercer y último nivel del proceso es el PTK, que es la ultima clave para encriptar las tramas de datos IEEE 802.11 unicast.

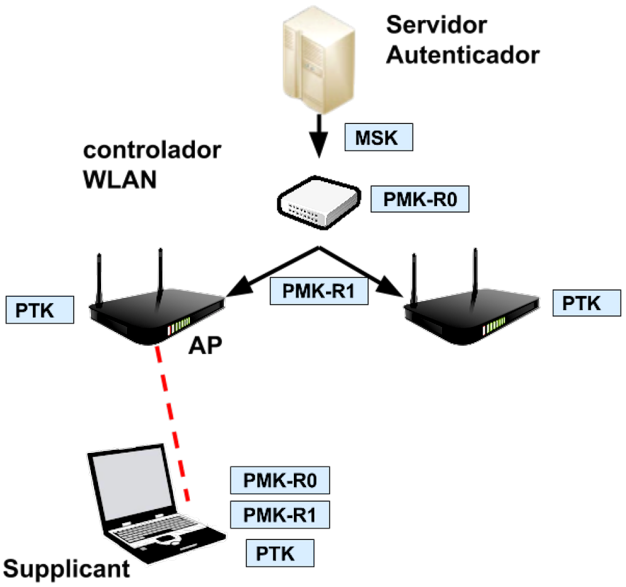

Figura 2.5: Representación proceso de jerarquía de las claves.

Tras la asociación inicial, dos nuevos métodos se definen para que una estación cliente pueda moverse entre los AP. Las transiciones FT BSS pueden ser "por el aire" (over-the-air) o "por el DS" (over-the-DS).

2.3.1. Over-the-Air FT BSS

El intercambio de tramas entre la estación cliente y un punto de acceso empieza con el intercambio de las tramas de autenticación Open System y las tramas de asociación. Son un total de cuatro tramas, sin incluir los ACKs. Después el intercambio 802.1X/EAP entre el supplicant y el servidor RADIUS, que requiere varias tramas. Para finalizar, el intercambio 4-Way Handshake se necesita para crear la encriptación dinámica final de las claves. Ya sabemos que el propósito FT y de otras técnicas de roaming rápido es eliminar la necesidad del intercambio 802.1X/EAP cada vez que el cliente se mueve, aunque las

tramas de autenticación y reasociación seguirán apareciendo.

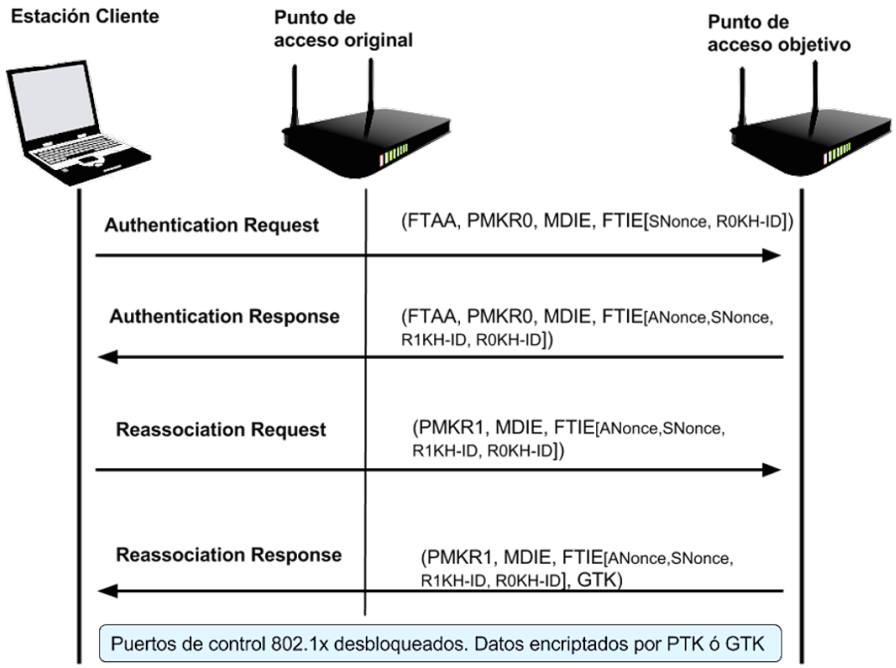

Figura 2.6: Representación Intercambio de mensajes Over-the-Air.

Las tramas request/response de autenticación y las tramas request/response de reasociación llevan una carga con un algoritmo de autenticación FT, *FT Authentication Algorithm (*FTAA*)*, junto con números aleatorios, nonces, y otro tipo de información. En este tipo de transición, la STA cliente se comunica directamente con el AP objetivo usando una autenticación estándar IEEE 802.11 con el FTAA. La clavePMK-R1 es el material que se envía para conseguir la clave final, PTK.

2.3.2. Over-the-DS FT BSS

La alternativa es el método over-the-DS fast BSS transition, que requiere el uso de tramas Action, en la infraestructura de cable IEEE 802.3 [34], para completar el proceso de creación PTK. Las tramas FT Action request/response se envían por el DS, pero las tramas de reasociación entre la STA y el AP se envían por el aire. Al igual que en el proceso anterior, la clave PMK-R1 se utiliza para crear el PTK.

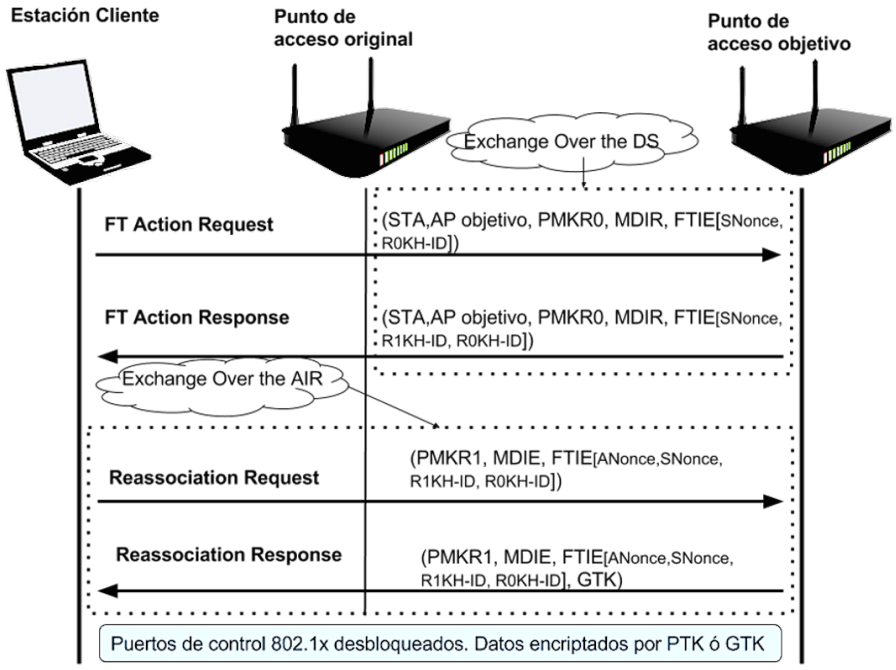

Figura 2.7: Representación Intercambio de mensajes Over-the-DS.

2.4. Seguridad en redes IEEE 802.11

Los mecanismos de seguridad del estándar IEEE 802.11 han sufrido muchos cambios desde sus inicios. Hay tres tipos de mecanismos de seguridad pre-RSNA: autenticación Open System, autenticación por clave compartida (*Shared Key authentication*) y encriptación Wired Equivalent Privacy (WEP). Estos tres métodos de seguridad y el más actual , RSN, están definidos en el estándar IEEE 802.11.

Se pueden diferenciar dos tipos claros de mecanismos, los dos primeros métodos pre-RSNA corresponden a la seguridad de cara a realizar una conexión, mientras que la encriptación WEP y métodos RSN definen la seguridad de la privacidad. Si bien los tres sistemas de seguridad pre-RSNA deberían estar obsoletos y ser evitados, siguen estando integrados en la mayoría de los dispositivos IEEE 802.11 para proporcionar compatibilidad con los equipos ya existentes.

A lo largo de los años, diferentes soluciones de seguridad que no aparecen en ningún estándar han sido implementadas para mejorar la seguridad de las redes inalámbricas o para compensar las deficiencias que pudieran existir en el estándar. Por ejemplo, Virtual Private Network (VPN) sobre red inalámbrica, Filtrado MAC, Segmentación del SSID, etc., que proporcionan mejoras y capacidades adicionales al estándar.

2.4.1. Mecanismos de seguridad pre-RSNA

Autenticación

Como ya sabemos, la autenticación es el primer paso de los dos que hay que realizar para conectarse a un BSS IEEE 802.11. Antes de que un cliente pueda pasar datos por la red debe autenticarse y asociarse, en ese orden, al BSS elegido. Nos referimos a la autenticación IEEE 802.11 que ocurre al nivel 2 del modelo OSI, una conexión inicial entre el punto de acceso y la estación móvil para validar que la STA es un dispositivo IEEE 802.11. Se definen dos tipos de autenticación: Open System y por clave compartida.

Autenticación Open System

La autenticación Open System es el único sistema de seguridad pre-RSNA que prevalece, es el método más simple de autenticación. Proporciona autenticación sin ningún tipo de verificación, es básicamente un saludo entre la STA y el AP. Se asume que los dispositivos tienen toda la información apropiada para conectarse a la red, es decir, toda estación será validada durante la autenticación Open System.

Dentro de un mismo BSS, este tipo de autenticación ocurre gracias a un intercambio de tramas entre la estación y el punto de acceso. Open System utiliza dos mensajes para realizar la autenticación, el cliente que busque unirse a un BSS manda el primer mensaje que contiene su identidad IEEE 802.11 y una petición de autenticación. El segundo mensaje contiene el resultado de autenticación y una vez terminado el intercambio, la estación se declara autenticada. Este proceso también se utiliza en una Independent BSS (IBSS), más comúnmente llamada *ad hoc* WLAN.

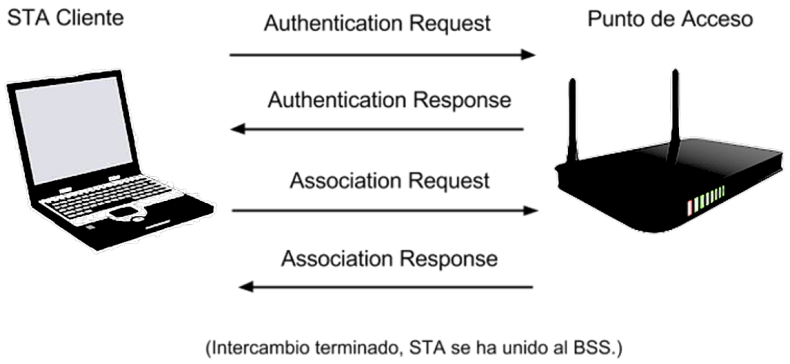

Figura 2.8: Proceso de autenticación y asociación con Open System.

La autenticación Open System ocurre después de que una estación sabe de la existencia de un AP mediante el escáner pasivo o activo. El proceso de autenticación debe de

completarse para que la asociación pueda llevarse a cabo. Una vez que la autenticación Open System y la asociación se realizan, el cliente establece una conexión a Nivel 2 con el punto de acceso y pasa a ser miembro del BSS.

La encriptación WEP es opcional con autenticación Open System, puede usarse para la protección de datos. WEP se utiliza únicamente para encriptar la carga MAC Service Data Unit (MSDU) de los Niveles 3-7 de las tramas de datos IEEE 802.11 y sólo cuando la estación cliente se ha autenticado y asociado, por lo que no es parte del proceso de autenticación.

La autenticación Open System no necesita ser segura ya que hay otros métodos de autenticación más avanzados, como la autenticación 802.1X/EAP, que realizan otro tipo de autenticación después de ésta.

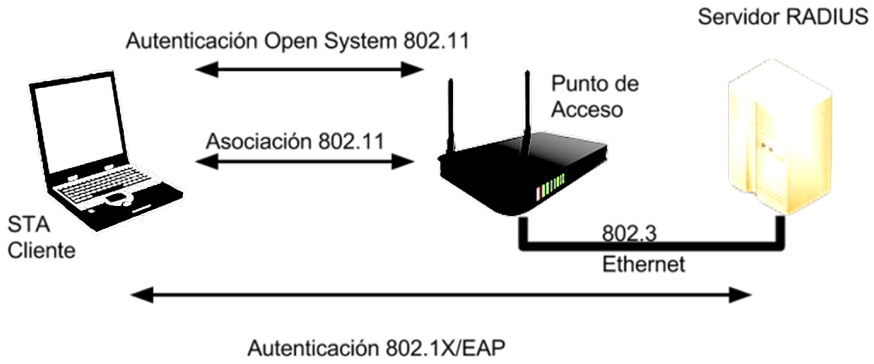

Figura 2.9: Proceso de Autenticación Open System con autenticación posterior 802.1X/EAP.

Authenticación por clave compartida

Este tipo de autenticación (*Shared Key authentication*) utiliza WEP para autenticar a las estaciones cliente y requiere que una clave estática WEP esté configurada en la STA y el punto de acceso. Ya que WEP es obligatorio, la autenticación no funcionará si las claves no son idénticas. El proceso de autenticación es similar al Open System pero incluye el envío de retos y sus respuestas entre el AP y la STA dentro del mismo BSS. Esta autenticación también puede usarse entre dos estaciones en un IBSS.

La autenticación por clave compartida consiste en un intercambio de cuatro tramas. El cliente manda un *Authentication Request* al AP y este responde con un reto en texto claro en una trama *Authentication Response*. La STA encripta el reto y lo vuelve a enviar al punto de acceso, el AP lo desencripta y mira si hay coincidencia. Si está correcto, la misma clave que se utilizó para la autenticación se utilizará para encriptar las tramas de datos IEEE 802.11.

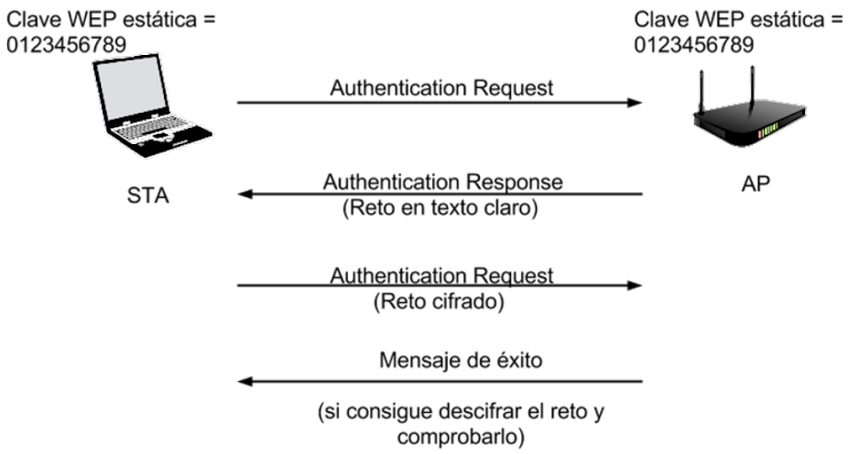

Figura 2.10: Proceso de autenticación por clave compartida.

A pesar de que este tipo de autenticación pueda parecer más seguro que Open System, en realidad se presenta como el de mayor riesgo de seguridad. Cualquiera que capture la trama del reto en texto plano y la encriptada en la respuesta puede averiguar la clave WEP y desencriptar todas las tramas de datos IEEE 802.11. Usar encriptación WEP junto con la autenticación Open System da mejor resultado que la autenticación por clave compartida.

2.4.2. Encriptación WEP

WEP es un método de encriptación a Nivel 2 que utiliza el proceso de cifrado streaming *Alleged Rivest Cipher 4 (*ARC4*)*, la información que se encripta pertenece a las capas superiores. WEP y otros métodos de encriptación a Nivel 2 encriptan la carga MSDU de una trama de datos IEEE 802.11. El estándar IEEE 802.11 original define los dos métodos WEP de encriptación: 64-bit WEP y 128-bit WEP. Los tres principales objetivos de la encriptación WEP son la confidencialidad, el control de acceso y la integridad de la información, a través de la encriptación de los datos antes de su transmisión.

WEP proporciona control de acceso al medio, las estaciones que no tienen la misma clave WEP estática que el punto de acceso no pueden acceder a los recursos de la red. Una suma de comprobación (checksum) de integridad de datos, llamada *Integrity Check Value (*ICV*)*, se computa sobre los datos antes del cifrado y es usada para prevenir la modificación de estos.

El estándar IEEE 802.11 se refiere a la versión de 64 bits como WEP-40 y a la de 128 bits como WEP-104. La versión 64-bit WEP utiliza una clave estática secreta de 40 bits combinada con un número de 24-bit seleccionado por los drivers de la tarjeta del dispositivo. Este número de 24 bits se llama *Initialization Vector (*IV*)*, se envía en texto

plano y se crea nuevo para cada trama. El estándar no especifica los algoritmos para crear el IV. El cifrado 128-bit WEP usa una clave estática de 104 bits y también se combina con un IV de 24 bits.

Una clave estática WEP puede generarse con caracteres hexadecimales (0–9 y A–F) o caracteres American Standard Code for Information Interchange (ASCII). La clave 40-bit consiste en 10 caracteres hexadecimales o 5 ASCII, mientras que la clave 104-bit consiste en 26 caracteres hex. o 13 ASCII. No todas las estaciones o los puntos de acceso soportan los dos caracteres. Muchos APs y estaciones soportan hasta cuatro claves WEP diferentes y pueden seleccionar una por defecto.

La clave de transmisión es la clave estática que se utiliza para cifrar los datos por la radiotransmisión. Los dispositivos pueden utilizar una clave para encriptar el tráfico de salida y otra clave para descifrar el tráfico entrante. Aún así, la clave usada debe de coincidir en los dos lados del enlace para que el cifrado/descifrado se hagan correctamente. Cuando un dispositivo crea una trama WEP cifrada, un identificador de clave se añade al campo del IV indicando cual de las 4 posibles claves se ha usado para encriptar y cual se usará para desencriptar los datos.

Proceso WEP

WEP ejecuta una comprobación de redundancia cíclica, *Cyclic Redundancy Check (*CRC*)*, en la información en texto plano que se va a cifrar y le añade al final un valor de comprobación de integridad, ICV. Se genera el IV de 24 bits y se combina con la clave secreta. A continuación, WEP pasa la clave estática y el IV por un algoritmo pseudo-aleatorio para crear bits de datos aleatorios llamados *keystream*. Los bits aleatorios del keystream se combinan con los bits de los datos en texto plano mediante un proceso XOR Booleano y el resultado final es el texto cifrado WEP.

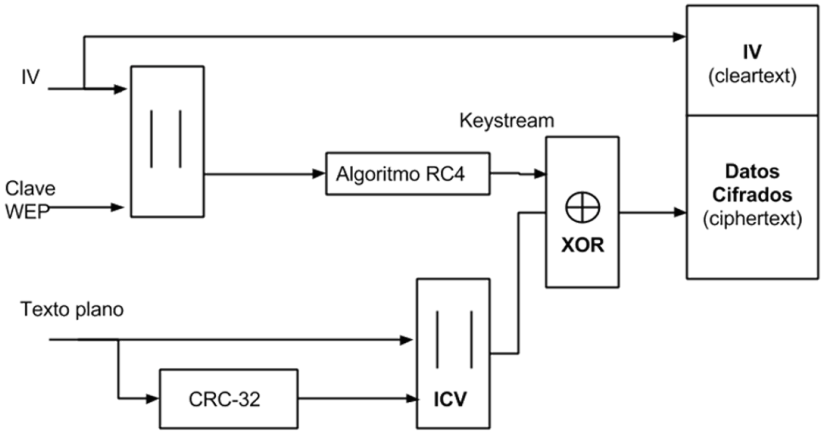

Figura 2.11: Representación proceso encriptación WEP.

Para descifrar la trama, WEP extrae el IV y el identificador de clave, para saber que clave usar. Luego, introduce la clave y el IV por el algoritmo pseudoaleatorio para generar el keystream. Éste se combina con el texto cifrado y se utiliza un proceso XOR Booleano. El resultado final es la desencriptación del texto cifrado y la creación de la información en texto claro. Para comprobar el proceso y validar el texto descifrado, WEP ejecuta el CRC sobre la información conseguida y lo compara con el ICV del texto cifrado. Si los dos son idénticos bit a bit, la trama se considera válida.

El proceso de encriptación es igual para las dos versiones de cifrado WEP. Desafortunadamente, WEP tiene debilidades, ha sufrido ataques a lo largo de los años y se han conseguido elaborar softwares para romper las claves en menos de 5 minutos, con una combinación de esos ataques. Aún así, es mejor utilizar WEP que no usar ningún método de cifrado.

2.4.3. Robust Security Network

La regulación IEEE 802.11i [32] se modificó incluyendo la definición de mejores métodos de cifrado y de autenticación, RSN y *Robust Security Network Associations (*RSNA*)*.

Una asociación de seguridad es un conjunto de políticas y claves usadas para proteger la información. Los sistemas RSNA necesitan dos dispositivos IEEE 802.11 para realizar el proceso de autenticación y asociación al igual que para crear las claves dinámicas mediante el proceso *4-Way Handshake*. Este tipo de asociación se define como RSNA, es decir, dos dispositivos deben compartir claves dinámicas de cifrado que son únicas entre ellos. Counter Mode with Cipher-Block Chaining Message Authentication Code Protocol (CCMP)/Advanced Encryption Standard (AES) es un método de encriptación obligatorio mientras que Temporal Key Integrity Protocol (TKIP)/RC4 es opcional.

TKIP

TKIP es un protocolo de seguridad que fue creado para remplazar la encriptación WEP. Cuando WEP fue atacado, las redes IEEE 802.11 se quedaron sin un sistema de seguridad fiable. El grupo de seguridad IEEE 802.11i [32]definió TKIP para proporcionar una solución mejor de seguridad sin necesidad de remplazar los equipos. La intención fue crear una solución temporal de seguridad hasta que los fabricantes de WLANs pudieran proporcionar hardware que soportase la encriptación CCMP/AES.

El estándar IEEE 802.11 define dos protocolos de confidencialidad e integridad de datos RSNA: TKIP y CCMP, con soporte TKIP opcional. En abril de 2003, Wi-Fi Alliance introdujo las certificaciones Wi-Fi Protected Access (WPA), que requieren el uso de cifrado TKIP.

Al igual que WEP, TKIP utiliza el algoritmo ARC4 para realizar el proceso de cifrado y descifrado. TKIP introduce términos al cifrado WEP:

- **Claves Temporales (Temporal Keys)** – Utiliza claves de cifrado dinámicas. Dos dispositivos utilizan un proceso 4-Way Handshake para crear claves unicast, dinámicas y únicas. Se crean para protegerse de diferentes tipos de ataques. Pueden ser de dos tipos:
  - **PTK** –Para cifrar tramas unicast.
  - **GTK** – Para cifrar tramas multicast o broadcast.
- **Secuencias (Sequencing)** – TKIP utiliza un *TKIP Sequence Counter (*TSC*)* para secuenciar los MAC Protocol Data Unit (MPDU)s enviados. La estación IEEE 802.11 suelta todos los MPDUs que se reciben fuera de orden. Se implementa para protegerse de los ataques de repetición y reinyección.
- **Mezcla de claves (Key Mixing)** – Se utiliza un complejo proceso de mezcla criptográfica de dos fases y la información que se introduce en el cifrador RC4. Se diseñó para protegerse de las colisiones de IV conocidos y los ataques por claves débiles. Las fases de la mezcla son:
  - **Fase 1** – Se crea *TKIP-Mixed Transmit Address and Key (*TTAK*)* mediante la clave temporal, la dirección emisora (*Transmit Address (*TA*)*) y el TSC.
  - **Fase 2** – Se crea la información para introducir en el algoritmo ARC4 combinando el TTAK, la clave temporal y el TSC.
- **Integridad de Datos Mejorada (Enhanced Data Integrity)** – Utiliza una comprobación de integridad más fuerte llamado *Message Integrity Code (*MIC*)*. Se utiliza para defenderse de los ataques de falsificación y cambio de bit. El MIC se calcula mediante la dirección destino (Destination Address (DA)), la dirección origen (Source Address (SA)), precedencia MSDU y los datos en texto plano MSDU completos desencriptados.
- **Contramedidas (TKIP Countermeasures)** – Ya que el diseño de TKIP MIC no es perfecto y puede comprometerse la integridad del mensaje, TKIP implementa contramedidas. Las contramedidas evalúan la probabilidad de que haya una falsificación y cuanta información necesita el atacante para aprender la clave. Los tipos de contramedidas son:
  - **Logging** – Los fallos del MIC tienen que ser registrados.
  - **60 Second Shutdown** – Si ocurren dos fallos en menos de 60 segundos, la estación y el AP bloquean todas las tramas TKIP durante 60 segundos.
  - **Nuevas Temporal Keys** – Como característica adicional de seguridad, las claves PTK y GTK deben cambiar.

El argumento TKIP MIC no consigue remplazar al WEP ICV porque el MIC se sigue considerando débil, TKIP protege el MIC con encriptación haciendo que el ataque sea más complicado. WEP ICV ayuda a prevenir falsas detecciones de fallos MIC que harían que las contramedidas TKIP se pusieran en funcionamiento.

Una vez que el MIC se crea y se agrega al MSDU en texto claro, IEEE 802.11 MAC realiza el procesado del nuevo MSDU. Si la fragmentación está habilitada, es posible que se compongan mas de un MPDU. La comprobación de integridad se ejecuta sobre el MPDU y se agrega el WEP ICV al MPDU. La función XOR Booleana se ejecuta sobre el

keystream y el MPDU/ICV para crear una carga cifrada y se calcula una secuencia de comprobación de la trama (*Frame Check Sequence (*FCS*)*) sobre estos campos. Cuando una estación reciba una trama, comprobará el FCS, ICV y el TSC de todos los MPDUs antes de verificar el MIC. Esto evita una contramedida por fallo de MIC.

CCMP

CCMP es un protocolo de seguridad que fue creado como parte de la regulación de seguridad IEEE 802.11i [32] y fue diseñado para remplazar TKIP y WEP. CCMP utiliza el cifrador por bloques AES en vez del RC4. CCMP es obligatorio para redes de seguridad robustas, RSN . En Septiembre de 2004, Wi-Fi Alliance anunció la segunda versión de *Wi-Fi Protected Access certification*, llamada WPA2, que requiere el uso del cifrador CCMP/AES. Los dispositivos IEEE 802.11 que sólo soportaban WEP y TKIP tuvieron que modificar su hardware para poder soportar este proceso de encriptación.

CCMP se compone de diversos elementos que proporcionan diferentes funciones:

- **CounterMode (CTR)** – Se utiliza para proporcionar confidencialidad de datos.
- **Cipher-Block Chaining (CBC)**
- **Cipher-Block Chaining Message Authentication Code (CBC-MAC)** – Proporciona autenticación e integridad.

El proceso CCMP utiliza la misma clave para encriptar la carga MSDU y para comprobar la integridad criptográfica. La comprobación de integridad se utiliza en los datos MSDU y en las cabeceras MAC del MPDU.

El método de encriptación CCMP utiliza el cifrador por bloques AES, éste usa una clave de 128 bits y cifra los datos en bloques de 128 bits. Las entradas utilizadas en CCMP para el proceso de integridad incluyen:

- **Claves Temporales (Temporal Keys)** – Igual que en TKIP, CCMP utiliza claves temporales de 128 bits PTK o GTK.
- **Número de Paquete (Packet Number (PN))** – Parecido a un número de secuencia TKIP, el PN identifica la trama y se incrementa con cada transmisión.
- **Nonce** – Número Aleatorio que se genera una única vez y calcula a partir del PN, datos del Quality of Service (QoS) y del TA.
- **Trama IEEE 802.11 MPDU** – El MSDU se encripta y protege con un MIC. La cabecera del MPU no va protegida por el MIC.
- **Datos Adicionales (Additional Authentication Data (AAD))** – Se crea mediante fragmentos de la cabecera MPDU, se usa para la integridad de los datos de la cabecera MAC.

El proceso de encriptación CCMP de la carga en texto plano MPDU es el siguiente:

1. Se crea el PN de 48 bits. El número se incrementa para cada MPDU individual, aunque se mantiene cuando se realiza una retransmisión.

2. Algunos campos del MPDU se utilizan para construir el AAD. El MIC proporciona protección de la integridad de esos campos, en la cabecera MAC, y al cuerpo de la trama. La estación receptora debe validar la integridad de las partes protegidas de la cabecera MAC.

3. Se crea un Nonce a partir del PN, dirección emisora (TA) e información utilizada en QoS.

4. Una cabecera CCMP de 8 octetos se construye e incluye el identificador de clave y el PN, que se divide en 6 octetos.

5. El cifrador CCMP, que utiliza AES, crea la comprobación de integridad y encripta los datos de capas superiores. La clave temporal, el nonce, ADD y los datos se procesan para poder crear el MIC de 8 bytes. La carga MSDU del cuerpo de la trama y el MIC se cifran en bloques de 128 bits.

6. La cabecera MAC se añade a la cabecera CCMP, al MSDU cifrado y al MIC también cifrado. Una secuencia de comprobación de trama, FCS, se calcula sobre los campos de la cabecera y el cuerpo de la trama. El CRC de 32 bits resultante se posiciona en el campo FCS.

4-Way Handshake

4-Way Handshake es el proceso final utilizado para generar claves por pares para el cifrado de transmisiones unicast PTK y claves temporales para grupos en transmisiones broadcast o multicast. (GTK)

Requiere tramas EAP over LAN (EAPOL) para intercambiar información criptográfica entre la estación cliente y el AP. Como indica su nombre, utiliza 4 de estos mensajes para intercambiar esta información. Utiliza funciones pseudoaleatorias, *Pseudorandom Function (*PRF*)*, para obtener un valor pseudoaleatorio a partir de una clave, la dirección MAC del AP (Access point Address (AA)), la dirección MAC de la estación (SPA) y dos tipos de nonces: *Authenticator Nonce (*ANonce*)* y *Supplicant Nonce (*SNonce*)*. Los nonces, números aleatorios, sólo se utilizan una vez.

El proceso es el siguiente, ilustrado en la Figura 2.12:

1. **4-Way Handshake Mensaje 1**
   El AP y la STA crean sus propios números aleatorios, ANonce y SNonce. El AP manda el primer mensaje EAPOL y se lo envía con el ANonce a la estación. La estación ya tiene todo lo necesario para crear la clave PTK.

2. **4-Way Handshake Mensaje 2**
   La STA envía el mensaje EAPOL-KEY con el SNonce al AP, así tiene todo lo necesario para usar las PRF. El cliente también manda su información RSN y el MIC para que el punto de acceso pueda validarlo. El punto de acceso obtiene la clave que se puede usar para cifrar tráfico unicast.

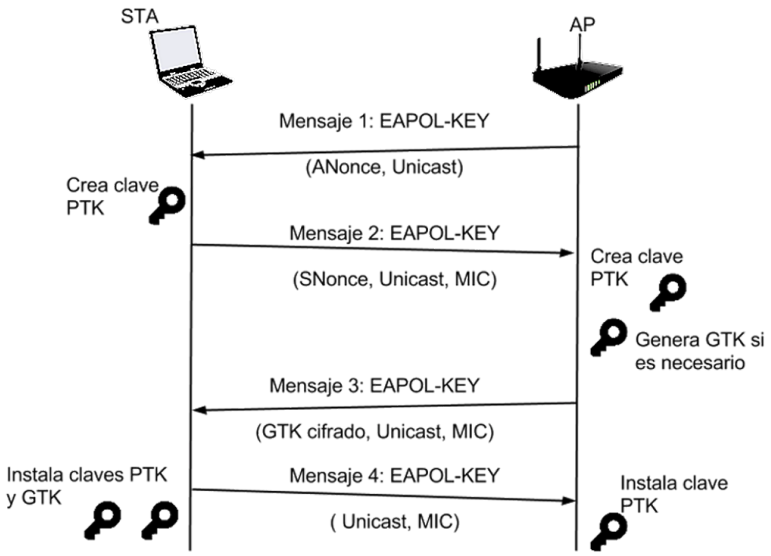

Figura 2.12: Intercambio de mensajes en el proceso 4-Way Handshake.

3. **4-Way Handshake Mensaje 3**
   Si es necesario el AP obtiene la clave GTK. El punto de acceso envía la trama EAPOL-Key a la estación que contiene el ANonce, información RSN del AP y el MIC. La clave GTK también irá dentro del mensaje protegida por la clave PTK.

4. **4-Way Handshake Mensaje 4**
   La estación manda al punto de acceso el último mensaje para confirmar que la clave temporal ha llegado.

2.4.4. WPA/WPA2

El sistema de seguridad original del estándar IEEE 802.11 resultó ser ineficiente y poco seguro para las redes inalámbricas. El grupo de trabajo de seguridad del IEEE 802.11 [30] trabajó en las debilidades del sistema y en 2004 probó un nuevo sistema. La regulación IEEE 802.11i [32]se introdujo en el estándar en Junio de ese mismo año .

Como ya se ha mencionado, Wi-Fi Alliance introdujo la certificación WPA, con cifrado TKIP/RC4, usando la versión del trabajo IEEE 802.11i [32]para definir las mejoras de seguridad que se podía implementar en los dispositivos ya existentes. Se convirtió en un componente obligatorio para la prueba de interoperabilidad y certificación.

WPA puede utilizar dos tipos de mecanismos para gestionar las claves, un servidor externo de autenticación (por ejemplo, RADIUS) y EAP, como usa IEEE 802.1X [37], o por clave pre-compartida (*pre-shared keys*) sin necesidad de servidores adicionales. Wi-Fi Alliance los hace llamar “WPA-Enterprise” y “WPA-Personal” respectivamente. Los dos

métodos crean una clave de sesión para el punto de acceso y la estación cliente.

En Septiembre de 2004 se comenzaron las pruebas de interoperabilidad de certificación WPA2, éste incorporaba el método de cifrado CCMP con el algoritmo de encriptación AES. WPA2 soporta autenticación 802.1X/EAP y clave pre-compartida, siendo compatible con WPA.

La migración del proceso de cifrado TKIP al CCMP se puede observar en la regulación IEEE 802.11n [38], que expone que una estación de alto rendimiento (*High Throughput*, HT) no puede utilizar encriptación WEP o TKIP cuando se comunica con otra estación que soporta sistemas de cifrado mejores. En 2009 Wi-Fi Alliance comenzó las pruebas del estándar IEEE 802.11n [38] para el cumplimiento de este requisito. Actualmente, los fabricantes de productor WLAN siguen ofreciendo el soporte TKIP y WEP pero no es una función predeterminada.

2.5. IEEE 802.1x

El estándar IEEE 802.1x-2004 [33] no es específicamente un estándar inalámbrico, es un protocolo de control de acceso basado en los puertos. Proporciona un método para la restricción del acceso en redes basadas en autenticación de información, define un control de acceso de red cliente-servidor para dispositivos que se conectan mediante Ethernet y un protocolo de autenticación.

Este protocolo permite a los controladores restringir el acceso al medio a dispositivos externos que se encuentren detrás del controlador por puerto 802.1X. Puede implementarse tanto en medios de cableado como inalámbricos. Los dispositivos que deseen conectarse deben autenticarse primero y tener autorización antes de que ningún paquete procedente de o dirigido a dispositivos externos puedan pasar por el controlador de puerto 802.1X.

Define tres componentes principales y cada uno desempeña un papel en la autenticación. Estos tres componentes trabajan juntos para asegurar que sólo los usuarios debidamente validados puedan acceder al medio. El protocolo de nivel dos EAP se utiliza en IEEE 802.1X para validar a los usuarios a nivel 2. Los tres componentes son los siguientes:

- **Supplicant**. Cliente que solicita la autenticación y el acceso a los recursos de la red. Cada uno de los supplicant tiene credenciales de autenticación que son verificadas por el servidor de autenticación. Utiliza EAP para comunicarse con el servidor a nivel 2. No podrá comunicarse a niveles superiores hasta que la autenticación no se realice. En las WLAN, los clientes suelen ser dispositivos portátiles como ordenadores o smartphones.
- **Autenticador (Authenticator)**. Dispositivo que bloquea o permite el tráfico de datos mediante el puerto. Sólo se permite paso al tráfico de autenticación mientras que otro tipo de tráfico de datos es bloqueado hasta que la identidad del supplicant se verifica. Tiene dos tipos de puertos: puerto no controlado (uncontrolled port) y el puerto controlado (controlled port). El puerto sin control se utiliza para el tráfico EAP y se mantiene abierto desde el principio, en cambio, el puerto controlado

se abre una vez realizada la autenticación permitiendo que otro tipo de tráfico penetre en la red. En las WLAN, los autenticadores suelen ser puntos de acceso o controladores.

- **Servidor de Autenticación (Authentication Server (AS))**. Servidor que verifica y valida las credenciales de autenticación del supplicant que solicita el acceso y le notifica al Autenticador que el cliente ha sido autorizado. Tiene diversas bases de datos para guardar las credenciales de los supplicant. El cliente y el servidor se comunican mediante el protocolo de nivel 2 EAP. El estándar 802.1X define el servidor de autenticación como el servidor RADIUS.

2.5.1. EAP

EAP es un sistema de autenticación que soporta diversos métodos, está definido en el RFC 3748[39] para el uso del estándar IEEE 802.1X . EAP es un protocolo de nivel 2 bastante flexible, se ejecuta sobre niveles de Enlace como el protocolo *Point-to-Point Protocol* o IEEE 802, sin necesidad de paquetes IP. Se puede utilizar en autenticaciones de un solo sentido o de dos sentidos, llamadas *Mutual Authentication* . Estas autenticaciones no solo requieren que el servidor autorice al cliente sino que también el supplicant debe validar la autenticidad del servidor.

Tipo paquete	Nombre	Descripción
0000 0000	EAP-Packet	Tipo de trama EAP encapsulada. La mayoría de las tramas EAP son EAP-Packet.
0000 0001	EAPOL-Start	Trama opcional que puede utilizar el Supplicant para iniciar un proceso EAP.
0000 0010	EAPOL-Logoff	Trama que finaliza una sesión EAP y cierra los puertos virtuales.
0000 0011	EAPOL-Key	Trama utilizada para intercambiar información de clave dinámica.
0000 0100	EAPOL- Encapsulated(ASF-Alert)	Trama utilizada para enviar alertas.

Cuadro 2.1: Tipos de trama EAP.

Los mensajes EAP se encapsulan en tramas EAPOL, se utilizan entre el Supplicant y el Autenticador. Estas tramas EAPOL se traducen a EAP en RADIUS entre el Autenticador y el Servidor de autenticación. Hay cinco tipos de tramas EAP, como podemos ver en el Cuadro 2.1.

Proceso autenticación

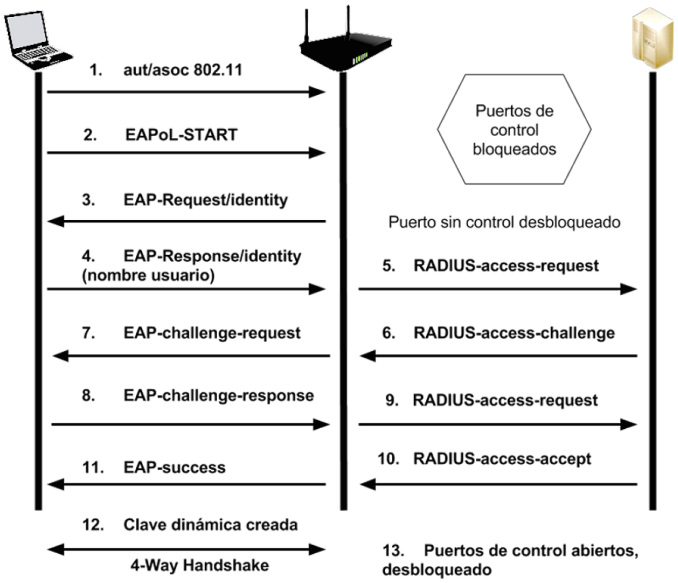

Figura 2.13: Proceso de autenticación EAP.

1. El cliente 802.11, supplicant, se asocia con el punto de acceso y se une al BSS. Los dos puertos, sin control y con control, están bloqueados en el autenticador porque todavía no se ha iniciado el proceso de autenticación.
2. El Supplicant inicia el proceso enviando una trama EAPOL-START al Autenticador. Es una trama que puede no ser utilizada por los diferentes tipos de EAP.
3. El Autenticador envía una trama IEEE 802.11 EAP-Request para solicitar la identidad del cliente. Es una trama obligatoria.
4. El Suplicant contesta con una trama EAP-Response Indentity con la identidad del cliente en texto plano. A partir de este punto, el puerto no controlado se abre para poder permitir que pase tráfico EAP.
5. El Autenticador encapsula la trama EAP-Response en un paquete RADIUS y lo envía al Servidor de autenticación.
6. El Servidor busca la identidad del cliente en sus bases de datos de usuarios y contraseñas y se dispone a envíar un desafío o reto de contraseña al Supplicant en un paquete RADIUS.
7. El AP le envía el reto de contraseña al Supplicant en una trama IEEE 802.11 EAP.
8. El Supplicant aplica unas funciones hash a la contraseña con algoritmos MD-5 o MS-CHAPv2, envía el resultado devuelta al AS en una trama EAP.

9. El Autenticador encapsula la respuesta en una paquete RADIUS y se lo envía al AS.
10. El AS aplica la misma función hash para verificar que la respuesta es correcta y entonces enviar una respuesta de éxito o fracaso devuelta al cliente.
11. El AP envía la respuesta en una trama EAP al cliente. Si la respuesta es de éxito, el cliente es autenticado.
12. El último paso es la negociación 4-Way Handshake entre el Autenticador y el Supplicant para poder generar las claves de encriptación dinámica.
13. Una vez se ha completado la autenticación EAP a nivel 2 y creado la clave dinámica, el puerto controlado se desbloquea para permitir el acceso de tráfico a la red.

El envío de la identidad del cliente en texto plano y la validación de credenciales mediante el débil proceso de funciones hash supone un riesgo para la seguridad. Este tipo de tráfico puede ser capturado usando un analizador de protocolos WLAN. Se han encontrado numerosas debilidades en los primeros métodos de autenticación EAP. Hoy en día, los métodos EAP más seguros emplean autenticación por túnel (tunneled authentication) para enviar las credenciales de identidad y contraseñas. El método EAP más seguro y común utiliza autenticación *Transport Layer Security (*TLS*)* o autenticación TLS-*tunneled*.

Los métodos más débiles, como EAP-MD5 y EAP-LEAP, tienen sólo una identidad del cliente mientras que los métodos que utilizan tunelaje, tienen dos identidades del supplicant. Estas dos identidades se suelen llamar *outer identity* e *inner identity*. La primera se puede ver en texto plano fuera del túnel, por defecto *"anonymous"*, pero la segunda va protegida dentro del túnel TLS.

No se debe confundir la encriptación utilizada en el túnel TLS con la de nivel 2 utilizada para proteger la carga de la trama de datos IEEE 802.11. La encriptación TLS se crea y existe durante unos pocos milisegundos, el propósito de la autenticación por túnel es la de proporcionar un canal seguro para proteger las credenciales de identidad.

2.5.2. EAP-Protected Extensible Authentication Protocol (PEAP)

EAP-Protected Extensible Authentication Protocol (EAP-PEAP), o simplemente PEAP, crea un túnel de encriptación TLS dónde la *inner identity* del supplicant se valida y las credenciales van protegidas.

PEAP debe ser el método EAP más común y ampliamente utilizado en las WLAN, esto es porque es el método más seguro y popular hasta el momento. Hay muchas versiones de PEAP pero las tres principales son:

- EAP-PEAPv0 (EAP-MSCHAPv2)
- EAP-PEAPv0 (EAP-TLS)
- EAP-PEAPv1 (EAP-GTC)

PEAP es conocido también por el nombre "EAP *inside* EAP" ("EAP dentro de EAP") porque el proceso de autenticación dentro del túnel TLS es también otro método EAP. PEAPv0 utiliza en su interior EAP-MSCHAPv2 o EAP-TLS y PEAPv1 utiliza EAP-GTC. La principal diferencia de estas tres versiones es el método utilizado dentro del túnel.

Proceso autenticación PEAP

Este proceso conlleva dos fases. La primera consiste en establecer un túnel seguro usando EAP-TTLS con el Servidor Autenticador y la segunda fase es el proceso de autenticación del cliente.

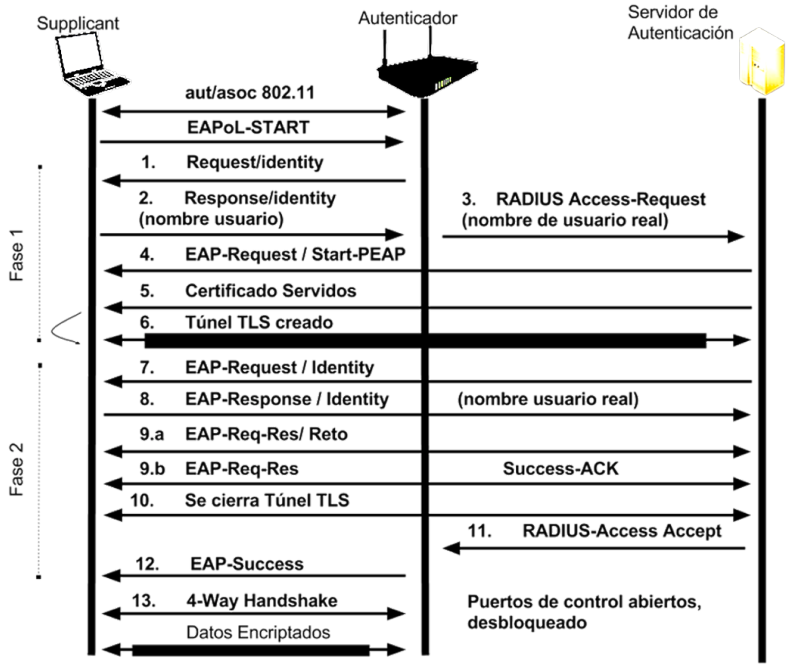

Figura 2.14: Proceso de autenticación PEAP.

1. El Autenticador envía una trama EAP-Request para solicitar la identidad del Supplicant.
2. El Supplicant responde con una trama Eap-Response con el outer identity en texto plano, no es la identidad real del cliente sino un nombre falso.
3. El puerto no controlado se desbloquea en el Autenticador para que el tráfico EAP pueda pasar. El AP envía el outer identity al Servidor de autenticación.
4. La respuesta solamente informa al Servidor que hay un cliente que quiere conectarse.

5. El AS envía el certificado del servidor al Supplicant, el cliente valida el certificado y autentica al Servidor.
6. El túnel point-to-point TLS encriptado se crea entre el Servidor y el Supplicant. Una vez se ha creado el túnel, la fase 2 puede comenzar.

---

7. El Servidor le pide al Supplicant su identidad real.
8. El Supplicant responde con el inner identity, que es el nombre de usuario real y se encuentra oculto gracias a la encriptación del túnel TLS
9. Se poduce el intercambio de retos de clave y sus respuestas hash usando el protocolo de autenticación dentro del túnel.
10. Se cierra el túnel TLS.
11. El Servidor envía un paquete RADIUS de éxito o fracaso al Supplicant.
12. El Autenticador envía la respuesta al Cliente en una trama EAP-Success o EAP-Failure.
13. Si la respuesta del Servidor es de éxito, se procede a realizar la negociación 4-Way Handshake y así terminar el proceso.

2.5.3. Autenticación basada en MAC

Este tipo de autenticación es un enfoque alternativo al 802.1X autenticando clientes conectados a un puerto. Permite que sólo clientes con una dirección MAC específica puedan acceder al medio y pasar datos por el puerto. A los clientes con direcciones MAC que no aparezcan en la lista de direcciones MAC permitidas se les deniega el acceso al puerto y a la red asociada.

Se puede crear la lista de direcciones MAC permitidas en un servidor RADIUS, usado para la autenticación basada en MAC. Permite que clientes no-802.1x puedan añadirse de forma segura y acceder al medio.

El proceso de autenticación es más simple y rápido que 802.1x, comienza cuando el puerto habilitado para la autenticación MAC recibe un paquete con una dirección origen MAC desconocida.

Un paquete Access-Request se envía al Servidor RADIUS con la dirección MAC del cliente al igual que el nombre de usuario y la contraseña. El Servidor comprueba en la lista si puede conceder el acceso a dicho cliente y procede a enviar el mensaje de éxito, Access-Accept, o fallo, Access-Reject, al Supplicant. Si el servidor envía el mensaje de éxito, el puerto queda habilitado para transmitir datos.

Capítulo 3

Diseño

Este proyecto consiste en el estudio de una red WLAN y el análisis, en una red 802.11r [35], de la aleatorización de las direcciones MAC de un dispositivo 802.11.

Para poder formar la red requerida, se han utilizado una serie de herramientas software y dispositivos hardware. La red de infraestructura está compuesta de una estación cliente, dos puntos de acceso y un servidor autenticador (RADIUS). Además, se ha utilizado un analizador de redes inalámbricas para poder capturar el tráfico.

3.1. Herramientas software

3.1.1. GNU/Linux

GNU (`http://www.gnu.org/`) es un sistema operativo multiusuario, multitarea, multiplataforma y multiprocesador que consta de una colección de diversos programas (aplicaciones, herramientas de desarrollo, etc.). Es una implementación de libre distribución UNIX. GNU (GNU's Not Unix) fue desarrollado en 1984 en el Proyecto GNU, éste se concibió para devolver el espíritu cooperativo a la comunidad y así eliminar los obstáculos impuestos por los propietarios del software privado.

En un sistema Unix, el núcleo o kernel es el componente que asigna los recursos del dispositivo a los programas que el usuario ejecuta y se comunica con el hardware. GNU se usa normalmente con Linux, desarrollado por Linus Torvalds. GNU/Linux funciona tanto en modo consola o terminal, común en distribuciones para servidores, como en entorno gráfico, orientado al usuario final tanto empresarial como de hogar.

El proyecto contaba con varias herramientas fundamentales para el manejo del programa pero el núcleo en desarrollo, llamado Hurd, no estaba completo, comenzaron a usar Linux. Linus Torvalds sigue coordinando el trabajo de cientos de desarrolladores y responsables de subsistemas para seguir con la evolución del kernel.

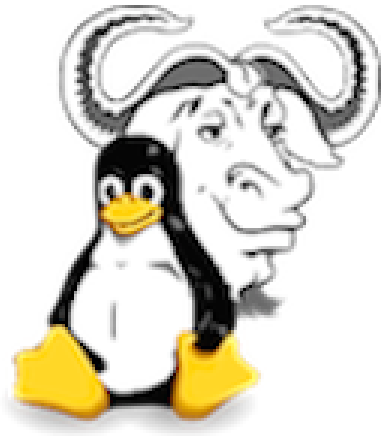

Figura 3.1: Logo GNU y Linux [10]

Debian GNU/Linux

Algunas organizaciones utilizan una base GNU/Linux como sistema operativo, es el caso de Debian GNU/Linux (`https://www.debian.org/`). Debian es una organización formada por voluntarios dedicada a desarrollar y promocionar el software libre.

En 1993, Ian Murdock invitó a todos los desarrolladores de software para contribuir en una distribución basada en el núcleo Linux, así comenzó el Proyecto Debian. Los desarrolladores Debian se encargan de diferentes tareas como el análisis legal de licencias de software, diseño gráfico, escribir documentación y mantener paquetes de software.

Debian GNU/Linux está formada por un gran número de paquetes, cada uno de ellos contiene ejecutables, documentación, scripts e información para la configuración. Hasta la fecha, en Debian GNU/Linux, han existido once versiones estables, siendo la versión 8.0 Jessie la actual. La versión anterior, Wheezy, ha pasado a ser la versión *oldstable* o estable antigua y la versión en pruebas y en desarrollo se llama "Stretch".

En este proyecto se ha utilizado una distribución del sistema operativo GNU/Linux basado en Debian Wheezy llamada Raspbian. Esta distribución se utiliza en las placas Rapsberry pi, de la que hablaré más adelante. También se ha utilizado otra distribución de Debian llamada Voyage Linux, que se ejecuta en plataformas con procesador x86 como Alix.

3.1.2. Hostapd

Hostapd (*Host access point daemon*) es un espacio de software libre de usuario capaz de convertir una tarjeta de interfaz de red en un punto de acceso y en servidores de autenticación. Implementa puntos de acceso IEEE 802.11 [30], autenticadores IEEE 802.1X/WPA/WPA2/EAP [37], cliente RADIUS [45], servidor EAP y el servidor de autenticación RADIUS. La versión actual, hostapd-2.4, soporta Linux (controladores (drivers) Host AP,

madwifi y mac80211) y FreeBSD (net80211).

Hostapd es un programa diseñado para trabajar en segundo plano y actuar como el componente motor (backend component) de control de autenticación. Este programa soporta las siguientes características:

- WPA-PSK (WPA-Personal)
- WPA con servidor EAP o servidor externo RADIUS (WPA-Enterprise)
- CCMP, TKIP,WEP-104 y WEP-40
- WPA e IEEE 802.11i/RSN/WPA2 [32]
- RSN: PMKSA
- IEEE 802.11r [35]
- IEEE 802.11w [36]
- Servidor de Autenticación RADIUS con EAP
- Wi-Fi Protected Setup (WPS)

3.1.3. Wpa_supplicant

Wpa_supplicant es una multiplataforma con un cliente WPA para Linux, Berkeley Software Distribution (BSD) [20], Mac OS X y Windows con soporte para WPA y WPA2(IEEE 802.11i/RSN [32]). Se puede utilizar tanto en ordenadores de sobremesa cómo en dispositivos portátiles, actuando como estación cliente. Implementa las claves de negociación con un autenticador WPA, controla los movimientos roaming y la autenticación/asociación 802.11 del driver WLAN.

Al igual que Hostapd, Wpa_supplicant es un programa diseñado para funcionar en segundo plano y actuar como el componente motor de las conexiones inalámbricas. Wpa_supplicant se desarrolla al unísono con Hostapd por lo que las versiones coinciden, la versión actual es la 2-4. Wpa_supplicant tiene una interfaz para usar en terminal, llamada wpa_cli, y da la posibilidad de instalar una interfaz gráfica (Graphical User Interface (GUI)), wpa_gui, para poder controlar y seleccionar las diferentes características que ofrece.

3.1.4. FreeRadius

FreeRadius (`http://freeradius.org/`) es el más popular y más utilizado servidor RADIUS de software libre en el mundo. Sirve como base de múltiples ofertas comerciales, suministra los servicios de autenticación, autorización y contabilización (Authentication, Authorization and Accounting, AAA) de diversas compañías y es ampliamente utilizado por la comunidad académica, como por ejemplo Eduroam.

Figura 3.2: Logo FreeRADIUS [9]

El proyecto fue iniciado en 1999 por Alan DeKok y Miquel van Smoorenburg, quien colaboró anteriormente en el desarrollo de Cistron RADIUS. Se desarrolló usando un diseño modular para fomentar la participación de la comunidad, llegando a ser uno de los más completos y versátiles gracias a la diversa variedad de módulos que lo componen. FreeRADIUS soporta más tipos de autenticación que ningún otro servidor de software libre. Por ejemplo, FreeRADIUS es el único servidor de RADIUS que puede soportar EAP y servidores virtuales. Actualmente, incluye soporte para todos los protocolos comunes de autenticación y bases de datos, como LDAP y SQL.

MySQL

En este proyecto se eligió una Structured Query Language (SQL) para la base de datos de FreeRADIUS. El software MySQL proporciona un servidor de base de datos muy rápido, robusto y multiusuario. MySQL permite administrar base de datos, creando tablas e introduciendo datos, modificándolos o eliminándolos, etc.

MySQL tiene una doble licencia, los usuarios pueden elegir entre usar el software como un producto de software libre o pueden adquirir una licencia comercial. Está diseñado para entornos de alta producción de datos, con altas cargas de trabajo. Es la base de datos de software libre de mayor aceptación mundial.

3.1.5. Macchanger

Para poder realizar el análisis y cambiar las direcciones MAC de la estación cliente, se utilizó Macchanger. Macchanger es una utilidad de Linux para visualizar y manipular las direcciones MAC de las interfaces de red de un dispositivo. Al igual que los softwares anteriormente descritos, Macchanger es un programa de código abierto. Es realmente sencillo de utilizar y manejar para cualquiera que necesite realizar análisis, test u otras actividades con adaptadores de red.

Proporciona funcionalidades como asemejar la dirección MAC a una dirección concreta, inventada o existente, del mismo fabricante u otro cualquiera; poner una dirección completamente aleatoria y mostrar una lista de direcciones dónde elegir.

3.1.6. Wireshark

Wireshark (`https://www.wireshark.org/`) creado por Gerald Combs (conocido como Ethereal hasta 2006), es un analizador multi-plataforma de protocolos de red de software libre. Se distribuye bajo la Licencia Pública General de GNU (GPL). Se utiliza en este estudio ya que permite examinar los paquetes de una red existente o "viva" y archivos de paquetes almacenados en disco.

Figura 3.3: Logo de Wireshark [27].

Se puede examinar los datos de una captura de tráfico de forma interactiva, filtrando los paquetes necesarios y profundizando hasta el nivel de detalle requerido. Wireshark, que posee una interfaz gráfica, soporta un gran número de protocolos e incluye un lenguaje de filtro entre muchas otras características.

3.2. Dispositivos Hardware

3.2.1. Raspberry Pi

Raspberry Pi (`https://www.raspberrypi.org/`) es una placa de computación (Session Border Controller (SBC)) de bajo costo y tamaño que se puede conectar a un monitor o televisión y utilizar con un teclado y ratón estándar. Fue desarrollada en Reino Unido por la fundación Raspberry Pi, con el objetivo de estimular la enseñanza de ciencias de la informática en las escuelas.

Raspberry Pi es un pequeño dispositivo que posibilita explorar el mundo de la informática y aprender a programar en lenguajes como Python. Ofrece todas las funcionalidades de un ordenador de sobremesa, como navegar por internet, juegos, ver videos en alta definición, hacer hojas de cálculo, documentos y programar.

Para poder usar la Raspberry Pi se necesita una tarjeta SD o microSD para almacenar el sistema operativo y el software. El sistema operativo se puede elegir en la página oficial www.raspberrypi.org según la preferencia del usuario. Como se indica anteriormente, en este proyecto se utilizó Raspbian.

Existen diversos modelos Raspberry Pi, los cuales son los siguiente:

- **Raspberry pi A**. Versión más básica, 45 gr, consumo 1.5 W y 256 MB de memoria RAM a 400 Hz.

- Chip: Broadcom BCM2835
- CPU ARM1176JZF-S, 700 MHz
- Procesador gráfico: VideoCore IV, 250 Mhz
- HDMI 1.4
- Vídeo RCA
- Salida de auriculares 3.5 mm
- 1 Puerto USB
- Conector de cámara CSI
- Conector de tarjeta SD
- 8 conectores GPIO

- **Raspberry pi B**. Mismo hardware que el modelo A, pero tiene 512 MB de memoria RAM, consumo 3.5W, un segundo puerto USB y una conexión de red Ethernet 10/100. Fue el primer modelo en salir al mercado. Representada en la Figura 3.4.
- **Raspberry pi A+**. Mismo hardware que el modelo A, pero con 17 conectores GPIO, soporte de tarjetas microSD, sistema de audio mejorado, más pequeña, 23gr y consumo de tan sólo 1W.
- **Raspberry pi B+**. Mismo hardware que el modelo B, añade dos puertos USB, soporte de tarjetas microSD, consumo 3W y audio mejorado.
- **Raspberry pi 2 B**. Nuevo chip Broadcom BCM2836, eso conlleva una nueva CPU ARM Cortex-A7 de 4 núcleos a 900 MHz y 1GB de memoria RAM a 450 Hz. El resto del hardware coincide con el modelo B+.

En este estudio se ha utilizado el modelo Raspberry pi B, una raspberry como estación cliente y dos como puntos de acceso.

Figura 3.4: Raspberry Pi modelo B.[22]

3.2.2. ALIX

ALIX son placas de sistema manufacturadas por PC Engines, pueden utilizarse como routers inalámbricos, firewalls, para crear VPNs, etc. Utiliza un procesador x86 basado en Advanced Micro Devices, Inc (AMD) Geode.

Necesita una tarjeta CompactFlash para almacenar el sistema operativo y el software utilizado. El software es elegido por el usuario, puede elegir entre distribuciones de FreeBSD, Linux (Voyage Linux elegido para este proyecto), NetBSD, OpenBSD y otros tipos.

Las diferentes versiones pueden tener de 1 a 3 puertos Ethernet, 1 o 2 ranuras para miniPCI y un puerto serie. Según el modelo, puede tener además una conexión VGA, audio, conectores GPIO y una memoria SDRAM de 128 o 256 MB.

3.2.3. Linksys

Linksys fue, desde 2003 hasta 2013, la marca de productos para el mercado doméstico y de pequeñas empresas del líder mundial en telecomunicaciones Cisco. En 2013 la compañía Belkin se hizo con la empresa y el control de la compañía. Los productos de hogar se venden bajo la marca Linksys, abarcan adaptadores wi-fi, routers, puntos de acceso, switchs, equipos VoIP y sistemas de almacenamiento en red.

El router utilizado en este proyecto es el llamado Linksys WRT160NL, tecnología Wireless N, sistema operativo Linux y soporte WPS. Es un router neutro, es decir, necesita una conexión Ethernet que provenga de módem o switch con acceso a Internet. Tiene cuatro puertos Ethernet, un puerto USB, conectividad Bluetooth y WiFi, y dos antenas con conectores R-SMA.

3.2.4. Otros

Para completar la red inálambrica, poder conectarnos a internet y desarrollar el proyecto, se utilizó el hardware disponible en la universidad:

- **Switch** NetGear GS608. 8 puertos Gb hasta 1000Mbps y soporte para Windows, Mac Os y Linux.
- **Servidor** Hp Intel Core 2 Quad de 4 núcleos Q-9400.
- **Cables Ethernet**

3.3. Diseño de la red

El diseño de la red, con los diferentes puntos de acceso, fue la siguiente:

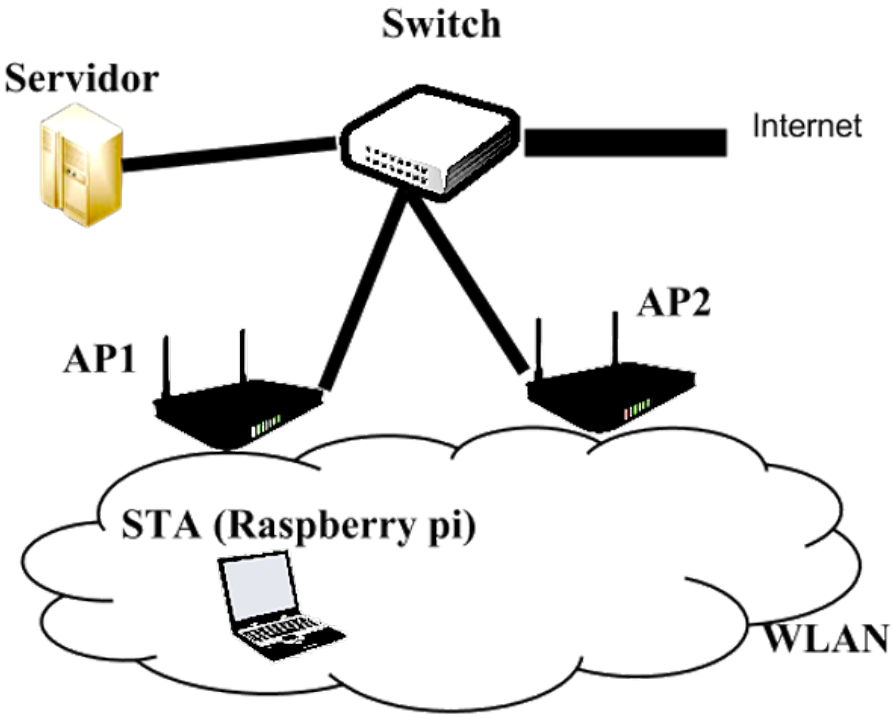

Figura 3.5: Diseño de la red implementada en el proyecto.

Capítulo 4

Configuración

En este apartado se encuentran definidos los parámetros importantes de los ficheros de configuración de los distintos programas. Los ficheros de configuración se encuentran en la página web de desarrollo de cada programa: Hostapd [11], Wpa_supplicant [26] y Freeradius [8]

4.1. Configuración AP

Hostapd contiene un fichero de configuración, el cual se puede modificar y configurar al gusto del usuario. Los puntos de acceso se han configurado con diferentes métodos de seguridad, por lo que los ficheros varían entre ellos.

WEP

Como está indicado en el capítulo anterior, Hostapd soporta encriptación WEP-104 y WEP40. La configuración es bastante sencilla y rápida, hay que variar algunos términos del fichero de ejemplo. Hay que indicar la interfaz utilizada, el driver, el canal, el nombre del SSID a utilizar, el tipo de autenticación, y por supuesto la clave WEP que se va a utilizar. La configuración es la siguiente:

```
interface=wlan0
bridge=br0
driver=nl80211
auth_algs=1              % bit 0 = Open System; 1 = Shared Key.
ssid=TESTWEP
channel=11                       % 2.4 GHz
wep_default_key=0        % Se selecciona la clave de las 4 disponibles.
wep_key0=123456789a
```

WPA/WPA2-PSK

En primer lugar, se eligió una configuración WPA o WPA2-PSK sin 802.11r para comprobar la diferencia. La configuración es sencilla, al igual que la anterior hay que cambiar únicamente ciertos parámetros:

```
interface=wlan0
bridge=br0
driver=nl80211
auth_algs=1
ssid=test
channel=11

          ##### WPA/IEEE 802.11i configuration #####
wpa=3                          % bit 0= WPA;
                               bit 1= IEEE 802.11i/RSN (WPA2)
wpa_passphrase=12345678        % Contraseña utilizada
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP              % Indicamos el tipo de cifrado permitido
```

En la configuración de WPA o WPA2-PSK con soporte 802.11r se debe añadir otros parámetros para que los puntos de acceso estén sincronizados y se pueda efectuar el movimiento rápido entre APs.

```
interface=wlan0
bridge=br0
driver=nl80211
auth_algs=1
ssid=test
channel=11

                ##### WPA/IEEE 802.11i configuration #####
wpa=3                                  % bit 0= WPA;
                                       bit 1= IEEE 802.11i/RSN (WPA2)
wpa_passphrase=12345678                % Contraseña utilizada
wpa_key_mgmt=WPA-PSK FT-PSK            % FT significa que 802.11r está activo
wpa_pairwise=TKIP CCMP                 % Indicamos el tipo de cifrado permitido
rsn_pairwise=TKIP CCMP                 % Indicamos tipo cifrado para RSN/802.11i

                    ##### IEEE 802.11r configuration #####
mobility_domain=a1b2
nas_identifier=crowd.local
r1_key_holder=000102030405

% Listas R0kh y R1kh del mismo dominio de movilidad
% ¡MAC address¿¡NAS Identifier¿¡128-bit key as hex string¿
r0kh=MAC_AP2 crowd.local 0f0e0d0c0b0a09080706050403020100
r1kh= MAC_AP2 00:01:02:03:04:05 000102030405060708090a0b0c0d0e0f
```

La configuración del otro punto de acceso se diferencia en los parámetros de las listas R0kh y R1kh :

```
r0kh=MAC_AP1 crowd.local 000102030405060708090a0b0c0d0e0f
r1kh=MAC_AP1 00:01:02:03:04:05 0f0e0d0c0b0a09080706050403020100
```

Otro parámetro importante en esta configuración define la diferencia entre los tipos de autenticación en el movimiento entre APs: Over-the-Air y Over-the-DS. Se encuentra dentro del apartado de configuración 802.11r

```
ft_over_ds=1    % 0= Over-the-Air; 1=Over-the-DS
```

RADIUS

Para utilizar la autenticación externa 802.1X/EAP [37] con un servidor RADIUS [45] se debe añadir unos parámetros a la configuración, al igual que configurar FreeRADIUS allá dónde se vaya a utilizar.

En el fichero de configuración Hostap se debe incluir y cambiar lo que viene a continuación:

```
      ##### IEEE 802.1X-2004 related configuration #####
ieee8021x=1
eapol_version=2
           ##### RADIUS client configuration #####
own_ip_addr=DireccionIP_APx                % Dirección IP del
                                           AP que se esté configurando
nas_identifier=crowd.local
# RADIUS authentication server
auth_server_addr= DireccionIP_Servidor
auth_server_port=1812
auth_server_shared_secret=12345678
# RADIUS accounting server
acct_server_addr= DireccionIP_Servidor
acct_server_port=1813
acct_server_shared_secret=12345678
         ##### WPA/IEEE 802.11i configuration #####
wpa_key_mgmt=WPA-EAP
```

Si se quiere utilizar con soporte para 802.11r se debe incluir los parámetros que se han indicado anteriormente para tal configuración y cambiar wpa_key_mgmt=WPA-EAP por wpa_key_mgmt=FT-EAP WPA-EAP.

4.2. Configuración STA

En la estación cliente hay que poner las configuraciones correspondientes a las de los puntos de acceso. Los ficheros de configuración del programa Wpa_supplicant son más sencillos que los anteriores, únicamente hay que definir la red a la que se quiere conectar:

WEP

```
network={
        ssid= " TESTWEP "
        key_mgmt=NONE
        wep_key0= " 123456789a "
}
```

WPA/WPA2-PSK

```
network={
        ssid= " test "
        psk= "12345678"
        priority=1
        pairwise=CCMP
        group=TKIP
        key_mgmt=WPA-PSK
}
```

La configuración en Wpa_supplicant para soporte 802.11r es la siguiente:

```
network={
        ssid= " aoliva "
        psk= "12345678"
        group=TKIP
        scan_ssid=1
        key_mgmt=FT-PSK WPA-PSK
        pairwise=CCMP TKIP
}
```

RADIUS

Como ya se ha señalado anteriormente, hay dos configuraciones para la autenticación con servidor externo RADIUS.

- **Sin soporte 802.11r**

```
network={
        ssid= " aoliva "
        identity= " aoliva "
        password= " 12345678 "
        group= CCMP TKIP
        scan_ssid=1
        key_mgmt= WPA-EAP
        eap=TTLS
        pairwise=CCMP TKIP
}
```

- **Con soporte 802.11r**. El único parámetro que se debe modificar es key_mgmt= WPA-EAP por key_mgmt=FT-EAP WPA-EAP.

4.3. Configuración Servidor

En el Servidor, se debe instalar FreeRADIUS, crear una base de datos y modificar alguno de los archivos que incluye este programa. La base de datos, llamada en este proyecto "freeradius", consiste en una serie de tablas e inputs que son manipuladas con MySQL. Los archivos de configuración que se deben modificar en FreeRADIUS son: clients.conf, radiusd.conf y sql.conf.

```
%clients.conf
client 192.168.124.0/24 {              % Elegimos la red de clientes
secret = 12345678
nastype = crowd.local
require_message_authenticator = no
}
```

```
%radiusd.conf
listen {
ipaddr = DireccionIP_Servidor
port = 0                               % Se utiliza el puerto por defecto
type = auth                            % Paquetes de autenticación.
interface = eth0
}
listen {
ipaddr = DireccionIP_Servidor
port = 0
type = acct
interface = eth0
}
```

```
                                %sql.conf
sql {
database = “ mysql”
# Connection info:              % Datos para acceder a MySQL
server = “ <localhost> ”
login = “ <loginuser> ”
password = “ <password> ”
radius_db = “ freeradius ”      %Nombre de la base de datos
}
```

4.4. Configuración de la red

Se ha configurado una red con direcciones Ip del dominio 192.168.124.0/24, tienen este tipo de dirección los puntos de acceso, la interfaz eth0 del servidor y de la estación cliente. También una pequeña subred, 10.0.1.0/24, ha sido configurada para realizar las pruebas y análisis entre el nodo móvil, interfaz wlan0, y el servidor, eth0.

La configuración de estas redes se han realizado de forma temporal o parcial, lo que significa, que si se reinician los equipos, las direcciones ip se borran. El proceso es el siguiente:

1. Deshabilitar la interfaz a cambiar, con el comando: ifconfig <Interfaz_a_cambiar> down.
2. Configurar la dirección ip de la interfaz: ifconfig <Interfaz_a_cambiar> <dirección_ip>.
3. Habilitar interfaz: ifconfig <Interfaz_a_cambiar> up.

También, para poder realizar la captura de tráfico se creó una interfaz inalámbrica virtual en modo monitor, mon0. Se configuró para escuchar el tráfico en el canal 11, canal en el que se configuraron los puntos de acceso y estación. Esta configuración se realiza de la siguiente forma:

1. Elegir tipo y nombre de la interfaz a crear: sudo iw phy phy0 interface add mon0 type monitor.
2. Habilitar la nueva interfaz: sudo ip l s mon0 up.
3. Deshabilitar la interfaz asociada: sudo ifconfig wlan0 down.
4. Cambiar el canal: sudo iw dev mon0 set channel 11.
5. Habilitar las interfaces: sudo ifconfig <Interfaz> up

Capítulo 5

Pruebas de Escalabilidad

Este estudio se realizó para poder comprender el funcionamiento de una red WLAN y los diversos mensajes intercambiados entre cliente y servidor o punto de acceso para poder acceder a la red. Además, se quería observar el comportamiento de la red cuando la dirección MAC de la estación cliente se modificaba con frecuencia.

Una vez finalizado el estudio de la documentación y la configuración de los diversos dispositivos, la red y los elementos fueron puestos a prueba. La evaluación del proyecto se efectuó de forma progresiva, primero observando que las configuraciones eran las correctas, que la red ofrecía servicio de internet; y finalizando con el efecto de la aleatorización de las direcciones MAC en el Servidor RADIUS creado. Una breve explicación de la utilización del analizador de paquetes Wireshark durante las pruebas se encuentra en el Apéndice E.

En esta sección se detallarán dichas pruebas:

- **Prueba I** — Se comprobó que la configuración de la red con sus diferentes tipos de seguridad y autenticación era la correcta.
- **Prueba II** — Se observó el efecto del movimiento en una red 802.11r y se comparó el tiempo de duración de dicho movimiento.
- **Prueba III** — Se estudió el efecto del cambio de la dirección MAC en dicha red.
- **Prueba IV** — Siguiendo con la prueba anterior, se comprobó el efecto sobre el servidor RADIUS creado.

5.1. Prueba I – Comprobación de la configuración

Se realizaron dos tipos de experimentos en este apartado, la comprobación de los puntos de acceso y la conexión a internet ofrecida, utilizando teléfonos móviles y ordenadores portátiles; y la conexión de la estación cliente (Raspberry Pi) con el punto de acceso.

Las diferentes configuraciones de los tipos de seguridad en Hostapd fueron sencillas de realizar, aunque se comprobó en un principio que los puntos de acceso tras la autenticación y asociación no ofrecían acceso a internet. Ésto ocurrió por la falta de un puente,

comúnmente llamado bridge, entre las interfaces wlan0 y eth0 (explicado en el Apéndice B), una vez realizado, la conexión fue completa.

Posteriormente, se comprobó que la configuración del Wpa_supplicant fuera la correcta. Se utilizó el comando **PING** para comprobar la conexión a internet de la estación cliente. Este comando permite que el equipo envíe un paquete a una dirección IP determinada, y si el destino responde significa que se tiene conexión a internet. Se comprobó con cada tipo de seguridad y autenticación configuradas.

También se utilizó **Iperf**, que es una herramienta para analizar la calidad del enlace de red. Primero se creó una subred entre el nodo móvil o estación cliente y el servidor. La latencia de un enlace o tiempo de respuesta (RTT), se puede medir con el comando **PING** anteriormente descrito. Para examinar la variación de latencia (*jitter*) y la pérdida de datagramas, se utiliza Iperf ejecutando una prueba de Protocolo de Datagramas de Usuario, User Datagram Protocol (UDP).

Se utilizó el analizador de red Wireshark para capturar el intercambio inicial entre la estación cliente y los puntos de acceso y así comprobar que eran acordes al estudio previo realizado. Para poder disponer únicamente de los paquetes necesarios, se utilizó el filtro que ofrece este programa y también la utilidad para desencriptar los paquetes capturados con la clave correcta. Una explicación más detallada del funcionamiento de estas utilidades de Wireshark se encuentra en el Apéndice E. Los intercambios de mensaje son los siguientes:

- **WEP**.

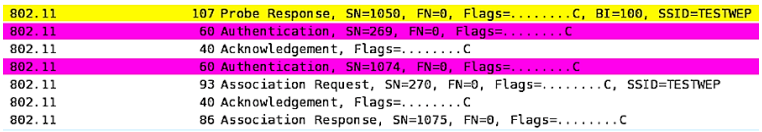

Figura 5.1: Intercambio inicial con seguridad WEP

- **WPA/WPA2-PSK**. Se observó que la estación cliente debe hacer este intercambio con los APs aún teniendo soporte para 802.11r.

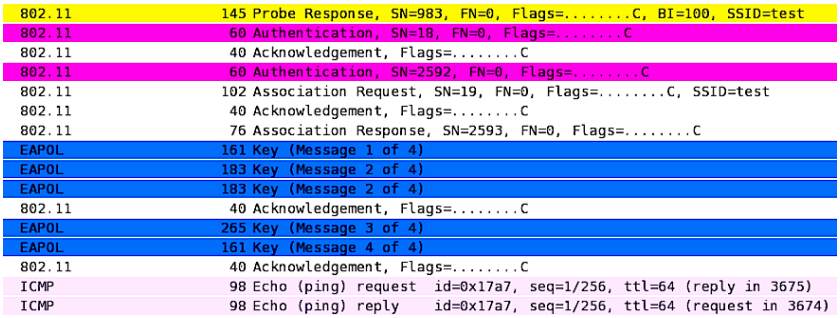

Figura 5.2: Intercambio inicial con seguridad WPA/WPA2-PSK

- **Con RADIUS**. Este intercambio ocurre en los dos puntos de acceso cuando no se utiliza una red 802.11r pero cuando existe ese tipo de red, sólo realiza el intercambio con el primer AP al que se asocia la STA cliente.

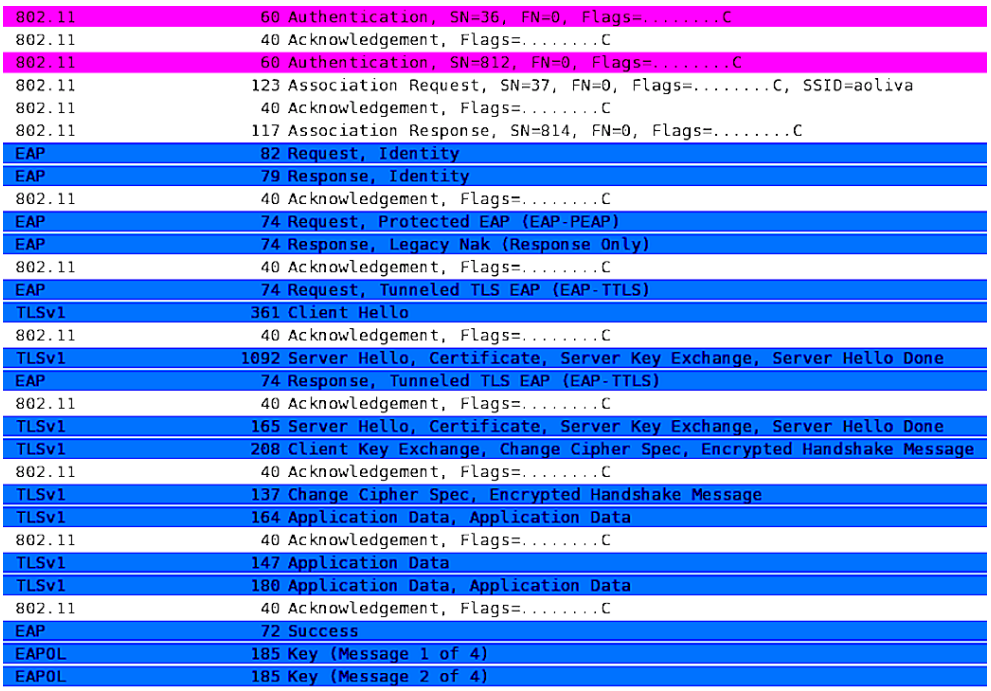

Figura 5.3: Intercambio inicial con autenticación RADIUS

5.2. Prueba II – Comparación Tiempo Roaming

A lo largo de los años, el protocolo 802.11 se ha vuelto más complejo. La introducción de diferentes sistemas de seguridad ha resuelto muchos problemas pero a su vez han creado muchos otros, por ejemplo, el aumento en el tiempo de roaming.

Aquellas redes que utilizan protocolos de seguridad sencillos, como WEP, tienen la ventaja de conseguir un tiempo de roaming <50ms pero la baja seguridad supone un inconveniente cuando la red debe abarcar más allá de una pequeña cantidad de usuarios, además de su alta vulnerabilidad a diversos ataques.

5.2.1. WEP

La prueba realizada con el protocolo de seguridad WEP mostró una media en el tiempo de roaming de 28,79 ms y una varianza de $2{,}035e^{-5}$ s. La mediana de la prueba fue 29,28 ms y la desviación estándar 4,51 ms.

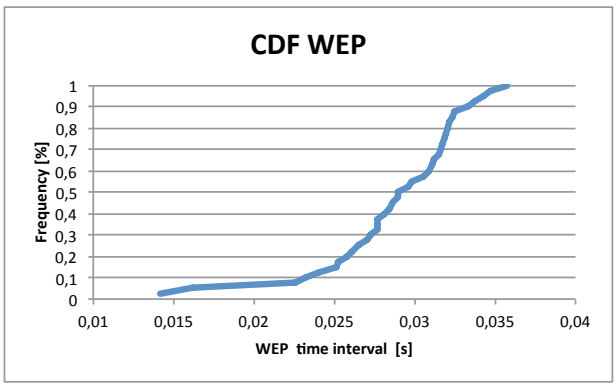

Figura 5.4: CDF realizado para seguridad WEP

5.2.2. WPA o WPA2-PSK

Si se utiliza WPA o WPA2 con clave compartida previa, el cliente y el punto de acceso realizan un intercambio de claves después de los mensajes de autenticación y asociación aumentando en cierta medida el tiempo de roaming.

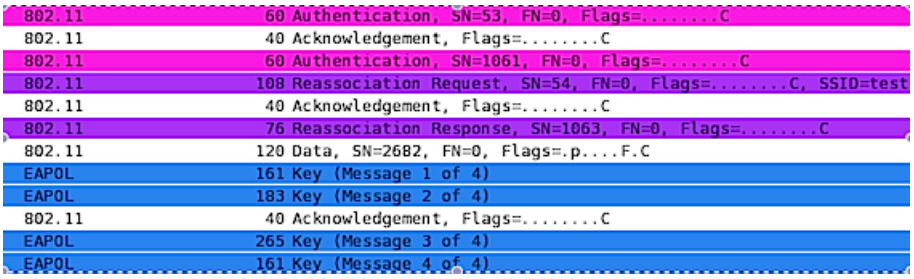

Figura 5.5: Intercambio mensajes en roaming con seguridad WPA o WPA2-PSK.

Este intercambio se domina 4-Way Handshake, se utiliza para intercambiar información aleatoria (nonces), la dirección de la estación, el SSID y la clave, transformadas en pequeñas subclaves mediante el protocolo EAPOL. Este tipo de redes también sufren problemas de escalabilidad cuando se enfrentan a un gran número de usuarios con la misma clave compartida, además, el conocimiento de esta clave junto a la observación de los 4-Way Handshake de otro usuario facilita el descifrado de su tráfico de datos.

En esta prueba se obtuvo una media 71,15 ms, una varianza $4{,}698e^{-5}$ s, la mediana de 70,21 ms y la desviación estándar 6,85 ms.

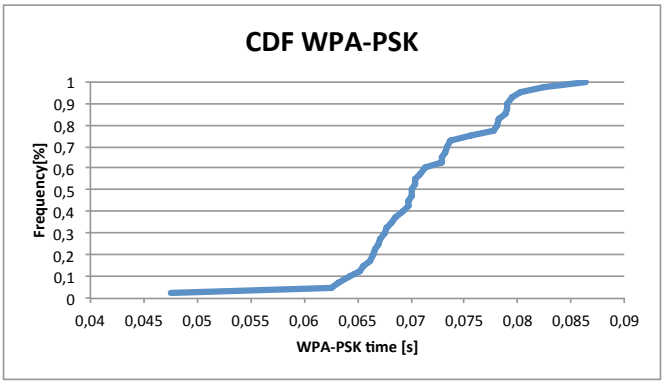

Figura 5.6: CDF realizado para seguridad WPA2-PSK

IEEE 802.11r consigue reducir el tiempo significativamente, usa dos formas diferente de autenticación: Over-the-Air y Over-the-DS. Al estar conectados al mismo controlador, en este estudio, se puede hablar de un intercambio de mensajes Intra Controller.

En el proceso de autenticación Over-the-Air el cliente se comunica directamente con el punto de acceso elegido para el cambio con el algoritmo FT. La estación envía un mensaje FT Authentication Request al punto de acceso objetivo y este responde con un FT Authentication Response. Una vez realizada la autenticación, el cliente envía un mensaje

Reassociation Request y el punto de acceso responde con Reassociation Response. Tras este intercambio, se completa el proceso de roaming.

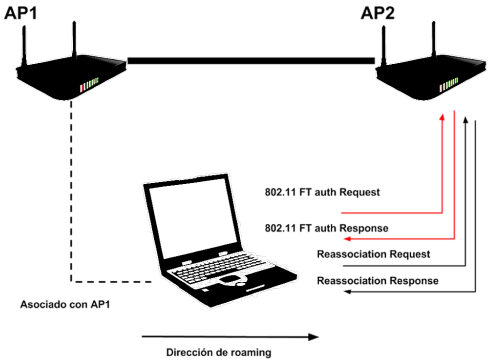

Figura 5.7: Roaming Intra Controller con proceso de autenticación Over-the-Air

En el otro proceso, Over-the-DS, el cliente se comunica con el objetivo a través del punto de acceso al que se encuentra asociado, y pasando por el controlador, mediante paquetes FT. El intercambio de mensajes en este proceso es más complejo, los mensajes de autenticación se intercambian con el punto de acceso en el que se encuentra asociado, tras un intercambio de información entre los puntos de acceso de la misma red, los mensajes Reassociation son realizados entre el cliente y el punto de acceso objetivo para el roaming.

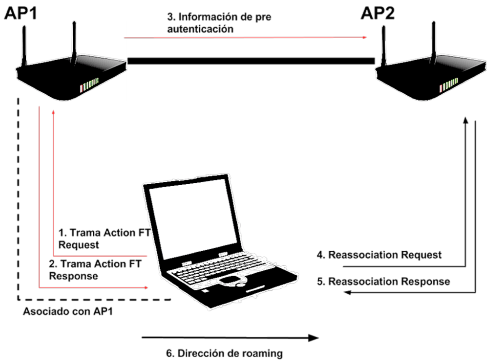

Figura 5.8: Roaming Intra Controller con proceso de autenticación Over-the-DS

Para diferenciar entre estos dos tipos de autenticación se puede observar, en el paquete capturado por Wireshark, un bit que marca la diferencia, en la sección “IEEE 802.11 wire-

less LAN management frame", apartado "Tagged parameters" y pestaña "Tag : Mobility Domain".

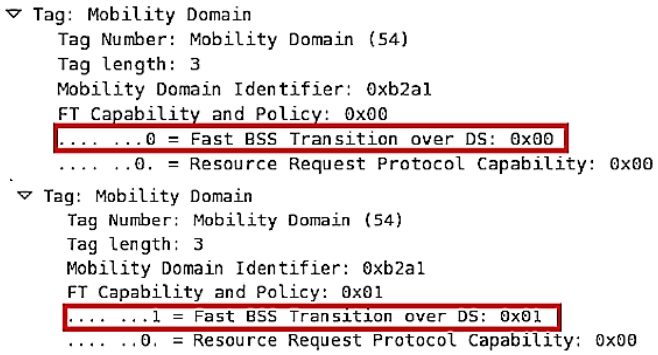

Figura 5.9: Bits de comparación entre FT Over-The-Air y FT Over-The-DS.

Utilizando el proceso de autenticación Over-the-Air, se obtuvo una media de 32,12 ms y una varianza de $1{,}532e^{-5}$ s, con una mediana igual a 31,05 ms y una desviación estándar de 3,91 ms.

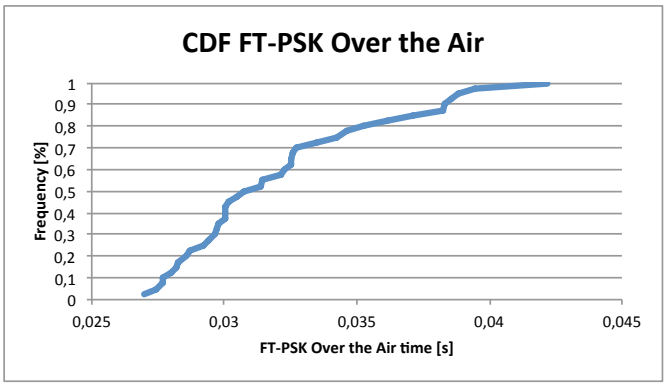

Figura 5.10: CDF realizado para seguridad FT-PSK Over-the-Air.

Mientras que con el proceso Over-the-DS, se obtuvo una media de 35,05 ms y una varianza de $3{,}246e^{-5}$ s. La mediana son 35,30 ms y la desviación estándar de 5,69 ms.

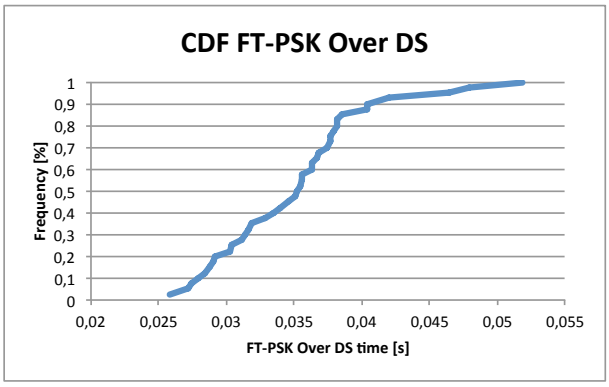

Figura 5.11: CDF realizado para seguridad FT-PSK Over-the-DS.

5.2.3. RADIUS

Cuando se utiliza un proceso de autenticación con el protocolo 802.1X sin ninguna optimización de roaming rápido (fast roaming), el intercambio de mensajes de inicio de sesión se efectúa en todos los puntos de acceso utilizados. Como se muestra en la Prueba I y en la Figura 5.3

Una vez iniciada la sesión, cuando se realiza el roaming, el intercambio de mensaje es igual que en WPA o WPA2 con clave compartida.

802.11	60 Authentication, SN=50, FN=0, Flags=.....C
802.11	40 Acknowledgement, Flags=.....C
802.11	60 Authentication, SN=3373, FN=0, Flags=.....C
802.11	147 Reassociation Request, SN=51, FN=0, Flags=.....C, SSID=aoliva
802.11	40 Acknowledgement, Flags=.....C
UDP	1512 Source port: 40079 Destination port: 5001
802.11	117 Reassociation Response, SN=3375, FN=0, Flags=.....C
802.11	120 Data, SN=1164, FN=0, Flags=.p....F.C
EAPOL	185 Key (Message 1 of 4)
EAPOL	203 Key (Message 2 of 4)
802.11	40 Acknowledgement, Flags=.....C
EAPOL	267 Key (Message 3 of 4)
EAPOL	163 Key (Message 4 of 4)

Figura 5.12: Intercambio mensajes roaming con RADIUS.

Debido a la seguridad de este proceso, se puede observar un aumento en el tiempo de roaming. La media obtenida en este caso fue 75,16 ms y la varianza $4{,}408e^{-5}$ s. La mediana de esta prueba se sitúa en los 75,71 ms y la desviación estándar 6,63 ms.

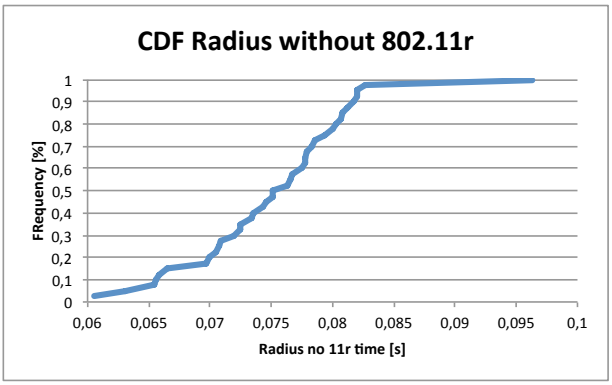

Figura 5.13: CDF realizado con RADIUS sin 802.11r.

5.2.4. RADIUS con 802.11r

Utilizando 802.11r, el proceso inicial de conexión se efectúa únicamente en el primer punto de acceso de la red y cuando se realiza el cambio de punto de acceso el intercambio de clave desaparece consiguiendo una reducción en el tiempo de roaming.

El resultado obtenido con la autenticación Over-the-Air fue la siguiente; una media de 39,93 ms y una varianza $1{,}477e^{-5}$ s. La mediana fue 40.53 ms y la desviación estándar de 3,84 ms.

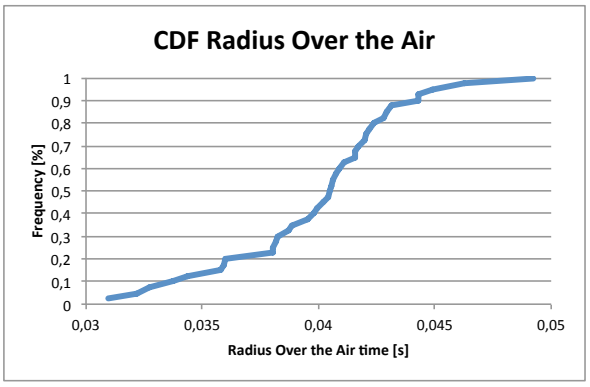

Figura 5.14: CDF realizado con RADIUS Over-the-Air.

Utilizando la autenticación Over-the-DS, la media fue 39,47 ms y la varianza $1{,}505e^{-5}$ s. La mediana del experimento se sitúa en unos 39,93 ms y la desviación estándar 3,88 ms.

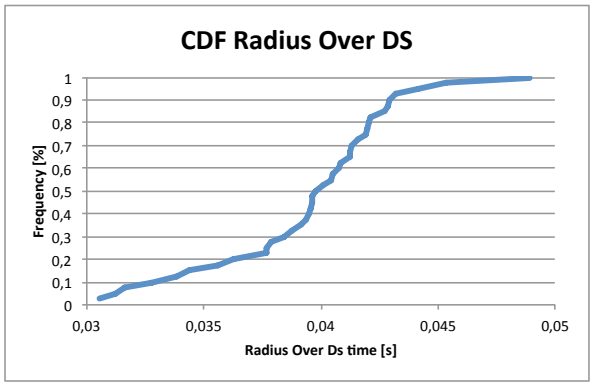

Figura 5.15: CDF realizado con RADIUS Over-the-DS.

5.3. Prueba III – Cambio de la dirección MAC

En esta prueba, después de comprobar el correcto funcionamiento de la red y su configuración, se cambió la dirección MAC de estación cliente con la utilidad Macchanger. El proceso para cambiar la dirección MAC es relativamente sencillo:

1. Se debe actuar como super-usuario. Esto se realiza con el comando **sudo su**
2. Antes de efectuar el cambio, se debe detener la interfaz inalámbrica que se quiere modificar. En nuestro caso la interfaz es **wlan0** y se detiene con el comando **ifconfig wlan0 down**
3. Se cambia la dirección MAC, Macchanger ofrece distintas formas:
   - Creando un número aleatorio con el comando **macchanger -r wlan0**
   - Eligiendo una dirección MAC específica con el comando **macchanger -m <DirecciónMACElegida> wlan0**
   - Cambiarla a otra del mismo fabricante con el comando **macchanger -a wlan0**
4. Se pone de nuevo en funcionamiento la interfaz con el comando **ifconfig wlan0 up**
5. Se realiza la prueba.
6. Si después de realizar la prueba se quiere restaurar la dirección MAC: se detiene la interfaz, se utiliza el comando **macchanger -p wlan0** y se vuelve a subir la interfaz. La dirección se restaura también si se apaga o reinicia el ordenador.

Se observó, en un principio, que la dirección MAC no se modificaba de cara al punto de acceso y que la conexión seguía con la dirección inicial. Este problema, después de mucho estudio, se comprobó que sucedía por la versión de Wpa_supplicant utilizada, Wpa_supplicant 2.3. El 15 de Marzo de 2015, se liberó la versión 2.4 de Hostapd y Wpa_supplicant que añadía soporte para la aleatorización de las direcciones MAC para el

driver nl80211. Una vez instalada esta nueva versión, la dirección MAC se podían modificar correctamente.

Gracias a esta nueva versión se pudieron realizar tres pruebas:

1. Cambiar la dirección MAC según se asociaba la estación cliente a un punto de acceso.
2. Realizar un handover o proceso de roaming y cambiar la dirección MAC al finalizar el proceso.
3. Cambiar la dirección MAC antes de realizar el proceso de roaming.

Se pudo comprobar que al cambiar la dirección MAC, en todos los casos, se creaba un nuevo cliente en el punto de acceso y se realizaba de nuevo el intercambio inicial de mensajes. Al cabo de un tiempo, el punto de acceso borraba el cliente con la dirección MAC antigua de la lista de clientes activos y asociados.

Durante el tiempo que se tarda en hacer el proceso de cambio de dirección MAC y el nuevo intercambio de mensajes de autenticación y asociación, la estación cliente se encuentra en un tiempo de desconexión de la red. Dado este problema, se calculó el tiempo medio en realizar el intercambio inicial para cada uno de los tipos de configuración disponibles.

- **WEP** — Similar a la media de roaming realizada en la Prueba II ya que utiliza únicamente una autenticación Open System. La media fue 29,53 ms.
- **WPA/WPA2-PSK** — El intercambio inicial consta de autenticación, asociación y 4-Way Handshake para todas las configuraciones con WPA/WPA2-PSK, se obtuvo una media de 71,21 ms.
- **RADIUS** — Con autenticación RADIUS la media en el intercambio inicial para nuevos clientes fue de 355,59 ms, para todas las configuraciones.

A estos tiempos se deben sumar una media de 15 ms, que es lo que se tarda en cambiar la dirección MAC del dispositivo, para saber el tiempo aproximado de desconexión de la estación cliente.

5.4. Prueba IV – Servidor RADIUS

El motivo de esta prueba era analizar la escalabilidad del servidor RADIUS y lo que pudiera ocurrir al superar un posible límite del número de clientes. Como se observó en la Prueba III, el cambio de dirección MAC originaba la creación de nuevos clientes.

Para alcanzar este posible límite, los puntos de acceso debían dejar los clientes activos durante el tiempo suficiente sin desasociarlos. En la configuración de Hostapd se debía modificar un parámetro para determinar este tiempo, este parámetro es:

| ap_max_inactivity=300 %El AP verifica la inactividad del cliente(300–> 5 mins) |

Se modificó este parámetro progresivamente para verificar su funcionalidad, se empezó con 6 minutos en los cuales se llegaban a crear 36 clientes simultáneos. Una vez se comprobó que funcionaba y los clientes se desasociaban pasado ese tiempo, se procedió a modificarlo para que tardase 15 horas en verificar la actividad del cliente, lo que corresponde a ap_max_inactivity=54000. En 15 horas se podrían crear hasta 540 clientes activos.

Se puso a prueba la red con dos Raspberry Pi como punto de acceso y el Servidor RADIUS, se observó que un pequeño error se originaba una vez aceptados entre 45 y 50 clientes. Se modificó la red quitando el servidor RADIUS y utilizando únicamente las configuraciones para WPA/WPA2-PSK. Se comprobó que el mismo error ocurría tras asociar ese número de clientes. El error, que aparecía en el debug de los puntos de acceso, fue el siguiente:

```
wlan0: STA <DirecciónMAC> IEEE 802.11: Could not add STA to kernel driver
wlan0: STA <DirecciónMAC> IEEE 802.11: deauthenticated due to local deauth request
```

Dado que el error parecía ser problema del núcleo del driver del dispositivo, se cambió el equipo. En vez de utilizar dos Raspberry Pi como AP se utilizaron dos placas base ALIX con software Voyage Linux 0.9.2 . Se instaló el programa Hostapd y se introdujeron las configuraciones, una vez preparado se realizó la Prueba I. Posteriormente, se quiso comprobar que el error anterior no ocurriese con estos dispositivos.

Con estos nuevos dispositivos se consiguió alcanzar entre 165 y 170 clientes activos al mismo tiempo, tras alcanzar este número de clientes otro error diferente surgió:

```
WPA: wpa_sm_step() called recursively
wlan0: AP-STA-DISCONNECTED <DirecciónMAC>
wlan0: STA <DirecciónMAC> IEEE 802.11: deauthenticated due to local deauth request
```

Tras alcanzar ese número de clientes, los puntos de acceso desasociaban a éstos y volvía a empezar el proceso de autenticación de nuevos clientes y así sucesivamente.

Un último intento se realizó con el Router Linksys WRT160NL, tras configurarlo se realizó una pequeña prueba para comprobar si la estación se podía conectar. Comprobado su correcto funcionamiento, se realizó la prueba. Se pudo comprobar que este dispositivo deautenticaba y desasociaba los clientes una vez se iniciaba el proceso para cambiar la dirección MAC de la estación cliente. Este router no dispone de un parámetro configurable para poder modificar el tiempo de comprobación de inactividad.

Con esta prueba se concluyó que los equipos proporcionados no tienen la suficiente capacidad para poder gestionar un alto número de clientes activos simultáneos y así alcanzar un posible límite en el Servidor RADIUS.

Capítulo 6

Gestión del proyecto

Este apartado recoge los aspectos más relevantes relacionados con el proyecto, tales como la planificación; un desglose de las distintas tareas realizadas a lo largo de este trabajo fin de grado, y el coste asociado al proyecto.

6.1. Planificación

Debido a la extensión de un trabajo fin de grado, se optó por dividir el proyecto en cinco fases principales con sus respectivas tareas:

Fases y Tareas	Horas empleadas
1. Estudio Previo	
I. Estudio redes IEEE 802.11 y Seguridad	50 h
II. Estudio Documentación de herramientas Software	30 h
2. Diseño de la red	
I. Planificación de los Dispositivos Hardware a utilizar	10 h
II. Preparación e Instalación de Software	20 h
3. Configuración de los dispositivos	
I. Configuración Hostapd	
I.i Configuración Inicial con diversos métodos de seguridad	15 h
I.ii Configuración 802.11R	10 h
I.iii Configuración con Autenticación 802.1X	10 h
II. Configuración Wpa_supplicant	
I.i Configuración Inicial con diversos métodos de seguridad	15 h
I.ii Configuración 802.11R	10 h
I.iii Configuración con Autenticación 802.1X	10 h
III. Configuración servidor RADIUS	15 h
4. Pruebas Escalabilidad y su documentación	
I. Comprobación configuración	
I.i Inicial	10 h
I.ii 802.11R	10 h
I.iii Autenticación 802.1X	15 h
II. Comparación Tiempo de Roaming	25 h
III. Prueba efecto MAC spoofing	20 h
IV. Prueba escalabilidad servidor RADIUS	30 h
5. Realización de la Memoria	
I. Redacción	60 h
II. Corrección y Maquetación	15 h
Total Horas	380 h

Cuadro 6.1: Fases y tareas del proyecto y horas empleadas.

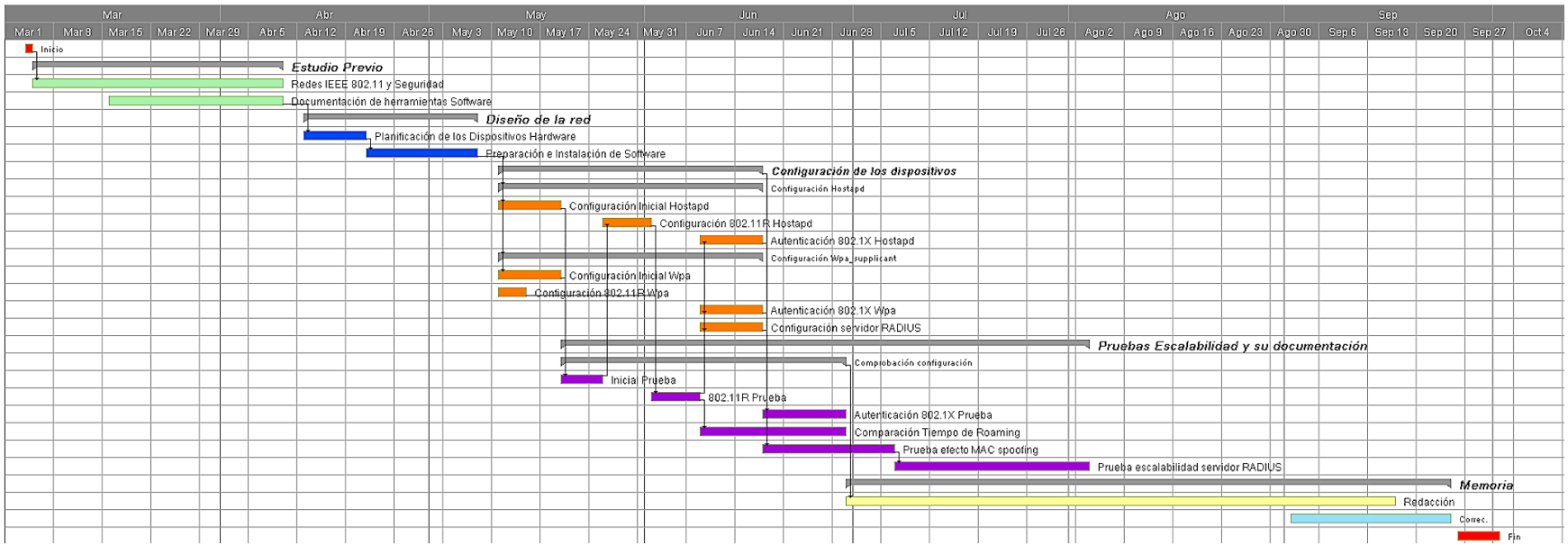

Figura 6.1: Diagrama de Gantt de la planificación del proyecto.

Las distintas fases se han desarrollado de manera no lineal, como se puede observar en el diagrama de Gantt de la figura anterior, Figura 6.1. Por ejemplo, para realizar la tarea de las configuraciones de los dispositivos para soporte IEEE 802.11r, las tareas de configuraciones iniciales y su comprobación debía ser realizada con anterioridad. De la misma forma, la redacción de la memoria se empezó antes de terminar el estudio completo.

6.2. Análisis económico

Costes Materiales

En el Capítulo 3 se señalaron los elementos utilizados durante el proyecto, tanto software como hardware. A continuación, se muestra una tabla con el precio correspondiente de cada uno de ellos:

Elementos	Precio (€)
Herramientas Software	
GNU/Linux	Software libre
Raspbian Debian Wheezy	Software libre
Hostapd	Software libre
Wpa_supplicant	Software libre
FreeRadius	Software libre
MySQL	Software libre
Macchanger	Software libre
Wireshark	Software libre
Dispositivos Hardware	
Raspberry Pi Model B	35,95 x3
Caja Transparente Raspberry Pi Model B	8,95 x3
Fuente Alimentación 5V	7,95 x3
Tarjeta SD 8GB Clase 10 Kingston	8,95 x3
Adaptador USB inalámbrico TL-WN722N	8,80 x2
Ubiquiti Networks SR-71 WLAN USB	118,43
Cable HDMI v1.4	4,95
Combo Teclado + Ratón USB	11,95
Cable de red Ethernet con conectores RJ45	5,99 x4
Caja de Aluminio de interior ALIX2D2 2 LAN Roja	7,50 x2
ALIX2D2	86,63 x2
Linksys WRT160NL Router Neutro 802.11n	69
Netgear GS608	34,90
Hp Intel Core 2 Quad Q9400	87,89
Total	742,34

Cuadro 6.2: Precio de los elementos utilizados software y hardware durante el proyecto.

Costes de Personal

Para la realización de este proyecto ha sido necesaria la participación de dos Ingenieros de Telecomunicaciones, un Ingeniero Junior y un Ingeniero Senior. Considerando la experiencia de ambos ingenieros y las horas empleadas, los costes de personal son los siguientes:

Personal	Horas	Precio/Hora (€/h)	Importe (€)
Ingeniero Senior	50	60	3.000
Ingeniero Junior	330	30	9.900
		Total	12.900

Cuadro 6.3: Coste de Personal.

Coste Total

Los costes totales del proyecto comprenden el coste de material, software y hardware, el coste de personal y los costes indirectos. Los costes indirectos se estiman como un 10 % del resto de costes y comprenden los gastos de electricidad y agua del personal, así como la tarifa de Internet consumida durante el transcurso del proyecto. El coste total del proyecto es el siguiente:

Concepto	Precio (€)
Coste Material	742,34
Coste de Personal	12.900,00
Costes indirectos	1.364,23
Subtotal	15.006,57
IVA (21 %)	3.151,38
Total	18.157,95

Cuadro 6.4: Coste Total del proyecto.

Capítulo 7

Conclusion

This chapter includes the conclusions of the project; as well as how the project could be improved in future line of work.

7.1. Conclusions about the project

The main goal of this project was to analyze the behaviour of the wireless network when changing the MAC address of a client station. More specificatly, a 802.11r WLAN network. In order to perform this research, a 802.11 WLAN network had to be built from scratch.

The implementation of a wireless network and its procedure was unknown by the author, as well as the variety of programs used during the project. This project has helped to understand more deeply the working process behind a wireless connection and its different security and authentication methods.

After the development of the network and the initial tests performed, it could be asserted that initial requirements have been fulfilled: the network works properly and the MAC address change behaviour was analyzed. Further tests were unfinished as the equipment did not have the capacity to accomplish them.

Based on the results of the second test, IEEE 802.11r reduces significantly the roaming duration as the level of security increases, an improvement of nearly 50 ms was measured. Despite of using this support the time duration could not be reduced to the WEP encryption roaming duration, 29 ms approximately.

When a station changes its MAC address a new client is created, so the initial exchange messages have to be performed each time the change occurs. Taking into account the duration of the initial exchange and the time the network interface maintains turned off, it is a huge data loss during a connection. Imagine a client is downloading a big packet of data, say university documents, and the MAC address starts to change; all remaining data would get lost.

7.2. Project difficulties

First of all, the lack of knowledge of the programs, technologies and programming languages, such as SQL, used during the project was the first stone to dodge. An exhaustive search task was developed during the first period in order to comprehend the subject and learn how to manage the project's development.

Secondly, the configuration took a long time to be performed as there are many ways to do so. These programs are still under development as new functionalities and features in WLAN networks are being release more and more often.

Furthermore, some software difficulties had been present during the project. On the one hand, software daemon called *ifplugd*, which configures a ethernet interface when a cable is plugged in, popped up during the tests and unset the virtual IP addresses of the devices making the test fail. This error was avoided by making the daemon service stop and killing its processes.

On the other hand, during Test III we noticed that the MAC address did not change in the WPA_supplicant configuration. As explained in section 5.3 Prueba III, this was caused by the program itself because an old version was being used. The latest version 2.4, was released during the second period of the project. Also, the Hostapd version had to be updated, version 2.4 as well, to continue with the test performance.

However, hardware difficulties have been also present. As it has been mentioned in section 5.4 Prueba IV, the access points were changed in an attempt to achieve a result. Also, during the medium period of the project one of the SD cards from a Raspberry Pi got deleted and a new set up had to be done.

7.3. Future work

Having developed a wireless network with 802.11r support, gives room for improvements in many aspects. Although our analysis of MAC spoofing in this type of network did not reveal much, there are also several possible future lines of work. Here is a list with some ideas:

- **Create an application to control the MAC spoofing.** A graphic interface could be created and let the user control when and for how long the MAC spoofing should be operative. Therefore, some data loss could be avoided.
- **Combine the above application with an Intrusion detection application.** Whenever the Control MAC spoofing application is on and a intruder is detected, a MAC spoofing process will start.
- **Try to block Deauthentication frames.** If a user wants to change its MAC address, the wireless interface has to be turned down and a Deauthentication frame is sent to the access point. Moreover, if someone is capturing the wireless traffic they could notice you are changing the MAC address and even knowing if you are the next MAC address to appear.

- **Use multiple wireless interfaces.** Using Multiple interfaces could help with the data loss, as if a wireless interface with a random MAC address is connected to an SSID downloading a set of data, the other interface, with another random MAC address, could connect with the AP for other processes. After the downloading is finished, the first interface would randomize its MAC address or maintain in a sleep mode until a new MAC spoofing is needed.

Apéndices

Apéndice A

Summary

A.1. Introduction

The introduction of IEEE's 802.11 standards has enabled a mass market. Nowadays, everyone has a portable device and can perform a wireless connection at home, offices or even public areas. A direct consequence of its high market penetration is to suffer some possible attacks or threats related with the costumer's privacy. Also, mobility is one of the most important concerns in these type of networks. Therefore, several amendments to the basic 802.11 standard have been developed or are under development by the 802 LAN/MAN IEEE Standards Committe (LMSC) Working Group (WG).

The principal privacy threaten Institute of Electrical and Electronics Engineers (IEEE) 802.11 equipment is facing today is that they are trackable devices. The device contains a unique hardware identity that gets registered on every Access Point (AP) the station goes by or associate to, when the wireless interface is on. This unique hardware number or physical address is the Media Access Control (MAC) address. Several organizations pointed out this privacy issue to the IEEE 802 Executive Committee on 2014. These organizations are Internet Engineering Task Force (IETF), Internet Architecture Board (IAB), National Institute of Standards and Technology (NIST) and enterprises as Cisco and IntelDigital, all of them are working together to get to a solution in a study group. The Executive Committee (EC) created, on July 2014, the IEEE 802 EC Privacy Recommendation Study Group (SG).

Among the several lines of work of the SG, this paper focuses on the implication of MAC address changes. The randomization of these addresses is the most likely solution to avoid device tracking. A few software programs provide this type of service, under special conditions. These softwares do not provide address changing during a wireless connection, that is to say, being associated to an AP.

The main purpose of this project is to analyze the behavior of the network when performing a MAC address change while being associated to an AP. To make it more useful, the analysis was performed in a IEEE 802.11r network. The project required to implement this type of network, with different types of security methods, and using a packet network analyzer.

The IEEE 802.11r, known as the fast secure roaming amendment, works in a mobility domain performing Basic Service Set (BSS) transitions. BSS transitions requires cooperation between the access points in the same Extended Service Set (ESS) but the details of their communication are not defined in the standard, vendors decide how to complete this function.

In a IEEE 802.11r network, when a client Station (STA) first enters the mobility domain an authentication process takes place. Beyond that moment, when the station moves between access points, the client will be using Fast Basic Service Set Transition (FT) BSS transitions.

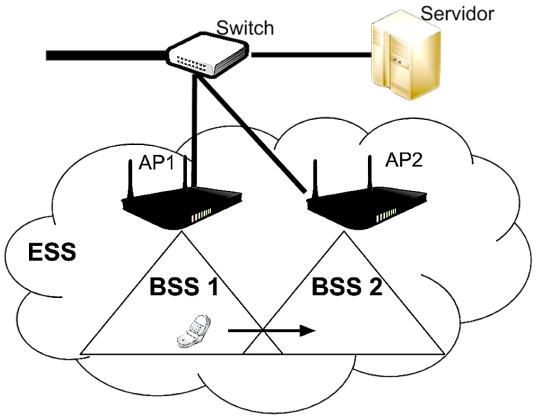

Figura A.1: BSS transition.

During the FT initial mobility domain association, the STA exchanges with the AP the IEEE 802.11 Open System request/response frames. Afterwards, both devices indicate a FT process will be performed in the future during the association frame exchange. Later on, a 4-Way Handshake takes place to create the encrypted keys.

Subsequently, when the STA roams two types of FT BSS transition could be performed: Over-the-Air and Over-the-DS. As the name suggests, Over-the-Air FT BSS transition frame exchange occurs between the STA and the target AP over the wireless network. Two types of frames, with their following responses, are performed, *Authentication* and *Reassociation* frames. These frames are arranged as Management frames.

On the other hand, Over-the-DS FT BSS transition has two ways of exchanging frames. First the STA sends FT *Action* frames to the target AP through the original associated AP. The original AP forwards these frames through the Distribution System (DS) to the target ap. When the Response frame gets to the STA, the following frames are sent by the wireless network, over the air. Those frames sent by air are *Reassociation* frames.

In this project, several security mechanisms were studied and implemented: pre-RSNA methods, such as Open System authentication, Shared key authentication and WEP encryption, and RSN methods, such as WPA and WPA2. Additionally, an access control protocol based on ports defined in the IEEE 802.1x-2004 standard were also implemented, a Remote Authentication Dial-In User Service (RADIUS) server.

A.2. Design overview and analysis

The deployment of the network was performed with several hardware devices and software tools, a list of them is provided:

1. **Hardware devices**

   - Raspberry pi
   - Alix
   - Linksys
   - NetGear GS608
   - Intel Core 2 Quad
   - Ethernet cables.

2. **Software tools**

   - Gnu/Linux and based distributions
   - Hostapd
   - Wpa_supplicant
   - Freeradius
   - MySQL
   - Macchanger
   - Wireshark

The infrastructure network design consists on two access points using Hostapd, one client station with Wpa_supplicant, a switch and a server running Freeradius. Two Raspberry pi, two Alix and a Linksys are used as access points, an additional Raspberry pi is used as the client station, the switch is NetGear GS608 and an Intel Core 2 Quad as the server. The network is represented in the next Figure A.2:

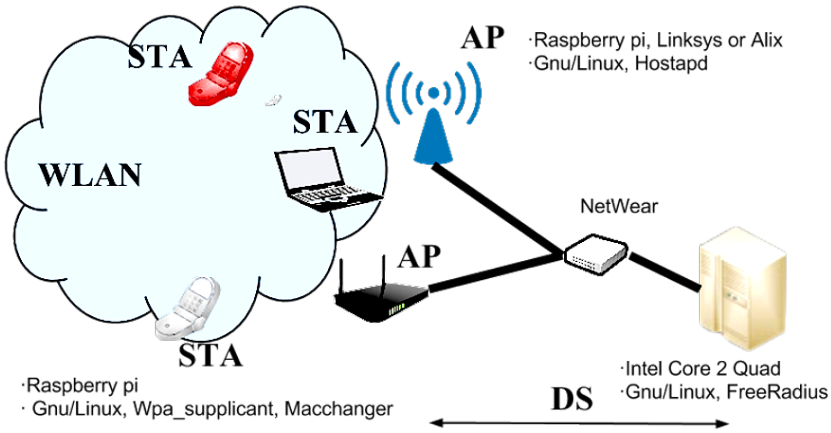

Figura A.2: Infrastructure Network Design.

Once the network was established, a set of tests were performed to complete the study. These tests were executed progressively, test one had to be completed to perform test two and so on :

1. **Test I** — Check the correct settings of the implemented network looking through the messages exchanged, and Hostapd, Wpa_supplicant and FreeRadius configuration files with the following security and authentication methods:
   - WEP encryption.
   - WPA/WPA2-PSK security.
   - IEEE 802.1X authentication.
   - All the above with IEEE 802.11r support.

   Nevertheless, every time a new functionality was added, the network was tested to check whether it worked properly or not.
2. **Test II** — Monitor the roaming process in an IEEE 802.11r network and compare the time duration on each type of configuration, with and without 802.11r support. The analyzer Wireshark has been used to capture the traffic generated during the roams and to measure the time intervals.
3. **Test III** — Test the effect of changing the MAC address using the Linux utility Macchanger, in three different situations:
   - Just when the STA first associate to an AP.
   - First roam to an AP and then change the MAC address.
   - Change the address before performing the next roaming.
4. **Test IV** — Test the services scalability of a RADIUS server performing MAC address spoofing.

A.3. Conclusions

Based on the above tests results, the roaming time duration depends on the setting a customer uses to implement the wireless network. Using the lowest type of security method, WEP encryption, is the fastest roaming performance, whereas the highest level of security with IEEE 802.1X authentication lasts the most. IEEE 802.11r reduces significantly the roaming duration while increasing the level of security, an improvement of nearly 50 ms was measured. Despite of using this support the time duration could not be reduced to the WEP encryption roaming duration.

Performing MAC address spoofing during a wireless connection consequence is the creation of a new client each time the address is changed. This outcome causes an appreciable loss of data, as the initial message exchange has to be performed again. There exists a time where the mobile device remains disconnected as the wireless interfaces have to be disabled when spoofing the MAC address.

Adding the disconnected time to the duration of the initial message exchange, there is a lack of connectivity that could be crucial in certain wireless connections, such as when downloading or uploading information or great packets of data. Not to mention, the software issues MAC address randomization generates on those applications that base their working process on this identifier.

Furthermore, the creation of new clients had been used to test the service scalability of a RADIUS server but some hardware issues appeared during the process. As a result of this controversy it was found that some access points can not hold up a high amount of active clients at the same time due to a kernel capacity problem, so the RADIUS service scalability could not be tested with the hardware provided.

After the development of the network and with all the test runs, it can be asserted that the initial requirements of this project have been fulfilled as the network works properly and the analysis was performed and documented. There are several improvements that could be made in order to enhance the study or to perform as a different line of work:

- **Try to block Deauthentication frames.** To avoid the deauthentication of the MAC address when disabling the wireless interface.
- **Create an application to control the MAC spoofing.** Choose to use this support or not.
- **Combine the above application with an Intrusion detection application.** A MAC spoofing process will start whenever a intruder is detected.
- **Use multiple wireless interfaces.** Spoof the MAC address of one of them while the other is on a wireless connection.

Apéndice B

Introducción IEEE 802.11

En 1980 se creó un comité en el Institute of Electrical and Electronics Engineers (IEEE) con el fin de crear estándares para las tecnologías que trabajasen sobre redes de área local, *Local Area Networks (*LAN*)*, y de área metropolitana, *Metropolitan Area Networks (*MAN*)*, recibió el nombre de "*802 LAN/MAN IEEE Standards Committe (*LMSC*)*" . Se compone de diversos Grupos de Trabajo, Working Groups (WGs), que elaboran la documentación técnica y especificaciones individuales que constituyen los estándares que se centran en las disciplinas de LANs y MANs.

IEEE 802.1	Bridging and Management
IEEE 802.2	Logical Link Control
IEEE 802.3	Ethernet
IEEE 802.11	Wireless LANs
IEEE 802.15	Wireless PANs
IEEE 802.16	Broadcast Wireless MANs
IEEE 802.17	Resilient Packet Rings
IEEE 802.19	TV White Space Coexistence Methods
IEEE 802.20	Mobile Broadband Wireless Access
IEEE 802.21	Media Independent Handover Services
IEEE 802.22	Wireless Regional Area Networks

Cuadro B.1: Grupos de trabajo IEEE 802 activos.

El estándar 802.1, Definición Internacional de Redes, detalla la relación entre los estándares 802 IEEE y el Modelo de Referencia para Interconexión de Sistemas Abiertos (Open System Interconnection (OSI)) de la Organización Internacional de Estándares (International Organization for Standardization (ISO)). Este Modelo se creó, en 1984, para ayudar a los diseñadores de red a implementar redes que pudieran comunicarse y trabajar en conjunto, el objetivo principal era conseguir mayor compatibilidad y interoperabilidad entre las diferentes tecnologías de red utilizadas por los distintos fabricantes a nivel mundial. Se divide en siete niveles o capas numeradas, cada una de las cuales ilustra/efectúa una función de red específica.

Núm.	Nivel	Función
7	Aplicación	Datos normalizados
6	Presentación	Interpretación de los datos
5	Sesión	Diálogos de control
4	Transporte	Integridad de los mensajes
3	Red	Encaminamiento
2	Enlace	Detección de Errores
1	Físico	Conexión de equipos

Cuadro B.2: Niveles complementados en el modelo OSI de ISO

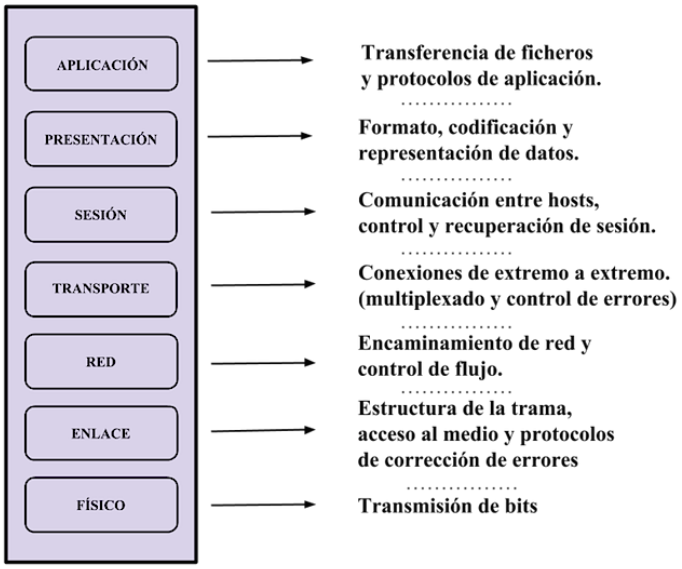

Figura B.1: Cada nivel se ocupa de una determinada labor, prestando servicio al nivel superior.

Los objetivos del comité LMSC se centran en la definición de los niveles más bajos de este modelo, concretamente en el nivel Físico y en el nivel de Enlace que está dividido en dos subcapas: Enlace Lógico (Logical Link Contro (LLC)) y el de Control de Acceso al Medio (Media Access Control (MAC)). La subcapa MAC son un conjunto de normas que determinan como acceder al medio y el envío de datos, mientras que los detalles de la transmisión y la recepción pertenecen a la capa Física. La mayoría de los estándares

802 definen una parte de la capa Física o de la subcapa MAC o de ambas. El estándar 802.2, Control del Enlace Lógico, asegura que los datos sean transmitidos de forma fiable por la capa de Enlace centrándose en la definición del LLC, como podemos observar en la Figura B.2.

El estándar 802 más común basado en el funcionamiento de las capas Física y MAC es el 802.3, Redes CSMA/CD o *Ethernet*, el cual define el funcionamiento del método de Acceso Múltiple con Detección de Colisiones,Carrier Sense Multiple Access network with Collision Detection (CSMA/CD), en varios medios. También define la conexión de redes por cable coaxial, por cable par trenzado y fibra óptica, *Fiber Distributed Data Interconnect (*FDDI*)*.

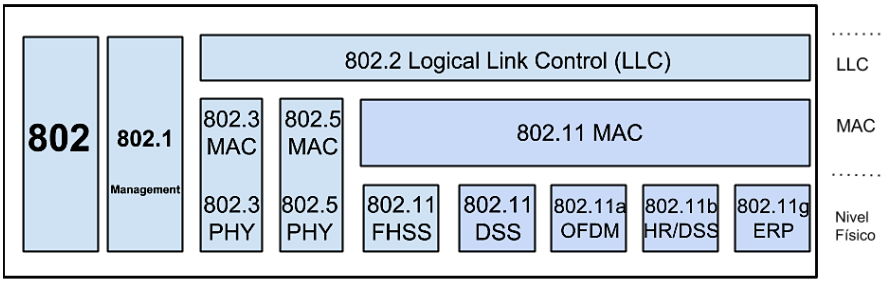

Figura B.2: Nivel Físico y de Enlace utilizado por los estándares IEEE 802.

Si un usuario debe conectarse a la red por cable, se ve drásticamente reducida su capacidad de movimiento. Para solucionar esta dificultad, en septiembre de 1990, se definió el estándar 802.11 que especifica las normas de funcionamiento en la red de área local inalámbrica, Wireless Local Area Networks (WLAN). Fue diseñado para proporcionar una experiencia lo más parecida posible a la conexión por cable y para trabajar en los rangos de frecuencias Industriales, Científicas y Médicas (rango ISM). El primer estándar 802.11 fue liberado en 1997.

Uno de los logros del 802.11 fue conseguir la unión de dos disciplinas diferentes, diseño de radio analógica y diseño de protocolos de red. El estándar 802.11 se adapta completamente al marco de trabajo del comité 802 LMSC, los sistemas compatibles con el estándar se pueden añadir a las redes existentes de forma transparente, definiéndolo así como un estándar de red. Las redes inalámbricas IEEE 802.11 soportan los protocolos de red, la encapsulación y las aplicaciones de uso que se definieron con anterioridad en el estándar IEEE 802 LAN.

La especificación 802.11 incluye la subcapa MAC y dos capas físicas: Espectro Ensanchado por Salto de Frecuencia, *Frequency-Hopping Spread-Spectrum (*FHSS*)*, y Espectro Ensanchado por Secuencia Directa, *Direct-Sequence Spread-Spectrum (*DSSS*)*. Revisiones posteriores a 802.11 han definido nuevas partes de la capa Física. Por ejemplo, 802.11a describe una capa física basada en *Orthogonal Frequency Division Multiplexing (*OFDM*)* y 802.11b específica un nivel *High-Rate Direct-Sequence (*HR/DSSS*)* .

Niveles OSI en 802.11

Capa Física

Para poder implementarlo, la capa Física es relativamente compleja, cuenta de dos componentes principales: *Physical Layer Convergence Procedure (*PLCP*)*, para asignar las tramas MAC con el medio, y *Physical Medium Dependent (*PMD*)* , para enviar esas tramas. El PLCP marca la frontera entre la subcapa MAC y la capa Física, este componente añade tramas a los mensajes que se transmiten "por el aire" .

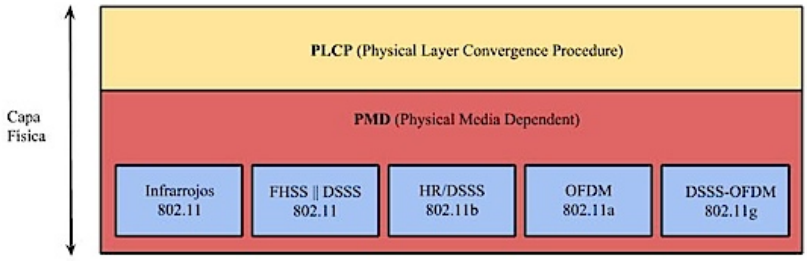

Figura B.3: Capa Física del estándar 802.11.

La capa MAC se refiere a una trama 802.11 como MAC Protocol Data Unit (MPDU), mientras que la capa Física la llama *PLCP Service Data Unit (*PSDU*)* . El PLCP prepara el PSDU para transmitir creando el *PLCP Protocol Data Unit (*PPDU*)* que es modulado por el PMD, y después transmitido.

Nivel de Enlace

El nivel de Enlace 802.11 se divide en dos subcapas:

- La parte superior es el LLC , IEEE 802.2, que es idéntico para todas las tecnologías 802.
- La parte inferior es la subcapa MAC, que es idéntica para toda la tecnología 802.11. El estándar 802.11 define las operaciones en esta subcapa, actúa como interfaz entre la capa inferior Física y la superior de la capa de Enlace, LLC.

MSDU

Cuando la capa de Red (capa o nivel 3) le envía datos a la capa de Enlace (capa o nivel 2), la información se entrega al LLC y se convierte en *MAC Service Data Unit (*MSDU*)*. El MSDU contiene datos del LLC y de las capas 3 a la 7. Se define como la carga de

datos (payload) que contiene el mensaje a transmitir y datos LLC.

Existen tres principales tipos de tramas 802.11; tramas *Management* (Administración), tramas de Control y tramas de Datos. Sólo las tramas de Datos llevan carga MSDU en el cuerpo de la trama. El tamaño del cuerpo de la trama se define por el tamaño máximo del MSDU (2,304 bytes) y algún resto de la encriptación.

MPDU

Una vez que el LLC manda el MSDU a la subcapa MAC, un encabezado MAC se añade para poder identificar al MSDU y se encapsula en una MPDU. Una MPDU es una trama 802.11 que contiene dos encabezados MAC, un cuerpo de tamaño variable y un *trailer*. Cuando estos elementos se unen correctamente, la trama está preparada para enviarla a la capa Física.

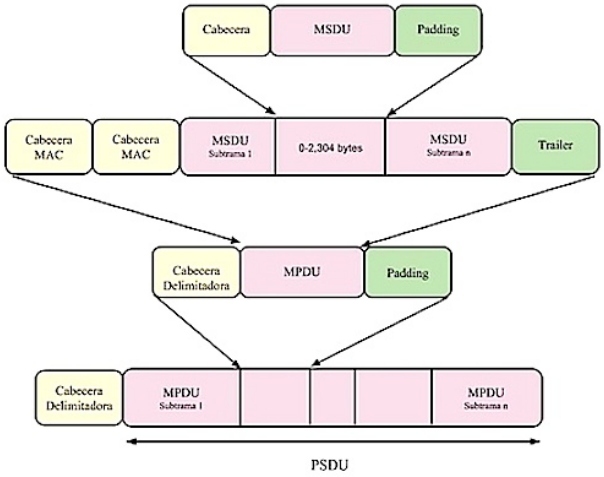

Figura B.4: Encapsulación de las tramas del nivel Enlace al Físico.

Nomenclatura

El protocolo 802.11 consta principalmente de cuatro componentes:

Distribution System (DS)

Es un componente lógico utilizado para encaminar los mensajes a su destinatario. Cuando varios puntos de acceso están colocados para cubrir un área, deben de comunicarse a través del DS para poder localizar las estaciones móviles. 802.11 no especifica ningún tipo de tecnología para poder implementar este componente, normalmente se compone de

una combinación de medios DS, como Ethernet y dispositivos puentes (bridging engines) formando una red troncal (backbone network).

Puntos de acceso (APs)

Estos dispositivos realizan la función de transformar las tramas del protocolo 802.11 a otro tipo para comunicarse con el resto del mundo, se llama *wireless-to-wired bridging function*. Efectúan muchas otras funciones pero esta es sin duda la más importante.

Medio Inalámbrico (WLAN)

Se utiliza para enviar los mensajes de estación en estación, esta arquitectura permite varios tipos de capa física para poder soportar 802.11 MAC. En sus orígenes dos capas físicas de radio frecuencia (RF) y una de infrarrojos fueron definidas.

Estaciones (STA)

La red está diseñada para poder enviar información a través de éstas, son aparatos electrónicos con interfaces para red inalámbrica. Normalmente se tratan de ordenadores o tecnología portátil.

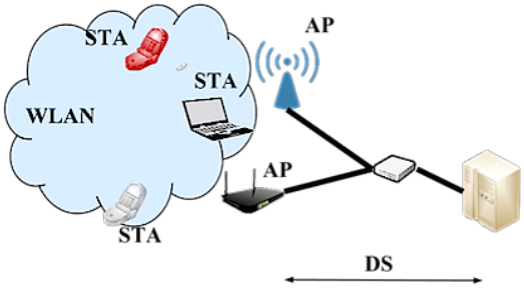

Figura B.5: Componentes principales de una red 802.11

Tipos de estructuras

La estructura básica de la red 802.11 es la *basic service set* (BSS), consiste en un grupo de estaciones que se comunican entre ellas. El área donde se realiza la comunicación se llama *basic service area*.

Red Independiente

Las estaciones en una *Independent BSS* (IBSS) se comunican directamente entre ellas y deben encontrarse en un rango preciso para que pueda realizar esta comunicación. La red 802.11 más pequeña que puede existir es una IBSS con dos estaciones. Normalmente, estas redes se establecen para cortos periodos de tiempo y son más conocidas como ad hoc BSSs o redes ad hoc. Por ejemplo, se crean para conferencias de trabajo o eventos sociales.

Red de Infraestructura

Estas redes se distinguen por el uso de un punto de acceso, utilizado para todo tipo de comunicaciones. Si dos estaciones móviles quieren comunicarse entre ellas, la información debe de dar dos saltos. Primero, la estación emisora pasaría su mensaje al punto de acceso y, después, el punto de acceso redireccionaría el mensaje a la estación destino. El área de servicio, en este tipo de red, abarca todo punto donde pueda llegar el punto de acceso, este tipo de transmisión de información (multihop) tiene dos ventajas principales:

- No hay una distancia mínima entre las estaciones móviles. Consume más capacidad que en una comunicación directa pero no hay tanta complejidad en la capa física de los dispositivos.
- Un punto de acceso en esta red puede ayudar a una estación que no quiera consumir mucha batería.

En una red de infraestructura, las estaciones deben asociarse a un punto de acceso para poder obtener servicio de red. La Asociación es el proceso por el cual una estación se une a una red 802.11; parecido al acto de conectar un cable Ethernet a la red. El punto de acceso tiene la responsabilidad de garantizar o denegar esa asociación basado en el mensaje *Association Request* recibido. Una estación puede estar asociado solo con un punto de acceso a la vez. El estándar 802.11 no establece un límite de estaciones que puedan estar asociadas a un mismo punto de acceso, eso depende de la implementación física del punto de acceso y el rendimiento de la red inalámbrica.

Extended service area

Una BSS puede dar cobertura a una pequeña oficina o una casa, pero no puede abarcar grandes superficies. 802.11 permite unir varias BSSs y formar un *Extended Service Set* (ESS) mediante una red *backbone*.

Las estaciones en una misma ESS pueden comunicarse entre ellas aunque estén en diferentes BSS y moviéndose por ellas. La comunicación entre las estaciones en una misma ESS debe realizarse mediante la capa de enlace. Los puntos de acceso actúan como puentes, así que se requiere que la red troncal también sea una red de conexión de nivel 2. Varios puntos de acceso en un área pequeña pueden ir conectados a un mismo centro de actividad (hub) o conmutador (switch), o pueden usar LANs virtuales para poder extender el área. Los puntos de acceso en una ESS trabajan al unísono para permitir que el mundo exterior utilice una única dirección MAC para poder comunicarse con una estación dentro de la ESS. El router utiliza una única dirección MAC para enviar tramas a una estación móvil; el punto de acceso al que esta asociado la estación móvil es el que realiza este envío. El router ignora la posición de las estaciones y confía en los puntos de acceso para enviar esas tramas.

Servicios de Red

IEEE 802.11 ofrece nueve servicios; sólo tres de ellos son para la transmisión de información y los otros seis son operaciones de administración que permiten seguir el rastro de los nodos móviles y enviarles sus respectivas tramas.

El servicio DS (distribution system service, DSS) se compone de los servicios de la subcapa MAC proporcionados por el DS. Ya que el IEEE no especifica la implementación del DS, la arquitectura que usa el DSS puede ser utilizada por diferentes tipos de WLANs, incluidos APs y controladores WLAN.

El servicio STA (station service, SS) lo usan todas las estaciones 802.11 clientes incluyendo los APs, ya que tienen funcionalidades de STA. La mayoría de los fabricantes de controladores WLAN implementan una arquitectura de MAC dividida, eso conlleva que algunos de los servicios MAC los maneja el controlador y otros los puntos de acceso basados en controladores.

Los servicios de red ofrecidos son los siguientes:

Distribution

Este servicio se usa en las redes de infraestructura siempre que las estaciones móviles quieren transmitir datos. Cuando un punto de acceso acepta una trama, circula por el *distribution service* para llegar a su destino. Cualquier tipo de comunicación que use puntos de acceso pasa por el DS, incluyendo aquellos nodos móviles conectados al mismo punto de acceso.

Integration

Es un servicio ofrecido por el DS; permite la conexión del DS con una red no-IEEE 802.11. No está especificada por el 802.11 excepto el servicio que se debe ofrecer.

El DSS conecta los puntos de acceso al DS. El principal papel de los puntos de acceso es transformar el servicio de la red de cableado a la red inalámbrica; se consigue mediante los servicios de Distribución e Integración.

Association

La transmisión de tramas a las estaciones móviles es posible gracias a que estas se conectan, o asocian, a los puntos de acceso. El DS puede utilizar la información de registro para saber que punto de acceso utilizar para cualquier estación conectada. 802.11 especifica las funciones que el DS debe de ofrecer utilizando la información de asociación pero no obliga a implementarlo de una forma concreta.

Reassociation

Cuando una estación móvil se mueve entre basic service áreas en una misma ESS, la estación debe evaluar la fuerza de la señal y cambiarse de punto de acceso, si lo considera necesario. Este proceso es iniciado por la estación móvil cuando las circunstancias señalan que un cambio de punto de acceso sería beneficioso para la conexión. Una vez se completa el cambio, el DS actualiza la posición en la que se encuentra el dispositivo.

Dissasociation

Este servicio es utilizada por la estación para terminar una asociación, se borra toda la información de movilidad de la estación guardada en el DS.

Authentication

Las redes inalámbricas no ofrecen el mismo nivel de seguridad físico que las redes por cable, por eso se necesita procesos de autenticación adicionales para asegurarse de que los dispositivos que acceden a la red están autorizados a hacerlo. La autenticación es un pre-requisito para que una estación pueda asociarse con un punto de acceso.

Deauthentication

Este proceso termina una relación de autenticación, un efecto secundario es la finalización de cualquier asociación.

Entrega MSDU

Las redes no serían útiles si no consiguieran transmitir la información a su destino. Las estaciones tienen el servicio de entrega MSDU, que es el responsable de hacer llegar los datos al final del camino.

Tramas 802.11

Las tramas 802.11 son diferentes a las tramas de red de cableado como las de IEEE 802.3, las cuales utilizan un sólo tipo de trama de datos. El estándar IEEE 802.11 utiliza tres principales tipos de trama: management, de control y de datos. Estos tipos, a su vez, se dividen en diversos subgrupos.

Tramas Management

Las tramas 802.11 management componen la mayoría de tipos de trama en una WLAN. Las estaciones inalámbricas utilizan estas tramas para conectarse y desconectarse de un BSS. No son necesarias en las redes de cableado ya que la función que realizan se ejerce conectando y desconectando el cable de la red físicamente. En una red inalámbrica las estaciones las usan para buscar una red WLAN compatible, autenticarse con dicha red (asumiendo que se permita la conexión), y para finalizar, asociarse (normalmente con un AP) para garantizar el acceso a la red.

Otra forma de llamar a las tramas 802.11 management es *Management MAC Protocol Data Unit (*MMPDU*)*. Tienen un encabezado MAC, un cuerpo de trama y un trailer. Éstas tramas no llevan ninguna información de capas superiores por lo que no contienen MSDU encapsulados. Los campos de información en el cuerpo tienen un tamaño fijo pero los elementos de información tienen tamaño variable y son opcionales.

Las tramas Management tienen 12 subtipos, aquí la lista definida según en el estándar 802.11:

1. Association Request
2. Association response
3. Reassociation request
4. Reassociation response
5. Probe request
6. Probe response
7. Beacon
8. Announcement traffic indication message (ATIM)
9. Disassociation
10. Authentication
11. Deauthentication
12. Action

Tramas de Control

Las tramas de control 802.11 ayudan con el envío de tramas de datos. Bajo las condiciones ideales, las tramas de control deberían escucharse por todas las estaciones en un mismo BSS; por ello, se deberían transmitir en la tasa básica (basic rate). Se usan para limpiar el canal, adquirir el canal y ofrecer tramas acknowledgments (ACK) unicast. Contienen únicamente información de encabezado y un trailer, no tienen cuerpo.

La lista de los 8 subtipos de tramas de control definida por el estándar 802.11 es la siguiente:

1. Power Save Poll (PS-Poll)
2. Request to send (RTS)
3. Clear to send (CTS)
4. Acknowledgment (ACK)
5. Contention Free-End (CF-End)
6. CF-End + CF+ACK
7. Block ACK Request (BlockAckReq)
8. Block ACK (BlockAck)

Tramas de Datos

La mayoría de las tramas de datos 802.11 llevan los datos MSDU que vienen de los protocolos de capas superiores. El MSDU de las capas 3-7 se encripta por razones de seguridad. Sin embargo, algunas tramas no llevan carga MSDU, porque no existe carga de datos de las capas 3-7, pero tienen un control MAC específico dentro de un BSS. Hay un total de 15 subtipos de trama de datos, llamadas habitualmente *simple data frame*.

Se muestra una lista de los subtipos de tramas de datos definidos por el estándar 802.11 a continuación:

1. Data (simple data frame)
2. Null function (sin carga MSDU)
3. Data + CF-ACK
4. Data + CF-Poll
5. Data + CF-ACK + CF-Poll
6. CF-ACK (sin carga MSDU)
7. CF-Poll (sin carga MSDU)
8. CF-ACK + CF-Poll (sin carga MSDU)
9. QoS data
10. QoS Null (no MSDU payload)
11. QoS data + CF-ACK
12. QoS data + CF-Poll
13. QoS data + CF-ACK + CF-Poll
14. QoS CF-Poll (no MSDU payload)
15. QoS CF-ACK + CF-Poll (no MSDU payload)

La diferencia entre las tramas 802.3 y las tramas 802.11 son los campos de dirección MAC. Las tramas 802.3 tienen únicamente una dirección origen (Source Address, SA) y una dirección destino (Destination Address, DA) en el encabezado de la capa dos, mientras que, las tramas 802.11 tienen cuatro campos de dirección en el encabezado MAC. Normalmente, las tramas 802.11 sólo usan tres de los campos de dirección MAC. Sin embargo, en las tramas enviadas en una *wireless distribution system* (WDS) necesitas los cuatro campos. El contenido de los cuatro campos pueden incluir las siguientes direcciones MAC: Receptor (receiver address, RA), Emisor (tramsmitter address, TA), Identificador BSS (basic service set identifier, BSSID), Destino (destination address, DA) y Origen/-Fuente (source address, SA). Aunque el número de campos es diferente, los dos estándares tienen un SA, un DA y utilizan el mismo formato de dirección MAC.

Campos de direcciones

Una trama 802.11 puede contener hasta cuatro campos de direcciones, cada campo está numerado ya que cada uno se utiliza para un propósito distinto dependiendo en el tipo de trama. La dirección 1 es para el receptor, la 2 para el emisor, el 3 se utiliza como filtro por el receptor y el 4 sólo se utiliza si existe bridging inalámbrico.

El direccionamiento en 802.11 sigue las reglas y especificaciones iguales que las otras redes IEEE 802, las direcciones son de 48 bits. Si el primer bit enviado al medio físico es un 0, se habla de una dirección *unicast* (de una sola estación), y por el contrario, si es un 1 se trata de una dirección *multicast*. Se trata de una dirección *broadcast*, cuando se manda a todas las estaciones del medio inalámbrico, si todos los bits son 1s.

Dirección Destino // Destination address

Como en Ethernet, es el identificador de 48 bits IEEE MAC que corresponde al último receptor de la trama y maneja la trama para procesar en los niveles superiores del Modelo OSI.

Dirección Fuente // Source address

Identifica la fuente de transmisión, sólo una estación puede ser la fuente.

Dirección del Receptor // Receiver address

Indica que estación inalámbrica debe ser la que procese la trama, siendo igual que la Dirección Destino. Si la trama va destinada a un nodo en una red Ethernet conectada a un punto de acceso, el receptor será la interfaz inalámbrica del punto de acceso y el destino el router asociado a la red Ethernet.

Dirección del Emisor // Transmitter address

Esta dirección de 48 bits IEEE MAC identifica la interfaz inalámbrica que transmite una trama en un medio inalámbrico, se utiliza sólo cuando existe *bridging* (puente) inalámbrico.

Basic Service Set ID (BSSID)

Las estaciones asociadas a una BSS deben tener un identificador para poder diferenciar las distintas LANs inalámbricas de la zona, el BSSID es una dirección MAC usada por las interfaces inalámbricas de los puntos de acceso. En una red Ad hoc se genera un número aleatorio para el identificador y con el bit Universal/Local a 1 para evitar cualquier conflicto con las direcciones MAC asignadas oficialmente.

La mayoría de las tramas utilizan las direcciones de fuente, destino y BSSID. El número de los campos de dirección depende de cómo viaje la trama a través del DS.

Funciones subcapa MAC

Acceso al Medio // Medium Access

El enlace MAC del 802.11 ofrece diversas funciones: acceso al medio inalámbrico, unirse, moverse y dejar la red, y seguridad. El método de acceso Distributed Coordination Function (DCF) es obligatorio en el estándar 802.11 que ofrece además un mecanismo para compartir acceso al medio inalámbrico en un área común. El acceso a la red está controlado por un protocolo de contención llamado Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Este protocolo es parecido, pero no igual, al método utilizado en el cableado Ethernet, CSMA/CD. Si dos o más estaciones están transmitiendo al mismo tiempo sus señales pueden colisionar y puede resultar imposible que el receptor distinga una señal nítida. CSMA/CA obliga a escuchar si el medio está libre o no y bloquearlo cuando se transmita.

Request-to-Send / Clear-to-Send (RTS/CTS)

Los nodos ocultos existen en las redes inalámbricas provocando colisiones en las señales, lo que reduce el rendimiento.. El mecanismo 802.11 RTS/CTS pueden usarlo opcionalmente las estaciones y los puntos de acceso para anunciar la intención de transmisión de datos unicast y tramas management durante un cierto umbral de tiempo para limitar el tiempo de retransmisión cuando existen nodos ocultos.

Management

EL estándar 802.11 define un Management Information Base (MIB) que contiene parámetros que inciden en las operaciones de una WLAN. Es posible la interacción con el MIB mediante el protocolo *Simple Network Management Protocol (*SNMP*)* en una red IP.

Transmisión de tramas // Frame transmission

El propósito de 802.11 es mover los paquetes de niveles superiores a través de las interfaces inalámbricas. Esto conlleva la encapsulación de los paquetes en tramas de información 802.11. Una estación debe seguir unas instrucciones específicas para poder enviar una trama cuando las condiciones del medio sean las ideales. Los elementos de tiempo son la clave de este proceso. Cuando una estación recibe tramas unicast o de management la contestación inmediata con tramas de confirmación positiva (positive acknowlgedment frames, ACK) es muy importante.

Tiempo de Acceso // Access Timing

IEEE 802.11 define cuatro intervalos de tiempo que definen prioridad y el acceso de la estación al medio, espacios intertramas, InterFrame Spaces (IFS).

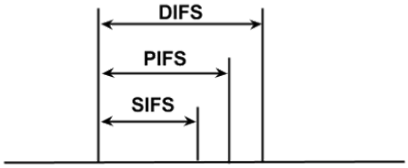

Figura B.6: Diferencia de longitud entre las diferentes intertramas.

- SIFS (Short IFS): Es el más corto de los intervalos, proporcionan el mayor nivel de prioridad de acceso al medio. Lo utilizan:
  - Tramas Acknowledgement (ACK)
  - Clear-to-Send (CTS)
  - Segundo fragmento de una ráfaga
- PIFS (Point Coordination Function (PCF) IFS): Este es el intervalo con el que los puntos de acceso que estén operando bajo PCF tienen preferencia a aquellas estaciones que trabajen en modo DCF. Los puntos de acceso solo usan este modo cuando envían *beacon* o para retransmitir tramas cuando no han recibido una trama ACK.
- DIFS (DCF IFS): Todas las estaciones operando bajo DCF utilizan este intervalo para transmitir tramas de información o management.
- EIFS (Extended IFS): Las estaciones con modo DCF utilizan este intervalo siempre y cuando la capa física haya indicado a la MAC que una transmisión iba a comenzar pero que la recepción de una trama MAC no se hubiera recibido de la forma correcta.

$$\text{PIFS} = \text{SIFS} + \text{Ranura de Tiempo}$$
$$\text{DIFS} = \text{SIFS} + \text{Ranura de Tiempo} + \text{Ranura de Tiempo}$$

Apéndice C

Organizaciones

C.1. IEEE

El Institute of Electrical and Electronics Engineers (IEEE) es una asociación profesional formada en 1963 por la unión de American Institute of Electrical Engineers (AIEE), que fue creada en 1884, y Institute of Radio Engineers (IRE), fundada en 1912. Hoy en día, es la mayor asociación mundial de profesionales técnicos con casi medio millón de miembros alrededor del mundo. Su principal objetivo es la promoción educativa y técnica las ingeniería eléctrica y electronica, telecomunicaciones, informática y de las disciplinas afines.

Figura C.1: Logo IEEE .[12]

El logo de IEEE representa el diseño en forma de diamante de la regla de la mano derecha, conocida por los matemáticos e ingenieros para resolver cálculos. Fue la unión de los logos de las dos asociaciones fundadoras y se creó en el momento de la constitución de la asociación.

El IEEE incluye 38 sociedades técnicas, organizadas en torno a los campos técnicos especializados, con más de 300 organizaciones locales que celebran reuniones periódicas. El IEEE Standards Association se encarga de la estandarización de las actividades del IEEE. Uno de los grupos de estándares más importantes del IEEE es el IEEE 802 Local Area Networks (LAN)/Metropolitan Area Networks (MAN), el cual incluye el estándar IEEE 802.3 Ethernet y el estándar IEEE 802.11 Wireless Local Area Networks (WLAN).

C.2. Wi-Fi Alliance

Wi-Fi Alliance es una asociación industrial global y sin ánimo de lucro que tiene más de 300 compañías como miembros dispuestos a promocionar el crecimiento de las WLAN. La tarea principal de esta asociación es comercializar la marca Wi-Fi y sensibilizar a los consumidores del desarrollo de las tecnologías 802.11. Fue fundada en 1999 con el nombre *Wireless Ethernet Compatibility Alliance (*WECA*)* se cambió el nombre en 2002.

Figura C.2: Logo Wi-Fi Alliance.[24]

La principal tarea de Wi-Fi Alliance es asegurar la interoperabilidad de la tecnología WLAN realizando pruebas y certificando el producto. Durante los primeros días del estándar 802.11, Wi-Fi Alliance definió adicionalmente algunos requerimientos ambiguos para los estándares y propuso unas reglas para asegurar la compatibilidad entre los diferentes fabricantes. Los productos que pasan el proceso de certificación reciben el Wi-Fi Interoperability Certificate que proporciona información detallada de las certificaciones Wi-Fi de los productos individuales. Estos certificados no sólo aseguran la interoperabilidad de radio (802.11a, 802.11b) también certifican capacidades adicionales como la seguridad, multimedia, convergencia y compatibilidad de características especiales.

Según su página oficial (`http://www.wi-fi.org`), el lema de esta asociación es :

"Connecting everyone and everything, everywhere"
"Conectar a todo y todos, en todas partes"

Según avanzan las tecnologías 802.11, nuevos programas Wi-Fi CERTIFIED son detallados por Wi-Fi Alliance. Y la misión común es consiguir la colaboración de todos sus miembros.

Apéndice D

Configuraciones e instalaciones

Raspberry Pi

El proceso para configurar una Raspberry Pi desde el principio es el siguiente:

1. Elegir sistema operativo que se va implementar y descargar desde la página oficial.
2. Insertar tarjeta SD en el PC y formatear.
3. Copiar el sistema operativo en la tarjeta SD.
4. Retirar la tarjeta SD e introducirla en la Raspberry Pi.
5. Conectar teclado, HDMI, ratón y cable de red. Conectar también el cable de alimentación eléctrica.
6. Escribir raspi_config y seleccionar expandir partición.
7. La Raspberry Pi ya se puede utilizar.

Bridge

Un bridge o puente se utiliza para conectar dos interfaces de red a Nivel 2. Se utiliza, normalmente, para compartir el servicio de red entre varios dispositivos. Consiste en conectar una interfaz con otra que tenga acceso a una red amplia, como internet, y dejar que la interfaz unida pueda utilizar el servicio de red. El proceso para realizar un bridge es el siguiente:

1. En el terminal del AP introducir este comando: **sudo apt-get install bridge-utils**
2. Crear un bridge con : **brctl addbr br0**
3. Asociar a una interfaz: **brctl addif br0 eth0**; **brctl addif br0 wlan0**
4. Configurar la dirección IP de la interfaz elegida a cero: **ifconfig eth0 0.0.0.0**; **ifconfig wlan0 0.0.0.0**
5. Iniciar el bridge: **ifconfig br0 up**

6. Configurar una dirección IP y la máscara subred : ifconfig br0 <DirecciónIP> netmask <Máscara> up
7. El bridge está configurado y actúa como una interfaz única.

Apéndice E

Wireshark

Existen diversos métodos con los cuáles se puede medir un evento de roaming. Estas variaciones existen porque las organizaciones, empresas y distintos desarrolladores tienen diferentes puntos de vista sobre lo que constituye un roam completo. Cada método se puede utilizar en escenarios diferentes, lo que realmente es importante es mantener una coherencia en el enfoque del estudio con el fin de establecer una base para todo el análisis.

El método utilizado en este proyecto es uno de los más comunes, se trata de medir la duración del proceso desde el comienzo de la autenticación y el final del 4-Way Handshake (o el final de la asociación en algunos casos).

El analizador de paquetes Wireshark se puede utilizar como filtro para poder identificar paquetes de interés en un proceso roaming en una red inalámbrica WLAN. El filtro de visualización de paquetes se puede aplicar ya sea durante la captura de tramas o al finalizar ésta. Si se aplica en el primer caso se puede ir observando que el proceso de roaming se está realizando y está siendo capturado correctamente. A continuación, una tabla con los filtros más importantes y los utilizados en este proyecto:

Filtro	**Trama capturada**
wlan.fc.type=0	Trama Management
wlan.fc.type_subtype=0	Association request
wlan.fc.type_subtype=1	Association response
wlan.fc.type_subtype=2	Reassociation request
wlan.fc.type_subtype=3	Reassociation response
wlan.fc.type_subtype=4	Probe request
wlan.fc.type_subtype=5	Probe response
wlan.fc.type_subtype=11	Authentication
wlan.fc.type_subtype=12	Deauthentication
wlan.fc.type_subtype=13	Action frames
wlan.addr=<MAC_address>	Tramas de dirección

Cuadro E.1: Tipos de filtros Wireshark y tramas que capturan.

Se pueden combinar dos filtros con los parámetros lógicos AND y OR, se representan con && y — respectivamente. Se introducen en la barra de herramientas que aparece en la parte superior de Wireshark y definida como “Filter:”, cómo se muestra en la Figura :

Figura E.1: Filtro de Wireshark.

Las reglas de colores (Coloring rules), que se encuentran en el menú de visualización, resultan muy útiles a la hora de diferenciar los paquetes. Esta funcionalidad permite al investigador realizar las pruebas con más fluidez. A continuación, se muestra la regla de colores empleada en este proyecto:

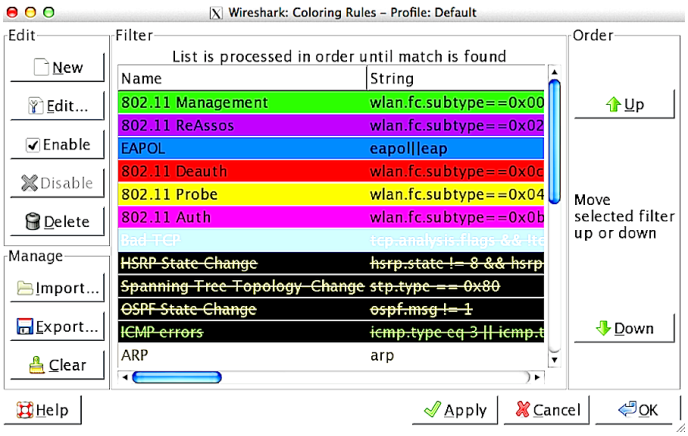

Figura E.2: Reglas de Colores en Wireshark para el proyecto.

Para poder realizar el análisis manual del evento roaming, se debe establecer una referencia de tiempo. Esto permite a Wireshark calcular automáticamente la diferencia de tiempos de las tramas siguientes a la marca de referencia. Se debe poner la marca de referencia en la primera trama del proceso roaming, la trama Authentication request, después, identificar la última trama y fijarse en la columna de tiempo, “Time”. El valor de la columna es el tiempo transcurrido en el evento roaming. Para establecer la marca de referencia en Wireshark, se debe seleccionar la trama y elegir en el menú “Edit” la opción “Set Time Reference (toggle)”.

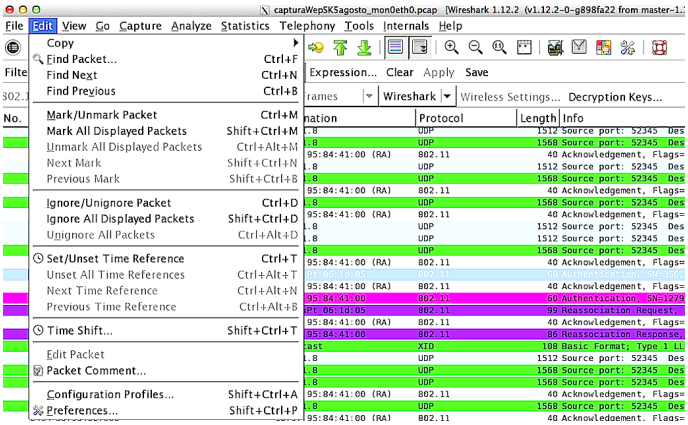

Figura E.3: Cómo establecer una marca de referencia de tiempo.

Una vez establecida la marca y medido los tiempos, se procede al estudio de cada tipo de red configurada y la comparación de dichos tiempos de duración.

Glosario

Ad-hoc Una red inalámbrica, también referida como peer-to-peer, dónde los dispositivos comunican unos con otros directamente sin usar un punto de acceso como hub de comunicación.

ASCII Código normalizado americano para el intercambio de información. Código de 7 elementos establecido para conseguir la compatibilidad entre diversos servicios de datos.

Backbone Segmento central de una red de área extendida que soporta una gran capacidad de tráfico. Red de rango superior que conecta entre sí los nodos de la misma.

Bandas ISM Industrial, Scientific and Medical bands. Tres bandas en 900MHz, 2,4 y 5,8GHz que fueron originalmente reservadas para uso bajo licencia en aplicaciones industriales, científicas y médicas.

Base de Datos Database. Conjunto de datos operacionales utilizados por todas las aplicaciones de una organización. Suelen contener cantidades masivas de información.

Bridge Puente. Elemento que permite enlazar redes de igual naturaleza, y cuya función es gestionar el tráfico de mensajes entre ambas. Trabaja en la capa de enlace OSI.

Broadcast Sistema de transmisión por el cual se envía un paquete a todos los receptores o estaciones de una red.

Cabecera Parte inicial de un mensaje o paquete, que normalmente contiene información para el control y encaminamiento del mismo.

Calidad de Servicio QoS. Es un parámetro significativo a la apreciación que el usuario hace de un determinado servicio, compuesto de varios factores.

Campo Field. Cada uno de los datos individuales de un registro o ficha, como pueden ser el nombre, dirección, etc. Zona reservada para un conjunto de datos.

Canal de transmisión Enlace a través del cual se realiza el envío de información desde un equipo a otro.

Carácter Letra, número, símbolo, signo, etc., que forma parte de un mensaje, o que se usa para funciones de control.

Cifrado Cyphering. Procedimiento por el cual la información original se transforma en otra, siguiendo determinados algoritmos de conversión, de forma que resulte ininteligible.

Conectividad Connectivity. Capacidad de un dispositivo informático para comunicarse con otros.

Controlador Controller. Dispositivo que actúa como interfaz entre un ordenador y la red o entre ésta y un grupo de terminales.

Data rate Velocidad de transferencia, número medio de elementos binarios, caracteres o bloques transferidos por unidad de tiempo desde el emisor hasta el receptor.

Datos Conjunto de información codificada en un formato aceptable para los ordenadores y terminales.

Dirección Secuencia de elementos binarios que indican el destino final de una comunicación o de un conjunto de datos.

Encriptación Consiste en la alteración de la señal original, de tal forma que no pueda ser reconocida, empleando un código secreto.

Enlace Conjunto de elementos, que bajo el control de un procedimiento, establece una conexión entre un equipo emisor y otro receptor.

Ethernet Red de área local con topología de bus sobre cable coaxial, que sigue la norma IEEE 802.3, utilizando el protocolo CMSA/CD.

Fichero Una colección de datos estructurados de una determinada manera y empleados con un determinado propósito.

Handshaking Intercambio de códigos y señales entre dos terminales previo al establecimiento de la comunicación.

Hardware Conjunto de elementos físicos, mecánicos o eléctricos que integran un ordenador o terminal.

Hub Dispositivo de red que proporciona un punto central de conexión para otros dispositivos.

Interconexión Conjunto de medios de interacción de una serie de componentes físicos y lógicos.

Interfaz Nexo de interconexión, hardware o software, que facilita la interconexión/comunicación entre dos dospositivos.

Internet Nombre de la red internacional más grande, conectando miles de nodos en todo el mundo, que procede de la red Arpanet.

Jitter Variación de latencia. Distorsión producida en una señal por la variación inesperada de una de sus características.

Latencia Tiempo transcurrido desde que un paquete es enviado desde su fuente a su destino.

Modulación Proceso por el cual se varía la señal portadora, en amplitud, frecuencia o fase, según la señal a transmitir.

Multicast Técnica que permite enviar la copia de un paquete a un conjunto seleccionado de posibles destinos.

Multiplexar Método para compartir un canal de transmisión por varios usuarios de forma simultánea. Las técnicas más habituales son por División de Frecuencia (FDM), y por División de Tiempo (TDM).

Módem Equipo MOdulador/DEModulador que transforma las señales digitales en analógicas y viceversa, para que puedan ser transmitidas por un circuito telefónico adecuadamente.

Nodo Punto de una red de datos, donde se interconectan varias unidades funcionales a líneas de transmisión de datos.

Paquete Conjunto de datos de información y caracteres de control, que transmitidos en bloques de mayor o menor longitud, disponen de la información necesaria para alcanzar su destino.

Procesador Unidad que controla el flujo de datos entre el ordenador principal y la red de transmisión de datos, proporcionando las conexiones necesarias.

Protocolo Conjunto de normas y reglas utilizado para establecer y mantener una comunicación de datos entre las diversas estaciones que componen un enlace.

Puerto Interfaz de un ordenador, configurado en modo terminal, y a través del cual se realiza la entrada/salida de datos.

Punto de acceso Access Point. Dispositivo de red inalámbrico que actúa como hub y conecta una red inalámbrica a una red de cable o a internet.

Red local Red de comunicaciones de altas prestaciones, diseñada para la interconexión de equipos que se encuentran próximos.

Red de datos Conjunto de elementos que interconectan ordenadores y terminales, basándose en una red de telecomunicaciones.

Router Nodo que asume las funciones de encaminar el tráfico de la red hacia los nodos de destino siguiendo la ruta más apriopiada; al operar a nivel de red, depende del protocolo.

Servidor Procesador que proporciona un servicio específico a la red.

Software Conjunto de programas y aplicaciones que pueden ser ejecutados sobre un ordenador.

Terminal Dispositivo de entrada/salida, de propósito general, que realiza el control de la transferencia de información según un determinado protocolo.

Trama Frame. Unidad empleada por algunos protocolos de comunicaciones, que contiene información a transmitir, así como campos de control.

Tráfico Cantidad de información cursada por una vía de comunicación.

Tunnelling Técnica para crear un enlace seguro en una red encapsulando los paquetes acorde a un protocolo.

Unicast Método por el cual un paquete es enviado a un destino único.

Bibliografía

[1] "802.1x port-based authentication howto." [Online]. Available: http://tldp.org/HOWTO/html_single/8021X-HOWTO/

[2] Arch linux wpa_supplicant. [Online]. Available: https://wiki.archlinux.org/index.php/WPA_supplicant

[3] "Archlinux." [Online]. Available: https://wiki.archlinux.org/

[4] "Cisco." [Online]. Available: http://www.cisco.com/web/ES/index.html

[5] "Configuring ieee 802.1x portbased authentication." [Online]. Available: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2950/software/release/12-1_22_ea11x/configuration/guide/scg/sw8021x.html#wp1029843

[6] "Debian." [Online]. Available: https://www.debian.org/

[7] "Download raspbian." [Online]. Available: https://www.raspberrypi.org/downloads/raspbian/

[8] "Freeradius configuration files." [Online]. Available: http://wiki.freeradius.org/config/Configuration-files

[9] "The freeradius project." [Online]. Available: http://freeradius.org/

[10] "Gnu/linux logo." [Online]. Available: https://upload.wikimedia.org/wikipedia/commons/thumb/c/c9/Gnulinux.svg/170px-Gnulinux.svg.png

[11] "Hostapd configuration file." [Online]. Available: https://w1.fi/cgit/hostap/plain/hostapd/hostapd.conf

[12] "Ieee logo." [Online]. Available: http://www.ieee.org/about/toolkit/masterbrand/20040815

[13] "Internet architecture board." [Online]. Available: https://www.iab.org/

[14] "The internet engineering task force." [Online]. Available: https://www.ietf.org/

[15] "Linksys-wrt160nl." [Online]. Available: http://www.pccomponentes.com/linksys_wrt160nl_router_neutro_802_11n___usb.html

[16] Mac privacy. [Online]. Available: http://www.ietf.org/blog/2014/11/mac-privacy/

[17] "National institute of standards and technology." [Online]. Available: http://www.nist.gov/

[18] "Netgear-gs608." [Online]. Available: http://www.amazon.es/Netgear-GS608-300PES-Switch-puertos-Gigabit/dp/B000BZUGLM

[19] "Pc engines." [Online]. Available: http://www.pcengines.ch/order1.php?c=2

[20] "Qué es bsd." [Online]. Available: https://www.freebsd.org/doc/es_ES.ISO8859-1/articles/explaining-bsd/article.html

[21] "Raspberry pi." [Online]. Available: https://www.raspberrypi.org/

[22] "Raspberry pi b." [Online]. Available: http://www.raspipc.es/public/home/

[23] "Redzone." [Online]. Available: http://www.redeszone.net/

[24] "Wifi alliance." [Online]. Available: http://www.wi-fi.org/

[25] "Wireshark." [Online]. Available: https://www.wireshark.org/

[26] Wpa_supplicant configuration file. [Online]. Available: https://w1.fi/cgit/hostap/plain/wpa_supplicant/wpa_supplicant.conf

[27] "The zfone™ project." [Online]. Available: http://zfoneproject.com/wireshark.html

[28] "Logical link control," *ANSI/IEEE Std 802.2-1985*, 1984.

[29] *An introduction to wireless technology.* IBM International Technical Support Organization. Raleigh Center, 1995.

[30] "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," *IEEE Std 802.11-1997*, pp. i–445, 1997.

[31] *Certified Wireless Analysis ProfessionalTM Official Study Guide*, 2004.

[32] "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: Amendment 6: Medium access control (mac) security enhancements," *IEEE Std 802.11i-2004*, pp. 1–190, July 2004.

[33] "Ieee standard for local and metropolitan area networks port-based network access control," *IEEE Std 802.1X-2004 (Revision of IEEE Std 802.1X-2001)*, 2004.

[34] "Ieee std 802.3 - 2005 part 3: Carrier sense multiple access with collision detection (csma/cd) access method and physical layer specifications," *IEEE Std 802.3-2005 (Revision of IEEE Std 802.3-2002 including all approved amendments)*, vol. Section1, 2005.

[35] "Ieee standard for information technology– local and metropolitan area networks– specific requirements– part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 2: Fast basic service set (bss) transition," *IEEE Std 802.11r-2008 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008)*, pp. 1–126, July 2008.

[36] "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 amendment 4: Protected management frames," *IEEE Std 802.11w-2009 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, and IEEE Std 802.11y-2008)*, pp. 1–111, Sept 2009.

[37] "Ieee standard for local and metropolitan area networks - port-based network access control," *IEEE Std 802.1X-2010 (Revision of IEEE Std 802.1X-2004)*, pp. C1–205, Feb 2010.

[38] "Ieee standard for information technology-telecommunications and information exchange between systems-local and metropolitan networks-specific requirements-part ii: Wireless lan medium access control (mac) and physical layer (phy) specifications: Amendment 9: Interworking with external networks," *Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11w-2009, IEEE Std 802.11n-2009, IEEE Std 802.11p-2010, IEEE Std 802.11z-2010, and IEEE Std 802.11v-2011*, pp. 1–208, Feb 2011.

[39] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible authentication protocol (eap)," Internet Requests for Comments, RFC Editor, RFC 3748, June 2004, http://www.rfc-editor.org/rfc/rfc3748.txt. [Online]. Available: http://www.rfc-editor.org/rfc/rfc3748.txt

[40] B. Aboba and P. Calhoun, "Radius (remote authentication dial in user service) support for extensible authentication protocol (eap)," Internet Requests for Comments, RFC Editor, RFC 3579, September 2003, http://www.rfc-editor.org/rfc/rfc3579.txt. [Online]. Available: http://www.rfc-editor.org/rfc/rfc3579.txt

[41] D. Akin, "Robust security network (rsn) fast bss transition (ft)," https://www.cwnp.com/wp-content/uploads/pdf/802.11_RSN_FT.pdf, CWNP - Certified Wireless Network Profesional, Tech. Rep.

[42] M. Alleven, "Ieee study group recommends improvements in wi-fi security," *FierceWirelessTech*, July 2015. [Online]. Available: http://www.fiercewireless.com/tech/story/ieee-study-group-recommends-improvements-wi-fi-security/2015-07-09

[43] F. Bersani and H. Tschofenig, "The eap-psk protocol: A pre-shared key extensible authentication protocol (eap) method," Internet Requests for Comments, RFC Editor, RFC 4764, January 2007.

[44] Cisco, "802.11r, 802.11k, and 802.11w deployment guide, cisco ios-xe release 3.3," http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/5700/software/release/ios_xe_33/11rkw_DeploymentGuide/b_802point11rkw_deployment_guide_cisco_ios_xe_release33/b_802point11rkw_deployment_guide_cisco_ios_xe_release33_chapter_01.pdf.

[45] P. Congdon, B. Aboba, A. Smith, G. Zorn, and J. Roese, "Ieee 802.1x remote authentication dial in user service (radius) usage guidelines," Internet Requests for Comments, RFC Editor, RFC 3580, September 2003.

[46] A. Cooper, H. Tschofenig, B. Aboba, J. Peterson, J. Morris, M. Hansen, and R. Smith, "Privacy considerations for internet protocols," Internet Requests for Comments, RFC Editor, RFC 6973, July 2013.

[47] D. D. Coleman, D. A. Westcott, B. E. Harkins, and S. M. Jackman, *CWSP Certified Wireless Security Professional Official Study Guide: Exam PW0-204*. SYBEX, 2011.

[48] F. S. Foundation, "El sistema operativo gnu." [Online]. Available: https://www.gnu.org/gnu/linux-and-gnu.html

[49] M. S. Gast, "802.11® wireless networks: The definitive guide," http://www.itc.edu.kh/bib/ebook/storage/802.11%20Wireless%20Networks%20The%20Definitive%20Guide.pdf, 2002.

[50] G. R. Hiertz, D. Denteneer, L. Stibor, Y. Zang, X. P. Costa, and B. Walke, "The ieee 802.11 universe," IEEE Communications Magazine, January 2010.

[51] J. M. Huidobro, *Comunicaciones. Interfaces, modems, protocolos, redes y normas.* PARANINFO. S.A., 1992.

[52] ——, *Comunicaciones. Guía Rápida.* PARANINFO. S.A., 1995.

[53] IEEE. Ieee 802 ec privacy recommendation study group. [Online]. Available: http://www.ieee802.org/PrivRecsg/

[54] J. Leary and P. Roshan., *Wireless LAN Fundamentals: Mobility.* Cisco Press., 2004.

[55] J. Malinen. hostapd: Ieee 802.11 ap, ieee 802.1x/wpa/wpa2/eap/radius authenticator. [Online]. Available: http://w1.fi/hostapd/

[56] B. O'Hara and A. Petrick, *EEE 802.11 Handbook: A Designer's Companion.* Standards Information Network IEEE Press, 2005.

[57] L. Parziale, D. T. Britt, C. Davis, J. Forrester, W. Liu, C. Matthews, and N. Rosselot, *TCP/IP Tutorial and technical overview.* IBM redbooks, 2006.

[58] B. Potter and B. Fleck, *802.11 Security.* O'Reilly, 2002.

[59] S. Rackley, *Wireless Networking Technology. From Principles to Successful Implementation.* Newnes, 2007.

[60] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote authentication dial in user service (radius)," Internet Requests for Comments, RFC Editor, RFC 2865, June 2000, http://www.rfc-editor.org/rfc/rfc2865.txt. [Online]. Available: http://www.rfc-editor.org/rfc/rfc2865.txt

[61] D. Tse and P. Viswanath, "Fundamentals of wireless communication," http://www.eecs.berkeley.edu/ dtse/book.html, 2005.

[62] C. M. D. Viegas and F. Vasques, "Real-time communication in ieee 802.11 wireless mesh networks: A prospective study," http://paginas.fe.up.pt/~prodei/dsie11/images/pdfs/s6-2.pdf.

[63] B. H. Walke, S. Mangold, and L. Berlemann, *IEEE 802 Wireless Systems: Protocols, Multi-Hop Mesh / Relaying, Performance and Spectrum Coexistence.* WILEY, 2006.

[64] D. A. Westcott, D. D. Coleman, P. Mackenzie, and B. Miller, *Certified Wireless Analysis Professional Official Study Guide PW0-270*, 2011.

[65] S. Xu, S. Papavassiliou, and S. Narayanan, "Layer-2 multi-hop ieee 802.11 architecture: design and performance analysis," http://ant.comm.ccu.edu.tw/course/94_WLAN/1_Papers_C/Layer-2%20multi-hop%20IEEE%20802.11%20architecture,%20design%20and%20performance%20analysis.pdf, October 2004.