FACULTAD DE INGENIERÍA

INSTITUTO UNIVERSITARIO AERONÁUTICO

Trabajo Final de Ingeniería en Telecomunicaciones

Estudio de la norma 802.11r para la implementación de una red celular sobre WiFi

Director:

Ing. Juan Cayetano Galleguillo

Alumno:

Fornés Diego Raúl

Fecha:

1er Cuatrimestre 2016

Índice general

Índice de Ilustraciones

Prologo

"You can't connect the dots looking forward; you can only connect them looking backwards. So you have to trust that the dots will somehow connect in your future. You have to trust in something — your gut, destiny, life, karma, whatever. This approach has never let me down, and it has made all the difference in my life."

Steven P. Jobs

Stanford commencement speech, June 2005

Prefacio

El estándar IEEE 802.11, comúnmente conocido como WiFi, es utilizado globalmente como medio de comunicaciones inalámbricas. La mayoría de las implementaciones WiFi tienen un rango efectivo de solamente desenas de metros, por lo cual para que un dispositivo de comunicación en movimiento pueda recorrer mayores distancias este debe poder pasar de un punto de acceso a otro conforme se desplaza. En un entorno de automoción, esto podría dar lugar fácilmente a una transferencia cada cinco a diez segundos. Las transferencias ya son compatibles con el estándar preexistente. La arquitectura fundamental para los traspasos es idéntico para la norma IEEE 802.11 con y sin el agregado IEEE 802.11r: el dispositivo móvil es enteramente responsable de decidir cuándo requiere pasar a otro punto de acceso y cuál es el nuevo punto de acceso indicado. En los comienzos de la norma IEEE 802.11, el traspaso fue una tarea mucho más simple para el dispositivo móvil. Se requería de sólo cuatro mensajes para que el dispositivo establezca una conexión con un nuevo punto de acceso (cinco si se cuenta el mensaje opcional "Me voy", que el cliente puede enviar al punto de acceso que esta por dejar). Sin embargo, como se añadieron características adicionales para el estándar, incluyendo 802.11i con la autenticación 802.1X y 802.11e WMM con las peticiones de control de admisión, el número de mensajes requeridos subió dramáticamente. Durante el tiempo que se intercambian estos mensajes adicionales, el tráfico del dispositivo móvil, incluidos los procedentes de las llamadas de voz, no se puede procesar, y el usuario escuchará pérdidas cercana a segundos, cuando en general, la mayor cantidad de retraso o pérdida que el entorno puede introducir en una llamada de voz es de tan solo unos 50 ms o menos.

La enmienda IEEE 802.11r se puso en marcha para tratar de deshacer la carga que la seguridad y la calidad de servicio han añadido al proceso de traspaso, y restaurar de nuevo el traspaso de cuatro mensajes original. De esta manera, los problemas de traspaso no se eliminan, pero al menos se devuelven al statu quo.

La principal aplicación actualmente previsto para el estándar 802.11r es VoIP ("voz sobre IP", o la telefonía basada en Internet) a través de teléfonos móviles diseñados para trabajar con redes inalámbricas de Internet, en lugar de (o además de) las redes celulares estándares.

El informe **Estudio de la norma 802.11r para la implementación de una red celular sobre WiFi**, está dividido en capítulos y de nuevo vuelto a dividir en capítulos más pequeños para que su lectura sea lo más fluida posible; para luego, cuando llegue la etapa de consulta o

referencia, los tópicos se encuentra claramente identificables a modo de repaso o rápida búsqueda. A grandes rasgos, se comienza con una breve introducción sobre comunicaciones móviles sobre WiFi prestando especial atención al proceso de roaming y para continuar la justificación y necesidad del proyecto. Luego se presenta una prueba de laboratorio, puesta en marcha por el autor, donde se exhibe de primera mano el funcionamiento y las ventajas de tener una red 802.11r, como así también se presentan los equipos utilizados, sus características, configuraciones y modo de empleo. Finalmente se presentara una solución estándar para un potencial cliente basados en la norma 802.11r. Cada capítulo comienza con una breve introducción del tema a desarrollar, clave para estimular la discusión y profundizar el análisis.

Agradecimientos

En principio quisiera agradecer a mi familia, a mis amigos y compañeros, y a todos aquellos que de alguna u otra manera me influenciaron o dieron consejos útiles para el desarrollo de este trabajo. No quisiera dejar de mencionar al excelente staff académico del Instituto Universitario Aeronáutico, por su buena disposición para apoyarme en la realización de este trabajo. Una especial mención a mi tutor de tesis el Ing. Juan Cayetano Galleguillo gracias por creer en mí, por su paciencia, por enseñarme, por motivarme y por su actitud siempre positiva. También quisiera destacar el apoyo de mi compañero el Ing. Jorge Tretiakov cuyo ejemplos y consejos fueron indispensables para el armado de este documento. Finalmente quisiera agradecer a mis compañeros de trabajo de AT&T por su aporte con opiniones concejos y experiencia, y a la empresa en general por su apoyo para permitirme dedicarme a la realización de este proyecto.

Resumen ejecutivo

El informe delinea las distintas etapas que conforman al proyecto. Se comienza con la justificación, el problema planteado, las hipótesis al respecto y los objetivos y alcance del proyecto. Luego, en el marco teórico, se busca explicar el funcionamiento del roaming dentro de la norma IEEE 802.11 y los aportes de la enmienda IEEE 802.11r para acelerar este proceso de traspaso sin deteriorar los servicios de seguridad y calidad de servicio, de la manera más sencilla y clara posible.

Una vez conocido el funcionamiento y requerimientos del estándar IEEE 802.11r, se intentara probar el funcionamiento y el potencial de una red WiFi 802.11r en diferentes escenarios por medio del montando de una red 802.11r de laboratorio. Se buscara familiarizar al lector con la norma y su empleo en la práctica, como así también listar algunos equipos y topologías que lo soportan entre otros detalles técnicos para su implementación.

Dedicaremos un capitulo al análisis de los datos y experiencias obtenidas de las pruebas y finalmente se presentara una reflexión y conclusión en donde se apreciara o no las ventajas que este tipo de red tiene en relación con las actuales y que tan factible y viable resultaría su comercialización.

Como extra se presentará un diseño de una solución estándar de red WiFi 802,11r para prestar servicios de comunicaciones inalámbricas con fast-roaming basándonos en lo ya estudiado y probado.

1. Título y subtítulo

Estudio de la norma 802.11r para la implementación de una red celular sobre WiFi.

1.1. Palabras claves

- **Estación(STA):** Equipos móviles con placas inalámbricas
- **Punto de acceso (AP):** Es una entidad que posee las propiedades de una STA y además provee acceso a otras STA al DS (distribution system) a través del WM (Wireless Medium)
- **Sistema de distribución (DS):** Es el sistema que se utiliza para interconectar los diferentes BSSs e integrarlos con las LAN cableadas.
- **Basic Service sets (BSS):** Agrupación lógica de STAs, que lograron sincronizarse a un AP. Esta definición no implica que cada estación pueda comunicarse entre sí.
- **Independent BSS (IBSS):** También conocida como red ad hoc, consiste en solo 2 estaciones conectadas entre sí.
- **Extended Service sets (ESS):** Agrupamiento de BSS para abarcar una mayor área dentro del mismo agrupamiento lógico
- **Station Service (SS):** Conjunto de servicios que permiten que la MAC trasmita las MDSUs entre STAs dentro de una BSS.
- **Destribution system services (DSS):** Conjunto de servicios provistos por el DS que permiten a la capa MAC intercambiar las MSDUs entre estaciones que no se encuentran en el mismo entorno inalámbrico.
- **Over the air (OTA):** Indica que el proceso se realiza puramente a través del aire.
- **Over the DS (ODS):** Indica que parte del proceso se realiza a través del DS.
- **Pre-shared key (PSK):** clave previamente compartida.
- **Master session key (MSK):** Clave maestra de sesión.
- **Autenticación 802.1x:** control de acceso a red basada en puertos.

- **Voice Over IP (VoIP):** Comunicación telefónica a través de una red IP.
- **Wireless Network Controller:** Dispositivo encargado de centralizar la gestión de los APs.
- **Estructura Fat-APs:** Hace referencia a la situación en que los APs trabajan en modo autónomo.
- **Roaming:** Capacidad de un dispositivo para moverse de una zona de cobertura a otra.
- **WiFi:** Mecanismo de conexión de dispositivos electrónicos de forma inalámbrica.
- **Voice over WLAN (VoWLAN):** Comunicación telefónica a través de una red IP inalámbrica.
- **Unidad de servicio MAC (MSDU):** Unidad de servicio de datos recibida de la subcapa Ethernet superior LLC.
- **Internetwork Operating System (IOS):** Es un paquete de funciones de enrutamiento, conmutamiento, trabajo de internet y telecomunicaciones que se integra estrechamente con un sistema operativo multitarea.
- **Service Set Identifier (SSID):** Código de máximo 32 caracteres alfanumérico incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esta red.
- **Basic Service Set Identifier (BSSID):** Dirección de 48 bits que identifica a la BSS que pertenece, por lo general es el valor de la dirección MAC del AP.
- **Control de enlace lógico (LLC):** Parte superior de la capa enlace en las redes de área local.
- **Media Access Control (MAC):** Parte Inferior de la capa enlace en las redes de área local.
- **Lightweight Access Point Protocol:** o Protocolo Ligero para Puntos de Acceso (LWAPP) es un protocolo de red utilizado para la gestión centralizada de varios puntos de acceso en una red inalámbrica WLAN.
- **Power over Ethernet (PoE):** es una tecnología que incorpora alimentación eléctrica a una infraestructura LAN estándar Power over Ethernet se regula en una norma

denominada IEEE 802.3af, y está diseñado de manera que no haga disminuir el rendimiento de comunicación de los datos en la red o reducir el alcance de la red.

1.2. Justificación del proyecto

Se parte de la idea de que la tecnología VoWLAN (voz por ip via Wifi) es una tecnología que conviene por diversas ventajas que tienen que ver con costos, simplificación de topología, uniformización de servicios y más con respecto a la tecnología celular convencional en pequeñas zonas geográficas. Se busca estudiar las últimas técnicas (802.11r) para crear un producto de calidad superior para mejorar y ampliar la experiencia del usuario WiFi y así satisfacer la creciente necesidad del acceso a la información en todo momento y en todo lugar.

1.3. Problema

A pesar de que la extensión 802.11r sobre la norma IEEE 802.11 promete ser la solución para ofrecer un servicio de telefonía móvil sobre WiFi con un roaming rápido, sin descuidar la seguridad y la calidad de servicio percibida por la STA móvil previo al momento del traspaso, no se cuenta con un fácil acceso a información sobre su implementación, rendimiento y equipos que soporten sus requerimientos debido a que es una norma muy reciente. Por lo cual no se cuenta con la certeza de que con la tecnología de red actualmente ofrecida en el mercado se logre implementar fácilmente esta norma, y si los resultados de la implementación de la misma serán los esperados para cumplir lo prometido.

1.4. Hipótesis

Por lo poco Visto de material obtenido de 3ra mano, se considera que a pesar que se deba recurrir a la tecnología de última generación, una red 802.11r es de implementación sencilla y no tan costosa.

También se considera que la norma 802,11r puede significar un salto importante en pos de posibilitar un servicio de telefonía móvil sobre WiFi con un aceptable nivel de calidad y seguridad.

1.5. Objetivos generales

Como objetivo principal se pretende describir y analizar el funcionamiento y las características principales de la norma IEEE 802.11r y los cambios que esta propone frente a la norma 802.11 para lograr un roaming más rápido sin descuidar la seguridad y calidad de servicio. Como así también observar estas características y ventajas en la práctica por medio de una implementación en un entorno de laboratorio.

Existen objetivos secundarios y específicos que son definidos a continuación:

A) Demostrar que la tecnología VOWLAN (voz por ip via wifi) es una tecnología que conviene por diversas ventajas que tienen que ver con costos, simplificación de topología, uniformización de servicios y más.
B) Presentar una solución estándar para la implementación de una red WiFi con fast roaming.

1.6. Alcances

Se busca ofrecer un documento que proporcione al lector la suficiente información, en relación a la norma 802.11r, que le permita interiorizarse con sus características, ventajas y desventajas y luego poder decidir si este tipo de red satisface sus necesidades relacionadas con la comunicación móvil, y el acceso a la información de manera inalámbrica en general.

No se pretende explorar todas las características de la norma 802.11r en detalle y su impacto en frente a todo tipo de escenario y aplicación que quiera trabajar sobre ella.
No es la intención de este documento compara este tipo de entornos de red con el provisto con la red celular GSM actual, aunque supone ciertas similitudes en cuanto a características y servicios prestados.

Tampoco busca incurrir en todos los pasos que implica la creación de un producto relacionado con la prestación de un servicio de telefonía móvil sobre WiFi a pesar de que se presente una posible solución estándar para su implementación.

2. Introducción

Aunque la telecomunicación como estudio unificado de las comunicaciones a distancia es una idea reciente, la comunicación e intercambio de información es una necesidad básica desde el comienzo de los tiempos. Conforme las distintas civilizaciones empezaron a extenderse por territorios cada vez mayores fue necesario un sistema organizado de comunicaciones que permitiese el control efectivo de esos territorios. Hoy en día el intercambio de información es vital a tal punto que debe ser casi instantáneo desde cualquier parte del mundo, con fines críticos como conocer el estado y ubicación de nuestros seres queridos hasta el pedido de auxilio o asistencia con alguna situación adversa, como así también con aplicaciones menos criticas como el acceso a una cada vez más amplia gama de formas entretenimiento.

Sistema de comunicaciones móviles

Las comunicaciones móviles se dan cuando tanto el emisor como el receptor están, o pueden estar, en movimiento. La movilidad de estos dos elementos que se encuentran en los extremos de la comunicación hace que no sea factible la utilización de hilos (cables) para realizar la comunicación en dichos extremos. Por lo tanto utilizan básicamente la comunicación vía radio.

Las comunicaciones móviles no aparecieron de forma comercial hasta finales del siglo XX. Los países nórdicos fueron los pioneros en disponer de sistemas de telefonía móvil, Radio-búsquedas (GPS), redes móviles privadas o Trunking. Los sistemas de telefonía móvil avanzados fueron el siguiente paso. Después llegó la telefonía móvil digital y con la rápida adopción mundial de las agendas personales, laptops (computadores portátiles), netbooks (miniordenadores) y un sin fin de dispositivos las comunicaciones móviles se usaron cada vez más para conectarse vía radio con otros dispositivos o redes. Finalmente cabe destacar la fusión entre comunicaciones móviles e Internet, lo que fue el verdadero punto de inflexión positivo para estos dos elementos.

3. Marco Teórico

El objetivo de este capítulo es introducir las posibilidades y limitaciones del roaming, como se definió en el estándar 802.11 original y los beneficios que la extensión 802.11r ofrece a dicho proceso. Para lo cual se introducen brevemente algunos componentes y términos relacionados con WLAN, roaming y la norma 802.11. También se muestra los servicios que la norma 802.11 ofrece y la evolución del estándar a medida que las extensiones de la misma fueron apareciendo (802.11i, 802.11e y 802.11k). Finalmente se introduce la extensión 802.11r, sus aportes al proceso de roaming y su funcionamiento a grandes rasgos.

3.1. Roaming

Se lo define como servicio de conectividad extendida de una red a otra región. A pesar de que hay un consenso básico de que el roaming inalámbrico implica la finalización de la conexión con una antena y el inicio de le conexión con otra, aún hay mucha confusión alrededor del termino cuando nos acercamos a los detalles.

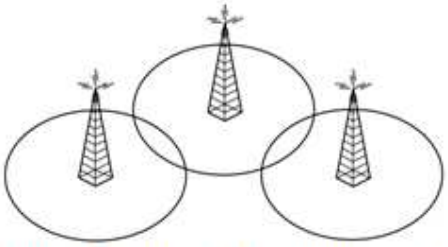


Figura 3.1.1: Tres celdas superpuestas.

Escenario materia de estudio:

En la figura 3.1.2 vemos un típico caso de roaming, cuando un usuario utilizando un teléfono móvil atraviesa el área de cobertura provista por dos antenas de una misma red. Nótese la existencia de un área de superposición de cobertura de las 2 antenas, donde la comunicación con las 2 antenas es posible.

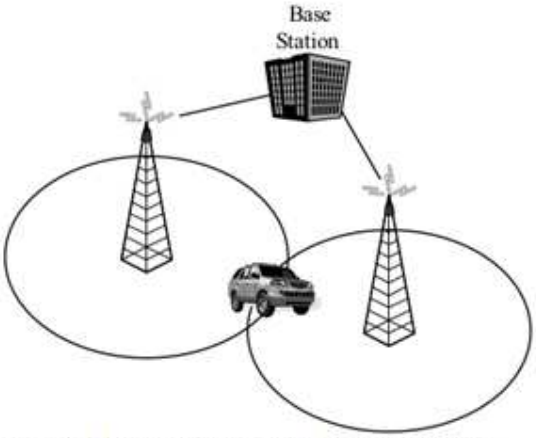


Figura 3.1.2: Ejemplo estándar de roaming.

A continuación se presentan 3 ejemplos ilustrativos de diferentes tipos de roaming:

1)

Figura 3.1.3: Usuario hablando por teléfono de un auto en movimiento.

2)

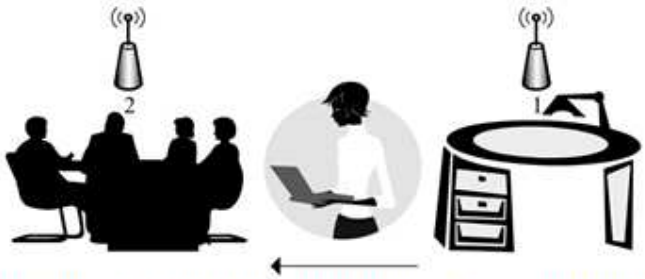


Figura 3.1.4: Una persona trabajando en una notebook mientras camina en una habitación.

Considerando los 2 primeros ejemplos (Figura 3.1.3 y 3.1.4), asumiendo que la persona inicialmente se está comunicando a través de la antena número 1 y el movimiento la aleja de dicha antena y lo acerca al rango de cobertura de la segunda antena. También se supone que las 2 antenas son administradas por el mismo proveedor y son partes de la misma red. Luego la red administra el traspaso del usuario de una antena a otra, esto se llama roaming local.

3)

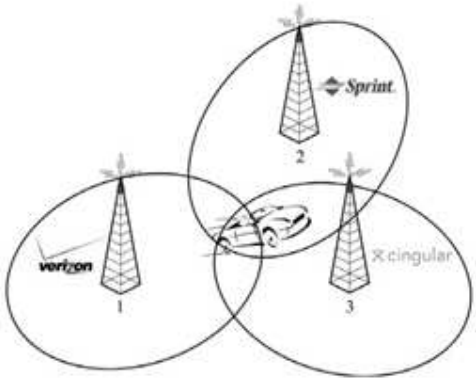


Figura 3.1.5: Un usuario llega a un área no cubierta por su proveedor local.

En el tercer ejemplo (Figura 3.1.5) asumimos que el usuario está comunicándose a través de la antena número uno, administrada por el proveedor local, cuando este llega al límite del rango de cobertura de dicha antena. También se asume que las 2 antenas capases de proveer cobertura al usuario en ese momento son de redes diferentes. El usuario debe re asociarse a una de las 2 nuevas antenas como se mencionó en el ejemplo anterior pero con la dificultad de tener que decidir a cual red asociarse y luego esperar que esta red lo admita. Esta situación se conoce como roaming global.

Este documento solo está destinado a escenarios plasmados por el primer y segundo ejemplo únicamente.

3.2. WLAN

WLAN es un sistema de comunicación de datos inalámbrico flexible y utilizado como alternativa a la LAN cableada o como extensión de esta. Utiliza tecnología de RF que permite mayor movilidad a los usuarios al minimizarse las conexiones físicas. Mientras que WiFi hace referencia a un conjunto de estándares para redes inalámbricas basados en las especificaciones IEEE 802.11(x). Es una alternativa eficaz y de bajo costo para las comunicaciones de banda ancha y con las incorporaciones de los nuevos estándares de IEEE (802.11(x)) existe la posibilidad de prestar nuevos servicios como VoIP y Video striming. También se destaca su versatilidad y el fácil acceso al Hardware requerido para su funcionamiento.

Desafíos que plantea una red inalámbrica en relación con la red cableada:

- Las direcciones lógicas no hacen referencia a ubicaciones físicas.
- El impacto del medio a utilizar en el diseño y performance:
    - No tiene fronteras, más que la determinación lógica de que usuario forma parte de la red y que usuario no.
    - No tiene protección física de señales interferentes.
    - Es un medio mucho menos confiable.
    - Tiene topologías dinámicas.
    - Falta de conexión total, por lo que el asumir que todos los usuarios pueden escuchar los demás usuarios en este caso no es acertado.
    - Presenta variaciones de tiempo de respuesta y propiedades del medio asimétricas.
    - Puede experimentar interferencia proveniente de otras redes Wi-Fi lógicamente separadas.
- El impacto de manejar estaciones (STA) móviles
    - Están en movimiento
    - Usan batería (requiere administración)

- La interacción con las capas superiores, ya sea de la IEEE o no.

Tipos de redes Inalámbricas (WLANs):

Es posible configurar las WLANs con diferentes arquitecturas dependiendo del requerimiento del sistema. Los tipos de arquitecturas físicas son:

- Ad hoc
- Infrastructure
- Mesh

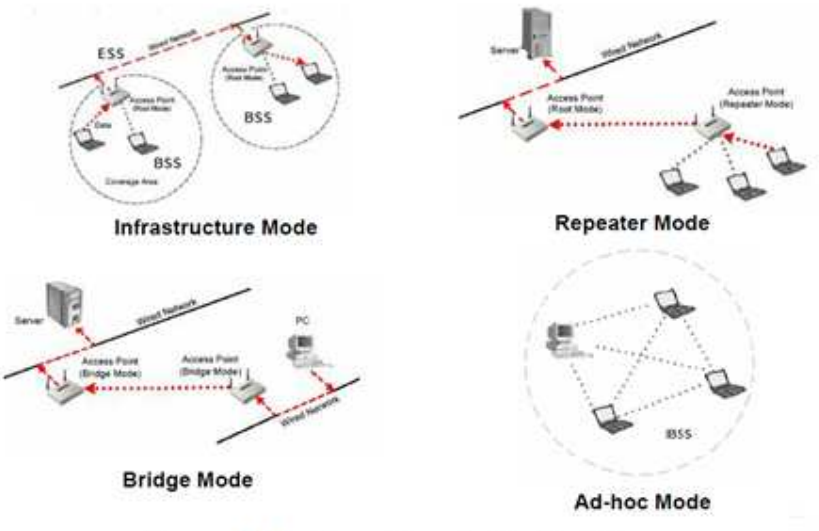


Figura 3.2.1: Tipos de redes Inalámbricas.

WLAN Ad hoc:

Las redes inalámbricas Ad hoc, también conocida como WLANs peer-to-peer, requiere únicamente de las estaciones clientes (STAs) 802.11 en red:

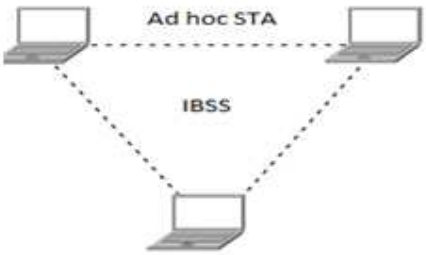


Figura 3.2.2: WLAN Ad hoc.

Como no requerimos de un punto de acceso común (AP) en este tipo de red los paquetes viajan directamente a las estaciones destino sin ningún intermediario. Es muy sencilla de implementar y requiere poca configuración.

La primera estación Ad hoc activa inicia una IBSS y empieza a enviar tramas balizas que son requeridas para informar sobre la presencia de la red Ad hoc y mantener la sincronización a

lo largo de ella. Otras estaciones pueden elegir unirse a la red Ad hoc luego de recibir la trama baliza y aceptando las condiciones de la IBSS.

Infrastructure WLAN:

Esta es la arquitectura de WLAN más común. En esta configuración uno o más AP conectan las STA entre ellas y al sistema de distribución (DC). Cada AP forma un área de cobertura, conocida como BSS, que permite a las STA dentro de esta comunicarse con el AP. Esto permite a las STA conectarse entre sí y con los servidores y aplicaciones de red a través del sistema de distribución.

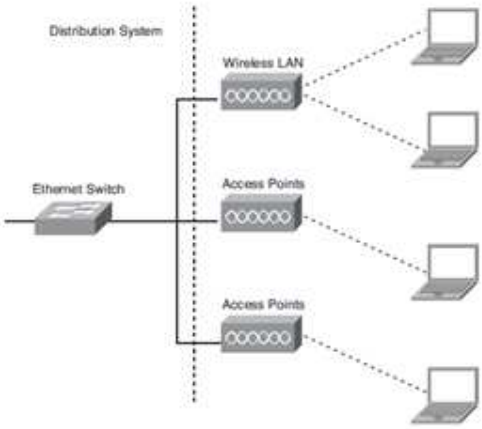


Figura 3.2.3: Infrastructure WLAN.

Si se instalaran los AP de tal manera de que sus radios de cobertura se superpongan, los STA móviles de los usuarios podrían saltar de un AP a otro sin notar ninguna pérdida de servicio (roaming).

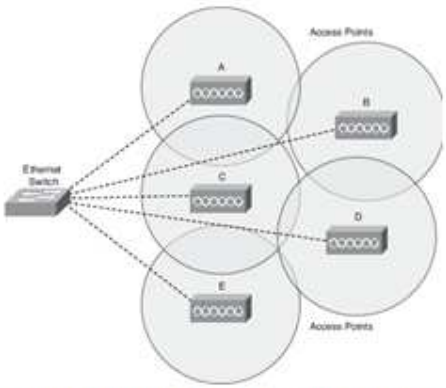


Figura 3.2.4: WLAN con multiceldas superpuestas que soportan roaming.

La tarjeta de red de la STA automáticamente decidirá y re-asociara con el AP con la señal más fuerte. Por lo general el usuario no percibe perdida del servicio alguna, sin embargo las llamadas de voz por IP (VoIP) pueden verse afectadas o incluso terminadas so el tiempo de roaming es mayor a 150ms.

Mesh WLAN:

La infraestructura Mesh utiliza nodos Mesh que son similares a los AP pero utilizan el aire para contactarse entre ellos. De esta manera la WLAN no requiere de cableado Ethernet alguno.

Los nodos Mesh son AP adaptados para conectarse entre ellos por aire utilizando un protocolo Mesh propietario.

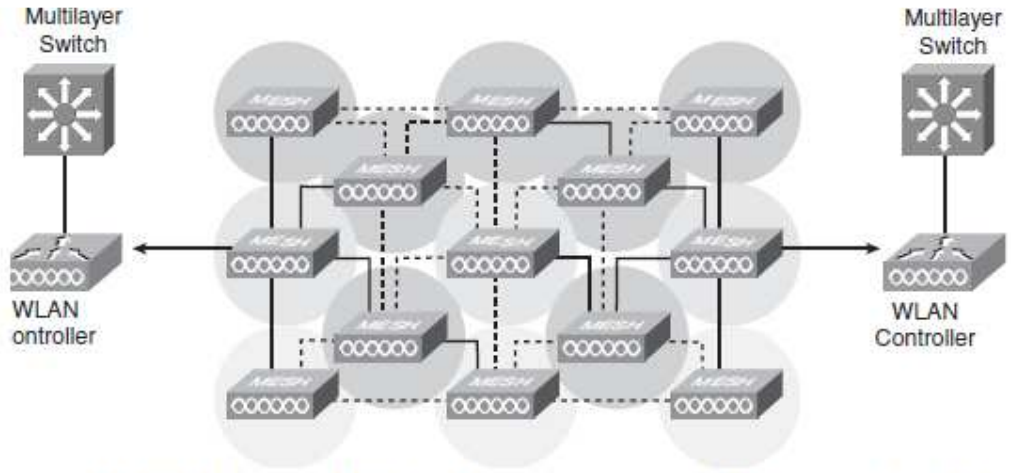


Figura 3.2.5: Red Mesh con APs Mesh que se interconectan de manera inalámbrica.

Cada nodo implemente un protocolo de enrutamiento para direccionar los paquetes entre los clientes y sistemas de distribución.

La latencia puede variar mucho en este tipo de red dependiendo de la cantidad de usuarios y saltos que son existentes entre ellos o con el DS. El tiempo de roaming y ruteo puede afectar a servicios como la voz por IP.

3.3. Estándar IEEE 802.11

El estándar 'IEEE 802.11' define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una

WLAN para así resolver los desafíos listados anteriormente que plantea esta tecnología. Los protocolos de la rama 802.x definen la tecnología de redes de área local y redes de área metropolitana.

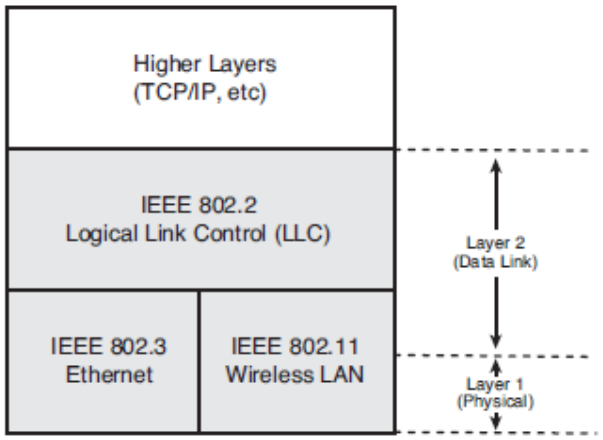


Figura 3.3.1: Familia de estándares IEEE 802 alocados en las capas 1 y 2 del modelo OSI.

Subcapa MAC 802.11:

El estándar 802.11 define en su capa de control de acceso al medio (MAC, medium access control) una serie de funciones para realizar las operaciones propias de las redes inalámbricas. La capa MAC se encarga, en general, de gestionar y mantener las comunicaciones entre estaciones 802.11, bien sean puntos de acceso a adaptadores de red. La capa MAC tiene que coordinar el acceso a un canal de radio compartido y utilizar su capa Física (PHY) 802.11b o 802.11g para detectar la portadora y transmisión y recepción de tramas. También cuenta con un módulo de detección y posible corrección de errores.

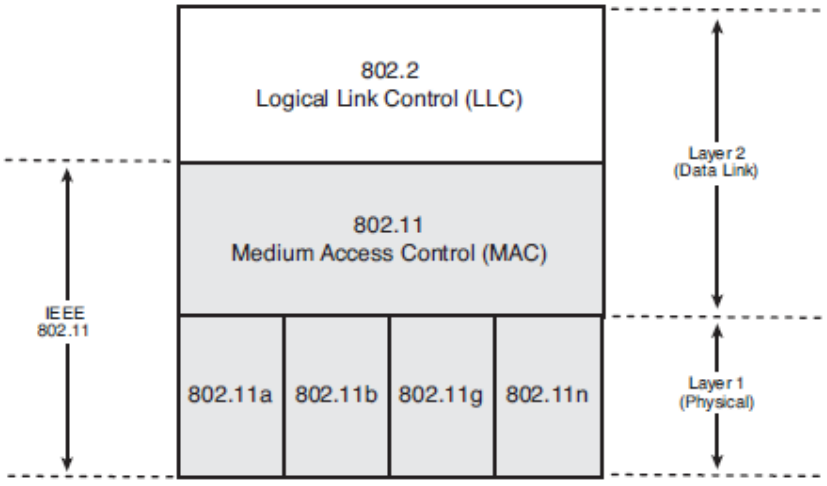


Figura 3.3.2: Funciones WLANs relacionadas con la capa Data link y fisica

Capa Física 802.11 (802.11 Phy):

Incluye todas las especificaciones necesarias para definir la composición de las señales que son enviadas a través de la WLAN. Por ejemplo 802.11 Phy define el tipo de modulación, frecuencia, y el proceso de sincronización de señal para cada tipo de WLAN (802.11a, 802.11b, 802.11g y 802.11n).

IEEE 802.2 (Capa LLC):

IEEE 802.2 es el IEEE 802 estándar que define el control de enlace lógico (LLC). La subcapa LLC presenta una interfaz uniforme al usuario del servicio enlace de datos, normalmente la capa de red.

Ofrece 3 tipos de servicios:

- Servicio sin conexión y sin confirmación de entrega.
- Servicio orientado a la conexión.
- Servicio sin conexión con confirmación de entrega

Para ello esta subcapa que añade las etiquetas estándar de 8-bit DSAP (Destination Service Access Point) y SSAP (Source Service Access Point) a los paquetes del tipo de conexión. También usado en funciones auxiliares como Control de flujo. El Subnetwork Access Protocol (SNAP) permite valores EtherType usados para especificar el protocolo transportado encima de IEEE 802.2, y también permite a los fabricantes definir sus propios espacios de valores del protocolo.

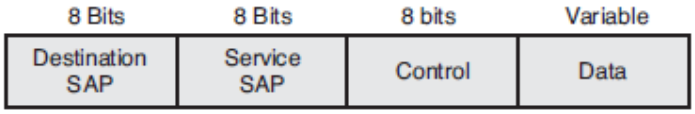


Figura 3.3.3: Encabezado LLC de una PDU.

El campo control en LCC tiene bits que indica si la trama es de alguno de los siguientes tipos de tramas:

- Información: contiene datos del usuario
- Supervisión: Control de flujo y control de errores
- Sin numerar: Varios protocolos de control de PDUs

3.3.1. Servicios IEEE 802.11

La norma 802.11 debe proveer los siguientes servicios:

- Soporte para servicios de entra de información asíncrona y también con requerimientos de tiempo (VoIP).
- Posibilidad de expandir la cobertura a través de un DS como por ejemplo Ethernet.
- Capacidad para múltiples transmisiones de alta velocidad.
- Servicios multicast (trasmisión a varios destinos de manera simultánea).
- Servicios de autenticación y asociación.
- Compatibilidad con las normas 802.11 anteriores (ejemplo: 802.11b y 802.11g).

El estándar presta especial atención a las siguientes características que difieren mucho de las LANs cableadas:

- **Mecanismo de seguridad:** Para simular la protección provista por un cable, se implementan varios métodos de encriptación y autenticación.
- **Métodos de aprovechamiento de AB:** Como el espectro en frecuencia es limitado la capa física debe implementar mecanismos para su mejor aprovechamiento.
- **Administración de la energía:** Como los radios 802.11 por lo general deben montarse en equipos pequeños con limitada energía, 802.11 incluye opciones para activar modos de ahorro de energía.

IEEE 802.11 define servicios que proveen las funciones que la capa LCC requiere para enviar las MDSUs entre 2 entidades en la red. Estos servicios se dividen en 2 categorías:

- Servicios de estación (SS): Incluye autenticación, des autenticación, privacidad y entrega de MDSUs.
- Servicios de sistema de distribución (DSS): Incluye asociación, des asociación, distribución, integración y re asociación.

Station Service (SS)

Conjunto de servicios que permiten que la MAC trasmita las MDSUs entre STAs dentro de una BSS.

- Autenticación:

Se utiliza para emular la conexión física en una red LAN. Establece la identidad de una STA que quiere enviar un mensaje a otra, tanto en una BSS como en una IBSS. Si la autenticación mutua no ha sido correctamente aceptada entre 2 STAs, no se podrá establecer una asociación.

La norma define 2 métodos de autenticación:

  - Open system: Permite que cualquier STA se pueda comunicar con la DS.

  - Shared Key: Utiliza WEP para demostrar el conocimiento de la clave de encriptación WEP.

También acepta nuevos métodos de autenticación. Una STA puede estar autenticada con varias otras STA al mismo tiempo.

- Pre autenticación:

Este servicio permite autenticarte con otro AP estando ya asociado a un AP para un futuro traspaso. Esto es muy útil ya que el servicio de autenticación toma mucho tiempo, y en el caso de una re asociación el servicio se podría ver muy afectado por la demora en la autenticación.

- De autenticación:

Este servicio se utiliza cuando se desea terminar una autenticación vigente. Esto causara en la disociación de la STA. Puede ser requerida por ambas parte y el resultado es una notificación y no una petición.

- Confidencialidad de datos:

Se utiliza para emular la confidencialidad que provee la red cableada, para ello el estándar provee 3 tipo de encriptación posibles para proteger el contenido del mensaje: WEP, TKIP y CCMP. WEP y TKIP están basadas en el algoritmo ARC4 y CCMP está basado en el estándar de encriptación avanzada (AES). Se provee un medio para que las STA puedan escoger que algoritmo usar para cada asociación.

Destribution system services (DSS)

Conjunto de servicios provistos por el DS que permiten a la capa MAC intercambiar las MSDUs entre estaciones que no se encuentran en la misma WM.

- Distribución:

Es solicitado por cada mensaje de datos enviado por o hacia cualquier STA operando en una ESS cuando este mensaje debe pasar a través del DS.

Es tarea del servicio de distribución el de enviar el mensaje al destino correcto dentro del DS (Al AP correspondiente a la BSS que la STA destino corresponda). Como se lleva esto a cabo dentro de la DS no se especifica en esta norma, pero si se debe proveer al DS con suficiente información para que este pueda llevar a cabo esta tarea. Esta información se obtiene por medio de los 3 mensajes relacionados con la asociación (Asociación, Re asociación, and Des asociación).

A pesar que este estándar no especifica cómo debe ser la implementación del DS, si reconoce y soporta el uso del WM como DSM.

- Integración

Si el DS determina que la STA destino es un miembro de la LAN (cableada), el destino del DS no va a ser un AP si no un portal. Estos mensajes causan que el DS tenga que invocar a la función Integración. El servicio de Integración es responsable de proveer lo que sea necesario para enviar un mensaje desde la DSM al medio LAN. Los detalles de la función Integración son específicos a la implementación del DS y no forman parte de este estándar.

- Asociación:

Previo a que una STA pueda transmitir mensajes de datos a través de un AP, este debe asociarse al AP primero. El acto de asociarse se realiza por medio del servicio Asociación, quien provee el mapeo entre el AP y la STA al DS. El DS usa esta información para brindar el servicio de distribución. El servicio Asociación es suficiente para soportar STA móviles que se mantienen en la misma BSS.

En cada instante cada STA no puede estar asociado con más de un AP, esto asegura que el DS pueda determinar a qué AP pertenece cada STA. Un a ves que la asociación es finalizada las STA pueden hacer uso del DS (a través del AP) para comunicarse. El servicio de

asociación siempre es iniciado por las STAs y no por el AP. Las STA sondean los AP disponibles y el servicio que estos prestan y en base a esto deciden iniciar el proceso de asociación con alguno de ellos.

- Re asociación:

Provee las funciones extras requeridas para soportar STA móviles con transición de BSS dentro de una ESS. Permite "mover" una asociación desde un AP a otro, al mismo tiempo que informa al DS sobre el cambio. También permite cambiar los atributos de una determinada asociación sin terminarla. La re asociación siempre es iniciada por la STA móvil.

- Des asociación:

Se utiliza cuando una asociación debe ser terminada. Este servicio informa al DS que elimine la asociación mencionada. Este servicio puede ser solicitado por cualquier STA (no-AP y AP) y se trata de una notificación y no un pedido, es decir no puede rechazarse.

- Reserva de recursos QoS:

Permite enviar tramas con QoS, entre STA en la misma BSS, utilizado acceso al canal controlado, o basado en la conexión. En cada TXOP, una entidad organizadora de tráfico en la STA selecciona una trama para ser transmitida, entre las tramas al frente de las diferentes colas, basándose en las UP requeridas y/o los valores en los parámetros de las especificaciones de tráfico (TSPEC) para la MSDU determinada.

3.3.2. Conectividad en 802.11

Una determinada STA cliente debe primero conectarse a una red 802.11 antes de poder enviar cualquier tipo de datos. Este proceso es automático y comprende las siguientes acciones:

Paso 1. Escaneo

Paso 2. Autenticación

Paso 3. Asociación

A continuación se presenta brevemente como se lleva a cabo cada uno de estos pasos.

Escaneo:

Es el primer paso para que una estación (STA) móvil forme parte de una BSS.

Tan pronto como la STA 802.11 es activada, debe encontrar las redes 802.11 en rango. Esto es necesario para identificar un AP al que la STA puede conectarse. La STA logra esto en la etapa de búsqueda utilizando la función escaneo.

Existen 2 tipos de escaneos.

- Escaneo Pasivo:

LA STA sintoniza cada canal de frecuencia (RF), y escucha por un periodo de tiempo en búsqueda de una trama baliza proveniente de algún AP (Infrastructure WLAN) u otra STA (ad hoc WLAN). Por defecto los AP trasmiten una baliza cada 100 ms en un canal RF específico. La esta registra la intensidad de la señal de la trama baliza y continúa buscando otros AP. Por lo general, las STA elijen el AP que haya enviado la trama baliza con la mayor intensidad de señal.

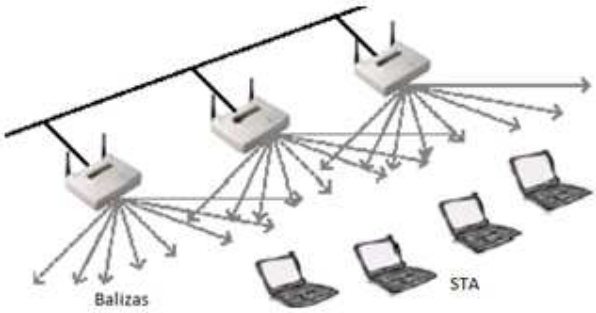


Figura 3.3.4: STAs escaneando la WLAN de modo pasivo.

- Escaneo Activo:

La STA intenta localizar un AP transmitiendo una trama *probe request* (solicitud de prueba) y espera por una trama *probe respond* (respuesta de prueba).

La trama *probe request* puede ser dirigida a un AP en particular (unicast) o a todos los APs (Broadcast).

La trama *probe respond* del AP es similar a la trama Baliza.

Basado en la respuesta del AP, la STA decide conectarse al mismo o no.

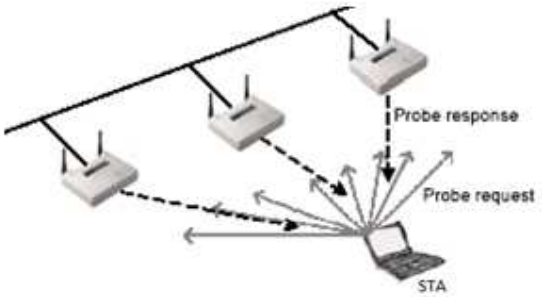


Figura 3.3.5: STA escaneando la WLAN de modo activo.

Autenticación:

Debido a que a las WLANs usualmente se propagan fuera de áreas físicamente controladas, la STA primero debe ser autenticada por el AP antes de unirse a la BSS. El estándar 802.11 incluye los siguientes métodos de autenticación:

- Sistema de autenticación abierta (Open system): Es la autenticación por defecto que simplemente anuncia el deseo de asociarse con otra STA o AP.

- Autenticación de clave compartida (Share key authentication): Esta opción requiere un intercambio de tramas más riguroso, para asegurar que la STA solicitante sea autenticada basado en el conocimiento de la clave WEP.

- Autenticación basada en puertos IEEE 802.1X: Provee una autenticación más compleja a través del uso de servidores de autenticación.

o Autenticación Abierta (open system):

La STA que inicia el proceso de autenticación envía una trama de autenticación 802.11 dirigida al AP con el cual quiere conectarse indicando el deseo de autenticarse con la red. El AP responde con una trama de autenticación 802.11 que indica el éxito o fracaso, de dicha autenticación, por medio del estado del código localizado en el cuerpo de la trama de autenticación.

Figura 3.3.6: Autenticación abierta 802.11.

En este caso cualquier STA puede autenticarse exitosamente con la WLAN. La STA cliente no necesita enviar ningún tipo de credencial para acceder a la WLAN.

- Autenticación de clave compartida:

Fue creada para proveer un nivel más alto de seguridad que el sistema abierto. Para que una STA utilice este sistema, debe implementar encriptación WEP.

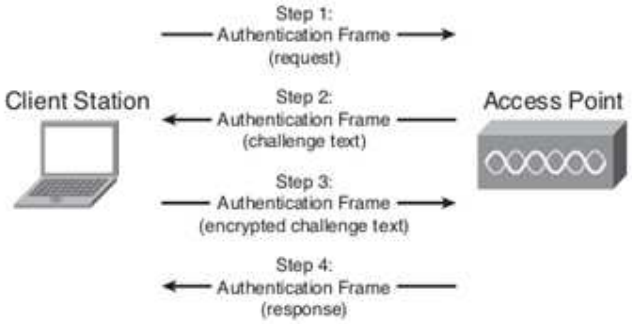


Figura 3.3.7: Autenticación de clave compartida en 802.11.

El proceso de autenticación de clave compartida sigue los siguientes pasos:

1. Una STA envía una trama de autenticación al AP solicitando una clave de autenticación compartida.
2. Cuando el AP recibe la trama de autenticación inicial, el AP responde con una trama de autenticación que incluye un texto de 128 octetos generado por el servicio WEP.
3. La STA cliente convierte este texto en una trama de autenticación, la encripta con la clave compartida, y la envía al AP.
4. El AP desencripta el valor del texto utilizando la misma llave compartida y la compara con el texto original. Si hay coincidencia, el AP responde con una trama de autenticación indicando el éxito o fracaso de la autenticación.

- Autenticación 802.1X basado en puertos:

La extensión 802.11i a la norma 802.11 introduce 802.1x como un método de autenticación opcional. Aplica un protocolo llamado EAP (protocolo de autenticación extensible) a ambos WLAN y LAN cableada y soporta múltiples métodos de autenticación.

El proceso inicia con una STA no autorizada que intenta conectarse con el autenticador (802.11 AP). El AP responde habilitando un puerto para trasmitir solamente los paquetes EAP del cliente hacia el servidor de autenticación localizado en el lado cableado del AP. El AP bloquea cualquier otro tipo de tráfico, como HTTP, DHCP, y POP3, hasta que el AP pueda verificar la identidad del cliente utilizando un servidor de autenticación (por ejemplo RADIUS).

El proceso de autenticación 802.1X basado en puertos sigue los siguientes pasos:

1. El cliente envía un mensaje EAP-start. Esto inicia una serie de intercambio de mensajes para autenticar al cliente.
2. El AP responde con un mensaje EAP-request de identidad.
3. El cliente envía un mensaje EAP-respond que contiene la identidad del servidor de autenticación.
4. El Servidor de autenticación utiliza un algoritmo específico para verificar la identidad del cliente.
5. El Servido de autenticación envía un mensaje de autorización o rechazo la AP.
6. El AP envía un mensaje EAP-success (o reject) al cliente.
7. Si El servidor autentica al cliente, el AP abrirá otros puertos al cliente permitiendo tráfico adicional.

Asociación:

Luego de ser autenticada, la STA debe asociarse con el AP para completar el proceso de conexión. Esto es necesario para sincronizar la STA con el AP, para ello se debe compartir información importante como intervalo de baliza y velocidades de transmisión soportadas. La STA inicia la asociación enviando una trama de requerimiento de asociación que contiene elementos como el identificador de conjunto de servicios (SSID) y velocidad de datos permitida al AP.

El AP responde enviando una trama de asociación respuesta que contiene un identificador de asociación acompañado con otros datos relacionados con el AP.

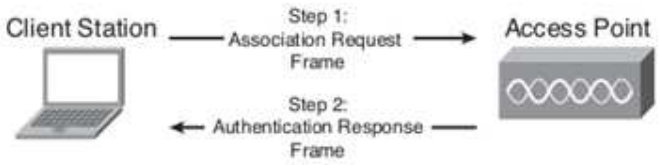


Figura 3.3.8: Asociación 802.11, primer paso para conectarse a una WLAN.

Una vez que la asociación se completa, las tramas 802.11 de datos pueden transitar entre la STA y el AP libremente.

Re asociación:

Si la STA se mueve, la calidad de la señal entre el AP y la STA puede disminuir. Como resultado, las STA continúan escaneando los canales periódicamente e intenta desasociarse con otro AP de ser necesario.

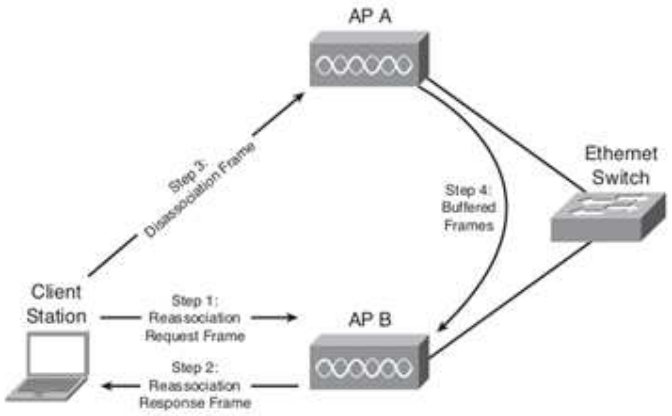


Figura 3.3.7: Proceso de re-asociación en 802.11, permite el traspaso a una STA.

Como se ve en la figura una STA puede estar inicialmente conectado a una red por medio del AP A. A medida que la STA se acerca al AP B, la calidad de la señal entre la STA y al AP empieza a disminuir, en algún punto (Antes de que la STA no pueda comunicarse con el AP A), la STA inicia el proceso de re asociación enviando una trama de requerimiento de re asociación 802.11 al AP B. El AP B responde con una trama respuesta de re asociación indicando el éxito o fracaso en la re asociación, y luego la STA envía la trama des asociación 802.11 al AP A. El AP A reenvía cualquier trama 802.11 que se encuentre almacenada en su memoria al AP B para que esta la pueda entregar a la STA. Terminado este proceso, la STA y el AP B pueden iniciar el intercambio de tramas de datos 802.11.

3.3.3. Tipos de tramas en 802.11

El estándar IEEE 802.11 divide las tramas en 3 categorías según su fusión, administración, control e intercambio de datos entre STAs y APs.

Tramas de administración:

El propósito de estas tramas es establecer y mantener la comunicación entre la STA y el AP. Ya que proveen servicios como asociación y autenticación.

El campo de duración de las trama de administración es 32768 durante el periodo libre de contención (contention-free), que le da suficiente tiempo para establecer la comunicación antes que otra estación pueda acceder al medio. Durante el periodo de contención el campo de duración se dispone de la siguiente manera:

- Si la dirección destino es un grupo de direcciones, el campo de duración es 0.
- Si el campo más fragmento es 0 y el destino es una dirección única, luego el campo duración contiene el tiempo en microsegundos requerido para trasmitir una trama ACK mas un corto periodo de espacio inter-trama.
- Si el campo más fragmento es 1 y el destino es una dirección única, luego el campo duración contiene el tiempo en microsegundos requerido para transmitir el siguiente fragmento más 3 cotos periodos inter-tramas.

Carga de una trama administración:

802.11 describe una serie de elementos que residen en el cuerpo de las tramas administración. Las siguientes son las más comunes:

- Número de algoritmo de autenticación
- Número de secuencia de transacción de autenticación
- Texto desafío
- ID de asociación (AID)
- Código de estado
- Código de razón
- Intervalo de baliza
- Intervalo de escucha

- Mapa indicador de trafico
- Información de capacidad
- Estampilla de tiempo
- SSID (identificador de grupo de servicios)
- Taza de trasmisión soportadas

Trama de administración solicitud de asociación:

Una STA envía esta trama a un AP si desea asociarse el. La STA logra asociarse al AP cuando este se lo permite

Trama de administración respuesta de asociación:

Luego de recibir una trama de solicitud de asociación, el AP envía una trama de respuesta de asociación indicando si el pedido de asociación de la STA es aceptado o no.

- Trama de administración solicitud de re asociación:

Una STA enviara este tipo de trama a un AP si quiere re-asociarse con un AP. Una re-asociación puede ocurrir si una STA se mueve fuera de rango de un AP y entra en el rango de otro. La STA requerirá re-asociarse con el nuevo AP para que este se entere que debe negociar el re-envió de tramas de datos con el viejo AP.

- Trama de administración respuesta de re-asociación:

Luego de recibir una trama de re-asociación, el AP responderá con una trama respuesta de re-asociación indicando si el pedido de re-asociación de la STA es aceptado o no.

- Trama de administración solicitud de prueba:

Una STA envía una solicitud de prueba para obtener información de otra STA o AP. Por ejemplo una STA podría enviar una trama de este tipo a todas las estaciones para determinar que AP están en rango para una posible asociación.

- Trama de administración respuesta de prueba:

Si una STA o AP recibe una trama solicitud de prueba, la STA responderá con este tipo de tramas conteniendo información específica de sí mismo. Esta trama es similar a la trama baliza, con la diferencia que no lleva la información TIM y que son generadas solamente en respuesta de una trama solicitud de prueba.

- Trama de administración Baliza:

En una WLAN de infraestructura, un AP envía tramas balizas periódicamente para proveer sincronismo entre las STAs. El periodo entre tramas balizas es generalmente 100 milisegundos por defecto. Esta taza de tramas balizas (10 por segundo) suele ser suficiente para la mayoría de las aplicaciones, pero hay ciertas aplicaciones que pueden requerir una tasa más elevada como el roaming rápido, y otras se benefician con una taza menor como el ahorro de energía.

La baliza incluye una estampilla de tiempo que todas las STA utilizan para refrescar lo que en 802.11 se conoce como TSF (función de sincronización de tiempo). Si un AP soporta la función de punto de coordinación, utiliza una trama baliza para anunciar el inicio de un periodo libre de contención. Si la red es una IBSS, todas las STA envían una baliza periódicamente para mantener el sincronismo.

Una trama baliza típica tiene una longitud de 50 bytes. No hay un periodo reservado para las balizas, y deben ser enviadas utilizando la función de coordinación distribuida. Si otra STA está enviando una trama cuando debe enviarse una baliza, el AP debe esperar. Como resultado, el tiempo entre tramas puede ser más largo de lo esperado, sin embargo las STA compensan esta inexactitud utilizando el valor en la estampilla de tiempo dentro de la baliza para resetear sus relojes luego de recibir una baliza.

- Tramas de administración ATIM:

En una WLAN ad hoc, una STA con tramas almacenadas de otras STAs envía una trama ATIM (mensaje indicador de anuncio de trafico) a cada STA durante la ventana ATIM, que sucede inmediatamente de enviada una baliza. La STA luego envía las tramas almacenadas a las STAs correspondientes. La trama ATIM advierte a las STA en modo sueño que se mantengan activas el tiempo suficiente para recibir todas las tramas almacenadas.

- Tramas de administración des-asociación:

Si una STA o AP desea terminar una asociación, enviara una trama des-asociación a la STA en cuestión. Una sola trama des-asociación puede terminar con la asociación con más de una STA utilizando o direcciones generales (Multicast).

- Tramas de administración autenticación:

Una STA envía una trama autenticación a una STA o AP con la que quiere autenticarse. La secuencia de autenticación consiste en la trasmisión de una más tramas autenticación, dependiendo del tipo de autenticación que está siendo implementado (Sistema abierto o llave compartida).

- Tramas de administración des-autenticación:

Una STA envía esta trama a una STA o AP con la que quiere terminar una comunicación segura.

- Trama de administración Acción:

Esta trama permite agregar más tipos de tramas, dentro del espacio limitado destinado a subtipos de tramas de administración adicional. El cuerpo de esta trama incluye códigos que identifican muchos tipos de tramas y funciones, como por ejemplo QoS y operaciones de requerimientos de velocidades altas.

- Tramas de administración Acción no ACK:

Esta trama tiene el mismo uso que la trama acción, excepto que no requiere que la STA receptora envié un ACK.

Tramas de control:

Proveen la funcionalidad necesaria para asistir en la correcta entrega de las tramas de datos. Esta incluye a funciones como ACK y RTS/CTS.

- Trama de control de encapsulado:

Esta trama encapsula la trama original y agrega un campo de control HT, que son requeridas en operaciones 802.11n.

- Trama de control solicitud de bloque ACK:

Esta trama es enviada desde una STA para solicitar que una STA confirme la recepción de un determinado bloque de tramas (ACK).

- Trama de control bloque ACK:

Para evitar enviar un ACK por trama, una solo ACK es enviada para confirmar la recepción exitosa de múltiples tramas.

- Trama de control activación de ahorro de energía:

Cuando una STA recibe esta trama, la STA refresca su vector contador de acceso al medio (NAV), en junto con otros parámetros indica el tiempo que trascurrirá antes de poder enviar una trama.

- Trama de control solicitud para enviar (RTS):

Una STA puede enviar una trama RTS a otras STA para negociar él envió de tramas de datos. El valor en el campo de duración, es el tiempo que la STA necesita para enviar la trama, más una trama CTS, más una trama ACK, más 3 intervalos cortos inter-tramas (SIFS).

- Trama de control permiso para enviar (CTS):

Luego de recibir una trama RTS, la STA envía una trama CTS para autorizar el periodo que la STA trasmisora requiere para enviar sus tramas.

- Tramas de control ACK:

Cuando una STA recibe una trama sin errores debe enviar una trama ACK a la STA trasmisora para confirmar su correcta recepción.

- Trama de control finalización de periodo libre de contención (CF End):

Anuncia la finalización del periodo libre de contención. En esta trama el campo de duración es siempre 0, y el campo RA contiene la dirección grupal (broadcast).

- Trama de control CF End + CF ACK:

Esta trama confirma el periodo libre de contención y anuncia la finalización de una trama CF. En esta trama, el campo de duración es siempre 0, y el campo RA contiene la dirección grupal (broadcast).

Tramas de Datos:

El mayor propósito de este tipo de trama es la de transportar información (MSDUs), a la STA destino. El campo duración contiene el tiempo en milisegundos necesarios para transmitir la trama y recibir un ACK. La carga útil total de la trama puede ser de 7955 Bytes como máximo, por consiguiente la mayoría de los datos intercambiados requieren múltiples tramas de datos para llevar la carga completa.

Algunos fabricantes utilizan la trama de datos nula, que tiene la carga de la trama de datos vacía, para transportar información especial de control a otras STA. Otros utilizan la trama de datos nula como parte de su escaneo activo.

3.4. Evolución del estándar IEEE 802.11

A consideración de este documento, el estándar IEEE 802.11 para WLANs es por lejos el más implementado en el mundo. Se comenzó a trabajar en este estándar en los comienzos de 1990. En ese momento, el estándar 802.11, fue visto en gran medida como una alternativa mediocre a la red cableada Ethernet 802.3 que en ese momento conectaba la mayoría de los usuarios a internet. El concepto de soportar aplicaciones con altos requerimientos de QoS como VoIP no era una de las prioridades del diseño. Sin embargo desde el 2000, se tornó evidente que las WLANs 802.11 serían utilizadas para aplicaciones que demandan QoS. De manera similar, que en el diseño original, se prestó relativa poca atención las áreas relacionadas con la seguridad como autenticación y encriptación. Actualmente se toma por sentado que la seguridad del primer intento de conexión con una red 802.11 es un requerimiento importante en la implementación de esta tecnología. En paralelo con estos cambios, la capa física de 802.11 ha sufrido una cantidad importante de mejoras, y en el proceso ha incrementado notablemente la velocidad y rango de esta tecnología con la incorporación de 802.11a, 802.11b, 802.11g, 802.11n entre otras.

Esta combinación de factores: incremento de la velocidad, mayor rango de cobertura, requerimientos QoS, Y de seguridad se han combinado para crear una serie de desafíos para la implementación de WLANs 802.11, y también para el comité IEEE 802.11.

Para abordar estas crecientes demandas por parte del usuario, el comité IEEE 802.11 formo deferentes grupos de trabajo para abordar los diferentes factores ya mencionados.

La siguiente figura muestra los grupos formados por 802.11 como líneas de tiempo.

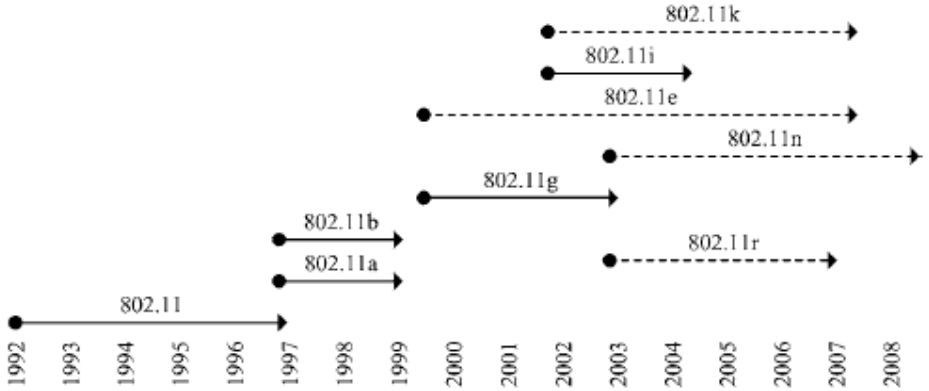


Figura 3.4.1: Línea de tiempo de grupos de trabajo 802.11.

El círculo negro indica cuando el proyecto fue aprobado. Una línea continua seguida de una flecha indica cuando el estándar fue rectificado. Una línea punteada indica que el estándar está todavía en progreso y aún no ha sido rectificado. Se debe notar que el trabajo de los grupos 802.11r y 802.11n está todavía en proceso.

3.4.1. Estándar 802.11, capa física

El estándar básico relacionado con la capa física en 802.11 fue rectificado en 1997. La limitación de la relativa baja velocidad de 1-2 Mbps, en comparación con la red cableada Ethernet 802.3, aseguro que se iniciaran varios grupos de investigación para confeccionar estándares de alta velocidad. A continuación se resumen las diferencias entre el estándar original y las variantes que fueron introducidas inmediatamente para satisfacer la demanda de mayor velocidad y rango de operación.

Name	Ratification Date	Frequency Band (GHz)	Theoretical Speed (Mbps)	Average Range	Transfer Mechanism
802.11	1997	2.4	1–2	–	DSSS FHSS
802.11a	1999	5.8	54	25 m	OFDM
802.11b	1999	2.4	11	55 m	CCK
802.11g	2003	2.4	54	55 m	CCK OFDM
802.11n	TBD	2.4 and 5	540	TBD	OFDM MIMO

Figura 3.4.2: Características físicas de 802.11.

El término “transfer mechanism” describe el mecanismo de modulación utilizado.

3.4.2. Grupos de trabajo relacionados con el roaming

En las próximas secciones nos enfocamos en los grupos 802.11i, 802.11e, 802.11k y 802.11r ya que estos grupos de trabajos son los que tienen mayor influencia en el roaming rápido y seguro en 802.11 (también dedicaremos un capitulo solamente a 802.11r y sus aportes a cada grupo de trabajo). Observaremos como 802.11i se ocupa de la seguridad, 802.11k de tomar mediciones y trasmitirlas para que las STA seleccionen un AP inteligentemente para el traspaso y 802.11e tomara la responsabilidad de negociar las reservas necesarias para el QoS requerido. Finalmente el estándar 802.11r intentara combinar todo el trabajo relacionado con un roaming rápido proveniente de los otros grupos en un intento de unificarlos en un único estándar.

3.4.3. IEEE 802.11i

El grupo de trabajo 802.11i fue creado en 2001 con el objetivo de proveer un acceso seguro a las redes 802.11. Esto comenzó como resultado de la reacción negativa del mercado a las vulnerabilidades de WEP que hasta ese momento era el único mecanismo de seguridad que 802.11 ofrecía.

El estándar 802.11i define procedimientos RSN (Robust Secure Networks) que ocurren durante la fase de asociación; Esto permite al cliente y el AP determinar la seguridad de la conexión de esta asociación particular. La siguiente figura ilustra le procedimiento de asociación 802.11 expandido para incluir la información RSN.

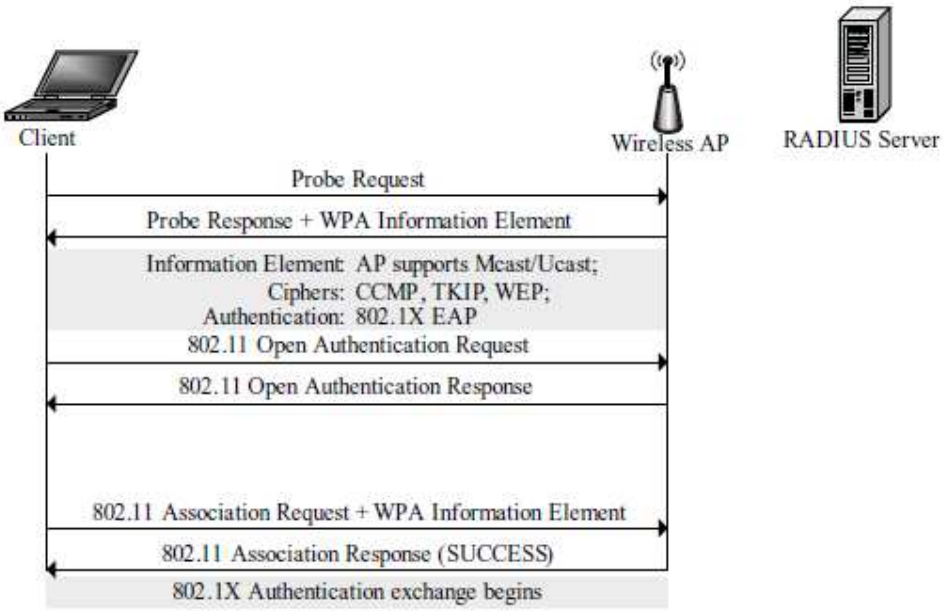


Figura 3.4.3: Establecimiento de la conexión en 802.11 utilizando 802.11i.

Una de las limitaciones más notorias de WEP es la encriptación simétrica de las tramas de datos basado en una forma particularmente vulnerable de utilizar el método de encriptación Riverst Cipher 4 (RC4). Con el fin de solucionar este inconveniente, el grupo i desarrollo dos nuevos métodos de encriptado: Temporal Key Integrity Protocol (TKIP) y Counter Mode CBC/MAC Protocol (CCMP).

TKIP de hecho utiliza el método de encriptado RC4 de una mejor manera, solucionando las vulnerabilidades expuestas en WEP. CCMP está basada en un método de encriptado fundamentalmente diferente y mucho más robusto, Advanced Encryption Standard (AES). Una de las ventajas de TKIP es que al estar basado en RC4, se puede implementar utilizando el mismo hardware 802.11 basado en WEP, en cambio CCMP es necesario adquirir un nuevo tipo de hardware para poder implementarlo.

3.4.3.1. Encriptado en 802.11i

A pesar del tipo de seguridad seleccionada, y sin importar el tipo de encriptado utilizado, el encriptado en 802.11i requiere de dos claves: Pairwise Transient Key (PTK) y Group Transient Key (GTK). La clave PTK se utiliza para encriptar el trafico unicast desde la STA al AP y desde el AP a la estación. La clave GTK es utilizada por el AP para encriptar el

tráfico broadcast/multicast enviado a todos las STAs dentro de la BSS, y las STA requieren de esta clave para poder des-encriptar este tráfico. A continuación se muestra el modo de operación básico de este encriptado:

1. La STA se asocia al AP y negocia los parámetros de seguridad utilizados dentro del proceso de asociación.
2. El AP autentica al usuario, con el método de autenticación seleccionado.
3. Se ejecuta un protocolo de validación de claves de 4 vías, para negociar el PTK entre la STA y el AP.
4. Las claves temporales acordadas son programadas dentro de los parámetros locales 802.11, utilizando el tipo de encriptado negociado, y luego se encriptan las tramas.

El paso 3 es igual a pesar del método de autenticación seleccionado (Personal o Enterprise), el saludo de 4 vías es utilizado en ambos casos para entregar la clave PTK a partir de la clave PMK. Ambos casos difieren en la fuente de PMK. En el caso del modo personal la clave PMK se supone ya conocida por la STA y el AP antes de la asociación. Esto es así debido a que PMK se supone ser parte de las claves previamente compartidas, que se encuentran estáticamente configuradas en los AP y las STAs que esperan asociarse entre sí.

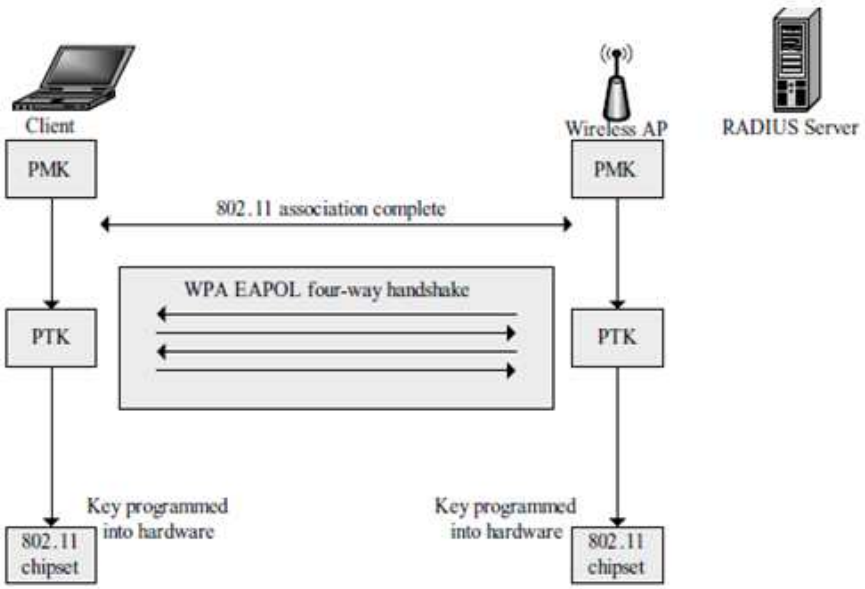


Figura 3.4.4: Modo de operación básico de encriptado con modo de seguridad Personal.

En el caso del método de seguridad Enterprise, la clave PMK es entregada de manera dinámica a través del proceso de autenticación en el paso 2. Esto aumenta mucho el grado de entropía debido a que la clave PMK también es diferente en cada sesión iniciada.

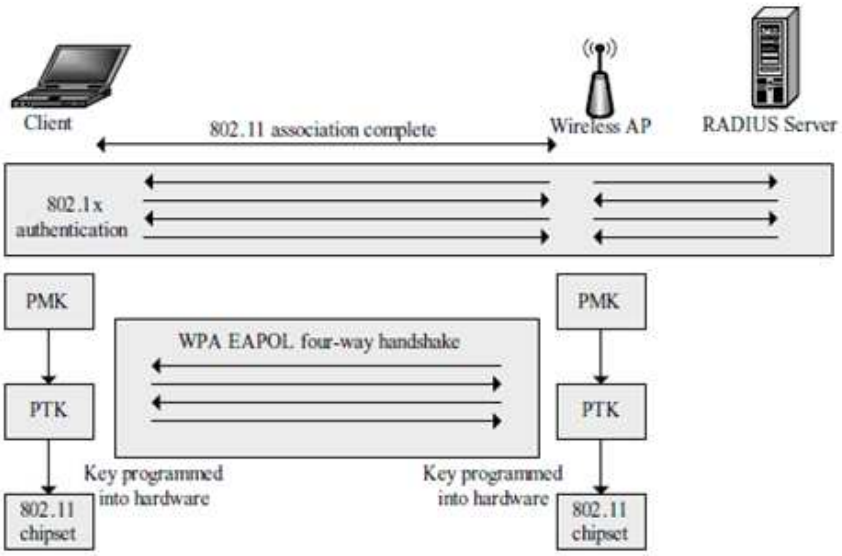


Figura 3.4.5: Modo de operación básico de encriptado con modo de seguridad Enterprice.

3.4.3.2. Pre-autenticación en 802.11i

Uno de las mejoras más importantes provistas por 802.1i es la pre-autenticación. Esta herramienta es muy relevante con respecto al roaming, debido a que la seguridad robusta obtenida por el grupo i es lograda a expensas de mayor complejidad. Esta complejidad se manifiesta en términos de latencias entre la asociación y la posibilidad de la estación de comenzar a utilizar 802.11 para enviar sus tramas de datos. Si esta demora sucede solamente un ves en el comienzo de sesión, la demora adicional, que ronda las desenas de mili segundos, puede ser aceptable. Sin embargo en un entorno donde se esperan traspasos de dispositivos móviles, la implementación en bruto de 802.11i puede resultar en que esta demora esté presente en cada inicio del proceso de roaming. El grupo i reconoció que este inconveniente es inaceptable en una tecnología que se considera cada vez más como medio para usuarios VoIP móviles.

La pre-autenticación disminuye la latencia capturando parte de la información referida a las claves obtenidas durante la autenticación (paso 2) y enviándola al AP que posiblemente

albergue a la STA luego del roaming. Esto se logra por medio de realizar el proceso de autenticación con el futuro AP por medio del AP actual a través del DS (usualmente la red cableada).
Esta técnica permite la comunicación de la STA y el futuro AP sin interrumpir el flujo de datos con el actual AP.

A pesar de que 802.11i presenta algunas herramientas para lograr un roaming rápido y seguros, el hecho es que no son suficientes para lograr un roaming que permite que aplicaciones críticas como VoIP no se vean deterioradas o interrumpidas durante el proceso.

3.4.4. IEEE 802.11e

El grupo 802.11e se encarga de estandarizar los aspectos de 802.11 relacionados con proveer garantías de QoS, relacionados con las perdidas y demoras en el entorno impredecible de 802.11.
El estándar 802.11 original incluye algunos conceptos básicos relacionados con QoS. Estas ideas estaban basadas en dividir el tiempo entre 2 tramas balizas en 2 fases: Contention Period (CP) y Contention-Free Period (CFP). El acceso al medio durante el periodo CP es dirigida por el Distributed Control Funtion (DCF) encontrado en el AP (por lo general basado en CSMA/CA). Durante este periodo CFP, el Point Coordination Function (PCF) decide cuando una determinada STA tiene permitido trasmitir, el PCF comunica esto a la STA por medio de una trama CF-Poll. El hecho de que el PCF este centralizado en un AP permite que el acceso al medio sea determinista, lo cual es necesario para poder garantizar QoS. El estándar 802.11 original no provee detalles de cómo debe ser dirigido el acceso al medio. El grupo 802.11e expande estos conceptos básicos para proveer mecanismos más ricos y mejor especificados para QoS en 802.11.

El estándar 802.11e provee la reserva de QoS de dos maneras. La primera se conoce como Enhanced Distributed Channel Access (EDCA) y está basada en una extinción de DCF llamada Enhanced DCF (EDCF). Este mecanismo define diferente colas de tráfico para diferentes tipos de tráfico, de tal manera que el tipo de tráfico con mayor prioridad logre obtener un mejor acceso al medio durante el periodo CP. Sin embargo, como el proceso aun es contention-based (best-effort), no se logra una garantía verdadera de QoS en este modo. A

pesar de la falta de una garantía firme, muchos creen que la alta prioridad provista a las tramas de VoIP en este modo otorga un nivel de servicio aceptable para voz. Este modo a veces se conoce como WiFi Multimedia Mode (WMM).

El segundo mecanismo se conoce como Hybrid Coordinator Funtion Controlled Channel Access (HCCA). Este mecanismo está basado en una versión mejorada de PCF llamada Hybrid Coordination Funtion (HCF). Una de las mejoras más importantes en relación al PCF original es que el Hybrid Coordinator (HC) puede permitir el acceso durante el CFP en el orden que decida, y no solo en modo round robin, como sucedía en el caso de PCF. Esta flexibilidad otorga a HCF la capacidad de otorgar un mayor nivel de garantía de QoS. La segunda mejora más importante es que, al igual que EDCF, el HCF provee diferente clases de tráfico. El hecho de que el HC pueda permitir a una STA enviar múltiples tramas seguidas en un intervalo de tiempo determinado, es la tercera diferencia importante con el estándar 802.11 original. Esta herramienta será muy útil si el HC sabe que la cantidad de tráfico sensible a QoS que la STA tiene en cola requiere un intervalo de tiempo mayor para lograr el nivel de QoS esperado. Una cuarta mejora que vale la pena notar es que el HCF puede interrumpir el CP para otorgar acceso inmediato al medio a una STA promedio de la trama CF-Poll. Este modo es también conocido como WMM Scheduled Access (WMM-SA). A continuación se exhibe un ejemplo que muestra al EDCF y al HCF en una BSS con QoS (QBSS) con dos STAs con QoS (QSTAs).

La figura 3.4.6 muestra, que desde un único AP, se realizan intercambios de tramas con dos STAs a través de los 2 medios de acceso EDCA y HCCA. En el modo HCCA, las STAs pueden enviar tramas únicamente luego de recibir la trama CF-Poll proveniente del AP.

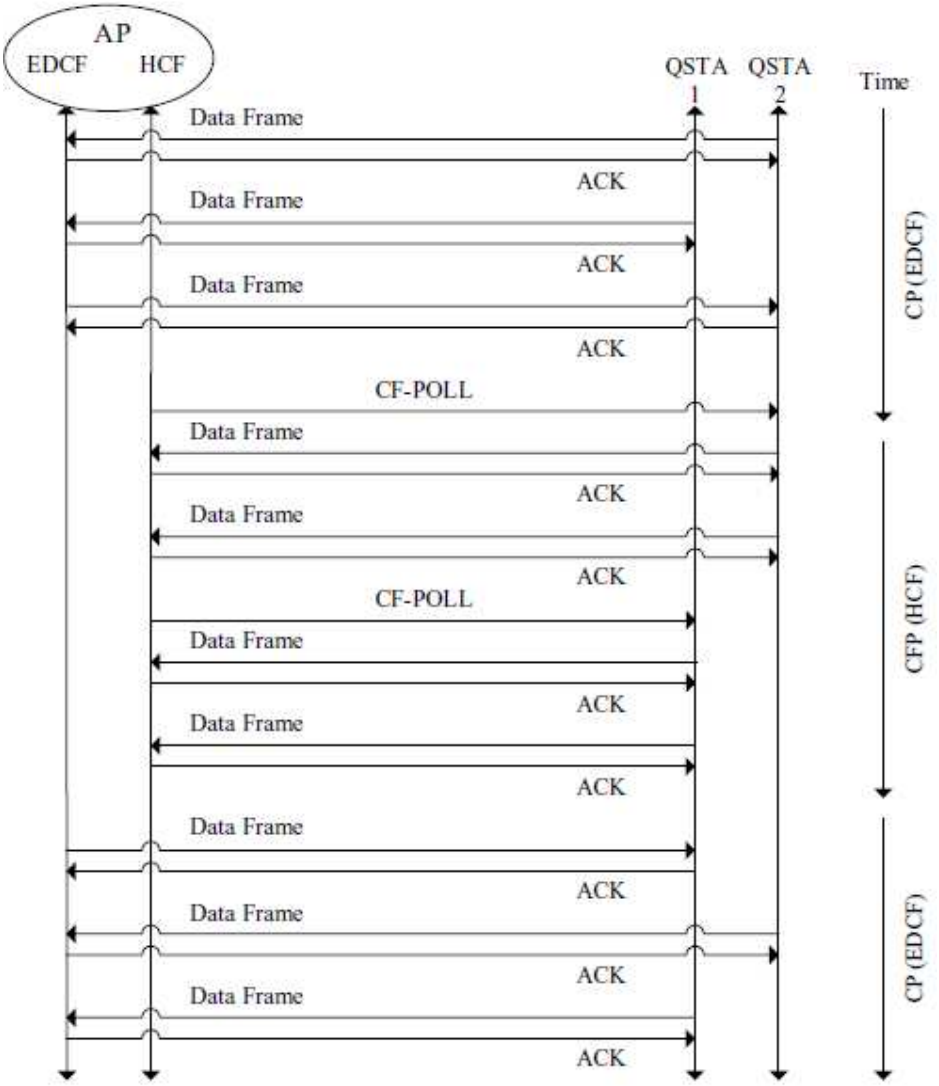


Figura 3.4.6: Las funciones EDCF y HCF en 802.11e.

3.4.5. IEEE 802.11k

El estándar 802.11k también conocido como Radio Resource Measurement (RRM) aporta capacidad, fiabilidad y facilidad de mantenimiento a las WLANs por medio de mediciones. La información obtenida es puesta a disposición de la red a través de una interface estándar denominada Management Information Database (MIB).

Cuando se implementa 802.11k. La STA mantendrá una lista de STAs y APs conocidos dentro de su rango. Las entradas de la lista incluirán estadísticas del enlacen, utilización del canal, taza de trasmisión, y los márgenes del vínculo, a medida que esta información es

reportada por dichas STAs y APs. Las especificaciones también soportan reportes asíncronos a una entidad de red administradora de eventos de asociación y autenticación.

Para soportar estas estadísticas, hay un número de reportes definidos por parte de 802.11k, se listan a continuación:

- Beacon Report
- Frame Report
- Station Statistics Report
- Channel Load Report
- Medium Sensing Time Histogram Report
- Noise Histogram Report
- Location Configuration Information (LCI) Report
- QoS Metrics Report
- Link Measurement Report
- Neighbor Report
- Measurement Pause

Cada uno de esto reportes, con excepción del Mesurement Pause, definen un par de tramas solicitud/Respuesta, donde la información es requerida en la solicitud y es devuelta en la respuesta. Algunas veces la información es enviada inmediatamente, y en otras ocasiones, la trama solicitud inicia un intervalo de medición que al concluir organiza la información y la envía en la trama respuesta. En este caso, cuando un intervalo de medición cero es requerido, esto dicta que la STA debe responder instantáneamente con los valores estadísticos requeridos.

Todas reportes en la lista, exceptuando Link Mesurement Report y Neighbor Report, son comunicados a través de una trama Solicitud de Mediciones, y una trama Respuesta de Medición correspondiente. Un campo de tipo de servicio en la trama Solicitud de Medición especifica el tipo de reporte solicitado. Las 2 excepciones (Link Mesurement Report y Neighbor Report) son tratadas de manera separada ya que estas mediciones no son formalmente solicitadas, sino que simplemente son reportes de información que las STAs y APs ya tienen almacenada.

La trama Beacon Report, es utilizado por las STA para aprender que canales perciben como activos las otras STA. La solicitud puede realizarse de 3 maneras: pasivamente, activamente

y el modo de tabla. En ambos modos pasivo y activo, la solicitud inicia un intervalo de medición de longitud específica. Al final de este intervalo, la información obtenida por la STA de las tramas Balizas o tramas prueba/respuesta son reportadas al solicitante. La diferencia entre estos dos es que activamente hace referencia a que la solicitud de medición es desencadenada por una trama solicitud proveniente de una STA. En modo Pasivo, no se genera una solicitud de medición, el inicio de las mediciones se da a partir de una trama baliza enviada periódicamente. En ambos casos, la información devuelta es referente a los canales y BSSID especificadas en la solicitud de Beacon Report. En el modo tabla baliza, no hay intervalo de medición, y la STA devuelve la información ya almacenada en su tabla baliza.

La trama Frame Report, es utilizado por una STA para solicitar un resumen de información referente a las tramas recibidas por la STA receptora. La STA que recibe esta solicitud devuelve un reporte resumido de las tramas recibidas desde cada una de las direcciones de donde recibe tramas. Por cada una de estas direcciones, se envían 4 campos de información, el contador de tramas recibidas, el promedio del indicador de energía recibida en el canal (RCPI), BSSID, y la dirección de transmisión.

Una STA envía una solicitud de Link Mesuramente Report a otra STA para obtener las mediciones relacionadas con su nivel de energía de trasmisión y una estimación del margen del vínculo. Esta información permite entender la capacidad instantánea del vínculo para una posible solicitud de QoS.

Cuando una STA recibe una solicitud de Station Statistics Report, esta responde con una trama de reporte de mediciones de radio que contiene estadísticas de la interface sobre la cual se recibió la solicitud. Estas estadísticas comprenden los siguientes contadores:

- Transmitted fragments
- Multicast transmitted frames
- Transmit failures
- Retries
- Multiple retries
- Duplicate frames
- RTS successes
- RTS failures
- ACK failures

- Received fragments
- Multicast received frames
- FCS errors
- Transmitted frames

Reportes adicionales importantes para roaming:

Los 6 reportes restantes son particularmente importantes para lograr un roaming rápido. Una solicitud de Medium Sensing Time Histogram Report provee un medio flexible para que una STA obtenga una variedad de reportes complejos de otra STA. Hay 4 tipos de histogramas que se pueden solicitar:

- Received Power Indicator (RPI) Time Histogram
- Clear Channel Assessment (CCA) Idle Time Histogram
- CCA Busy Time Histogram
- Network Allocation Vector (NAV) Busy Time Histogram

Todos los histogramas previamente mencionados proveen un indicador de la disponibilidad relativa al medio RF, percibida por la STA que está siendo indagada.

Una solicitud de Channel Load Report devuelve la porción del intervalo de tiempo de medida estipulado durante el cual la STA receptora percibe el canal especificado como ocupado.

El reporte Noise Histogram Report consiste en un histograma de medición de energía proveniente de equipos no pertenecientes a 802.11. Estas lecturas de energía se obtienen por medio del muestreo del canal especificado solo cuando el CCA indica que el medio esta libre para ser utilizado.

La solicitud de LCI Report devuelve la información de latitud, longitud y altitud de un objetivo. Una STA puede solicitar la ubicación correspondiente a sí mismo o a la STA receptora. Si la STA receptora no cuenta con los medios para proveer esta información, el campo de datos de la trama respuesta son ceros.

La solicitud de QoS Metrics Request establece la QSTA destino y la clase de tráfico para el cual se medirá el tiempo en cola. La QSTA destino se identificara por medio de la dirección MAC a donde se están enviando las tramas con la clase de servicio especificada. La clase de tráfico es especificado con un numero desde 0 a 15 indicando la prioridad de dicho tráfico (0-7) o el TPSEC (8-15). La demora en cola es presentada en forma de histograma.

El reporte Neighbor Report contiene información proveniente de la tabla MIB dot11RRMNeighborReportTable que contiene información referente a APs vecinos. Una STA obtiene este reporte enviando una trama de solicitud de Neighbor Report al AP con el que se encuentra actualmente asociado. Esta información puede ser utilizada por la STA para determinar posibles candidatos de roaming.

Los últimos 6 reportes pueden mejorar notablemente el proceso de roaming en 802.11. Mientras más información se obtenga relacionada a la actual topología de red, niveles RF, y estados de QoS, es posible realizar decisiones de roaming mas informadas y por lo tanto mejores. Es por este que 802.11k cumple un rol muy importante a la hora de buscar un roaming rápido.

3.5. Estándar 802.11r

3.5.1. Introducción a Fast roaming

El estándar 802.11 original incorpora el roaming de una manera muy simple. Sin embargo, la limitada velocidad y seguridad provista por el estándar original durante el roaming hace muy difícil la implementación de aplicaciones de voz seguras. El grupo de trabajo 802.11r fue encargado con la tarea de estandarizar aspectos que reduzcan el tiempo de transición durante el roaming 802.11, referido como transición de BSS en 802.11r.

De las principales mejoras creadas para lograr un roaming 802.11 seguro y rápido para aplicaciones de Voz, el estándar 802.11r es el menos maduro, ya que otros estándares ya han sido ratificados o están más cerca de serlo que el 802.11r. Esto se debe a que fue necesario que otros grupos terminen de desarrollar sus soluciones (802.11i, 802.11e y 802.11k) antes de que 802.11r las pueda integrar.

Una solución completa de rápida transición de BSS incluirá la aplicación de 802.11e que aporta la sobrecarga de información sobre el estado de QoS del AP en las tramas balizas. Del estándar 802.11k que aporta reportes sobre los vecinos y otras medidas que la STA puede utilizar para decidir que AP elegir para re asociarse. A pesar que este tipo de información es claramente parte importante para mejorar el proceso de roaming, el como la STA elige el AP

con el que re asociarse escapa a los objetivos de la norma 802.11r. El objetivo de 802.11r es minimizar el tiempo que una STA pierde conectividad con el DS. En muchos de los casos el DS es la red inalámbrica que interconectan a los APs. Perder conexión con el DS implica un corte en el flujo de datos de las aplicaciones del usuario, algo que debe ser minimizado especialmente para tráfico de tiempo real, como la voz.

El estándar 802.11r define el término dominio móvil (MD) como el grupo de APs con soporte para transiciones rápidas a los que la STA puede re asociarse en el momento que lo requiera. Todos los APs en un dominio móvil están interconectados por un mismo DS. Para poder describir las STAs y APs que soportan 802.11r, se introducen los términos STAs de transición rápida (TSTA) y APs de transición rápida (TAP).

3.5.2. Antes y después de 802.11r

Transiciones de BSS antes de 802.11r:

Basados en técnicas pre-802.11r, una transición de BSS segura para aplicaciones con requerimientos de QoS pasan por las siguientes 5 etapas:

1. Escaneo en búsqueda posible de APs a los que desasociarse.
2. Autenticación abierta 802.11. Este intercambio solo sucede por compatibilidad con la norma 802.11 original pero no se trata de la verdadera autenticación. La autenticación ocurre en el paso 4.
3. Re asociación.
4. Intercambio PTK (pares de claves transitorias). La complejidad de este paso varía dependiendo si se utiliza almacenamiento de claves, pre autenticación, o una re autenticación 802.1X completa para proveer el PMK (par de calves maestras). Incluso si se utilizaran los medios abreviados de almacenado de clave y pre autenticación, se requerirá un intercambio de cuatro vías para entregar las PTK. La técnica de almacenamiento de clave es una alternativa a la técnica pre autenticación que, al igual que en pre autenticación, tiene la PMK disponible para los posibles candidatos para una re asociación.
5. Control de admisión de QoS con el nuevo AP.

Considerando estas cinco etapas en serie, incluso si asumimos la latencia más corta de re asociación, el tiempo total de transición de BSS probablemente sea medido en el orden de muchas desenas de milisegundos o más, que probablemente interrumpa o termine una conversación de voz. Adicionalmente, como la admisión de QoS sucede al final, si la admisión falla, la estación deba iniciar el proceso de roaming nuevamente con otro posible candidato.

Transición de BSS en 802.11r:

El estándar 802.11r comprime las cinco etapas descriptas anteriormente de dos maneras, agregando el saludo de cuatro vías dentro del intercambio 802.11 de autenticación/asociación y reserva previa de recursos QoS. Nuevo elementos informativos son introducidos por la norma 802.11r. El elemento informativo de dominio móvil (MDIE) provee información que identifica el dominio móvil actual. El elemento informativo de transición rápida (FTIE) permite la publicación de información respecto a la infraestructura de red, la reservación de recursos, y políticas de seguridad.

Ambos el MDIE y el FTIE están presentes en las tramas balizas, prueba respuesta, pedidos de asociación y respuestas de asociación enviadas de una TAP a una TSTA. En la etapa final del desarrollo de la norma 802.11r, el grupo de trabajo decidió extender la información de FTIE para incluir campos pertenecientes a los mensajes 802.11i EAPOL-Key, por medio del agregado de información referente a la seguridad a las tramas de autenticación y de asociación 802.11. Esto reduce significativamente la latencia introducida por la transición de BSS debido a que el paso 4 del proceso descripto previamente puede ser incorporado en los pasos 2 y 3 sin incrementar el tiempo de intercambio de tramas en los mismos. Este es el primero de los 2 métodos fundamentales que la norma 802.11r utiliza para disminuir el tiempo de transición de BSS.

El segundo método se conoce como preservación (precervation), que permite a la TSTA realice el paso 5 del proceso descripto antes que el paso 2 y 3. Hay dos mecanismos para llevar a cabo la preservación: A través del DS (OTD: over the DS) y a través del aire (OTA, over the air). Utilizando OTD, la TSTA se comunica a la posible TAP objetivo, por medio del DS pasando a través del AP con el que se encuentra asociado en ese momento. OTD es el método preferido dentro de 802.11r debido a que otorga los beneficios de preservación sin la necesidad de interrumpir el flujo de datos. El método opcional OTA requiere que la TSTA realice el intercambio de autenticación solicitud/respuesta 802.11 directamente con el TAP

objetivo para la re asociación. Este intercambio es ampliado en 802.11r para incluir el pedido de reserva de QoS de la TSTA. Debido a que el método OTA permite a la TSTA reservar recursos sin la necesidad de terminar su asociación con su actual TAP, este método provee una alternativa para optimizar recursos.

El estándar 802.11r permite adicionalmente a realizar las transiciones rápidas de BSS con QoS sin utilizar el método de preservación, y en cambio realizar la reserva de recursos luego de terminado el proceso de asociación en el momento de la trasmisión de datos. Este tipo de entrega de QoS es apropiada cuando la TSTA detecta que el TAP en cuestión esta escasamente cargado y probablemente pueda cumplir con sus requerimientos de QoS. La TSTA puede determinar esto de la información incluida en las tramas balizas o tramas prueba respuestas provista por el AP en cuestión o por los reportes 802.11K de los vecinos.

3.5.3. Conceptos y terminologías de 802.11r

La figura muestra 3 aristas diferentes que ilustran algunas de las facetas del estándar 802.11r.

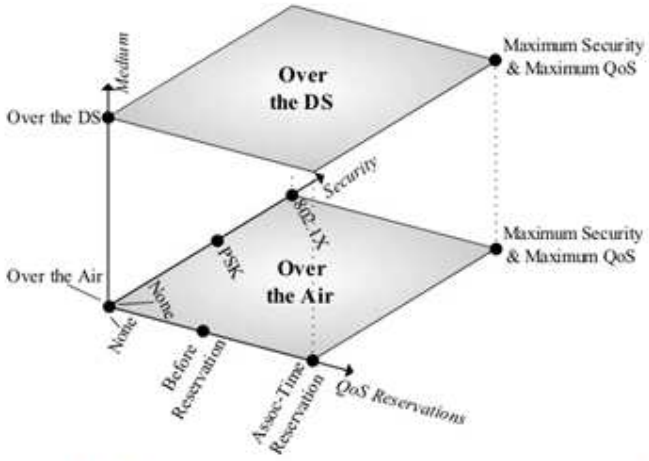


Figura 3.5.1: Posibilidades pre-traspaso contempladas por el estándar 802.11r.

Todas las permutaciones dentro de estas aristas son permitidas por 802.11r. Primero, en el reino de la seguridad, tenemos 3 paradigmas distintivos que requieren soporte: Sin seguridad 802.11i, 802.11i PSK, y autenticación 802.1X completa. Con respecto al QoS, puede no

haber soporte para reserva de QoS, soporte para reserva previo al traspaso, y soporte para reserva durante el traspaso. Segundo, para cualquier intercambio 802.11r permitidos previo a la asociación con el nuevo AP, hay 2 posibilidades de implementación: A través del Aire (OTA) o a través del DS (ODS). Ambos referidos a diálogos entre la STA y el objetivo AP previo a la asociación con el nuevo AP.

El dialogo OTA es una comunicación directa entre la STA y el AP. Debido a que la única trama de administración que se pueden intercambiar en este estado no asociado son las tramas de autenticación 802.11, el dialogo OTA se realiza enteramente por medio del agregado de la información deseada en las tramas de autenticación abierta 802.11 sin requerir seguir necesariamente el proceso normal de solicitud y respuesta de asociación. La STA puede seguir asociada al actual AP y sin embargo intercambiar información con el futuro AP a través de las tramas de autenticación abiertas.

Los otros intercambios previos a la asociación entre la STA y el objetivo son los que fueron descriptos por 802.11i. En este caso. El dialogo ocurre en dos etapas. La primera es la etapa inalámbrica entra la STA y su actual AP, y la próxima es realizada a través del DS que interconecta el futuro AP con el resto de la Red. La opción de 802.11r ODS se basa en este precedente. En contraste a la OTA en el caso de ODS, la información no se agrega a las tramas de autenticación 802.11. En cambio, un nuevo Tipo de Trama (FT: Frame Type) es creada por 802.11r. Esta trama se conoce como FT action frame (trama acción). La trama acción FT son trasmitidas desde la STA a su AP actual y estas son entregadas al AP objetivo a través del DS.

OTA y ODS representan 2 opciones que ofrecen funcionalidades muy similares, por lo cual sin importar que opción se utiliza, todas las permutaciones de seguridad y QoS dentro de 802.11r están disponibles. Una razón por la que el implementador prefiera elegir ODS antes que OTA es para evitar demoras generadas por el cambio de canales en la trasmisión de la STA para poder comunicarse con el nuevo AP.

3.5.4. Elementos de una arquitectura 802.11r

En la Figura 3.5.2 se presentaran los componentes de una arquitectura 802.11r. Muchos de estos componentes no son nuevos. Parte del trabajo de 802.11r ha sido definir estos componentes y sus relaciones de manera más precisa.

Una de las razones de esto es que originalmente 802.11 asumió que funciones específicas residirían en hardwares específicos de la estructura 802.11. A medida que la complejidad del hardware fue creciendo, 802.11r y la arquitectura Fat-AP tradicional fueron abordadas por una variedad de arquitecturas inalámbricas distribuidas (Figura 3.5.3). Por esto se tornó imprescindible definir funciones precisas, para permitir la posibilidad de que se implementen en componentes de hardware diferentes de diferentes fabricantes.

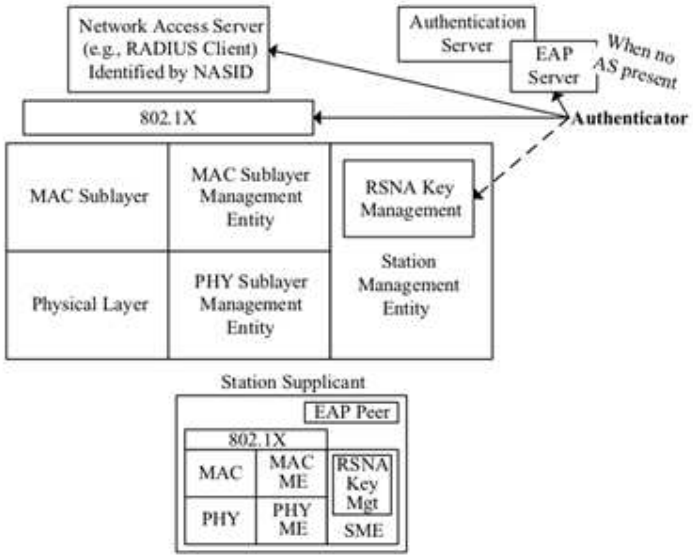


Figura 3.5.2: Entidades de la arquitectura del estándar 802.11r.

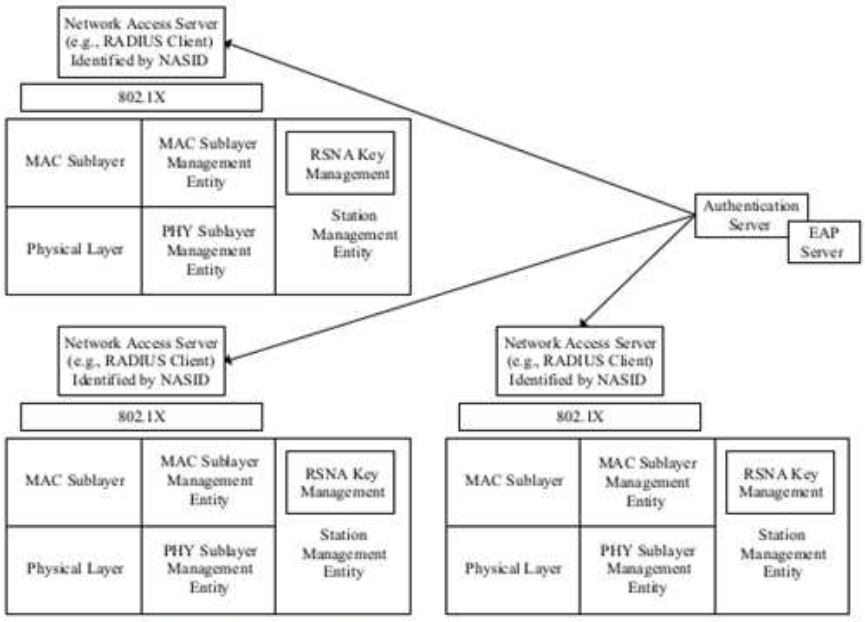


Figura 3.5.3: Entidades de una arquitectura Fat-AP en el estándar 802.11r.

La principal diferencia entre una estructura Fat-AP y la estructura general de conmutado inalámbrico, es que dentro de la estructura general pueden existir muchas variantes en las especificaciones del fabricante. Por ejemplo, en algunos casos, la entidad MAC existe enteramente en los Thin-AP, mientras que en otras las funciones MAC están divididas entre el AP y la entidad controladora central. Vemos el SME en las 3 figuras. Dentro del SME reside la función de administración de claves RSNA (asociación de red de seguridad robusta). La administración de claves RSNA es la nueva terminología para lo que se conocía como administración de claves 802.1X en los comienzos de los trabajos relacionados con la seguridad en 802.11. Esta administración de claves, en conjunto con el control de puertos 802.1X en el AP, comprenden las funciones de autenticación descriptas en los comienzos de 802.11. El hecho de que estas 2 funciones puedan estar en diferentes dispositivos de red (por ejemplo. el MDC y el AP) hace que sea importante que 802.11r los defina de manera clara como entidades diferentes.

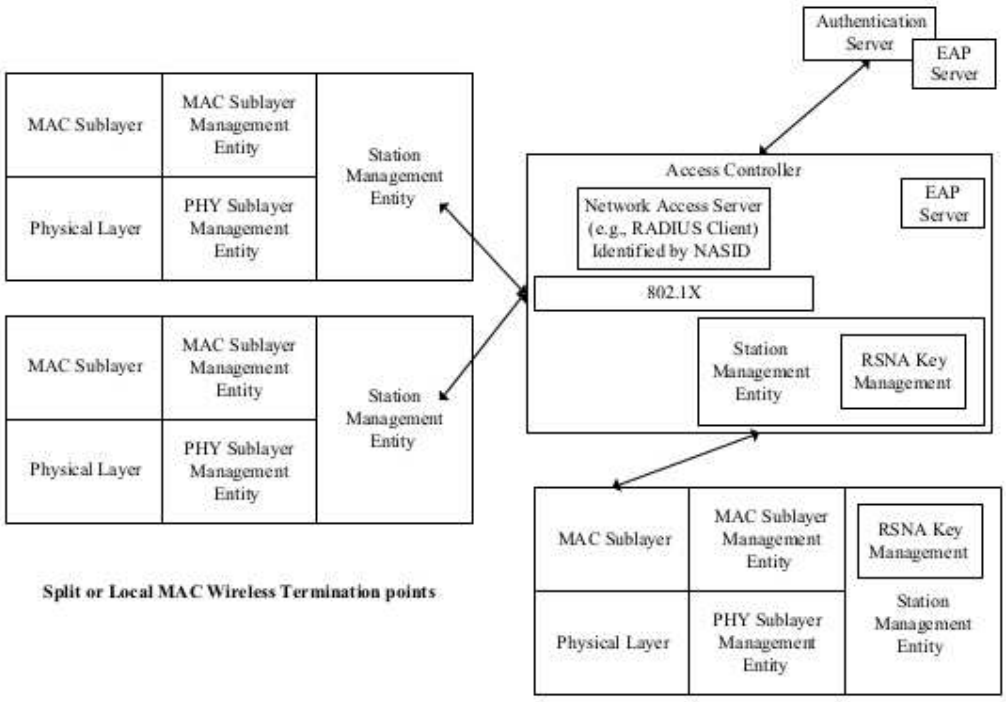


Figura 3.5.4: Entidades de una estructura de conmutado inalámbrico 802.11r general.

3.5.5. Nuevo conceptos de seguridad (Su relación con 802.11i)

802.11i define un concepto conocido como Par de claves maestras (PMK) que se utilizan para generar la sesión de claves dinámicas llamadas par de claves transitorias (PTK). Mientras que los conceptos fundamentales alrededor de estas claves no fueron alteradas por 802.11r, hay terminología nueva relacionados con ellos.

La figura 3.5.5 muestra 2 cambios fundamentales en la jerarquía de claves 802.11i. Similar al estándar 802.11i, la jerarquía comienza con la clave que es generada durante la negociación 802.1X completa o, en el caso del modo PSK, estáticamente configurada en la STA y AP. La clave generada en la autenticación 802.1X se llama Clave de sesión maestra (MSK). En el caso del modelo claves previamente compartidas (PSK), se utiliza el término PSK. En ambos caso, sin embargo como se ve en el diagrama jerárquico, la clave superior no se utiliza para crear la clave PTK, como era en el caso de 802.11i. En cambio se crea otro nivel PMK, el primer nivel se conoce como PMK-R0 y se utiliza para generar un segundo nivel conocido como PMK-R1, que a sus ves se utilizara para generar la clave PMK. La figura 3.5.5 muestra que se crearan múltiples claves PMK-R1 en un determinado MD, uno por cada BSSID. Debido a que ahora tenemos múltiples PMKs en un dominio, un nuevo concepto llamado key

holder (portador de claves) es creado. El portador de claves PMK-R0 se conoce como R0KH y el portador de claves PMK-R1 es conocido como R1KH.

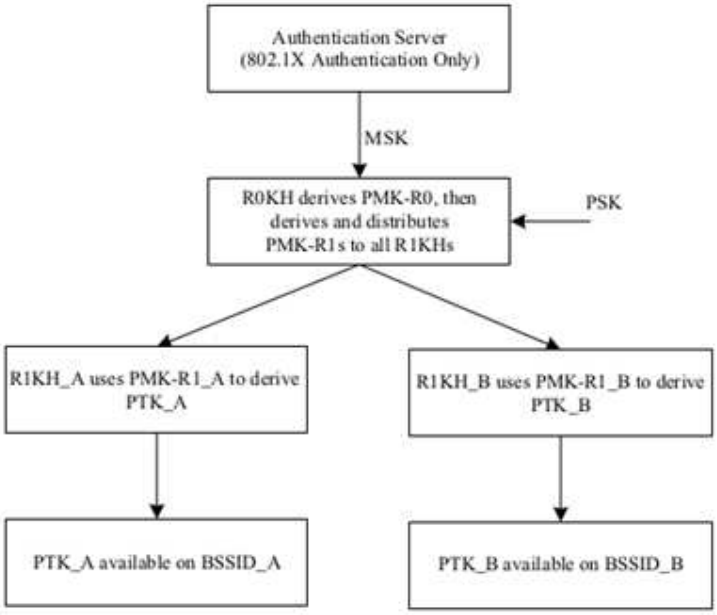


Figura 3.5.5: Jerarquía de los elementos claves en 802.11r.

El R0KH reparte un PMK-R1 por cada uno de los R1KHs en el MD. Para una arquitectura de red computada, sería conveniente que el PMK-R1 fuera el mismo para todos los APs conectados al controlador, pero esto crea una vulnerabilidad a la seguridad. La razón por la que PMK-R1 fue creado diferente a PMK-R0 fue con el objetivo de que este fuera específico para cada AP, y así debe permanecer para evitar debilidades en la seguridad.

Como ejemplo ilustrativo en una red de arquitectura conmutada, el R0KH puede residir en el controlador central y los R1KHs pueden existir en los APs que comparten el MD conformado por ese controlador.

La Figura 3.5.6 muestra las claves 802.11r, sus portadores, y su relación de manera gráfica. Por dentro se presenta el flujo que siguen las claves desde una entidad a otra. La figura muestra los componentes involucrados en la de gestión de claves RSNA dentro de una SME con más detalles.

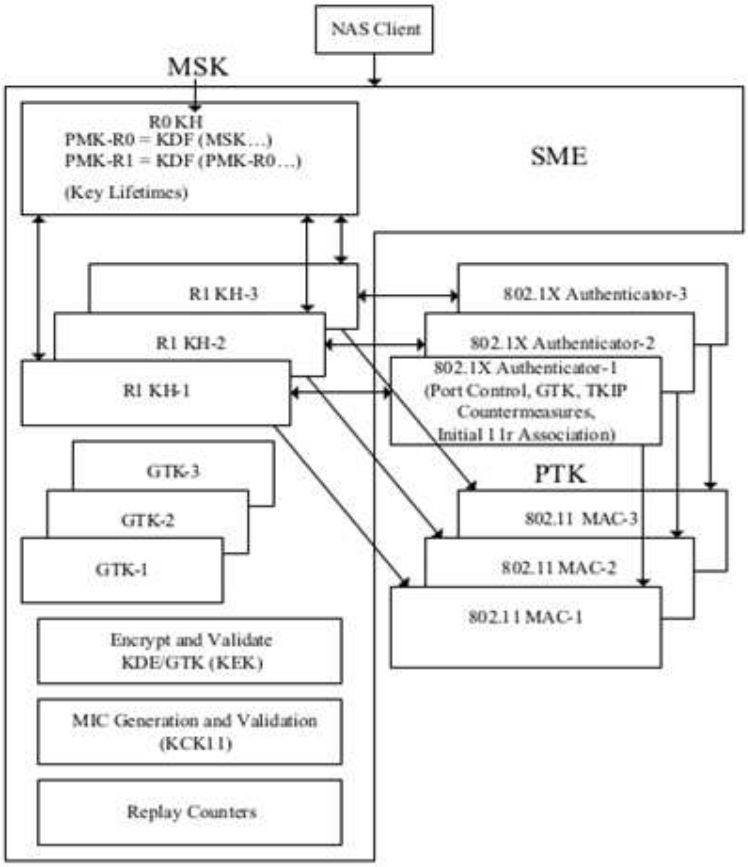


Figura 3.5.6: Las claves en 802.11r, sus portadores y relaciones entre ellos.

En algunas implementaciones, estas entidades residirán en el mismo dispositivo, y en otras, en dispositivos diferentes. El R0KH residirá en el mismo equipo físico donde las funcionalidades de autenticación 802.1X y cliente NAS residen. El R0KH-ID es el NAS ID de 48 octetos del cliente NAS. El R1KH-ID es la dirección MAC de 6 octetos de la entidad física que es el portador autorizado de la clave PMK-R1. La función que cada una de estas entidades toma en 802.11r son: NAS-ID recibe el MSK del servidor de autenticación, genera la PMK-R0 utilizando la MSK, y transfiere esta PMK-R0 al R0KH. El R0KH acepta esa PMK-R0 y genera múltiples PMK-R1s con ella y los transfiere a los respectivos R1KHs. El R1KH acepta los PMK-R1 y los utiliza durante el saludo de cuatro vías con la STA, de esta manera se entrega el PTK en el AP con el que vamos a re asociarnos. Todo esto sucede dentro de SME. El PTK luego es transferido a la entidad MAC.

La STA puede enviar el PMK-R1 específico a un AP basado en la información intercambiada durante la re asociación. Esto se debe a que la STA aún tiene posesión de la clave PMK-R0

de su primera asociación. Esta compleja infraestructura asegura que cualquier par STA-AP en el MD puedan generar claves PTKS únicas utilizando solamente el limitado intercambio de tramas permitido por 802.11r.

3.5.6. Reserva de recursos (Su relación con 802.11e)

El procedimiento de reserva de recursos 802.11e utiliza una solicitud ADDTS (add TSPEC) seguido del intercambio de asociación y autenticación para solicitar una reserva de recursos especificados en el TSPEC. Así como 802.11r incorpora el intercambio de seguridad 802.11i dentro de los mensajes de autenticación y re asociación, el estándar 802.11r permite incorporar estas solicitudes de recursos TSPEC dentro del mismo intercambio.

El intercambio completo de rápida transición de BSS para una estación que requiere reserva de recursos comprende 6 mensajes, a diferencia del intercambio de 4 mensajes cuando no hay QoS involucrado. Este intercambio se logra agregando 2 nuevas tramas de autenticación abiertas, autentication-ACK and autenticacion-confirm, como tercer y cuarto mensaje. Un determinado AP en un MD pude requerir que se utilice el intercambio completo de 6 mensajes para la reserva de recursos. Alternativamente puede dar la opción de utilizar el intercambio simple de 4 mensajes, agregando la solicitud TSPEC dentro de las tramas de re asociación. En el caso del intercambio de 4 mensajes la STA no sabrá si la reserva fue exitosa o no hasta que la re asociación finalizado.

El inconveniente de la reservación de recursos en 802.11r es que toma 4 mensajes para saber si la reserva será otorgada por el AP o no. Si el STA requiere asegurarse de que tendrá los recursos requeridos disponibles antes de asociarse, el intercambio de 4 mensajes debe completarse antes que la re asociación en sí, por ende, se requieren 6 mensajes para finalizar el proceso de roaming. Se recuerda que previo al comienzo de la re asociación, la STA puede mantener activa la comunicación con su actual AP sin detener el flujo actual de datos a pesar de estar tratando de reservar recursos en otro AP. Cabe denotar que en cualquiera de los casos, el hecho de que el AP deniegue la reserva de recursos no causa que la re asociación falle. La STA siempre tiene la opción de decidir continuar o no con la re asociación a pesar de no obtener la reserva de recurso esperada.

Incluso con el intercambio completo de seis mensajes para la reserva de QoS, el AP puede denegar la solicitud de reserva en el cuarto mensaje. En este caso, la STA tiene un número de opciones. La STA puede temporalmente demorar el proceso de roaming e intentar reservar los escasos recursos en el AP con la esperanza que un requerimiento más modesto pueda ser aprobado. La STA puede abandonar este AP e intentar conseguir estos recursos con otro AP candidato. Finalmente, puede permitir que la re-asociación se complete sin ningún tipo de reserva de recursos y luego de finalizada enviar una trama ADDTS 802.11e al AP modificando los recursos solicitados.

Es importante entender que utilizando el protocolo de reserva FT de 6 mensajes, los recursos han sido reservados en el cuarto mensaje, pero esto no significa que la estación deba completar el traspaso inmediatamente, sin embargo este intervalo está limitado por una cantidad de tiempo especificada por el AP en el cuarto mensaje. El AP dispone esta limitación para prevenir la situación en que una STA reserve los recursos mucho antes de requerir el traspaso.

Existe un procedimiento opcional en 802.11r donde la STA puede consultar la disponibilidad de recursos sin de hecho reservarlos. Esta consulta de recursos utiliza un tipo de solicitud conocido como Resource Information Container (RIC) similar al utilizado para la reserva de recursos, pero ningún recurso es reservado en este caso. Esta opción es muy útil para un STA que tiene que decidir entre varios AP candidatos.

El estándar 802.11r permite que la STA ejecute el proceso de reserva de recursos, sin llegar a re-asociarse, con varios APs al mismo tiempo. La STA solo puede asociarse con uno, por supuesto, como lo específica los requerimientos de las especificaciones básicas 802.11. Cualquier otra reserva, solicitada en los demás APs con los que la STA no se asoció, eventualmente expirara luego del límite de tiempo ya comentado.

3.5.7. Elementos Informativos en 802.11r

Hay 4 elementos informativos principales utilizados en 802.11r para cargar la información de roaming, seguridad, y QoS dentro de las tramas de administración 802.11 existentes. Estos son los siguientes:

• The Fast Transition Information Element (FTIE)

• The Mobility Domain Information Element (MDIE)

• The Robust Secure Networks Information Element (RSNIE)

• The RIC Data Information Element (RDIE) para reserva de recursos

Otro elemento de menor importancia que es utilizado para la transición rápida de BSS es el elemento informativo timeout (TIE).

El identificador de domino móvil (MDIE) identifica un grupo de APs dentro de una misma ESS que constituye un único dominio móvil que soporta la rápida transición de BSS. Cabe destacar que en general se asume que el dominio móvil (MD) comprende el grupo completo de APs dentro de una ESS. El MDIE está presente en muchas tramas relacionadas con 802.11r que fluyen entre la STA y el AP. El rol del MDIE es describir las capacidades de un MD al que un determinado AP, con el que la STA pretende asociarse, pretense. Sin importar en qué tipo de trama aparezca el MDIE, debería tener el mismo valor publicado por el AP en sus tramas balizas y/o tramas prueba-respuesta, y normalmente su valor será igual para todos los APs dentro del mismo MD.

El elemento MDIE contiene el identificador de dominio móvil, y los valores relacionados con las capacidades de rápida transición de BSS y políticas de reserva de recursos. El último valor incluido son cuatro bits; que describen el soporte de las cuatro funciones básicas: capacidad de rápida transición de BSS, reserva a través del aire, reserva a través del DS, y las opciones de reserva QoS. El bit de rápida transición de BSS será 1 dentro de un MD que soporta dicha función (en una red 802.11r siempre será 1). Los próximos dos bits indica si la reserva de recursos es realizada por uno de esos medios (aire o DS), si los dos bits son 0 significa que no hay opción de reserva de recursos. Cuando el último bit es 1, la STA debe primero realizar una reserva de recursos QoS previamente a la re asociación. Esta configuración indica que debe realizarse el proceso de reserva completo (el intercambio de 6 tramas) si se quiere realizar un reserva de recursos. Si este último bit es 0, la STA tiene la opción de realizar la reserva utilizando el intercambio de 4 tramas.

El FTIE contiene campos que permiten que el intercambio de cuatro vías 802.11i (intercambio de EAPOL Key) sea incluido en las tramas multipropósito de autenticación y re-asociación. El FTIE también aparece en un número de diferentes mensajes definidos por 802.11r. Es un elemento de longitud variable y puede contener diferentes fragmentos de información en varias etapas del intercambio. El FTIE publicada en un trama baliza presenta

su forma más simple, y solo contiene el valor de recursos de transición de BSS. En general, mientras más cercano a la finalización de la rápida transición de BSS el FTIE sea publicado, más información contendrá. Esta información incluye los campos MIC relacionado con la seguridad, ANonce, y SNonce. El FTIE también puede incluir la identidad del portador de clave PMK-R0. Dependiendo de la etapa del intercambio, el FTIE puede incluir el ID del portador de la clave PMK-R1 y GTK. Como MIC, ANonce y SNonce, el GTK es un concepto relacionado con 802.11i que ahora encuentran un nuevo medio de transporte, el FTIE.

Las tramas balizas y prueba/respuesta no son partes del proceso de transición rápida de BSS descripto en 802.11r, pero cumplen el importante rol de comunicar las capacidades de transición rápida de BSS del MD al que un AP pertenece. Bajo el estándar 802.11r, estas tramas incluirán ambos elementos MDIE y FTIE.

El elemento RSNIE es heredado de 802.11i y fue reutilizado en una nueva rama por 802.11r para lograr una transición rápida de BSS. Su propuesta original era publicar las capacidades de seguridad de un AP y una STA entre ellos, durante el proceso de asociación. Si el nivel de seguridad era aceptable para ambas partes, seguidamente se iniciaba el intercambio relacionado con la autenticación. Similar a OKC, en 802.11i, el estándar 802.11r se vale del campo PMKID para comunicar al AP la clave que la STA quiere utilizar para la nueva asociación. El estándar 802.11r mejora el OKC por medio de la carga del intercambio de claves de cuatro vías, aun requerido por OKC, dentro de las tramas multipropósitos de autenticación-abierta y asociación, y así reducir las tramas requeridas en el proceso de roaming.

El elemento TIE es utilizado para comunicar varios intervalos de tiempo relacionados con la rápida transición de BSS. Actualmente hay dos tipos de intervalos de tiempo definidos por TIE. Estos son: el intervalo de tiempo límite de re-asociación (Reassociation Deadline Interval) y el intervalo de tiempo de vida de clave (Key Lifetime Interval). El TIE es utilizado solamente en el tercer mensaje del proceso de asociación inicial. El tiempo límite de re-asociación representa el tiempo máximo permitido que una STA puede esperar para re-asociarse luego de recibir el mensaje de autenticación ASK (el cuarto mensaje). Cuando este tiempo expira, la STA debe abandonar el intento de transición. El intervalo de tiempo de vida de clave especifica el máximo tiempo de uso de las claves PTKs utilizadas durante el proceso de transición dentro de un MD.

Los requerimientos de reserva de recursos están agrupados en una RIC que consiste en un o más elementos informativos (RDIE), donde cada RDIE corresponde a una solicitud de recursos particular. Cada solicitud de recursos consiste en un RDIE seguido de una o más descripciones de recursos correspondientes al pedido. A pesar de que puede haber múltiples características descriptas por cada recurso, solo un recurso es reservado por cada RDIE. El RDIE permite el análisis de los recursos requeridos incluyéndolos en un campo de longitud variable. A continuación se muestra el proceso de creación de los RDIE utilizadas para la solicitud de recursos.

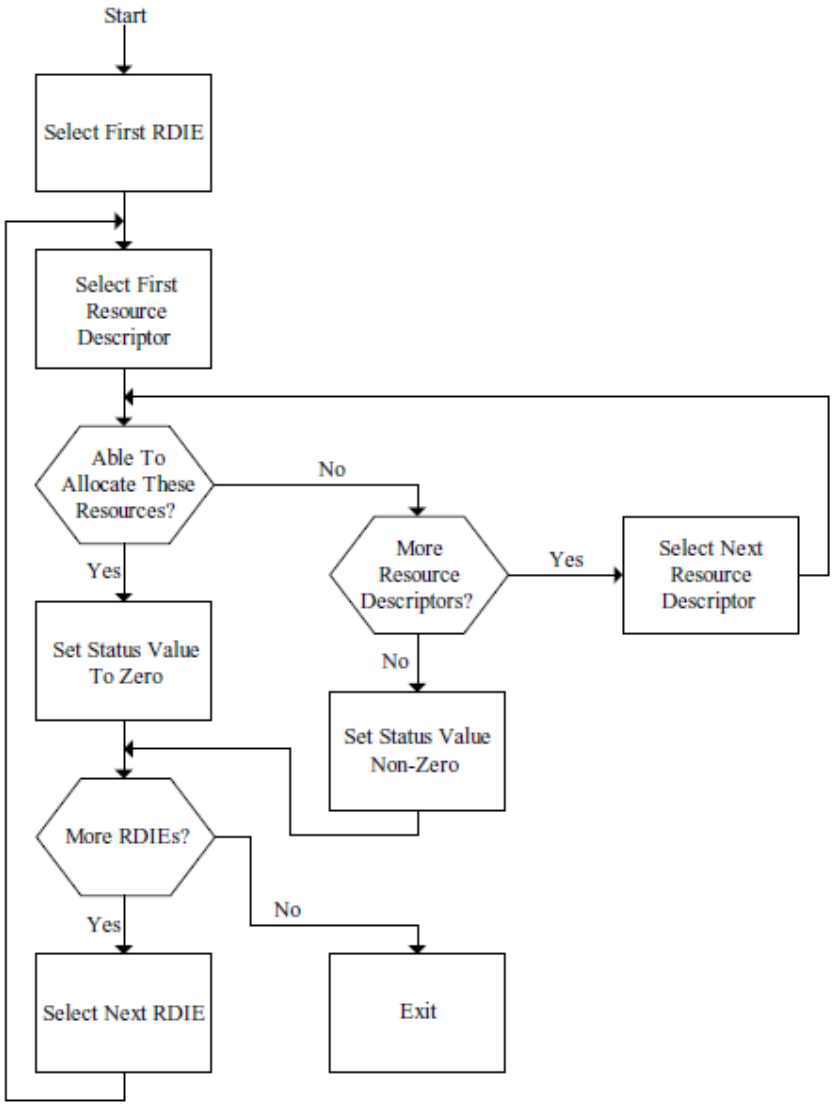


Figura 3.5.7: Procesamiento de contenedores de información de recursos.

El RDIE también incluye un bit de estado, que se utiliza en la respuesta del requerimiento. El valor de este bit indica si el pedido fue aceptado o no.

La descripción de recursos en 802.11r corresponde a las normas de 802.11e. Específicamente, un descriptor de recurso consiste en un elemento TSPEC y opcionalmente un TCLASS que son utilizados en una solicitud ADDTS en 802.11e. El estándar 802.11r ha alineado intencionalmente el formato de los descriptores de recursos con los encontrados en 802.11e para lograr consistencia. Estos contenedores de información de recursos son intercambiados en un par de tramas solicitud/respuesta conocido como solicitud RIC y respuesta RIC. La solicitud y respuesta comparten el mismo formato. Dentro del contexto en que una STA está solicitando que los recursos sean reservados por el AP dentro de una BSS. Cuando la solicitud RIC es transmitida, la STA solicita que los recursos representados por todos los contenedores sean otorgados. La respuesta RIC será enviada por el AP a la STA en el mismo formato que la solicitud, con el BIT de estado en cada RDIE indicando si este recurso puede ser garantizado o no.

4. Intercambio de protocolos en 802.11r (casos de estudio)

4.1. Introducción

En esta sección se presentaran 8 diagramas de protocolo que muestran las formas básicas en que el intercambio de tramas sucede en 802.11r. Como se mencionó en la sección 3.5.3 puede haber un número de diferentes posibilidades en la etapa previa al traspaso en 802.11r. En los ejemplos que se presentan en esta sección, consideramos ambos casos OTA y ODS. El protocolo de rápida transición de BSS es siempre igual sin importar el tiempo de autenticación utilizado (PSK o el 802.1x completo).En el caso de los ejemplos con reserva de recursos, se utiliza el protocolo de reserva FT completo para resaltar la diferencia entre el intercambio de 6-mensajes y el simple de 4-mesajes. Suponemos que en todos los casos que la asociación inicial en el MD ya ha ocurrido.

Es importante entender que la autenticación abierta 802.11 cumple un roll fundamental en cuanto a como 802.11r reduce el conteo de tramas durante el traspaso. El estándar 802.11r también explota el hecho de que a pesar que una STA pueda pertenecer a una sola BSS a la

vez, 802.11 permite el intercambio de tramas de autenticación con otras BSS sin tener que terminar la asociación con el actual AP. Mediante el enriquecimiento del tipo de información que la trama de autenticación puede transportar, 802.11r permite acordar la seguridad y reserva de QoS antes del traspaso.

Una vez que la STA 802.11r inicia el proceso de roaming, el estándar especifica que la STA debe agregar la información referente a la seguridad y QoS dentro del intercambio básico de 4-tramas que siempre ocurre en estos casos, el conocido intercambio solicitud/respuesta de autenticación y el intercambio solicitud/respuesta de re-asociación. Un ejemplo claro de mejora en la eficiencia es el caso ya mencionado de pre-autenticación en 802.11i, en donde se requiere las 4-tramas de asociación seguidas de las 4-tramas de intercambio de claves EAPOL, en este caso se reduce un intercambio de 8-tramas en solo 4-tramas. El estándar 802.11r ofrece un vasto grupo de alternativas para soportar transiciones rápidas de BSS con seguridad y reserva de QoS.

4.2. Transición rápida de BSS OTA, sin QoS, sin Seguridad

En esta sección se expone el intercambio más básico para una rápida transición de BSS OTA. Como se ve en la figura 4.1 la STA ya ha identificado el AP destino antes de trasmitir la trama de autenticación abierta inicial. La primera trama de autenticación contiene 2 campos particularmente relevantes, estos son los atributos FT y MDIE. FT indica que el algoritmo de autenticación utilizado es el correspondiente al de rápida transición de BSS. MDIE indica que esta trama de autenticación incluye el elemento informativo MDIE ya mencionado. Este elemento debe ser idéntico a los MDIE que fueron publicados por el AP dentro de las tramas balizas o tramas prueba/respuesta. Las siguientes 3 tramas fluyen normalmente como seria en una red sin 802.11r, con una trama de respuesta de autenticación seguida por el par de tramas re-asociación solicitud/respuesta. La respuesta de autenticación transporta el mismo mensaje FT y MDIE que la trama solicitud. El par de tramas re-asociación también transportan el mismo MDIE.

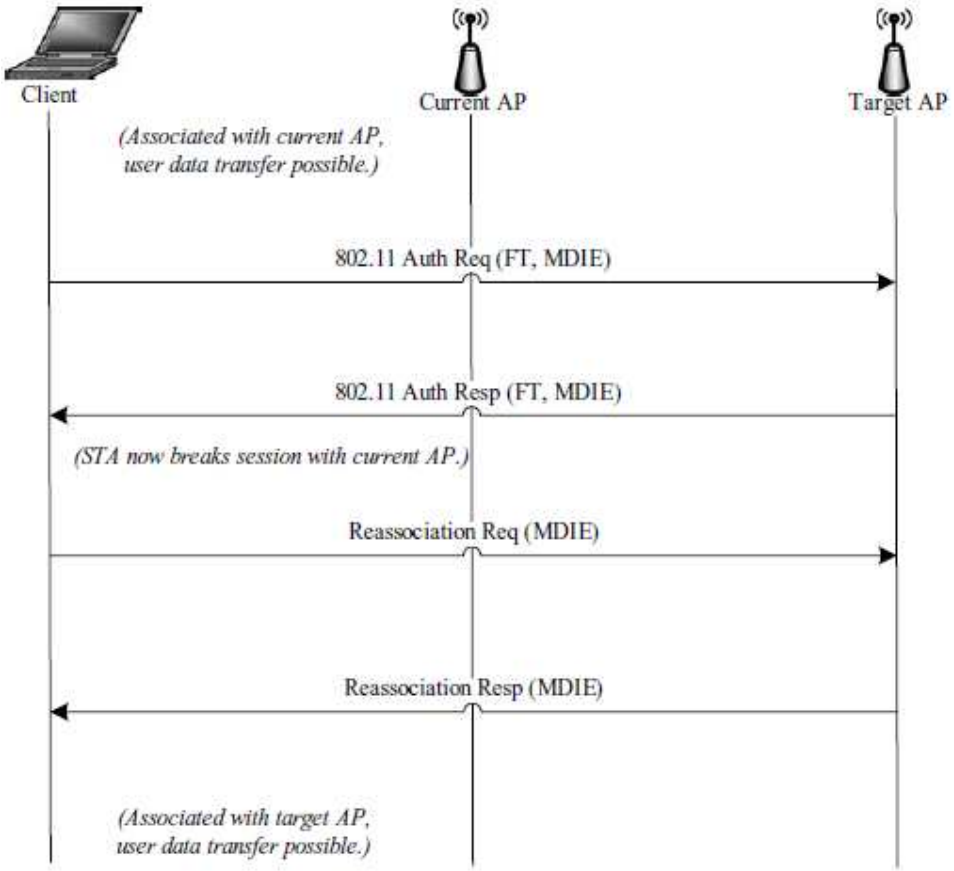


Figura 4.1: Fast roaming OTA sin QoS, sin Seguridad

Se puede notar que en el caso de una transición 802.11r que no involucre QoS o seguridad, no hay una diferencia sustancial con respecto a 802.11. Ya que el moverse a otro AP también involucra un intercambio de 4-tramas, como sería en 802.11r. Esto evidencia que 802.11r es un estándar que ayuda a mejorar la seguridad y reserva de QoS dentro del proceso traspaso. Tanto los protocolos de seguridad como de QoS agregan una cantidad significativa de mensajes requeridos durante el proceso de roaming, así que si ninguno de estos protocolos es parte de la transición, hay muy pocos beneficios obtenidos por el uso del estándar 802.11r.

4.3. Transición rápida de BSS ODS, sin QoS, sin Seguridad.

La figura 4.2 nos muestra el intercambio más básico en transiciones rápidas de BSS ODS. Un concepto fundamental de esta sección es que a pesar de si la transición rápida de BSS es realizada en OTA o ODS, cierta porción clave de información debe ser comunicada para que

el proceso 802.11r tenga lugar. Algunas veces, esta información esta implícitamente comunicada como resultado del protocolo en uso, y otras veces necesita ser comunicada explícitamente dentro de la carga de tramas durante el intercambio. Las 2 primeras tramas en la figura 4.2 son un claro ejemplo de esto.

La diferencia básica que vemos en ODS en relación con OTA es que la información referente a la transición rápida de BSS, que en OTA es trasmitida dentro de las tramas de autenticación abierta, en ODS se comunica por medio de tramas FT action-request. Claramente, todas las comunicaciones en 802.11 se realizan a través del aire (OTE), pero en el caso de tramas FT action-request, la STA trasmite estas tramas a través del aire al AP al que está actualmente asociado que no es el verdadero AP destino. Luego el AP, con el que la STA se encuentra asociado, hace uso de la DS para entregar esta información al AP destino, para lo cual debe conocer su identidad previamente.

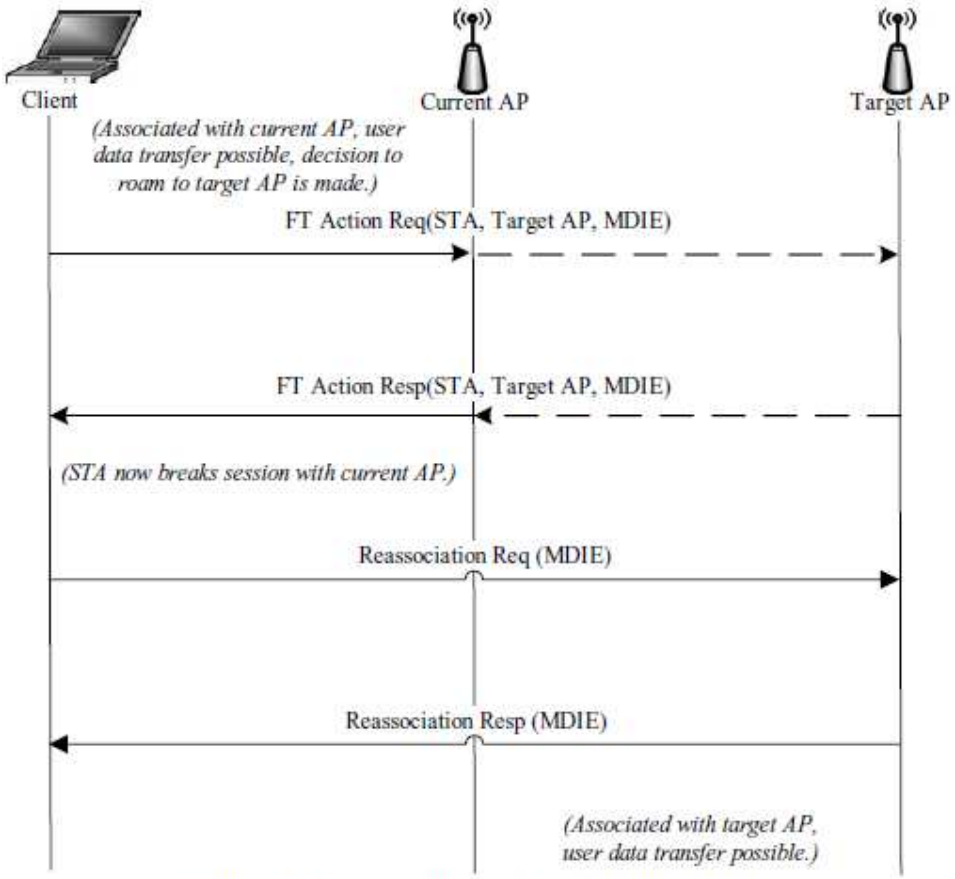


Figura 4.2: Fast roaming ODS sin QoS, sin Seguridad

En el caso de OTA, el AP destino es alcanzado directamente por medio de una trasmisión 802.11 con la dirección destino configurada con el BSSID destino, en cambio en el caso ODS, la dirección del AP destino es comunicada explícitamente dentro de la carga de la primer trama FT action-request.

Esta información será luego utilizada por el AP actual para transportar el mensaje al AP destino. La línea punteada en la figura denota la porción del camino en donde se utiliza el DS como medio (usualmente la red cableada 802.3). Luego el par re-asociación solicitud/respuesta es exactamente igual que en OTA.

4.4. Transición rápida de BSS sin QoS con Seguridad.

La figura 4.3 ilustra los pasos adicionales en los que el protocolo incurre cuando se agrega una seguridad más robusta en el caso OTA.

Notamos que el intercambio de autenticación que se exige aquí ahora contiene 2 elementos informativos nuevos FTIE y RSNIE. El FTIE es utilizado para transportar el ANonce desde la STA al AP y devolver el SNonce del AP a la STA. Este es el proceso de carga de los elementos de seguridad, transportados en el intercambio de 4-vias en 802.11i, dentro del intercambio de autenticación y asociación en 802.11r. Como sucede en el intercambio de claves de 4-vias, vemos que los elementos ANonce y SNonce fueron intercambiados dentro de las 2 primeras tramas.

El elemento RSNIE contiene información referente a la preferencia de seguridad y capacidades del lado trasmisor. A medida que nos movemos hacia la tercer y cuarta trama, vemos que FTIE y RSNIE son utilizados para transportar información que antes eran transportadas en el tercer y cuarto mensaje del intercambio de claves de 4-vias EAPOL. Adicionalmente a ANonce y SNonce, el FTIE contiene el mensaje de chequeo de integridad. El RSNIE incluye el PMKR1Name. La respuesta del AP incluye la misma información y el GTK, comprimiendo toda la información de calves grupales 802.11i dentro del intercambio básico de 4 tramas.

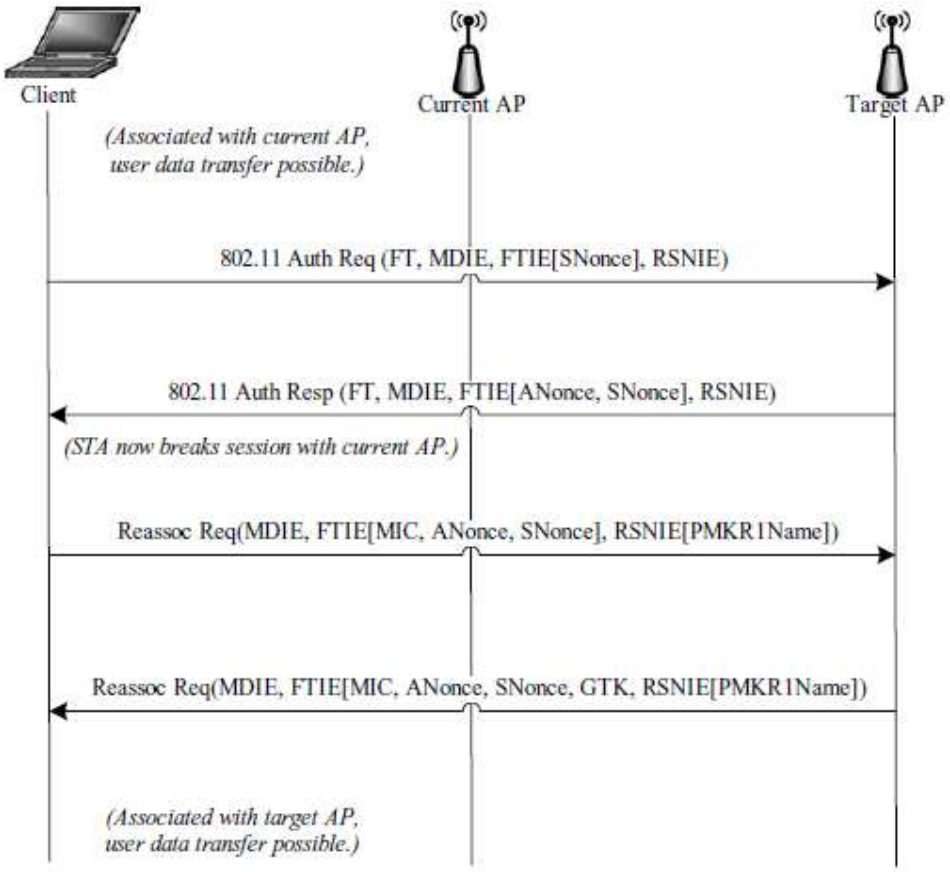


Figura 4.3: Fast roaming OTA sin QoS, con Seguridad.

En la figura 4.4 se ilustra la misma situación pero para el caso ODS. La forma más sencilla de explicar este intercambio es ver sus diferencias con el anterior. La seguridad de la asociación resultante luego del intercambio es igual para ambos casos, la única diferencia es que en el primer caso la primera mitad del intercambio es realizado directamente contra el AP destino a través de tramas de autenticación abierta por el aire (OTA), y en este último es realizado indirectamente por el DS a través del AP al que la STA se encuentra asociada. Por este motivo, las tramas intercambiadas durante la fase de asociación son iguales para ambos casos. La única diferencia que vemos en este caso es que la información de seguridad correspondiente a las 2 primeras tramas del intercambio de claves de 4-visa de 802.11i son transportadas dentro de las tramas FT action-request y FT action-response.

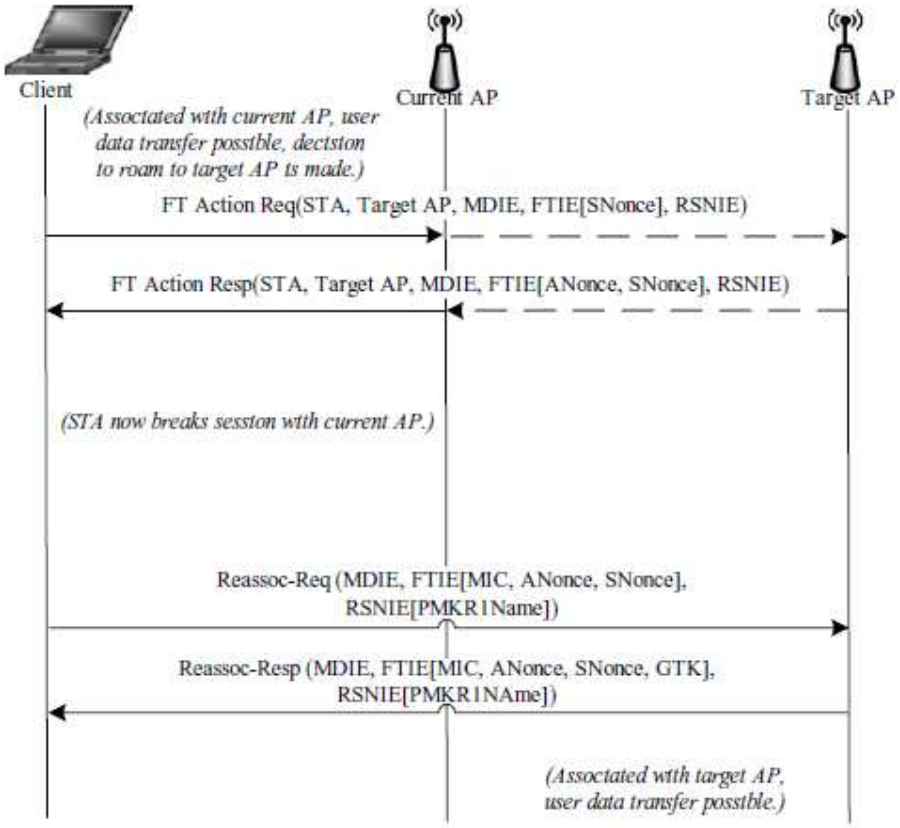


Figura 4.4: Fast roaming ODS sin QoS, con Seguridad.

Las próximas graficas muestran el intercambio 802.11r incorporando la reserva de QoS. Estas graficas (4.5-4.8) fueron construidas a partir de las gráficas sin QoS que las presiden (4.1-4.4) correspondientemente. Una rápida comparación muestra que la figura 4.5 extiende la figura 4.1 agregando 2 nuevas tramas de autenticación seguidas del par inicial de solicitud/respuesta. Esta tercera y cuarta trama son las nuevas tramas ACK de autenticación y confirmación de autenticación creada para el estándar 802.11r. Ellas transportan la solicitud RIC y la respuesta RIC que se utilizan para negociar una serie de recursos, antes de que el proceso de roaming tenga lugar.

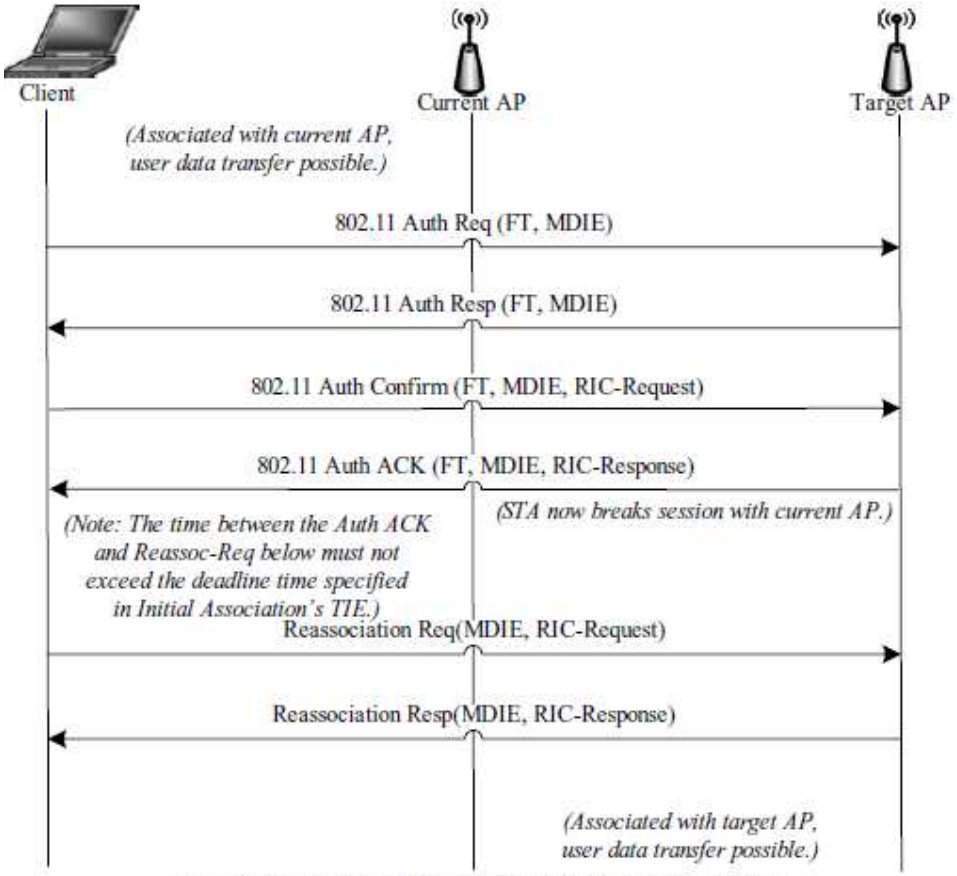


Figura 4.5: Fast roaming OTA con QoS, sin Seguridad.

El hecho de que los mensajes solicitud RIC y respuesta RIC son diferidos en la tercer y cuarta trama del intercambio resulta en que la asociación de seguridad entre el AP destino y la STA esté suficientemente establecida para permitir la protección de los mensajes solicitud RIC y respuesta RIC por medio de la confirmación de integridad. Mientras que este punto es irrelevante en el caso de una implementación sin seguridad, el intercambio RIC sigue siendo diferido al tercer y cuarto mensaje por consistencia.

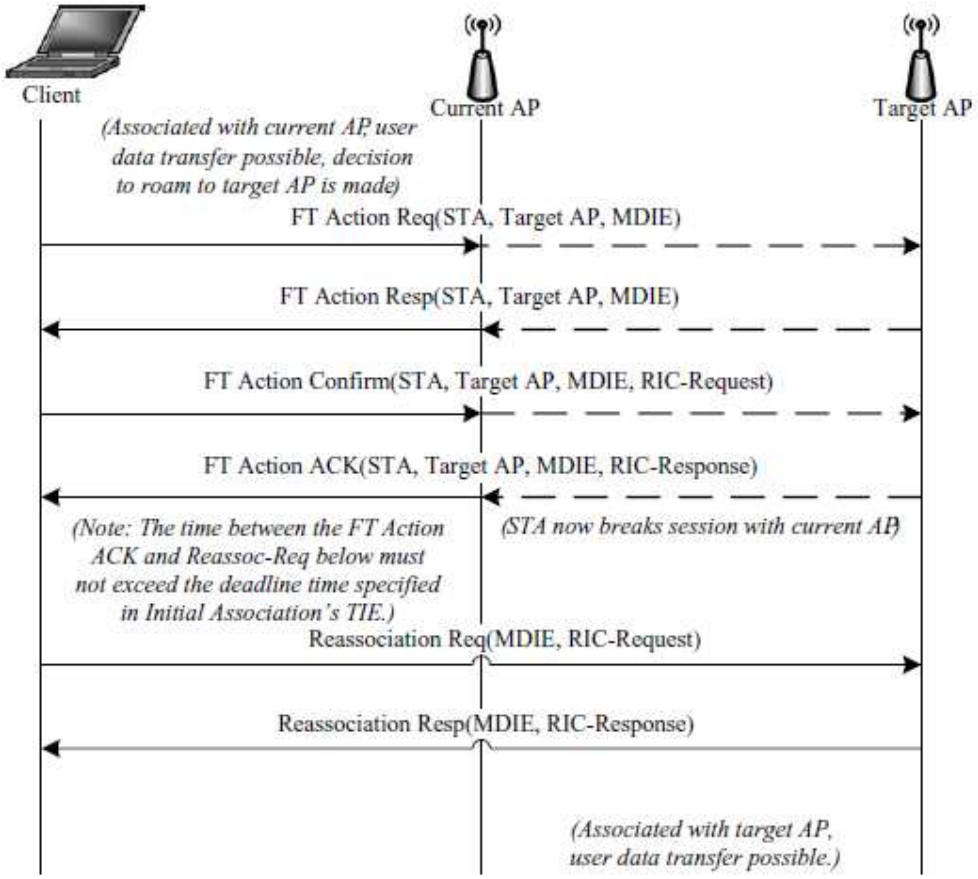


Figura 4.6: Fast roaming ODS con QoS, sin Seguridad.

La figura 4.6 muestra los mismos elementos informativos, transportados en las tramas de autenticación de la figura 4.5, pero en la figura 4.6 son transportados en las correspondientes tramas FT-action. Ya sea a través de los modos OTA u ODS, ambos intercambios confirman que los recursos solicitados son reservados ante de la re-asociación. En ambos casos, el traspaso es realizado en el intercambio de las 2 tramas finales, donde la solicitud y respuesta exitosa de re-asociación señala la finalización de re-asociación con el AP destino.

La figura 4.7 evoluciona de la figura 4.5, agregando seguridad al modo OTA con QoS. La figura 4.8 hace lo mismo para el modo ODS con QoS.

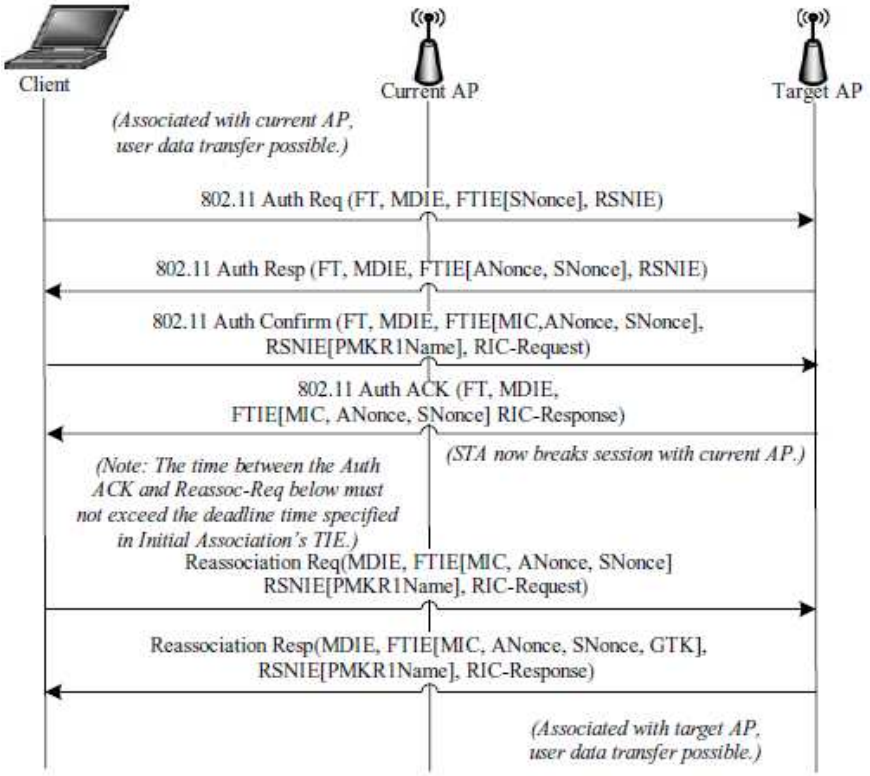


Figura 4.7: Fast roaming OTA con QoS, con Seguridad.

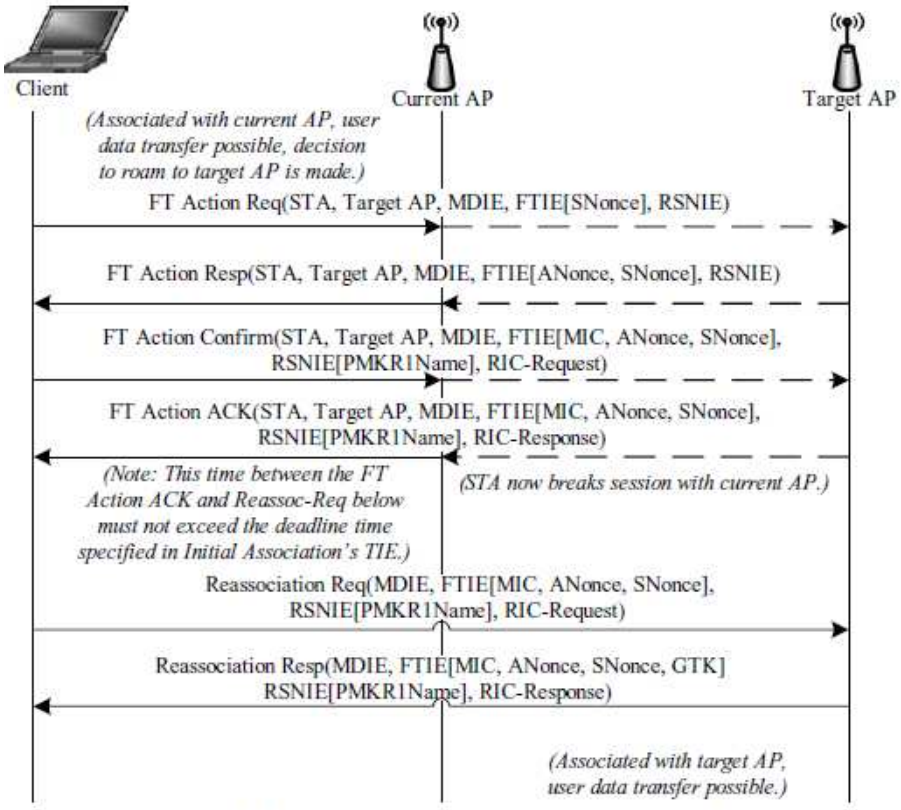


Figura 4.8: Fast roaming ODS con QoS, con Seguridad.

5. Implementación de una red 802.11r en un entorno de laboratorio

5.1. Introducción

En este capítulo se intentara probar el funcionamiento y el potencial de una red WiFi 802.11r en diferentes escenarios por medio del montando de una red 802.11r de laboratorio. Se buscara familiarizar al lector con la norma y su empleo en la práctica a partir de las experiencias adquiridas por el autor durante el experimento. Se presentaran los equipos utilizados y el porqué de su selección, se listaran sus características, precios, posibles proveedores, etc. Se pondrá a disposición del lector el conexionado de los mismos como así también su configuración en los diferentes escenarios plateados. Una vez lograda la red 802.11r deseada se procederá a ponerla a prueba, se presentaran las variables a medir (principalmente el tiempo de roaming) como así también las herramientas de captura y métodos de medición. Llegando al final del capítulo se presentaran las capturas obtenidas y las mediciones logradas en los diferentes escenarios. Por último encontramos una conclusión sobre los valores obtenidos y una reflexión por parte del autor.

5.2. Casos de estudio

A continuación se planteara un escenario de laboratorio destinado a realizar mediciones y capturas de tramas 802.11 durante la operación de equipos inalámbricos que se encuentre traspasando el límite del rango de cobertura de un AP (AP1) y entrando en el rango de cobertura de otro AP (AP2). Se buscara medir con precisión el tiempo de renegociación con el segundo AP utilizando diferentes protocolos de roaming y de seguridad. A partir de los resultados obtenidos se concluirá si el tiempo que lleva la renegociación puede o no generar inconvenientes en aplicaciones críticas sensibles a cortes breves en la conexión.

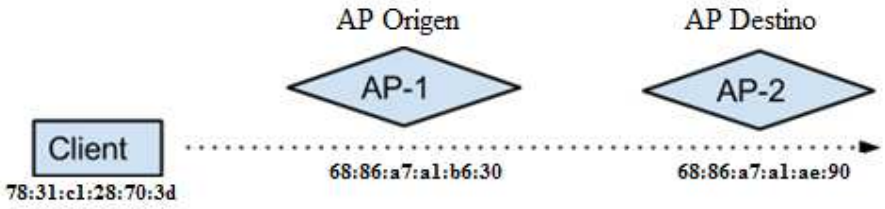


Figura 5.2.1 Caso de estudio, STA pasando del AP1 al AP2

El experimento busca constatar cuan más rápido sucede la re asociación en un entorno 802.11 con autenticación WPA2, cuando se aplica la extensión de la norma 802.11r. Se plantearan 3 escenarios durante los cuales se realizaran las pruebas:

- Sin aplicar la norma 802.11r, se medirá el tiempo entre la primera trama de autenticación 802.11 dirigida al AP2 y el mensaje de intercambio de claves final (EAPOL Key 4).
- Aplicando la norma 802.11r por aire (directamente entre los APs y las STA), para este escenario se analizara el tiempo transcurrido desde la primera trama de autenticación 802.11 dirigida al AP2 hasta la trama final de respuesta de re asociación proveniente del AP2.
- Aplicando la norma 802.11r a través de un DS (las operaciones 802.11r son controladas desde la red cableada), para este escenario se medirá el tiempo entre la primera trama Acción (Pedido de Acción de un FT al AP1) y la trama final de respuesta de re asociación del AP2

Mi meta aquí es eliminar las variaciones introducidas por los protocolos de capas superiores, por tal motivo no estoy midiendo tramas de datos, por ejemplo pings desechados, CoWIFI, iperf etc.

5.3. Topología

Se utilizara una topología de WLAN estructure (explicada en el capítulo 3.2) que contara con dos BSS interconectadas por medio de un DS constituido por una controladora y una red cableada Ethernet 802.3. Estas BSS serán dispuesta y configuradas de tal manera que ambas formen parte de la misma ESS. Por motivos de simplicidad del proyecto se optó por una estructura tipo light-weight APs (LWAPP) donde los APs son controlados de manera centralizada a través de una controladora que realiza la mayor parte de la inteligencia de red y proporciona los servicios tanto de DS con de SS. Las ventajas son:

- Utilizar Punto de acceso lo más sencillos y baratos posibles. Se le quita todo el trabajo posible.
- Centralizar el trabajo de filtrado, QoS, autenticación y cifrado en un dispositivo centralizado.

- Proporcionar un mecanismo de encapsulación y transporte independiente del vendedor.

5.3.1. Lista de equipos

La selección de equipos fue uno de los desafíos más grandes del proyectos, debido a que la tecnología es nueva y no ha sido ratificada aun, los equipos que soportan la norma IEEE 802.11r no abundan en lo absoluto, y los equipos que si lo soportan son equipos de última generación de proveedores importantes, por lo que no resultan nada económicos y en el caso de la argentina son muy difícil de conseguir.

Luego de una ardua búsqueda en la web (Foros, Publicaciones, noticias, etc.), consulta a proveedores, prestadores de servicios, e inclusive a fabricantes se llegó a lo no muy alentadora conclusión de que unos de los pocos fabricantes que soportan esta norma son Cisco por el lado de los equipos de red (APs, network controller, etc.) y Apple por el lado de los equipos para los usuarios (STA). A pesar de que estos fabricantes son muy conocidos por la excelente calidad de sus productos, también son conocidos por su elevado costo y actualmente son muy difícil de conseguir en la Argentina.

Sin embargo gracias a un gran esfuerzo de logística se logró conseguir los siguientes equipos para llevar a cabo las pruebas previamente descriptas:

- 2 APs Cisco Aironet 3502i. (3000 A$R cada uno).
- 1 WNC Cisco 2504 Wireless Controller (6000 A$R)
- 1 Apple IPhone 5s (utilizado como STA cliente).
- Cable UTP categoría 5 para el conexionado de los APs y el Switch. (15 A$R/m).

Cabe destacar que dentro de la familia Cisco Aironet se podría haber elegido cualquiera de los Cisco APs que soporten el IOS 5.2(2)JB (Ejemplo: Cisco Aironets 802, 1260, 1040, 1140, 3500i, 3500e, 3600i, 3600e, 2600i, 2600e, 1600i, 1600e, 1550) se optó por el 3502i porque dentro de las opciones que se podían conseguir en nuestro mercado, este es un equipo muy completo que no solo soporta 802.11r sino que también la norma 802.11n que nos permite alcanzar velocidades de hasta 320Mbps. Esta velocidad casi nos permite independizarnos de la taza de trasmisión a la hora del diseño de una red que soporte VoIP ya que cada llamada requiere como mucho 64Kbps.

Debido a que 802.11r no especifica las características del DS, es irrelevante el tipo de cableado o Switch a utilizar. Se optó por la controladora Cisco 2504 para tener homogeneidad en la red y de esta manera simplificar su construcción.

Dentro del mundo Apple las STA que soportan la norma 802.11r comprende: Todos los Iphone a partir del 4s, los IPad a partir de la 3ra generación y los Iphod tuch de cuarta generación en adelante. Como regla general cualquier dispositivo Apple que soporte su versión de IOS 6 en adelante soporta fast roaming 802.11r. En este caso se utilizara un Iphone 5s, pero cualquiera de los otros equipos listados hubiera sido una opción válida.

5.3.2 Conexionado

El conexionado en el que se incurrió para crear el DS es muy básico, simplemente se dispusieron ambos APs a una distancia suficiente para crear una ESS en donde se pueda dar la situación en que se requiera del proceso de traspaso, aproximadamente unos 20 metros. Nota en la práctica se pueden lograr mayores distancias según su ubicación y configurado. Luego se extiendo un cable Ethernet categoría 5 desde los APs a los puertos Giga0/3 y Giga0/4 de la controladora ya que estos puertos poseen PoE (norma IEEE 802.3af). El único dispositivo que requiere alimentación es la controladora lo que facilito la elección de ubicación de los APs. En la Figura 5.3.1 se muestran los 2 APs y la PC con la que se llevó a cabo las configuraciones y oficio de servidor de autenticación conectados a la controladora y entre medio la PC MAC que se utilizó para las capturas.

Figura 5.3.1 Foto Explicativa del conexionado

El STA cliente (el Iphone 5s) se dispondrá dentro del área de cobertura del AP1 inicialmente, para luego acercarse al área de cobertura del Ap2. Se dispondrá una PC con la placa de red en modo promiscuo entre los APs para captar todas las tramas de negociación entre la STA y los dos APs.

Cabe aclarar que para que la prueba se alejaron los APs, de tal manera que se del traspaso de uno al otro.

5.3.3 Configuración y puesta a punto

Una vez obtenidos los equipos el primer paso fue asegurarse que la versión del IOS de dichos equipos soporten las funciones requeridas para crear el tipo de red WiFi deseada, específicamente si las versiones de los sistemas operativos soportaban la norma 802.11r Fast roaming.

Se comenzó con la controladora para la cual se averiguo, una vez incurrido en los primeros pasos para su puesta en marcha (Ver configuración inicial en bibliografía) donde simplemente se configura un perfil de administrador y una IP de acceso, se llegó al menú principal web, donde por fortuna se confirmó que la versión del IOS soportaba las funcionalidades requeridas. Se conocía con anterioridad que la opción de transición rápida fue agregada a partir de la versión 7.6.100 en la controladora. Esta información se encontró a través de la página de Cisco, esta página se encuentra en la bibliografía.

Figura 5.3.2 Menú principal de la controladora

Seguido a esto se antes de conectarlo a la controladora se revisó el IOS de los APs por medio del puerto consola en este caso el IOS era una versión que no soportaba las transiciones rápidas. Se utilizó la página de Cisco para descargar la última versión de IOS

(ap3g1_rcvk9w8_tar.153_3.JA3) y se utilizó el procedimiento encontrado en el Apéndice A para cargarlo a los APs.

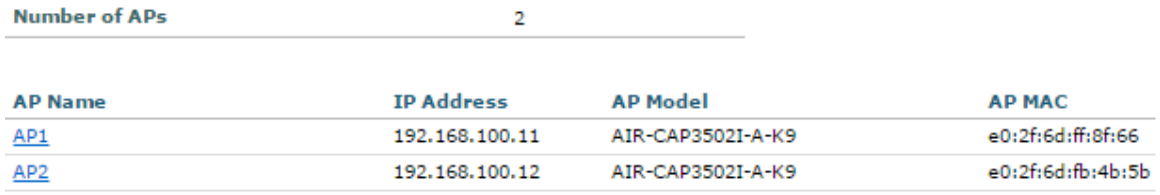
Luego de contar con la certeza que se tenía los equipos y versiones de software adecuados se procedió a la asociación de los APs a la controladora. Para la primera asociación los APs requieren de un servidor DHCP que asigne una IP dentro del rango en que fue configurada la red de administración de la controladora para que la asociación pueda llevarse a cabo, para evitar la necesidad de configurar un servidor DHCP se le asignó una IP estática a cada AP por medio de un comando CLI introducido por consola:

AP#lwapp ap ip address <IP address> <subnet mask>

Se configure toda la red de administración en un rango 192.168.100.0/24.

- Controladora: 192.168.100.10
- AP1: 192.168.100.11
- AP2: 192.168.100.12

A partir de este punto el Cisco 2504 toma control de los APs y son agregados a su lista de equipos inalámbricos (Figura 5.3.3).



Number of APs	2		
AP Name	**IP Address**	**AP Model**	**AP MAC**
AP1	192.168.100.11	AIR-CAP3502I-A-K9	e0:2f:6d:ff:8f:66
AP2	192.168.100.12	AIR-CAP3502I-A-K9	e0:2f:6d:fb:4b:5b

Figura 5.3.3 Lista de APs incorporados a la controladora

A partir de este punto, toda red inalámbrica creada en la controladora es trasmitida por defecto por todos los APs dentro de su grupo Wireless. Las posibilidades y complejidad que se puede lograr con este tipo de equipos son muy altas de hecho este equipo soporta hasta 75 APs. Pero para lograr las mediciones requeridas por este documento se incurrió a una configuración estándar muy sencilla.

A continuación el paso a paso de la creación de la red WiFi (FastRoamingTest): creación

WLAN → Create New → GO

Figura 5.3.4 Creación de la red WiFi

SSID: FastRoamingTest → Apply

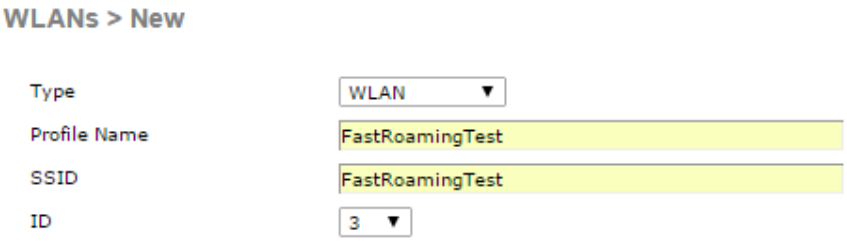


Figura 5.3.5 Configuración del SSID

La Red es creada con todas las opciones por defecto, a las cuales modificaremos las opciones referentes a la autenticación, asociación y re asociación.

Figura 5.3.6 Configuración de método de autenticación

Según la prueba se aplicó la configuración de rápida transición o no (Figura 5.3.6).

Y se seleccionó el tipo de autenticación 802.1x introducido por 802.11i para aumentar la seguridad y robustez de la red (ver capítulo 3.4.3). Se utilizó una PC con sistema operativo Linux y un servidor Radius gratuito conocido como FreeRadius para oficiar de entidad autenticadora, para más detalles ver Apéndice B.

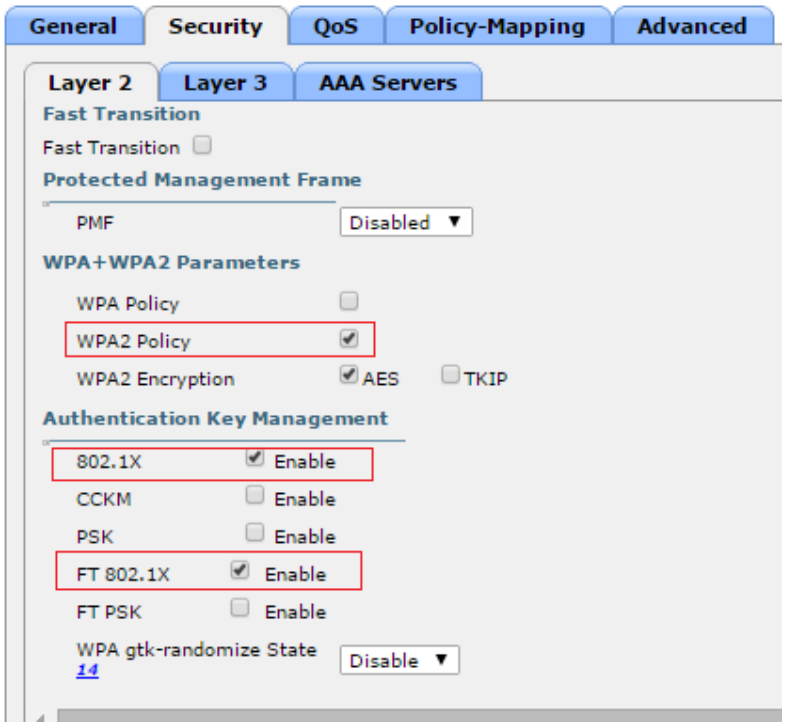


Figura 5.3.7 Configuración de método de autenticación

A nivel físico únicamente se configuro los canales en los que trabajan cada AP (Figura 5.3.8).

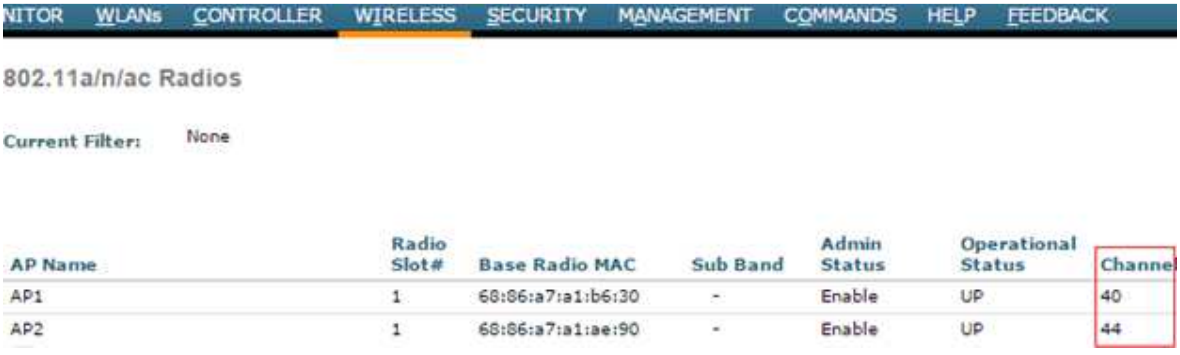


Figura 5.3.8 Canales Configurados

En este momento se contaba con una red ESS con las siguientes características:

Hostname	**AP1**	**AP2**
ESSID	FastRoamingTest	FastRoamingTest
Band	5Ghz	5Hhz
PW	8dBm	8dBm
Security	WPA2	WPA2
Channel	40	44
Key managment	802.1x	802.1x
802.11r	Según la prueba lo requiera	Según la prueba lo requiera

Figura 5.3.9 Parámetros configurados

- SSID: El SSID es el mismo así se logra crear una ESS.
- Band: Se optó por la banda de 5Hz principalmente porque es mucho menos usada en relación a la banda 2,4Ghz y así facilitar la lectura de las futuras capturas.
- PW: Se utilizó una configuración de Potencia moderada para no tener que disponer los APs tan lejos uno del otro y que de todas manera suceda el traspaso del equipo STA.
- Security: Como mecanismo de autenticación se utilizó WPA2 por su robustez y popularidad.
- Channel: Se utilizaron Canales adyacentes para facilitar la captura de ambos canales simultáneamente.
- Key Management: Como método de autenticación se utilizó la norma 802.1x para acceder a un servidor de Radius que simula el método de autenticación de usuario y contraseña muy habituales en un entorno de oficina.

- 802.11r: El Parámetro 802.11r se encuentra como uno de los parámetros a configurar dentro de los parámetros de la WLAN creada, y se habilito para la prueba con fast roaming. La Figura 5.7 muestra cómo se seleccionó la opción.

5.4. Método y herramientas de medición

Para la captura de tramas se utilizó una PC MAC con OSX Yosemite versión 10.10.2. Con el objetivo de obtener la medición más precisa posible durante prueba se configuro el programa capturado de tramas de OSX para capturar 40 Mhz con los AP configurados en canales adyacentes en la banda de 5Ghz de tal manera que contenga los 2 canales en uso. De esta manera se obtendrá solo una captura con todas las tramas de ambos APs. Desde la terminal (Figura 5.4.1):

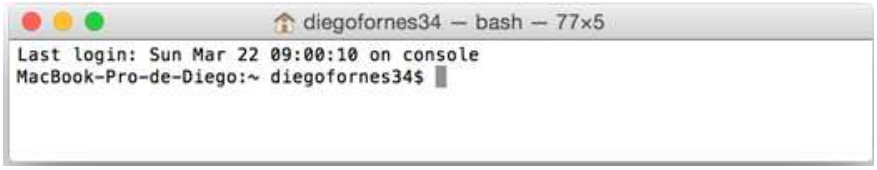


Figura 5.4.1 Terminal OSX

Se cargaron las siguientes librerías para tener las herramientas de sistema necesarias

/System/Library/PrivateFrameworks/Apple80211.framework/Versions/Current/Resources/airport

sudo ln -s /System/Library/PrivateFrameworks/Apple80211.framework/Versions/Current/Resources/airport /usr/bin/airport

Luego se utilizó el siguiente comando para ver todas las redes que se encuentran en rango y corroborar que los 2 APS se encuentren en la lista y con los canales correspondientes:

airport en0 scan

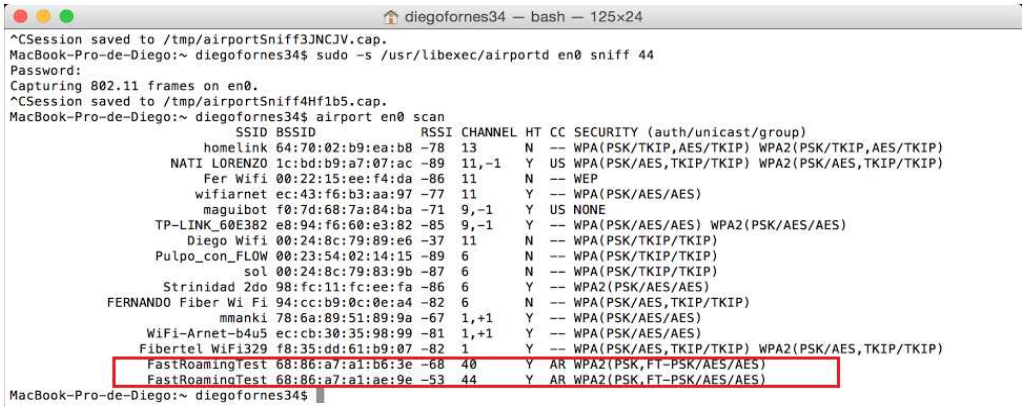


Figura 5.4.2 Escaneo del aire

Finalmente se utilizara el comando:

sudo -s /usr/libexec/airportd en0 sniff <Channel>

Para monitorear los canales deseados y de esta manera apreciar todo el proceso de re-asociación.

Una vez que se dé por terminado el periodo de monitoreo con Ctrl+C un archivo .cap será guardado en el disco con todas las tramas capturadas durante el periodo entre que se ejecutó el comando y se le dio fin con Ctrl+C.

Finalmente se utilizara el programa WireShark para abrir los archivos .cap, leer e interpretar las tramas capturadas.

5.5. Implementación

Durante este capítulo se presentarán las pruebas realizadas y sus características distintivas. Se explicara nuevamente de forma breve en que consiste la prueba y se exhibirán en forma de impresión de pantalla extractos de las capturas obtenidas y el método de análisis del material utilizando el software de análisis de tramas WireShark.

Para todas las pruebas se parte de tener la red funcionando con la configuración requerida para cada prueba, se dispuso la laptop espía entre los APS de tal manera de poder capturar las tramas correspondientes al traspaso de un AP al otro. Se inició la PC espía en modo de captura como se explicó en el capítulo anterior, finalmente con todo preparado se asocia la STA cliente (el Iphone 5s) con la ESS en las cercanías del AP1 para asegurarnos que en un comienzo la STA se encuentre asociada a dicho AP. Luego se prosiguió a alejar la STA del

AP1 en dirección al AP2 hasta lograr la re-asociación deseada con el mismo. Por último se guardaron las capturas y fueron analizadas utilizado el ya mencionado software Wireshark.

5.5.1. Prueba 1: Sin aplicar la norma 802.11r Sin Seguridad

Para esta prueba se configuro una ESS compuesta por dos APs en canales sin aplicar ningún mecanismo de autenticación y sin aplicar la norma 802.11r. Se consiguió la captura FastRoamingTest(No802.11r,NoSecurity).pcap.

Para poder encontrar el tiempo transcurrido entre ciertas tramas en Wireshark se localizó la primera trama, en este caso la trama de autenticación 802.11 hacia el AP-2, utilizando el filtro *wlan.fc.type_subtype==0x0b*

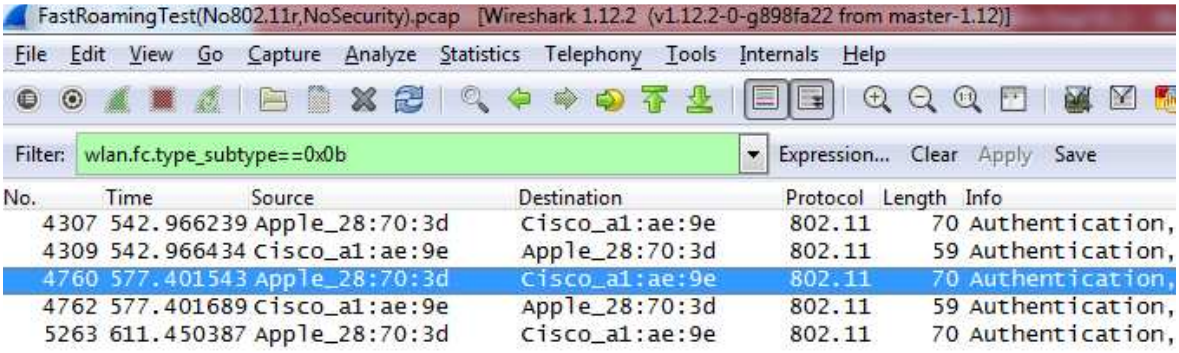


Figura 5.5.1 Trama de autenticación sin seguridad sin FastRoaming

Se la selecciona utilizando el click derecho del mouse y luego Edit-->Set/Unset Time Reference:

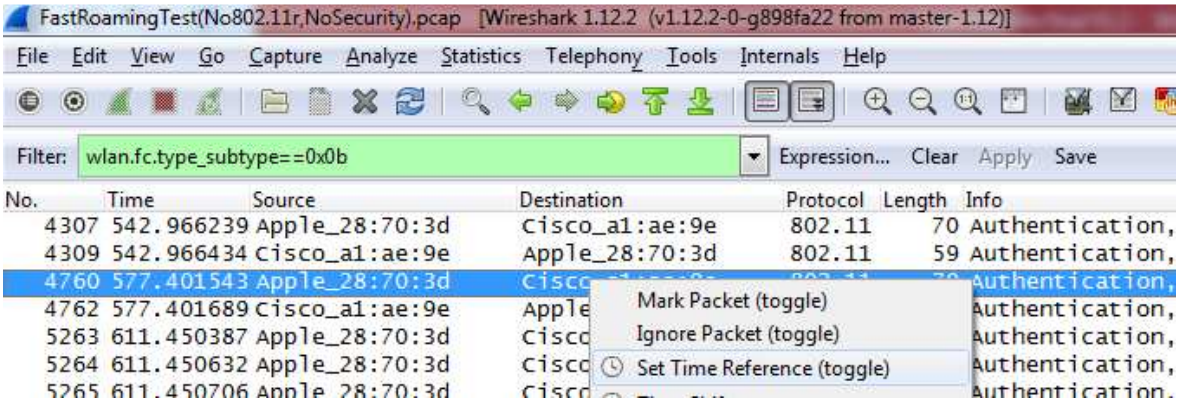


Figura 5.5.2 Configuración de trama de referencia

Se nota luego que el campo tiempo de referencia es cero.

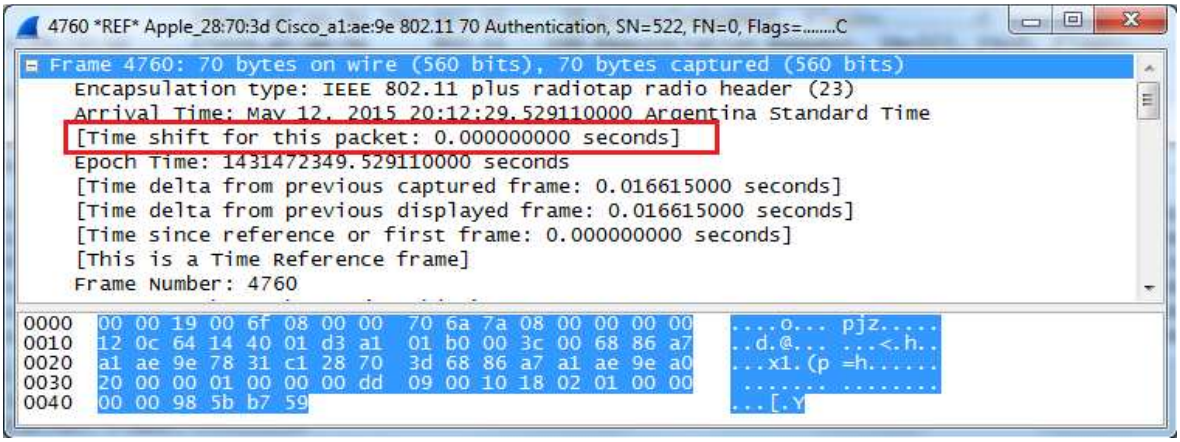


Figura 5.5.3 Tiempo de referencia cero

Luego se buscó la trama respuesta de re asociación (Reassociation Response) por parte el AP2 hacia la STA cliente y se tomó nota del tiempo transcurrido hasta su arribo:

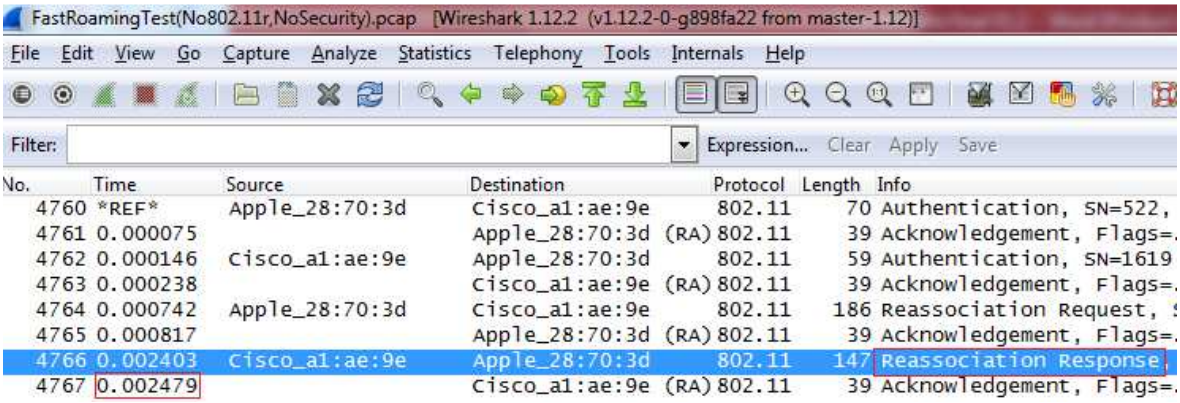


Figura 5.5.4 Trama respuesta de re asociación no seguridad no FastRoaming

Se tomó como tiempo de re asociación el tiempo de recepción de la trama ACK correspondiente al acuse de recibo de la trama respuesta de re asociación por parte de la STA cliente.

El resultado fue de un tiempo de re asociación de 2,479 ms.

5.5.2. Prueba 2: Sin aplicar la norma 802.11r con seguridad 802.1x

Para esta prueba se utilizó la misma ESS compuesta por dos APs en canales adyacentes, pero esta vez utilizando 802.1X WPA-2 como método de autenticación sin aplicar la norma 802.11r. Se consiguió Seguridad802.1xNoFastRoaming.pcap.

De la misma manera se localizó la primera trama de autenticación 802.11 hacia el AP-2, utilizando el filtro *wlan.fc.type_subtype==0x0b*, se la selecciona utilizando el click derecho del mouse y luego Edit-->Set/Unset Time Reference:

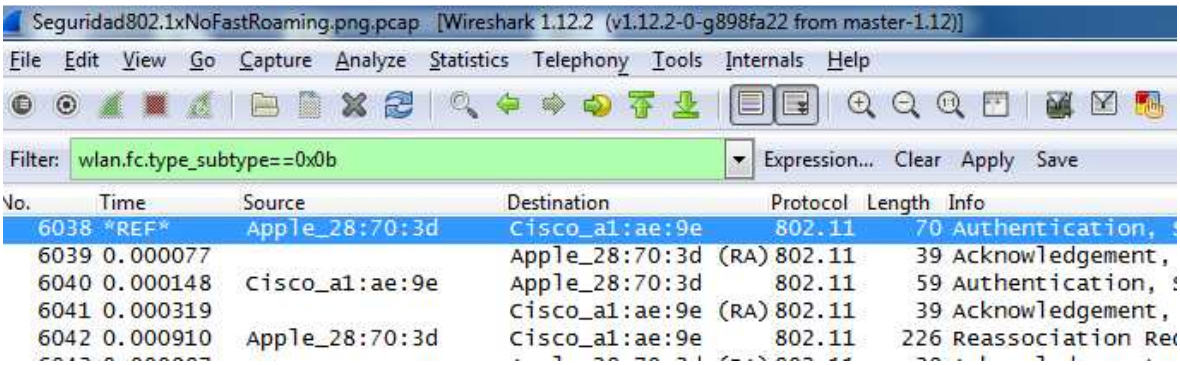


Figura 5.5.5 Trama autenticación con seguridad sin FastRoaming

Luego se busca la cuarta trama de intercambio de claves (EAPOL key) que significa que se ha completado el intercambio de claves compartidas, exceptuando el ACK 802.11 por supuesto. Para encontrarlo se escribió “EAPOL” en el cuadro del filtro y se seleccionó la última.

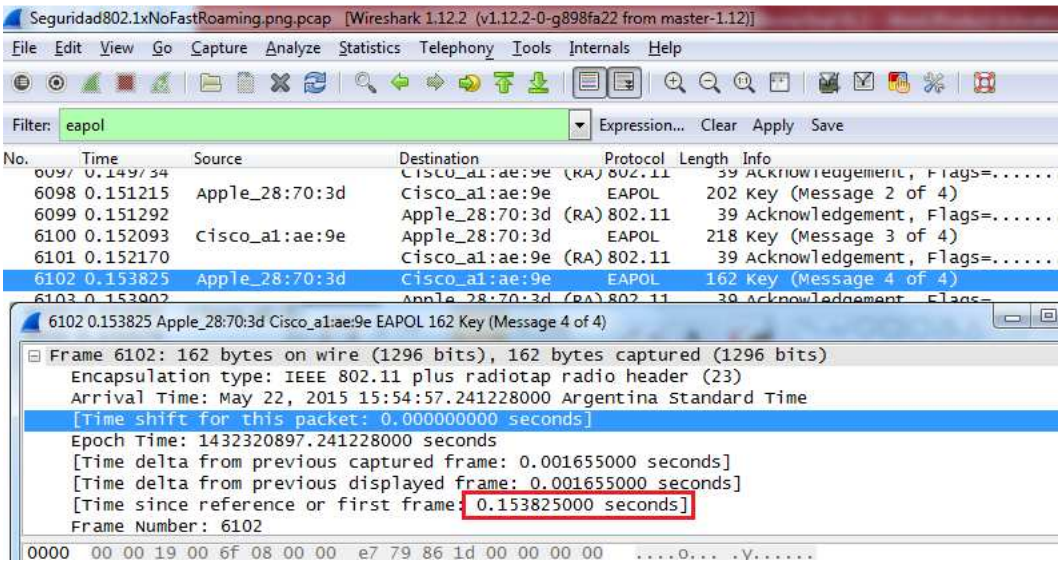


Figura 5.5.6 Trama EAPOL 4 con seguridad sin FastRoaming

El resultado fue de un tiempo de re asociación de 0,153825 segundos; o 150 ms aproximadamente.

5.5.3. Prueba 3: Aplicando la norma 802.11r OTE

Para esta prueba se utilizó la misma ESS pero habilitando el traspaso rápido 802.11r directamente entre los APs y STAs, se obtuvo el archivo de captura Seguridad802.1xFastRoamingOTA.pcap.

Nuevamente se buscó la trama de autenticación enviada al AP2.

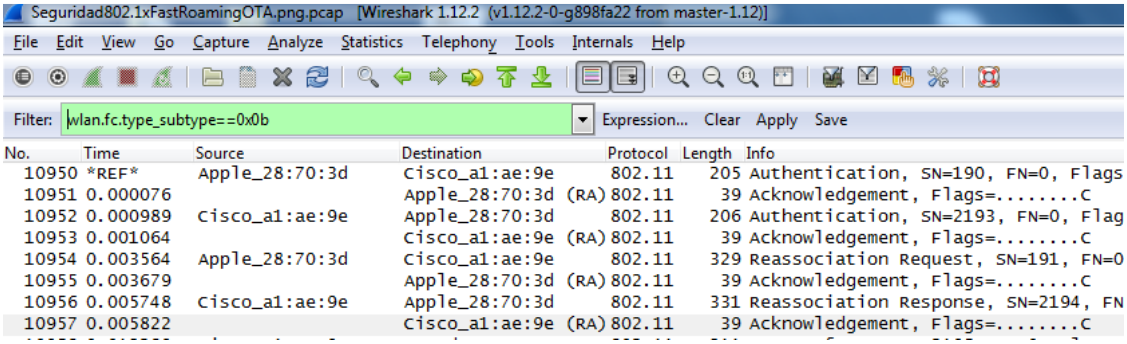


Figura 5.5.7 Trama autenticación con seguridad con FastRoaming

En esta primera trama (line 10957) vemos en el dominio móvil, que se trata de una transición rápida de BSS, e inclusive el campo Over-the-DS es 0.

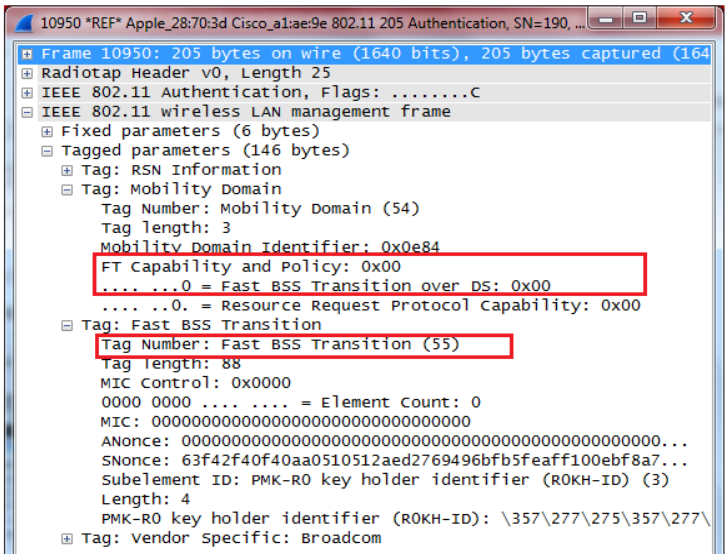


Figura 5.5.8 Campos de trama relacionados con la transición rápida de BSS

Se configura el tiempo de referencia en esta trama, y se procede a buscar la última trama que en este caso es la trama respuesta re asociación exitosa del AP2 (línea 10955).

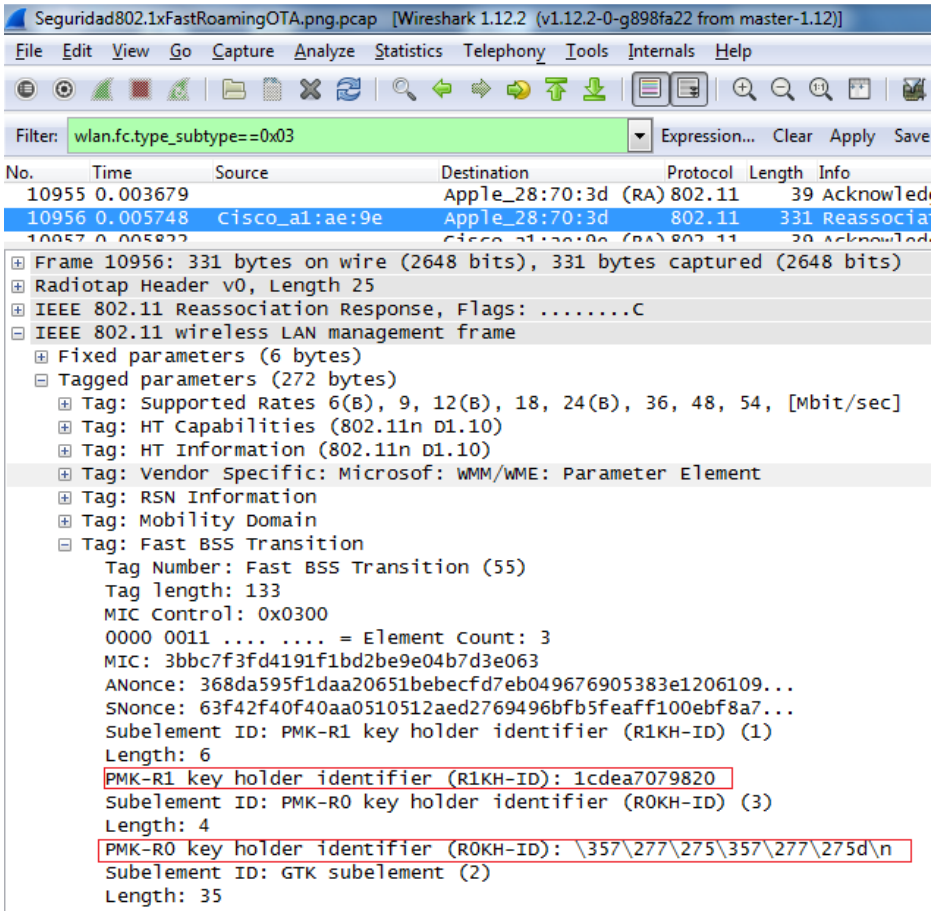


Figura 5.5.9 Trama respuesta de re asociación con seguridad con FastRoaming

Como se puede apreciar durante la re-asociación, en este caso el intercambio de claves están incluidos en las tramas de autenticación y re-asociación, por este motivo en este caso no se encuentran las tramas EAPOL que mostramos en la captura de la prueba anterior. De esta manera se reduce significativamente el tiempo requerido para la re-asociación.

El resultado fue de un tiempo de re asociación de 0,0058 segundos; o 5,8 ms aproximadamente.

5.5.4. Prueba 4: Aplicando la norma 802.11r ODS

Para esta prueba se utilizó la misma ESS pero habilitando el traspaso rápido 802.11r a través de la red cableada (DS), se obtuvo el archivo de captura Seguridad802.1xFastRoamingODS.pcap.

Esta prueba es un poco más complicada, debido a que la primer trama del proceso es una trama Acción (FT action request) dirigida al AP1. Esta trama (línea 1163) es reenviada a través del DS (Ethernet 802.3 en este caso) al AP2. Note la inclusión del término 'Target AP' (AP2):

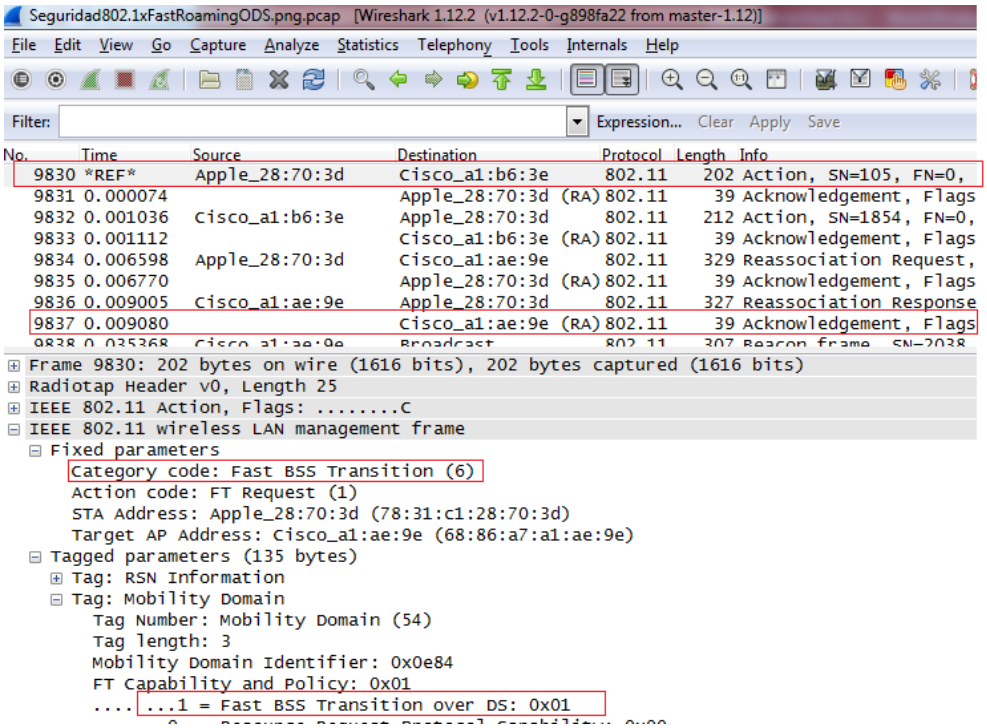


Figura 5.5.10 Tramas de transición rápida ODS

Esto nos muestra un tiempo de re asociación (roaming) de 0,009080 segundos, o 9,08ms aproximadamente.

5.6. Análisis de los datos obtenidos

Con una red segura (WPA2) que no aplica la norma 802.11r se tiene un tiempo de re asociación de 150ms.

Con una red segura (WPA2) aplicando la norma 802.11r directamente en el Aire se tiene un tiempo de re asociación de 5,8ms.

Con una red segura (WPA2) aplicando la norma 802.11r a través del DS se tiene un tiempo de re asociación de 9,08ms.

Notamos una gran diferencia entre el escenario WLAN actual y el presentado por la norma 802.11r en cuanto al tiempo de re asociación en una red segura. La diferencia de tiempo entre 16ms y 150ms suele ser la diferencia de tiempo permitida para muchas aplicaciones sensibles a la latencia para no tener un efecto muy notorio. Hay que tener en cuenta que este es solo el tiempo de re asociación MAC, a esto hay que agregarle el tiempo que lleva procesar la información de capas superiores. Para una conversación de VoWiFi, los 150ms pueden ser muy notorio o inclusive causar la pérdida de la llamada. Además, esta prueba se realiza en un ambiente controlado, donde el medio estaba completamente disponible para la prueba, en una red más cargada este tiempo puede ser mayor volviendo imposible la continuidad del uso de aplicaciones sensibles a la latencia en redes sin la norma 802.11r en funcionamiento.

6. Diseño de una solución de red para voz sobre una WLAN 802.11r

En este capítulo se presenta un breve plan de negocio para prestar un servicio WiFi utilizando la norma 802.11r. Una vez ya conocida la norma y los equipos requeridos para que funcione correctamente, se buscara plantear el armado de una red WiFi 802.11r destinado a un barrio cerrado con dificultades de acceso a los prestadores de servicios de telecomunicaciones convencionales. Se estimara la inversión inicial en función a la cantidad de APs requeridos para cubrir todo el barrio, como así también el costo del DS que los interconecte (Controladora, cableado, switches, routers, etc.). Luego se proyectarán los clientes potenciales y cuanto se les solicitara en concepto de instalación y costo del servicio. Finalmente se calculara la VAN y la TIR del proyecto y así ver cuán rentable resulta.

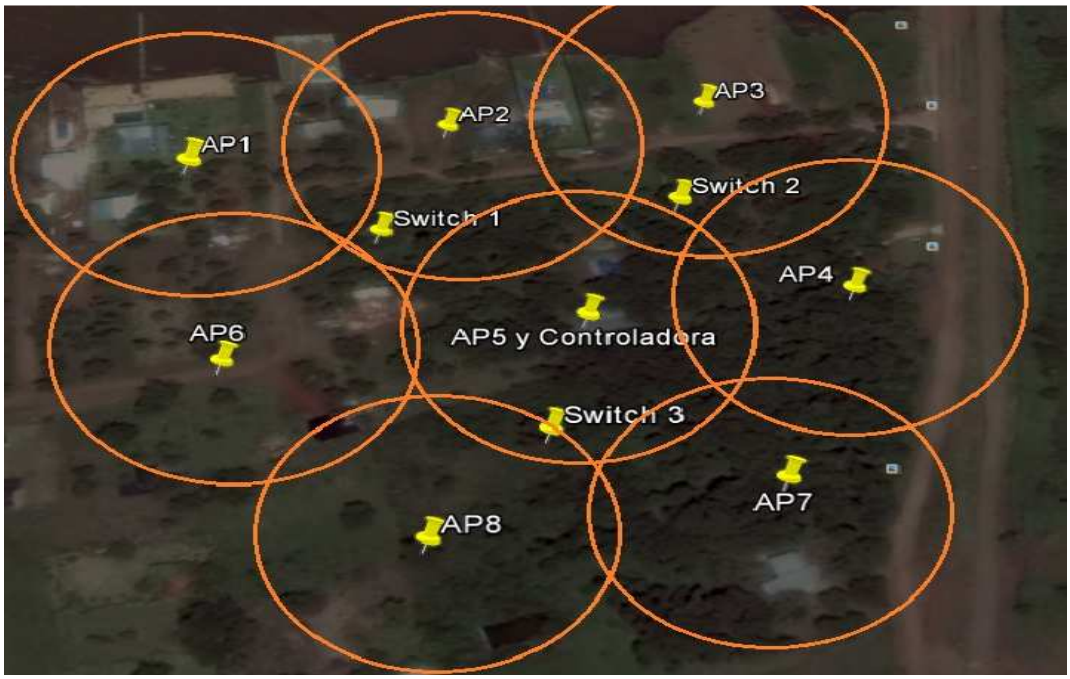


Figura 6.1 Área de cobertura en barrio cerrado

Inversión Inicial:

Se estimó que para una área de aproximadamente (750 m2) se requerirá 8 APs y con el costo de 3000 A$R por cada AP tendríamos un costo inicial de 24.000 A$R en concepto de APs. Luego se requerirá de una controladora, la controladora más económica que se encontró para trabajar con estos APs tiene un precio de aproximadamente 6.000 A$R. Se estima que se deberá incurrir en aproximadamente 500 m de cableado Ethernet con un costo aproximado de 10 A$R por metro de cable se tendría 5.000 A$R en concepto de cableado. Se requería por lo menos 3 switches con puertos PoE para recibir los APs con un costo de 1.000 A$R por cada uno. Y finalmente un router para poder prestar diferente servicios como salida a internet entre otros con un costo aproximado de 4000 A$R. Se agrega un costo de 10.000 A$R en concepto de mano de obra para el cableado estructurado requerido. Adicionalmente se agrega 8.000 A$R para gastos varios. Finalmente se cuenta con una Inversión Inicial requerida de 60.000A$R.

Inversión Inicial		
	Costo	Total
8 Aps	24.000	
Controladora	6.000	
3Switches con PoE	3.000	
500 m cable Ethernet	5.000	
Router	4.000	
Mano de Obra	10.000	
Contingencias	8.000	
		60.000

Figura 6.2 Inversión inicial para WLAN 802.11r

Costos de Mantenimiento:

A pesar de que una vez finalizada la instalación y puesta a punto, el costo de mantenimiento de la red es casi nulo se contempla un costo de mantenimiento de 20.000 A$R anual por si hay que incurrir en alguna reparación o soporte al usuario, con incrementos de 5.000 A$R anuales debido a la inflación.

ISP:

Se estima un costo de aproximado de 12.000 A$R el primer en concepto de Proveedores de Internet, esto costo se ve duplicado en el segundo año estimado que el número de clientes se va a ver fuertemente incrementado y por lo cual se requerirá un servicio más veloz para soportar la cantidad de usuarios.

Pago de servicio:

Luego de una pequeña encuesta en la zona sabemos que existen 11 vivienda ocupadas permanentemente y con otras 7 que solamente concurren los fines de semanas. De las 11 personas que viven en la zona 8 de ellas confirmaron que les interesa el servicio. En función a la capacidad de pago de los clientes y el interés mostrado por el servicio ofrecido, se decidió que un costo de 500 A$R mensual sería adecuado en un comienzo. También se les cobrara un costo de instalación de 1.500 A$R por única vez. Suponiendo que el primer año solamente se contara con los 8 clientes interesados tendríamos una proyección anual de 48.000 A$R de pago del servicio y 12.000 A$R en pago de instalación.

Se espera que entre el primer y segundo año la población del barrio se verá incrementada y se espera duplicar el número de usuarios tomando en cuenta que los que no adquirieron el servicio en un comienzo también se vean interesados en adquirirlo luego de ver su funcionamiento y sumado al hecho de que la tecnología para el usuario final cada vez será de más fácil acceso. Llegando así al ingreso anual de 96.000 A$R y un extra en concepto de instalación de 12.000 AR$ para el segundo año. A Partir de este punto se estima que el ingreso en concepto de pago de servicio se va a ver ligeramente incrementado solamente en concepto de incremento del costo del servicio por la inflación.

A continuación se lista el conjunto de ingresos y egresos ya explicados en manera de tabla (figura 6.2).

Periodo (años)	0	1	2	3	4	5
Costos A$R						
Inversión	-60.000					
Costos de mantenimiento		-20.000	-25.000	-30.000	-35.000	-35.000
ISP		-12.000	-24.000	-28.000	-30.000	-30.000
Ingresos A$R						
Cuota Clientes		48.000	90.000	100.000	110.000	110.000
Costo de instalación	12.000		14.000		5.000	
Valor residual						15.000
Utilidades A$R						
Utilidades	-48.000	16.000	55.000	42.000	50.000	60.000

Figura 6.3 Flujo de caja para cálculo de VAN

Al final del cuadro se tienen las utilizadas netas.

Calculo de VAN:

$$\mathrm{VAN} = \sum_{t=1}^{n} \frac{V_t}{(1+k)^t} - I_0$$

- Vt representa los flujos de caja en cada periodo t.
- Io es el valor del desembolso inicial de la inversión.
- n es el número de períodos considerado, en nuestro caso 5.

- k, d o TIR es el tipo de interés, se tomara k = 0,5.

Utilizando la formula y las utilidades encontradas en la figura 6.2 obtenemos una VAN = 30967,4.

Esto significa que si las predicciones aquí esbozadas son acertadas el proyecto tendrá un excedente de ganancia de aproximadamente 30.967 A$R y por lo tanto se justifica llevar a cabo el proyecto bajo estas condiciones.

7. Conclusión y Reflexión

El marco teórico ayudó a enmarcar al lector en el funcionamiento teórico de las redes WLAN, los conceptos y problemáticas que plante el roaming, y finalmente las mejoras que la nueva norma 802.11r propone para lograr un roaming rápido sin perder seguridad ni calidad de servicio en el proceso.

Luego se llevó a la práctica lo estudiado para comprobar su funcionamiento y rendimiento como así también familiarizarse con los equipos, y las ventajas y dificultades que presenta la puesta en marcha de una red con estas características. Se pudo observar que a pesar de algunas dificultades para adquirir los equipos que la soporten debido a lo innovador de esta tecnología, no es imposible y sus costos no son tan elevados como se creía al comienzo del proyecto. También, a pesar que en un comienzo presento un desafío su puesta en marcha debido a la escasa información encontrada al respecto, el conexionado y configurado al que se debe incurrir es relativamente simple.

Se pudo probar que las mejoras en cuanto al tiempo requerido para el traspaso de un AP a otro para una STA en movimiento es muy significativa y determinante para algunas aplicaciones que son muy sensibles a los cortes en la conexiones como la Voz sobre IP (VoIP). Y como se puede apreciar en las capturas a pesar de lograr una mejora muy notoria en el tiempo de re asociación, el encriptado, la autenticación y las prestaciones de QoS siguen siendo las mismas, es decir no se sacrifica robustez para mejorar los tiempos de respuesta.

Se observó que gracias a la nueva tecnología 802.11n y contando con equipos muy estables y con muy buena cobertura se pueden cubrir grandes áreas con pocos equipos y con la facilidad de que solo requieren de un conexionado Ethernet ya que la alimentación eléctrica la provee la misma conexión Ethernet (PoE) disminuyendo los costos de instalación.

Finalmente por la experiencia adquirida en este documente, es consideración del autor que es muy factible la prestación de un entorno WLAN aplicando la norma 802.11r donde se preste un servicio de VoIP inalámbrico que no se vea interrumpido o deteriorado por un posible traspaso de un AP a otro por el movimiento de la STA cliente. Sin embargo actualmente se trataría de un servicio con un costo de instalación un poco elevado transformándolo en un producto Premium para una economía emergente como la nuestra, y tomando en cuenta que solamente las STA móviles de última generación únicamente soportan la norma en cuestión.

8. Bibliografía

Libros y Publicaciones:

IEEE Computer Society, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

IEEE Computer Society, Part11 Amendment 2: Fast Basic Service Set (BSS) Transition.

Veriwave 802.11 WLAN Systems - a tutorial.

Jim Geier from Cisco, Designing and Deploying 802.11n Wireless Network.

Raymond Greenlaw y Paul Goransson, Secure Roaming in 802.11 Networks.

Páginas WEB y Foros:

Apple, equipos que soportan 802.11r: http://support.apple.com/kb/HT5535

Cisco, Controladoras que soportan 802.11r:

http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps10315/product_bulletin_c25-707629_ps2706_Products_Bulletin.html

Cisco, Capturas y debugs en WLANs:

http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/116493-technote-technology-00.html

Wikipedia, cálculo de VAN: http://es.wikipedia.org/wiki/Valor_actual_neto

Cisco, puesta en marcha de APs 3500:

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/3500/quick/guide/ap3500getstart.html

Laurence Schoultz, Configuración Inicial de controladora cisco 2504:

https://www.youtube.com/watch?v=qZX8max1PR8

Cisco, configuración de controladora Cisco para trabajar bajo la norma 802.11r:

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

Mike Abalos, Ejemplo de implementación de red 802,11r:

http://www.mikealbano.com/2014/06/80211r-80211k-fast-bss-transition.html

Sams Wireless, Cambio de IOS para los APs Cisco:

http://samswireless.blogspot.com.ar/2011/01/surveying-with-3502-followup-post.html

Configuración de servidor de autenticación FreeRadius para Linux:

http://wiki.freeradius.org/guide/Basic-configuration-HOWTO

9. Anexos

Anexo A: Cambio de IOS para C3502i

Herramientas requeridas:

- PC con placa de red Ethernet 802.3 configurada con la IP 10.0.0.2/24
- Servidor TFTP corriendo en la PC
- El IOS que se desea instalar (ap3g1_rcvk9w8_tar.153_3.JA3)
- AP 3502i con alimentación externa conectado a la PC por medio de un cable Ethernet directo.

Para convertir el IOS:

- Paso 1) Duplicar el IOS que se está por instalar y cambiar el nombre a uno de ellos por ap3g1-k9w7-tar.default, colocar estos dos archivos en la carpeta raíz del servidor TFTP.
- Paso 2) Oprimir el botón mode del AP y conectamos la alimentación, soltar el botón mode una vez que el color del led en el AP se torna rojo.
- Paso 3) Esperar que el AP cargue la Imagen del servidor TFTP.

Si tuviéramos acceso consola del AP veríamos lo siguiente:

```
button is pressed, wait for button to be released...
button pressed for 22 seconds
process_config_recovery: set IP address and config to default 10.0.0.1
process_config_recovery: image recovery
image_recovery: Download default IOS tar image tftp://255.255.255.255/ap3g1-k9w7-
tar.default
```

```
Unable to create temp dir "flash:/update"
examining image...
extracting info (293 bytes)
Image info:
    Version Suffix: k9w7-.124-25d.JA
    Image Name: ap3g1-k9w7-mx.124-25d.JA
    Version Directory: ap3g1-k9w7-mx.124-25d.JA
    Ios Image Size: 5673472
    Total Image Size: 6502912
    Image Feature: WIRELESS LAN
    Image Family: AP3G1
    Wireless Switch Management Version: 7.0.94.21
Extracting files...
ap3g1-k9w7-mx.124-25d.JA/ (directory) 0 (bytes)
ap3g1-k9w7-mx.124-25d.JA/html/ (directory) 0 (bytes)
```

Una vez que el IOS fue completamente cargado este se reiniciara.