ANEXO A. ESTÁNDAR 802.11r

A.1 JERARQUÍA DE LLAVES FT (802.11r)

Para lograr una transición rápida entre BSSs se necesita realizar los procedimientos normales de una transición pero de manera más rápida y eficaz; para lograr la consecución de este objetivo el proceso completo de autenticación 802.1x debe eliminarse una vez se ha realizado la primer asociación en el dominio de movilidad, es decir, se debe permitir las posteriores transiciones a otros APs del mismo dominio de movilidad sin tener que realizar el proceso de autenticación 802.1x en cada uno de los APs a los cuales se realiza la transición. Este sistema es definido por el estándar 802.11r y se logra a través de una nueva jerarquía de llaves llamada Jerarquía de Llaves FT. La jerarquía de Llaves FT se puede usar con 802.1x o con PSK. [1]

El estándar utiliza una jerarquía de 3 niveles de llave el cual provee separación entre los poseedores de llave. La jerarquía usada por el autenticador se observa en la Figura A-1 [1], así mismo existe una jerarquía idéntica para el cliente móvil o suplicante y las funciones son realizadas por el correspondiente S0KH y S1KH, en donde S es por suplicante.

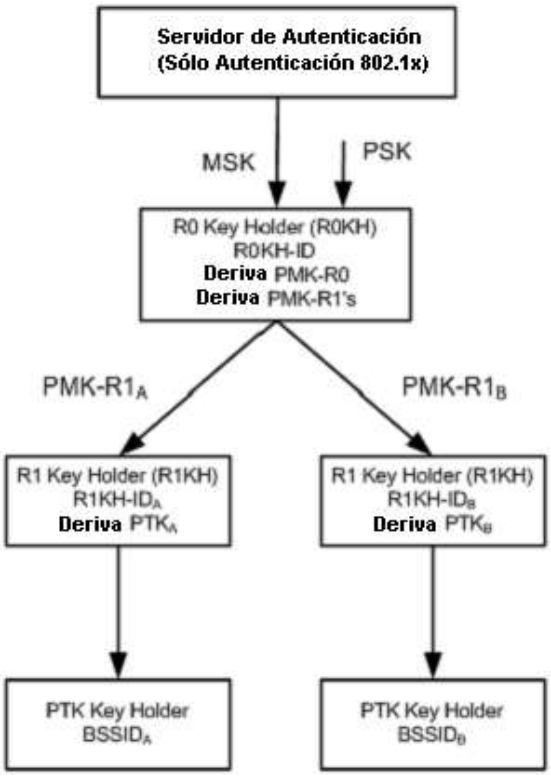

Figura A-1 Jerarquía FT en el autenticador.

A continuación se definen las llaves y niveles de llaves. [1]

a) El primer nivel de llave es la PMK-R0. Esta llave es derivada en función de la MSK o PSK. Esta se almacena en los PMK-R0 *Key Holders*, R0KH y S0KH.
b) El Segundo nivel de llave es la PMK-R1, esta llave es derivada tanto por S0KH como por el R0KH.
c) El tercer nivel de llave en la jerarquía es la PTK, esta llave define las llaves reales de protección de la información en 802.11 y 802.1x. La llave PTK es derivada por los tenedores de llave, R1KH y S1KH.

Como se puede ver en la Figura A-1 el R0KH computa la PMK-R0, a partir de una PSK o de una MSK resultado de una autenticación 802.1x exitosa entre el suplicante y el servidor de autenticación.

Luego de que se ha autenticado exitosamente el suplicante, el R0KH debe borrar cualquier asociación de seguridad PMK-R0 dentro del MD perteneciente al S0KH del suplicante autenticado. También debe borrar todas las asociaciones de seguridad PMK-R1 derivadas de la PMK-R0 borrada anteriormente. Las PMK-R1s son generadas por el R0KH y se asume que son entregadas a los R1KHs dentro del mismo MD. Las PMK-R1s se usan para derivar las PTK. Una vez y se recibe una nueva PMK-R1 para un S0KH, el R1KH elimina la asociación de seguridad anterior PMK-R1 y las asociaciones de seguridad PTKs derivadas de este PMK-R1 anterior.

El estándar asume que la PSK es específica a un simple S0KH y un simple R0KH. El tiempo de vida de la PMK-R0, PMK-R1 y PTK están ligados directamente al tiempo de vida de la PSK o MSK. La jerarquía FT deriva las llaves usando la función de derivación de llaves (KDF, *Key Derivation Function*) la cual usa etiquetas separadas para distinguir las derivaciones. Durante una transición rápida FT la estación móvil o suplicante debe negociar o solicitar al AP destino el mismo tipo de cifrado que se uso en la asociación inicial al MD. La distribución de las llaves entre el R0KH y los R1KHs no está dentro de las definiciones u objetivos de este estándar, por lo cual se asume que las PMK-R1's son distribuidas de manera segura, ya que los APs pertenecientes al ESS se encuentran dentro del sistema de distribución el cual no es objeto de 802.11. La PMK-R0 puede ser eliminada por el R0KH luego de que las PMK-R1's se han entregado, el R0KH solo necesita mantener las asociaciones de seguridad PMK.R1's. La PTK tiene tres llaves componentes y estas son [1][1]: KCK, KEK y la TK

Llave de confirmación de llave (KCK, *Key Confirmation Key*), esta llave se usa para probar la autenticidad del origen de los datos en los mensajes de llave EAPOL.

La llave de llave de cifrado (KEK, *Key Encryption Key*), es con la que se logra la confidencialidad de los datos en los mensajes de llave EAPOL.

La llave temporal (TK, *Temporal Key*), esta llave es específica para tipos de cifrado que dependen del proveedor de la tecnología.
La derivación de llaves en la jerarquía FT es una función delegada a los R0KH y R1KH,

En esta jerarquía de llaves el saludo de 4 vías realizado para el traspaso de elementos en la generación de llaves utilizando mensajes EAPOL, es reemplazado, ya que estos elementos se incluyen en las tramas de autenticación y asociación.

Estos son los componentes principales:

El autenticador:
Es el que redirige los mensajes EAP entre el suplicante y el servidor de autenticación.
Este también recibe la MSK desde el AS.
Deriva la llave PMK-R0 a partir de la MSK.
Transfiere la PMK-R0 al PMK-R0 *key Holder (*R0KH*)*.
Este es identificado por el NAS-ID.

El R0KH:
Es la primera entidad con la que se realiza la primera asociación.
Realiza funciones de gestión de llaves RSNA. Actúa como un autenticador.

Recibe la PMK-R0, Deriva PMK-R1 y la transfiere a R1KH, se identifica mediante el R0KH-ID

El R1KH:
Realiza funciones de gestión de llaves RSNA. Actúa como un autenticador. Es el primero u otro subsiguiente autenticador.
Recibe la PMK-R1 desde R0KH.
Realiza el saludo de 4 vías con el suplicante.
Deriva la PTK y se identifica mediante el R1KH-ID

Cuando un autenticador no es R0KH recibe la PMK-R1 del autenticador R0KH.
Todas las llaves componentes de la PTK, son derivadas por los R1KHs. Las llaves que componen la PTK son: KCK-11, KEK, KCK-1X, TK

A.2 ASOCIACIÓN INICIAL FT EN EL DOMINIO DE MOVILIDAD

Esta es la primera asociación (reasociación) dentro del dominio de movilidad, donde la entidad de gestión de la estación habilita su futuro uso de los procedimientos de FT. En la primera asociación se permiten peticiones de reasociación para permitir que suplicantes que no tienen habilitado o no soportan protocolos FT puedan asociarse y de esta manera permitir un funcionamiento o coexistencia de la red con los dos tipos de *roaming.*

Asociación FT inicial en el dominio de movilidad en una RSN.

Cuando una estación se va a asociar en un dominio de movilidad en el que se soporta los protocolos FT, ella misma indica si soporta o no los procedimientos de FT mediante la transmisión del MDIE y la seguridad que soporta a través del elemento de información de red con seguridad robusta (RSNIE, *Robust Security Network Information Element*), la cual es una trama que contiene información acerca de RSN u 802.11i, en esta trama se indica tipos de autenticación, cifrado y cosas relacionadas con seguridad en la red, el AP responde mediante la inclusión del Elemento de información de FT (FTIE, FT *Information Element*), elemento de información de dominio de movilidad (MDIE, *Mobility Domain Information Element*) y el RSNIE en la trama de respuesta de asociación. Luego de que la autenticación 802.1x tuvo éxito, si es necesario la estación y el AP realizan un saludo de 4 vías FT. Al final de la secuencia se abre el puerto 802.1x y se establece la jerarquía de llaves FT. Este proceso se aprecia en la Figura A-2 [1], la estación inicia los procesos de asociación realizando una petición de autenticación con el sistema abierto.

Es de remarcar en este momento, que los sistemas de autenticación de RSN utilizan únicamente como algoritmo de autenticación inicial de 802.11 el sistema abierto (OS*, Open System*), nunca el sistema de clave o llave precompartida (PSK*, Pre-Shared Key*).

Como segundo paso, el AP envía su respuesta de autenticación abierta a la estación móvil.

Como tercer paso, la estación envía una petición de asociación en la que incluye el MDIE y también se incluye el RSNIE en el cual indica sus capacidades de seguridad, los valores que están presentes en estos elementos de información deben coincidir con los que el AP anunció anteriormente en el *Beacon* o en la respuesta de sonda o *Probe Response*, de lo contrario el AP rechazará la petición de asociación.

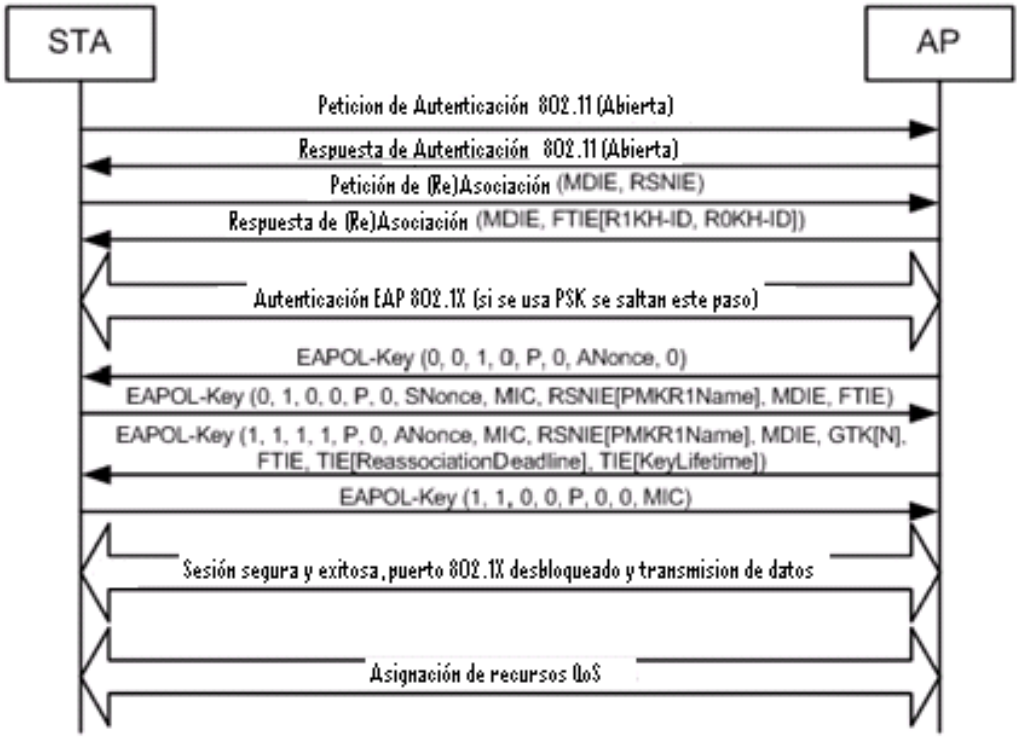

Figura A-2 Asociación inicial FT al dominio de movilidad en una red RSN.

El cuarto paso es el envío de la respuesta de asociación por parte del AP la cual incluye un MDIE, con los contenidos que había anunciado en los *Beacon* o en las respuestas de sonda. También se incluye dentro de la respuesta el FTIE el cual debe incluir las identidades o identificaciones de los tenedores de llave o *key holders*, estos valores son R0KH-ID Y R1KH-ID.

Una vez se logra una autenticación satisfactoria tanto por parte de la estación móvil como del AP, el S0KH Y El R0KH proceden con el quinto paso el cual es la autenticación 802.1x (esta se pasa por alto en caso de usarse PSK) usando tramas EAPOL transportadas en 802.11. Luego, después de lograr la autenticación el R0KH recibe la MSK, si ya existe una jerarquía de llaves o distribución ya existe para esta estación móvil y es perteneciente al mismo MD (o sea que tienen el mismo MDID), el R0KH debe borrar las asociaciones de seguridad PMK-R0 y PMK-R1, luego vuelve a calcular PMK-R0, PMK-R1 y PMKR0Name, y pone a disposición de R1KH en el AP la PMK-R1 con el cual la estación móvil está asociada. En caso que el AS o la STA no logren autenticar su contrario enviarán un mensaje de desasociación a su par. Cuando el atributo de tiempo de vida de la MSK, es provisto por el AS, el tiempo de vida de la PMK-R0 no puede ser superior a este mismo tiempo. Cuando se usa PSK el tiempo de vida de las asociaciones de seguridad PMK-R0, PMK-R1 y PTK debe ser el valor de la variable MIB dot11FTR0KeyLifetime. El sexto paso es el intercambio de mensajes conocido como saludo de 4 vías (4 *Way HandShake*) entre el R1KH y el S1KH, a continuación se describe este proceso [1]:

a. R1KH→S1KH: (ANonce)

b. S1KH→R1KH: Nonce, MIC, RSNIE[PMKR1Name], MDIE, FTIE

c. R1KH→S1KH: ANonce, MIC, RSNIE[PMKR1Name], MDIE, FTIE [ReassociationDeadline], TIE[KeyLifetime]

d. S1KH→R1KH:MIC

a. Este primer mensaje contiene el *Anonce* el cual es un valor aleatorio que genera el R1KH y se lo envía al suplicante, una vez el suplicante tiene este mensaje puede derivar o calcular la PTK, la cual usa la KCK para incluir la seguridad de MIC en el siguiente mensaje.

b. Este mensaje va desde el S1KH al R1KH, y en este se incluye el Nonce el cual es el valor aleatorio generado por el AP para la creación de la PTK, además este mensaje ya está con la seguridad de MIC, además a esto ya se incluyen valores de los elementos de información, los cuales son PMKR1Name en el campo de PMKID y los valores de MDIE y FTIE que deben coincidir con los mismos valores de estos campos en la trama de respuesta de petición de asociación.

c. El tercer mensaje va desde el R1KH al S1KH, el R1KH incluye el PMKR1Name, este debe ser idéntico al del mensaje anterior y que es enviado por el S1KH, aquí también se incluye un valor importante y es el tiempo límite de espera para la reasociación, este valor se encuentra en el TIE [ReassociationDeadline], también la duración de la llave PTK que se encuentra en el TIE [KeyLifetime]. El FTIE y el MDIE deben ser idénticos como en la trama de respuesta de asociación. El tiempo límite de la reasociación debe ser el mismo en todo el MD, y este tema no está especificado en este estándar.

d. El cuarto y último mensaje del saludo, es una especie de ACK, con este se le indica al AP que el suplicante instaló las llaves para cifrado (PTK) en esa sesión, luego de que el AP recibe este mensaje, también instala las llaves (PTK) para iniciar el cifrado de datos.

Luego de que se completa exitosamente el saludo a 4 vías entre R1KH y S1KH, se inicia el conteo del temporizador del tiempo de vida de la PTK, para que la asociación de la PTK no sea mayor a la que se envió en el mensaje 3, TIE [KeyLifetime]. Una vez y se acaba el tiempo de las llaves, la STA debe realizar de nuevo los procedimientos de asociación inicial al MD FT.

A.3 PORTADORES DE LLAVE (*KEY HOLDERS*, KH)

La Figura A-3 presenta las entidades que se encargan de la gestión de las llaves en 802.11r. En la parte del autenticador se localizan el portador de Llave R0(R0KH, *R0 Key Holder*) y el portador de Llave R1(R1KH, *R1 Key Holder*), R0KH es el encargado de calcular las llaves PMK-R0 y PMK-R1, y el cálculo de la PTK es hecha por el R1KH. En la parte del suplicante se encuentra el portador de llave S0 (S0KH, *S0 Key Holder*) y el portador de Llave S1 (S1KH, *S1 Key Holder*), S0KH es el encargado de calcular las llaves PMK-R0 y PMK-R1, y el cálculo de la PTK es hecha por el S1KH

Figura A-3 Arquitectura del portador de llaves FT.

- **Portadores del autenticador.**

Los encargados de derivar las llaves en la jerarquía de llaves FT son R0KH y R0H1. Para una transición rápida entre BSSs las funciones del autenticador 802.1x se distribuyen entre estos dos portadores. El autenticador le envía al R0HK la MSK que resultó de la autenticación EAP, y el R1KH se comunica con el autenticador para abrir el puerto controlado. El R0KH deriva la PMK-R0 y también se encarga de derivar la PMK-R1 para cada R1KH dentro del dominio de movilidad (MD*, Mobility Domain)*. El R1KH y el S1KH son los encargados de derivar la PTK.

También en este contexto entran los valores de R0KH-ID y R1KH-ID, los cuales deben ser únicos dentro del MD, estos valores son comunicados a las estaciones móviles en el MD así como a los otros portadores*.* El valor del R0KH-ID está ligado de manera directa a la generación de la llave PMK-R0 y así mismo el R1KH-ID está ligado con la generación de la llave PMK-R1.

- **Portadores del suplicante.**

Los responsables de la derivación de las llaves en la jerarquía FT en el suplicante son S0KH y S1KH, estas son entidades que se asumen están físicamente en el suplicante o estación inalámbrica. Las funciones de éste componente son similares a las del R0KH y R1KH en el autenticador, esto es, El S0KH interactúa con el bloque funcional de 802.1x para recibir la MSK resultado de la autenticación EAP y S1KH interactúa con 802.1x para abrir le puerto controlado, así mismo, S0KH deriva la PMK-R0 para usar en el MD ya sea utilizando la MSK o la PSK. S1KH y R1KH derivan mutuamente la PTK.

El S0KH y el S1KH deben identificarse por la dirección del suplicante. Así mismo el S0KH no deben exponer de manera indebida la llave PMK-R1 a terceros a menos que sean pares autorizados S1KH's. Los S1KH no deben exponer su llave PMK-R1a nadie.

A.4 SECUENCIA DE AUTENTICACIÓN FT

Este proceso comprende 4 conjuntos de elementos de información FT (FTIE), a cada uno de estos se le da el nombre de mensajes. Estos mensajes están incluidos en las tramas del protocolo FT o el protocolo de solicitud de recursos FT (RRFT, *Resource Request FT Protocol*). Se debe aclarar que esta secuencia es siempre iniciada por la estación y siempre va dirigida al AP destino. Los primeros dos mensajes de la secuencia le permiten a la estación y al AP intercambiar identificadores de la asociación, intercambio del *Anonce* y *Snonce*, con estos valores se crean PTKs nuevas, también con los primeros dos mensajes se logra que el AP destino y la estación móvil computen o deriven la PTK. El tercer y cuarto mensajes demuestran que el otro par está presente, autentican los IEs y habilitan la petición de recursos autenticada.

Cuando una estación invoca el protocolo FT, entonces los 2 primeros mensajes de la secuencia se llevan usando tramas de autenticación o tramas de acción. Los mensajes 3 y 4 de la secuencia se llevan en tramas de reasociación y respuesta de reasociación. Cuando una estación invoca el FTRRP hay 2 mensajes mas, estos 5 y 6 mensajes se llevan en tramas de reasociación y respuesta de reasociación, independientemente de la forma en que se transporten los mensajes, estos llevan los mismos IEs. Los IEs que se involucran en este proceso son: FTIE, RSNIE, MDIE, TIE y RIC.

La estación móvil usa el primer mensaje para iniciar la transición rápida FT, la estación

incluye la R0KH-ID y el *Snonce*[1] en el FTIE, además el PMKR0Name en el RSNIE. El AP destino puede utilizar el PMKR0Name para derivar el PMKR1Name, y si el AP destino no tiene identificada la PMK-R1 a través del PMKR1Name, puede tratar de pedir la llave PMK-R1 desde R0KH el cual está identificado por el R0KH-ID. La STA también incluye un valor nuevo de *Snonce* para la asociación segura que se está creando, además sirve como muestra de que el par esta activo en el cuarto mensaje.

En el segundo mensaje el AP destino responde las peticiones de la STA. El AP destino proporciona los identificadores y nombres de los KH usados para generar la PTK. El AP destino al igual que la STA provee un *Anonce*, con los mismos fines que el anterior.

El tercer mensaje lo usa la STA para evaluar si el AP destino tiene una llave PTK válida. Sí no se solicitan recursos, no se incluye el RIC.

Y por último, el cuarto mensaje lo usa el AP destino para hacer una confirmación final de la transición, este establece que el AP tiene la PMK-R1 y está participando en la asociación. Aquí se debe resaltar que el RIC no estará si en el mensaje anterior no se hicieron peticiones de recursos.

A.5 PROTOCOLO DE TRANSICIÓN RÁPIDA DE BSS (FT)

Este protocolo tiene la opción de solicitar recursos como parte de la asociación a diferencia del Protocolo de Pedido de Recursos FT (FTRRP, *FT Resource Request Protocol*) el cual soporta el pedido de recursos antes de la reasociación. Como se había mencionado con anterioridad, el proceso se puede realizar por dos métodos OTA o ODS, a continuación se revisan estos dos métodos.

A.5.1 Protocolo FT sobre el aire (OTAFTP, *Over the Air FT protocol*).

El OTAFTP en un ambiente RSN se describe a continuación [1]:

La estación y el AP utilizan la secuencia de autenticación FT para especificar la asociación segura PMK-R1, y para proveer valores del *Snonce* y *Anonce* con lo cual se consigue establecer protección contra repeticiones, prueba de vida y la llave PTK. Con este intercambio se logra generar una PTK nueva antes de que ocurra la reasociación. La asociación de seguridad PTK se usa para proteger las reasociaciones siguientes.

Para lograr la transición deseada en este caso, se debe realizar un intercambio como el de la Figura A-4[1], el cual se describe a continuación.

Primero que todo se envía una petición de autenticación al AP destino y éste, retorna un mensaje de respuesta de autenticación. En la trama de petición de autenticación el campo `Source Address` debe ser la dirección MAC de la STA y el `Destination Address` debe ser el BSSID del AP destino. Los valores de los elementos de información usados (RSNIE, FTIE, MDIE) deben ser idénticos a los que el AP anuncio con anterioridad en sus *beacons* o en las respuestas de las sondas. En caso de que algo de los elementos no coincida se rechaza la petición de autenticación con alguno de los códigos usados para ello.

[1] Snonce: Valor aleatorio generado por el cliente móvil o suplicante

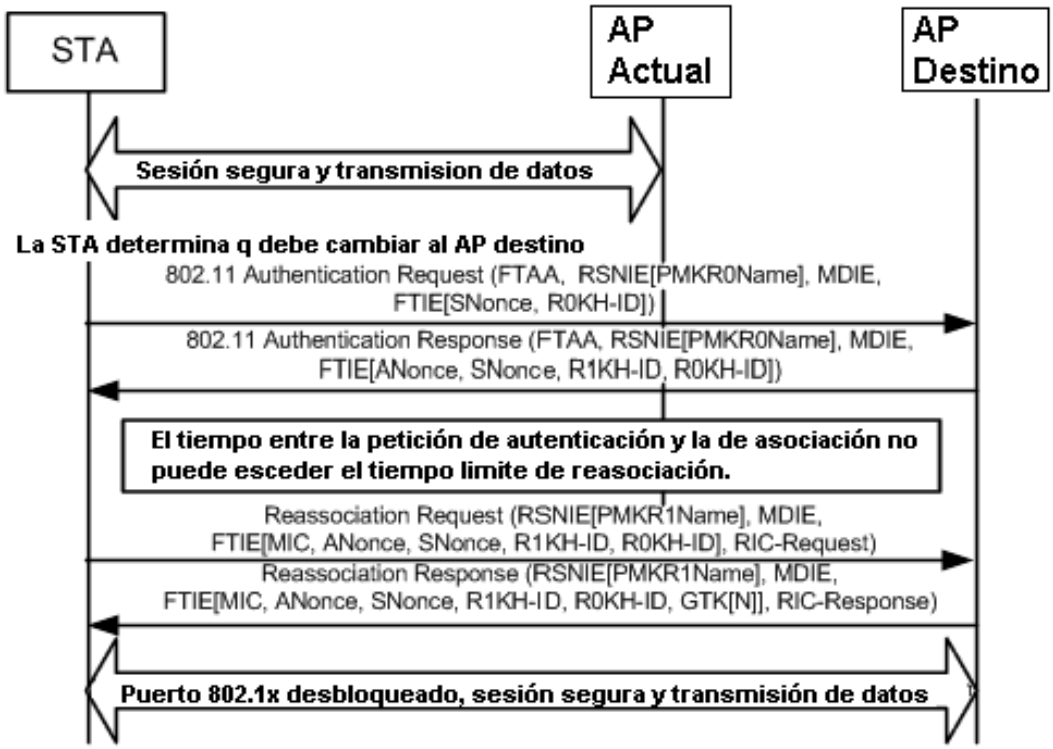

Figura A-4 Protocolo FT sobre el aire - OTFTP.

El segundo paso es la trama de respuesta de autenticación enviada por el AP destino hacia la STA. Aquí el campo de *Source Address* debe ser el BSSID del AP destino, y la *Destination Address* debe ser la dirección MAC de la STA. El R1KH usa el valor de la PMKR0Name para calcular la PMKR1Name, si con esto no logra obtener la llave PMK-R1, puede obtenerla a través del R0KH el cual identifica mediante el R0KH-ID que recibió de la STA en el mensaje numero uno. Una vez recibe la PMK-R1 el AP debe borrar todas las asociaciones seguras anteriores, PMK-R1SA y PTKSAs.

Ahora tanto el AP destino como la STA calculan unas PTKs nuevas a partir de los *Nonces* y de la PMK-R1, pero, si no recibe una petición de asociación antes de que se acabe el tiempo límite para ello, debe borrar estas asociaciones seguras.
Es en estos dos mensajes de autenticación donde se logra el proceso clave de generar unas nuevas llaves o asociaciones seguras sin necesidad de requerir nuevamente un saludo de 4 vías con tramas EAPOL, y también se elimina la necesidad de la autenticación con el servidor 802.1x, ya que es el R0KH quien le entrega la PMK-R1 al AP destino para realizar la nueva derivación de llaves en esta nueva asociación segura.

Los mensajes 3 y 4 son iguales a los de la sección A.4 donde se explica la secuencia de autenticación

A.5.2 Protocolo FT sobre el sistema de distribución (*Over the* DS FT *protocol*, ODSFTP).

Antes de revisar el protocolo en sí, se necesita hacer un análisis de las tramas que se usan para este propósito, estas son las tramas de acción. Estas tramas contienen la información para realizar la transición y se inician desde la STA hacia el AP destino pasando a través del AP con el que está actualmente asociada la STA

Tramas de acción

Para soportar el ODSFTP se especifican 4 nuevas tramas, estas tramas llamadas de acción son las siguientes [1]:

1. Trama de petición FT: En la Figura A-5 [1] se ve el detalle de la trama, esta trama va desde la STA hacia el AP destino. En el campo de categoría va el valor correspondiente a tramas de acción, en el campo de acción va el valor dependiendo el tipo de trama de acción, en este caso petición FT, en el campo de dirección de STA va el valor de BSSID del AP destino, y el cuerpo de la trama contiene los elementos de información, RSNIE, MDID y FTIE, con los cuales se realiza el intercambio y/o autenticación de la información para la transición al AP destino de una manera rápida.

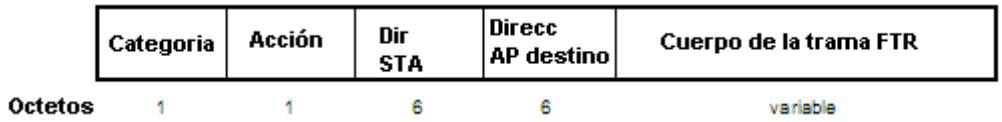

Figura A-5 Trama de petición FT (FTR).

2. Trama de Respuesta FT: esta trama es enviada desde el AP a que se encuentra conectado actualmente la STA como respuesta de la trama anterior. En la Figura A-6 [1] se detalla la trama.

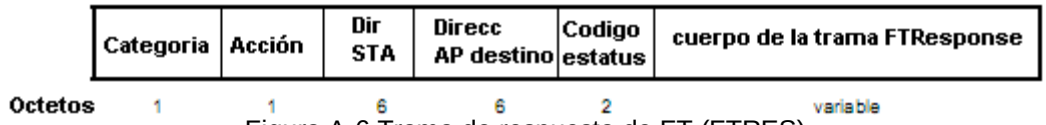

Figura A-6 Trama de respuesta de FT (FTRES).

Como dato adicional tiene el campo `código de estatus`. Algunos de los valores que puede tomar este campo y sus definiciones son: 28= R0KH inalcanzable, 52= conteo invalido de la trama FT, 53= PMKID inválido, 54= MDIE inválido o 55= FTIE inválido. Si el valor de este campo es 0, quiere decir que la trama es válida y en el cuerpo de la trama se introducen los valores de los elementos de información RSNIE, MDIE y FTIE, para continuar con el intercambio

3. Trama de confirmación FT: esta trama de confirmación FT le confirma al AP destino la recepción del *Anonce* y la presencia activa de la PTKSA. También se puede utilizar para hacer una petición de recursos esto en el caso del protocolo FT con petición de recursos el cual está fuera de este análisis. En la Figura A-7 [1] se detalla la trama FTC.

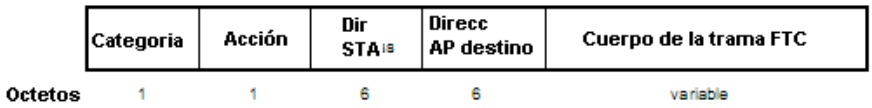

Figura A-7 Trama de confirmación FT.

En el campo `Categoría` está el valor de las tramas de acción, en el campo `Acción` está el valor de FTC, en el campo de dirección STA, está la dirección MAC de la STA, en `dirección AP destino` está el BSSID del AP destino, y en `Cuerpo de la trama` van los IEs siguientes, RSNIE, MDIE, FTIE y adicionalmente está el RDIE el cual se usa con el protocolo de petición de recursos el cual no es tratado en este estudio.

4. Trama FT de ACK: esta trama es transmitida por el AP en el cual la STA está actualmente asociada como respuesta a la trama de confirmación FT. La trama en detalle se puede observar en la Figura A-8 [1].

	Categoria	Acción	Dir STA^{ss}	Direcc AP destino	Código estatus	Cuerpo de la trama FTA
Octetos	1	1	6	6	2	variable

Figura A-8 Trama FT ACK.

El campo `Categoría` se establece en el valor de tramas de acción, el campo de `Acción` corresponde al valor de FT ACK, el campo `dir STA` es la dirección de la STA, el campo `dirección AP destino` es el BSSID del AP destino, el campo `código de estatus` se define igual que en el mensaje 2 FT *Response*, y también como en el FT *Response* si el valor del código de estatus es 0, el `Cuerpo de la trama` tiene los valores de RSNIE, MDIE, FTIE, RDIE y trae como IE adicional el TIE, el cual está presente si se solicitaron recursos en la trama FTC y contiene el tiempo límite de reasociación.

Una vez explicadas las tramas de acción FT las cuales son fundamentales para el entendimiento del protocolo ODSFTP, se procede con el protocolo en sí.

En la Figura A-9 [1] se aprecia la secuencia o pasos para llevar a cabo el protocolo FT con el método llamado “sobre el sistema de distribución”.

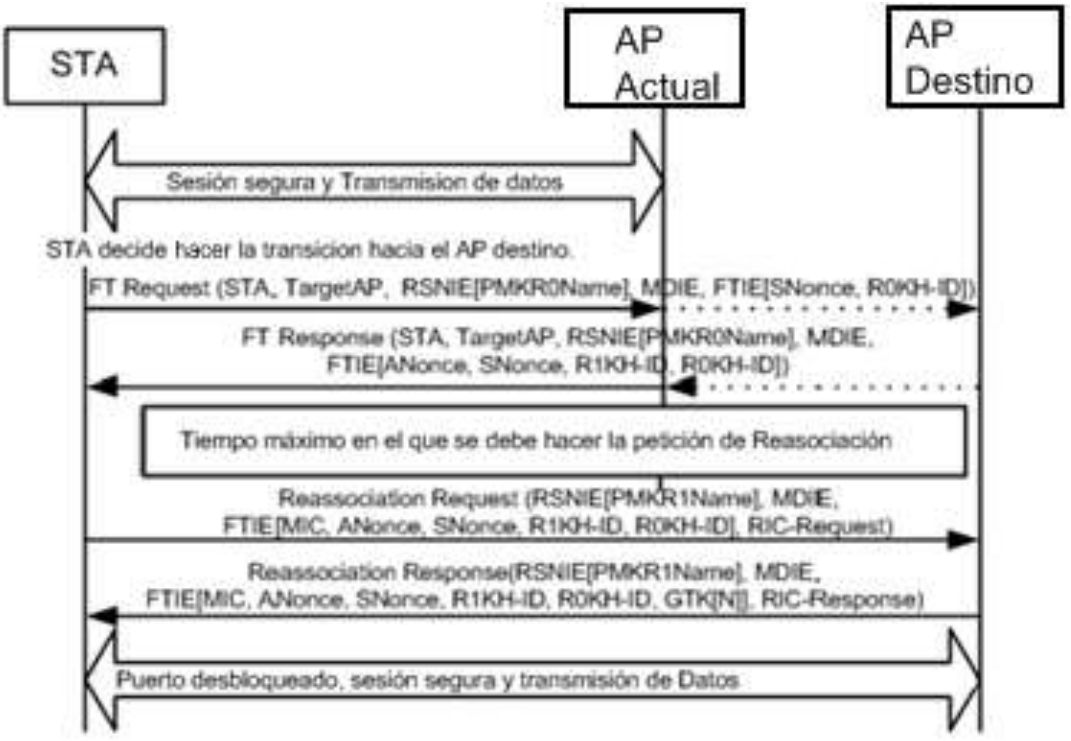

Figura A-9 Protocolo FT sobre el DS.

Para lograr una ODSFT hacia un AP destino, la estación y el AP destino deben realizar un intercambio de mensajes a través del actual AP utilizando tramas de acción las cuales se definieron con este fin específico. Antes de iniciarse el proceso se puede

observar que la STA tiene una sesión segura para la transmisión de datos con el AP actual, luego el AP mediante los algoritmos apropiados decide que debe hacer la transición hacia el AP destino, es en este momento donde empieza la secuencia FT.

El primer mensaje es enviado desde la STA hacia el AP destino, este mensaje es una trama de petición FT vista anteriormente, en esta trama están los valores de: dirección de la STA, el BSSID del AP destino, también está el valor de PMKR0Name, el MDID, el *Snonce* y el R0KH-ID. Si alguno de los IEs no concuerda con los anunciados previamente por el AP destino, la trama se descarta.

El segundo mensaje es la respuesta de petición FT, una vez se ha verificado que los valores de IEs del mensaje anterior sean correctos, se genera este mensaje. En el campo `dirección de STA` es la dirección MAC de la STA, y el campo `dirección de AP destino` está el BSSID del AP destino. Dentro de los valores dentro de los IEs que se envían están, PMKR0Name, MDID, *Anonce, Snonce*, R1KH-ID, R0KH-ID, y en caso de usarse el RIC *Request*, o petición de RIC. El R1KH del AP destino y la STA usan el valor de la PMK-R1, PMKR1Name, *Anonce* y *Snonce* para calcular la PTK.
Luego del mensaje 2, entra en funcionamiento la característica del valor de tiempo límite de reasociación del TIE. Este tiempo es el máximo que el AP debe esperar para recibir el tercer mensaje, el cual es la petición de reasociación, si no llega este mensaje en el tiempo estipulado, la transición rápida no se realiza. El tercer y cuarto mensaje comprenden lo que es la etapa de reasociación de la STA al AP destino.

El tercer mensaje es la petición de reasociación desde la STA hacia el AP destino. En la Figura A-9 [1] se ve como la STA entrega en el mensaje los valores de PMKR1Name, MDIE*, Anonce, Snonce*, R1KH-ID, R0KH-ID, y opcionalmente RIC *Request*. El R1KH del AP destino verifica el MIC en el mensaje para verificar que sea correcto. Si los valores del MDIE no concuerdan con los que anuncio el AP destino, el paquete de reasociación se descarta. Si los valores del FTIE de la petición de reasociación también son diferentes se rechaza la petición, así mismo con los valores del RSNIE.

Luego el cuarto mensaje es la respuesta de reasociación, el S1KH de la STA verifica que el MIC sea correcto para corroborar que el mensaje sea auténtico. Una vez la reasociación fue exitosa, la PTKSA se establece o instala, el AP destino abre el puerto controlado para la comunicación normal de la STA, ahora la STA esta autenticada y asociada con el AP destino, el cual se convierte en el AP actual, así mismo el estado con el AP anterior pasa a ser desautenticado y desasociado. También cuando se logra una reasociación exitosa, se debe eliminar las asociaciones seguras que se tenían con el AP anterior como la PTKSA. Así mismo se debe iniciar el contador del tiempo de vida de la llave PTK.

A.6 FTP CON PETICIÓN DE RECURSOS

El protocolo FT con petición de recursos es otra de las posibilidades que ofrece 802.11r, al igual que el protocolo FT, este nuevo protocolo FTRRP, es el protocolo FT con la diferencia que se agregan mensajes para poder realizar una petición de recursos al AP destino antes de hacer la transición hacia él, al igual que el FTP, éste tiene dos métodos por medio de los cuales se puede usar o implementar y son OTA y ODS. Debido a que este protocolo se usa en conjunto con el estándar IEEE 802.11e el cual se refiere a calidad de servicio y el presente trabajo de grado no revisa estos temas, por lo cual no se trata a fondo esta parte del estándar 802.11r.

REFERENCIAS BIBLIOGRÁFICAS

[1] IEEE, “802.11r-2008”, [en línea] julio 2008, Disponible en: <http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=&isnumber=4573291arnumber=4573292>[consulta septiembre 2008]