(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 400 937**

(51) Int. CI.:

H04L 12/28 (2006.01)
H04L 12/22 (2006.01)
H04W 84/12 (2009.01)
H04W 12/06 (2009.01)
H04L 29/06 (2006.01)
H04W 92/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **10.03.2003 E 03710565 (7)**

(97) Fecha y número de publicación de la concesión europea: **12.12.2012 EP 1486036**

(54) Título: **Compatibilidad entre varias normas WLAN**

(30) Prioridad:

08.03.2002 US 363326 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.04.2013

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)
SILLESKARSGATAN 47
S-421 59 V FROLUNDA, SE

(72) Inventor/es:

RYDNELL, GUNNAR;
LINDSKOG, JAN;
ROMMER, STEFAN y
JOHANSSON, PER-ERIK

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCION

Compatibilidad entre varias normas WLAN.

Campo de la Invención

La presente invención se refiere a aspectos de la seguridad en el área de las LANs Inalámbricas de acceso público (WLAN). Más específicamente, la invención atañe a la compatibilidad entre varias versiones de las normas W-LAN.

Antecedentes

La mayoría de las WLANs de acceso público actuales usa Puntos de Acceso de conformidad con la norma IEEE 802.11, en particular con la 802.11b. Una norma 802.11a más moderna ha ganado también popularidad. En lo que sigue a continuación las normas anteriores serán referidas como normas antiguas.

Una próxima versión de la norma, IEEE 802.11i se enfoca a la mejora de la Seguridad. Se ha encontrado la necesidad de disponer de una nueva estructura de seguridad que supere el bajo nivel de seguridad de la norma 802.11b, incluyendo los ya violados cifrado WEP y autenticación de la capa MAC. Por consiguiente, se incluyen un nuevo algoritmo de cifrado, AES, y un nuevo mecanismo de autenticación, basado en la autenticación mutua, señalización EAP y 802.1x en la nueva estructura de seguridad, como se describe en IEEE 802.11i.

WECA es una organización industrial para promocionar la WLAN IEEE 802.11 y para establecer requisitos de inter-operatividad para productos 802.11. WECA está también escribiendo actualmente una práctica recomendada con el objetivo de aumentar la posibilidad de movilidad entre diferentes Proveedores de Servicios de Internet Inalámbricos (WISP). Esta práctica recomendada específica una arquitectura WLAN de acceso público que se describe brevemente a continuación.

El estado actual de la técnica, como recomienda el comité WISPr de WECA, es situar la tarea de autenticación en un nodo especial de la red, una Puerta de Control de Acceso Público (PAC). Los APs están todos conectados directamente al PAC y el único acceso al resto de la red se hace a través del PAC (véase la figura 1).

Los Puntos de Acceso usan autenticación de "sistema abierto" y no cifrado cuando se comunican con las STAs. No hay por consiguiente control de acceso en los APs. La autenticación real y el control de acceso se hacen en la puerta PAC. Las credenciales de de acceso o identificación se transportan entre la STA y el PAC sobre HTTP protegidas por SSL. El proceso es el siguiente: Cuando el usuario inicia el ordenador portátil, el NIC WLAN se asocia con un AP. El usuario inicia entonces un navegador de web en la STA. El PAC intercepta cualquier petición de HTTP y envía una página web de acceso a la STA. El usuario introduce el nombre del usuario y la contraseña en la página web. El PAC verifica entonces las credenciales, por ejemplo contra un servidor de autenticación distante. Si las credenciales son correctas, el PAC comienza a hacer seguir el tráfico entre la STA y el resto de la red.

Se ha reivindicado por WECA que esto es la solución implementada por la mayoría de los WISPs actuales. Esta arquitectura ha sido también implementada en la primera publicación de la solución Inter-trabajo WLAN-GPRS de Ericsson. En esa solución, a la puerta PAC se le llama Nodo que Sirve de Acceso (ASN).

Una norma de seguridad mejorada para la 802.11 se plantea en IEEE 802.11i. Esta nueva norma posibilitará realizar una autenticación mucho mejor en el AP que la que se logra con la norma 802.11-1999. La norma IEEE 802.11i usará IEEE 802.1X y la EAP como estructura de seguridad. Esto significa que ya no hay necesidad de una identificación de acceso basado en web en una puerta PAC, una solución satisfactoria se que puede conseguir precisamente con APs y STAs conformes con 802.11i-cualificada. La norma IEEE 802.11i especifica también algoritmos mejorados de cifrado cuya operación está íntimamente ligada al procedimiento de autenticación 802.1X.

Un problema en la seguridad tiene lugar cuando se mezcla equipo antiguo, es decir ejemplo, un equipo conforme con cualquier norma existente, con un equipo conforme a la norma 802.11i en la misma célula. El problema es simplemente de responsabilidad distribuida. De acuerdo con el modelo de referencia WECA para las redes WLAN antiguas, el PAC será responsable de autenticar las STAs antiguas, mientras que el propio AP, de acuerdo con el modelo IEEE 802.11i, será responsable de la autenticación de las nuevas STAs 802.11i. El filtrado y el control de acceso se hacen por ello en dos lugares de la red. Esta arquitectura puede facilitar el acceso a usuarios fraudulentos que indiquen al AP que es una STA antigua, mientras que al mismo tiempo indican al PAC que es una nueva STA habilitada por 802.11i. Se aprecia que esta STA puede estar accediendo al sistema sin ninguna autenticación en absoluto.

El documento EP1081895 según la técnica anterior describe una red que comprende una LAN (red de área local) a la cual están conectados un cierto número de puntos de acceso (APs). La LAN está conectada a un servidor de autenticación, un encaminador con cortafuegos interno, una VPN (red privada virtual) para acceso distante y un encaminador con cortafuegos externo que se conecta a Internet. Se proporcionan dispositivos de autenticación (tales como tarjetas inteligentes) tanto en los APs como en los dispositivos inalámbricos que se comunican con los APs.

El servidor de autenticación trabaja en combinación con los APs y los dispositivos inalámbricos y sus respectivos dispositivos de autenticación para permitir el acceso sólo a aquellos autorizados por los administradores de las redes. Un operador habilita un canal aéreo de comunicación entre el dispositivo inalámbrico y el AP, durante el cual se intercambia un mecanismo de cifrado para la comunicación futura.

El dispositivo inalámbrico determina si el AP es un punto de acceso valido analizando un mensaje de autenticación. Si no es valido, se inhabilita el canal aéreo de comunicaciones entre el dispositivo inalámbrico y el AP. Si el AP es válido, un segundo dispositivo de autenticación en el dispositivo inalámbrico genera una clave de identificación que implica un nombre de acceso y una contraseña para un operador. El AP analiza una parte descifrada del segundo mensaje de autenticación para determinar si el dispositivo inalámbrico es válido. Si es válido, el AP habilita un canal de control con el servidor de autenticación. El servidor de autenticación verifica el nombre de acceso y la contraseña del operador. Si no es válido, el servidor de autenticación rechaza el acceso a la LAN cableada.

El documento WO0143467 según la técnica anterior muestra una red inalámbrica que comprende un servidor de comunicación inalámbrica, un interruptor que se conecta a Internet y una pluralidad de puntos de mini-acceso conectados por cable, usando protocolos existentes, tales como Ethernet, para conectar al servidor de comunicación inalámbrica.

El servidor de comunicación inalámbrica controla los puntos de mini-acceso y filtra el tráfico innecesario y envía los datos relevantes a los puntos correctos de mini-acceso. Además, el servidor inalámbrico incluye la gestión del punto de mini-acceso, seguridad QoS, etc.
Los puntos de mini-acceso son dispositivos simples, que raramente necesitan actualización, y que sólo se requieren para recibir datos o información de la gestión del receptor y enviar los datos al servidor inalámbrico. No se necesita que los puntos de mini-acceso examinen los datos para determinar adonde enviarlos. El filtrado en el servidor inalámbrico se basa en la identificación de la unidad distante, por lo cual se usa la dirección de la unidad distante.

El documento WO0203730 según la técnica anterior muestra una disposición que comprende un terminal móvil que comprende a su vez una tarjeta SIM (Módulo de Identidad de Abonado) de GSM y un interfaz 802.11 WLAN (LAN inalámbrica) para comunicarse con un AP. El terminal móvil puede habilitar una red ad hoc con otros terminales móviles equipados con WLAN, así como con una red WLAN que comprenda un acceso a Internet a través de un controlador de acceso público (PAC) que controla el acceso a Internet. El terminal móvil puede acoplarse a la red de telefonía móvil que comprende entidades GSM (Sistema Global para Comunicaciones con Móvil) tales como un MSC/VLR (centro de Conmutación móvil/registro de lugares de visita) y una entidad para proporcionar la autenticación desde un terminal móvil equipado con WLAN a través de Internet por medio de la conocida señalización GSM a un Registro de Lugares de Origen (HLR) GSM para autenticar el módulo SIM.

Sumario de la Invención

Un primer objetivo es proporcionar un punto de acceso que proporcione autenticación y quizás a las estaciones móviles antiguas IEEE 802.11 WLAN además de proporcionar acceso a estaciones móviles IEEE 802.11i de manera segura y fiable.

Este objetivo se consigue por medio del contenido definido en las reivindicaciones 1 y 10.

Ventajas adicionales aparecerán a partir de la siguiente descripción detallada de la invención.

Breve descripción de las figuras

La figura 1 muestra una arquitectura conocida que incluye una puerta de acceso público que proporciona autenticación basada en WEP y que la filtra si la autenticación proporcionada no resulta aprobada.

La figura 2 muestra una arquitectura de red de acuerdo con una primera alternativa de una primera realización de invención, que incluye una puerta de Control de Acceso Público (PAC).

La figura 3 muestra un diagrama de flujo para un Punto de Acceso (AP) de una primera alternativa de una primera realización de acuerdo con la invención, residiendo el Punto de Acceso (AP) en una arquitectura de red como se muestra en la figura 2.

La figura 4 muestra aspectos del protocolo de señalización relativo a una estación antigua, el AP y a la Puerta de Control de Acceso Público (PAC) asociados, de acuerdo con la primera alternativa de una primera realización de la invención, operando el Punto de Acceso (AP) como se muestra en la figura 3.

La figura 5 muestra aspectos del protocolo de señalización relativo a una estación 802.11i, el AP y la Puerta de Control de Acceso Público (PAC) asociados, de acuerdo con la primera alternativa de la primera realización de la invención, operando el Punto de Acceso (AP) como se muestra en la figura 3.

La figura 6 muestra un diagrama de flujo para un punto de acceso de una segunda alternativa de una primera realización de la invención, residiendo el Punto de Acceso (AP) en una arquitectura de red como se muestra en la figura 1.

La figura 7 muestra aspectos del protocolo de señalización relativo a una estación antigua, el Punto de Acceso (AP) y la puerta de Control de Acceso Público (PAC) asociados, de acuerdo con la segunda

alternativa de la primera realización de la invención, operando el Punto de Acceso (AP) como se muestra en la figura 5, y

La figura 8 muestra aspectos del protocolo de señalización relativo a una estación 802.11i, el Punto de Acceso (AP) y la Puerta de Control de Acceso Público (PAC) asociados, de acuerdo con la segunda alternativa de la primera realización de la invención, operando el Punto de Acceso (AP) como se muestra en la figura 5.

Descripción detallada de las realizaciones preferidas de la Invención

Primera realización de la Invención

Se proporciona un nuevo protocolo de señalización entre un AP y un PAC de acuerdo con la primera realización de la invención.

En esta solución, el PAC realiza la identificación web y los APs implementan la funcionalidad 802.11i, de acuerdo con la arquitectura de referencia recomendada por WECA e IEEE. Se pueden autenticar tanto las STAs antiguas como las 802.11i. Las STAs antiguas se autentican sobre el interfaz web contra la puerta PAC y las STAs 802.11i-cualificadas se autentican usando EAP y 802.1X en el AP. La autenticación se realiza usualmente contra un servidor en el extremo trasero (un servidor AAA) y es sólo la función de control de acceso la que se realiza por medio del AP y el PAC, respectivamente. Nosotros, sin embargo, no nos ocuparemos de los detalles correspondientes a un servidor potencial AAA, ya que es la función de control de acceso la que es el centro de esta realización. La autenticación contra un servidor AAA es una implementación posible.

Con objeto de coordinar los aparatos de estado del control de acceso en el AP y en el PAC se tiene que introducir un nuevo protocolo de señalización entre AP y PAC. Existen diversas alternativas posibles:

Primera alternativa de la primera realización

En esta solución el PAC es el responsable de la identificación web, pero, por lo demás, es completamente transparente. El AP, por otra parte, filtra todos los marcos a/desde las STAs no autenticadas y enviará sólo los marcos de las STAs autenticadas.

Si una STA 802.11i-cualificada se asocia con el AP y realiza una autenticación satisfactoria 802.1X, el AP comienza a enviar marcos a/desde esta STA.

Si una STA antigua se asocia con el AP, el PAC tiene que autenticarla. El AP enviará marcos desde la STA al PAC de un modo reconocible y preferentemente seguro. El AP podría por ejemplo encapsular los marcos en un túnel IPSec al PAC. El AP y el PAC podrían también compartir un código secreto que el AP usara para cifrar y autenticar cada marco. En cualquier caso, el PAC puede reconocer estos paquetes como tráfico procedente de una STA no autenticada. El PAC puede entonces procesar esto paquetes. Si los paquetes contienen por ejemplo peticiones DHCP o peticiones HTTP para la página web de identificación, el PAC responde a las peticiones mientras que otros paquetes se rechazan. Cuando se completa satisfactoriamente la identificación web, el PAC envía un mensaje especial al AP diciéndole que la STA ha sido autenticada y que el AP puede iniciar el envío de tráfico a/desde la STA sin encapsularlo de ningún modo especial.

Una ventaja de esta solución es que se puede flexibilizar la arquitectura de la red; no todo el tráfico tiene que pasar a través del PAC. En su lugar, el PAC podría ser cualquier tipo de PC con un servidor HTTP/SSL (véase el ejemplo en la figura 2).

De acuerdo con la etapa 3-1 en la figura 3, el AP recibe un mensaje desde el AP, etapa 3-1, en la cual el AP determina si la estación es una estación antigua o una estación 802.11i, etapa 3-2.

Como se ilustra la figura 4, el antiguo procedimiento normal para asociación y autorización se efectúa permitiendo que la estación se comunique con el AP. Esto se ha mostrado por medio de la etapa 3-3 en la figura 3.

Cualquier mensaje procedente de la estación en cuestión generará el siguiente mensaje AP-PAC_data_ind desde el AP hacia el PAC, indicando al PAC que la estación necesita autenticación antes que el PAC.

Con objeto de realizar la identificación, se puede ajustar un temporizador de PAC en el AP y el tráfico se envía a y desde el PAC usando por ejemplo una encapsulación AP_PAC, etapa 3-5.

El PAC, por su parte, transmite una página de Identificación basada en WEB al AP, que es enviada a la estación. El usuario de la estación puede entonces proporcionar las credenciales de acuerdo con el procedimiento normal para la identificación, por ejemplo, un código PIN secreto.

El PAC responde con un mensaje AP_PAC_add_req, etapa 3-7, informando de si el PAC ha aceptado o excluido la estación. Si la estación resulta autenticada, etapa 3-8, el PAC "abre el interruptor" en el AP, y permite que el tráfico de la estación pase sin filtrar.

Si el procedimiento de identificación no se pudo completar dentro del tiempo límite indicado de acuerdo con el ajuste de tiempo del PAC y con la comprobación de acuerdo con la etapa 3-6, el AP paraliza la transferencia de tráfico desde la estación en particular.

Si- en lugar de una estación antigua- se detecta una estación 802.11i en la etapa 3-2, la estación antigua se asocia y se autentica con el AP de acuerdo con los procedimientos ordinarios de 802.11i, como se muestra en la figura 5, el AP "abre el interruptor" y envía cualquier tráfico. No se necesita ningún mensaje AP_PAC antes del PAC. Estas etapas se han mostrado en las etapas 3-4 y 3-9 en la figura 3.

Segunda alternativa de la primera realización

En esta solución, el filtrado de tráfico no autenticado es realizado por el PAC y no por el AP. Si el AP recibe un marco no destinado a él, él siempre hace seguir el marco. Este entonces llega al PAC para filtrar los cuadros no autenticados y para realizar el procedimiento de identificación web. Para ese propósito, se elige una arquitectura de acuerdo con la figura 1.

En la figura 6 se ha mostrado este procedimiento, por medio del cual, en la etapa 6-1, el AP recibe un mensaje procedente de una nueva estación y en la etapa 6-2 el AP determina si se encuentra una estación antigua o una estación 802.11i.

Si una STA 802.11i-cualificada envía marcos EAP destinados al AP, el AP los procesa (posiblemente enviándolos a un servidor AAA) y realiza el procedimiento de autenticación 802.1X, véase la etapa 6-4 en la figura 6. Si el procedimiento es satisfactorio, el AP envía un mensaje especial al PAC, etapa 6-9, indicando que la STA ha sido autenticada y que el PAC debe iniciar el envío de los marcos a/desde esta STA. Este mensaje se debe enviar preferiblemente de un modo seguro.

Si - al contrario - una antigua STA se asocia con el AP, como se ilustra en la figura 8, el AP realiza el procedimiento normal antiguo de asociación y de autenticación, etapa 6-3. Al mismo tiempo, un temporizador de PAC se ajusta en el AP con el mismo propósito que se ha expuesto anteriormente. El AP continúa enviando tráfico a y desde esta estación, etapa 6-5. Si durante este tiempo, la estación envía cualquier mensaje al PAC, el PAC responde con la devolución de la página de identificación web a la estación. Si se recibe una contraseña correcta en el PAC procedente de la estación, el PAC abre el interruptor en el PAC. Si, al contrario, se recibe una contraseña errónea, el PAC cierra el interruptor y transmite un mensaje AP_PAC_remove_req al AP, etapa 6-7, efectuando una detención de la transferencia de tráfico a la AP en cuestión entre el AP y el PAC y efectúa una desconexión de la estación antes del AP, etapa 6-10.

Tercera alternativa de la primera realización

De acuerdo con la tercera alternativa de la primera realización, el filtrado lo realizan tanto el AP como el PAC.
Esta solución es una combinación de las soluciones anteriores. Con objeto de transferir tráfico desde una STA, tanto el AP como el PAC deben enviar el marco.

En conclusión, la invención describe una nueva solución para el bien conocido problema de la seguridad en las WLANs 802.11. El método es compatible con protocolos normalizados por IEEE y WECA, pero va un paso más allá y específica un nuevo protocolo entre los nodos de red en la arquitectura de referencia WECA. Más aún, se describen 3 métodos alternativos, incluyendo modificaciones para la arquitectura de seguridad descritas por la arquitectura de referencia WECA.

Un mecanismo, tal como se describe aquí, será necesario con objeto de proporcionar una red WLAN segura cuando equipos con 802.11i comiencen a aparecer en el mercado. No es que se haya inventado un nuevo mecanismo de autenticación; la autenticación de una STA se hace usando los métodos de autenticación WECA e IEEE. La invención resuelve el problema de la responsabilidad distribuida, uniendo conjuntamente los protocolos de seguridad WECA e IEEE y sincronizando la información de seguridad en los nodos fijos en la columna vertebral de una red WLAN.

REIVINDICACIONES

1. Un punto de acceso (AP) capaz de realizar asociación y autenticación tanto de normas antiguas como de normas 802.11i, comprendiendo el punto de acceso medios adaptados para:

- si se encuentra (3-2; 6-2) una estación 802.11i (STA), realizar la asociación y la autenticación de 802.11i y si son satisfactorias (3-4), el punto de acceso hace que se envíen marcos a/desde la estación (3-9; 6-9),
- si se encuentra (3-2; 6-2) una estación antigua (STA), el punto de acceso está adaptado para:

  - realizar la asociación y autenticación (3-3; 6-3) del control de acceso de los medios antiguos y
  - si son satisfactorias, el punto de acceso está adaptado para continuar enviando tráfico a la estación a y desde una puerta de control de acceso público (PAC) (3-5; 6-5), permitiendo que esta puerta de control de acceso público (PAC) transmita una página de identificación basada en web a la estación antigua,
  - si la estación no es autenticada (3-8; 6-7) por la puerta de control de acceso público, el punto de acceso esta adaptado para detener (3-10; 6-10) la transferencia de tráfico a la estación entre el punto de acceso y la puerta de control de acceso público (PAC).

2. Un punto de acceso de acuerdo con la reivindicación 1, en el que la autenticación por medio de la puerta de acceso de control público se establece como satisfactoria si se recibe un mensaje (AP_PAC_add_req) desde la puerta de control de acceso público (3-7) que indica que la estación es autenticada (3-8) por la puerta de control de acceso público.

3. Un punto de acceso (AP) de acuerdo con la reivindicación 1 o con la reivindicación 2, que cuando realiza la asociación y la autenticación antiguas, el punto de acceso está adaptado para:

- ajustar un temporizador (3-3) en la puerta de control de acceso público (PAC)) y si el tiempo no ha transcurrido (3-6), enviar el tráfico (3-5) a y desde una puerta de control de acceso público (PAC) usando encapsulación (AP- PAC),
- si el tiempo ha transcurrido (3-6), detener (3-10) la transferencia de tráfico desde la estación entre el punto de acceso y la puerta de control de acceso público (PAC).

4. Un punto de acceso de acuerdo con cualquiera de las reivindicaciones precedentes, en el que el envío del tráfico (3-5) a y desde una puerta de control de acceso público (PAC), que permite que la puerta de control de acceso público (PAC) transmita una página de identificación basada en web a la estación antigua (*p.4, line 3-4*), se realiza usando encapsulación (AP-PAC), y en el que si la estación es autenticada por la puerta de control de acceso público (PAC), el punto de acceso se adapta para reenviar tráfico a y desde la estación sin encapsulación.

5. Un punto de acceso de acuerdo con cualquiera de las reivindicaciones precedentes, en el que el punto de acceso comprende un interruptor de 802.1X que se abre (3-9) tras la autenticación por medio de la puerta de acceso público (PAC) de forma que envíen marcos a y desde la estación.

6. Un punto de acceso de acuerdo con la reivindicación 1, en el cual el tráfico se detiene entre el punto acceso y la puerta de control de acceso público (6-10), si se recibe (6-7) un mensaje (AP_PAC_remove_req) desde la puerta de control de acceso público (PAC), que indica que la estación no está autenticada por la puerta de control de acceso público.

7. Un punto de acceso de acuerdo con la reivindicación 6, en el que:

-si se encuentra un estación 802.11i y si una asociación y una autenticación 802.11i de la estación son satisfactorias (6-4), se transmite (6-9) un mensaje (AP_PAC_ADD_REQ) a la puerta de control de acceso público (PAC) indicativo de que la puerta de control de acceso público debe abrir un interruptor 802.1X para la estación en la puerta de control de acceso público (PAC).

8. Un punto de acceso de acuerdo con la reivindicación 6 o con la reivindicación 7, en el que si se recibe un mensaje indicativo de identificación no satisfactoria (6-7) desde la puerta de control de acceso público (PAC), se desvincula además (6 –10) la estación en cuestión.

9. Un punto de acceso de acuerdo con cualquiera de las reivindicaciones precedentes, en el que el punto acceso está adaptado para usar autenticación 802. 1X en el punto acceso (3-4) para autenticar una estación 802.11i cualificada.

10. Un método para que un punto de acceso (AP) sea capaz de realizar la asociación y la autenticación tanto de una estación antigua como de una estación 802.11i, que comprende las etapas de:

- si se encuentra (3-2; 6-2) una estación 802.11i (STA), realizar la asociación y la autenticación de 802.11i y, si son satisfactorias (3-4), el punto de acceso hace que los marcos se envíen a/desde la estación (3-9; 6-9),
- si se encuentra (3-2; 6-2) una estación antigua (STA),

- realizar la asociación y autenticación (3-3; 6-3) de control de acceso de medios antiguos y
- si son satisfactorias, continuar enviando tráfico a la estación a y desde una puerta de control de acceso público (PAC) (3-5; 6-5), permitiendo que la puerta de control de acceso público (PAC) transmita una página de identificación basada en web a la estación antigua,
- si la estación no es autenticada (3-8; 6-7) por la puerta de acceso de control público, detener (3-10; 6-10) la transferencia de tráfico a la estación entre el punto de acceso y la puerta de control de acceso público (PAC).

11. Un método de acuerdo con la reivindicación 10, en el que la autenticación por la puerta de control de acceso público se establece como satisfactoria si se recibe un mensaje (AP_PAC_add_req) de la puerta de control de acceso público (3-7) de que la estación resulta autenticada (3-8) por la puerta de control de acceso público.

12. Un método de acuerdo con la reivindicación 10 o con la reivindicación 11, que cuando se realiza la asociación y autenticación antiguas, comprende

- establecer un temporizador (3-3) en la puerta de control de acceso público (PAC) y si el tiempo no ha transcurrido (3-6), enviar tráfico (3-5) a y desde una puerta de control de acceso público (PAC) usando encapsulación (AP-PAC),
-si el tiempo ha transcurrido (3-6), detener (3-10) la transferencia del tráfico desde la estación entre el punto de acceso y la puerta de control de acceso público (PAC).

13. Un método de acuerdo con cualquiera de las reivindicaciones 10-12, en el que el envío de tráfico (3-5) a y desde una puerta de control de acceso público (PAC) que permite que la puerta de control de acceso público (PAC) transmita una página de identificación basada en web a la estación antigua se realiza usando encapsulación (AP-PAC), y en el que si la estación es autenticada por la puerta de control de acceso público (PAC), enviando el tráfico a y desde la estación sin encapsulación.

14. Un método acuerdo con la reivindicación 10, en el que se detiene el tráfico entre el punto acceso y la puerta de control de acceso público (6-10), si se recibe (6-7) un mensaje (AP_PAC_remove_req) desde la puerta de control de acceso público (PAC), indicando el mensaje que la estación no ha sido autenticada por la puerta de control de acceso público.

15. Un método de acuerdo con la reivindicación 14, en el que

- si se encuentra una estación y si una asociación y una autenticación 802.11i de la estación es satisfactoria (6-4), se transmite (6-9) un mensaje (AP_PAC_ADD_REQ) a la puerta de control de acceso público (PAC) indicativo de que la puerta de control de acceso público debe abrir un interruptor 802.1X en la estación en la puerta de control de acceso público (PAC).

16. Un método acuerdo con la reivindicación 14 o con la reivindicación 15, en el que si se recibe un mensaje indicativo de identificación no satisfactoria (6-7) desde la puerta de control de acceso público (PAC), se desvincula (6-10) además la estación en cuestión.

17. Un método de acuerdo con cualquiera de las reivindicaciones precedentes 10-16, en el que una estación 802.11i cualificada es autenticada usando la autenticación 802. 1X en el punto acceso (3-4).

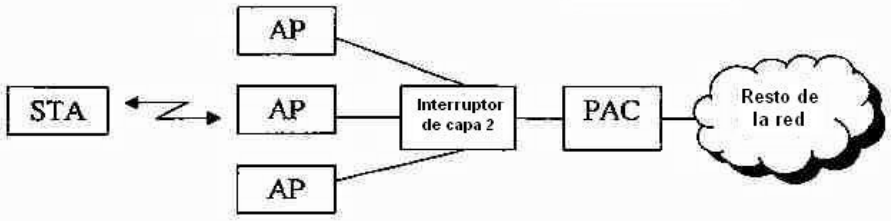
AP
STA
AP
Interruptor de capa 2
PAC
Resto de la red
AP

Fig. 1

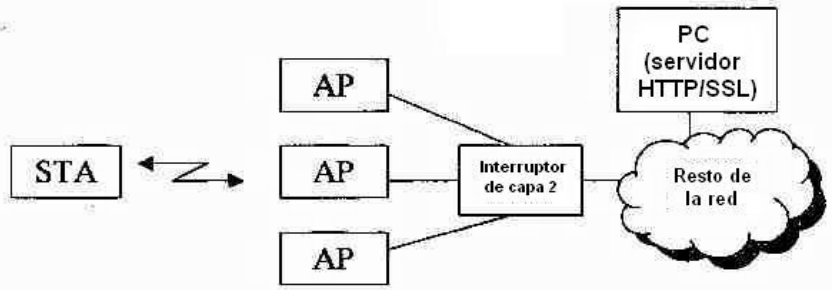
PC (servidor HTTP/SSL)
AP
STA
AP
Interruptor de capa 2
Resto de la red
AP

Fig. 2

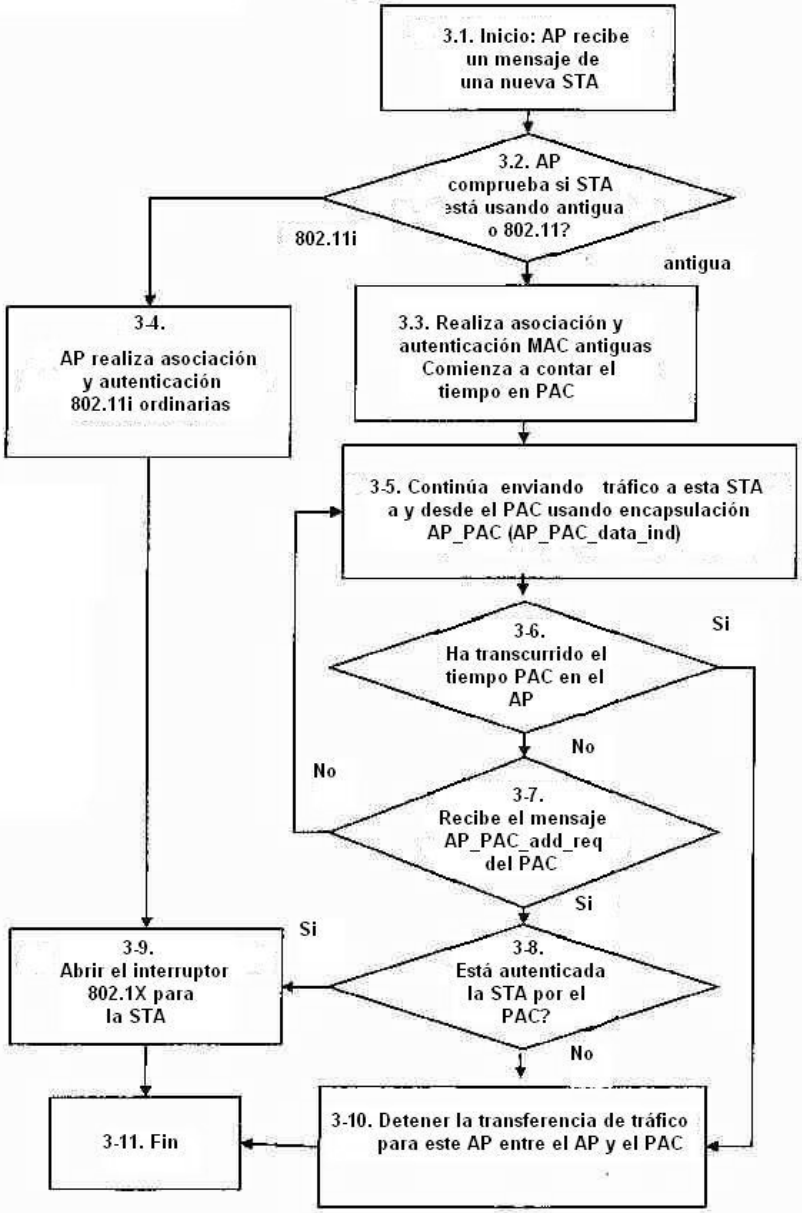
3.1. Inicio: AP recibe un mensaje de una nueva STA
3.2. AP comprueba si STA está usando antigua o 802.11?
802.11i
antigua
3-4. AP realiza asociación y autenticación 802.11i ordinarias
3.3. Realiza asociación y autenticación MAC antiguas Comienza a contar el tiempo en PAC
3-5. Continúa enviando tráfico a esta STA a y desde el PAC usando encapsulación AP_PAC (AP_PAC_data_ind)
3-6. Ha transcurrido el tiempo PAC en el AP
Si
No
No
3-7. Recibe el mensaje AP_PAC_add_req del PAC
Si
Si
3-9. Abrir el interruptor 802.1X para la STA
3-8. Está autenticada la STA por el PAC?
No
3-11. Fin
3-10. Detener la transferencia de tráfico para este AP entre el AP y el PAC

Fig. 3

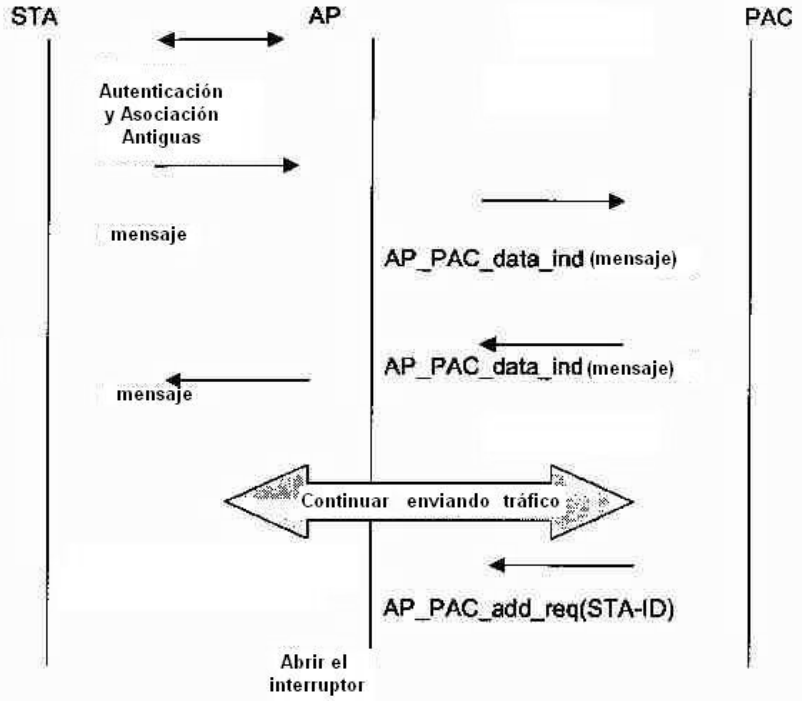
STA
AP
PAC
Autenticación y Asociación Antiguas
mensaje
AP_PAC_data_ind (mensaje)
AP_PAC_data_ind (mensaje)
mensaje
Continuar enviando tráfico
AP_PAC_add_req(STA-ID)
Abrir el interruptor

Fig. 4

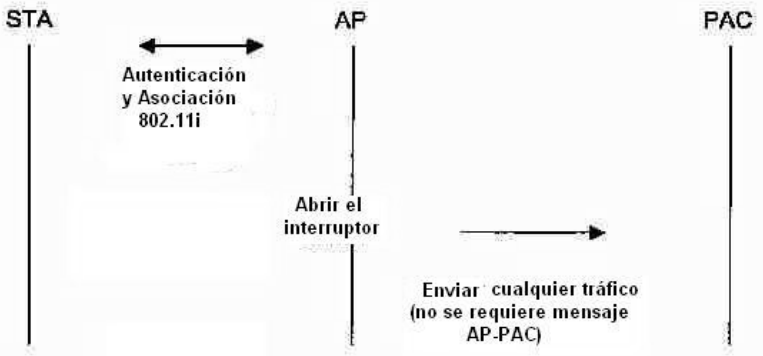
STA
AP
PAC
Autenticación y Asociación 802.11i
Abrir el interruptor
Enviar cualquier tráfico (no se requiere mensaje AP-PAC)

Fig. 5

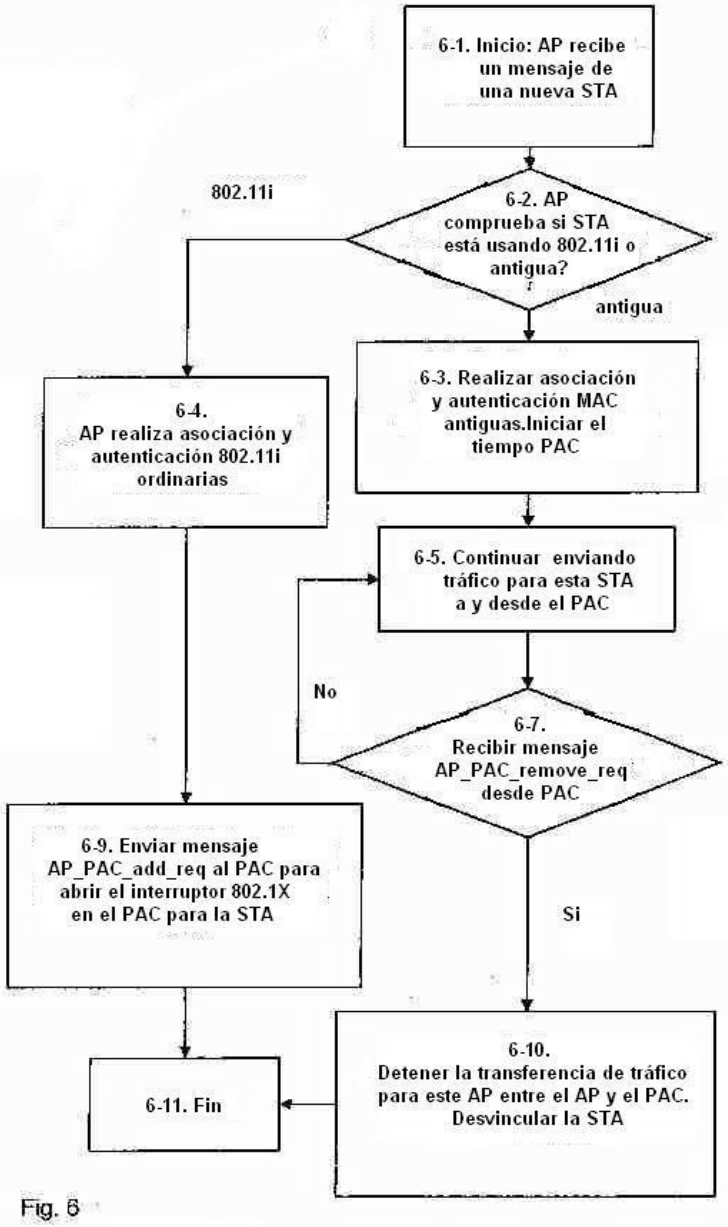
6-1. Inicio: AP recibe un mensaje de una nueva STA
802.11i
6-2. AP comprueba si STA está usando 802.11i o antigua?
antigua
6-3. Realizar asociación y autenticación MAC antiguas.Iniciar el tiempo PAC
6-4. AP realiza asociación y autenticación 802.11i ordinarias
6-5. Continuar enviando tráfico para esta STA a y desde el PAC
No
6-7. Recibir mensaje AP_PAC_remove_req desde PAC
Si
6-9. Enviar mensaje AP_PAC_add_req al PAC para abrir el interruptor 802.1X en el PAC para la STA
6-10. Detener la transferencia de tráfico para este AP entre el AP y el PAC. Desvincular la STA
6-11. Fin

Fig. 6

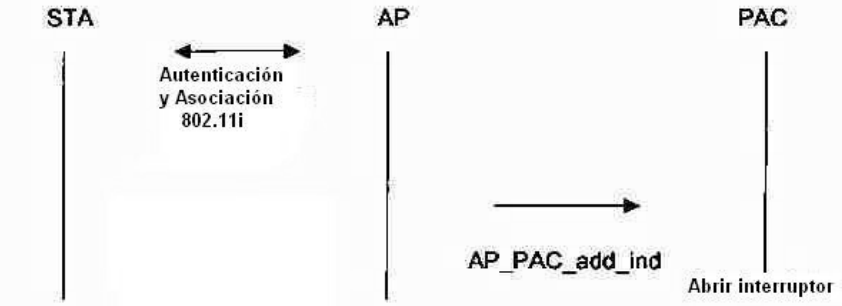
STA
AP
PAC
Autenticación
y Asociación
802.11i
AP_PAC_add_ind
Abrir interruptor

Fig. 7

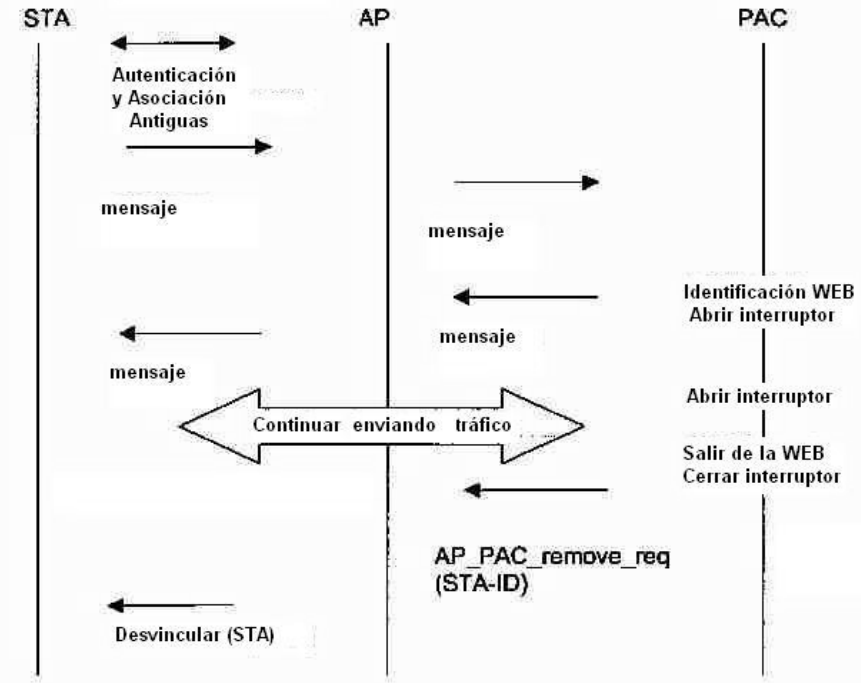
STA
AP
PAC
Autenticación
y Asociación
Antiguas
mensaje
mensaje
Identificación WEB
Abrir interruptor
mensaje
mensaje
Abrir interruptor
Continuar enviando tráfico
Salir de la WEB
Cerrar interruptor
AP_PAC_remove_req
(STA-ID)
Desvincular (STA)

Fig. 8