(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 June 2014 (19.06.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/090622 A1

(51) International Patent Classification:
*H04L 12/24* (2006.01)

(21) International Application Number:
PCT/EP2013/075248

(22) International Filing Date:
2 December 2013 (02.12.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
12306562.5 11 December 2012 (11.12.2012) EP

(71) Applicant: **THOMSON LICENSING** [FR/FR]; 1-5 rue Jeanne d'Arc, F-92130 Issy-les-Moulineaux (FR).

(72) Inventors: **VAN OOST, Koen**; Eenamelaan 17, B-2150 Borsbeek (BE). **VERWAEST, Frederik**; Hemelrijkstraat 5, B-2400 Mol (BE).

(74) Agent: **SCHMIDT-UHLIG, Thomas**; Deutsche Thomson OHG, European Patent Operations, Karl-Wiechert-Allee 74, 30625 Hannover (DE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,

*[Continued on next page]*

# (54) Title: AUTOMATIC RECONFIGURATION OF NETWORK DEVICES

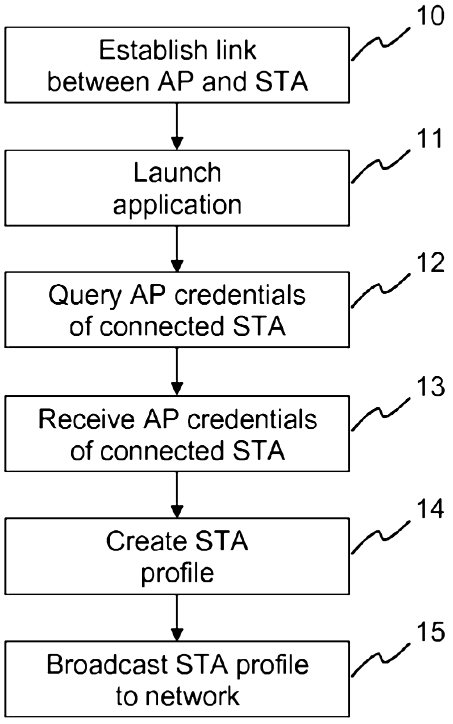
10
Establish link between AP and STA
11
Launch application
12
Query AP credentials of connected STA
13
Receive AP credentials of connected STA
14
Create STA profile
15
Broadcast STA profile to network

**Fig. 4**

**(57) Abstract**: A solution for automatic reconfiguration of network devices adapted to switch from the role of access point to the role of station and vice versa is described. In order to prepare a first network device (AP, STA1, STA2) for automatic configuration in the network, a profile of a second network device (AP, STA1, STA2) connected to said first network device (AP, STA1, STA2) via a network is received (13, 22). The profile comprises access point credentials of the second network device (AP, STA1, STA2). The received profile is compared (23) with existing profiles stored in a memory (43) of said first network device (AP, STA1, STA2) and is stored (14, 24) in said memory (43), if necessary. In case at a later time a role change of the first network device (AP) is determined (30), the stored profile is retrieved (31) from the memory (43) and used for connecting (32) the first network device (AP) to the second network device (AP(2)).

WO 2014/090622 A1

EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

**Published**:

— *with international search report (Art. 21(3))*

# AUTOMATIC RECONFIGURATION OF NETWORK DEVICES

## FIELD OF THE INVENTION

The invention relates to a solution for automatic reconfiguration of network devices adapted to operate in two different roles in a network. More specifically, the invention addresses a credential recovery and auto-provisioning mechanism, which ensures that after a reconfiguration of the network the network remains operational.

## BACKGROUND OF THE INVENTION

Today, especially due to the delivery of multimedia services over Wi-Fi, more and more equipment is being connected to the in house WLAN (WLAN: Wireless Local Area Network). However, a lot of devices do not yet have the necessary hardware "on board" to be able to connect to the WLAN, but simply connect on Ethernet. Hence there is a booming demand for Wi-Fi-to-Ethernet boxes that allow easy connection of the Ethernet devices to the WLAN. One of the reasons that a lot of devices deliberately choose not to integrate WLAN hardware is because of the high pace with which the underlying 802.11 technology is evolving. While it took 802.11bg roughly ten years to get to a mature market, 802.11n rose to popularity in three years only to be followed-up by 802.11ac in 2013. Practically this means that devices embedding Wi-Fi technology have the chance to get obsolete or at least less popular quite fast. This puts a lot of pressure on the product cost, motivating stand-alone Wi-Fi-to-Ethernet boxes.

From a production cost point of view, a device manufacturer is interested in building the most versatile product in order to spend as little as possible on hardware tooling, i.e.

production line, test software, etc., and as little as possible on logistic costs, e.g. caused by different product codes, different order numbers, software, required storage space, etc. Hence a single Wi-Fi-to-Ethernet device capable of being both AP and STA (AP: Access Point; STA: Station) is often realized, keeping production and logistic costs low. For ease of use, all devices receive AP credentials, which guaranties strong security. End users do not have to come up with clever passphrases and, through using WPS-PBC (WPS-PBC : Wi-Fi Protected Setup - 2.Push Button Configuration), do not even need to know the WPA (WPA: Wi-Fi Protected Access) passphrase of the AP. This further removes the need for any user interface on the bridge devices, reducing the complexity and cost even further.

Not having to perform a lot of networking functions, Wi-Fi-to-Ethernet boxes are deployed as 802.1d compliant bridges, forwarding packets transparently between the devices connected to the AP and devices connected to the STA.

The main problem to overcome with such Wi-Fi-to-Ethernet boxes is the configuration of the network credentials. Ideally, end-users do not have to be troubled with the configuration of those devices and should be capable of using the devices right out of the box. This implies that the out-of-the-box (OOB) settings must allow deploying a WLAN, which is commonly realized via “pre-pairing” two or more devices in production. An alternative is the usage of WPS-PBC configuration, which becomes applicable once the end user starts to expand his current WLAN.

However, problems arise when users start to physically alter the network. For example, when a user moves to a new home and does not know which box was the AP and which one was the STA.

This is an issue as there is an impact on the usable bandwidth and this could lead to not being able to connect to the WLAN anymore.

This is illustrated in Figs. 1 and 2 using a Wi-Fi LAN device as an example. In the example of Fig. 1 two STA devices STA1 and STA2 are connected to an AP, which in turn is connected to a central gateway or port of a broadband network. STA1 and STA2 have the credentials of the AP and hence are allowed on the WLAN. Because the two STA devices share the WLAN bandwidth using CSMA-CA (CSMA-CA: Carrier Sense Multiple Access with Collision Avoidance), each STA device roughly gets 50% of the available air-time, provided each is using the same PHY rate (PHY rate: Physical Layer rate).

When the end user decides to physically move the devices, the scenario can change as indicated in Fig. 2. As all the devices are generic, they all look the same. As a result the end user may unknowingly connect the devices in an incorrect way. Now the STA2 device is connected to the central gateway or port of the broadband network instead of the AP. This connection error cuts the available bandwidth to 33% per STA device. The reason of this bandwidth drop is the IEEE 802.11 infrastructure mode, which does not allow STA devices to exchange data directly with each other. Instead, all packets must go through the AP.

Thanks to the pairing or pre-pairing the Wi-Fi link will still work, but there is a substantial bandwidth loss. Note that the example given still considers equal PHY rate between the clients and the AP. If this starts to change due to external influences, e.g. fading, shadowing, interference, etc., the impact becomes a lot worse.

From the scenario in Fig. 2 it is apparent that a functional role change is required. Functional role change here means that an AP becomes an STA or an STA becomes an AP. This is needed in order to restore the air-time ratio and hence the total throughput towards a client.

A role change is by preference dynamic, e.g. using a discovery mechanism such as LLDP (LLDP: Link Layer Discovery Protocol), SSDP (SSDP: Simple Service Discovery Protocol) or even DHCP (DHCP: Dynamic Host Configuration Protocol), so that an end user is not troubled with a full, manual reconfiguration. A solution for determining a role change of network devices is described, for example, in US 7,380,025.

Fig. 3 illustrates what happens when a role change is performed. STA2 becomes a new access point AP(2) using its own set of credentials, i.e. BSSID (BSSID: Basic Service Set Identification) and WPA passphrase. The other devices can reconnect to the network, as they have been pre-paired. However, if the devices were not pre-paired, e.g. because the end user bought two separate devices, or a third device was added, or a device was replaced, the scenario of the role swap would lead to a disaster, as the other devices would not be able to reconnect to the network.

## SUMMARY OF THE INVENTION

It is an object of the present invention to propose a reliable solution for automatic reconfiguration of network devices.

According to the invention, a method for preparing a first network device for automatic configuration in a network, wherein the first network device (AP, STA1, STA2) is adapted to switch from the role of access point to the role of station and vice versa, comprises the steps of:

- receiving a profile of a second network device connected to said first network device via a network, wherein the profile of the second network device comprises access point credentials of the second network device;
- comparing the received profile with existing profiles stored in a memory of said first network device; and
- storing the profile of the second network device in the memory in case the profile is not yet stored in the memory.

Accordingly, a network device adapted to switch from the role of access point to the role of station and vice versa comprises:

- an input for receiving a profile of a second network device connected to said network device via a network, wherein the profile of the second network device comprises access point credentials of the second network device;
- a memory for storing the profile of the second network device in case the profile is not yet stored in the memory; and
- a comparator for comparing the received profile with existing profiles stored in the memory of said network device.

The invention proposes a credential recovery and auto-provisioning mechanism, which is preferably implemented as a software module included in the software running on the different network devices, namely the access point and the stations. Advantageously, the devices are provided with an auto role detection, meaning they figure out what their functional role is in the WLAN. Once this has been established, the WLAN can be set up through usage of WPS-PBC. If the WLAN is operational, loss of credentials will be countered by a software application that will retrieve the profiles, which comprise the access point credentials, of all the nodes of the network, i.e. the access point and all stations in the network.

The access point and/or the stations broadcast this info to all the nodes in the network. In this way all nodes are provided with the access point security credentials of all other nodes. This ensures that the WLAN can be restored once the devices are powered up again in a different configuration. The auto provision of the network credentials functions without interference of the end user. At the same time it is a much less costly and time consuming process than pre pairing the devices in production.

Advantageously, the access point requests each newly encountered station to send its profile. This ensures that also the access point security credentials of stations joining the network at a later time are available to all nodes.

Preferably, the profiles stored in the memory are broadcast into the network with a predetermined delay between subsequent profiles. In this way the different stations have sufficient time to process the each received profile. Otherwise further profiles might be missed by a station that is still busy with storing a previous profile.

Favorably, the step of broadcasting the profiles stored in the memory into the network is repeated after a predetermined time. In this way the profiles are also made available to a device that joined the network at a later time.

In order to reconfigure a network device after powering up again in a different configuration, a method for automatically configuring a first network device, which is adapted to switch from the role of access point to the role of station and vice versa, comprises the steps of:
- determining a role change of the first network device;

- retrieving a profile of a second network device from a memory, wherein the profile of the second network device comprises access point credentials of the second network device; and
- connecting the first network device to the second network device using the retrieved profile.

Accordingly, a network device adapted to switch from the role of access point to the role of station and vice versa comprises:
- a role detector for determining a role change of the network device;
- a memory access unit for retrieving a profile of a second network device from a memory, wherein the profile of the second network device comprises access point credentials of the second network device; and
- a network connector for connecting the network device to the second network device using the retrieved profile.

When after powering up a role change is determined, i.e. the former access point determines that it now needs to operate as a station, this station retrieves the access point security credentials of the former station that now operates as an access point from its memory. Using these credentials, the station is able to connect to the new access point.

For a better understanding the invention shall now be explained in more detail in the following description with reference to the figures. It is understood that the invention is not limited to this exemplary embodiment and that specified features can also expediently be combined and/or modified without departing from the scope of the present invention as defined in the appended claims.

## BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 shows a correctly configured network with one access point and two stations;

Fig. 2 depicts the network of Fig. 1 after exchanging the access point with one of the stations;

Fig. 3 illustrates a role change in the network of Fig. 2;

Fig. 4 illustrates a method according to the invention performed by an access point for credential retrieval and auto-provisioning,

Fig. 5 depicts a method according to the invention performed by a station for credential retrieval and auto-provisioning,

Fig 6 shows the credential retrieval and auto-provisioning mechanism in more detail,

Fig. 7 illustrates a method for reconfiguring a network using the retrieved credentials, and

Fig. 8 schematically depicts a network device according to the invention.

## DETAILED DESCRIPTION OF PREFERED EMBODIMENTS

In the following a solution according to the invention for a credential recovery and auto-provisioning mechanism is described.

Considering Fig. 1 again, the scenario illustrated in this figure is the “factory default” scenario. An end user has either received three devices that can be connected in every possible way, because they have been pre-paired, or the end user has connected the devices in a random order and has correctly established the WLAN. For example, the WLAN may have been set up using the WPS-PBC method twice, i.e. once for each station STA1, STA2.

In Figs. 4 and 5 methods according to the invention for credential retrieval and auto-provisioning performed by an access point and a station, respectively, are schematically illustrated. Fig. 6 shows the data exchange performed for credential retrieval and auto-provisioning in more detail. Once a link between the access point AP and a station STA1, STA2 is established 10, an application is launched 11 that queries 12 the access point credentials of the client STA1, STA2 that has connected to the access point AP. Preferably, the application uses either layer 2, i.e. the MAC-layer (MAC: Media Access Control), or layer 3, in the present example the IP-layer (IP: Internet Protocol), to communicate with the client STA1, STA2. At least layer 2 communication must be supported, because in a pure bridged network the access point AP and station devices STA1, STA2 do not need to receive an IP address. They need to have an IP address for WPS to work, but it does not need to be assigned by DHCP (DHCP: Dynamic Host Configuration Protocol).

The access point AP queries 12 the credentials from each connected station STA1, STA2 and, after receiving 13 the credentials, creates 14 station profiles, if such profiles are not yet available, and “broadcasts” 15 the credentials back into the network. Preferably, for the distribution of the credentials no real broadcast traffic will be used, as Wi-Fi does not guarantee reception of broadcast/multicast packets.

Instead, the application sends a broadcast frame, but the Wi-Fi MAC layer will convert it to a unicast frame that is directed to all stations STA1, STA2 that are present in the connection list of the access point AP.

Each time a new station connects to the access point AP, the access point AP queries 12 the station for its security credentials. After receiving 20 a query the station must reply 21 with a data frame containing a credential structure containing the BSSID and the WPA-PSK value (WPA-PSK: Wi-Fi Protected Access - Pre-shared key) or the WPA-key, should there be one. For this purpose a comma separated list is preferably used. The access point AP receiving 13 this info creates 14 a station profile containing the newly received information. An example of such a profile is a TR-181 / TR98 "endpoint":

| **Field** | **Value** |
|---|---|
| Device.WiFi.Endpoint.{i}.Profile.SSID | BSSID of the newly learned AP |
| Device.WiFi.Endpoint.{i}.Profile.Security.ModeEnabled | WPA2-Personal<br>WPA-WPA2-Personal |
| Device.WiFi.Endpoint.{i}.Profile.Security.PreSharedKey | WPA key of the newly learned AP |
| Device.WiFi.Endpoint.{i}.Profile.Security.KeyPassPhrase | WPA-PSK of the newly learned AP |

Once the access point AP has at least two station profiles, it starts informing the WLAN of the existing security credentials. The access point AP periodically sends 15 a profile, in a unicast data frame, to each associated device. In order to do that the access point AP is advantageously configured with two periodical inform parameters “InterProfilePeriod” and “ProfileBroadcastPeriod”. InterProfilePeriod controls the time in between the broadcast of two different profiles, e.g. two seconds. ProfileBroadcastPeriod controls the time between two subsequent broadcast cycles, e.g. one minute.

Upon reception 22 of a STA profile each station STA1, STA2 compares 23 the information with the existing information in its own data model and decides to add 24 a profile or discard 25 the info.

Once all nodes AP, STA1, STA2 of the WLAN have each other’s credentials stored in their respective data models an end user is safely allowed to disconnect the devices AP, STA1, STA2 and reconnect them in a random order. The auto role detection will guarantee that the access point AP remains connected to the gateway and that the WLAN can be set up as all nodes have the correct security credentials. A method for reconfiguring the network using the retrieved credentials is illustrated in Fig. 7. When a role change of the access pointe AP is determined 30, the profile of the new access point AP(2) is retrieved 31 from a memory. Using the credentials stored in this profile, the former access point, which no functions as a station, can connect 32 to the new access point AP(2).

Fig. 8 schematically depicts a network device 40 according to the invention. The network device 40 comprises an input 41 for receiving profiles of other network devices and a memory 43 for storing these profiles. A comparator 42 compares the received profiles with existing profiles stored in the memory 43 in order to avoid double entries in the memory. The device 40 further comprises a role detector 44 for determining a role change of the network device 40, e.g. a change from the role of “access point” to the role of “station”. In case a role change is determined, a memory access unit 45 retrieves a profile of a second network device AP(2) from the memory 43. Using the retrieved profile, a network connector 46 connects the network device AP to the second network device AP(2).

## CLAIMS

1. A method for preparing a first network device (AP, STA1, STA2) for automatic configuration in a network, wherein the first network device (AP, STA1, STA2) is adapted to switch from the role of access point to the role of station and vice versa, the method **comprising** the steps of:
   - receiving (13, 22) a profile of a second network device (AP, STA1, STA2) connected to said first network device (AP, STA1, STA2) via a network, wherein the profile of the second network device (AP, STA1, STA2) comprises access point credentials of the second network device (AP, STA1, STA2);
   - comparing (23) the received profile with existing profiles stored in a memory (43) of said first network device (AP, STA1, STA2); and
   - storing (14, 24) the profile of the second network device (AP, STA1, STA2) in the memory (43) in case the profile is not yet stored in the memory.

2. The method according to claim 1, **further** comprising the step of requesting (12) the second network device (STA1, STA2) to send its profile.

3. The method according to claim 1 or 2, **further** comprising the step of broadcasting (15) the profiles stored in the memory (43) into the network.

4. The method according to claim 3, **wherein** the profiles stored in the memory (43) are broadcast (15) into the network with a predetermined delay (InterProfilePeriod) between subsequent profiles.

5. The method according to claim 3 or 4, **wherein** the step of broadcasting (15) the profiles stored in the memory (43)

into the network is repeated after a predetermined time (ProfileBroadcastPeriod).

6. A method for automatically configuring a first network device (AP) in a network, wherein the first network device (AP) is adapted to switch from the role of access point to the role of station and vice versa, the method **comprising** the steps of:
- determining (30) a role change of the first network device (AP);
- retrieving (31) a profile of a second network device (AP(2)) from a memory (43); and
- connecting (32) the first network device (AP) to the second network device (AP(2)) using the retrieved profile.

7. The method according to claim 6, **wherein** the profile of the second network device (AP(2)) comprises access point credentials of the second network device (AP(2)).

8. The method according to claim 6 or 7, **wherein** the profile of the second network device (AP(2)) has been stored in the memory (43) using a method according to one of claims 1 to 7.

9. A network device (AP, STA1, STA2) adapted to switch from the role of access point to the role of station and vice versa, **characterized** in that the network device (AP, STA1, STA2) comprises:
- an input (41) for receiving (13, 22) a profile of a second network device (AP, STA1, STA2) connected to said network device (AP, STA1, STA2) via a network, wherein the profile of the second network device (AP, STA1, STA2) comprises access point credentials of the second network device (AP, STA1, STA2);

- a memory (43) for storing (14, 24) the profile of the second network device (AP, STA1, STA2) in case the profile is not yet stored in the memory (43); and
- a comparator (42) for comparing (23) the received profile with existing profiles stored in the memory (43) of said network device (AP, STA1, STA2).

10. A network device (AP) adapted to switch from the role of access point to the role of station and vice versa, **characterized** in that the network device (AP) comprises:
- a role detector (44) for determining (30) a role change of the network device (AP);
- a memory access unit (45) for retrieving (31) a profile of a second network device (AP(2)) from a memory (43), wherein the profile of the second network device (AP(2)) comprises access point credentials of the second network device (AP(2)); and
- a network connector (46) for connecting (32) the network device (AP) to the second network device (AP(2)) using the retrieved profile.

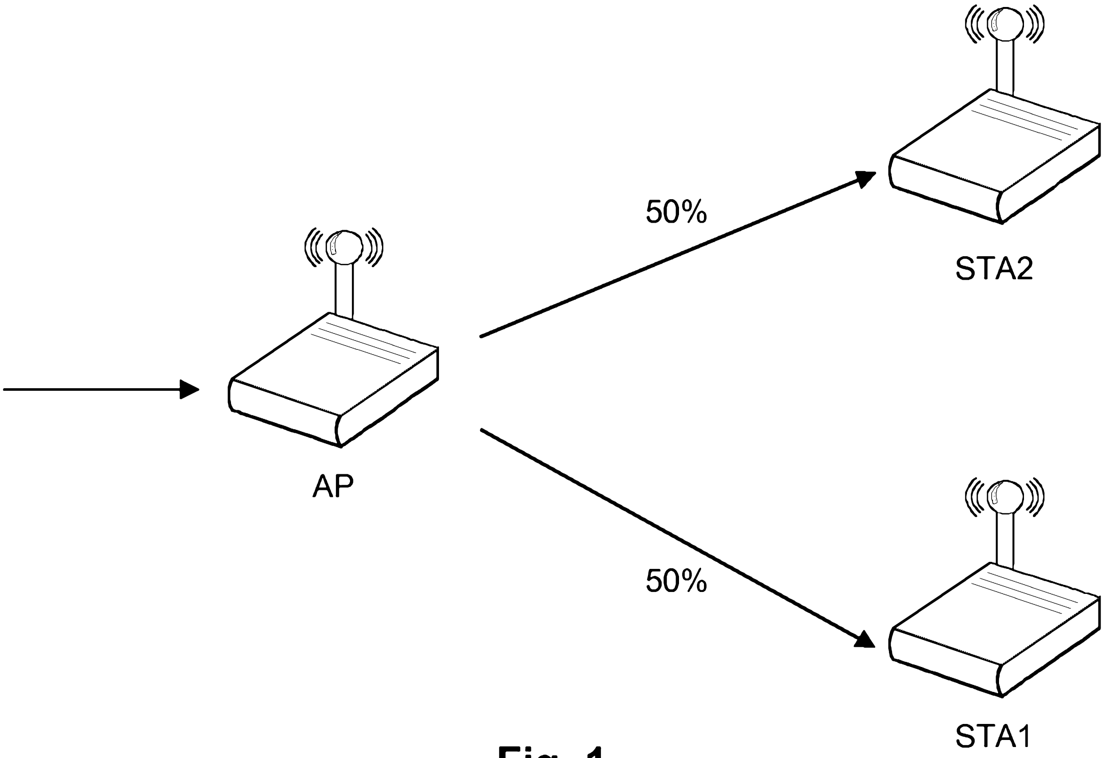

Fig. 1

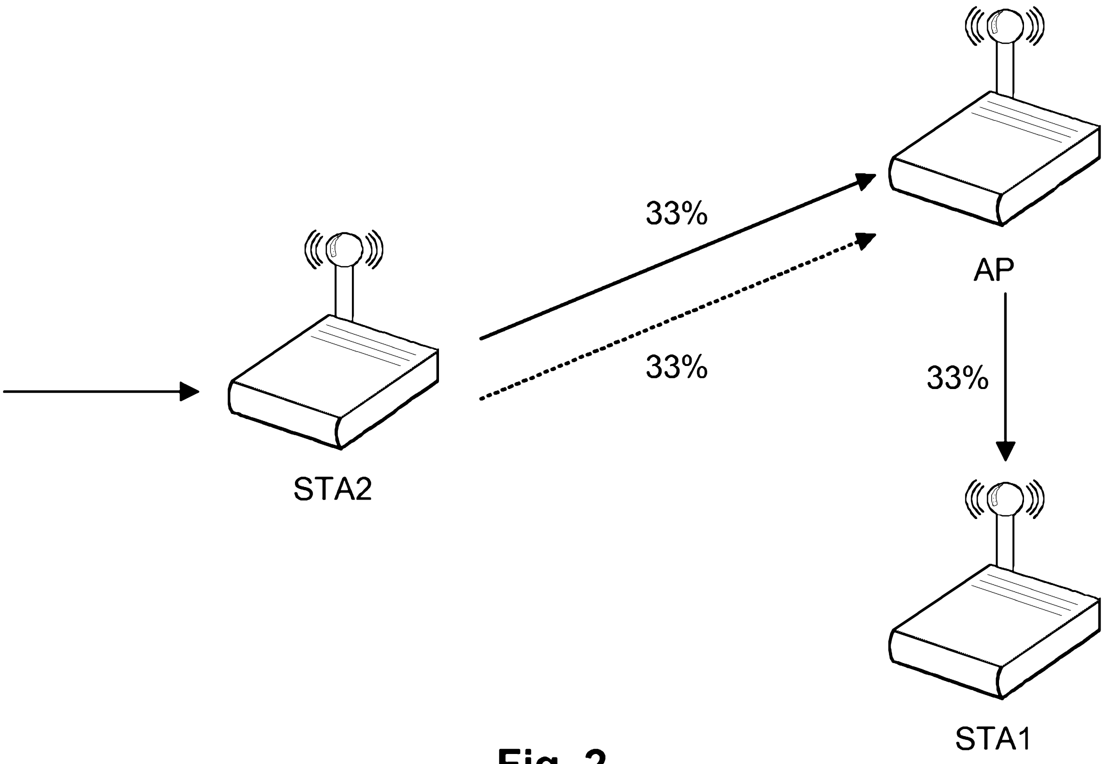

Fig. 2

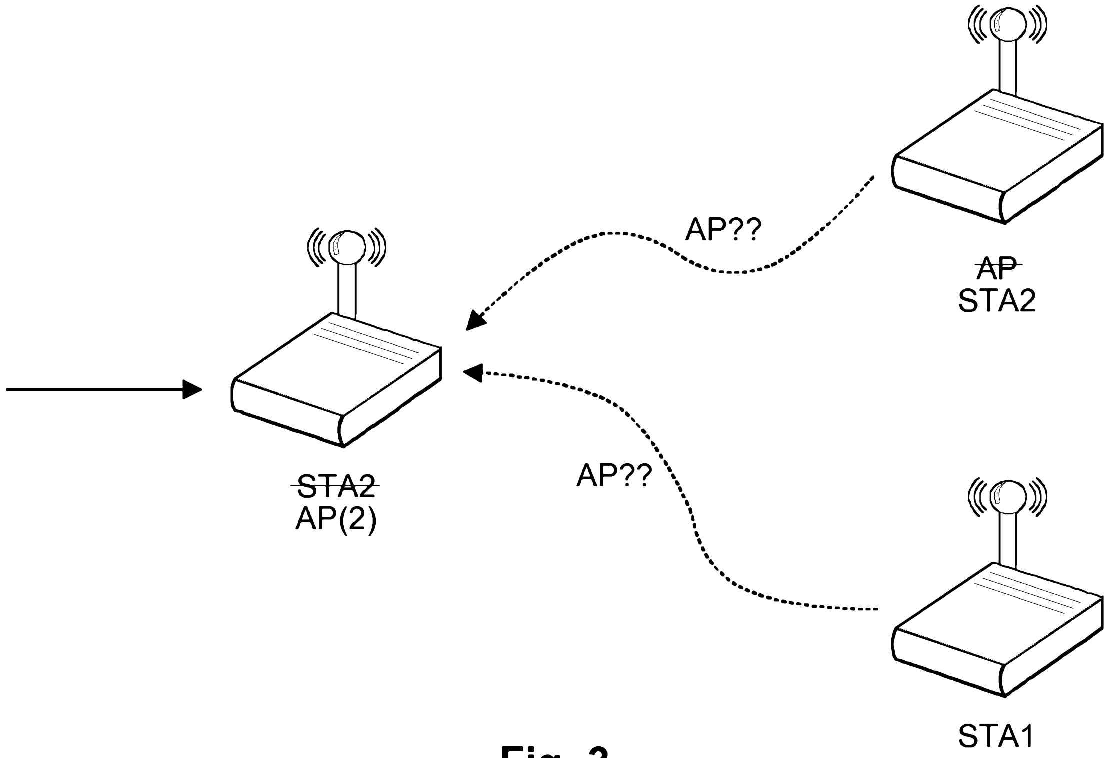
AP??
~~AP~~
STA2
~~STA2~~
AP(2)
AP??
STA1

Fig. 3

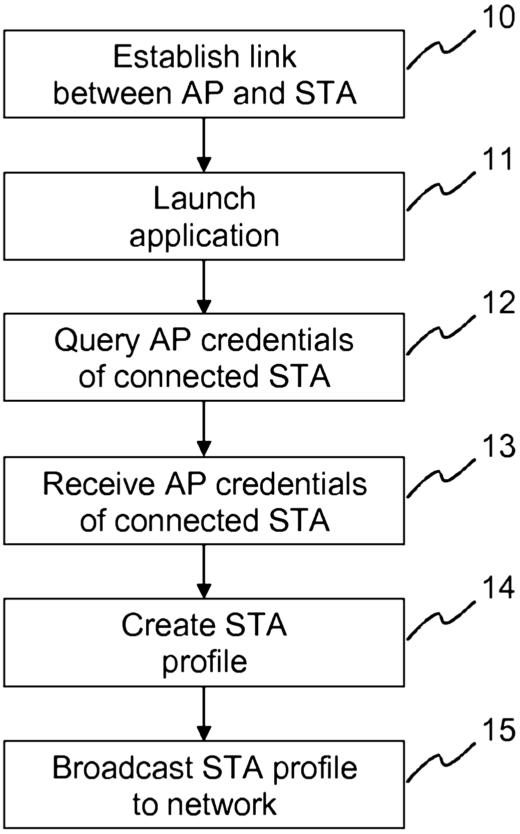
Establish link between AP and STA
10
Launch application
11
Query AP credentials of connected STA
12
Receive AP credentials of connected STA
13
Create STA profile
14
Broadcast STA profile to network
15

Fig. 4

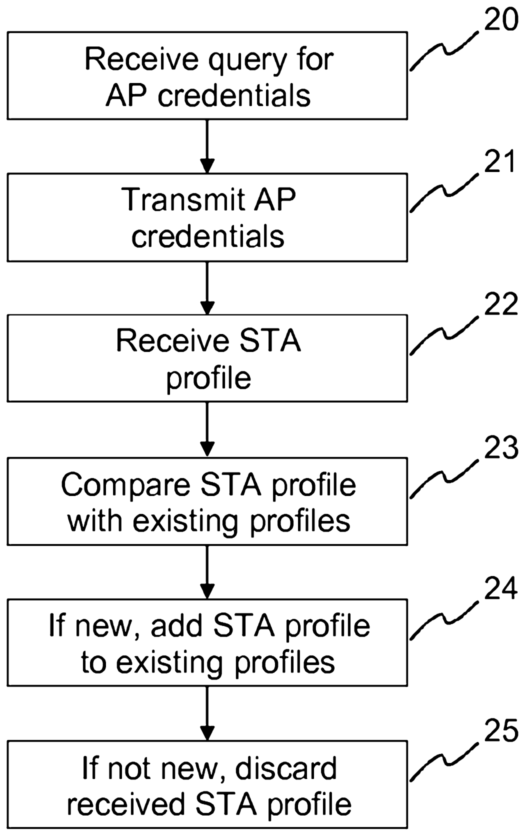
Receive query for AP credentials
20
Transmit AP credentials
21
Receive STA profile
22
Compare STA profile with existing profiles
23
If new, add STA profile to existing profiles
24
If not new, discard received STA profile
25

Fig. 5

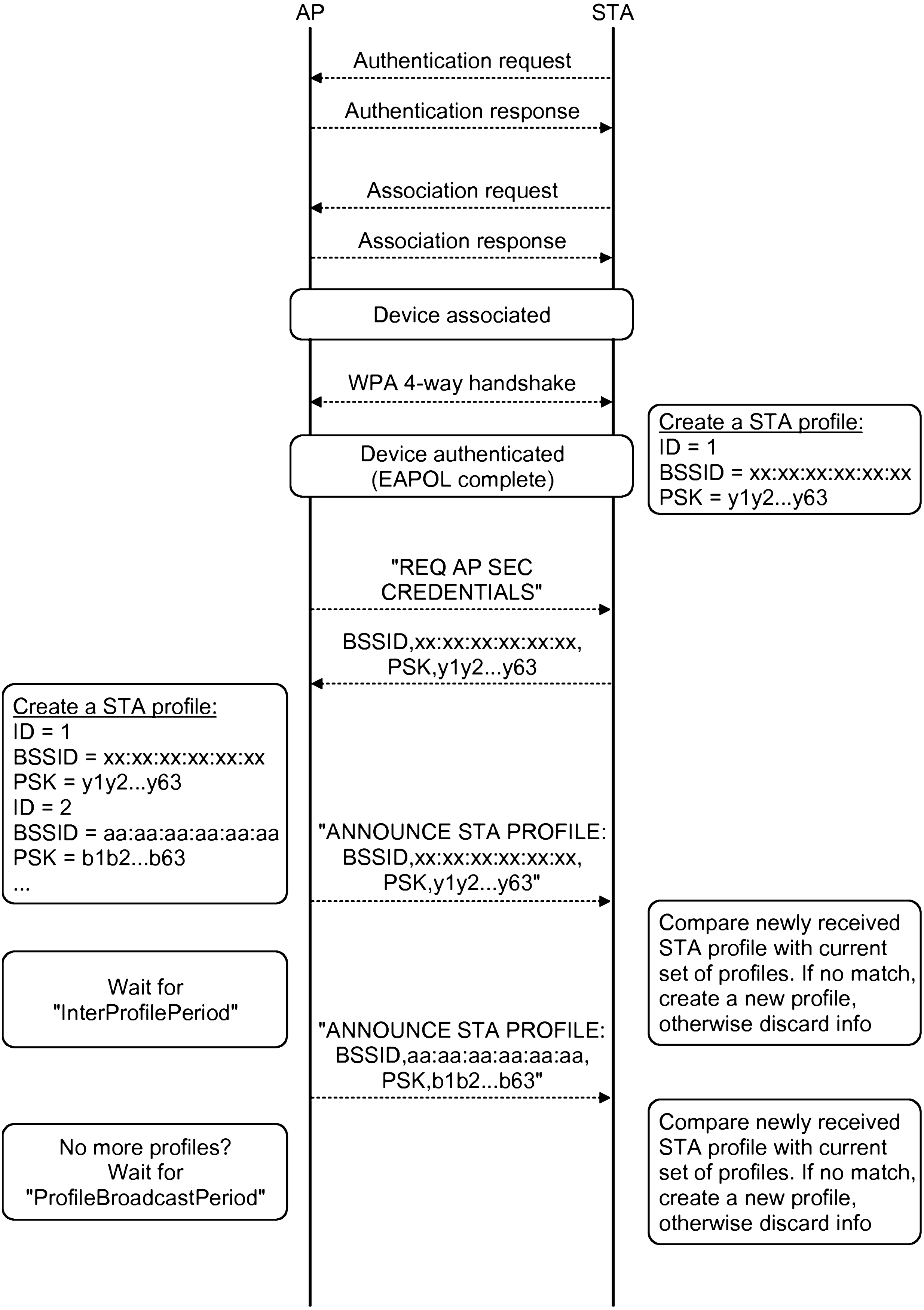
AP
STA
Authentication request
Authentication response
Association request
Association response
Device associated
WPA 4-way handshake
Create a STA profile:
ID = 1
BSSID = xx:xx:xx:xx:xx:xx
PSK = y1y2...y63
Device authenticated
(EAPOL complete)
"REQ AP SEC
CREDENTIALS"
BSSID,xx:xx:xx:xx:xx:xx,
PSK,y1y2...y63
Create a STA profile:
ID = 1
BSSID = xx:xx:xx:xx:xx:xx
PSK = y1y2...y63
ID = 2
BSSID = aa:aa:aa:aa:aa:aa
PSK = b1b2...b63
...
"ANNOUNCE STA PROFILE:
BSSID,xx:xx:xx:xx:xx:xx,
PSK,y1y2...y63"
Compare newly received STA profile with current set of profiles. If no match, create a new profile, otherwise discard info
Wait for "InterProfilePeriod"
"ANNOUNCE STA PROFILE:
BSSID,aa:aa:aa:aa:aa:aa,
PSK,b1b2...b63"
Compare newly received STA profile with current set of profiles. If no match, create a new profile, otherwise discard info
No more profiles?
Wait for
"ProfileBroadcastPeriod"

Fig. 6

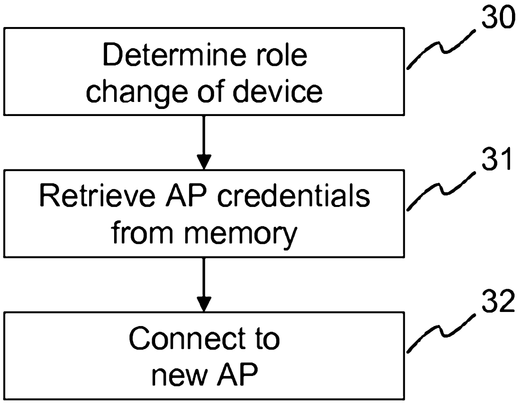
Determine role change of device
30
Retrieve AP credentials from memory
31
Connect to new AP
32

Fig. 7

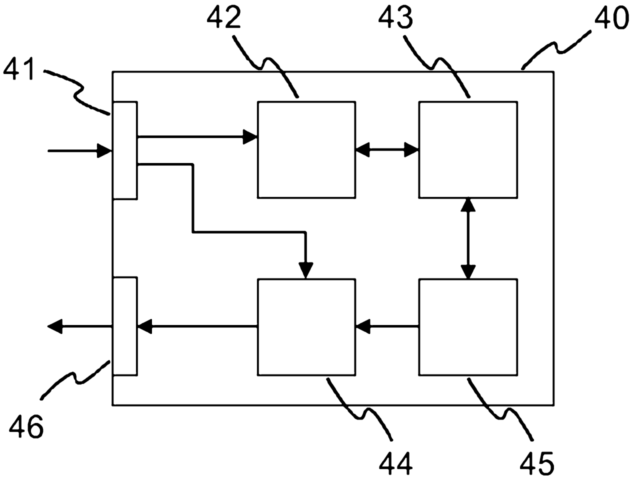
42
43
40
41
46
44
45

Fig. 8