

(43) International Publication Date  
19 June 2014 (19.06.2014)(51) International Patent Classification:  
*H04L 12/24 (2006.01)*

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

(21) International Application Number:

PCT/EP2013/075248

(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.

(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

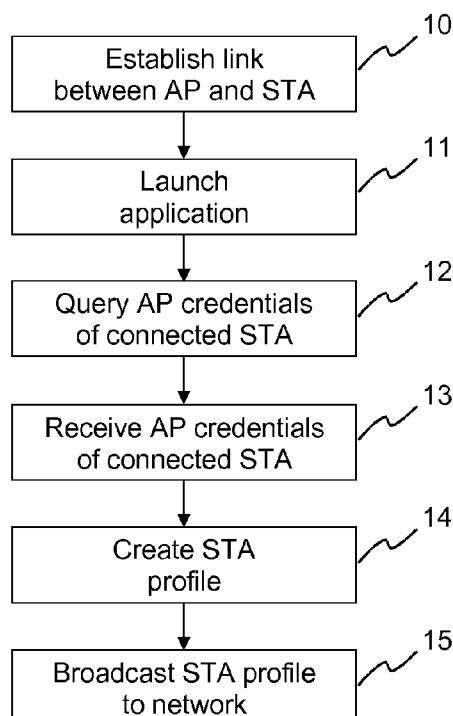
(71) Applicant: THOMSON LICENSING [FR/FR]; 1-5 rue Jeanne d'Arc, F-92130 Issy-les-Moulineaux (FR).

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

(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



(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)).

Fig. 4



EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, **Published:**  
LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, — *with international search report (Art. 21(3))*  
SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,  
GW, KM, ML, MR, NE, SN, TD, TG).

**AUTOMATIC RECONFIGURATION OF NETWORK DEVICES****FIELD OF THE INVENTION**

5 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  
10 network the network remains operational.

**BACKGROUND OF THE INVENTION**

Today, especially due to the delivery of multimedia services  
15 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  
20 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  
25 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-  
30 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

5 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 guarantees strong security. End users do not have to come up with clever passphrases and, through using WPS-PBC (WPS-PBC : Wi-Fi

10 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.

15

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.

20

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 25 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 30 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.

5 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  
10 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).

15

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  
20 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  
25 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  
30 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 5 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 10 (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.

15 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. 20 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.

25

## **SUMMARY OF THE INVENTION**

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

30

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.

10

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 5 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.

10

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.

15

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 20 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. 25 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 30 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
- 5 - 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  
10 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
- 15 - a network connector for connecting the network device to the second network device using the retrieved profile.

20 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  
25 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  
30 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;

5

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

10

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,

15

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

20

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

25

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

**DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS**

30

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 5 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.

10 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 15 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 20 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 25 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 30 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.

5

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

10 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 15 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 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.

20 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 5 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 10 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 15 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 20 Fig. 7. When a role change of the access point 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 25 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 30 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.
- 20 2. The method according to claim 1, **further** comprising the step of requesting (12) the second network device (STA1, STA2) to send its profile.
- 25 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.
- 30 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).

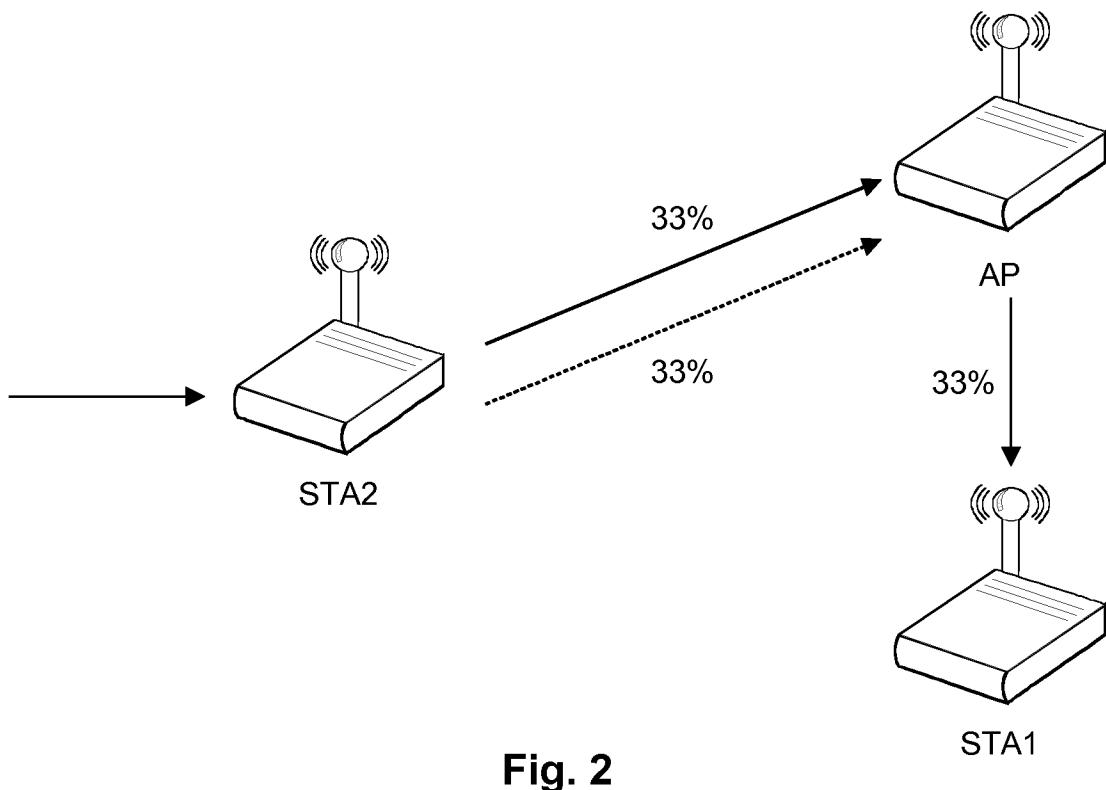
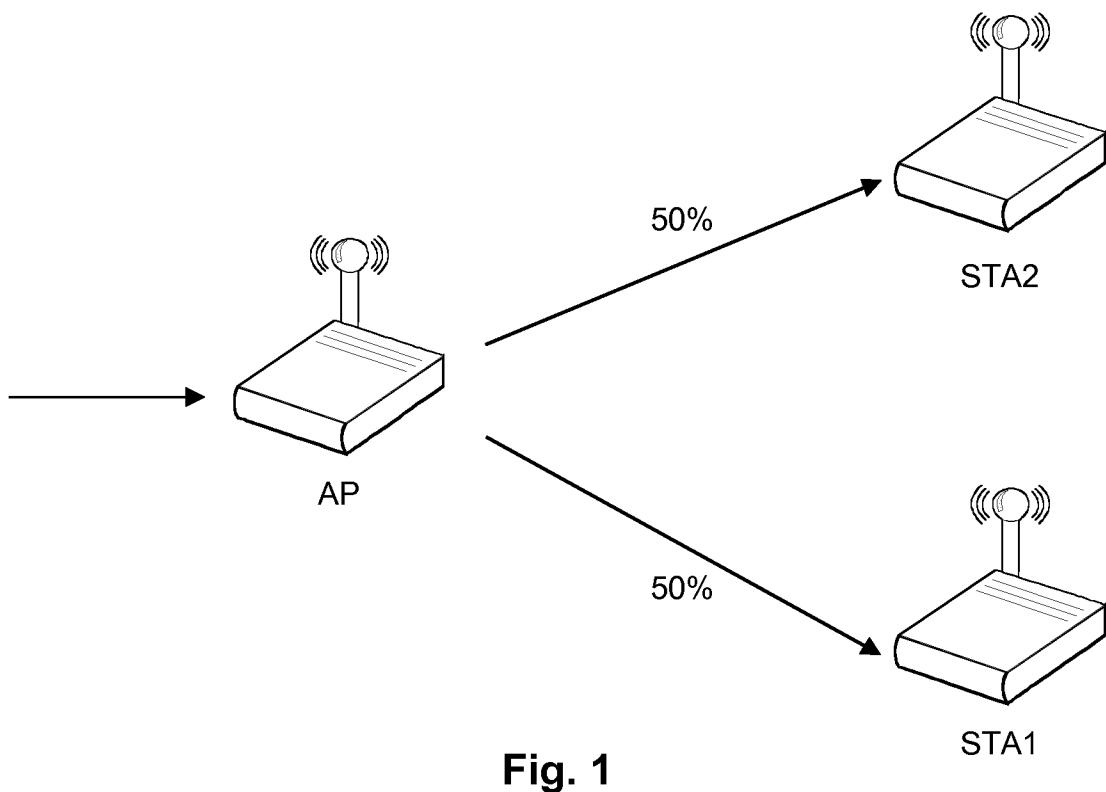
5 10. A network device (AP) adapted to switch from the role of access point to the role of station and vice versa,

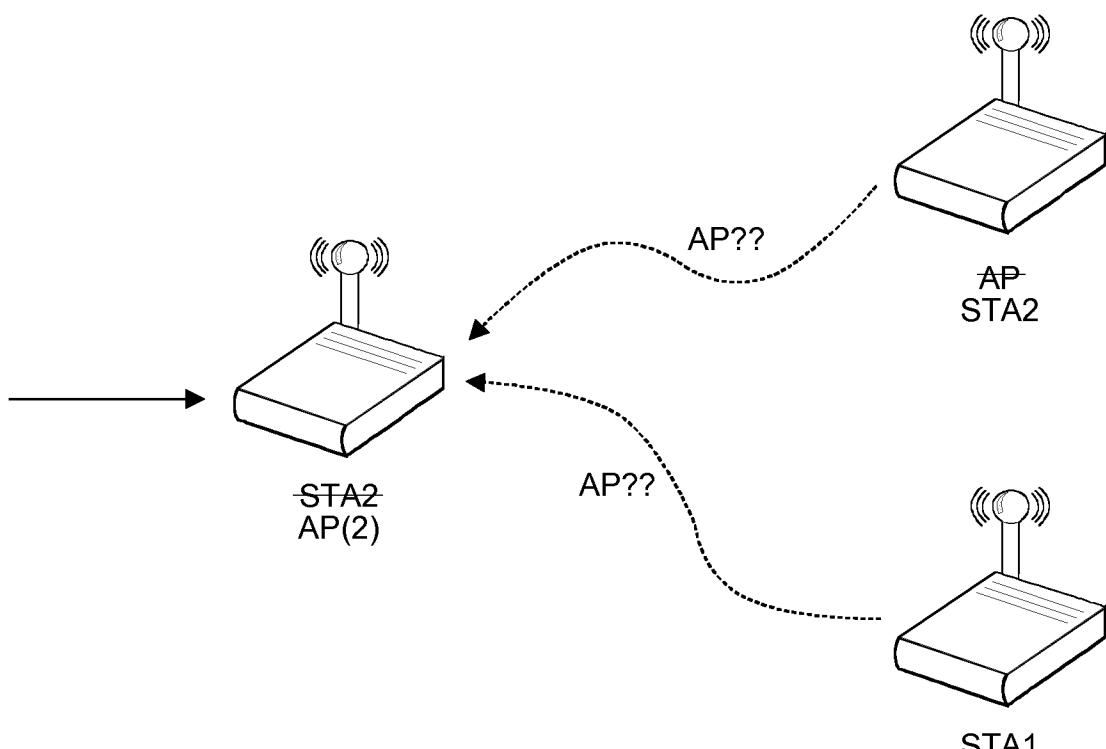
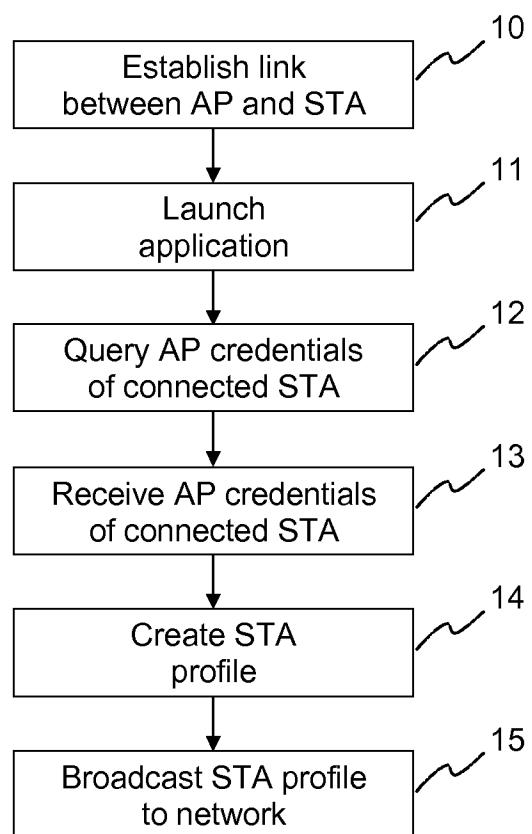
10 **characterized** in that the network device (AP) comprises:

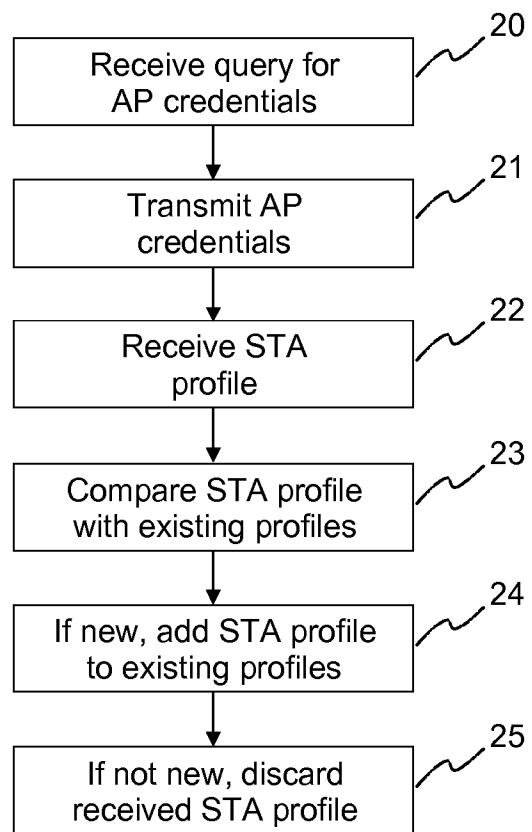
- a role detector (44) for determining (30) a role change of the network device (AP);
- a memory access unit (45) for retrieving (31) a profile of a second network device (AP(2)) from a memory (43), wherein the profile of the second network device (AP(2)) comprises access point credentials of the second 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.

15

20



**Fig. 3****Fig. 4**

**Fig. 5**

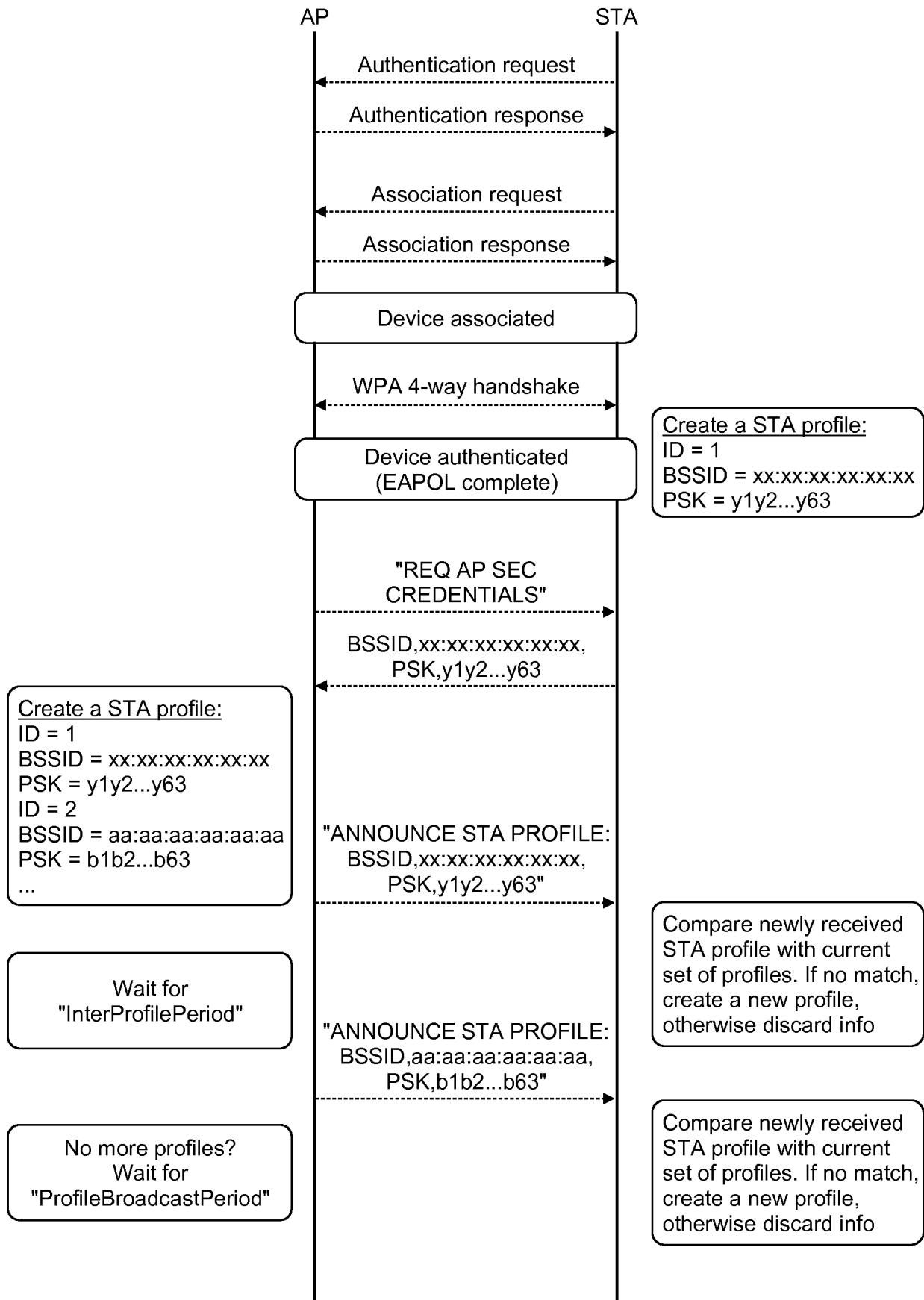
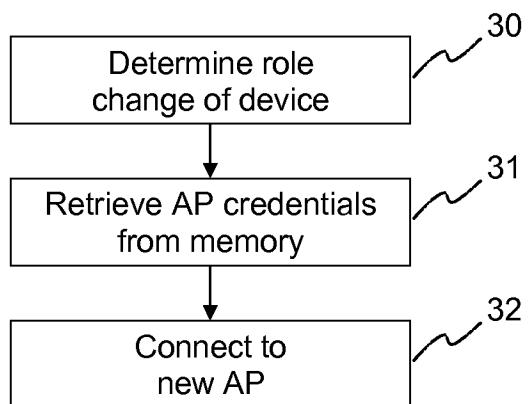
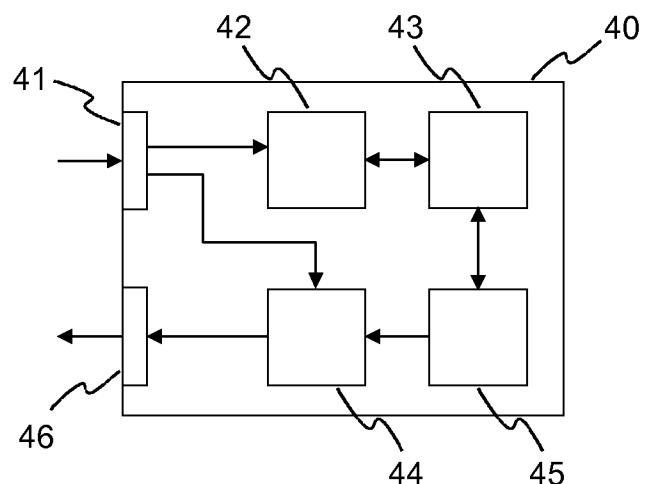


Fig. 6

**Fig. 7****Fig. 8**

# INTERNATIONAL SEARCH REPORT

International application No  
PCT/EP2013/075248

**A. CLASSIFICATION OF SUBJECT MATTER**  
INV. H04L12/24  
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)  
H04L H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, INSPEC, WPI Data

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 2 383 935 A2 (AIRTIES KABLOSUZ ILETISIM SANAYI VE DIS TICARET AN GULBAHAR MAHALLESI) 2 November 2011 (2011-11-02) paragraphs [0008], [0017] - [0022]	1-5, 9
A	-----	6-8, 10
X	WO 01/61965 A1 (SYGATE TECHNOLOGIES INC [US]; YEAP YUEN PIN [US]; ZHANG YADONG [US]) 23 August 2001 (2001-08-23) page 1, line 31 - page 4, line 15 page 8, line 1 - page 9, line 28	1-10
X	US 2006/182075 A1 (BRUNNER MARCUS [DE] ET AL) 17 August 2006 (2006-08-17) paragraphs [0006], [0011], [0015] - [0020]; claims 1-11	1-10
	-----	
	-/-	

Further documents are listed in the continuation of Box C.

See patent family annex.

\* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier application or patent but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
5 March 2014	12/03/2014
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer  Ceccarini, Giulio

## INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/075248

## C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2012/287817 A1 (YAMAGUCHI SATORU [JP]) 15 November 2012 (2012-11-15) paragraphs [0008], [0055], [0056], [0132]; claims -----	1,9
A	US 2007/079113 A1 (KULKARNI AMOL [US] ET AL) 5 April 2007 (2007-04-05) paragraphs [0012] - [0014], [0018], [0062] -----	1-5,9
X	US 7 380 025 B1 (RIGGINS CHRIS [US] ET AL) 27 May 2008 (2008-05-27) cited in the application column 8, line 4 - line 45 column 9, line 52 - column 10, line 17 -----	6,10
A	WO 2008/044877 A1 (LG ELECTRONICS INC [KR]; FEUILLETTE REMI [FR]) 17 April 2008 (2008-04-17) paragraph [0032] - paragraph [0048]; claims -----	1-5,9 1-10
1		

## INTERNATIONAL SEARCH REPORT

International application No.  
PCT/EP2013/075248

### Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1.  Claims Nos.:  
because they relate to subject matter not required to be searched by this Authority, namely:
  
2.  Claims Nos.:  
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
  
3.  Claims Nos.:  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

### Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1.  As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
  
2.  As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.
  
3.  As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
  
4.  No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

#### Remark on Protest

The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

No protest accompanied the payment of additional search fees.

**FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210**

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-5, 9

Method and apparatus for storing a profile of a different network device.

---

2. claims: 6-8, 10

Method and apparatus for connecting to a different device by using a stored profile after role change.

---

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No PCT/EP2013/075248
---

Patent document cited in search report	Publication date	Patent family member(s)			Publication date
EP 2383935	A2	02-11-2011	EP US	2383935 A2 2012213158 A1	02-11-2011 23-08-2012
-----					
WO 0161965	A1	23-08-2001	AU US US US WO	3830401 A 6961762 B1 2006069760 A1 2009313359 A1 0161965 A1	27-08-2001 01-11-2005 30-03-2006 17-12-2009 23-08-2001
-----					
US 2006182075	A1	17-08-2006	CN DE JP US	1822558 A 102005006872 A1 2006229943 A 2006182075 A1	23-08-2006 17-08-2006 31-08-2006 17-08-2006
-----					
US 2012287817	A1	15-11-2012	CN JP US	102855215 A 2012238998 A 2012287817 A1	02-01-2013 06-12-2012 15-11-2012
-----					
US 2007079113	A1	05-04-2007	NONE		
-----					
US 7380025	B1	27-05-2008	NONE		
-----					
WO 2008044877	A1	17-04-2008	US WO	2009239518 A1 2008044877 A1	24-09-2009 17-04-2008
-----					