



US 20080198826A1

(19) **United States**

(12) **Patent Application Publication**
Won

(10) **Pub. No.: US 2008/0198826 A1**

(43) **Pub. Date: Aug. 21, 2008**

(54) **METHOD AND SYSTEM OF DETECTING
DUPLICATE SSID VIA SELF-SCANNING IN
WLAN**

Publication Classification

(51) **Int. Cl.**
H04Q 7/24

(2006.01)

(52) **U.S. Cl.** **370/338**

(76) **Inventor: Sang-Yeon Won, Seoul (KR)**

Correspondence Address:
ROBERT E. BUSHNELL
1522 K STREET NW, SUITE 300
WASHINGTON, DC 20005-1202

(57) **ABSTRACT**

A method and a system of detecting a duplicate service set identifier (SSID) via self-scanning in a WLAN are provided. An access point (AP), when a scan request is given, generates a probe request packet by inserting a SSID of the AP thereinto, transmits the probe request packet to neighbor APs, receives probe response packets, in response to the probe request packet, from the neighbor APs, detects SSIDs from the probe response packets, and informs the presence of a neighbor AP, the SSID of which is the same as that of the AP, if any of the detected SSIDs is the same as the SSID of the AP.

(21) **Appl. No.: 12/071,531**

(22) **Filed: Feb. 21, 2008**

(30) **Foreign Application Priority Data**

Feb. 21, 2007 (KR) 10-2007-0017590

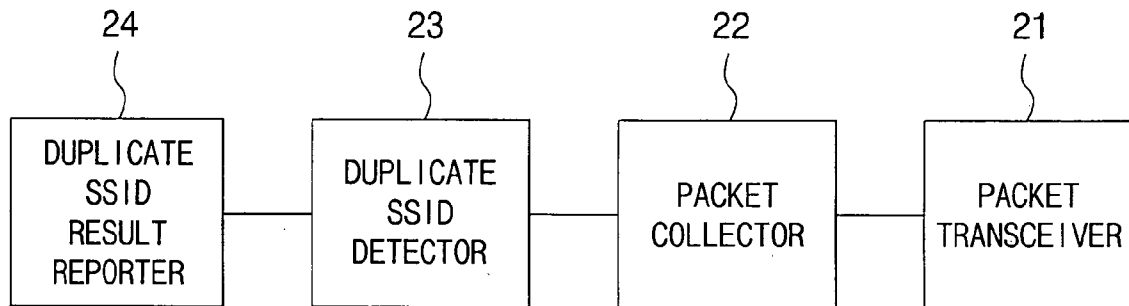


FIG. 1

Probe Request

Order	Information
1	SSID
2	Supported rates

Probe Response

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability Information	
4	SSID	
5	Supported rates	
6	FH Parameter Set	The FH Parameter Set Information element is present within Probe Response frames generated by STAs using frequency-hopping PHYs.
7	DS Parameter Set	The DS Parameter Set Information element is present within Probe Response frames generated by STAs using direct sequence PHYs.
8	CF Parameter Set	The CF Parameter Set Information element is only present within Probe Response frames generated by APs supporting a PCF.
9	IBSS Parameter Set	The IBSS Parameter Set Information element is only present within Probe Response frames generated by STAs in an IBSS.

FIG. 2

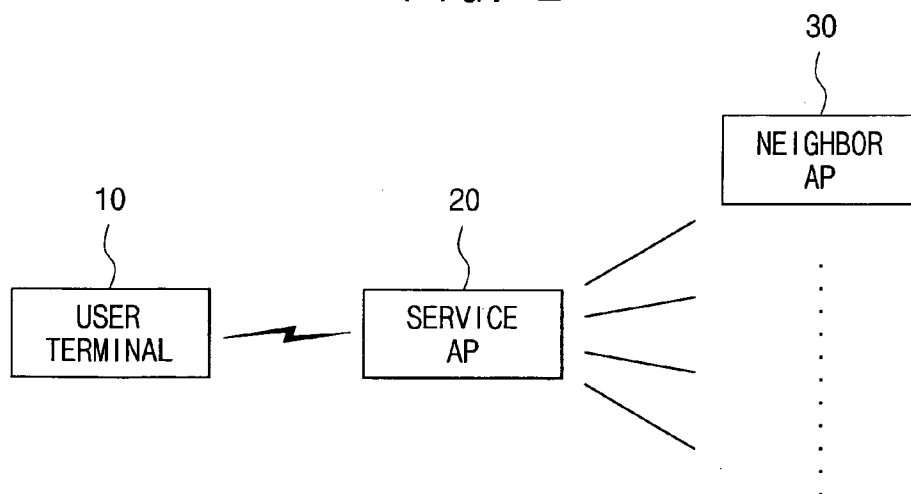


FIG. 3

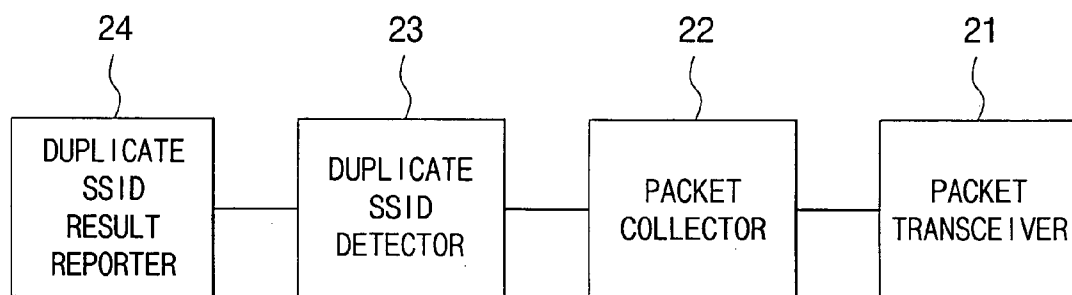
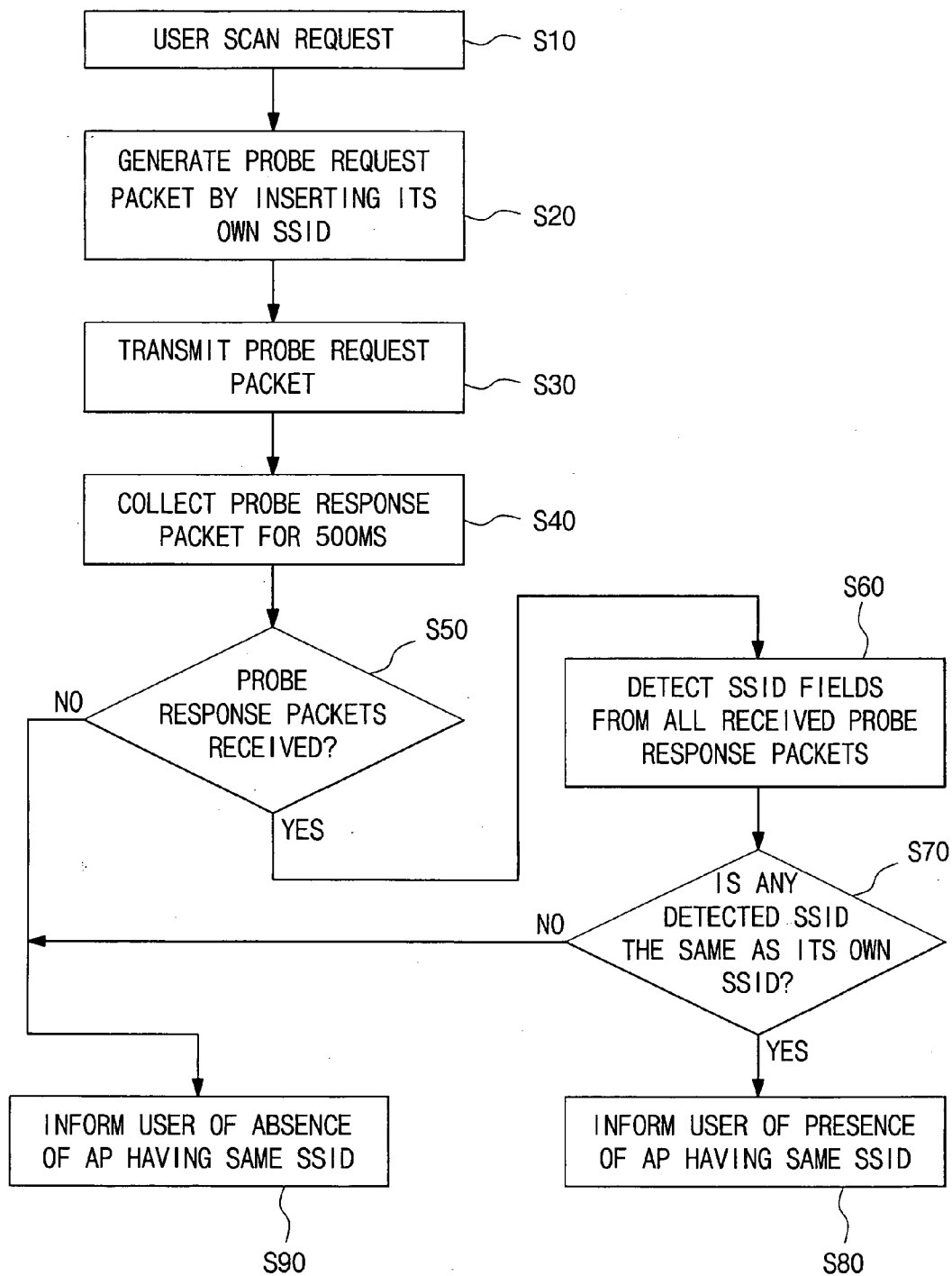


FIG. 4



METHOD AND SYSTEM OF DETECTING DUPLICATE SSID VIA SELF-SCANNING IN WLAN

CLAIM OF PRIORITY

[0001] This application makes reference to and claims all benefits accruing under 35 U.S.C. §119 from an application for METHOD AND SYSTEM OF DETECTING DUPLICATE SSID VIA SELF-SCANNING IN WLAN earlier filed in the Korean Intellectual Property Office on Feb. 21, 2007, and there duly assigned Serial No. 10-2007-0017590.

BACKGROUND OF THE INVENTION

[0002] 1. Field of the Invention

[0003] The present invention relates to an apparatus and method for TTR offset control in ADSL, more particularly, which can control TTR offset in order to remove NEXT or FEXT noise that would otherwise take place in services due to matching between ADSL and TCM-ISDN. The present invention relates to a method and a system of detecting a duplicate service set identifier (SSID) via self-scanning in a wireless local area network (WLAN).

[0004] 2. Description of the Related Art

[0005] Generally, in an 802.11 WLAN infrastructure mode, an access point (AP) establishes a network using an SSID, which is the same as that of a client, in order to provide a data service to the client.

[0006] Accordingly, the client can access the AP via the SSID of the network, to which it attempts to connect, in order to be provided with a suitable data service. That is, as described in the following paragraphs, the client transmits a probe request packet and then waits for a probe response packet in order to access an AP or to scan neighbor APs.

[0007] FIG. 1 is a view illustrating a general example of a probe request packet and a probe response packet. If the SSID field of the probe request packet, received from a client, is the same as that of the SSID of an AP or is a broadcast SSID, the AP transmits a probe response packet to the client by adding its own SSID to an SSID field of the probe response packet. Accordingly, in order to scan neighbor APs, the client transmits a probe request packet to the neighbor APs by adding a broadcast SSID thereto, and then collects AP information of a corresponding channel by referring to the SSID fields of probe response packets, received from the neighbor APs. This process is referred to as active scanning scheme.

[0008] On the contrary, the client can receive beacons, which are periodically transmitted from the neighbor APs, to collect AP information of a corresponding channel by referring to the SSID in the beacons. This process is referred to as passive scanning scheme.

[0009] WLAN users generally purchase APs, which are widely distributed in the market. However, in the case that a user attempts to use a purchased AP without changing the SSID setting thereof, the SSID of the purchased AP may be the same as that of a neighbor AP. If a neighbor AP present within a service set is accidentally using the same SSID, the client would be confused to identify an AP, to which it attempts to connect. Hence, abnormal data services can be caused. That is, the client may access an incorrect AP, and thus a data service may fail due to authentication failure. The client may repeat connection between two APs having the same SSID, thereby risking the stability of the service. It is

also possible that another client accesses the user AP to be freely provided with a data service.

[0010] A specific client can identify whether or not the same SSID is present by collecting neighbor AP information via active scanning or passive scanning. However, in the case of an AP having a hidden SSID, its beacon does not include SSID information. This type of AP also does not respond to a probe request, which uses a broadcast SSID.

[0011] When the client terminal scans the neighbor APs via a conventional scanning scheme, it is impossible to detect an AP having a hidden SSID. Therefore, the problem is that the presence of an AP, which has the same SSID as the user AP, cannot be identified.

SUMMARY OF THE INVENTION

[0012] It is an object of the invention to provide a method and a system of detecting a duplicate SSID via self-scanning in a WLAN, in which a specific scanning function is imparted to a client AP in order to quickly find and monitor a problem, which would take place owing to unintended presence of the same SSID, and also detect an AP having a hidden SSID, which cannot be detected using conventional scanning schemes, thereby detecting a duplicate SSID in neighbor APs.

[0013] According to an aspect of the present invention, the method of detecting a duplicate SSID in a WLAN includes steps of generating a probe request packet by inserting a service set identifier of a service access point to the probe request packet whenever a scan request is given, transmitting the probe request packet to neighbor access points, receiving probe response packets that are sent in response to the probe request packet from the neighbor access points, detecting service set identifiers included in the probe response packets, and informing presence of a neighbor access point whose service set identifier is the same as that of the service access point, if any of the detected service set identifiers is the same as the service set identifier of the service access point.

[0014] The method may further include a step of informing absence of a neighbor access point whose service set identifier is the same as that of the service access point, if none of the probe response packets is received from the neighbor access points. The method may further include a step of informing absence of a neighbor access point whose service set identifier is the same as that of the service access point, if none of the detected service set identifiers of the probe response packets is the same as the service set identifier of the service access point. The step of receiving probe response packets may further include a step of collecting the probe response packets for about 500 milliseconds. The scan request given to the access point is made by a client or a user.

[0015] According to another aspect of the present invention, the system of detecting a duplicate SSID in a WLAN includes a service access point (AP). The service AP generates a probe request packet by inserting a service set identifier of the service access point to the probe request packet whenever a scan request is given, transmits the probe request packet to neighbor access points, receives probe response packets that are sent in response to the probe request packet from the neighbor access points, detects service set identifiers of the probe response packets, and informs presence of a neighbor access point whose service set identifier is the same as that of the service access point if any of the detected service set identifiers is the same as the service set identifier of the service access point.

[0016] The service AP may include a packet transceiver for transmitting the probe request packet to the neighbor access points in response to the scan request from a user and for receiving the probe response packets sent in response to the probe request packet from the neighbor access points, a packet collector for collecting the probe response packets in order to acquire information of the neighbor access points, a duplicate service set identifier detector for detecting service set identifier fields of the probe response packets collected by the packet collector where the duplicate service set identifier detector determining whether or not any of the detected service set identifiers of the probe response packets is the same as the service set identifier of the service access point, and a duplicate service set identifier result reporter for informing a result from the duplicate service set identifier detector to the user.

[0017] The packet collector may operate to collect the packets whenever the user sets a SSID or in the event of abnormal data service.

[0018] The service access point may include a packet transceiver for receiving beacons transmitted from the neighbor access points, a packet collector for scanning the neighbor access points in order to acquire information of the neighbor access points, a duplicate service set identifier detector for detecting service set identifier fields of the received beacons where the duplicate service set identifier detector determining whether or not any of the detected service set identifiers of the beacons is the same as the service set identifier of the service access point, and a duplicate service set identifier result reporter for informing a result from the duplicate service set identifier detector to the user.

[0019] The service access point may broadcast the probe request packet in a predetermined channel. The service access point is coupled to a user terminal, and the scan request is given by the user terminal.

BRIEF DESCRIPTION OF THE DRAWINGS

[0020] A more complete appreciation of the invention, and many of the attendant advantages thereof, will be readily apparent as the same becomes better understood by reference to the following detailed description when considered in conjunction with the accompanying drawings in which like reference symbols indicate the same or similar components, wherein:

[0021] FIG. 1 is a view illustrating a general example of a probe request packet and a probe response packet; [0020] FIG. 2 is a block diagram schematically illustrating a system of detecting a duplicate SSID via self-scanning in a WLAN;

[0022] FIG. 3 is a block diagram illustrating the structure of the service AP of the system shown in FIG. 2; and

[0023] FIG. 4 is a flowchart illustrating a process of detecting a duplicate SSID via self-scanning in a WLAN according to the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0024] The present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments thereof are shown. Reference now should be made to the drawings, in which the same reference numerals and signs are used throughout the different drawings to designate the same or similar components. In the following description of the present invention, a

detailed description of known functions and components incorporated herein will be omitted when it may make the subject matter of the present invention rather unclear.

[0025] FIG. 2 is a block diagram schematically illustrating a system of detecting a duplicate SSID via self-scanning in a WLAN, and FIG. 3 is a block diagram illustrating the structure of the service AP of the detection system shown in FIG. 2.

[0026] As shown in FIGS. 2 and 3, the detection system of the present invention includes a user terminal 10, a service AP 20 for providing a data service to the user terminal 10 and a plurality of neighbor APs 30 for transmitting/receiving packets to/from the service AP 20. The user terminal 10 sends a scan request to the AP 20 in a service set. In response to the scan request from the user terminal 10, the service AP 20 generates a probe request packet by inserting the SSID of the AP 20 thereinto, sends the probe request packet to the neighbor APs 30, and then collects probe response packets, sent in response to the probe request packet from the neighbor APs 30. The time period for collecting the probe response packets is about 500 ms.

[0027] When the service AP 20 receives the probe response packets from the neighbor APs 30, it detects SSIDs from all the received probe response packets. If one of the detected SSIDs is the same as the SSID of the service AP 20, the service AP informs the client of the presence of an AP that uses the same SSID. However, if a probe response packet is not received or the same SSID does not exist, the service AP 20 informs the user terminal 10 of the absence of an AP that uses the same SSID.

[0028] In more detail, as shown in FIG. 3, the service AP 20 includes a packet transceiver 21, a packet collector 22, a duplicate SSID detector 23 and a duplicate SSID result reporter 24.

[0029] In response to a scan request from the user, the packet transceiver 21 transmits a probe request packet to neighbor APs and receives probe response packets therefrom.

[0030] The packet collector 22 collects packets by scanning the neighbor APs using a self-scanning scheme. The packet collector 22 operates to collect packets whenever the user sets an SSID or in the event of an abnormal data service. That is, the packet collector 22 can collect packets to acquire information on the neighbor APs in accordance with a passive scanning scheme or a self-scanning scheme. In the passive scanning scheme, the packet collector 22 scans the neighbor APs 30 by receiving beacons, which are periodically transmitted from the neighbor APs 30. In the self-scanning scheme, the packet collector 22 generates a probe request packet using its own SSID (the SSID of the service AP) in order to scan the neighbor APs based on responses.

[0031] Particularly, in the self-scanning scheme, an SSID set to a user AP (service AP) is inserted into an SSID field in a probe request frame, which is then broadcast to neighbor APs in a corresponding channel. When the probe request frame is received by the neighbor APs, if the SSID of any of the neighbor APs is the same as the SSID in the probe request frame, the neighbor AP having the same SSID transmits a probe response packet to the user AP by inserting its own SSID thereinto. Accordingly, the user AP can collect neighbor AP information based upon the SSID information of received probe response packets.

[0032] The duplicate SSID detector 23 detects SSID fields from all the packets, collected by the packet collector 22, and conducts inspection to detect any duplicate SSID that is the

same as the SSID of the service AP 20. That is, the duplicate SSID detector 23 identifies the presence of an AP, the SSID of which is the same as that of the service AP 20, using the neighbor AP information, which is collected by the packet collector 22, and sends an identification result (i.e., a duplicate SSID detection result) to the duplicate SSID result reporter 24.

[0033] The duplicate SSID result reporter 24 reports the duplicate SSID detection result, sent from the duplicate SSID detector 23, to the user.

[0034] More specifically, if any of the SSIDs, detected by the duplicate SSID detector 23, is the same as the SSID of the service AP 20, the duplicate SSID result reporter 24 informs the user of the presence of the AP that uses the same SSID. If any of the SSIDs, detected by the duplicate SSID detector 23, is not the same as the SSID of the service AP 20, the duplicate SSID result reporter 24 informs the user of the absence of the AP that uses the same SSID.

[0035] FIG. 4 is a flowchart illustrating a process of detecting a duplicate SSID via self-scanning in a WLAN according to the invention. As shown in FIG. 4, at first, a client sends a user scan request to an AP in a service set (S10). The scan request can also be checked directly by a user in the AP, in place of the client. In response to the scan request from the client, the AP in the service set generates a probe request packet by inserting its own SSID therein (S20), and transmits the generated probe request packet to neighbor APs (S30). The AP in the service set collects probe response packets, in response to the probe request packet, from the neighbor APs for about 500 ms (S40).

[0036] The AP in the service set determines whether or not the probe packets are received from the neighbor APs (S50), and if the probe response packets are received from the neighbor APs, detects SSIDs from all the probe response packets received therefrom (S60).

[0037] Next, the service AP determines whether or not any of the detected SSIDs is the same as its own SSID (S70), and if the same SSID is present, informs the client of the presence of an AP that uses the same SSID (S80).

[0038] If it is determined, in the step S50 of determining whether or not the probe packets are received from the neighbor APs, that no probe response packets are received, or it is determined, in the step S70 of determining whether or not any of the detected SSIDs is the same as its own SSID, that the same SSID is absent, the service AP informs the client of the absence of the AP that uses the same SSID (S90).

[0039] As set forth hereinbefore, the service AP can detect the presence of an AP, which has a hidden SSID, by transmitting the probe request packet having the SSID of the service AP and then acquiring neighbor AP information using the probe response packets, received from the neighbor APs. Accordingly, the user can readily understand a problem in a data service, which would take place due to the presence of a duplicate SSID. Therefore, the self-scanning scheme of the invention makes it possible to scan all the APs irrespective of their SSID types, which are set visibly or invisibly.

[0040] Although it is impossible for a client terminal to scan and detect APs having a hidden SSID in a WLAN, the self-scanning scheme of the invention makes it possible to detect the hidden SSID of neighbor APs.

[0041] According to the invention as set forth above, since a scanning function is imparted to the client AP, it is possible to prevent an unstable network service, which would take place due to the presence of a neighbor AP using the same

SSID. It is also possible to prevent a bandwidth decrease or a fee problem, which would be caused by others using the network of the user.

[0042] Furthermore, the self-scanning scheme of the invention makes it possible to detect an AP using a hidden SSID, which would not be detected by conventional scanning schemes, and also to solve uncertain network problems, which would be caused by the hidden SSID, thereby improving the reliability of a product.

[0043] While the present invention has been shown and described in connection with the preferred embodiments, it will be apparent to those skilled in the art that modifications and variations can be made without departing from the spirit and scope of the invention as defined by the appended claims.

What is claimed is:

1. A method of detecting a duplicate service set identifier in a wireless local area network, comprising:

generating a probe request packet by inserting a service set identifier of a service access point to the probe request packet whenever a scan request is given;

transmitting the probe request packet to neighbor access points;

receiving probe response packets that are sent in response to the probe request packet from the neighbor access points;

detecting service set identifiers included in the probe response packets; and

informing presence of a neighbor access point whose service set identifier is the same as that of the service access point, if any of the detected service set identifiers is the same as the service set identifier of the service access point.

2. The method according to claim 1, further comprising: informing absence of a neighbor access point whose service set identifier is the same as that of the service access point, if none of the probe response packets is received from the neighbor access points.

3. The method according to claim 1, further comprising: informing absence of a neighbor access point whose service set identifier is the same as that of the service access point, if none of the detected service set identifiers of the probe response packets is the same as the service set identifier of the service access point.

4. The method according to claim 1, wherein the step of receiving probe response packets further including a step of collecting the probe response packets for about 500 milliseconds.

5. The method according to claim 1, wherein the scan request given to the access point is made by a client or a user.

6. The method according to claim 1, further comprising: receiving beacons transmitted from the neighbor access points;

scanning the neighbor access points in order to acquire information of the neighbor access points;

detecting service set identifier fields of the received beacons;

determining whether or not any of the detected service set identifiers of the beacons is the same as the service set identifier of the service access point; and

7. A system of detecting a duplicate service set identifier in a wireless local area network, comprising:

a service access point, wherein the service access point generates a probe request packet by inserting a service set identifier of the service access point to the probe

request packet whenever a scan request is given, transmits the probe request packet to neighbor access points, receives probe response packets that are sent in response to the probe request packet from the neighbor access points, detects service set identifiers of the probe response packets, and informs presence of a neighbor access point whose service set identifier is the same as that of the service access point if any of the detected service set identifiers is the same as the service set identifier of the service access point.

8. The system according to claim 7, wherein the service access point informs absence of a neighbor access point whose service set identifier is the same as that of the access point, if none of the probe response packets is received from the neighbor access points.

9. The system according to claim 7, wherein the service access point informs absence of a neighbor access point whose service set identifier is the same as that of the access point, if none of the detected service set identifiers is the same as the service set identifier of the service access point.

10. The system according to claim 7, wherein the service access point collects the probe response packets for 500 milliseconds.

11. The system according to claim 7, wherein the service access point comprises:

- a packet transceiver for transmitting the probe request packet to the neighbor access points in response to the scan request from a user, and for receiving the probe response packets sent in response to the probe request packet from the neighbor access points;
- a packet collector for collecting the probe response packets in order to acquire information of the neighbor access points;
- a duplicate service set identifier detector for detecting service set identifier fields of the probe response packets

collected by the packet collector, the duplicate service set identifier detector determining whether or not any of the detected service set identifiers of the probe response packets is the same as the service set identifier of the service access point; and

a duplicate service set identifier result reporter for informing a result from the duplicate service set identifier detector to the user.

12. The system according to claim 11, wherein the packet collector operates to collect the probe response packets whenever the user sets a service set identifier or in an event of abnormal data service.

13. The system according to claim 7, wherein the service access point comprises:

- a packet transceiver for receiving beacons transmitted from the neighbor access points;
- a packet collector for scanning the neighbor access points in order to acquire information of the neighbor access points;
- a duplicate service set identifier detector for detecting service set identifier fields of the received beacons, the duplicate service set identifier detector determining whether or not any of the detected service set identifiers of the beacons is the same as the service set identifier of the service access point; and
- a duplicate service set identifier result reporter for informing a result from the duplicate service set identifier detector to the user.

14. The system according to claim 7, wherein the service access point broadcasts the probe request packet in a predetermined channel.

15. The system according to claim 7, wherein the service access point is coupled to a user terminal, and the scan request is given by the user terminal.

* * * * *