Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2670038 A1 2008/05/29

(21) 2 670 038

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2007/11/20
(87) Date publication PCT/PCT Publication Date: 2008/05/29
(85) Entrée phase nationale/National Entry: 2009/05/20
(86) N° demande PCT/PCT Application No.: CA 2007/002075
(87) N° publication PCT/PCT Publication No.: 2008/061349
(30) Priorité/Priority: 2006/11/21 (US60/866,753)

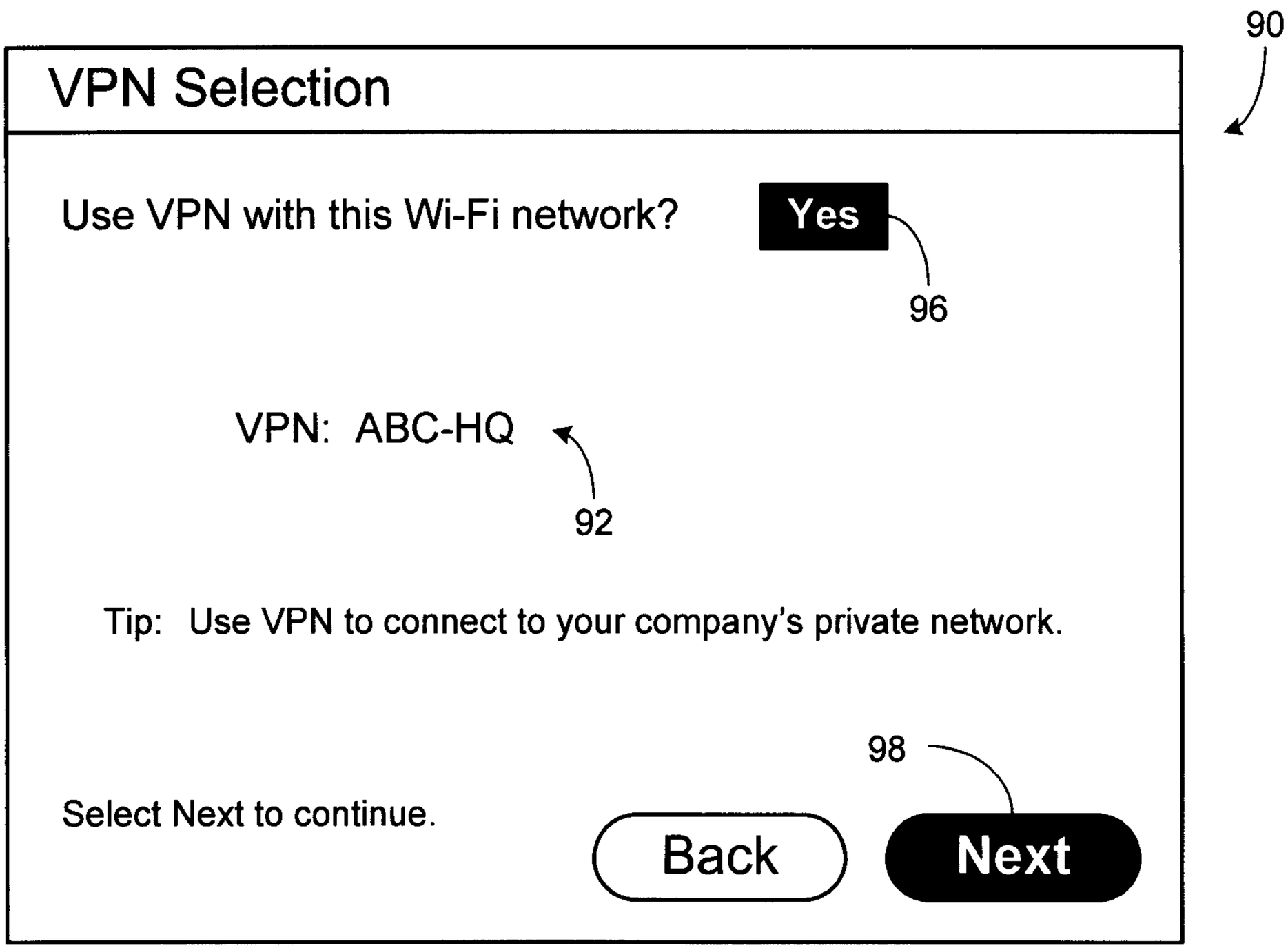
(51) Cl.Int./Int.Cl. *H04L 12/28* (2006.01), *H04L 12/24* (2006.01), *H04L 9/32* (2006.01)

(71) Demandeur/Applicant:
RESEARCH IN MOTION LIMITED, CA

(72) Inventeurs/Inventors:
SCOTT, SHERRYL LEE LORRAINE, CA;
SOMANI, ZAHEEN, CA;
FEDOTENKO, DENIS, CA;
REIF, ALEXANDER J., CA

(74) Agent: INTEGRAL IP

(54) Titre : TRAITEMENT DE CONNEXIONS DE RESEAU VIRTUEL PRIVE SUR UN RESEAU LOCAL SANS FIL
(54) Title: HANDLING VIRTUAL PRIVATE NETWORK CONNECTIONS OVER A WIRELESS LOCAL AREA NETWORK



(57) Abrégé/Abstract:
A wireless local area network "WLAN" client device has one or more virtual private network "VPN" profiles defined therein. In response to the WLAN client device connecting to a WLAN, a user of the WLAN client device is able to indicate whether to attempt to establish a VPN connection over the WLAN.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 May 2008 (29.05.2008)

PCT

(10) International Publication Number
WO 2008/061349 A1

(51) International Patent Classification:
H04L 12/28 (2006.01) *H04Q 7/20* (2006.01)
H04L 12/24 (2006.01) *H04Q 7/38* (2006.01)
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/CA2007/002075

(22) International Filing Date:
20 November 2007 (20.11.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/866,753 21 November 2006 (21.11.2006) US

(71) Applicant *(for all designated States except US)*: **RESEARCH IN MOTION LIMITED** [CA/CA]; 295 Phillip St., Waterloo, Ontario N2L 3W8 (CA).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **SCOTT, Sherryl Lee Lorraine** [CA/CA]; 1-135 Beverly Street, Toronto, Ontario M5T 1Y4 (CA). **SOMANI, Zaheen** [CA/CA]; 27-6071 Azure Road, Richmond, , British Columbia V7C 2P3 (CA). **FEDOTENKO, Denis** [IL/CA]; 969 Creekside Drive, Waterloo, Ontario N2V 2W5 (CA). **REIF, Alexander J.** [CA/CA]; 655 Windermere Road, #702, London, Ontario N5X 2W8 (CA).

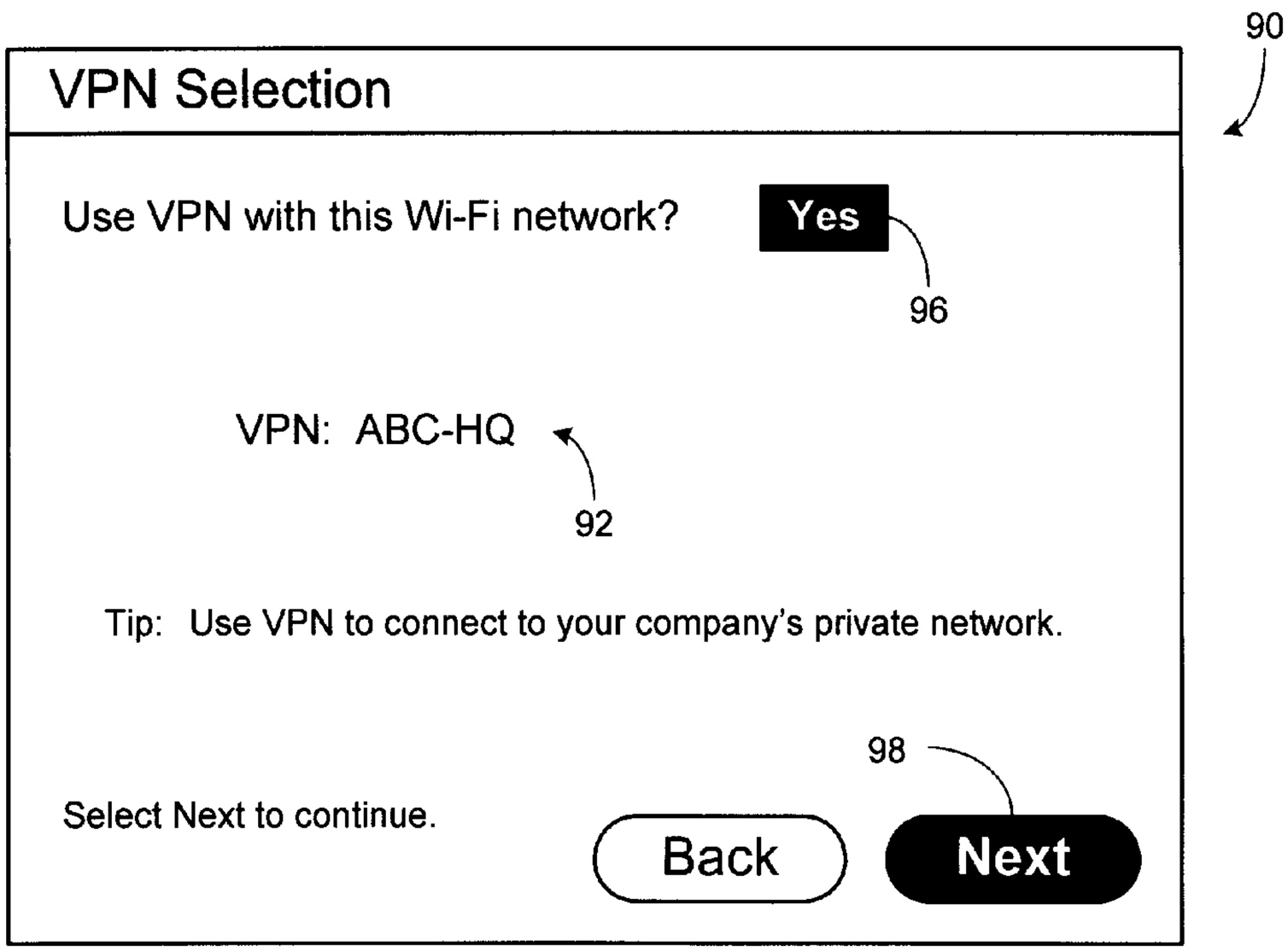
(74) Agent: **PATON, Miriam**; 1370 Don Mills Rd., Ste. 300, Toronto, Ontario M3B 3N7 (CA).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, 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, IS, JP, KE, KG, KM, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: HANDLING VIRTUAL PRIVATE NETWORK CONNECTIONS OVER A WIRELESS LOCAL AREA NETWORK



(57) Abstract: A wireless local area network "WLAN" client device has one or more virtual private network "VPN" profiles defined therein. In response to the WLAN client device connecting to a WLAN, a user of the WLAN client device is able to indicate whether to attempt to establish a VPN connection over the WLAN.

WO 2008/061349 A1

WO 2008/061349 A1

Declaration under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

— *with international search report*

— *with amended claims*

Date of publication of the amended claims: 17 July 2008

HANDLING VIRTUAL PRIVATE NETWORK CONNECTIONS OVER A WIRELESS LOCAL AREA NETWORK

BACKGROUND

[0001] A handheld device may be equipped with a wireless local area network (WLAN) communication interface through which the handheld device may be able to connect to a WLAN. IEEE 802.11 networks (also known as Wi-Fi™ networks) and ETSI HIPERLAN networks are examples of WLANs.

[0002] A WLAN client device may store in its memory one or more persistent connection profiles of WLANs, each labeled by a connection profile name. A persistent connection profile may include, for example, the service set identity (SSID) of the network, WLAN configuration parameters, security credentials, proxy information, default printer, file and printer sharing, firewall, and Internet Protocol (IP) network parameters. The SSID is also known as the network name. The persistent connection profiles may be assigned priorities, for example, by a user that has purchased the client device, a carrier who controls the sale of the client device, or an administrator of an enterprise that has purchased the client device. Generally, user action is required to delete a persistent connection profile from a client device.

[0003] Since a handheld device has a small display and small keyboard, care must be taken when designing a user interface of an application to be run on the handheld device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] Embodiments are illustrated by way of example and not limitation in the figures of the accompanying drawings, in which like reference numerals indicate corresponding, analogous or similar elements, and in which:

[0005] FIG. 1 is an illustration of an exemplary handheld device;

[0006] FIG. 2 is an illustration of an exemplary screen shown when a wireless local area network profile management application is launched and an exemplary menu associated with the application is opened by a user of the handheld device;

[0007] FIG. 3 is an illustration of an exemplary screen which may appear when a WLAN connection setup application is launched;

[0008] FIGs. 4-1 and 4-2 are illustrations of an exemplary screen which may appear while the handheld device is scanning for available wireless local area networks;

[0009] FIGs. 5-1, 5-2, and 5-3 are illustrations of an exemplary screen listing the results of the scanning;

[0010] FIGs. 5-4 and 5-5 are illustrations of other exemplary screens listing the results, in full or in part, of the scanning;

[0011] FIGs. 6-1, 6-2, 6-3, 6-4, 6-5, 6-6, 6-7, 6-8, 6-9 and 6-10 are illustrations of an exemplary screen for user input of security credentials for a wireless local area network;

[0012] FIG. 7 is an illustration of an exemplary screen which may appear while the device is attempting to connect to a particular wireless local area network;

[0013] FIGs. 8-1 and 8-2 are illustrations of an exemplary screen which may appear if the device successfully connects to the wireless local area network;

[0014] FIGs. 8-3 and 8-4 are illustrations of exemplary screens which may appear if the device is unable to connect to the wireless local area network;

[0015] FIGs. 9-1 and 9-2 are illustrations of an exemplary screen for virtual private network (VPN) selection;

[0016] FIGs. 10-1 and 10-2 are illustrations of an exemplary setup completion screen;

[0017] FIG. 11 is an illustration of an exemplary screen for manually adding a wireless local area network;

[0018] FIGs. 12-1 and 12-2 are illustrations of an exemplary screen of a wireless local area network profile management application;

[0019] FIG. 13 is an illustration of an exemplary screen for a wireless connections management application; and

[0020] FIG. 14 is a block diagram of an exemplary handheld device.

[0021] It will be appreciated that for simplicity and clarity of illustration, elements shown in the figures have not necessarily been drawn to scale. For example, the dimensions of some of the elements may be exaggerated relative to other elements for clarity.

DETAILED DESCRIPTION

[0022] In the following detailed description, numerous specific details are set forth in order to provide a thorough understanding of embodiments. However it will be understood by those of ordinary skill in the art that the embodiments may be practiced without these specific details. In other instances, well-known methods, procedures, components and circuits have not been described in detail so as not to obscure the embodiments.

[0023] FIG. 1 is an illustration of an exemplary handheld device 1. Device 1 has a display 2 and user input components such as a keyboard 4 and a trackball 6. Device 1 is equipped with a WLAN wireless communication interface for connecting to Wi-Fi networks, and is a WLAN client device.

[0024] Optionally, device 1 is also equipped with additional wireless communication interfaces, for example, a wireless wide area network (WWAN) communication interface for connecting to mobile networks and a wireless personal area network (WPAN) communication interface for connecting to a WPAN. A non-exhaustive list of mobile phone and data standards for WWANs includes 2G standards such as Global System for Mobile Communications (GSM) and Code Division Multiple Access (CDMA), 2.5G standards such as General Packet Radio Service (GPRS), 2.75G standards such as CDMA2000 and Enhanced Data rates for GSM Evolution (EDGE), and 3G standards such as Wideband CDMA (W-CDMA). Bluetooth® networks, Zigbee™ and ultra-wideband (UWB) networks are examples of WPANs.

[0025] Device 1 also comprises other components which for clarity are not shown in FIG. 1. The following description is based on an exemplary graphical user interface. Clearly, the functionality of the exemplary screens described below can be implemented using other graphical user-interface elements than those shown.

[0026] An exemplary home screen, which is the screen displayed in display 2 when device 1 is first turned on, is shown in FIG. 1. Icons representing applications of device 1 are displayed in a list 8. By navigating through list 8, a user of device 1 may select an icon 10 representing an options application. If the user selects icon 10, an options application will be launched. The screen may then show a window 12 listing a partial or entire list of options that the user can view and/or edit.

[0027] By navigating to and selecting the "Wi-Fi Connections" option 13, a WLAN profile management application will be launched.

[0028] FIG. 2 is an illustration of an exemplary screen 20 shown when the WLAN profile management application is launched and an exemplary menu 22 of commands associated with the application is opened by the user. Screen 20 and menu 22 are described in more detail below with respect to FIGs. 12-1 and 12-2. Selecting a menu item 24 entitled "New ..." from menu 22 will launch a WLAN connection setup application.

[0029] WLAN Connection Setup Application

[0030] FIG. 3 is an illustration of an exemplary screen 30 which may appear when the WLAN connection setup application is launched. Screen 30 includes a button 32 entitled "Scan for Networks" and a button 34 entitled "Manually Add Network".

[0031] If button 32 is selected, scanning for wireless local area networks will commence. Device 1 may employ passive scanning techniques, active scanning techniques or any combination thereof.

[0032] FIG. 4-1 is an illustration of an exemplary screen 40 which may appear while the device is scanning for available WLANs. If no available WLANs are found, a popup window 42 informing the user of this may appear, as shown in FIG. 4-2. If the user presses an OK button 44, the user will be presented again with screen 30.

[0033] FIGs. 5-1, 5-2, and 5-3 are illustrations of an exemplary screen 50 listing the results of the scanning. All available wireless local area networks that have been identified during scanning are listed. If the number of available networks exceeds that which can be viewed simultaneously, a scrollbar 51 may be used to scroll through the entire list.

[0034] In the example shown in FIGs. 5-1, 5-2, and 5-3, six different available wireless local area networks are listed. WLANs for which a persistent connection profile is saved in device 1 are identified in the list by connection profile name (e.g. "Home", "Coffee Shop") and WLANs for which a connection profile is not saved in device 1 are identified in the list by network name (e.g. "Rosencrantz", "Guildenstern", "Symbol"). WLANs for which a connection profile is saved in device 1 are further identified by the description "Saved", except for a WLAN to which device 1 is currently connected, if any. If device 1 is currently connected to a WLAN, that WLAN is displayed first in the list, regardless of its

signal strength as perceived by device 1. The WLAN to which device 1 may be further identified by the text description "Connected" or by a visual indicator 52, for example, a graphic, or by both. The text description and the visual indicator are displayed near an identifier of the WLAN to which the WLAN client device is currently connected. In this example, visual indicator 52 is a checkmark.

[0035] Available WLANs to which device 1 is not currently connected are displayed in the list ordered by decreasing received signal strength at device 1. Each available wireless local area network appears in the list with a visual indicator 53 of its signal strength as perceived by device 1. In this example, visual indicator 53 is a graphic of a radio tower broadcasting radio waves. The size and number of radio waves is indicative of the signal strength, which may be abstracted to three values: high, medium and low. In the example shown in FIGs. 5-1, 5-2 and 5-3, the WLAN to which device 1 is currently connected, identified by its connection profile name "Coffee Shop", is listed first even though it has a lower received signal strength than the WLAN identified by its network name "Rosencrantz".

[0036] Device 1 may identify the security configurations of the available WLANs from the scan results. For example, device 1 may identify whether the security configuration of the WLAN is none, Wired Equivalent Privacy (WEP), PSK (also known as "WPA-Personal") or IEEE 802.1X (also known as "WPA-Enterprise"). Each available wireless local area network for which a connection profile is not saved in device 1 appears in the list with a description of its security requirements (e.g. "No Security", "Security: WEP", "Security: WPA-Personal", "Security: WPA-Enterprise"). For anything other than "No Security", a visual indicator 54 of its security requirements is also displayed. In this example, visual indicator 54 is a graphic of a lock. In alternative implementations, different visual indicators could be used to indicate different security requirements.

[0037] As will be described in further detail below, device 1 may save a connection profile as a persistent connection profile or as a transient connection profile. Visual indicators may be employed to distinguish available WLANs for which transient connection profiles are saved in device 1 from available WLANs for which a persistent connection profile is saved in device 1. For example, the WLAN may appear in the list identified by its connection profile name (e.g. "Temporary") and its network name (e.g.

"Proxim"), concatenated into a single string. Moreover, that string may be displayed in italicized text.

[0038] Navigating to and selecting a particular available WLAN in the list will indicate that the user wants to have device 1 connect to the selected WLAN. If no security is required by the selected WLAN, device 1 may directly attempt to connect to the select WLAN, as described below with respect to FIG. 7. If security credentials are required, the user will be prompted to supply security credentials for the selected WLAN, as described below with respect to FIGs. 6-1, 6-2, 6-3, 6-4, 6-5, 6-6, 6-7, 6-8, 6-9 and 6-10.

[0039] FIG. 5-2 illustrates a view of screen 50 in which a menu 55 associated with screen 50 is opened by the user. Navigating to a particular available WLAN in the list and then selecting a menu item 56 entitled "Connect" has the same effect as selecting the list item. Navigating to a particular available WLAN in the list and then selecting a menu item 57 entitled "Refresh" will cause device 1 to scan again for wireless local area networks, as described above. Navigating to a particular available WLAN in the list and then selecting a menu item 58 entitled "Manage Saved Wi-Fi Networks" will launch the WLAN profile management application, which is described in more detail below with respect to FIGs. 12-1 and 12-2.

[0040] Navigating to a particular available WLAN in the list and then selecting a menu item 59 entitled "Network Details" will result in a popup window being shown with details of the particular available WLAN, as shown in FIG. 5-3. In this example, the user has selected the available WLAN with the network name "Rosencrantz", which has the strongest signal strength.

[0041] <u>Preferred Connection Profiles</u>

[0042] A user of device 1 may be able to designate one or more connection profiles of WLANs saved in the device as "preferred". For example, when creating a connection profile of a WLAN, there may a check box or radio button or other graphical user-interface element that enables the designation of the connection profile as preferred. In another example, menu 22 associated with the WLAN profile management application may include a menu item (not shown) the text of which toggles between "Preferred" if a selected connection profile is not designated as preferred and "Not Preferred" if the selected

connection profile is designated as preferred. Selecting that menu item will toggle the preferred/not preferred status of the selected connection profile. Other user interface means for enabling designation of one or more connection profiles as preferred or not preferred are also contemplated.

[0043] When displaying the results of scanning, available wireless local area networks matching preferred connection profiles may be treated differently than other available wireless local area networks. In one aspect, scan results may be filtered so that only matches to preferred connection profiles are displayed at the device. For example, the connection profiles named "Coffee Shop" and "Home" may have been designated as preferred and the results of the scanning may be such that there are available WLANs matching those connection profiles. As illustrated in FIG. 5-4, a screen 501 of available WLANs may display only those available WLANs that match one of the preferred connection profiles. To accomplish this, device 1 may include in a list of available WLANs those available WLANs for which a preferred connection profile is saved in device 1, and device 1 may exclude from the list any other available WLANs. Device 1 may then display the list or a portion thereof on its display.

[0044] In another aspect, a displayed list of available WLANs may distinguish in the list available WLANs for which a preferred connection profile is saved in device 1 from other available WLANs in the list. For example, the connection profiles named "Coffee Shop" and "Home" may have been designated as preferred and the results of the scanning may be such that there are available WLANs matching those connection profiles. As illustrated in FIG. 5-5, a screen 502 displaying a list of available WLANs may include a first sublist of available WLANs for which a preferred connection profile is saved in device 1 and a second sublist of the other available WLANs. The first sublist may include a header 504 that identifies the available WLANs in the sublist as preferred, and the second sublist may include a header 506 that is different than header 504.

[0045] One or more of the aspects of displaying a list of available WLANs that are described above with respect to FIGs. 5-1, 5-2 and 5-3 may also be applicable to the list of only those available WLANs that match one of the preferred connection profiles. Likewise, one or more of the aspects of displaying a list of available WLANs that are described above with respect to FIGs. 5-1, 5-2 and 5-3 may also be applicable to a list that distinguishes

between available WLANs that match one of the preferred connection profiles and other available WLANs, and may be applicable to the first sublist, the second sublist or both.

[0046] FIGs. 6-1, 6-2, 6-3, 6-4, 6-5, 6-6, 6-7, 6-8, 6-9 and 6-10 are illustrations of an exemplary screen 60 for user input of security credentials for a wireless local area network. If device 1 has identified the selected WLAN as having a PSK security configuration, screen 60 will appear as in FIG. 6-1, with editable text fields 61 and 62 to enable the user to input a password. This is the case for the example with the selected WLAN having the network name "Rosencrantz".

[0047] If device 1 has identified the selected WLAN as having a WEP security configuration, screen 60 will appear as in FIG. 6-2, with an editable text field 64 to enable the user to input a WEP key.

[0048] If device 1 has identified the selected WLAN as having an IEEE 802.1X security configuration, but is unable to which identify which Extensible Authentication Protocol (EAP) is being used, screen 60 will appear as in one of FIGs. 6-3, 6-4, 6-5, 6-6, 6-7, 6-8, 6-9 and 6-10, with a drop-down menu 65 of EAP-based security types.

[0049] In FIGs. 6-3, 6-4, 6-5, and 6-6, editable text fields 66 and 67 enable the user to input a user name and password. In FIGs. 6-7 and 6-8, the International Mobile Subscriber Identity (IMSI) of device 1 is displayed. In FIG. 6-9, a client certificate stored in device 1 is displayed. If more than one client certificate is stored in device 1, then as shown in FIG. 6-10, screen 60 includes a drop-down menu 68 listing the client certificates.

[0050] All of FIGs. 6-1, 6-2, 6-3, 6-4, 6-5, 6-6, 6-7, 6-8, 6-9 and 6-10 have a button 63 entitled "Next", which when selected by the user will cause device 1 to attempt to connect to the selected WLAN, using the security credentials provided in screen 60.

[0051] FIG. 7 is an illustration of an exemplary screen 70 which may appear while the device is attempting to connect to the selected WLAN. Upon successfully connecting to a WLAN, device 1 obtains an Internet Protocol (IP) address. If device 1 successfully connects to the selected WLAN and a connection profile of the selected WLAN is already saved in device 1, then screen 70 closes and, returning briefly to FIG. 1, an icon 14 is displayed in home screen 2. Icon 14 indicates to the user that the device is connected to a WLAN.

[0052] If device 1 successfully connects to a WLAN for which a connection profile is not saved in device 1, a connection profile screen may be displayed. FIGs. 8-1 and 8-2 are illustrations of an exemplary screen 80 which may appear if the attempt to connect to the WLAN is successful and a connection profile is not saved for the WLAN. The user is asked whether to save the connection information (e.g. SSID, security credentials, other information gleaned from the scan result or the connection process) in a persistent connection profile. By saving a persistent connection profile, the user will not need to reenter the security credentials when connecting to this WLAN in the future. A "Yes"/"No" toggle button 81 is displayed. An editable text field 82 enables the user to input a name for the persistent connection profile. If button 81 is set to "Yes", selecting a button 83 entitled "Next" causes device 1 to attempt to create a persistent connection profile for the newly connected WLAN with the connection profile name provided in text field 82. In this example, the user has provided the connection profile name "Suzie's Home" for the WLAN with the network name "Rosencrantz".

[0053] If a connection profile with that connection profile name is already saved in device 1, a popup window 84 as shown in FIG. 8-2 is displayed to inform the user of this and to enable the user to select, via a "Yes" button 85 or a "No" button, whether to replace the existing connection profile. If the user selects "Yes", then device 1 creates a persistent connection profile for the newly connected WLAN with the connection profile name provided by the user. If the user selects "No", popup window 84 disappears and the user is able to provide a different connection profile name via editable text field 82.

[0054] If device 1 is unable to connect to the WLAN because the security credentials provided in one of FIGs. 6-1, 6-2, 6-3, 6-4, 6-5, 6-6, 6-7, 6-8, 6-9 and 6-10 does not match the requirements of the WLAN, then the user is informed of this, for example, via a screen 86 as shown in FIG. 8-3. Selecting a button 87 entitled "Back" will bring the user back to one of FIGs. 6-1, 6-2, 6-3, 6-4, 6-5, 6-6, 6-7, 6-8, 6-9 and 6-10. In another implementation, instead of screen 86, a popup window with a single button may be displayed over screen 70.

[0055] If device 1 is unable to connect because it is out of the coverage area of the WLAN, then the user is informed of this, for example, via a screen 88 as shown in FIG. 8-4. Screen 88 differs from screen 80 only in that a description 89 explaining that the device

is out of the coverage area is displayed. By saving a persistent connection profile, the user will not need to reenter the security credentials when connecting to this WLAN in the future. This is helpful even in the situation where the user was unable to connect to the WLAN due to being out of the coverage area of the WLAN. If button 81 is set to "Yes", selecting button 83 entitled "Next" causes device 1 to attempt to create a persistent connection profile for the newly connected WLAN with the connection profile name provided by the user. As with screen 80, if a connection profile with that connection profile name is already saved in device 1, popup window 84 will be displayed.

[0056] If, in screen 80 or screen 88, toggle button 81 is set to "No", selecting button 83 entitled "Next" may cause device 1 to attempt to create a transient connection profile. A transient connection profile differs from a persistent connection profile in that its name is not chosen at creation by the user, and a transient connection profile has a limited lifetime. After a period of time, for example, 24 hours, a transient connection profile may be automatically deleted from the device without any user intervention. Alternatively, a transient connection profile may be stored in the device until overwritten with another transient connection profile. Persistent connection profiles, on the other hand, generally require user intervention in order to be deleted from the device.

[0057] Consider the situation where a user is in an area of WLAN coverage for a short period of time, for example, at an airport lounge. The user may choose not to save a persistent connection profile for the WLAN, knowing that he/she is not intending to be in that location for a long time. However, by saving a transient connection profile, if the device becomes disconnected from the WLAN, attempts to reconnect to the WLAN will be easier and require less intervention from the user, than if no connection information for the WLAN is stored in the device.

[0058] Transient connection profiles may be automatically assigned connection profile names, for example, "Temporary 1", "Temporary 2", etc. The SSID of the WLAN may be incorporated into the connection profile name of the transient connection profile.

[0059] If creation of the connection profile, whether persistent or transient, is successful, the device will proceed to display the next screen.

[0060] In alternate implementations, if in screen 80 or screen 88 select button 81 is set to "No", selecting button 83 entitled "Next" may cause device to proceed to the next screen without creating any connection profile.

[0061] A virtual private network (VPN) is a private communications network used to communicate confidentially over a publicly accessible network. VPN message traffic can be carried over a public network infrastructure (e.g. the Internet) on top of standard protocols. VPNs are used, for example, to enable employees to connect securely to a corporate network. If a VPN client application is installed on device 1 and one or more VPN profiles have been defined, then the next screen following screen 80 or screen 88 is a VPN selection screen, as shown in FIGs. 9-1 and 9-2. Otherwise the next screen is a setup completion screen, as shown in FIGs. 10-1 and 10-2.

[0062] FIGs. 9-1 and 9-2 are illustrations of an exemplary screen 90 for VPN profile selection. Screen 90 is displayed only if one or more VPN profiles have been defined in device 1. In alternate implementations, screen 90 is always displayed and enables a user to define a VPN profile if none are defined yet.

[0063] If a single VPN profile is defined in device 1, screen 90 is displayed as shown in FIG. 9-1, with an indication of the VPN profile, e.g. the label "ABC-HQ", displayed in a text field 92. If two or more VPN profiles are defined in device 1, screen 90 is displayed as shown in FIG. 9-2, with a drop-down menu 94 listing indications of the VPN profiles, for example, their labels.

[0064] A user specifies, via a "Yes"/"No" toggle button 96, whether to use one of the VPN profiles with the WLAN to which device 1 has just connected. If button 96 is set to "No", selecting a button 98 entitled "Next" causes a setup completion screen to be displayed. If button 96 is set to "Yes", selecting button 98 causes device 1 to attempt, using the VPN client application, to connect to establish a VPN connection according to the VPN profile which label is displayed in text field 92 or selected in drop-down menu 94. If a connection profile for the WLAN is saved, device 1 associates the VPN profile with the connection profile of the WLAN so that subsequent connections of the device to the WLAN will automatically attempt to establish a VPN connection according to the associated VPN profile after the device obtains an IP address.

[0065] FIGs. 10-1 and 10-2 are illustrations of an exemplary setup completion screen 100. By selecting a button 102 entitled "Finish", screen 100 closes and icon 14 is displayed in home screen 2 (see FIG. 1) to indicate to the user that the device is connected to a WLAN. Screen 100 includes a message 103 informing the user that the connection profile of the WLAN to which device 1 has connected has been saved. Screen 100 also includes a button 104 entitled "Prioritize Wi-Fi Profiles" which, if selected, will close screen 100 and launch the profile management application.

[0066] Hotspot Registration

[0067] A hotspot is a venue that offers access to the Internet via a wireless local area network. Upon connecting to the WLAN, a WLAN client device is given an IP address. Access to a public network such as the Internet is provided by the WLAN via a gateway. The gateway may implement one or more IP filtering rules to limit IP addresses that can be accessed by the WLAN client device, thus providing access to what is known as a "walled garden". Subscription may be required and fees may apply in order to gain access to the public network.

[0068] Once device 1 has successfully connected to a WLAN, it sends via the WLAN a hypertext transfer protocol (HTTP) request to a particular IP address that is not normally redirected. This occurs automatically in the background, without any intervention by the user and without providing any feedback to the user. If the device receives a redirection response to the HTTP request, then device 1 has detected that the WLAN to which it is connected is offered by a hotspot. In this situation, device 1 may display an indication of this. For example, device 1 may display screen 100 as it appears in FIG. 10-2, rather than as it appears in FIG. 10-1. As shown in FIG. 10-2, screen 100 includes a description 105 about hotspots and a button 106 entitled "Hotspot Registration". Selecting button 106 launches a browser application of device 1 with an IP address that ought to trigger an IP filtering rule of the gateway. The browser will be redirected to a captive portal of the hotspot that may enable the user to register for access to the public network.

[0069] In an alternate implementation, upon detecting in the background that a WLAN to which device 1 has just connected is offered by a hotspot, where access to the Internet is provided by the wireless local area network via a gateway, a browser application of device

1 is automatically launched with an IP address that ought to trigger an IP filtering rule of the gateway.

[0070] Manually adding Networks

[0071] Returning briefly to FIG. 3, if the user selects button 34 entitled "Manually Add Network", the user will be prompted to specify the WLAN that the user wants device 1 to connect to. FIG. 11 is an illustration of an exemplary screen 110 that may appear after the user selects button 34. Using keyboard 4, the user may type the name of the network (SSID), which will appear in an editable text field 112. In the example shown in FIG. 11, the user has typed "BLUEBIRD". If the user then presses a button 114 entitled "Next", the user will be prompted to supply security credentials for the WLAN via screen 60, as described above with respect to FIGs. 6-1, 6-2, 6-3, 6-4, 6-5, 6-6, 6-7, 6-8, 6-9 and 6-10.

[0072] In an alternate implementation, when the user presses button 114, device 1 may scan for a WLAN having "BLUEBIRD" as its SSID. Device 1 may employ passive scanning techniques, active scanning techniques or any combination thereof. From the scan results, device 1 may identify whether the security configuration of the WLAN is none, WEP, PSK or IEEE 802.1X. If no security is required, device 1 may directly attempt to connect to the WLAN, and screen 70 will be displayed with the text "Connecting to *BLUEBIRD* ..." instead of "Connecting to *Rosencrantz* ...". If security credentials are required, the user will be prompted to supply security credentials for the WLAN via screen 60, as described above with respect to FIGs. 6-1, 6-2, 6-3, 6-4, 6-5, 6-6, 6-7, 6-8, 6-9 and 6-10. If the scan results identify PSK as the configuration, screen 60 may appear as in FIG. 6-1. If the scan results identify WEP as the configuration, screen 60 may appear as in FIG. 6-2. If the scan results identify IEEE 802.1X but do not distinguish between the different types, screen 60 may appear with the drop-down options of security type restricted to the various EAP types.

[0073] WLAN Profile Management Application

[0074] FIGs. 12-1 and 12-2 are illustrations of exemplary screen 20 of a wireless local area network profile management application. Connection profiles of WLANs are listed in screen 20 in decreasing order of priority. The relative priority of connection profiles may affect the order in which those connection profiles are compared to scanning results and

therefore may also affect the order in which the device attempts to connect to WLANs matching those connection profiles. Connection profiles may be created with the lowest relative priority, by default.

[0075] The connection profile of the WLAN with which device 1 is currently connected may be automatically selected when opening screen 20, as indicated by a highlight bar 120. Further visual indications of the connection profile of the WLAN with which device 1 is currently connected include the connection profile name in a text field 121 near the description "Active Wi-Fi Connection" and a checkmark 122 next to the connection profile in the list. If device 1 is currently connected to a WLAN for which a connection profile is not saved, then the network name of that WLAN is displayed in text field 121. If device 1 is not connected to a WLAN, then text field 121 is blank or displays the text "None". A cross 123 identifies connection profiles of WLANs with which device 1 is not currently connected. If screen 20 is opened when device 1 is not connected to any WLAN, then the connection profile with the highest priority may be automatically selected. Alternatively, a newly created connection profile may be automatically selected in screen 20.

[0076] As is known in the art, scanning for WLANs may be performed in one of the following ways:

[0077] Manual Scans – A user initiates a scan for either a specific WLAN or for all available WLANs.

[0078] Background Profile Scans – Scans that occur from time to time in the background without user intervention, even if the device is already connected to a WLAN. Scan results are filtered to exclude WLANs having a received signal strength below a threshold. The enabled connection profile with the highest priority is then compared to the filtered scan results and if there is a match, the device attempts to connect to the matching WLAN. If there is no match, the enabled connection profile with the next highest priority is compared to the filtered scan results, and so on. Disabled connection profiles are not compared to the filtered scan results. The terms "enabled" and "disabled" are intended to distinguish between connection profiles of WLANs that are checked against results of background profile scans (and hence are termed "enabled") and connection profiles of WLANs that are not checked against the results (and hence are termed "disabled").

[0079] Neighbor Scans – Scans that occur from time to time in the background without user intervention, when the device is connected to a WLAN via an association with an access point. The scanning is restricted to neighboring access points within an IP subnetwork, based on the assumption that WLANs on different IP subnets have different SSIDs. If the quality of the wireless link between the device and the access point with which the device is associated drops below a threshold, the device may associate instead with a neighboring access point on the same IP subnetwork.

[0080] A visual indicator 124 of a broadcasting access point identifies enabled connection profiles and a visual indicator 125 of an access point with a cross identifies disabled connection profiles.

[0081] Returning briefly to FIG. 2, menu 22 associated with the WLAN profile management application applies to the selected connection profile. Selecting a menu item 25 entitled "Move Selection" enables the user to adjust the priority of the selected connection profile relative to the other connection profiles in the list by moving the selected connection profile within the list. For example, by adjusting a trackball or thumbwheel or by pressing the appropriate keys in a keyboard, the user may provide input to move the selected connection profile within the list. As the input is detected and processed, the list of connection profiles is updated to show the selected connection profile at a location in the list corresponding to the input. For example, if the input is a slight upwards motion of the trackball (where upwards is defined as the direction towards the top edge of the device), the selected connection profile will be displayed higher in the list than before.

[0082] The text of a menu item 26 toggles between "Disable" if the selected connection profile is enabled and "Enable" if the selected connection profile is disabled. Selecting menu item 26 will toggle the enabled/disabled status of the selected connection profile.

[0083] Selecting a menu item 27 entitled "Scan" will cause device 1 to scan for and attempt to connect to the WLAN matching the selected connection profile. A user may also initiate this by clicking the selected connection profile or providing other appropriate input (for example, pressing an "Enter" button on the keyboard) while a connection profile is selected and menu 22 is closed.

[0084] Returning to FIGs. 12-1 and 12-2, a Wi-Fi selection mode "Automatic"/"Manual" toggle button 126 allows the user to enable or disable background profile scanning. If button 126 is set to "Manual", as shown in FIG. 12-2, then radio buttons 127 appear next to the connection profiles and the user may select which of the connection profiles to scan for and attempt to connect to.

[0085] Other ways to launch Wireless Connections Management Application

[0086] Returning briefly to FIG. 1, icon 14 may appear in the home screen when device 1 is connected to a WLAN. If device 1 also has a WWAN communication interface, an icon 16 may appear in the home screen when device 1 is connected to a WWAN. Likewise, if device 1 also has a WPAN communication interface, an icon (not shown) may appear in the home screen when device 1 is connected to a WPAN. Selecting any of icons 14, 16 and the WPAN icon may launch a wireless connections management application. List 8 also includes an icon 18 which if selected will launch the wireless connections management application.

[0087] FIG. 13 is an illustration of an exemplary screen 130 shown when the wireless connections management application is launched. Selecting a menu item 132 entitled "Set Up Wi-Fi Network" will launch the WLAN connection setup application described above, beginning at screen 30 (described above with respect to FIG. 3).

[0088] Details of Handheld Device

[0089] FIG. 14 is a block diagram of an exemplary handheld device 1400. For clarity, some components and features of handheld device 1400 are not shown in FIG. 15 and are not described explicitly below. Handheld device 1400 includes a processor 1402 and a memory 1404 coupled to processor 1402. Handheld device 1400 includes an audio input element 1406, for example a microphone, an audio output element 1408, for example, a speaker, and an audio coder-decoder (codec) 1410, however, the technology described herein is also applicable to devices without these audio components.

[0090] Handheld device 1400 includes a display 1412 coupled to processor 1402. Handheld device 1400 also includes one or more user input elements 1414 coupled to processor 1402, for example, a keyboard and a trackball. Handheld device 1400 may include additional user input and/or output elements that are not shown in FIG. 15, for

example a thumbwheel. A keyboard may be embedded in full or in part within display 1412, i.e. display 1412 may be a touch screen.

[0091] Handheld device 1400 includes a WLAN communication interface 1416 coupled to processor 1402 and to an antenna 1418. Communication interface 1416 is compatible with one or more WLAN standards, for example, IEEE 802.11 or ETSI HIPERLAN, and includes a WLAN controller and a radio.

[0092] Handheld device 1400 optionally also includes a WWAN communication interface 1420 coupled to processor 1402 and to an antenna 1422. Communication interface 1420 is compatible with one or more WWAN standards, for example, cellular communication standards, and includes a WWAN controller and a radio.

[0093] Handheld device 1400 optionally also includes a WPAN communication interface 1424 coupled to processor 1402 and to an antenna 1426. Communication interface 1424 is compatible with one or more WPAN standards, for example, Bluetooth®, ZigBee™, radio frequency identification (RFID), ultra wideband (UWB) and the like.

[0094] Handheld device 1400 may optionally also include a Global Positioning System (GPS) receiver 1428 coupled to processor 1402 and to an antenna 1430.

[0095] Each communication interface includes a controller and a radio, and the radio is coupled to an antenna. Controllers may share the same hardware, but logically they are independent. Analog components of the radios may be shared, but digital components of the radios are most likely to be independent. Depending on the frequencies, antennas could be shared among the communication interfaces. By way of the communication interfaces and antennas, handheld device 1400 may be able to establish telephone and/or data communication sessions with other systems (not shown).

[0096] Data communication sessions may include data in the form of plain text, data files, voice files, image files, movie files, streaming audio, streaming video, animation, or any other suitable data form. A non-exhaustive list of examples for data communication sessions includes sending and receiving electronic mail (e-mail), sending and receiving instant messages, sending and receiving paging messages, sending and receiving short message service (SMS) messages, and any other suitable data communication sessions. For data communications supported by handheld device 1400, memory 1404 may store

respective application modules to be executed by processor 1402, for example, an e-mail application module 1432, an SMS application module 1434, a paging application module 1436, an instant messaging application module 1438, and a web browser application module 1440.

[0097] Memory 1404 stores a system management application module 1442 and may optionally store other application modules, for example, an address book or contacts application module 1444 and a calendar application module 1446. These application modules are just examples, and the technology described herein is also applicable to handheld devices with a different set of application modules.

[0098] Memory 1404 may store executable code 1448 which, when executed by processor 1402, implements a wireless connection setup application, and executable code 1450 which, when executed by processor 1402, implements a wireless connection profile management application.

[0099] Although the subject matter has been described in language specific to structural features and/or methodological acts, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to the specific features or acts described above. Rather, the specific features and acts described above are disclosed as example forms of implementing the claims.

What is claimed is:

1. A method for handling one or more virtual private network 'VPN' profiles defined in a wireless local area network 'WLAN' client device, the method comprising:

in response to connecting to a WLAN, enabling input, via a user input element of the WLAN client device, of an indication whether to attempt to establish a VPN connection over the WLAN using information stored in one of the one or more VPN profiles.

2. The method of claim 1, further comprising:

if more than one VPN profile has been defined in the WLAN client device, enabling selection, via a user input element of the WLAN client device, of which VPN profile to use in attempting to establish the VPN connection over the WLAN.

3. The method of claim 2, further comprising:

receiving, via a user input element of the WLAN client device, an indication to attempt to establish a VPN connection over the WLAN;

receiving, via a user input element of the WLAN client device, an indication of which VPN profile to use in attempting to establish the VPN connection; and

associating the VPN profile for which the indication has been received with a connection profile of the WLAN that is saved or to be saved in the WLAN client device.

4. The method of claim 2, further comprising:

receiving, via a user input element of the WLAN client device, an indication to attempt to establish a VPN connection over the WLAN;

receiving, via a user input element of the WLAN client device, an indication of which VPN profile to use in attempting to establish the VPN connection; and

attempting to establish the VPN connection.

5. The method of claim 1, further comprising:

if a single VPN profile has been defined in the WLAN client device, displaying via a display of the WLAN client device an indication of the VPN profile.

6. The method of claim 5, further comprising:

receiving, via a user input element of the WLAN client device, an indication to attempt to establish a VPN connection over the WLAN; and

associating the VPN profile with a connection profile of the WLAN that is saved or to be saved in the WLAN client device.

7. The method of claim 5, further comprising:

receiving, via a user input element of the WLAN client device, an indication to attempt to establish a VPN connection over the WLAN; and

attempting to establish the VPN connection.

8. A wireless local area network 'WLAN' client device comprising:

a processor;

an antenna;

a WLAN communication interface coupled to the processor and to the antenna;

a display coupled to the processor;

one or more user input elements coupled to the processor; and

a memory coupled to the processor, the memory storing one or more virtual private network 'VPN' profiles and storing executable code means which, when executed by the processor, in response to the WLAN client device connecting to a WLAN via the WLAN communication interface and the antenna, enables input via one of the user input elements of an indication whether to attempt to establish a VPN connection over the WLAN using information stored in one of the one or more VPN profiles.

9. The WLAN client device of claim 8, wherein the executable code means, when executed by the processor, if more than one VPN profile has been stored in the memory, enables selection via one of the user input elements of which VPN profile to use in attempting to establish the VPN connection over the WLAN.

10. The WLAN client device of claim 9, wherein the executable code means, when executed by the processor, receives via one of the user input elements an indication to attempt to establish a VPN connection over the WLAN, receives via one of the user input elements an indication of which VPN profile to use in attempting to establish the VPN connection, and associates the VPN profile for which the indication has been received with a connection profile of the WLAN that is saved or to be saved in the memory.

11. The WLAN client device of claim 9, wherein the executable code means, when executed by the processor, receives via one of the user input elements an indication to attempt to establish a VPN connection over the WLAN, receives via one of the user input elements an indication of which VPN profile to use in attempting to establish the VPN connection, and attempts to establish the VPN connection via the WLAN communication interface and the antenna.

12. The WLAN client device of claim 8, wherein the executable code means, when executed by the processor, if a single VPN profile has been stored in the memory, displays via the display an indication of the VPN profile.

13. The WLAN client device of claim 12, wherein the executable code means, when executed by the processor, receives via one of the user input elements an indication to attempt to establish a VPN connection over the WLAN, and associates the VPN profile with a connection profile of the WLAN that is saved or to be saved in the memory.

14. The WLAN client device of claim 12, wherein the executable code means, when executed by the processor, receives via one of the user input elements an indication to attempt to establish a VPN connection over the WLAN, and attempts to establish the VPN connection via the WLAN communication interface and the antenna.

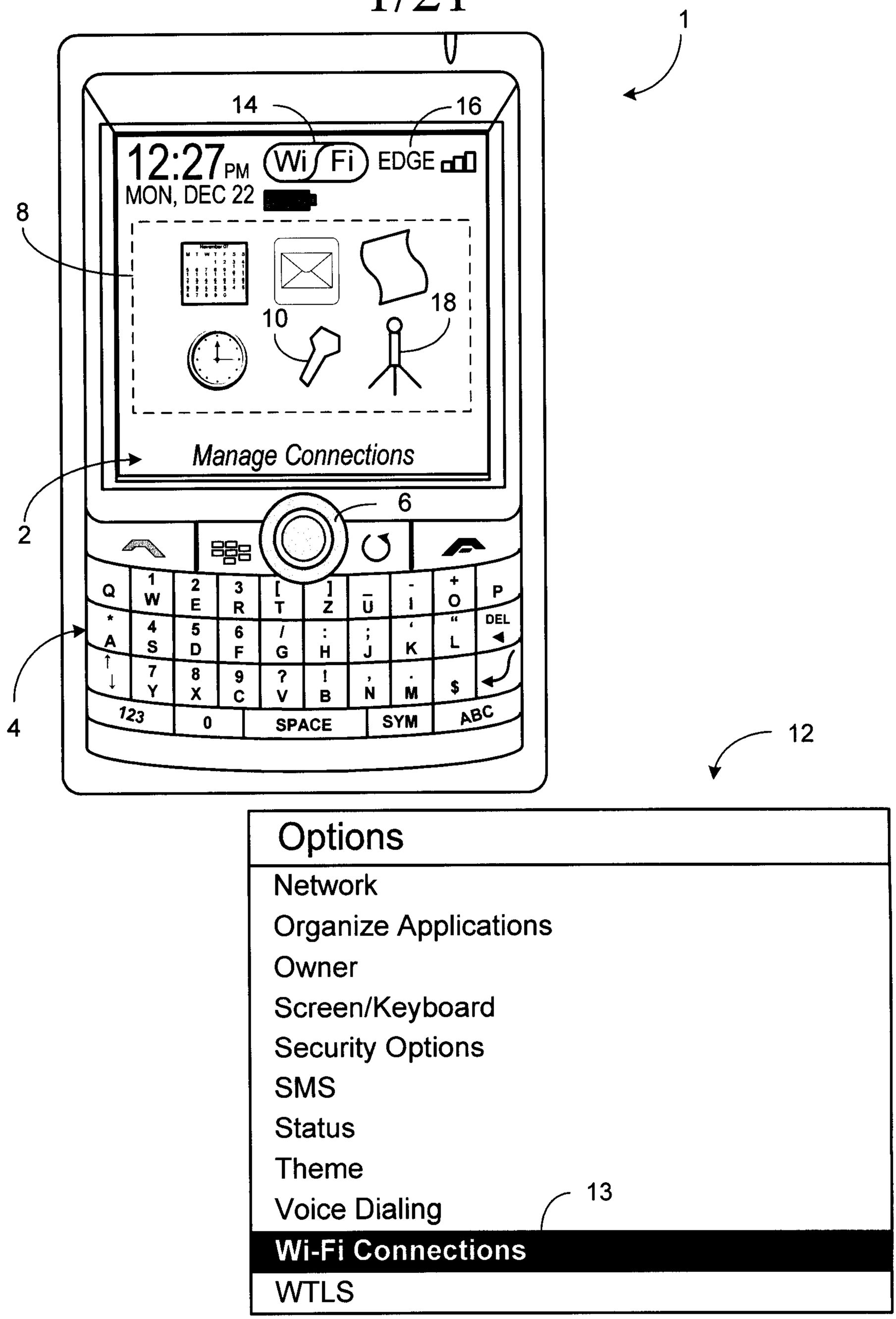

1
14
16
12:27 PM
Wi Fi
EDGE
MON, DEC 22
8
10
18
Manage Connections
2
6
4
12
Options
Network
Organize Applications
Owner
Screen/Keyboard
Security Options
SMS
Status
Theme
Voice Dialing
13
Wi-Fi Connections
WTLS

FIG. 1

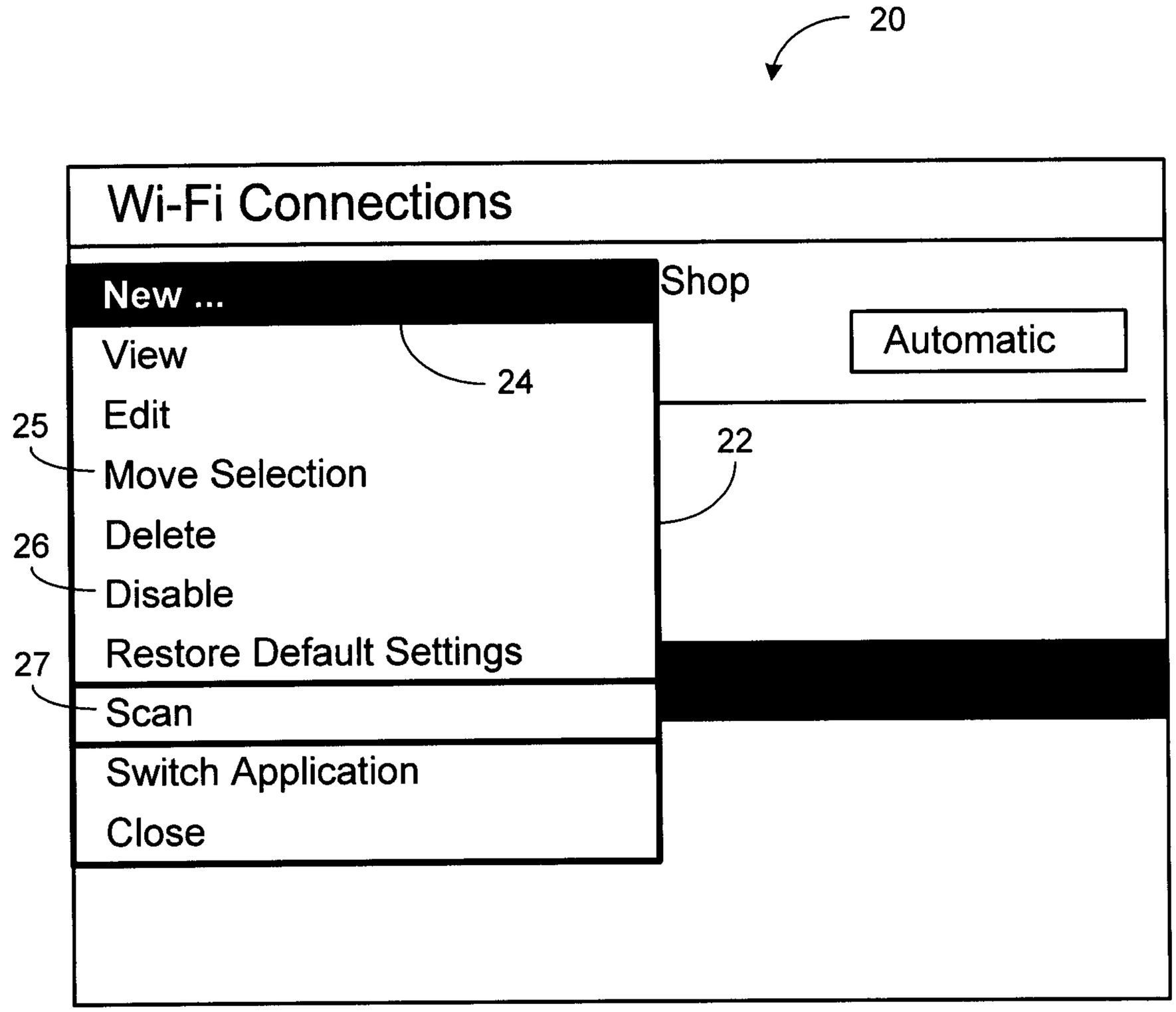

20
Wi-Fi Connections
New ...
View
Edit
Move Selection
Delete
Disable
Restore Default Settings
Scan
Switch Application
Close
Shop
Automatic
24
25
22
26
27

FIG. 2

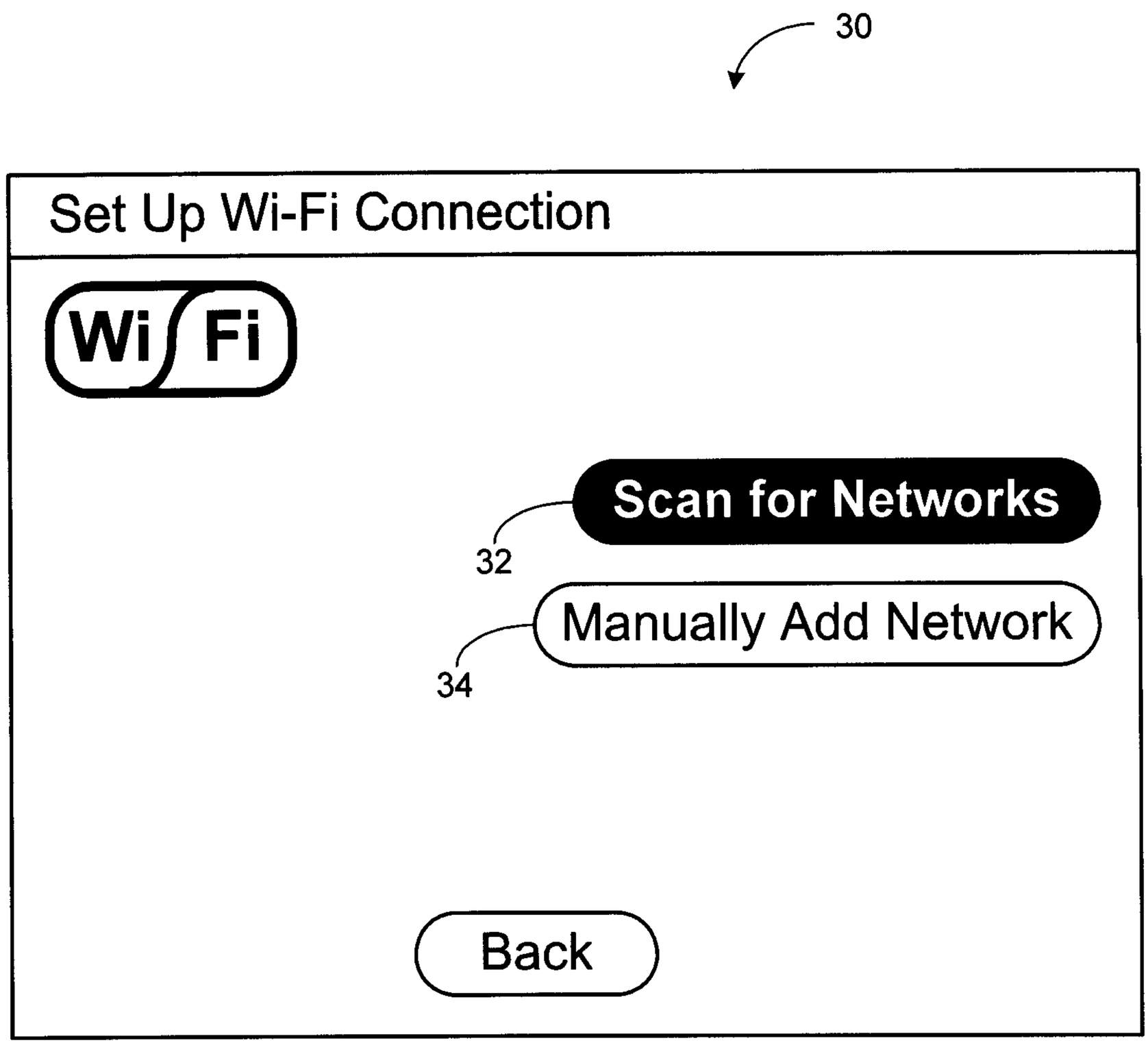

30
Set Up Wi-Fi Connection
Wi Fi
Scan for Networks
32
Manually Add Network
34
Back

FIG. 3

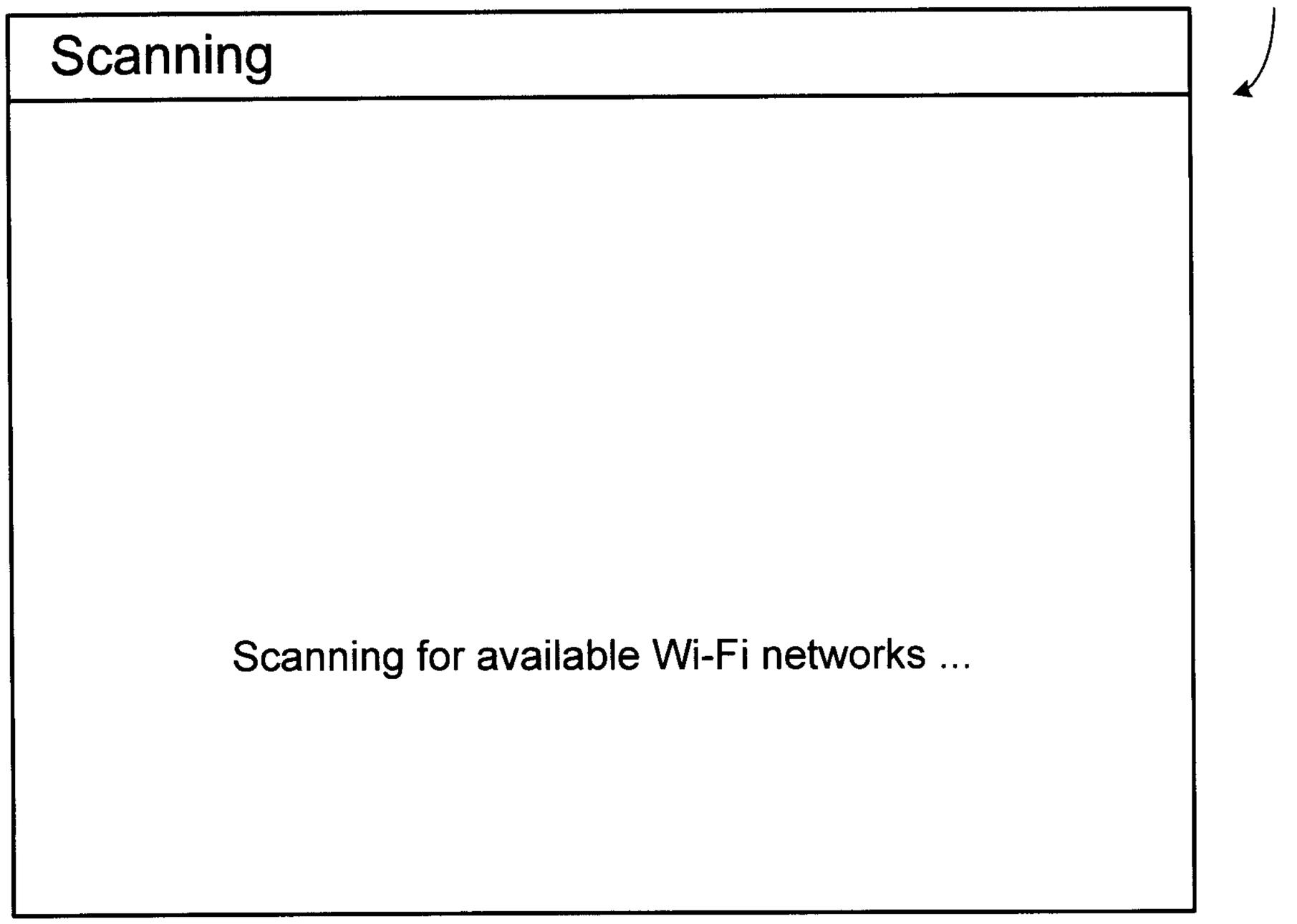

40
Scanning
Scanning for available Wi-Fi networks ...

FIG. 4-1

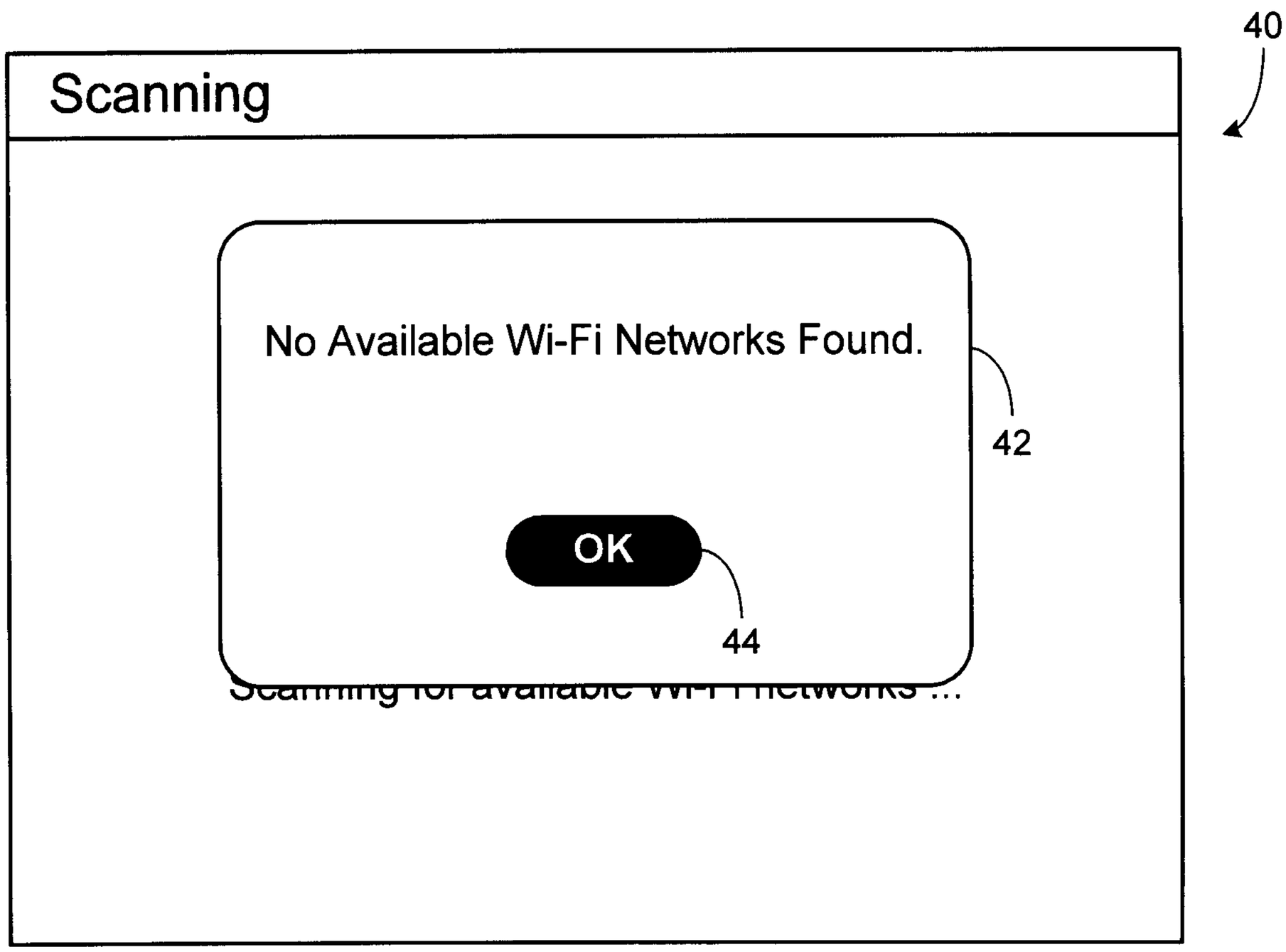

40
Scanning
No Available Wi-Fi Networks Found.
42
OK
44

FIG. 4-2

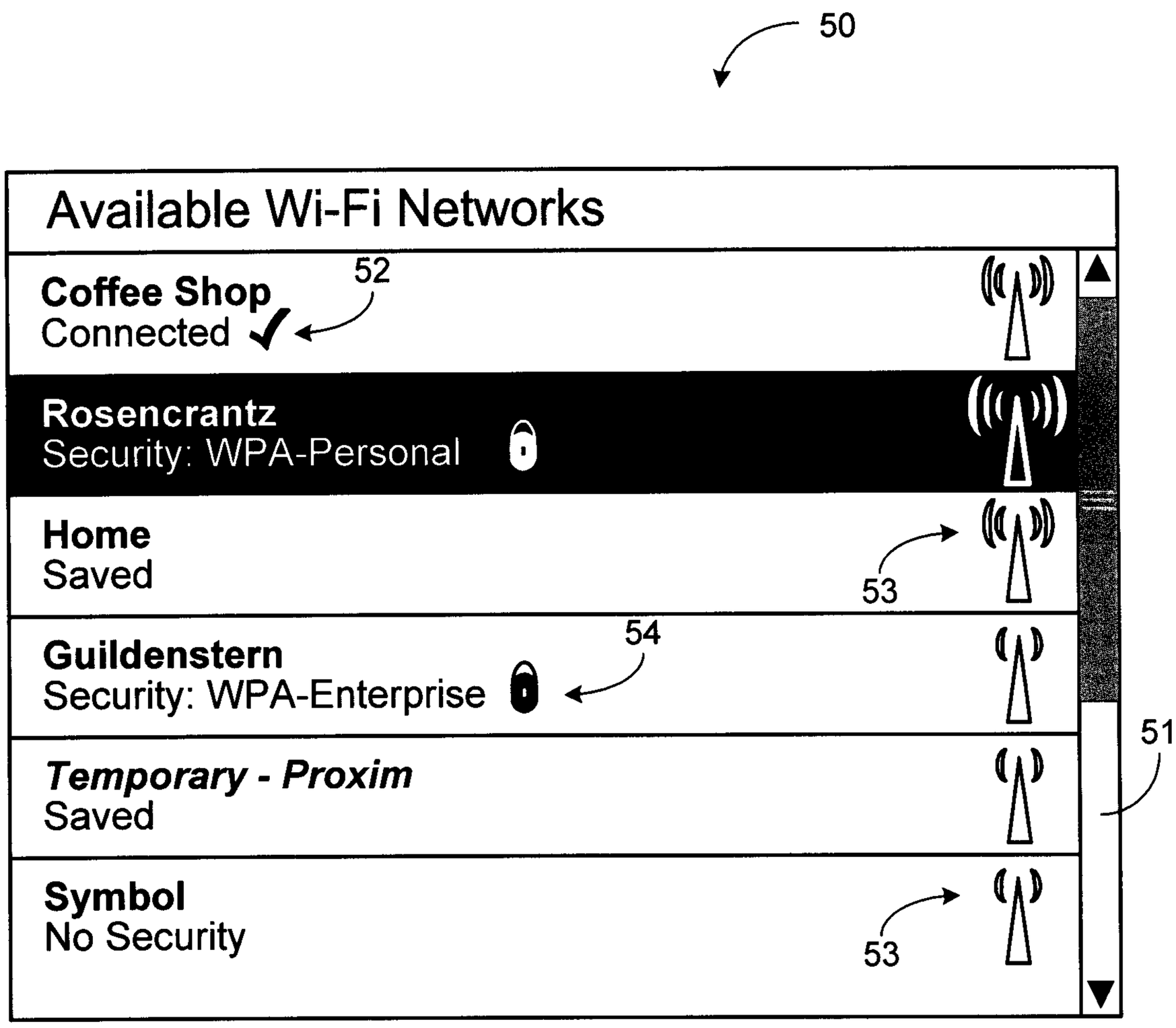

50
Available Wi-Fi Networks
Coffee Shop
Connected
52
Rosencrantz
Security: WPA-Personal
Home
Saved
53
Guildenstern
Security: WPA-Enterprise
54
Temporary - Proxim
Saved
Symbol
No Security
53
51

FIG. 5-1

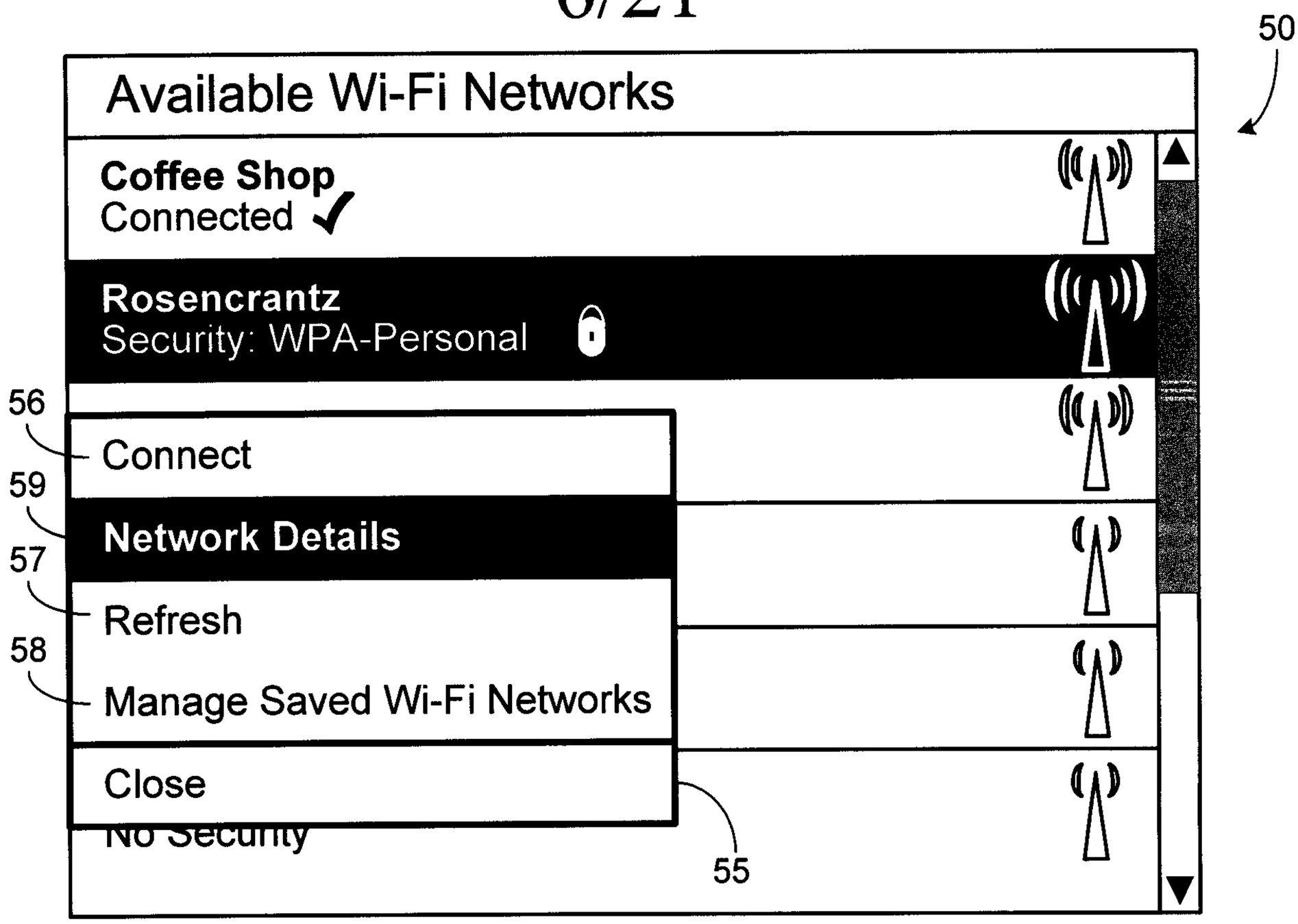

50
Available Wi-Fi Networks
Coffee Shop
Connected
Rosencrantz
Security: WPA-Personal
56
Connect
59
Network Details
57
Refresh
58
Manage Saved Wi-Fi Networks
Close
No Security
55

FIG. 5-2

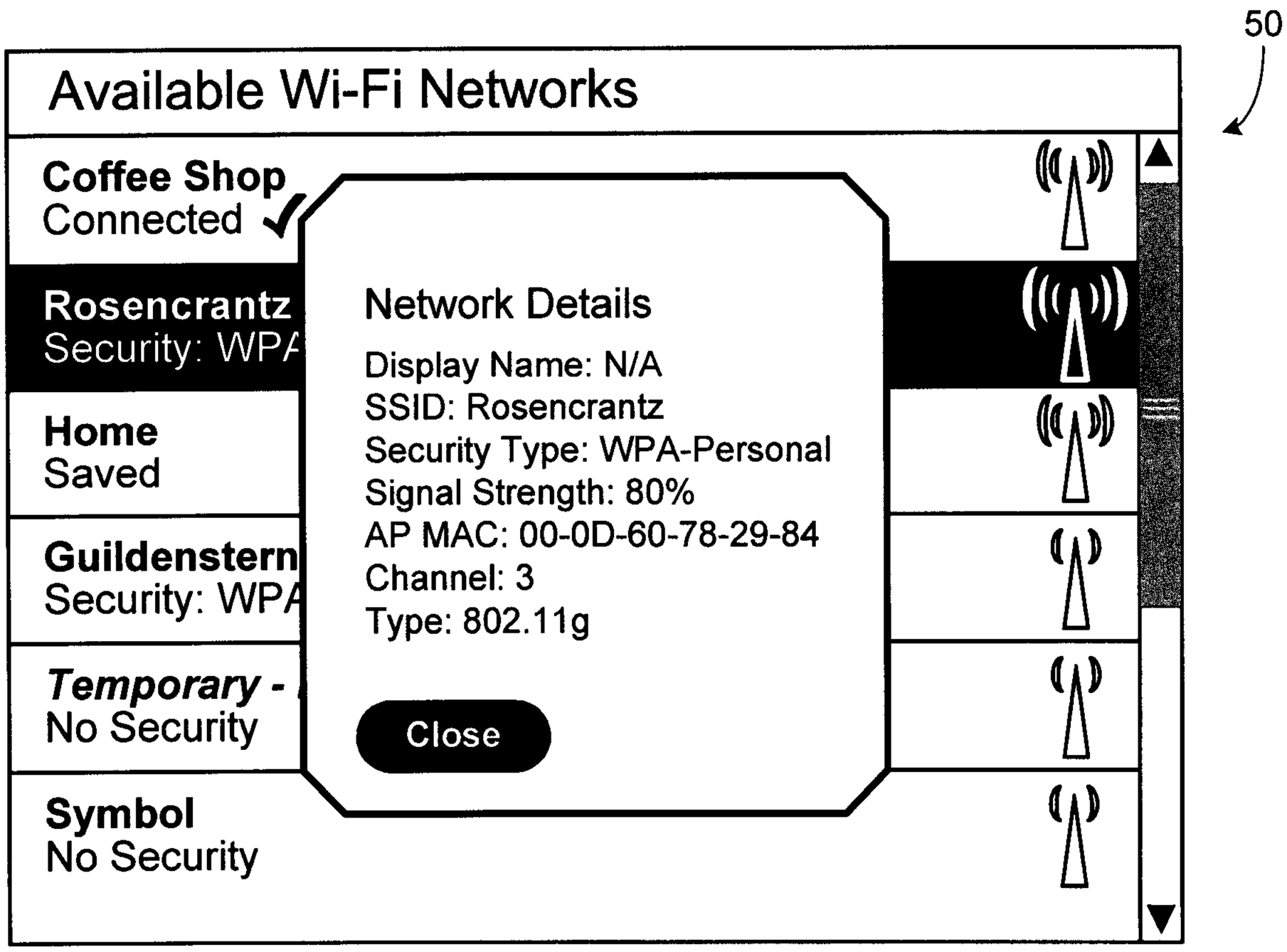

50
Available Wi-Fi Networks
Coffee Shop
Connected
Rosencrantz
Security: WPA
Home
Saved
Guildenstern
Security: WPA
Temporary -
No Security
Symbol
No Security
Network Details
Display Name: N/A
SSID: Rosencrantz
Security Type: WPA-Personal
Signal Strength: 80%
AP MAC: 00-0D-60-78-29-84
Channel: 3
Type: 802.11g
Close

FIG. 5-3

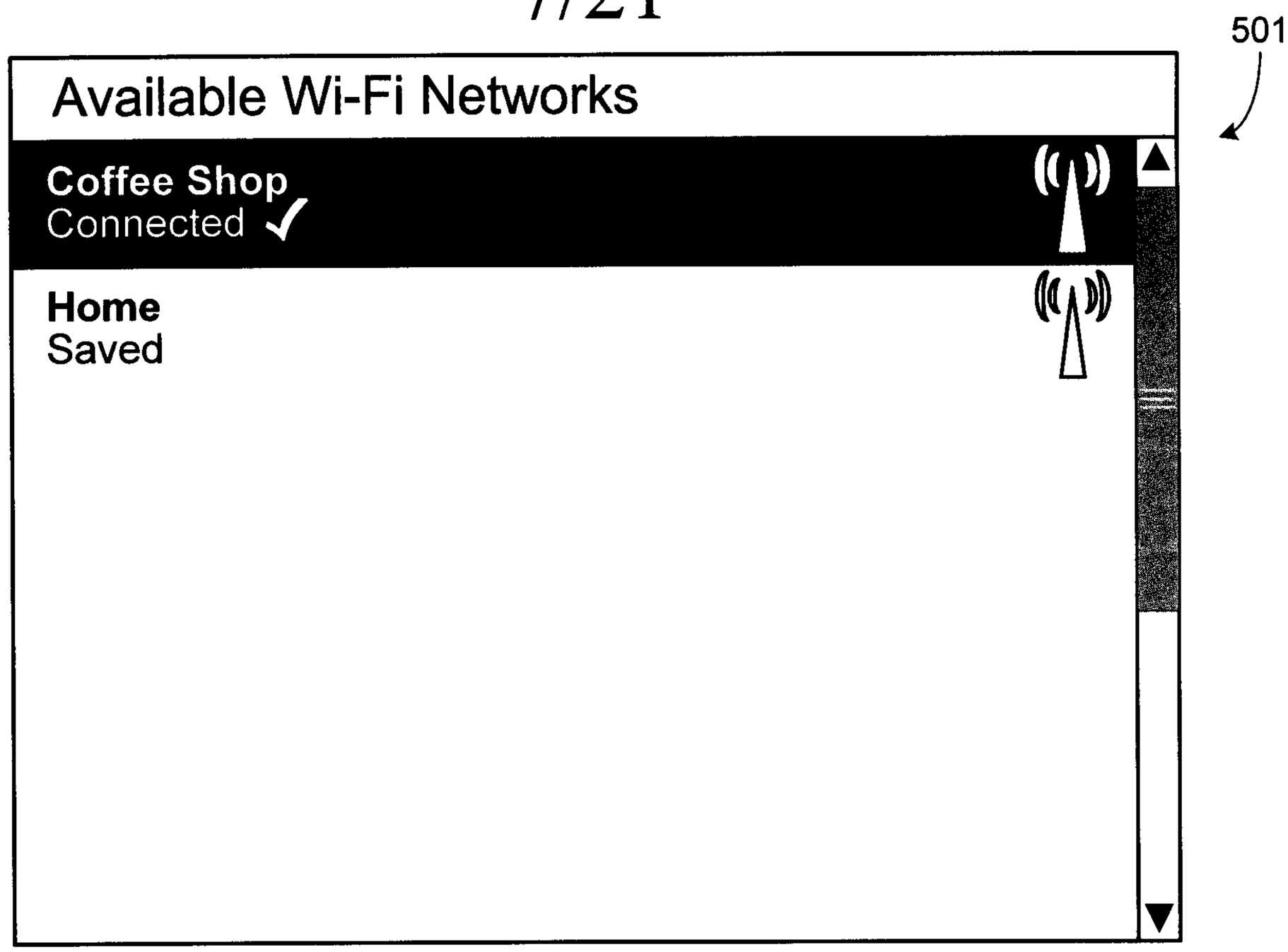

501
Available Wi-Fi Networks
Coffee Shop
Connected
Home
Saved

FIG. 5-4

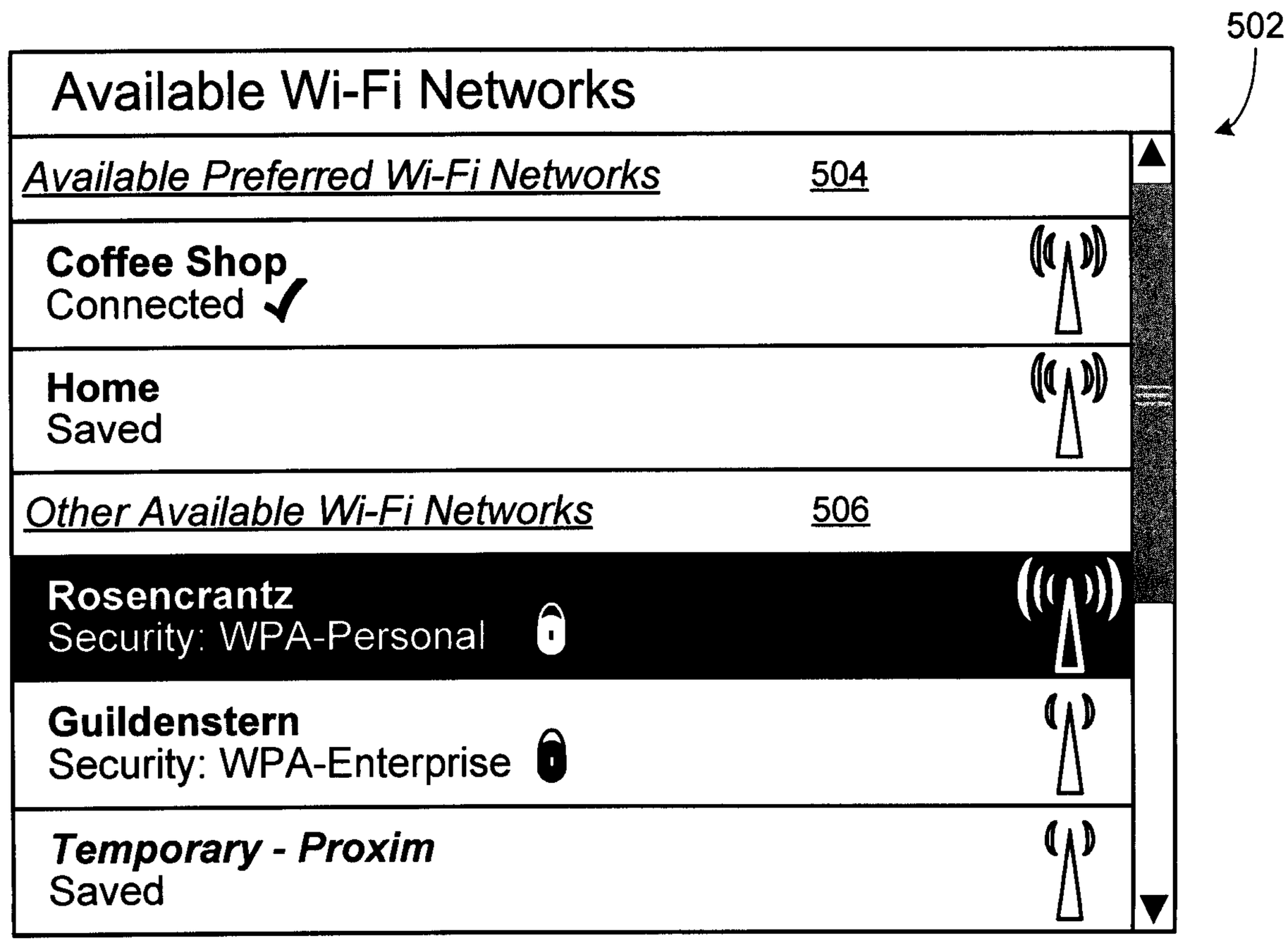

502
Available Wi-Fi Networks
Available Preferred Wi-Fi Networks
504
Coffee Shop
Connected
Home
Saved
Other Available Wi-Fi Networks
506
Rosencrantz
Security: WPA-Personal
Guildenstern
Security: WPA-Enterprise
Temporary - Proxim
Saved

FIG. 5-5

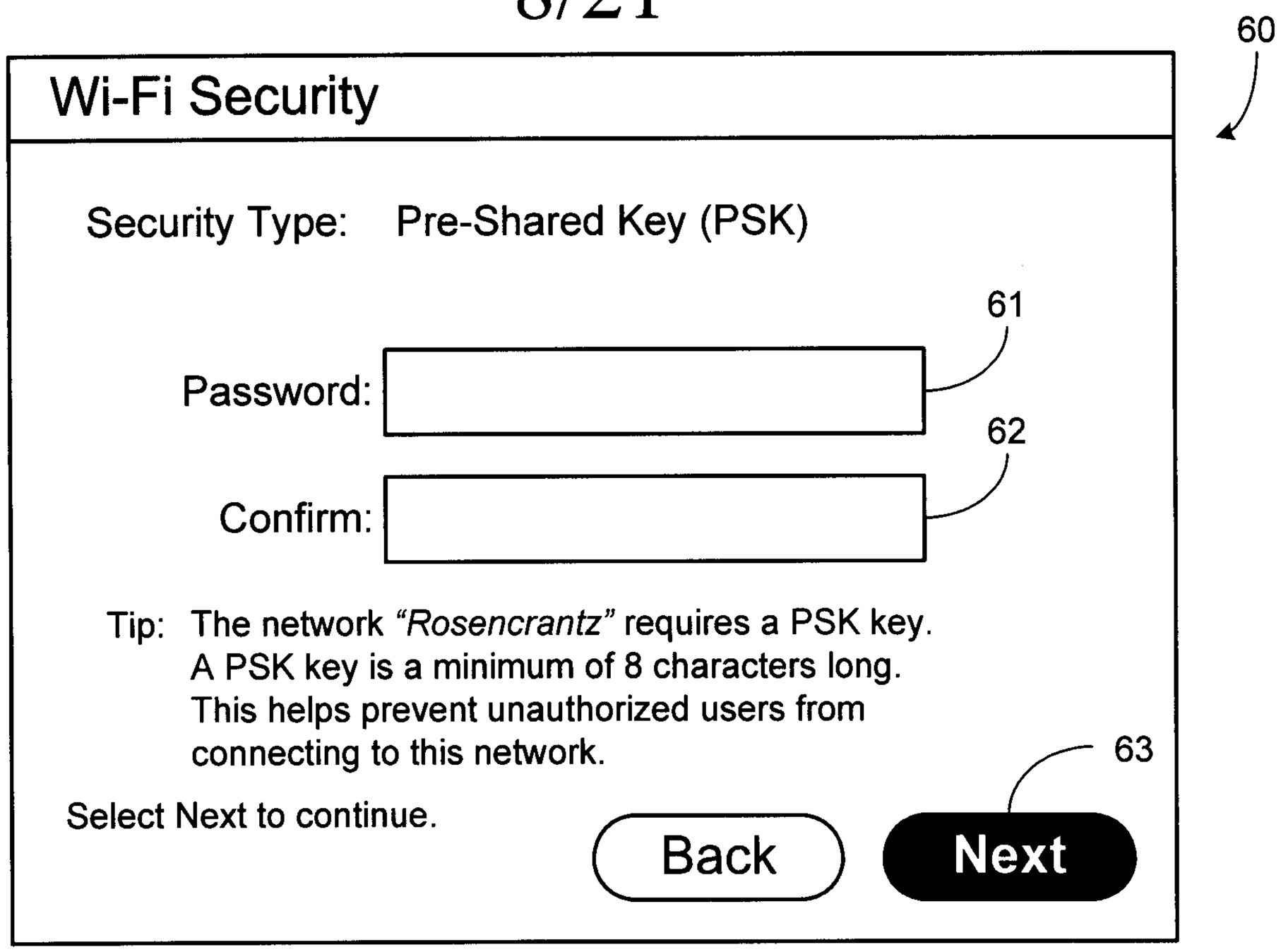

60
Wi-Fi Security
Security Type: Pre-Shared Key (PSK)
61
Password:
62
Confirm:
Tip: The network "Rosencrantz" requires a PSK key.
A PSK key is a minimum of 8 characters long.
This helps prevent unauthorized users from
connecting to this network.
63
Select Next to continue.
Back
Next

FIG. 6-1

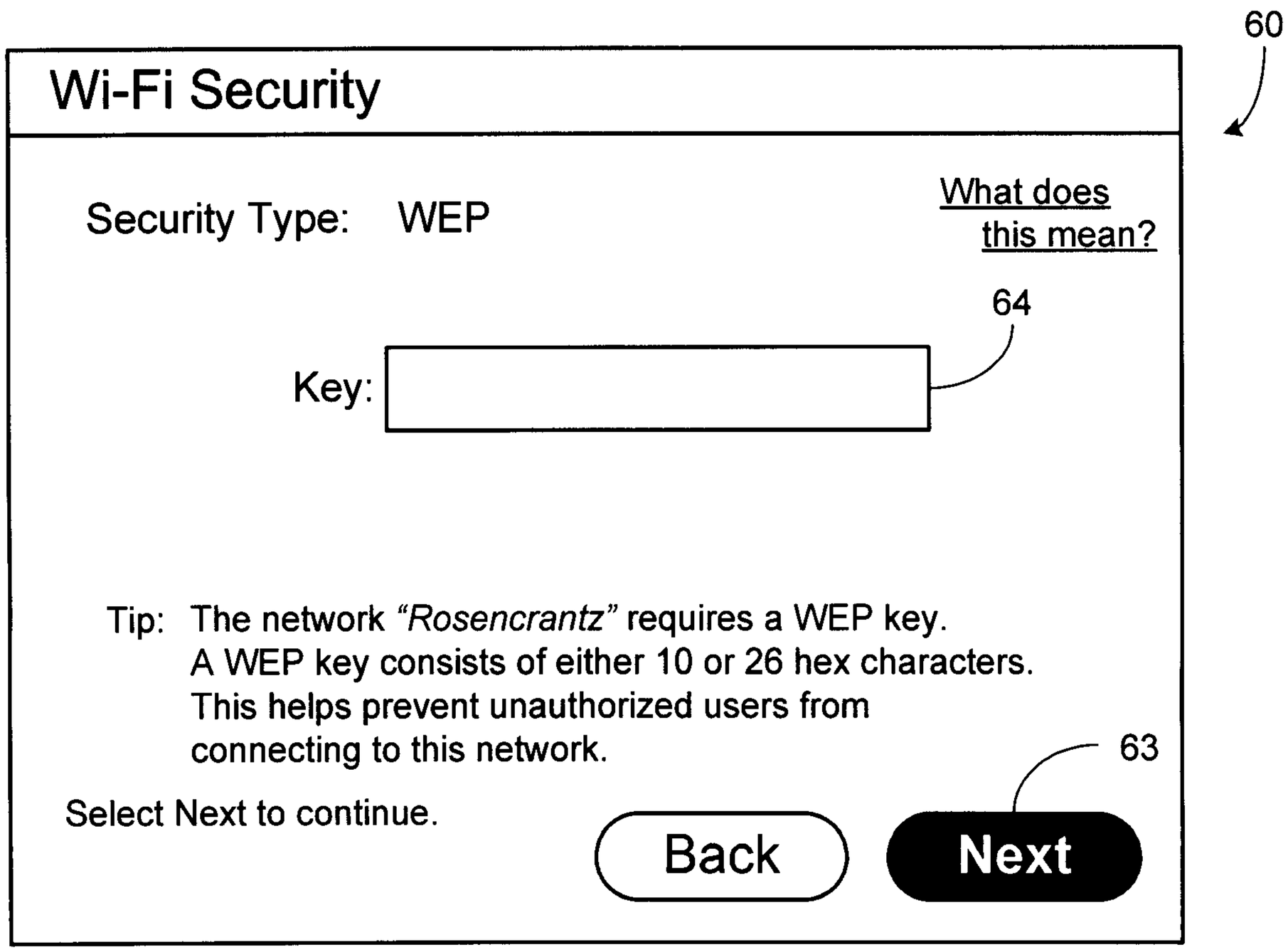

60
Wi-Fi Security
Security Type: WEP
What does
this mean?
64
Key:
Tip: The network "Rosencrantz" requires a WEP key.
A WEP key consists of either 10 or 26 hex characters.
This helps prevent unauthorized users from
connecting to this network.
63
Select Next to continue.
Back
Next

FIG. 6-2

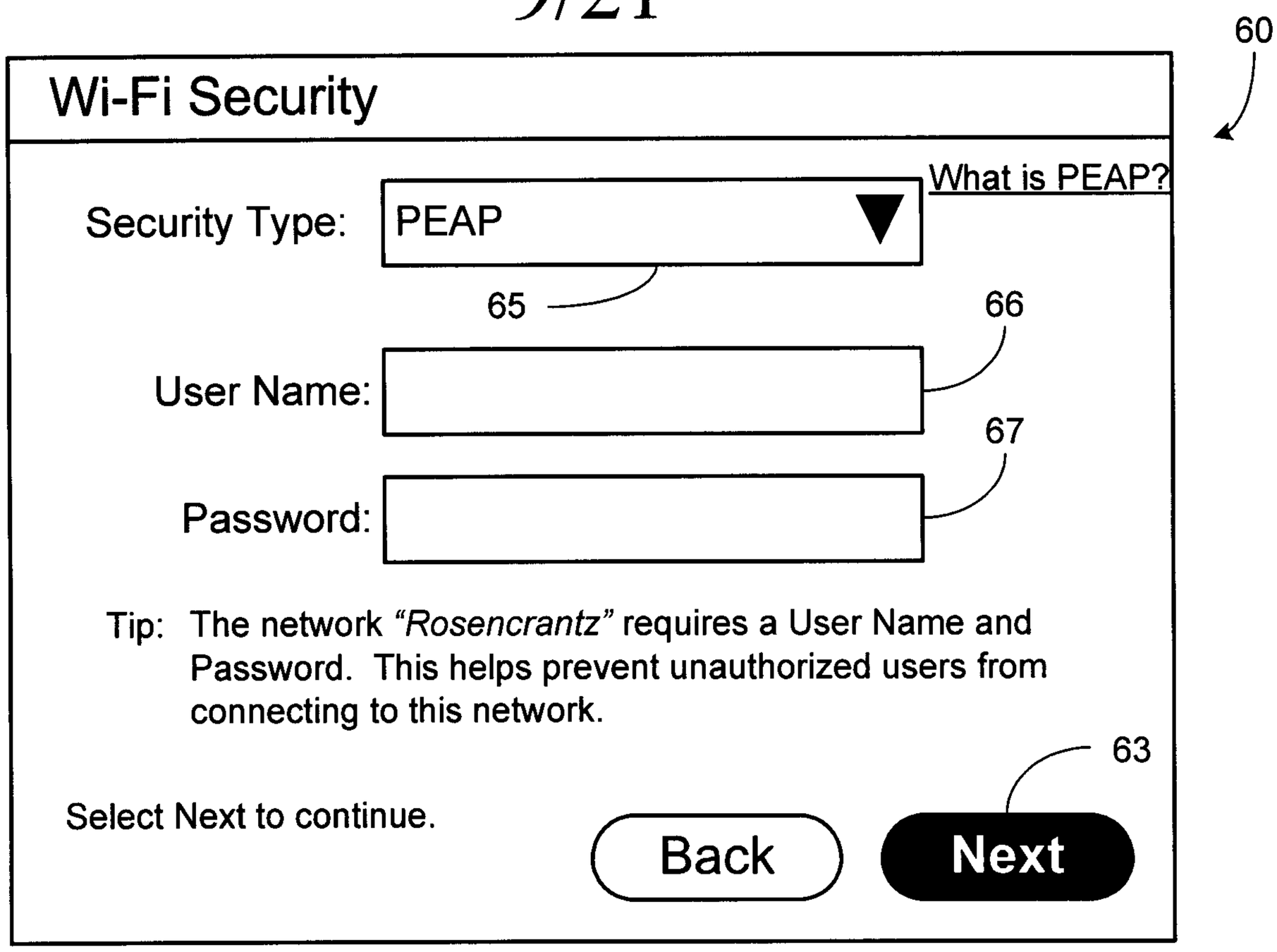

60
Wi-Fi Security
What is PEAP?
Security Type:
PEAP
65
66
User Name:
67
Password:
Tip: The network "Rosencrantz" requires a User Name and Password. This helps prevent unauthorized users from connecting to this network.
63
Select Next to continue.
Back
Next

FIG. 6-3

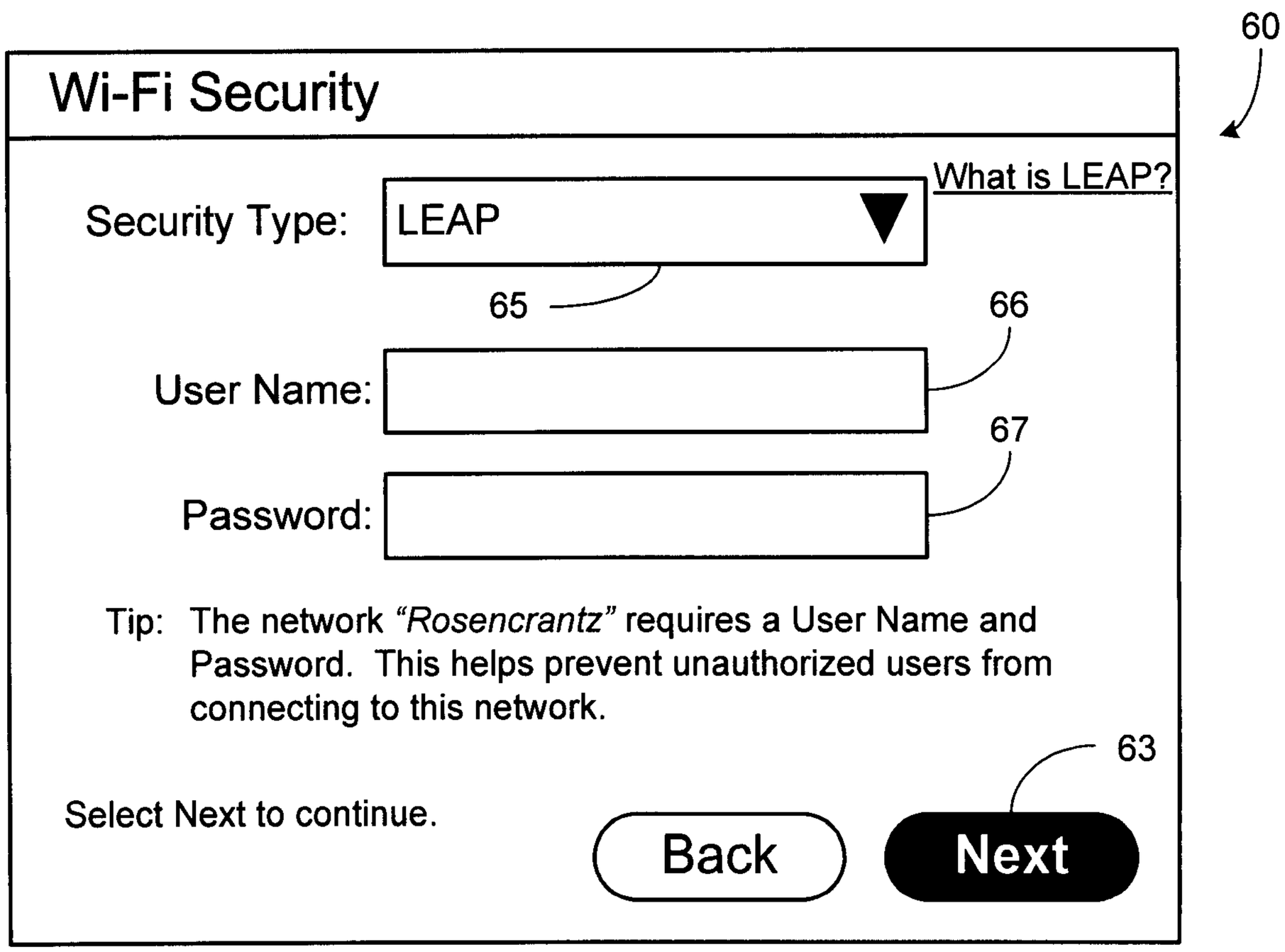

60
Wi-Fi Security
What is LEAP?
Security Type:
LEAP
65
66
User Name:
67
Password:
Tip: The network "Rosencrantz" requires a User Name and Password. This helps prevent unauthorized users from connecting to this network.
63
Select Next to continue.
Back
Next

FIG. 6-4

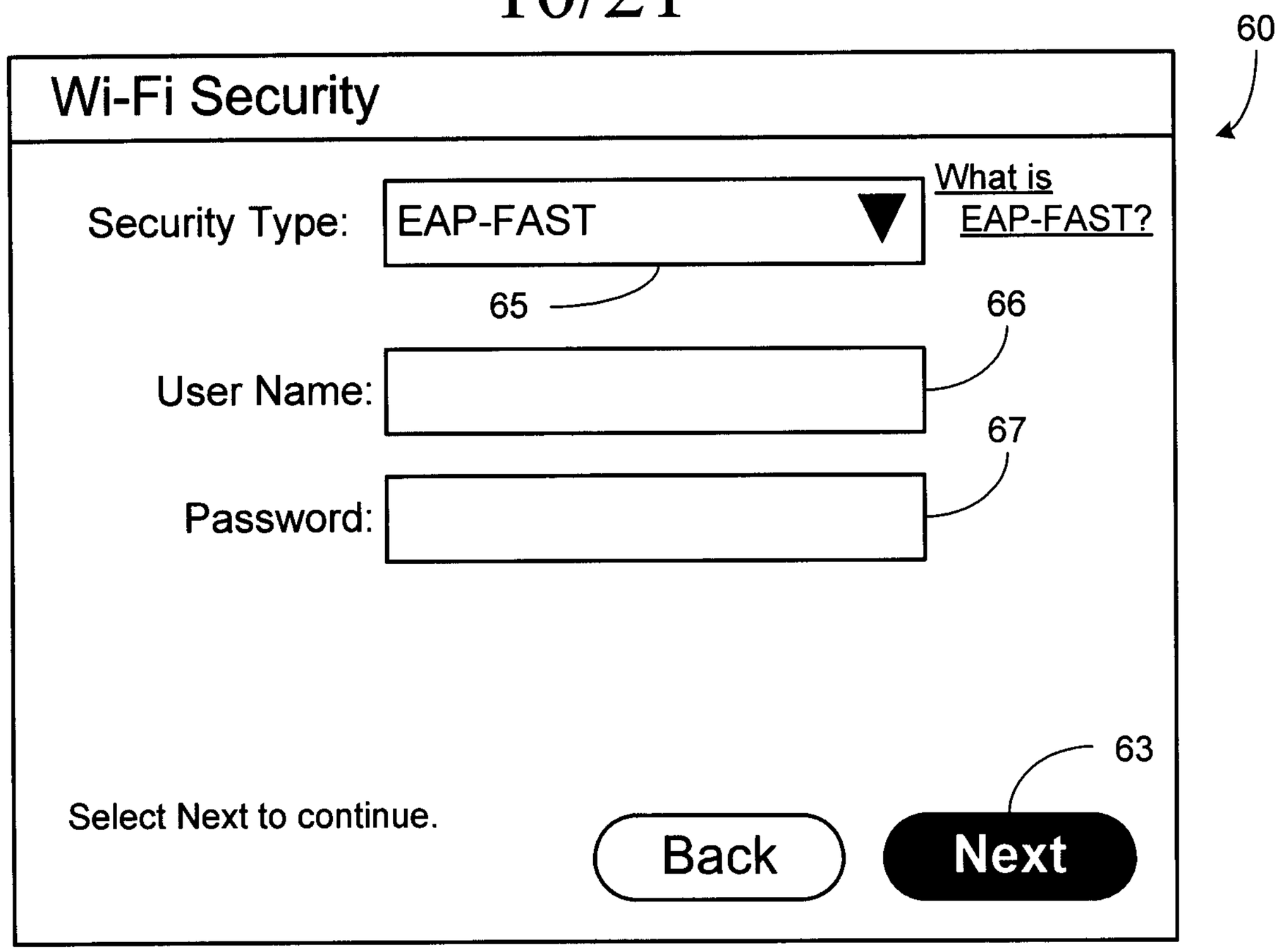

60
Wi-Fi Security
Security Type:
EAP-FAST
What is EAP-FAST?
65
66
User Name:
67
Password:
63
Select Next to continue.
Back
Next

FIG. 6-5

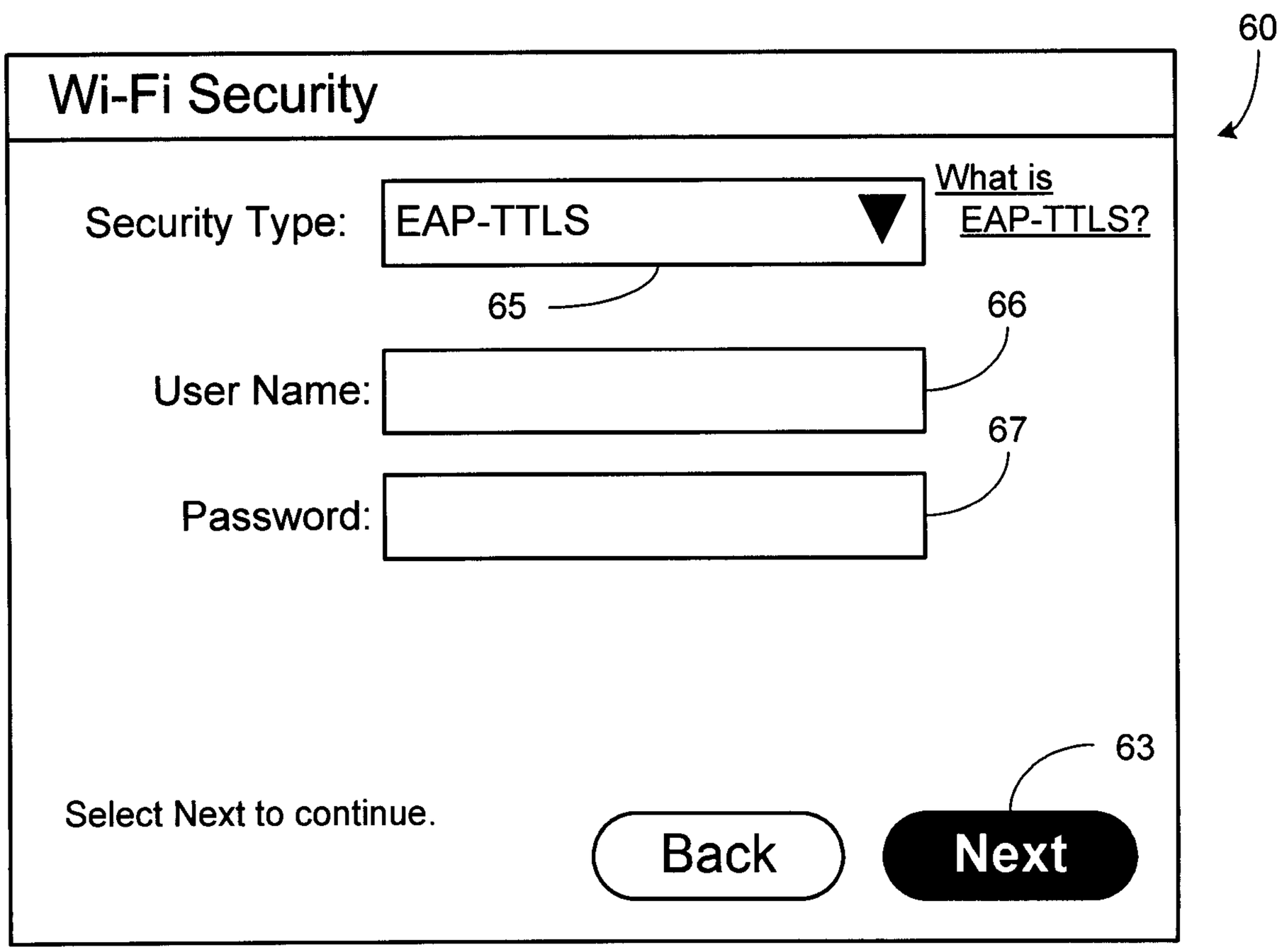

60
Wi-Fi Security
Security Type:
EAP-TTLS
What is EAP-TTLS?
65
66
User Name:
67
Password:
63
Select Next to continue.
Back
Next

FIG. 6-6

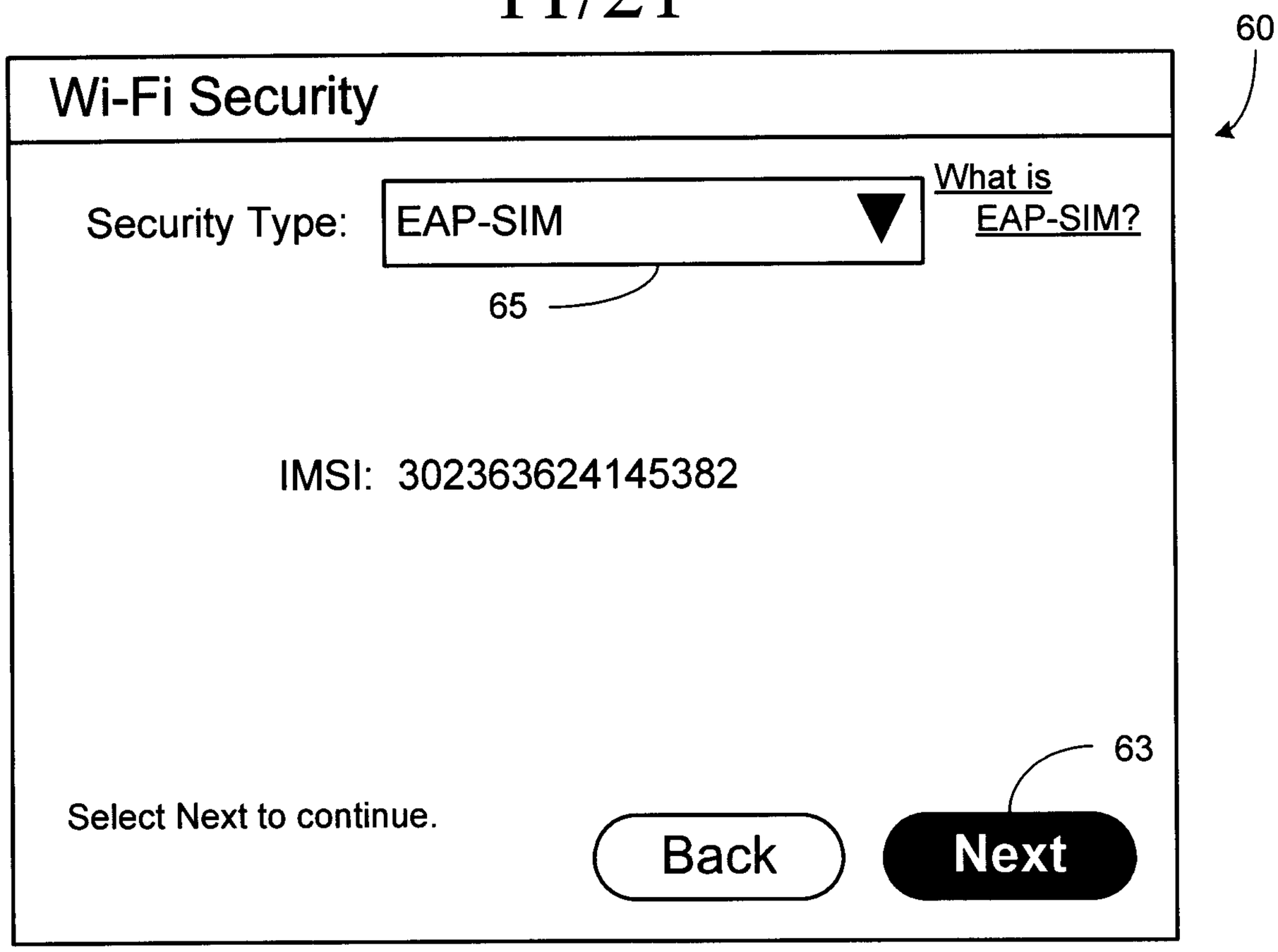

60
Wi-Fi Security
Security Type:
EAP-SIM
What is EAP-SIM?
65
IMSI: 302363624145382
63
Select Next to continue.
Back
Next

FIG. 6-7

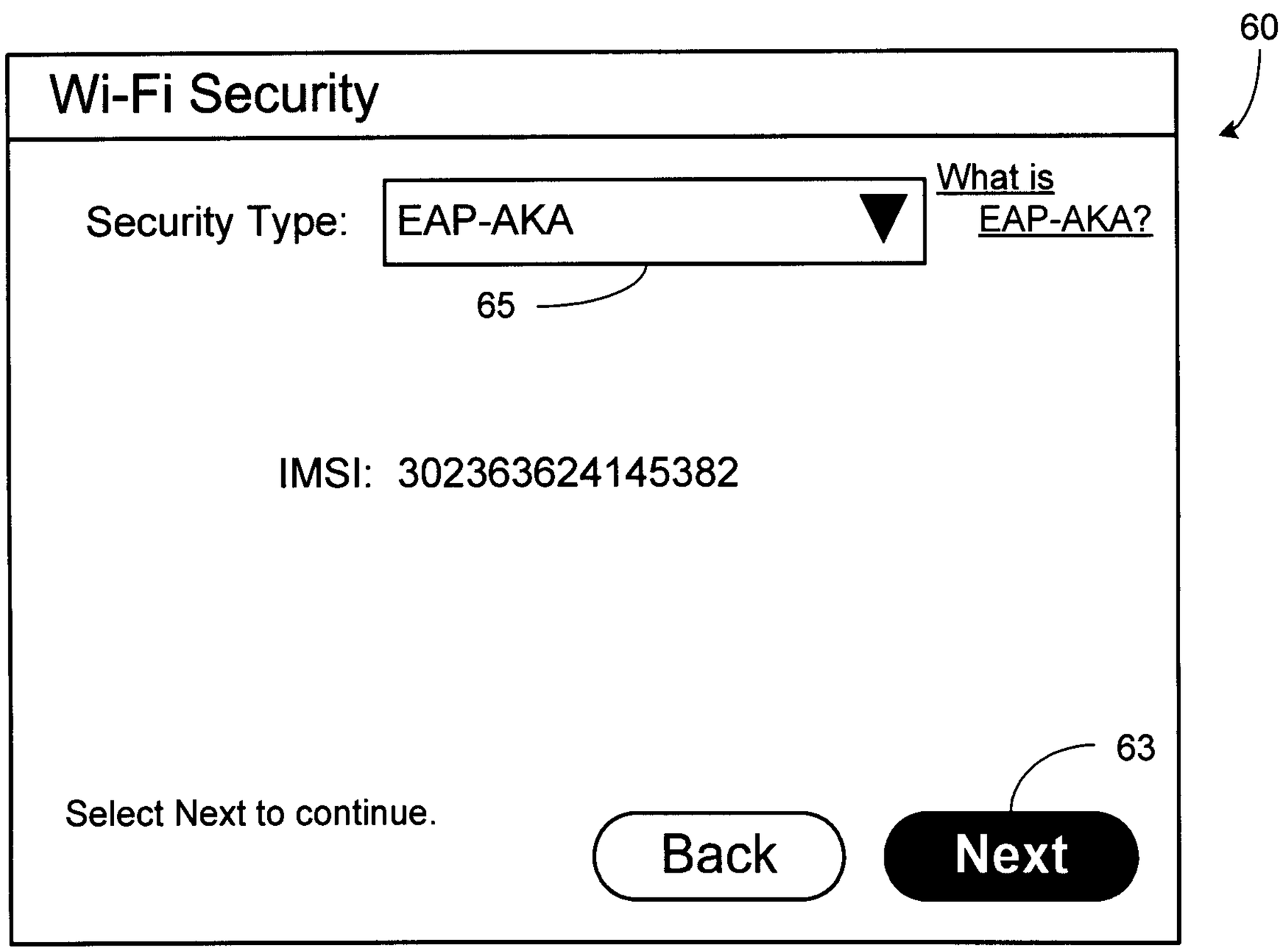

60
Wi-Fi Security
Security Type:
EAP-AKA
What is EAP-AKA?
65
IMSI: 302363624145382
63
Select Next to continue.
Back
Next

FIG. 6-8

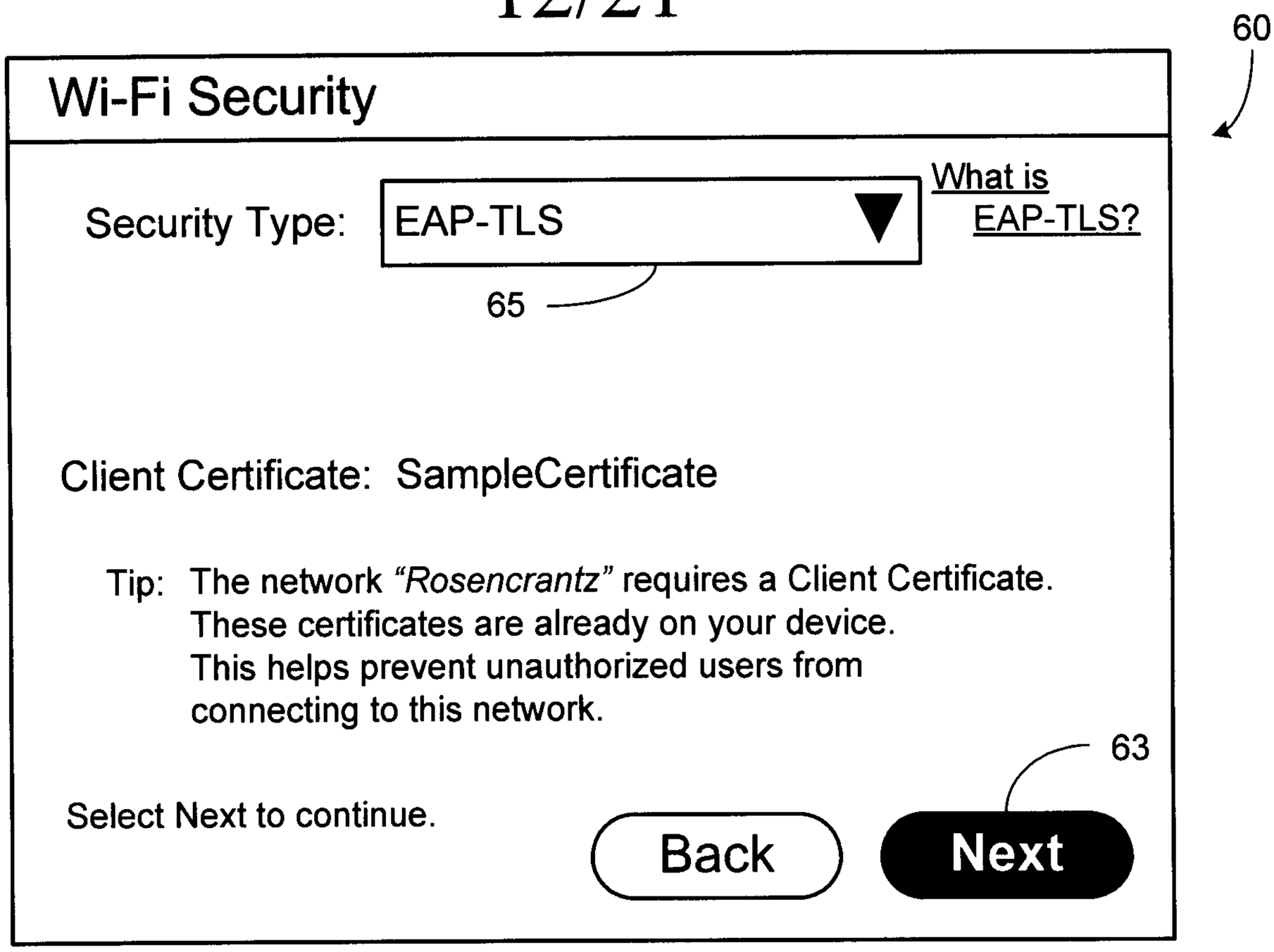


FIG. 6-9

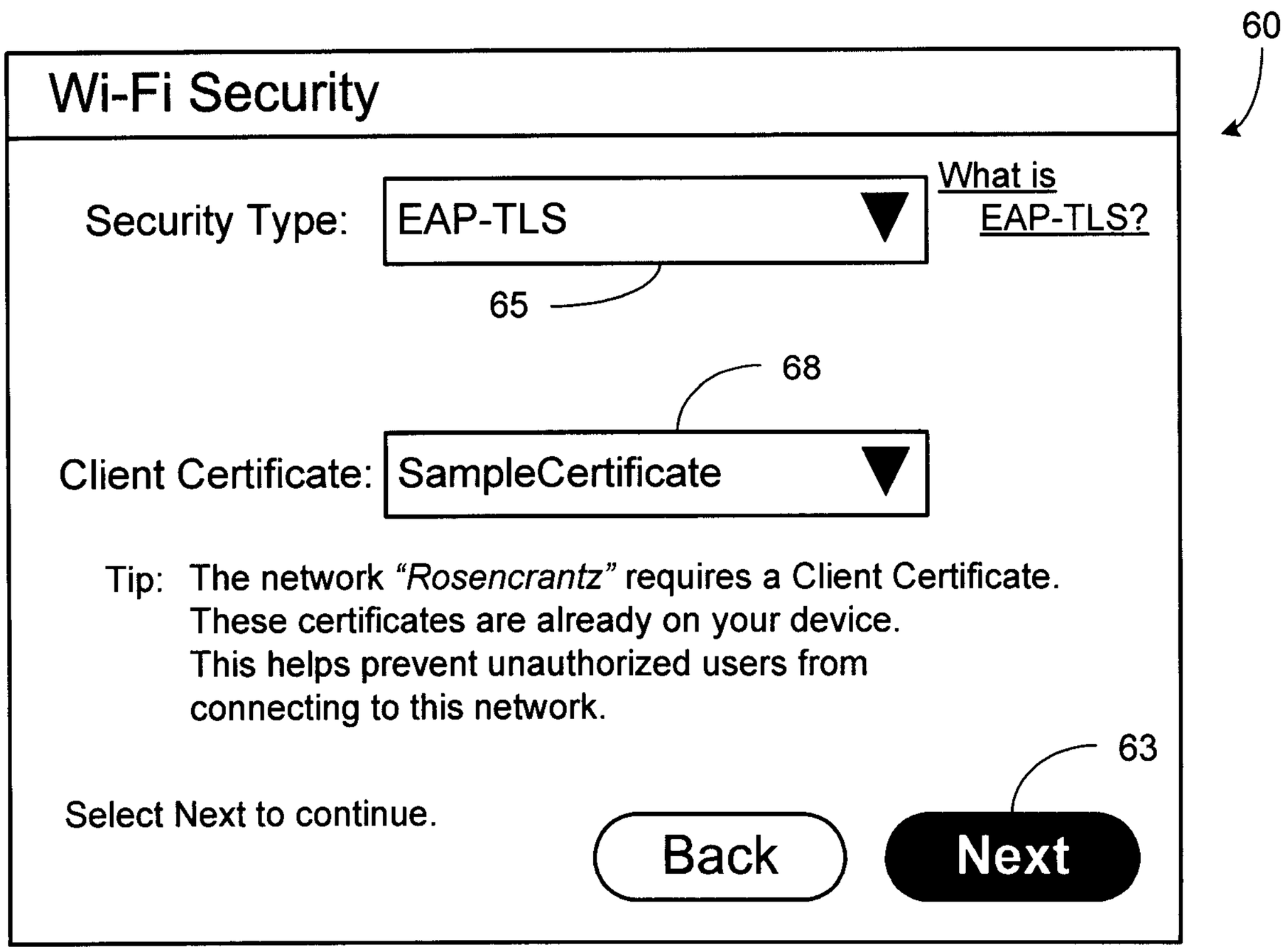


FIG. 6-10

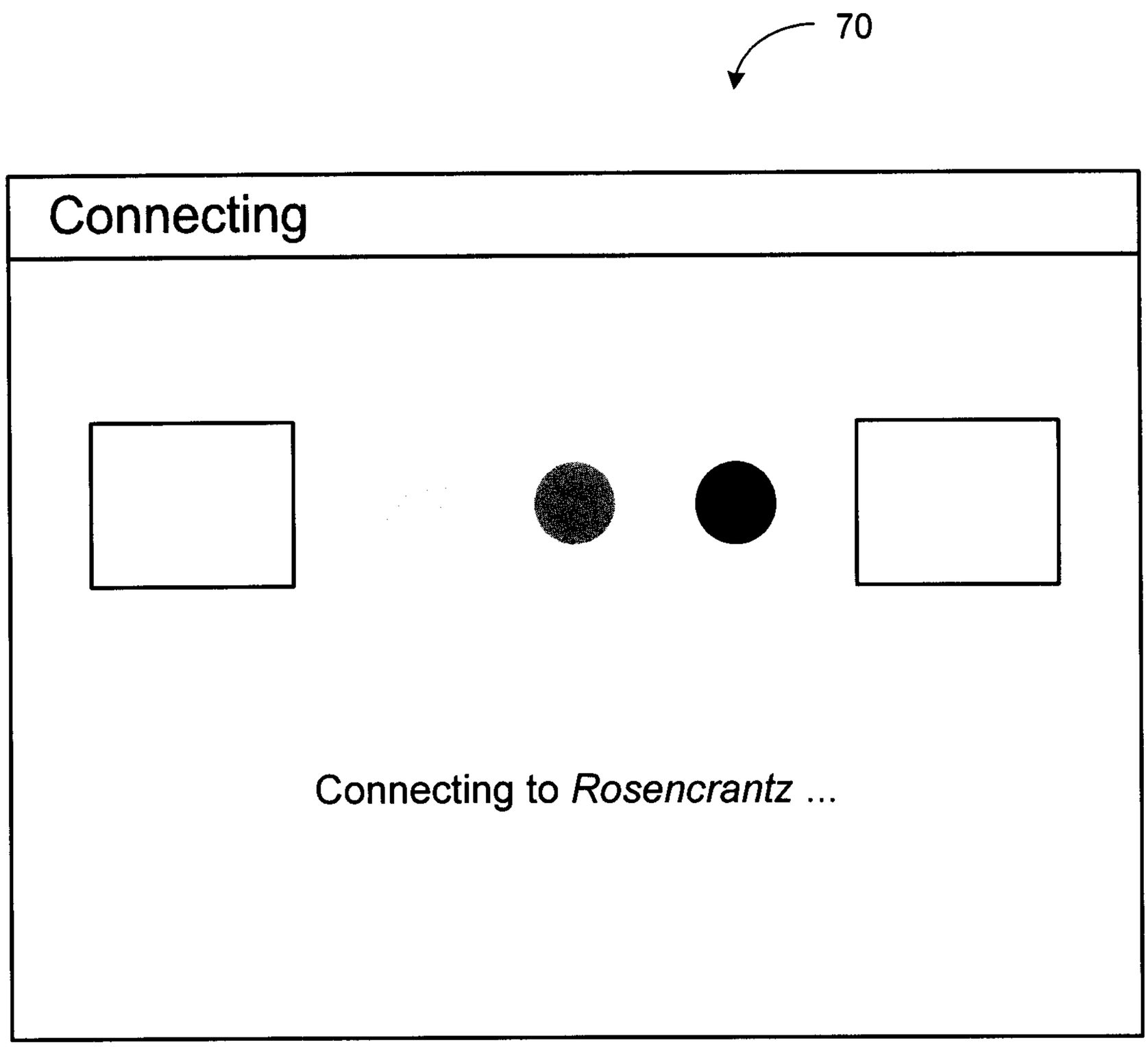


FIG. 7

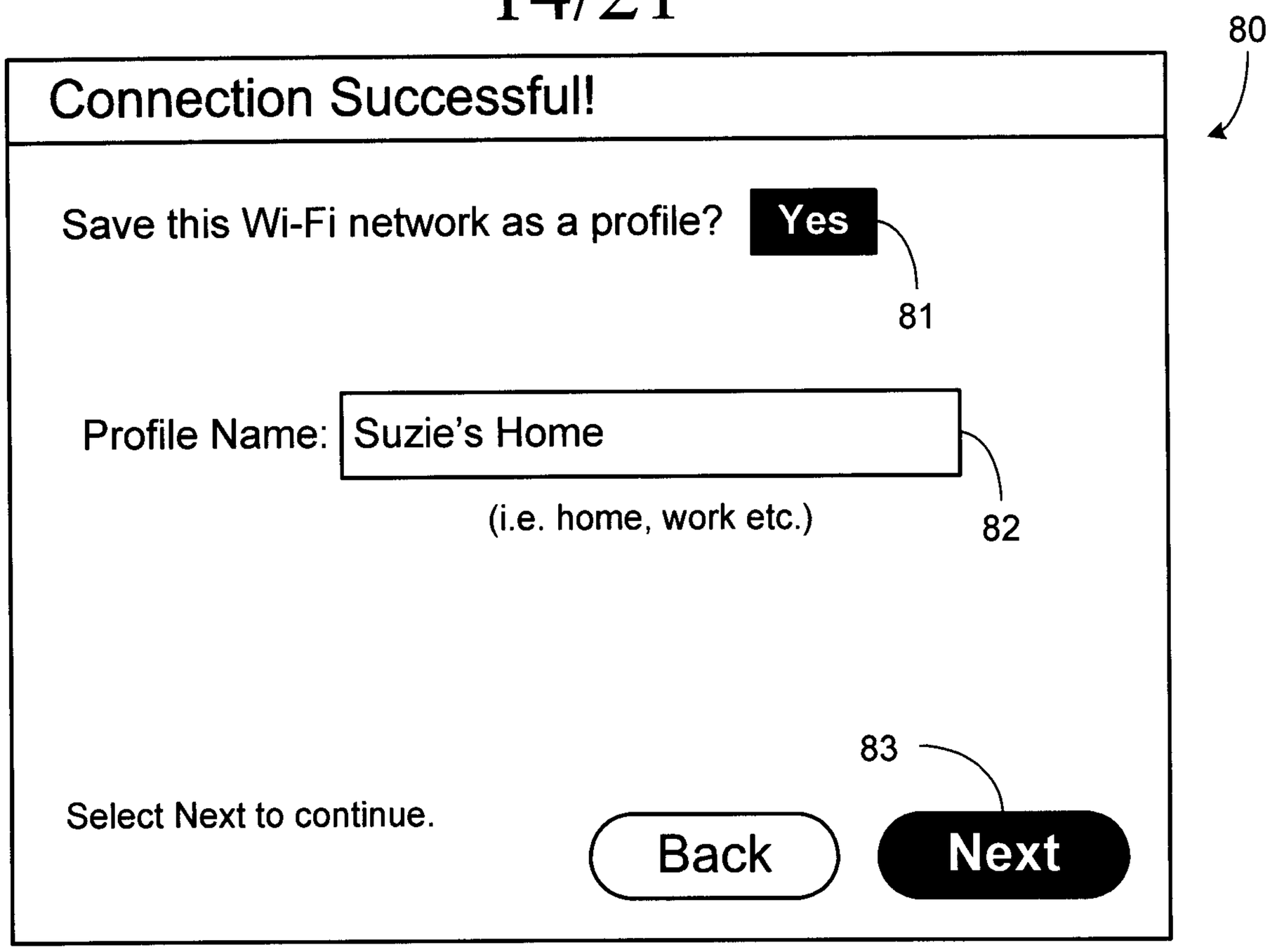

80
Connection Successful!
Save this Wi-Fi network as a profile?
Yes
81
Profile Name:
Suzie's Home
(i.e. home, work etc.)
82
83
Select Next to continue.
Back
Next

FIG. 8-1

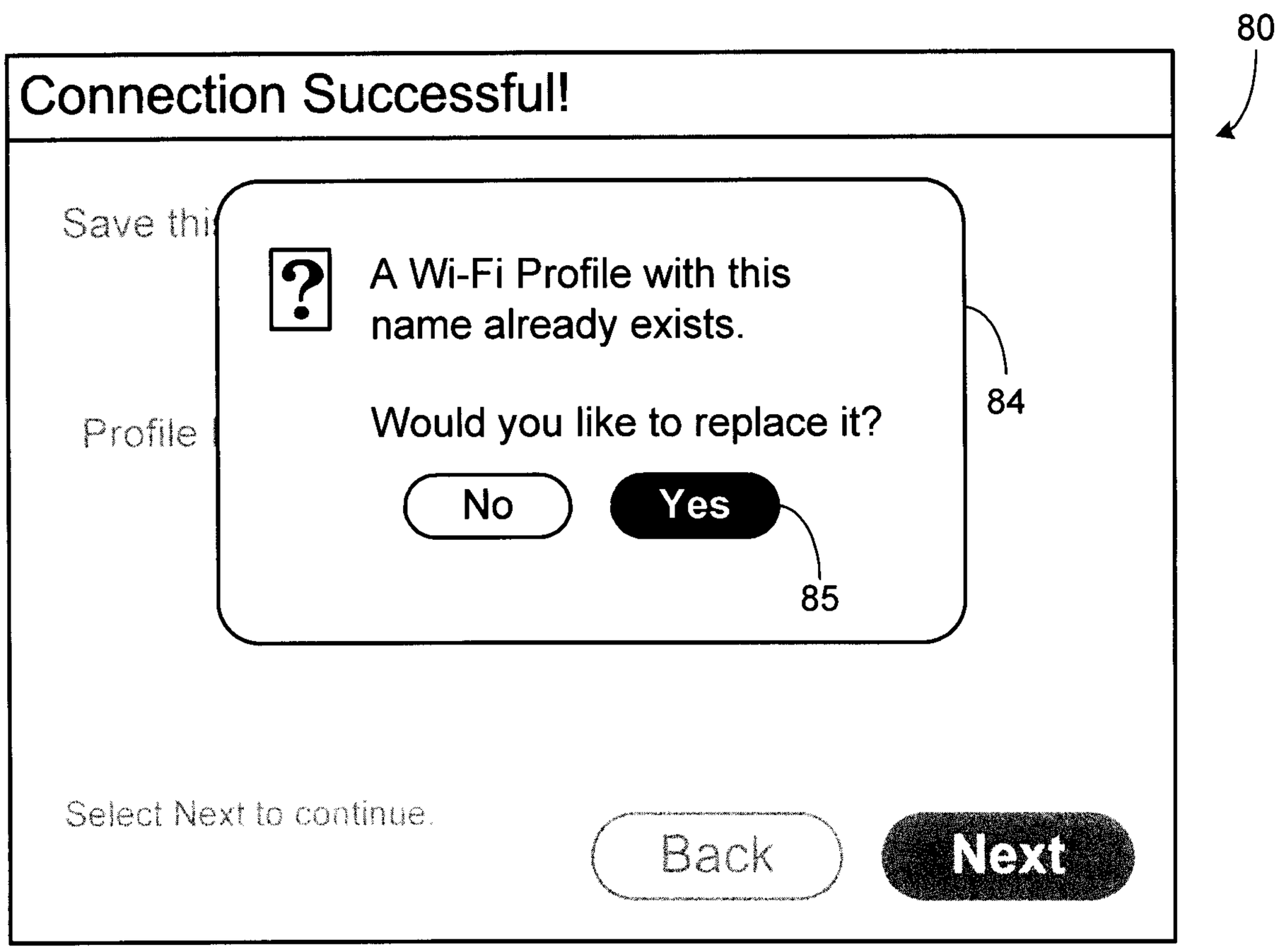

80
Connection Successful!
Save thi
Profile
A Wi-Fi Profile with this name already exists.
Would you like to replace it?
84
No
Yes
85
Select Next to continue.
Back
Next

FIG. 8-2

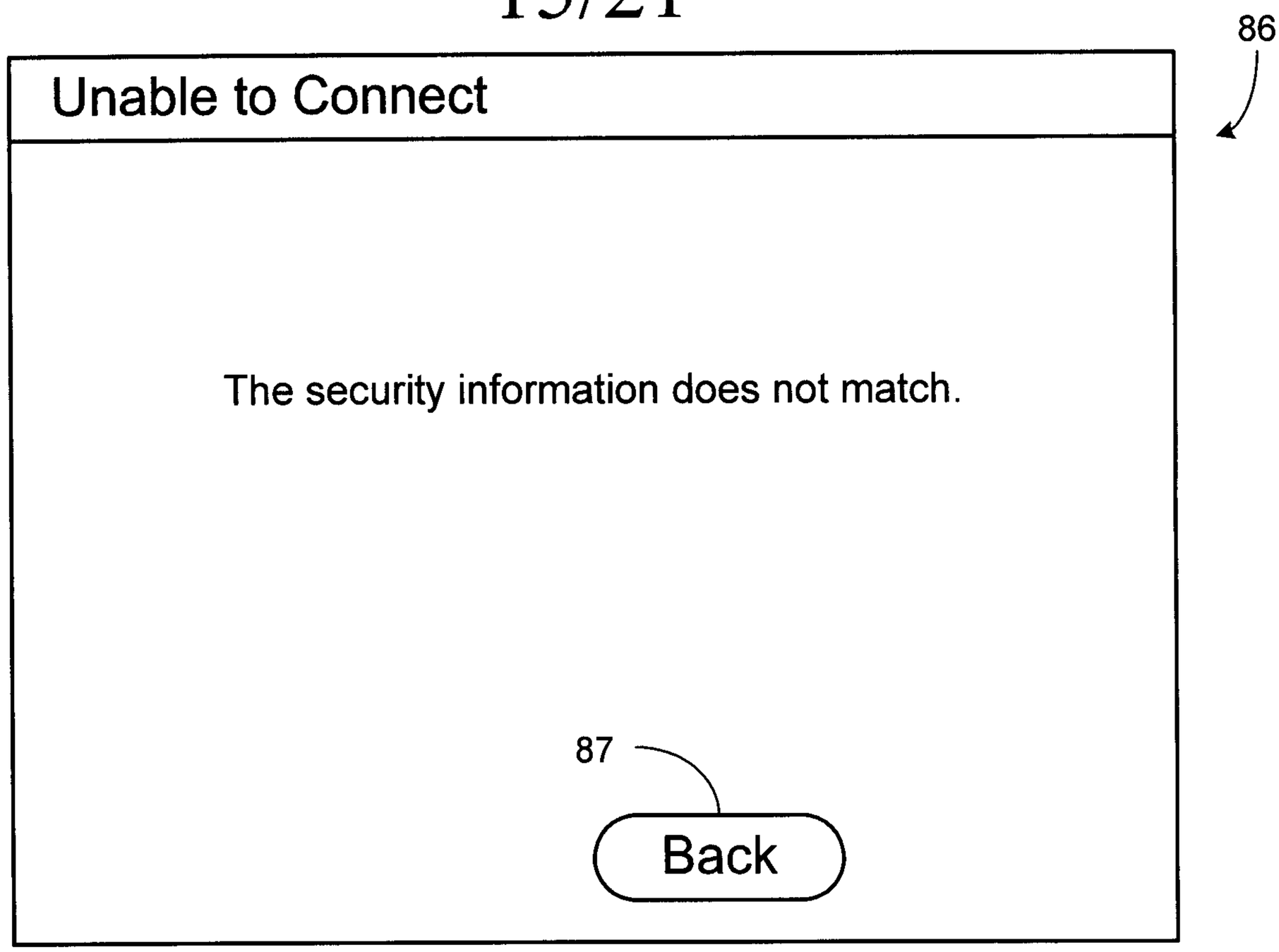

86
Unable to Connect
The security information does not match.
87
Back

FIG. 8-3

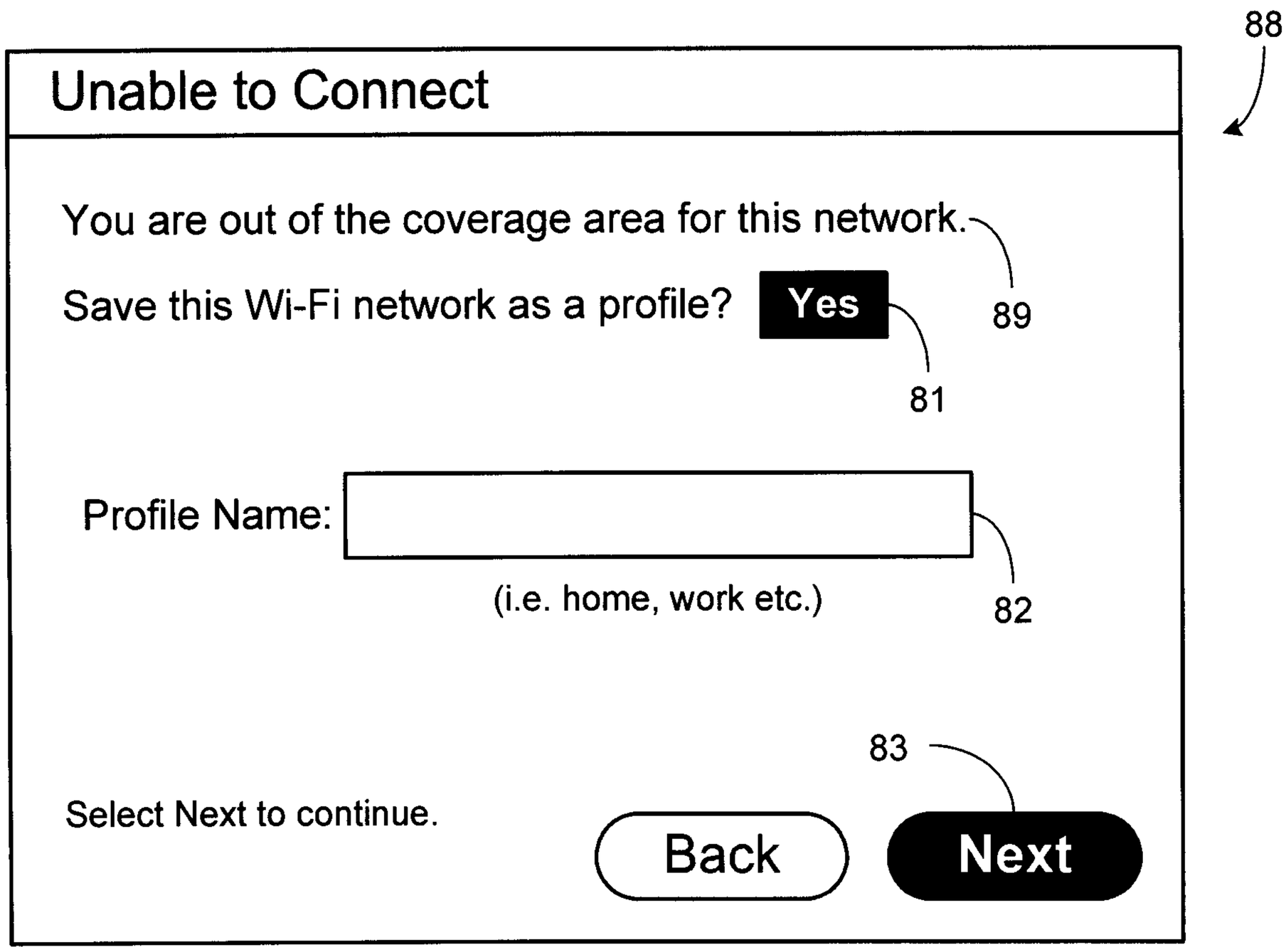

88
Unable to Connect
You are out of the coverage area for this network.
Save this Wi-Fi network as a profile?
Yes
89
81
Profile Name:
(i.e. home, work etc.)
82
83
Select Next to continue.
Back
Next

FIG. 8-4

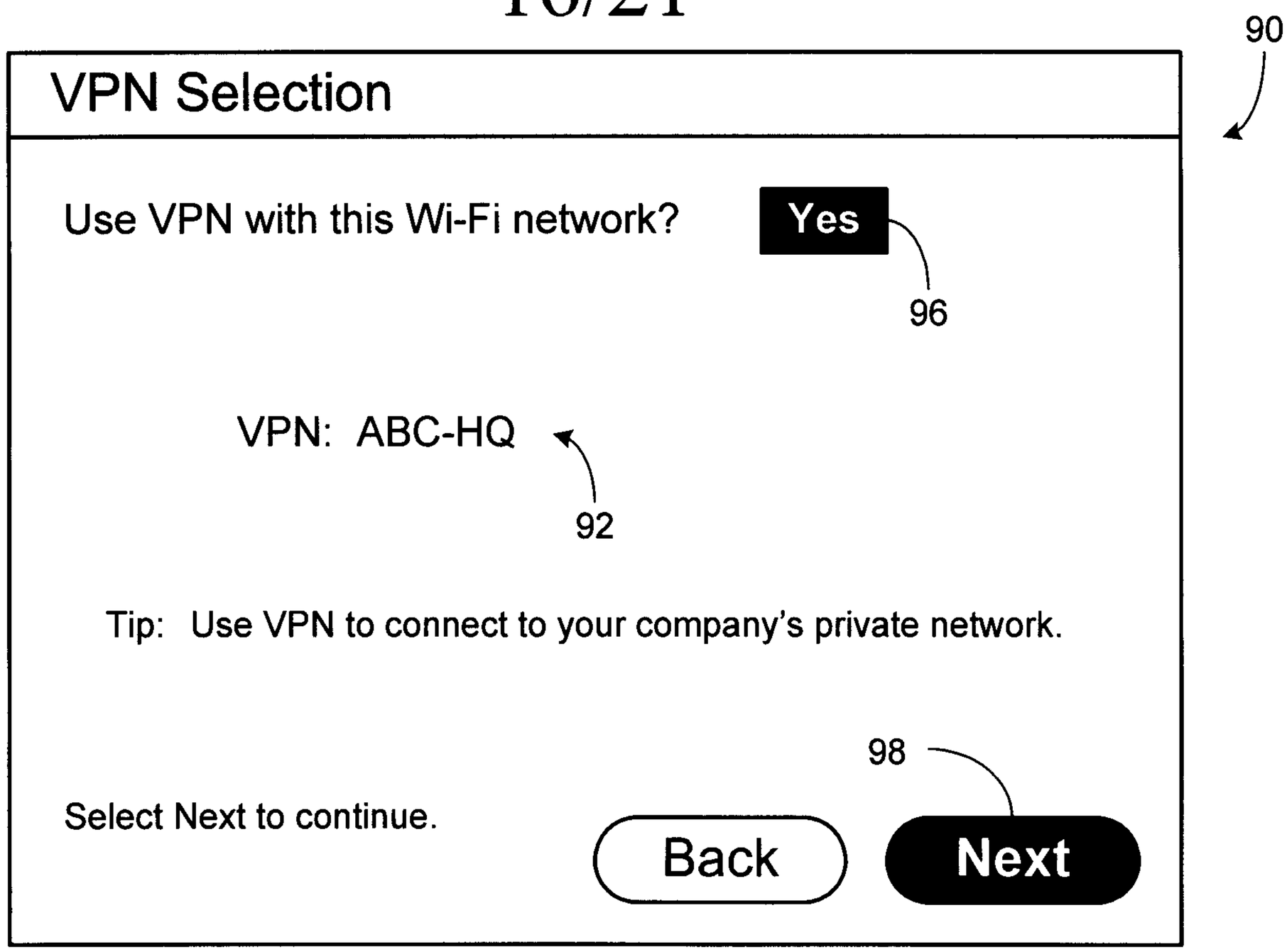

90
VPN Selection
Use VPN with this Wi-Fi network?
Yes
96
VPN: ABC-HQ
92
Tip: Use VPN to connect to your company's private network.
98
Select Next to continue.
Back
Next

FIG. 9-1

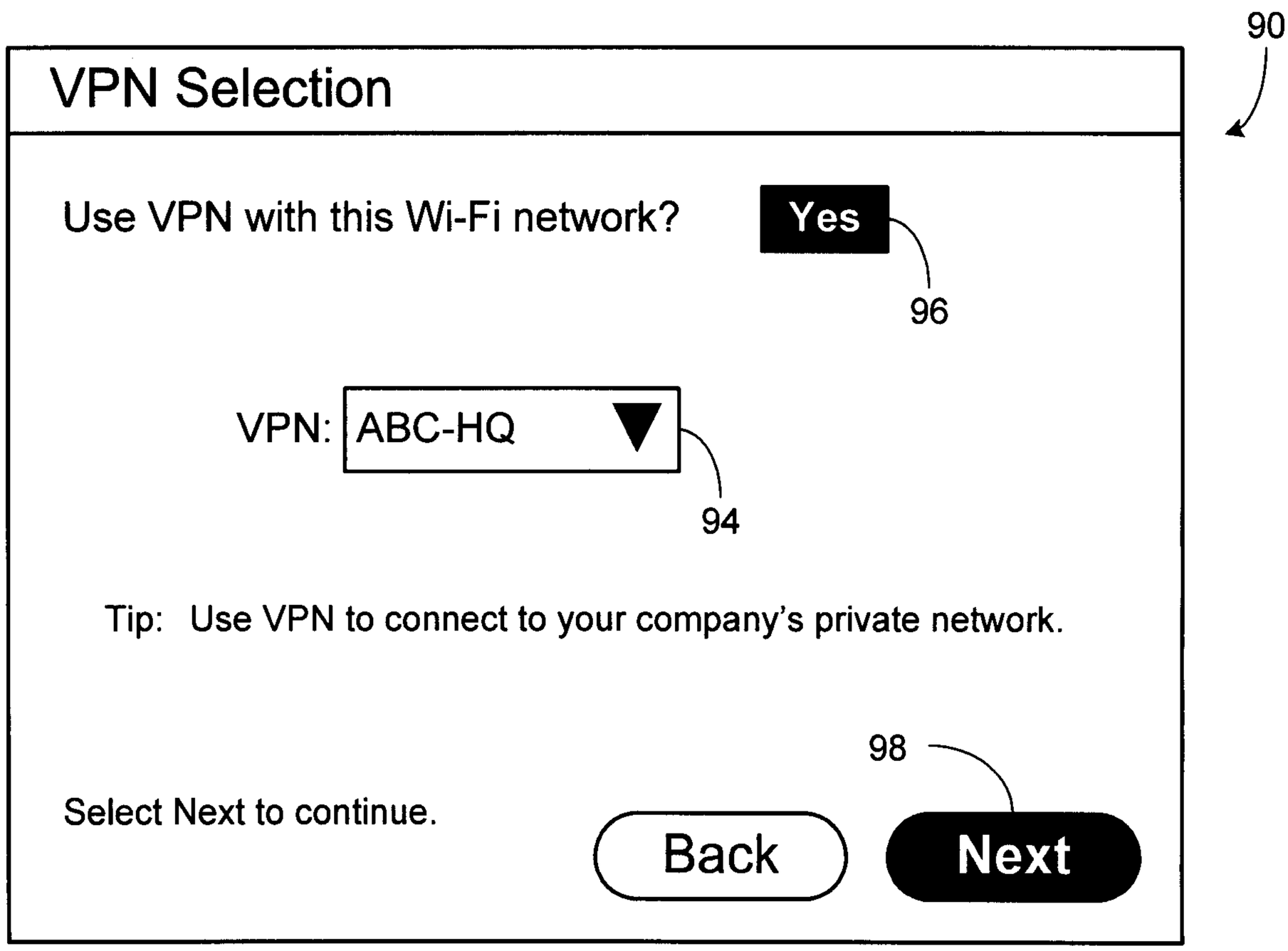

90
VPN Selection
Use VPN with this Wi-Fi network?
Yes
96
VPN: ABC-HQ
94
Tip: Use VPN to connect to your company's private network.
98
Select Next to continue.
Back
Next

FIG. 9-2

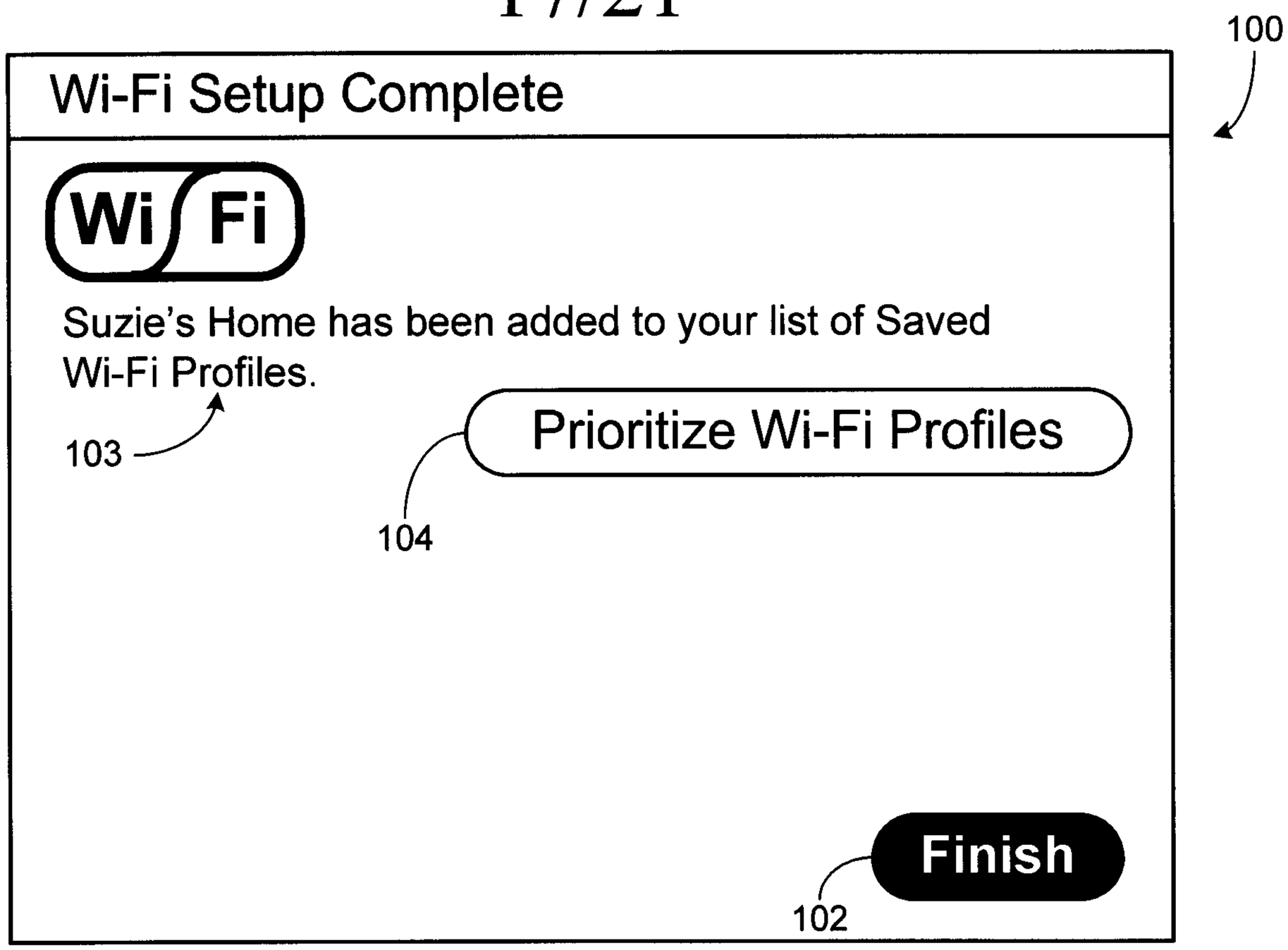


FIG. 10-1

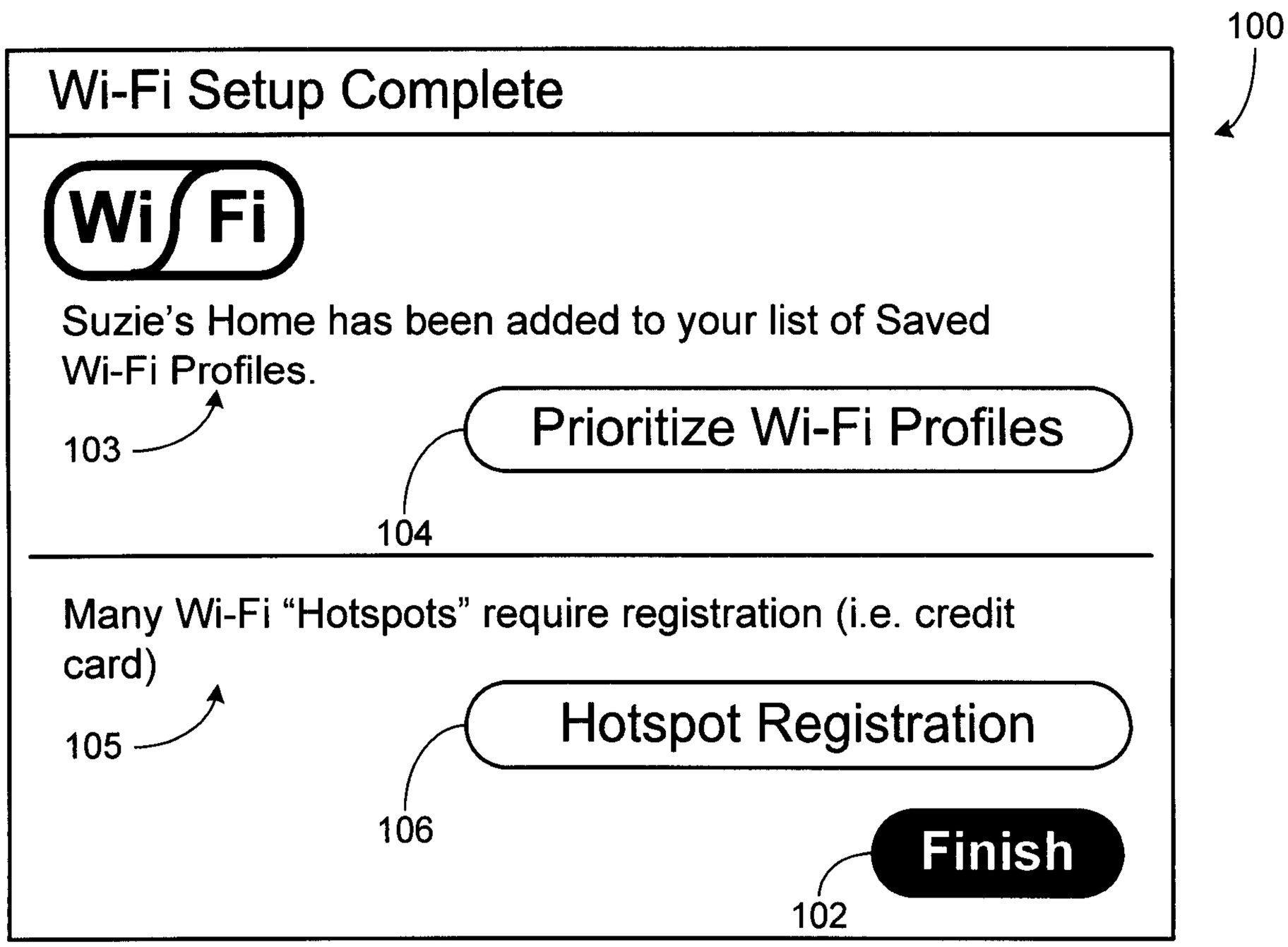


FIG. 10-2

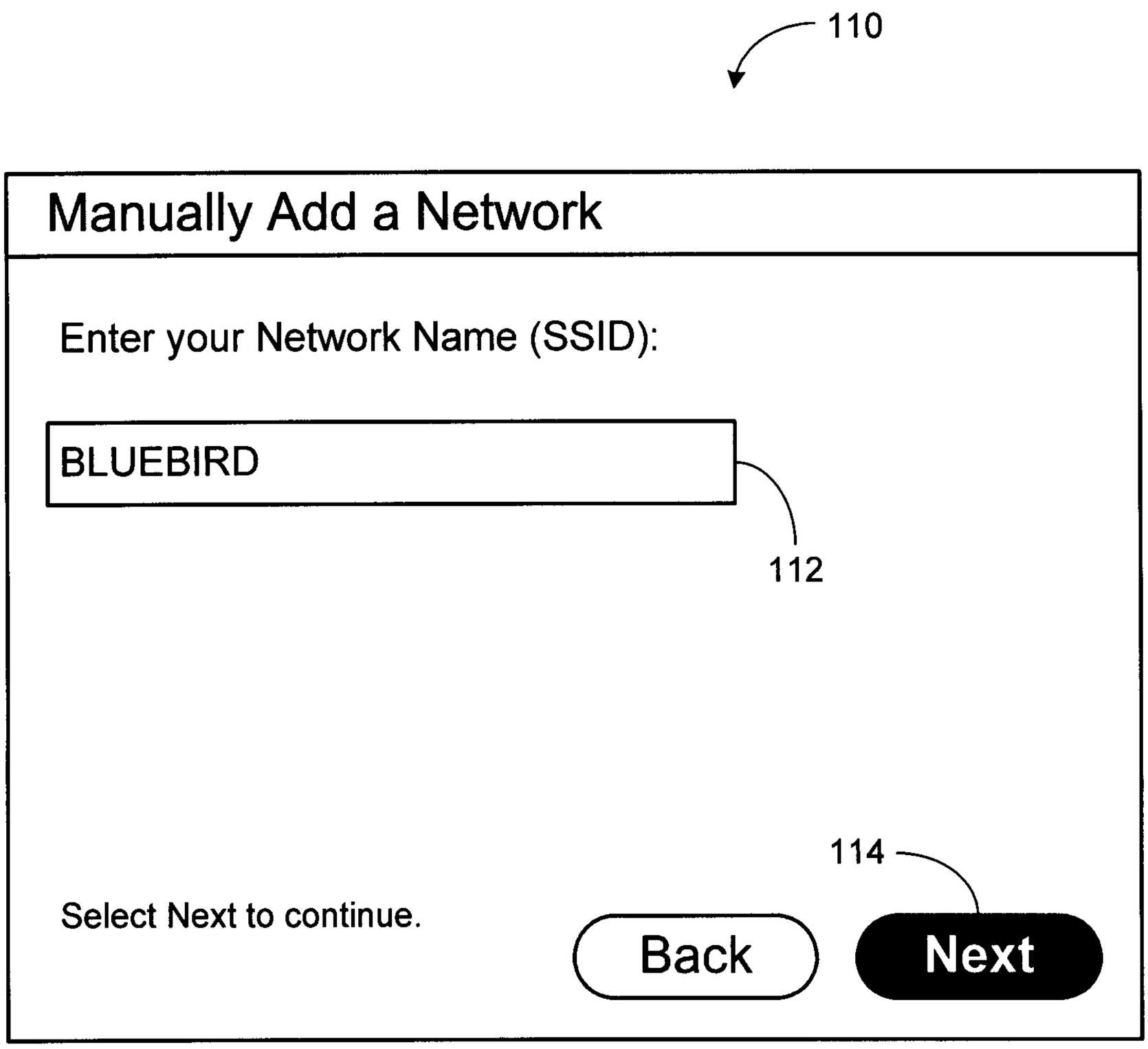

110
Manually Add a Network
Enter your Network Name (SSID):
BLUEBIRD
112
114
Select Next to continue.
Back
Next

FIG. 11

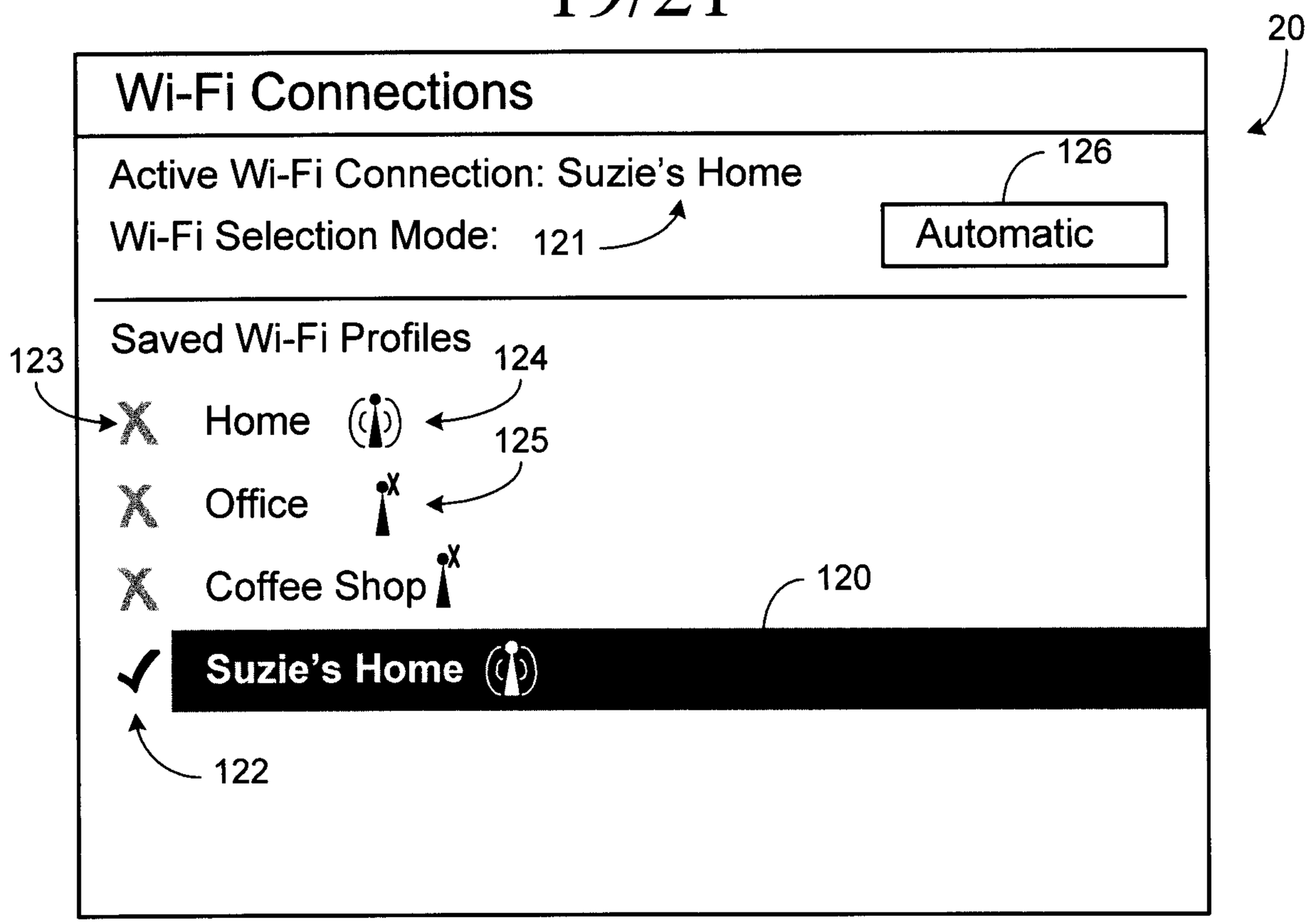


FIG. 12-1

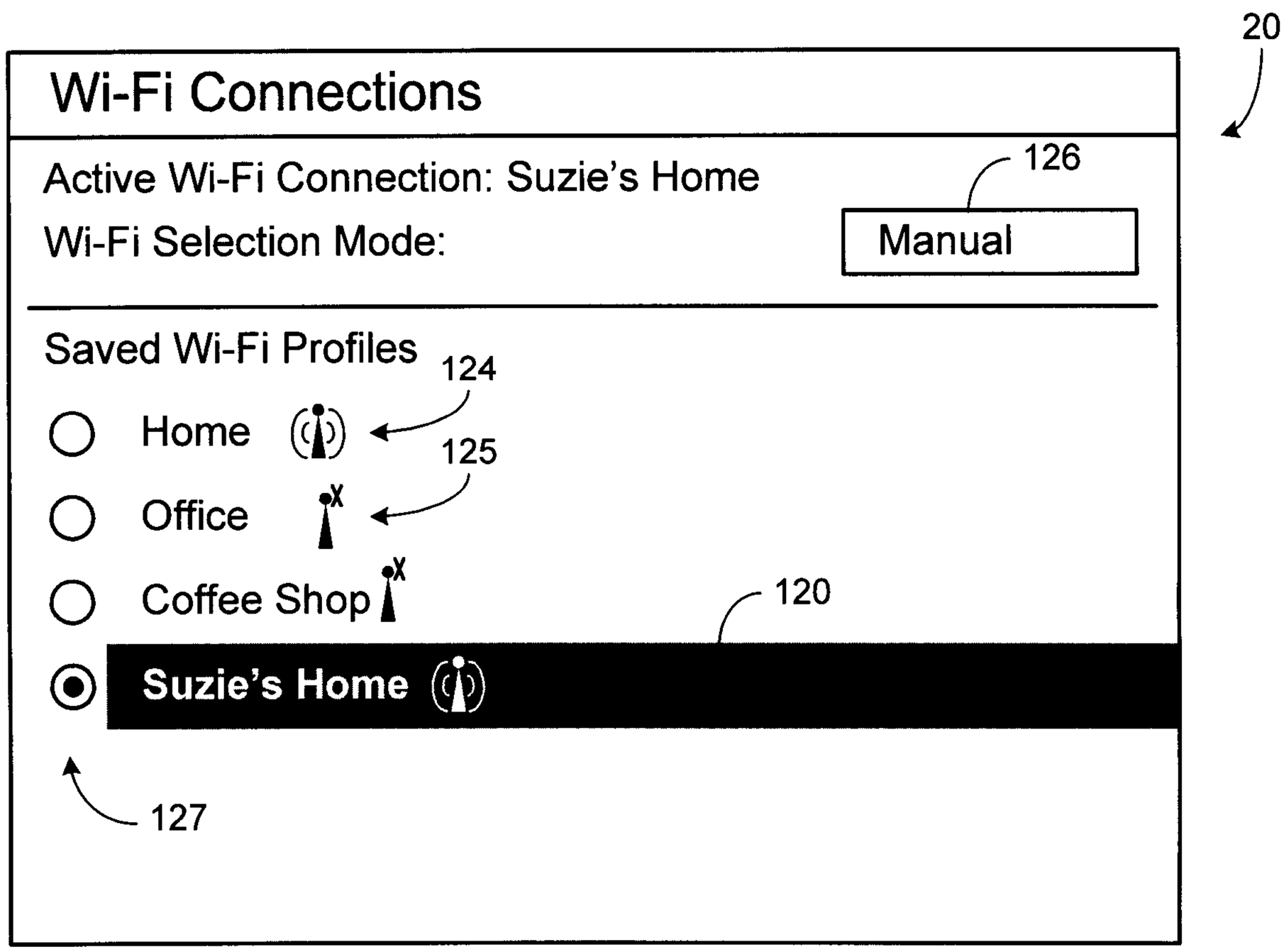


FIG. 12-2

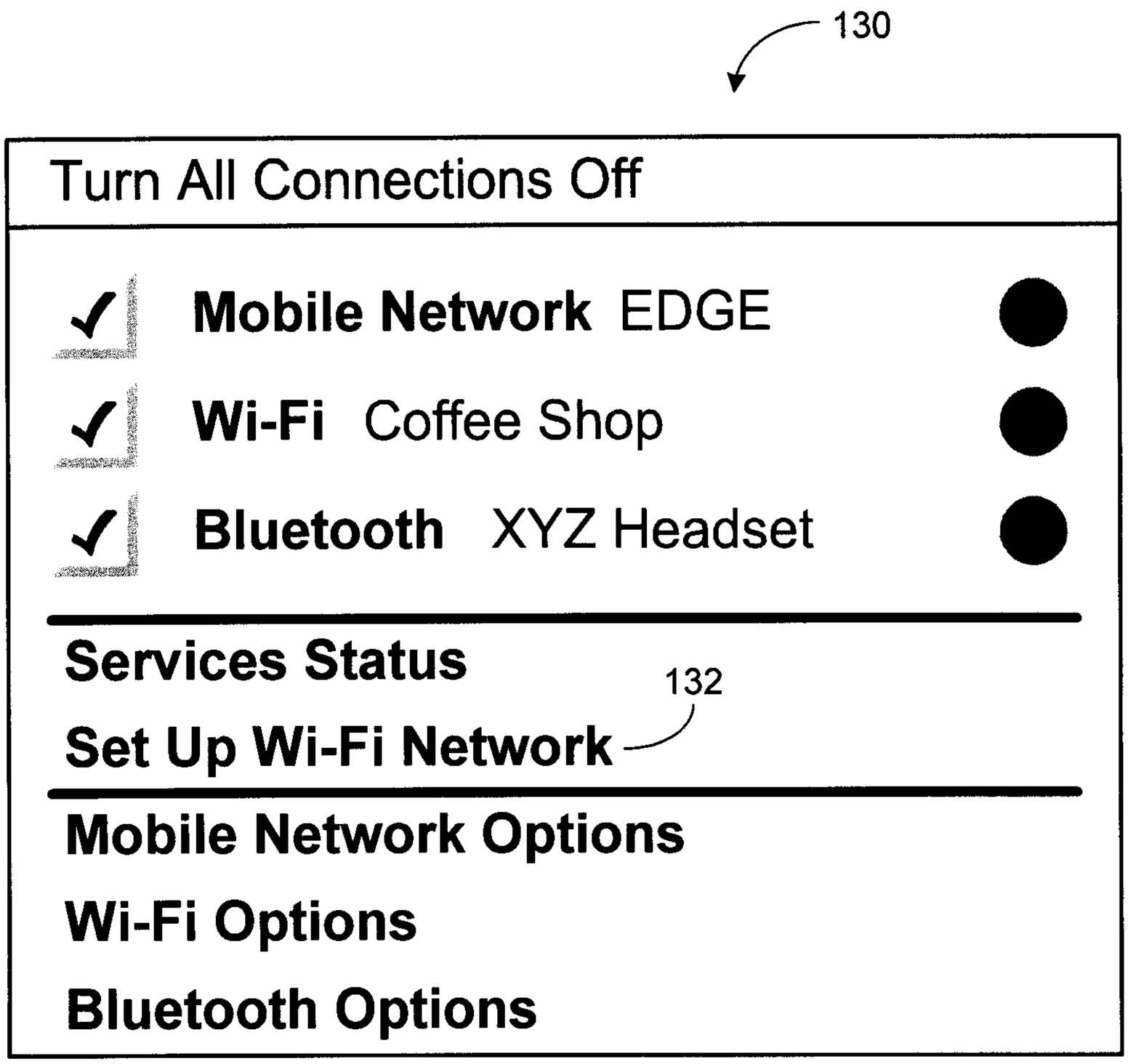

130
Turn All Connections Off
Mobile Network EDGE
Wi-Fi Coffee Shop
Bluetooth XYZ Headset
Services Status
132
Set Up Wi-Fi Network
Mobile Network Options
Wi-Fi Options
Bluetooth Options

FIG. 13

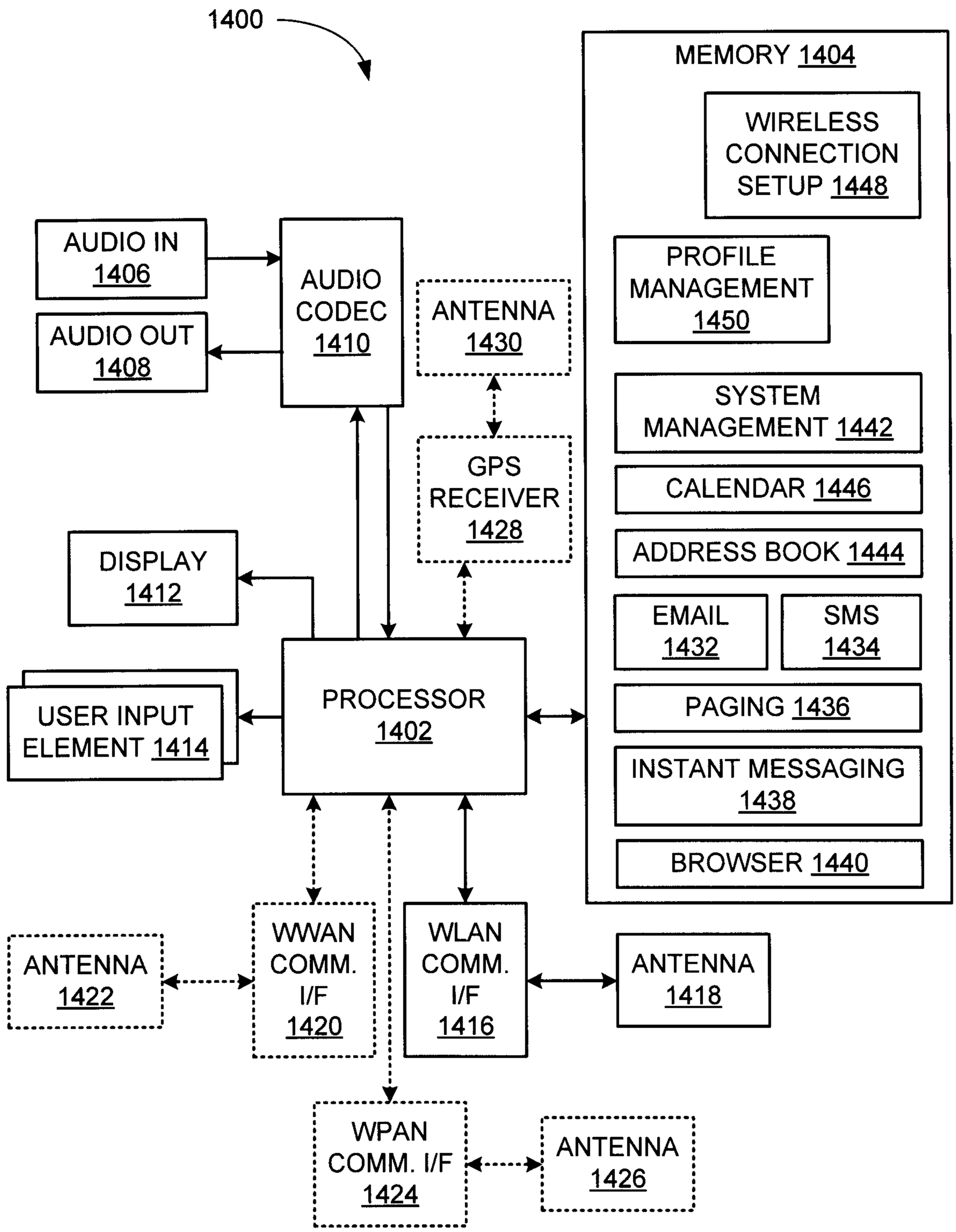
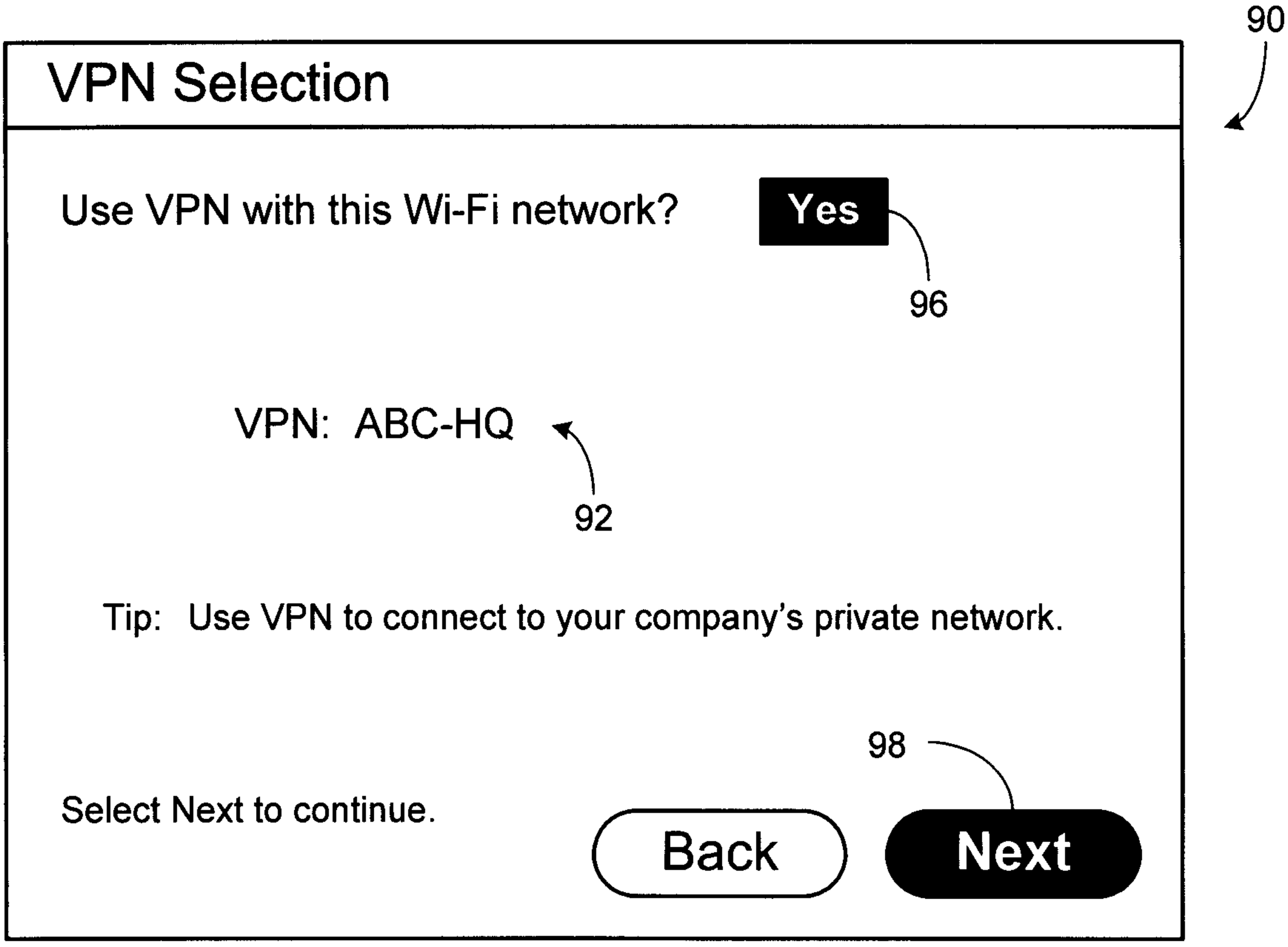

1400
MEMORY 1404
WIRELESS CONNECTION SETUP 1448
PROFILE MANAGEMENT 1450
SYSTEM MANAGEMENT 1442
CALENDAR 1446
ADDRESS BOOK 1444
EMAIL 1432
SMS 1434
PAGING 1436
INSTANT MESSAGING 1438
BROWSER 1440
AUDIO IN 1406
AUDIO OUT 1408
AUDIO CODEC 1410
ANTENNA 1430
GPS RECEIVER 1428
DISPLAY 1412
USER INPUT ELEMENT 1414
PROCESSOR 1402
ANTENNA 1422
WWAN COMM. I/F 1420
WLAN COMM. I/F 1416
ANTENNA 1418
WPAN COMM. I/F 1424
ANTENNA 1426

FIG. 14


90
VPN Selection
Use VPN with this Wi-Fi network?
Yes
96
VPN: ABC-HQ
92
Tip: Use VPN to connect to your company's private network.
98
Select Next to continue.
Back
Next