



(51) International Patent Classification:

H04W 48/18 (2009.01) H04W 4/26 (2009.01)

H04W 12/08 (2009.01)

(21) International Application Number:

PCT/CA2016/050968

(22) International Filing Date:

17 August 2016 (17.08.2016)

(25) Filing Language:

English

(26) Publication Language:

English

(72) Inventor; and

(71) Applicant: AFLATOONI, Aflatoon [CA/CA]; c/o Tribute Kiosk Inc., 73 Bannatyne Drive, Toronto, Ontario M2L 2P2 (CA).

(74) Agent: CHATTERJEE, Jaidip; c/o PatentAxis Inc., 10 King Street East, suite 500, Toronto, Ontario M5C 1C3 (CA).

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

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

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

(54) Title: SYSTEM FOR CONNECTING TO A SECURED WIRELESS LOCAL AREA NETWORK (WLAN) WHEN ROAMING BY MEANS OF PURCHASED SECURE ACCESS CREDENTIALS

(57) Abstract: Described herein is a wireless network broadcast device comprising: a network interface supporting secured communications with an Internet access point; a wireless adapter to establish a plurality of secured wireless network connections and an open unsecured wireless network connection directed to a web page hosted on a remote server and providing information relating to purchase of one of the plurality of secured wireless network connections; and a processor programmed to execute network security rules to isolate network communications data of each of the plurality of secured wireless network connections from all other network communications data passing through the wireless adapter. Neighbor subscribers can use the web page to purchase access to one of the secured wireless network connections and have a computing device configured for password protected wireless connection to one of the plurality of secured wireless network connections.



DEVICE FOR CONNECTING MULTIPLE WIRELESS NETWORKS TO AN INTERNET ACCESS POINT

BACKGROUND OF THE INVENTION

5 Field of the Invention

The invention relates to Internet access points, and more particularly to Internet access points shared by multiple users.

Description of the Related Art

10 The Internet is a worldwide system of interconnected computer networks involving communications infrastructure of many different types of communication networks. Communication networks may be distinguished based on geographical span. For example, a wide area network (WAN) provides communication in a broad geographic area covering national and/or international locations, on a smaller scale a metropolitan area network (MAN) covers a plurality of postal code areas within a city or state, on an even smaller scale a neighborhood area
15 network (NAN) typically spans a range of one to five bordering postal code areas, while a local area network (LAN) covers a small geographic area, such as a private residence, school or company. Personal area networks (PANs) are wireless LANs with a very short range (up to a few meters), enabling computer devices (such as PDAs and printers) to communicate with other nearby devices and computers, typically through near field communications, such as infrared or
20 near field radio.

Current options for most residential and small business subscribers to purchase Internet access is limited to Internet subscriptions from a small number of Internet service providers, constraining pricing competition and involving lengthy installation procedures including configuration of a router and modem provided by the Internet service provider. Attempts to
25 expand subscriber options have been achieved by Internet sharing implementations, such as a neighborhood area network (NAN) or a hotspot.

Both NANs and hotspots are examples of a shared wireless Internet access point, for example employing a Wi-Fi 802.11 wireless standard. A NAN typically covers a small number of blocks close to a wireless access point, for example communications mediated by a single
30 omnidirectional antenna can readily span a radius of one kilometer. NAN providers are usually individuals or a group that join to share an Internet broadband connection, for example DSL or

cable modem. Geographical span of a hotspot is typically limited to the wireless range of a router device, often being limited to a few hundred meters covering a building or several proximal/adjacent units within a building. Hotspot providers are often commercial establishments such as coffee shops, restaurants or airports.

5 While both NANs can allow users/subscribers to connect to the Internet quickly and at an efficient cost, both suffer from potential reduction of bandwidth speed related to increased levels of subscriber usage and lack of privacy of Internet communications between subscribers. Furthermore, while the desire to share Internet access may be recognized, communication of this desire to neighbors remains a cumbersome and inefficient task.

10 Accordingly, there is a continuing need for alternative devices and systems for providing a shared Internet access point.

SUMMARY OF THE INVENTION

In an aspect there is provided, a wireless network broadcast device comprising:

15 a first wireless adapter to establish password protected secured wireless communications with an Internet access point;

a second wireless adapter to establish a plurality of secured wireless network connections and an open unsecured wireless network connection directed to a web page hosted on a remote server and providing information relating to purchase of one of the plurality of secured wireless network connections; and

20

a processor communicative with both the first wireless adapter and the second wireless adapter, the processor programmed to execute network security rules to isolate network communications data of each of the plurality of secured wireless network connections from all other network communications data passing through the first wireless adapter.

25 In another aspect there is provided, a system for adding a secured wireless network connection to a wireless network broadcasting device, the system comprising:

a wireless network broadcast device configured to broadcast a first open unsecured wireless network connection and to broadcast a first secured wireless network connection uniquely accessible by a first subscriber, the open unsecured wireless network connection directed to a unique first web page providing information relating to purchase of a second secured wireless network connection of the wireless network broadcast device;

30

a remote server communicative with the wireless network broadcast device through an Internet access point, the remote server configured to receive a communication relating to purchase of the second secured wireless network connection by a second subscriber, and sending a communication to the wireless network broadcasting device to add the second secured wireless network connection uniquely accessible by the second subscriber.

In yet another aspect there is provided, a system for adding a secured wireless network connection for a subscriber in a mobility mode, the system comprising:

a first wireless network broadcast device configured to broadcast an open unsecured wireless network connection, to broadcast a home mode secured wireless network connection uniquely accessible by a first subscriber in a home mode, and to broadcast a mobility mode secured wireless network connection uniquely accessible by a second subscriber in a mobility mode, the home mode designated when the first subscriber initially establishes the home mode secured wireless network connection with the first wireless network broadcast device in a first wireless communication range and remains geographically within the first wireless communication range of the first wireless network broadcast device, a mobility mode designated when the second subscriber initially establishes a home mode secured wireless network connection with a second wireless network broadcast device in a second wireless communication range and moves geographically outside of the second wireless communication range of the second wireless network broadcast device and remains within the first wireless communication range of the first wireless network broadcast device;

a remote server communicative with the first wireless network broadcast device through an Internet access point, the remote server configured to receive information from the first wireless network broadcast device relating to the second subscriber, accessing a stored record of the second subscriber to designate the second subscriber in the mobility mode, and sending a communication to the first wireless network broadcasting device to add the mobility mode secured wireless network connection uniquely accessible by the second subscriber in the mobility mode.

In further aspects, methods and computer readable media for implementing the wireless network broadcast device are also provided.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows a system for providing a plurality of secured wireless network connections over a shared Internet access point;

Figure 2 shows an alternative implementation of the system shown in Figure 1;\

5 Figure 3 shows a communication path between a processor and memory in the wireless network broadcast device used in the system shown in Figure 1 or 2;

Figure 4 shows a block diagram of a performance parameter update of the system shown in Figure 1 or 2;

10 Figure 5 shows a block diagram of a network configuration update of the wireless network broadcast device shown in Figure 1 or 2;

Figure 6 shows a block diagram of a subscriber usage update of the system shown in Figure 1 or 2;

15 Figure 7 shows a block diagram of a network configuration update of the wireless network broadcast device shown in Figure 1 or 2, modified to accept two classes of subscribers – home subscribers and mobility subscribers;

Figure 8 shows a block diagram of automated addition of a network for a mobility subscriber to the wireless network broadcast device;

Figure 9 shows a block diagram of automated removal of a network for a mobility subscriber to the wireless network broadcast device.

20

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Referring to the drawings, Figures 1 and 2 show a system, generally designated by reference numeral 1, for providing a plurality of secured wireless network connections over a single shared Internet access point. The system 1 allows a subscriber of Internet services from an upstream Internet services provider (ISP) to in turn become a shared Internet service (SIS) provider of a plurality of secured wireless network connections, each of which may be assigned and sold to an individual neighboring subscriber. The system 1 employs a wireless network broadcast device 10 to broadcast at least one open unsecured wireless network connection and a plurality of secured wireless network connections. The wireless network broadcast device 10 is a computing device including multiple operably connected computing components contained with a housing 11, the computing components cooperatively interacting to broadcast at least one open unsecured wireless network connection and a plurality of secured wireless network connections.

25

30

The wireless network broadcast device 10 may be configured with any conventional hardware or programmable elements including a processor 12 for executing computer programmable code. The processor 14 is communicative with a memory 14 which stores computer programmable code and data generated during execution of the computer programmable code. The processor 14
5 may also be communicative with a display 16 or any suitable visual indicators, such as LED indicators. The processor 14 is also communicative with a local area network (LAN) adapter 18 and a first wireless LAN (WLAN) adapter 20 and optionally, a second WLAN adapter 22. The housing 11 may further support additional input/output devices or input/output ports as desired. The housing 11 also supports a power supply unit 24 which is operably connected with processor
10 12 and other computer components to distribute electric current as needed for operation. Communication of computing signals and electric current may be achieved using any conventional electric circuitry, for example computer bus architecture.

The first WLAN adapter 20 is controlled by processor 12 to broadcast at least one open unsecured wireless network connection 30 and a plurality of secured wireless network
15 connections, for example a first secured wireless network connection 31a and a second secured wireless network connection 31b. The at least one open unsecured wireless network connection 30 is broadcast with a network name, such as a service set identifier (SSID), that is selected by a SIS provider that uses the wireless network broadcast device 10, and more specifically uses the open unsecured wireless network connection 30, to advertise options for and sale of wireless and
20 secure shared Internet access to neighboring subscribers wishing to purchase Internet services. With purchase of Internet services, wireless enabled computing devices of first and second neighboring subscribers, 32a and 32b, can connect to first and second secured wireless network connections, 31a and 31b, respectively.

In order to purchase Internet access through one of the plurality of secured wireless
25 network connections, a neighbor interested in obtaining secured Internet access will initially connect to the at least one open unsecured wireless network connection 30 with a wireless enabled computing device. Connection of a wireless enabled computing device to the at least one open unsecured wireless network connection 30 can be achieved without a password authentication step. Connection of the neighbor's wireless enabled computing device to the at
30 least one open unsecured wireless network connection 30 directs an Internet browser installed on the neighbor's wireless enabled computing device to an Internet webpage or captive portal hosted on a remote server 60 that provides information relating to available data transmission speed

and/or permitted data transmission amounts over a preset time interval (for example, per month) for the plurality of secured wireless network connections. The webpage or captive portal can also provide prompts and dialogue boxes for payment functions, providing contact information and providing information to configure one of the plurality of secured wireless network connections, including a network name (eg, SSID), a network password, and options for encryption and securing Internet data communications. The webpage or captive portal can also provide ratings or reviews of the SIS provider that has installed the wireless network broadcast device 10. The webpage or captive portal can also provide a connectivity test to test connectivity speed of the neighbor's wireless enabled computing device with the wireless network broadcast device 10 prior to committing to purchase of secured Internet access. Any conventional method for testing connectivity speeds may be used. For example, the connectivity test can comprise a step of calculating time required for download and/or upload of a reference or standardized file or data packet – for example, any conventional check file – between the neighbor's wireless enabled computing device and remote servers 60 through the open unsecured wireless network connection 30.

The at least one open unsecured wireless network connection 30 is typically broadcast continuously during operation of the wireless network broadcast device 10. However, broadcast of the at least one open unsecured wireless network connection 30 may be paused as desired by the SIS provider in an ad-hoc fashion or based on any predetermined rule set such as a preset threshold for a maximum number of subscribers or wireless enabled computing devices or a preset threshold for amount of data transmission over a monthly time interval or a preset threshold for a minimum speed of data transmission.

Once the neighbor interested in obtaining secured Internet access provides sufficient information to satisfy predetermined verification and eligibility rules by communications through the at least one open unsecured wireless network 30 with the webpage or captive portal hosted on the remote server 60, the interested neighbor is considered a neighbor subscriber (eg., Subscriber A). Communications of the interested neighbor with the webpage or captive portal hosted on the remote server 60 can be encrypted (for example, using an https encryption protocol) to prevent misuse of the open unsecured wireless network 30 by a third party intent on stealing the interested neighbor's information, including for example credit card payment data. After the interested neighbor is established as a neighbor subscriber (eg., Subscriber A), communications between the remote server 60 and the wireless network broadcast device 10 configure the wireless network

broadcast device 10 to broadcast a first secured wireless network connection 31a with the network name (SSID) and password selected or preset by the neighbor subscriber. The neighbor subscriber (Subscriber A) can then use a wireless enabled computing device 32a to connect to the first secured wireless network connection recognizable and selectable by the preset SSID and providing authentication using the preset password. The enrollment process can then be repeated for a second neighbor subscriber (eg., Subscriber B) and repeated again to enroll further subscribers. Network security rules such as firewall, sandbox, jail and/or tunneling protocols are implemented to isolate data communication 38 of each of the plurality of secured wireless network connections from all other data transmission passing through wireless network broadcast device 10. As such, data transmission 38 of each neighbor subscriber is secured and isolated from data transmissions of all other subscribers and data transmissions of the SIS provider.

In order to secure and isolate data transmissions of each individual neighbor subscriber, a subnet organization may be imposed such that each wireless network broadcast device 10 is designated by a unique Internet Protocol (IP) address that includes a unique network identifier, typically obtained from router/modem 40 of the ISP, while each neighbor subscriber network is designated by a unique IP address that includes a unique combination of the network identifier and a subnet identifier, and each neighbor subscriber device is designated by a unique IP address that includes a unique combination of the network identifier, the subnet identifier and the machine identifier; IP address organization may be delineated even further, for example to include a unique identifier for each port within a device. Having the neighbor subscriber networks divided into subnets allows the wireless network broadcast device 10 and all the supported neighbor subscriber networks to be connected to the Internet with a single shared network address, while still providing secure and isolated data transmissions for each neighbor subscriber network. Based on unique IP addresses for subnet and subnet devices (each device may be considered a sub-subnet) the wireless network broadcast device 10 can be configured with routing tables that are accessed by internal gateways to manage routing of data transmissions to and from each neighbor subscriber network. Typically, the wireless broadcast network device 10 obtains IP address space from router/modem 40. Any conventional scheme to combine network address, subnet address and machine address may be used to organize IP addresses obtained and supported by the wireless network broadcast device 10, including for example Classless Inter-Domain Routing (CIDR) notation or Variable-Length Subnet Masking (VLSM) notation of IPv4 or IPv6 addresses. Both CIDR and VLSM techniques allow a network to be divided into variously sized

subnets, providing efficient use of IP address space and sizing networks more appropriately for local needs.

The SIS provider typically purchases Internet access from an ISP that provides network services over a geographic span that is larger than a neighborhood, such as a geography that spans a city, state, or country. As part of purchase of Internet access from the ISP, the SIS provider installs a router/modem 40 that provides an Internet access point to the ISP communications network 35 and ultimately to the Internet 50. The SIS provider maintains Internet access and a computing network through a network connection supported by the router/modem 40. The wireless network broadcast device connects to the router/modem 40 by a wired network cable (eg., Cat5) connection 34 with LAN adapter 18 as shown in Figure 1 or by a wireless network connection 36 with the second WLAN adapter 22 as shown in Figure 2. Any convenient method may be used to establish the wireless network connection 36 between the wireless network broadcast device 10 and the router/modem 40. For example, the wired network cable connection 34 may be used for initial automated configuration of the wireless network broadcast device 10, after which the SIS provider may access a unique account webpage where available wireless network connections that are within range of the wireless network broadcast device 10 are displayed with prompts for the SIS provider to select the appropriate SSID belonging to the SIS provider and to enter a corresponding password. The SSID and password information can then be sent to the wireless network broadcast device 10 to attempt to establish the wireless network connection 36 with the router/modem 40. If the wireless network broadcast device 10 establishes the wireless network connection 36 with the router/modem 40 using the SSID and password information, then a test may be performed to check connectivity speed and completeness of a standardized or reference file, and if the test achieves predetermined threshold criteria for success a notification to disconnect the wired network cable connection 34 may be sent to the SIS provider by any conventional messaging medium (eg., email, SMS text message) and/or may be posted to the SIS provider's dedicated account webpage. Steps to establish the wireless connection 36 may begin based on an automated protocol or may be triggered by a specific request from the SIS provider.

When enrolling in the system 1, the SIS provider undergoes verification and eligibility protocols which can include verification of contact information and address and submission of bank account information and/or credit card information and a security deposit. Information submitted during enrollment is used to setup an account for the provider and to populate the SIS

provider's advertising web page or captive portal that is linked to the at least one open unsecured wireless network connection 30.

After successful enrollment the SIS provider receives the wireless network broadcast device 10 programmed for automated connection with remote servers 60 once connected to router/modem 40. The wireless network broadcast device 10 is authenticated by any convenient rule set, including a hardware identifier unique to each wireless network broadcast device 10, and once authenticated can communicate and synchronize with configuration updates sent from a remote server 60. The wireless network broadcast device 10 can obtain the IP address from the dynamic host configuration protocol (DHCP) service of the router/modem 40, for example the processor 12 and/or the LAN adapter 18 may communicate with the router/modem 40 to obtain an IP address. For security, the SIS provider may be prevented from direct access or login to the wireless network broadcast device 10 as may be desired for customization or configuration of the device 10; instead customization and configuration selections, as well as device status and usage metrics of neighbor subscribers can be presented on a web page hosted on the remote servers 60 with reconfiguration of the wireless network broadcast device 10 achieved by communication with the remote servers 60.

Once the wireless network broadcast device 10 is authenticated it can be operational to broadcast the at least one open unsecured wireless network connection 30 to promote the wireless network service of the corresponding SIS provider.

The wireless network broadcast device 10 is any combination of computer hardware and computer programmable code that functions to support a plurality of secured wireless networks and at least one open network and supports analysis of usage of each of the secured wireless networks. Figure 3 is an illustrative example of communication paths between the processor 12 and memory 14 showing an example of operable connections of logical components in the wireless network broadcast device 10. Executable components of the processor 12 include a clock 71, usage tracker 72, data manager 73, router 74, and network security 75. Clock 71 can be accessed as desired to correlate an event with a time and optionally to record the time or the time correlated event in the memory 14. Clock 71 may be provided locally within the wireless network broadcast device 10 or time can be maintained based on a time service from a remote server. Clock 71 may provide timestamps 81 to be recorded in memory 14 or may be accessed by any other logical component to provide a time stamp as desired which may also be recorded in memory 14. Usage tracker 72 can be accessed to analyze and calculate usage of each of the

plurality of secured wireless networks and can be configured by tracking algorithms 82 stored in memory. The usage tracker 72 will generate usage data specific to each of the secured wireless networks and data manager 73 can record, organize and compile the usage data as desired, for example as usage statistics 83 recorded in memory 14 categorized according to each of the secured wireless networks. Router 74 is responsible for directing inbound and outbound data packets for network data traffic. Router 74 will maintain routing data 84 in memory typically in the form of routing tables and will typically be configured for TCP/IP protocol capability. Routers allow for connection of a plurality of logical groups of computer devices known as subnets, each with a different sub-network address. Network security 75 will be configured as desired to provide secured wireless networks including, for example firewall and/or VPN capability and will be configured according to security settings 85 such as rules and algorithms. Information maintained in memory as well as logical components executed by the processor may be modified as desired by configuration update communications between the wireless network broadcast device 10 and remote servers 60. Layout of logical components and their connections shown in Figure 3 is merely illustrative and any suitable combination, substitution or addition of conventional computing components may occur including, for example, combination of router and network security components or combination of usage tracker and data manager components.

In operation, the wireless network broadcast device 10 communicates with one or more remote servers to send and receive information that may trigger and/or execute an update event. Most update events can be accomplished by automated communication and synchronization between the wireless network broadcast device 10 and remote servers 60. For example, Figure 4 shows wireless network broadcast device logic 100 and server logic 102 for an update of a device performance parameter. The device initiates a connection with the server (step 104) and the server receives the connection request (step 105). The device requests a check file and downloads the check file (step 106) provided by the server (step 107). The check file is a standardized data file (such as a standardized image) served by a secured check file server. Upon download of the check file, the device can run a test on the file to check integrity, such as a cyclic redundancy check (CRC) to yield a checksum value. The device measures the time interval from the time of sending the request for the check file to the time of completion of the download (step 108) and uses the measured elapsed time and the known data size of the check file to calculate the device speed of connection to the Internet (step 110). To update the speed of connection the device requests connection to a server that stores the performance data (step 112) and the server receives the

connection request (step 114). The device provides an encrypted key (step 116) which the server validates (step 118). The server proceeds to validate a good standing of the account (step 120) and update a log and any change to the IP address corresponding to the device (step 122). The device provides the calculated speed of connection (step 124) prompting the server to update a speed record in a corresponding account (step 126). Upon completion of the update the server provides a response to the device (step 128) and the device validates the response to ensure that the calculated speed data has been properly recorded (step 130).

Figure 5 shows an example of wireless network broadcast device logic 140 and server logic 142 for a wireless network configuration update of the device. The device initiates a connection with the server (step 144) and the server receives the connection request (step 146). The device provides an encrypted key (step 148) which the server validates (step 150). The device requests a configuration update (step 156) prompting the server to provide a list of all network configurations linked to the corresponding account (step 154). The device receives the list of current network configurations (step 156) and validates the server response to ensure that the list of current network configurations is a complete transmission (step 158). The device determines whether a difference exists between the existing configuration of the device and the configuration lists received from the server (step 160). The determination of a difference may be based on a comparison of any suitable parameter including for example network names (eg, SSID), network passwords, number of secured networks defined, neighbor subscriber customization selections, SIS provider customization selections, MAC addresses, and the like. If no difference exists then the update is terminated. If a difference exists then an update is executed (step 164). The update can be executed using any convenient technique including, for example, a complete overwrite of the system configuration or a targeted update for each wireless network that is related to a detected difference (determined in step 160). The updated configuration is saved as the existing configuration (step 166) of the device, and the network interface is reloaded (step 168).

Figure 6 shows an example of wireless network broadcast device logic 180 and server logic 182 for an update of subscriber usage statistics to subscriber usage records stored on the server. The device tracks and records each subscriber's usage statistics derived from analysis of header information of all data packets sent and received through the device (step 184). At predetermined time intervals, that typically range from an hour to a day, the device initiates a connection with the server (step 186) and the server receives the connection request (step 188). The device provides an encrypted key (step 190) which the server validates (step 192). The device

provides subscriber usage statistics recorded since a previous update (step 194). The server updates subscriber usage records that are linked to an account corresponding to the device (step 196) and sends a completion response (step 198). The device validates the response to ensure a completed update (step 200) and resets subscriber usage statistics to begin tracking and recording subscriber usage over a current time interval (step 202).

The system 1 can be adapted to include a mobility function to provide Internet service to a neighbor subscriber that is travelling outside of a home range. When a mobility function is implemented each of the plurality of neighbor subscribers served by the system 1 can be categorized as either a home neighbor subscriber or a mobility neighbor subscriber. A home neighbor subscriber is a neighbor subscriber using a secured wireless network connection provided by an SIS provider linked or related to that neighbor subscriber at the time of enrollment, with the linked SIS provider being considered that neighbor subscribers home SIS provider; typically the secured wireless network connection is supported on the same wireless network broadcast device 10 that provided the open unsecure wireless network for enrollment unless the wireless network broadcast device has been changed subsequent to enrollment. By comparison, a mobility neighbor subscriber is a neighbor subscriber using a secured wireless network connection provided by an SIS provider that is not linked or unrelated to that neighbor subscriber at the time of enrollment. Thus, each neighbor subscriber and SIS provider pairing that is established at the time of enrollment of the neighbor subscriber is considered the home relationship, and all other neighbor subscriber and SIS provider interactions are categorized as a mobility relationship. Therefore, each neighbor subscriber can transition between categorization as a home neighbor subscriber or a mobility neighbor subscriber depending on whether the neighbor subscriber is within wireless range of wireless networks provided by the corresponding home SIS provider. The home neighbor subscriber computing device maintains a wireless network connection with its corresponding home SIS provider until the wireless network connection is lost or out of range, at which point a wireless network connection can be established between the neighbor subscriber and a different SIS provider in a mobility relationship.

To support transition from home to mobility subscriber/provider pairings while maintaining security and tracking of usage statistics, each wireless network broadcast device 10 can be configured to provide IP addresses that are specific to either home network connections or mobility network connections. For example, for each wireless network broadcast device 10 a first

specific range of unique internal/private IP addresses can be reserved for designation of home relationship wireless network connections, while a second specific range of internal/private IP addresses can be reserved for mobility relationship wireless network connections. In a specific illustrative example, IP address ranges supported by the system may range from 10.1.0.0 to 10.1.255.255 for home wireless network connection internal/private IP addresses, while ranging from 10.2.0.0 to 10.2.255.255 for mobility wireless network connection internal/private IP addresses. As a result of unique IP addresses specific to home versus mobility wireless network connections, at any given time a neighbor subscriber wireless network connection is designated with either a unique home IP address or a unique mobility IP address with usage statistics being calculated accordingly in the neighbor subscribers account as well as the home SIS provider account or the mobility SIS provider account as appropriate.

Rules for transitioning between a home relationship wireless network connection and a mobility relationship wireless network connection can be set according to any desired criteria to promote efficiency and predictability suited to a particular implementation of the system. For example, a mobility relationship wireless network connection may be triggered by a neighbor subscriber recognizing that a home wireless network is disconnected and/or unavailable and searching available wireless network connections for a network name (SSID) identifier representing an open unsecured wireless network of an SIS provider that is different than the home SIS provider. Alternatively, the system 1 may be automated to pole and recognize broadcast signals from devices and automatically establish wireless network connections in a mobility relationship when the home wireless network connection is unavailable or disconnected. Optionally, rules for initiating a diagnostic check of the home relationship wireless network connection may be established, including for example triggering a diagnostic check if the geographical proximity of the neighbor subscriber computing device and the home SIS provider wireless network broadcast device 10 is less than a predetermined threshold distance when the home relationship wireless network is disconnected. In another example, a diagnostic check may be triggered if more than a predetermined number of home neighbor subscriber networks are disconnected from their corresponding home SIS provider wireless network broadcast device simultaneously.

Figure 7 shows an example of wireless network broadcast device logic 220 and server logic 222 for a wireless network configuration update of the device for an implementation that includes both home and mobility wireless network connections. The device initiates a connection

with the server (step 224) and the server receives the connection request (step 226). The device provides an encrypted key (step 228) which the server validates (step 230). The device requests a configuration update (step 236) prompting the server to provide a list of all network configurations linked to the corresponding account (step 234). The list of all network configurations includes information relating to home networks and mobility networks as appropriate. For home networks the server returns user configured settings including subnet (eg., 10.1.3.0, 10.1.4.0, etc.), password and other network settings, while for mobility network the server selects the next available subnet range in the mobility network (eg., 10.2.1.0, 10.2.2.0, 10.2.3.0, etc.), and provides the network password and other network settings based on the neighbor subscribers account preferences and settings. The device receives the list of current network configurations (step 236) and validates the server response to ensure that the list of current network configurations is a complete transmission (step 238). The device determines whether a difference exists between the existing configuration of the device and the configuration lists received from the server (step 240). The determination of a difference may be based on a comparison of any suitable parameter including for example network names (eg, SSID), network passwords, number of secured networks defined, total network number, home mode network number, mobility mode network number neighbor subscriber customization selections, SIS provider customization selections, MAC addresses, and the like. If no difference exists then the update is terminated (step 242). If a difference exists then the list of configuration settings received from the server is parsed to extract configuration settings and identifiers and passwords for each subnet network (steps 244a to 244d), the parsed information is analyzed to ensure removal of a redundant or duplicate subnet network (step 244e), the network configurations for the device is updated (step 244f) and network security rules and tunnels are updated (steps 244g and 244h). Updates can be accomplished using any convenient technique including, for example, a complete overwrite of the system configuration of the device or targeted updates of networks impacted by a detected difference (as determined in step 240) The updated configuration is saved as the existing configuration (step 246) of the device, and the network interface is optionally refreshed or reloaded as desired (step 248).

To ensure that the list of network configurations provided in step 234 is kept current the server must periodically update the list of network configurations, particularly with respect to mobility network connections which are likely to be more transient than home network connections.

Figure 8 shows a wireless network broadcast device logic 260 and server logic 262 for automated recognition of a neighbor subscriber in range of a mobility wireless network connection and automated update of the list of network configurations for an SIS provider account by the server. The device captures and compiles a list of MAC addresses in proximity or within broadcast range (step 264). At predetermined time intervals, that typically range from 10 to 10000 times a day, the device initiates a connection with the server (step 266) and the server receives the connection request (step 268). The device provides an encrypted key (step 270) which the server validates (step 272). The device provides a list of MAC address in proximity of the device (step 274). The server analyzes the list and for each MAC address on the list determines whether the MAC address has been associated with a network (step 276). A MAC address association with a network can be verified using any convenient technique including, for example, maintaining a database of MAC addresses linked to neighbor subscriber accounts and/or SIS provider accounts. If the MAC address is not recognized by the server as a known MAC address then it is discarded (step 278) without further action and the analysis proceeds to the next MAC address on the list. If the MAC address is recognized, but is determined to be connected to a home network then the MAC address is discarded (step 282) without further action and the analysis proceeds to the next MAC address on the list. If the MAC address is recognized and is not connected to a home network then the server updates the list of network configurations to add the MAC address network configurations stored in the neighbor subscriber account settings using an appropriate mobility subnet IP address (step 284). Once the entire list of MAC addresses is processed the server sends a completion response (step 286). The device validates the response to ensure a completed update (step 288). When compiling the MAC address list (step 264) the wireless network broadcast device is only listening to computer broadcasts of MAC addresses to generate a list of MAC addresses in the vicinity – and is not engaging in two-way communication. Once a MAC address is recognized as associated with an existing neighbor subscriber and a mobility relationship secured wireless network connection is broadcast as part of a configuration update and the neighbor subscriber computer device automatically recognizes the network name (SSID) and password and connects that two-way encrypted communication begins between the wireless network broadcast device and the neighbor subscriber's computer device.

Figure 9 shows a wireless network broadcast device logic 300 and server logic 302 for automated recognition that a neighbor subscriber has disconnected from a mobility wireless network connection and automated update of the list of network configurations for an SIS

provider account by the server. The device compiles a list of all MAC addresses that are currently connected to and communicative with the device (step 304), and optionally includes a corresponding mobility subnet IP address for each connected MAC address. At predetermined time intervals, that typically range from 10 to 100 times a day, the device initiates a connection with the server (step 306) and the server receives the connection request (step 308). The device provides an encrypted key (step 310) which the server validates (step 312). The device provides the list of MAC addresses currently connected to the device (step 314). The server determines whether a difference exists between the existing mobility network configurations stored in memory on the server and the list of connected MAC addresses received from the device (step 316). If no difference exists then the update is terminated (step 318). If a difference exists then the list of mobility network configurations stored in memory on the server is updated to remove each network configuration that does not find a match within the list of connected MAC addresses received from the device (step 320). Once the mobility network configurations are updated so that no difference exists with the list of connected MAC addresses the server sends a completion response (step 322). The device validates the response to ensure a completed update (step 324).

An illustrative version and several variants of a system and method for providing a plurality of secured wireless network connections over a shared Internet access point have been described above without any intended loss of generality. Further variants, modifications and combinations thereof are contemplated and will be apparent to the person of skill in the art.

For example, a profile of a shared Internet service (SIS) provider may tolerate many variations including any natural person or entity having and purchasing an existing Internet service from an Internet service provider (ISP). Typically, the ISP will be government registered and will have a network coverage that is geographically distributed across a plurality of postal codes, for example at least distributed across a majority of the geographical area of a city or metropolitan region. While in certain examples the SIS provider may be an operational entity such as a business, often the SIS provider will be an individual or natural person having control of a single Internet access point installed within a residential unit wishing to monetize their Internet access by sharing their service with neighbor subscribers. The SIS provider can market and sell their existing Internet service access securely and safely through an open wireless network connection of the wireless network broadcast device. The SIS provider can order and obtain the wireless network broadcast device by any suitable method including, for example, a registration on an administrator website or a download of a software application that automates a

connection with an administrator server and navigates a registration process. The SIS provider can market Internet service to potential neighbor subscribers wirelessly, automatically and securely through the open wireless network connection as it will be directed to a computer hosted electronic marketing page controlled by the administrator and will not be directed to or provide
5 access to the SIS provider's personal network or local area network. In certain examples, each open wireless network connection of each wireless network broadcast device is directed to a customized marketing page, and the SIS provider will be able to customize their marketing page through any convenient process to present Internet service options or packages that are suited towards or supported by the existing Internet service of the provider. Customization selections
10 may occur through interaction with administrator controlled servers and in certain examples the wireless network broadcast device communicates and synchronizes with administrator controlled servers to update the marketing page to present and maintain at least one performance parameter, such as a speed of connection or an available data usage of the wireless network broadcast device.

A neighbor subscriber may be any natural person or entity purchasing access to a secured
15 wireless network connection broadcast by the wireless network broadcast device. In certain examples, the neighbor subscriber is an individual or natural person residing in a residential unit within broadcast range of the wireless network broadcast device. Using a wireless network connection enabled computer device, a potential neighbor subscriber can search for an open wireless network connection name known to be associated with the SIS provider or the SIS
20 system to be directed to the marketing page that provides marketing information related to the corresponding SIS provider's Internet service including, for example, pricing options and one or more performance parameters of the Internet service (eg., connection speed, data usage availability). The marketing page can itself or through links with further pages hosted on administrator controlled servers provide a graphical interface for a neighbor subscriber to register
25 for and purchase access to a secured wireless network connection using any suitable technique known in electronic commerce. The network name and password of the secured wireless network connection may be established through any suitable technique. For example, the registration and purchasing process can include a step of the neighbor subscriber selecting a customized and distinct network name and network password. In an alternative example, the network name and
30 password may be selected by the administrator and provided to the neighbor subscriber with the neighbor subscriber provided with options to change a network name and password through a subscriber account webpage hosted on an administrator controlled server. Additional security

measures such as sending time limited codes to neighbor subscribers by cellular network (eg, automated text or voice messages to a subscriber's cell phone) or email messages that are required to be inputted by the subscriber within the designated time limit may be implemented as desired. Subscribers can monitor usage and receive alerts for their consumption of services
5 through any convenient technique including, for example, through an application installed on a computer device or through login to an online account.

The open wireless network connection may be broadcast with any suitable network name (eg, SSID). The network name provides a notice function that a wireless network broadcast device is available for internet sharing. In one example, the network name of the open wireless
10 network connection may follow an established template with a first common portion of the network name set as a corporate or brand name and a second portion individually selected by a corresponding SIS provider. In alternative examples, a corporate or brand name is set to be the same network name for all open wireless network connections or conversely each network name is entirely set by the corresponding SIS provider. When the network name includes a corporate or
15 brand name common to multiple open wireless network connections within the system, an administrator of the system may engage in marketing of the corporate or brand name of the open wireless network name to enhance positive reputational recognition and confidence in network names (eg., SSID) of each open wireless network.

The wireless network broadcast device may be any suitable computing device that has at
20 least one processor (processor encompasses any type of computer processor including for example microprocessor or microcontroller or single chip integrated circuit architecture), a memory, a power supply input, a wireless adapter broadcasting a plurality of secured wireless network connections, and is configured for connection and communication with an Internet access point. Numerous optional features may be implemented as desired including for example,
25 a graphical display presenting alphanumerical characters, visual or lighted indicators such as LEDs, a dedicated wireless adapter for connection to the Internet access point, and the like. The wireless network broadcast device will include hardware or programmable code combinations as needed to establish a router component to maintain correct routing of data packets to and from each of the secured wireless networks, a network security component to ensure isolation of
30 communications for each secured wireless network connection from all other secured wireless network connections broadcast by the wireless network broadcast device, and optionally a usage

tracker component recording information related to usage of each of the secured wireless network connections.

The wireless adapter is typically configured to a Wi-Fi 802.11 communication standard. However, other communication standards or protocols may be used as suited to a particular implementation.

The router component of the wireless network broadcast device will typically be scaled to capabilities of home (residential) or small office routers, and will typically not be scaled to capabilities of larger enterprise and industrial routers. Similarly, the wireless network broadcast device will often be connected to an Internet access point of a residence or small office through an ISP that maintains a wider area network that covers at least a city or a metropolitan geography. The Internet access point will typically be a router or modem configured for residential or small office use.

While implementation of the wireless network broadcast device has been illustrated using residential or small office use, other implementations can readily be accomplished including for example incorporation of wireless network broadcast device within the existing network infrastructure of a government registered ISP.

The usage tracker component may be configured as desired to communicate with a remote server to maintain usage records in a memory. In certain examples, usage statistics are recorded in a memory of the wireless network broadcast device and are communicated at a predetermined time interval to the remote server configured to maintain subscriber usage records. Subscriber usage may be tracked according to any convenient usage parameter including time of use and amount of data uploaded or downloaded. For example, subscriber usage may be tracked by analyzing header information of data packets sent and received through a secured wireless network connection of the wireless network broadcast device.

The system may accommodate any type of end-user computing device, whether it be a neighbor subscriber computing device or an SIS provider computing device, provided the computing device includes a wireless network interface and includes an Internet browser. For example, the computing device may be a desktop, laptop, notebook, tablet, personal digital assistant (PDA), PDA phone or smartphone, gaming console, portable media player, and the like. The computing device may be implemented using any appropriate combination of hardware and/or software configured for wireless communication over a wireless network connection provided by the wireless network broadcast device. The computing device hardware components

such as displays, storage systems, processors, interface devices, input/output ports, bus connections and the like may be configured to run one or more applications to allow, for example, tracking of network usage, display of network usage metrics, customization of network parameters, and/or initiating a transition between a home mode and a mobility mode. The term
5 end-user computing device can encompass both a neighbor subscriber computing device and a SIS provider computing device. The terms end-user computing device and client computing device may be used interchangeably when the system is implemented in a client/server arrangement. Suitable protocols for handshakes and network security are implemented for connection and communication between the wireless network broadcast device and an end-user
10 computing device.

The server computer may be any combination of hardware and software components used to store, process and/or provide information relating to operation of a wireless network broadcast device including, for example, authentication of a wireless network broadcast device, configuration update of a wireless network broadcast device, tracking of network usage, display
15 of network usage metrics, customization of network parameters, and/or a transition between a home mode and a mobility mode. The server computer components such as storage systems, processors, interface devices, input/output ports, bus connections, switches, routers, gateways and the like may be geographically centralized or distributed. The server computer may be a single server computer or any combination of multiple physical and/or virtual servers including for
20 example, a web server, a performance tracker server, a usage tracker server, a configuration update server, a home/mobility mode server, an image server, an application server, a bus server, an integration server, a meta actions server, and the like. The server computer components such as storage systems, processors, interface devices, input/output ports, bus connections, switches, routers, gateways and the like may be configured to run one or more applications to, for example,
25 generate a unique identifier for a network connection, generate a unique identifier for a neighbor subscriber, generate a unique identifier for an SIS provider, generate a unique identifier for a wireless network broadcast device, generate a URL for a unique web page for promoting an SIS provider, populating the unique web page according to selected choices of the SIS provider, receive a request from a wireless network broadcast device including its unique identifier, send
30 the predetermined actions to the wireless network broadcast device, and/or receive the selection of one or more of the predetermined actions from an end-user computing device.

While the system has been illustrated using a client/server implementation, the system may also accommodate a peer-to-peer implementation.

The network may be a single network or a combination of multiple networks. For example, the network may include the Internet as a single network or may include the Internet in combination with one or more intranets, landline networks, wireless networks, and/or other appropriate types of communication networks. In another example, the network may comprise a wireless telecommunications network (e.g., cellular phone network) adapted to communicate with other communication networks, such as the Internet. Typically, the network will comprise a computer network that makes use of a TCP/IP protocol (including protocols based on TCP/IP protocol, such as HTTP, HTTPS or FTP).

The system may be adapted to follow any computer communication standard including Extensible Markup Language (XML), Hypertext Transfer Protocol (HTTP), Java Message Service (JMS), Simple Object Access Protocol (SOAP), Lightweight Directory Access Protocol (LDAP), and the like.

Network security provided in each wireless network broadcast device may be any combination of hardware and software that isolates communications data of each secured wireless network connection from all other network communications passing through the device, or more generally through the Internet access point. At a minimum, computer programmable code of network security rules are provided to isolate network communication data of each of the plurality of secured wireless network connections from all other network communications data passing through the device, or more generally through the Internet access point. The network security rules provide a firewall, a sandbox, a jail, and the like. The network security rules may provide a tunneling protocol including, for example, a virtual private network (VPN) protocol for tunneling and/or encryption such as Layer 2 Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP), Secure Shell (SSH), Microsoft Point-to-Point Encryption (MPPE), Secure Socket Tunneling Protocol (SSTP), Internet Protocol Security (IPsec), and the like. Other forms of network security include password secured network access. Password authentication may occur through any suitable protocol including wired equivalent privacy (WEP), Wi-Fi protected access (WPA or WPA2), lightweight extensible authentication protocol (LEAP), and the like. Hardware and/or firmware may be adapted to support network security rules as desired.

In certain examples, network security will at least include authentication, typically with a username and a password, and a firewall. Two- or three-factor authentication using, for example,

a security token such as a USB token or software token, a unique membership identifier, a time-limited mobile phone code, a fingerprint or retinal scan, and/or a digital certificate may be added as desired. A firewall enforces access policies such as what services are allowed to be accessed by the network users. Optionally, network security may include anti-virus software and/or an intrusion prevention system, more specifically a wireless intrusion prevention system. In further examples, network security options include tunneling protocols, MAC address filtering based on lists of approved MAC addresses, and end-to-end encryption.

The purpose of using unique identifiers is to be able to sort information relevant to each neighbor subscriber, SIS provider, wireless network broadcast device configuration update, usage metrics, subscriber purchasing interest, recognition of subscriber in mobility mode, and the like according to unique identifiers. Many different types of unique identifier schemes may be useful and any conventional scheme may be accommodated and used within the system. For example, a code scheme may be based on a unix time appended a numerical or alphanumerical incremental series. A portion of each unique identifier may have a random or entropy component. Each unique identifier may optionally be obfuscated through an encryption function or a hashing function. Hashing functions provide a convenient compromise of security and speed. Examples of hashing functions include MD5 or any of the Secure Hash Algorithms SHA1, SHA2 (SHA224, SHA256, SHA384, SHA512) and SHA3.

The system may accommodate any type of still or moving image file as may be suitable to generate a unique web page promoting SIS provider services or displaying usage metrics to SIS providers or neighbor subscribers. Suitable types of still and moving images include, for example, JPEG, PNG, GIF, PDF, RAW, BMP, TIFF, MP3, WAV, WMV, MOV, MPEG, AVI, FLV, WebM, 3 GPP, SVI and the like. Furthermore, a still or moving image file may be converted to any other file without hampering the ability of the system software to identify and process the image. Thus, the system may accommodate any image file type and may function independent of a conversion from one file type to any other file type.

Web pages promoting each SIS provider and prompts for directing subscriber purchasing interest may be represented by any convenient form or user interface element including, for example, a window, a tab, a text box, a button, a hyperlink, a drop down list, a list box, a check box, a radio button box, a cycle button, a datagrid or any combination thereof. Furthermore, the user interface elements may provide a graphic label such as any type of symbol or icon, a text label or any combination thereof. The user interface elements may be spatially anchored or

centered around the corresponding advertising display or prompt. Otherwise, any desired spatial pattern or timing pattern of appearance of user interface elements may be accommodated by the system. In certain examples, a web page may be customized by an SIS provider and types and orientation of graphic user interface elements may at least in part be selected by the SIS provider.

5 The terms mobility relationship and mobility mode are used interchangeably. The terms home relationship and home mode are used interchangeably. A home mode is designated when a neighbor subscriber computer device initially establishes the home mode secured wireless network connection with the wireless network broadcast device and remains geographically within the wireless communication range of the wireless network broadcast device. A mobility
10 mode is designated when the neighbor subscriber computer device moves geographically outside of the home mode wireless communication range of the home mode wireless network broadcast device and remains within the wireless communication range of another wireless network broadcast device for a predetermined period of time. Any convenient technique may be used for connecting a neighbor subscriber device in a home mode or a mobility mode. For example,
15 mobility mode of a neighbor subscriber computer device may be established based on MAC address capture as described for example in Figure 8 and compilation of MAC addresses that are captured over two consecutive captures separated by a predetermined time period to determine MAC addresses that are associated with a secured wireless network of the system and are disconnected from the corresponding home mode secured wireless network. In another example,
20 mobility mode may be designated using geolocation tracking of neighbor subscriber computer device as may occur through communications with a GPS component. In yet another example, mobility mode may be designated through automated connection or active subscriber directed connection of the neighbor subscriber computer device with an open wireless network of a wireless network broadcast device that is geographically separated from the home mode wireless
25 broadcast network device. An automated connection to open wireless networks may be mediated by having a common name for all open wireless networks of the system that are to be used to initiate and register neighbor subscribers, so that once enabled for wireless connection the neighbor subscriber computer device can automatically connect to an open wireless network to communicate information such as a MAC address to allow administrator controlled servers to
30 determine and configure a suitable mobility mode designation and connection.

A home mode designation need not be permanent and may be updated and modified depending on any desired rule set or predetermined event including, for example, a change of a

neighbor subscriber primary geographical location accompanied by a request for changing a home mode designation sent from the neighbor subscriber computer device. In another example, the system may automatically analyze and calculate secured wireless network connection activity of a subscriber and may automatically change designation of home mode from a first secured wireless network connection to a second geographically distinct secured wireless network connection if the subscriber usage of the second secured wireless network connection is greater than the first secured wireless network connection over a threshold time period. Although home mode and mobility mode designations may be modified and updated at any given time point home mode and mobility mode designations will be mutually exclusive such that a single wireless network connection cannot be designated a home mode and a mobility mode at the same time. Home mode and mobility mode secured wireless network connections will be geographically distinct in that the respective wireless communication geographical area of the home mode connection and the mobility mode connection will not be identical, but will encompass both non-overlapping and partially overlapping ranges. Often wireless communication geographical areas of home mode and mobility mode connections will be sufficiently geographically separated to be non-overlapping, as would typically occur for example if the home mode and mobility mode connections were supported by corresponding home and mobility wireless broadcast network devices that were located at least 400 meters apart in an urban setting without range-extenders. In other occurrences, wireless communication geographical areas of home and mobility mode connections may be geographically distinct and partially overlapping as may occur for example if the corresponding home and mobility wireless broadcast network devices were located 20 meters apart in an urban setting without range-extenders. In cases of overlapping geographical communication areas of home and mobility mode connections, the home mode may optionally be prioritized. Similar prioritization may be designated between first and second mobility modes, for example based on a system analysis of subscriber mobility mode recorded history.

Outside of a home mode wireless range, a neighbor subscriber computer device may need to be maintained for a predetermined period of time within a wireless range of a wireless network broadcast device before a mobility mode secured wireless network connection is initiated. The predetermined time period may be any convenient time period to achieve a threshold probability that the neighbor subscriber computer device will remain in a mobility mode connection with a designated mobility mode secured wireless network connection for a suitable period of time. The predetermined time period may be a function of any convenient technique including, for example,

a minimum time period between capture of the same MAC address on a first MAC address capture list and a second MAC address capture list. In another example, a minimum time period may be imposed between a MAC address capture and broadcasting a network in a mobility mode. The predetermined time limit may be administrator imposed or may be modified and updated by the system based on usage patterns as desired to make efficient use of computing resources to increase occurrences of mobility mode secured wireless network connections being maintained for a suitable period of time. The predetermined time period will typically be at least 10 seconds, and may be at least 20 seconds, at least 30 seconds, at least 1 minute, at least 2 minutes, or any other minimum time period as suited to a particular implementation.

Algorithms may be established for resolving potential conflicts between multiple wireless network broadcast device communications with a neighbor subscriber computer device when outside of a home mode and potentially in a mobility mode. For example, a neighbor subscriber computer device connected to a first mobility mode secured wireless network connection may require a system check and confirmation of disconnection of the neighbor subscriber computer device from the first mobility mode secured wireless network connection before establishing a connection to a potential second mobility mode wireless network connection. Typically, the system will be configured so that an end-user device only connects to a single secured wireless network over a minimum time period, such as 5 minutes, 10 minutes, 20 minutes, 30 minutes, 40 minutes, 50 minutes, 60 minutes or any other suitable minimum time period, and does not frequently flip back and forth between secured wireless network connections. Information relating to neighbor subscriber connections in home and mobility mode may be recorded and analyzed by automated algorithms to establish groupings of mobility mode secured wireless network connections associated with a neighbor subscriber identifier to enhance efficiency of mobility mode connections.

Home mode and mobility mode connections within each wireless network broadcast device may be distinguished based on categories of internal/private IP address. For example, a first range of private IP addresses may be reserved for home mode networks and sub-networks, while a second range of private IP addresses may be reserved for mobility mode networks and sub-networks.

The system described herein and each variant, modification or combination thereof may also be implemented as a method or as computer programmable code on a non-transitory computer readable medium (i.e. a substrate). The computer readable medium is a data storage

device that can store data, which can thereafter, be read by a computer system. Examples of a computer readable medium include read-only memory, random-access memory, CD-ROMs, magnetic tape, optical data storage devices and the like. The computer readable medium may be geographically localized or may be distributed over a network coupled computer system so that the computer readable code is stored and executed in a distributed fashion. Therefore, a non-transitory computer readable medium encompasses a single computer readable medium or a plurality of computer readable media cooperatively combining to implement a method or a system described herein. Furthermore, when a system or method is implemented with a plurality of computer readable media, the computer readable media may be distributed and installed on a plurality of devices, for example including a first computer readable medium installed on a wireless network broadcast device and a second computer readable medium installed on a remote server communicative with the wireless network broadcast device.

Embodiments described herein are intended for illustrative purposes without any intended loss of generality. Still further variants, modifications and combinations thereof are contemplated and will be recognized by the person of skill in the art. Accordingly, the foregoing detailed description is not intended to limit scope, applicability, or configuration of claimed subject matter.

WHAT IS CLAIMED IS:

1. A system for providing a plurality of secured wireless network connections over a shared Internet access point, the system comprising:

a first wireless network broadcast device supporting a first wireless communication range
5 and a second wireless network broadcast device supporting a second wireless communication range, the first and second wireless communication ranges being geographically distinct;

the first wireless network broadcast device connected to a first Internet access point and the second wireless network broadcast devices connected to a second Internet access point;

each of the first and second wireless network broadcast devices comprising a wireless
10 adapter to establish a plurality of secured wireless local area networks (WLANs) and an open unsecured WLAN directed to a web page hosted on a remote server and providing information relating to the plurality of secured WLANs and prompts to allow a subscriber to purchase one of the plurality of secured WLANs, and a processor programmed to execute network security rules to isolate network communications data of each of the plurality of secured WLANs from all other
15 network communications data passing through the wireless adapter;

a first plurality of subscribers, each of the first plurality of subscribers having purchased access to one of the plurality of the secured WLANs of the first wireless network broadcast device and having a computing device configured for password protected wireless connection to one of the plurality of secured WLANs;

20 a second plurality of subscribers, each of the second plurality of subscribers having purchased access to one of the plurality of the secured WLANs of the second wireless network broadcast device and having a computing device configured for password protected wireless connection to one of the plurality of secured WLANs;

the computing device of at least one of the second plurality of subscribers automatically
25 connected to one of the plurality of secured WLANs of the first wireless network broadcast device when the computing device of the at least one of the second plurality of subscribers is inside the first wireless communication range of the first wireless network broadcast device and outside the second wireless communication range of the second wireless network broadcast device.

30 2. The system of claim 1, wherein the one of the plurality of secured WLANs of the first wireless network broadcast device and the one of the plurality of secured WLANs of the second wireless

network broadcast device are accessed by the computing device of the at least one of the second plurality of subscribers using the same network name and password.

3. The system of claim 2, wherein the one of the plurality of secured WLANs of the first network broadcast device and the one of the plurality of secured WLANs of the second broadcast device
5 are assigned different private IP addresses.

4. The system of any one of claims 1 to 3, wherein the first Internet access point is a first router connecting to an upstream Internet service provider (ISP) and the second Internet access point is a second router connecting to an upstream ISP.

5. The system of any one of claims 1 to 4, wherein the networks security rules isolate network
10 communication data of each of the plurality of secured WLANs from all other network communications data passing through the first or second Internet access points.

6. The system of any one of claims 1 to 5, wherein the network security rules provide a firewall.

7. The system of any one of claims 1 to 6, wherein the network security rules provide a VPN protocol.

15 8. The system of any one of claims 1 to 7, wherein the first and second wireless network broadcast devices are configured to track subscriber usage and record subscriber usage statistics in a memory.

9. The system of claim 8, wherein subscriber usage statistics recorded in the memory of the first and second wireless network broadcast devices are independently communicated at a
20 predetermined time interval to the remote server configured to maintain subscriber usage records.

10. The system of claim 8, wherein subscriber usage is tracked by analyzing header information of data packets sent and received by the first and second wireless network broadcast devices.

11. A method for providing a plurality of secured wireless network connections over a shared Internet access point, the method comprising:

25 connecting a first wireless network broadcast device supporting a first wireless communication range to a first Internet access point;

connecting a second wireless network broadcast device supporting a second wireless communication range to a second Internet access point, the first and second wireless communication ranges being geographically distinct;

30 from each of the first and second wireless network broadcast devices broadcasting a plurality of secured WLANs and an open unsecured WLAN directed to a web page hosted on a

remote server and providing information relating to the plurality of secured WLANs and prompts to allow a subscriber to purchase one of the plurality of secured WLANs;

providing network security rules to isolate network communications data of each of the plurality of secured WLANs from all other network communications data passing through the first and second wireless network broadcast devices;

connecting a first plurality of subscribers to the plurality of secured WLANs of the first wireless network broadcast device, respectively, each of the first plurality of subscribers having a computing device configured for password protected wireless connection to one of the plurality of secured WLANs of the first wireless network broadcast device;

connecting a second plurality of subscribers to the plurality of secured WLANs of the second wireless network broadcast device, respectively, each of the second plurality of subscribers having a computing device configured for password protected wireless connection to one of the plurality of secured WLANs of the second wireless network broadcast device;

automatically connecting the computing device of at least one of the second plurality of subscribers to one of the plurality of secured WLANs of the first wireless network broadcast device when the computing device of the at least one of the second plurality of subscribers is inside the first wireless communication range of the first wireless network broadcast device and outside the second wireless communication range of the second wireless network broadcast device.

12. The method of claim 11, wherein the computing device of the at least one of the second plurality of subscribers uses the same network name and password when connecting to the one of the plurality of secured WLANs of the first wireless network broadcast device and when connecting to the one of the plurality of secured WLANs of the second wireless network broadcast device.

13. The method of claim 12, further comprising assigning different private IP addresses to the one of the plurality of secured WLANs of the first network broadcast device and the one of the plurality of secured WLANs of the second broadcast device.

14. The method of any one of claims 11 to 13, wherein the first Internet access point is a first router connecting to an upstream Internet service provider (ISP) and the second Internet access point is a second router connecting to an upstream ISP.

15. The method of any one of claims 11 to 14, wherein the networks security rules isolate network communication data of each of the plurality of secured WLANs from all other network communications data passing through the first or second Internet access points.

16. The method of any one of claims 11 to 15, wherein the network security rules provide a
5 firewall.

17. The method of any one of claims 11 to 16, wherein the network security rules provide a VPN protocol.

18. The method of any one of claims 11 to 17, further comprising configuring the first and second wireless network broadcast devices to track subscriber usage and record subscriber usage
10 statistics in a memory.

19. The method of claim 18, wherein subscriber usage statistics recorded in the memory of the first and second wireless network broadcast devices are independently communicated at a predetermined time interval to the remote server configured to maintain subscriber usage records.

20. The method of claim 18, wherein subscriber usage is tracked by analyzing header information
15 of data packets sent and received by the first and second wireless network broadcast devices.

21. A computer readable medium embodying a computer program for providing a plurality of secured wireless network connections over a shared Internet access point, the computer readable medium comprising:

computer readable code for connecting a first wireless network broadcast device
20 supporting a first wireless communication range to a first Internet access point;

computer readable code for connecting a second wireless network broadcast device supporting a second wireless communication range to a second Internet access point, the first and second wireless communication ranges being geographically distinct;

computer readable code for broadcasting, from each of the first and second wireless
25 network broadcast devices, a plurality of secured WLANs and an open unsecured WLAN directed to a web page hosted on a remote server and providing information relating to the plurality of secured WLANs and prompts to allow a subscriber to purchase one of the plurality of secured WLANs;

computer readable code for providing network security rules to isolate network
30 communications data of each of the plurality of secured WLANs from all other network communications data passing through the first and second wireless network broadcast devices;

computer readable code for respectively connecting a first plurality of subscribers to the plurality of secured WLANs of the first wireless network broadcast device, each of the first plurality of subscribers having a computing device configured for password protected wireless connection to one of the plurality of secured WLANs of the first wireless network broadcast
5 device;

computer readable code for respectively connecting a second plurality of subscribers to the plurality of secured WLANs of the second wireless network broadcast device, each of the second plurality of subscribers having a computing device configured for password protected wireless connection to one of the plurality of secured WLANs of the second wireless network
10 broadcast device;

computer readable code for automatically connecting the computing device of at least one of the second plurality of subscribers to one of the plurality of secured WLANs of the first wireless network broadcast device when the computing device of the at least one of the second plurality of subscribers is inside the first wireless communication range of the first wireless
15 network broadcast device and outside the second wireless communication range of the second wireless network broadcast device.

22. The computer readable medium of claim 21, wherein the computing device of the at least one of the second plurality of subscribers uses the same network name and password when connecting to the one of the plurality of secured WLANs of the first wireless network broadcast device and
20 when connecting to the one of the plurality of secured WLANs of the second wireless network broadcast device.

23. The computer readable medium of claim 22, further comprising computer readable code for assigning different private IP addresses to the one of the plurality of secured WLANs of the first network broadcast device and the one of the plurality of secured WLANs of the second broadcast
25 device.

24. The computer readable medium of any one of claims 21 to 23, wherein the first Internet access point is a first router connecting to an upstream Internet service provider (ISP) and the second Internet access point is a second router connecting to an upstream ISP.

25. The computer readable medium of any one of claims 21 to 24, wherein the networks security
30 rules isolate network communication data of each of the plurality of secured WLANs from all other network communications data passing through the first or second Internet access points.

26. The computer readable medium of any one of claims 21 to 25, wherein the network security rules provide a firewall.

27. The computer readable medium of any one of claims 21 to 26, wherein the network security rules provide a VPN protocol.

5 28. The computer readable medium of any one of claims 21 to 27, further comprising computer readable code for configuring the first and second wireless network broadcast devices to track subscriber usage and record subscriber usage statistics in a memory.

29. The computer readable medium of claim 28, wherein subscriber usage statistics recorded in the memory of the first and second wireless network broadcast devices are independently
10 communicated at a predetermined time interval to the remote server configured to maintain subscriber usage records.

30. The computer readable medium of claim 28, wherein subscriber usage is tracked by analyzing header information of data packets sent and received by the first and second wireless network broadcast devices.

15 31. A system for adding a secured wireless network connection for a subscriber in a mobility mode, the system comprising:

a first wireless network broadcast device configured to broadcast an open unsecured wireless network connection, to broadcast a home mode secured wireless network connection uniquely accessible by a first subscriber in a home mode, and to broadcast a mobility mode
20 secured wireless network connection uniquely accessible by a second subscriber in a mobility mode, the home mode designated when the first subscriber initially establishes the home mode secured wireless network connection with the first wireless network broadcast device in a first wireless communication range and remains geographically within the first wireless communication range of the first wireless network broadcast device, a mobility mode designated
25 when the second subscriber initially establishes a home mode secured wireless network connection with a second wireless network broadcast device in a second wireless communication range and moves geographically outside of the second wireless communication range of the second wireless network broadcast device and remains within the first wireless communication range of the first wireless network broadcast device;

30 a remote server communicative with the first wireless network broadcast device through an Internet access point, the remote server configured to receive information from the first wireless network broadcast device relating to the second subscriber, accessing a stored record of

the second subscriber to designate the second subscriber in the mobility mode, and sending a communication to the first wireless network broadcasting device to add the mobility mode secured wireless network connection uniquely accessible by the second subscriber in the mobility mode.

5 32. The system of claim 31, wherein a service set identifier (SSID) and a password of the mobility mode wireless network connection of the second subscriber with the first wireless network device is the same as the SSID and password of the home mode secured wireless network connection of the second subscriber with the second wireless network broadcast device.

10 33. The system of claim 31 or 32, wherein a private IP address assigned by the first wireless network device to the mobility mode wireless network connection of the second subscriber with the first wireless network device is different than a private IP address assigned by the first wireless network broadcast device to the home mode secured wireless network connection of the first subscriber with the first wireless network broadcast device.

15 34. The system of claim 33, wherein the private IP address assigned by the first wireless network device to the mobility mode wireless network connection of the second subscriber with the first wireless network device is different than the private IP address assigned by the second wireless network broadcast device to the home mode secured wireless network connection of the second subscriber with the second wireless network broadcast device.

20 35. The system of any one of claims 31 to 34, wherein the mobility mode is designated when the second subscriber remains within the first wireless communication range of the first wireless network broadcast device for a predetermined time of at least 10 seconds.

25 36. The system of any one of claims 31 to 35, further comprising a remote memory, the remote memory communicative with the remote server, the remote memory storing records of the first and second subscribers, each record comprising a unique identifier and a network usage statistic, the network usage statistic calculated based on time, data or both time and data in home mode and mobility mode.

37. The system of claim 36, wherein the unique identifier is a plurality of unique identifiers including at least one unique identifier established internally within the system and at least one unique identifier that is an industry standard.

30 38. The system of claim 37, wherein the at least one unique identifier that is an industry standard is a media access control (MAC) address of a subscriber device.

39. The system of any one of claims 31 to 35, wherein the information from the first wireless network broadcast device relating to the second subscriber includes a unique identifier of the second subscriber and the remote server determines whether the unique identifier is associated with a previously established secured wireless network connection within the system.

5 40. The system of claim 39, wherein the unique identifier is a MAC address, and the first wireless network broadcast device is configured to automatically capture and decode a MAC address transmission within the first wireless wireless communication range and to send the MAC address to the remote server.

10 41. A method for adding a secured wireless network connection for a subscriber in a mobility mode, the method comprising:

broadcasting, using a first wireless network broadcast device, an open unsecured wireless network connection, a home mode secured wireless network connection uniquely accessible by a first subscriber in a home mode, and a mobility mode secured wireless network connection uniquely accessible by a second subscriber in a mobility mode, the home mode designated when
15 the first subscriber initially establishes the home mode secured wireless network connection with the first wireless network broadcast device in a first wireless communication range and remains geographically within the first wireless communication range of the first wireless network broadcast device, a mobility mode designated when the second subscriber initially establishes a home mode secured wireless network connection with a second wireless network broadcast
20 device in a second wireless communication range and moves geographically outside of the second wireless communication range of the second wireless network broadcast device and remains within the first wireless communication range of the first wireless network broadcast device;

communicating information relating to the second subscriber from the first wireless network broadcast device to a remote server through an Internet access point,

25 the remote server accessing a stored record of the second subscriber to designate the second subscriber in the mobility mode, and

sending a communication from the remote server to the first wireless network broadcasting device to add the mobility mode secured wireless network connection uniquely accessible by the second subscriber in the mobility mode.

30 42. The method of claim 41, wherein a service set identifier (SSID) and a password of the mobility mode wireless network connection of the second subscriber with the first wireless

network device is the same as the SSID and password of the home mode secured wireless network connection of the second subscriber with the second wireless network broadcast device.

43. The method of claim 41 or 42, further comprising assigning a private IP address selected from a first predetermined range of IP addresses to the mobility mode wireless network connection of the second subscriber with the first wireless network device and assigning a private IP address selected from a second predetermined range of IP addresses to the home mode secured wireless network connection of the first subscriber with the first wireless network broadcast device.

44. The method of claim 43, further comprising assigning a private IP address selected from the first predetermined range of IP addresses to the mobility mode wireless network connection of the second subscriber with the first wireless network device and assigning a private IP address selected from the second predetermined range of IP addresses to the home mode secured wireless network connection of the second subscriber with the second wireless network broadcast device.

45. The method of any one of claims 41 to 44, wherein the mobility mode is designated when the second subscriber remains within the first wireless communication range of the first wireless network broadcast device for a predetermined time of at least 10 seconds.

46. The method of any one of claims 41 to 45, further comprising storing records of the first and second subscribers in a remote memory, each record comprising a unique identifier and a network usage statistic, the network usage statistic calculated based on time, data or both time and data in home mode and mobility mode.

47. The method of claim 46, wherein the unique identifier is a plurality of unique identifiers including at least one unique identifier established internally within the system and at least one unique identifier that is an industry standard.

48. The method of claim 47, wherein the at least one unique identifier that is an industry standard is a media access control (MAC) address of a subscriber device.

49. The method of any one of claims 41 to 45, further comprising determining whether a unique identifier of the second subscriber is associated with a previously established secured wireless network connection, wherein the information relating to the second subscriber from the first wireless network broadcast device includes the unique identifier of the second subscriber.

50. The method of claim 49, further comprising automatically capturing and decoding a MAC address transmission within the first wireless communication range and sending the MAC address to the remote server, wherein MAC address is the unique identifier of the second subscriber.

51. A computer readable medium embodying a computer program for adding a secured wireless network connection for a subscriber in a mobility mode, the computer readable medium comprising:

computer readable code for broadcasting, using a first wireless network broadcast device,
5 an open unsecured wireless network connection, a home mode secured wireless network connection uniquely accessible by a first subscriber in a home mode, and a mobility mode secured wireless network connection uniquely accessible by a second subscriber in a mobility mode, the home mode designated when the first subscriber initially establishes the home mode secured wireless network connection with the first wireless network broadcast device in a first wireless
10 communication range and remains geographically within the first wireless communication range of the first wireless network broadcast device, a mobility mode designated when the second subscriber initially establishes a home mode secured wireless network connection with a second wireless network broadcast device in a second wireless communication range and moves geographically outside of the second wireless communication range of the second wireless
15 network broadcast device and remains within the first wireless communication range of the first wireless network broadcast device;

computer readable code for communicating information relating to the second subscriber from the first wireless network broadcast device to a remote server through an Internet access point,

20 computer readable code for the remote server accessing a stored record of the second subscriber to designate the second subscriber in the mobility mode, and

computer readable code for sending a communication from the remote server to the first wireless network broadcasting device to add the mobility mode secured wireless network connection uniquely accessible by the second subscriber in the mobility mode.

25 52. The computer readable medium of claim 51, wherein a service set identifier (SSID) and a password of the mobility mode wireless network connection of the second subscriber with the first wireless network device is the same as the SSID and password of the home mode secured wireless network connection of the second subscriber with the second wireless network broadcast device.

30 53. The computer readable medium of claim 51 or 52, further comprising computer readable code for assigning a private IP address selected from a first predetermined range of IP addresses to the mobility mode wireless network connection of the second subscriber with the first wireless

network device and computer readable code for assigning a private IP address selected from a second predetermined range of IP addresses to the home mode secured wireless network connection of the first subscriber with the first wireless network broadcast device.

54. The computer readable medium of claim 53, further comprising computer readable code for
5 assigning a private IP address selected from the first predetermined range of IP addresses to the mobility mode wireless network connection of the second subscriber with the first wireless network device and computer readable code for assigning a private IP address selected from the second predetermined range of IP addresses to the home mode secured wireless network connection of the second subscriber with the second wireless network broadcast device.

10 55. The computer readable medium of any one of claims 51 to 54, wherein the mobility mode is designated when the second subscriber remains within the first wireless communication range of the first wireless network broadcast device for a predetermined time of at least 10 seconds.

56. The computer readable medium of any one of claims 51 to 55, further comprising computer readable code for storing records of the first and second subscribers in a remote memory, each
15 record comprising a unique identifier and a network usage statistic, the network usage statistic calculated based on time, data or both time and data in home mode and mobility mode.

57. The computer readable medium of claim 56, wherein the unique identifier is a plurality of unique identifiers including at least one unique identifier established internally within the system and at least one unique identifier that is an industry standard.

20 58. The computer readable medium of claim 57, wherein the at least one unique identifier that is an industry standard is a media access control (MAC) address of a subscriber device.

59. The computer readable medium of any one of claims 51 to 55, further comprising computer readable code for determining whether a unique identifier of the second subscriber is associated with a previously established secured wireless network connection, wherein the information
25 relating to the second subscriber from the first wireless network broadcast device includes the unique identifier of the second subscriber.

60. The computer readable medium of claim 59, further comprising automatically capturing and decoding a MAC address transmission within the first wireless communication range and sending the MAC address to the remote server, wherein the MAC address is the unique identifier of the
30 second subscriber.

61. A system for providing a plurality of secured wireless network connections over a shared Internet access point, the system comprising:

a plurality of providers, each of the plurality of providers controlling an Internet access point and a wireless network broadcast device connected to the Internet access point;

the wireless network broadcast device comprising a wireless adapter to establish a plurality of secured WLANs and an open unsecured WLAN directed to a web page hosted on a remote server and providing information relating to connection speed of the plurality of secured WLANs and prompts to allow a subscriber to purchase and configure one of the plurality of secured WLANs, and a processor programmed to execute network security rules to isolate network communications data of each of the plurality of secured WLANs from all other network communications data passing through the wireless adapter;

a plurality of subscribers, each of the plurality of subscribers having purchased access to one of the plurality of the secured WLANs and having a computing device configured for wireless connection to one of the plurality of secured WLANs.

62. The system of claim 61, wherein the Internet access point is a router connecting to an upstream Internet service provider.

63. The system of claim 62, wherein the wireless network broadcast device is connected to the router with a wired connection.

64. The system of claim 62, wherein the wireless network broadcast device is connected to the router with a wireless connection.

65. The system of any one of claims 61 to 64, wherein the wireless adapter is configured to an 802.11 communication standard.

66. The system of any one of claims 61 to 65, wherein the networks security rules isolate network communication data of each of the plurality of secured WLANs from all other network communications data passing through the Internet access point.

67. The system of any one of claims 61 to 66, wherein the network security rules provide a firewall.

68. The system of any one of claims 61 to 66, wherein the network security rules provide a sandbox.

69. The system of any one of claims 61 to 66, wherein the network security rules provide a jail.

70. The system of any one of claims 61 to 66, wherein the network security rules provide a VPN protocol.

71. The system of claim 70, wherein the VPN protocol is L2TP, PPTP or SSTP.

72. The system of any one of claims 61 to 71, wherein a unique web page is hosted for each of the plurality of providers.

73. The system of any one of claims 61 to 72, wherein the wireless network broadcast device is configured to track subscriber usage and record subscriber usage statistics in a memory.

5 74. The system of claim 73, wherein subscriber usage statistics recorded in the memory of the wireless network broadcast device are communicated at a predetermined time interval to a remote server configured to maintain subscriber usage records linked to a corresponding provider's account.

10 75. The system of claim 73, wherein subscriber usage is tracked by analyzing header information of data packets sent and received by the wireless network broadcast device.

76. A method for providing a plurality of secured wireless network connections over a shared Internet access point, the method comprising:

connecting a plurality of wireless network broadcast devices to a plurality of Internet access points, respectively;

15 broadcasting a plurality of secured WLANs from each device of the plurality of wireless network broadcast devices;

broadcasting an open unsecured WLAN from each device of the plurality of wireless network broadcast devices, the open unsecured WLAN directed to a web page hosted on a remote server;

20 providing information on the web page, the information relating to a connection speed of the plurality of secured WLANs and providing prompt on the web page to allow purchase and configuration of one of the plurality of secured WLANs;

25 providing network security rules to isolate network communications data of each of the plurality of secured WLANs from all other network communications data passing through the wireless adapter;

connecting a plurality of subscribers to the plurality of secured WLANs, respectively, each of the plurality of subscribers having purchased access to one of the plurality of the secured WLANs and having a computing device configured for password protected wireless connection to one of the plurality of secured WLANs.

30 77. The method of claim 76, wherein each of the plurality of Internet access points is a router connecting to an upstream Internet service provider.

78. The method of claim 77, further comprising connecting the wireless network broadcast device to the router with a wired connection.

79. The method of claim 77, further comprising connecting the wireless network broadcast device to the router with a wireless connection.

5 80. The method of any one of claims 76 to 79, wherein the wireless adapter is configured to an 802.11 communication standard.

81. The method of any one of claims 76 to 80, wherein the network security rules isolate network communication data of each of the plurality of secured WLANs from all other network communications data passing through each of the plurality of Internet access points.

10 82. The method of any one of claims 76 to 81, wherein the network security rules provide a firewall.

83. The method of any one of claims 76 to 81, wherein the network security rules provide a sandbox.

84. The method of any one of claims 76 to 81, wherein the network security rules provide a jail.

15 85. The method of any one of claims 76 to 81, wherein the network security rules provide a VPN protocol.

86. The method of claim 85, wherein the VPN protocol is L2TP, PPTP or SSTP.

87. The method of any one of claims 76 to 86, wherein each open unsecured WLAN is directed to a unique web page.

20 88. The method of any one of claims 76 to 87, further comprising tracking subscriber usage and recording subscriber usage statistics in a memory of each wireless network broadcast device.

89. The method of claim 88, further comprising sending usage statistics recorded in the memory of the wireless network broadcast device, at a predetermined time interval, to a remote server configured to maintain subscriber usage records.

25 90. The method of claim 88, wherein subscriber usage is tracked by analyzing header information of data packets sent and received by the wireless network broadcast device.

91. A computer readable medium embodying a computer program for providing a plurality of secured wireless network connections over a shared Internet access point, the computer readable medium comprising:

30 computer readable code for connecting a plurality of wireless network broadcast devices to a plurality of Internet access points, respectively;

computer readable code for broadcasting a plurality of secured WLANs from each device of the plurality of wireless network broadcast devices;

computer readable code for broadcasting an open unsecured WLAN from each device of the plurality of wireless network broadcast devices, the open unsecured WLAN directed to a web page hosted on a remote server;

computer readable code for providing information on the web page, the information relating to a connection speed of the plurality of secured WLANs and providing prompts on the web page to allow purchase and configuration of one of the plurality of secured WLANs;

computer readable code for providing network security rules to isolate network communications data of each of the plurality of secured WLANs from all other network communications data passing through the wireless adapter;

computer readable code for connecting a plurality of subscribers to the plurality of secured WLANs, respectively, each of the plurality of subscribers having purchased access to one of the plurality of the secured WLANs and having a computing device configured for password protected wireless connection to one of the plurality of secured WLANs.

92. The computer readable medium of claim 91, wherein each of the plurality of Internet access points is a router connecting to an upstream Internet service provider.

93. The computer readable medium of claim 92, further comprising computer readable code for connecting the wireless network broadcast device to the router with a wired connection.

94. The computer readable medium of claim 92, further comprising computer readable code for connecting the wireless network broadcast device to the router with a wireless connection.

95. The computer readable medium of any one of claims 91 to 94, wherein the wireless adapter is configured to an 802.11 communication standard.

96. The computer readable medium of any one of claims 91 to 95, wherein the network security rules isolate network communication data of each of the plurality of secured WLANs from all other network communications data passing through each of the plurality of Internet access points.

97. The computer readable medium of any one of claims 91 to 96, wherein the network security rules provide a firewall.

98. The computer readable medium of any one of claims 91 to 96, wherein the network security rules provide a sandbox.

99. The computer readable medium of any one of claims 91 to 96, wherein the network security rules provide a jail.

100. The computer readable medium of any one of claims 91 to 96, wherein the network security rules provide a VPN protocol.

5 101. The computer readable medium of claim 100, wherein the VPN protocol is L2TP, PPTP or SSTP.

102. The computer readable medium of any one of claims 91 to 101, wherein each open unsecured WLAN is directed to a unique web page.

10 103. The computer readable medium of any one of claims 91 to 102, further comprising computer readable code for tracking subscriber usage and recording subscriber usage statistics in a memory of each wireless network broadcast device.

104. The computer readable medium of claim 103, further comprising computer readable code for sending usage statistics recorded in the memory of the wireless network broadcast device, at a predetermined time interval, to a remote server configured to maintain subscriber usage records.

15 105. The computer readable medium of claim 103, wherein subscriber usage is tracked by analyzing header information of data packets sent and received by the wireless network broadcast device.

106. A system for adding a secured wireless network connection to a wireless network broadcasting device, the system comprising:

20 a wireless network broadcast device configured to broadcast a first open unsecured wireless network connection and to broadcast a first secured wireless network connection uniquely accessible by a first subscriber, the open unsecured wireless network connection directed to a unique first web page providing information relating to purchase of a second secured wireless network connection of the wireless network broadcast device;

25 a remote server communicative with the wireless network broadcast device through an Internet access point, the remote server configured to receive a communication relating to purchase of the second secured wireless network connection by a second subscriber, and sending a communication to the wireless network broadcasting device to add the second secured wireless network connection uniquely accessible by the second subscriber.

30 107. The system of claim 106, wherein the Internet access point is a router connecting to an upstream Internet service provider.

108. The system of claim 107, wherein the wireless network broadcast device is connected to the router with a wired connection.

109. The system of claim 107, wherein the wireless network broadcast device is connected to the router with a wireless connection.

5 110. The system of any one of claims 106 to 109, wherein the wireless network broadcast device is configured to an 802.11 communication standard.

111. The system of any one of claims 106 to 110, wherein the wireless network broadcast device is configured with network security rules to isolate network communication data of each of the first and second secured wireless network connections from all other network communications
10 data passing through the Internet access point.

112. The system of claim 111, wherein the network security rules provide a firewall.

113. The system of claim 111, wherein the network security rules provide a sandbox.

114. The system of claim 111, wherein the network security rules provide a jail.

115. The system of claim 111, wherein the network security rules provide a VPN protocol.

15 116. The system of claim 115, wherein the VPN protocol is L2TP, PPTP or SSTP.

117. The system of any one of claims 106 to 116, further comprising a second wireless network broadcasting device broadcasting a second open unsecured wireless network connection directed to a unique second web page, the second wireless network broadcasting device communicative with the remote server.

20 118. The system of any one of claims 106 to 116, wherein the wireless network broadcast device is configured to track subscriber usage and record subscriber usage statistics in a memory.

119. The system of claim 118, wherein subscriber usage statistics recorded in the memory of the wireless network broadcast device are communicated at a predetermined time interval to a second remote server configured to maintain subscriber usage records.

25 120. The system of claim 118, wherein subscriber usage is tracked by analyzing header information of data packets sent and received by the wireless network broadcast device.

121. A method for adding a secured wireless network connection to a wireless network broadcasting device, the method comprising:

30 broadcasting, from a wireless network broadcast device, a first open unsecured wireless network connection and a first secured wireless network connection uniquely accessible by a first subscriber, the open unsecured wireless network connection directed to a unique first web page

providing information relating to purchase of a second secured wireless network connection of the wireless network broadcast device;

receiving at a remote server communicative with the wireless network broadcast device through an Internet access point, a communication relating to purchase of the second secured
5 wireless network connection by a second subscriber; and

sending a communication from the remote server to the wireless network broadcasting device to add the second secured wireless network connection uniquely accessible by the second subscriber.

122. The method of claim 121, wherein the Internet access point is a router connecting to an
10 upstream Internet service provider.

123. The method of claim 122, further comprising connecting the wireless network broadcast device to the router with a wired connection.

124. The method of claim 122, further comprising connecting the wireless network broadcast device to the router with a wireless connection.

15 125. The method of any one of claims 121 to 124, wherein the wireless network broadcast device is configured to an 802.11 communication standard.

126. The method of any one of claims 121 to 125, further comprising providing network security rules to isolate network communication data of each of the first and second secured wireless network connections from all other network communications data passing through the Internet
20 access point.

127. The method of claim 126, wherein the network security rules provide a firewall.

128. The method of claim 126, wherein the network security rules provide a sandbox.

129. The method of claim 126, wherein the network security rules provide a jail.

130. The method of claim 126, wherein the network security rules provide a VPN protocol.

25 131. The method of claim 130, wherein the VPN protocol is L2TP, PPTP or SSTP.

132. The method of any one of claims 121 to 131, further comprising connecting a second wireless network broadcast device to the remote server through a second Internet access point, broadcasting a second open unsecured wireless network connection from the second wireless network broadcast device, and directing the second open unsecured to a unique second web page
30 hosted on the remote server.

133. The method of any one of claims 121 to 131, further comprising tracking subscriber usage and recording subscriber usage statistics in a memory of the wireless network broadcast device.

134. The method of claim 133, further comprising sending subscriber usage statistics recorded in the memory of the wireless network broadcast device, at a predetermined time interval, to a second remote server configured to maintain subscriber usage records.

135. The method of claim 133, wherein subscriber usage is tracked by analyzing header
5 information of data packets sent and received by the wireless network broadcast device.

136. A computer readable medium embodying a computer program for adding a secured wireless network connection to a wireless network broadcasting device, the computer readable medium comprising:

computer readable code for broadcasting, from a wireless network broadcast device, a first
10 open unsecured wireless network connection and a first secured wireless network connection uniquely accessible by a first subscriber, the open unsecured wireless network connection directed to a unique first web page providing information relating to purchase of a second secured wireless network connection of the wireless network broadcast device;

computer readable code for receiving at a remote server communicative with the wireless
15 network broadcast device through an Internet access point, a communication relating to purchase of the second secured wireless network connection by a second subscriber; and

computer readable code for sending a communication from the remote server to the
wireless network broadcasting device to add the second secured wireless network connection uniquely accessible by the second subscriber.

137. The computer readable medium of claim 136, wherein the Internet access point is a router
20 connecting to an upstream Internet service provider.

138. The computer readable medium of claim 137, further comprising computer readable code for connecting the wireless network broadcast device to the router with a wired connection.

139. The computer readable medium of claim 137, further comprising computer readable code for
25 connecting the wireless network broadcast device to the router with a wireless connection.

140. The computer readable medium of any one of claims 136 to 139, wherein the wireless network broadcast device is configured to an 802.11 communication standard.

141. The computer readable medium of any one of claims 136 to 140, further comprising
computer readable code for providing network security rules to isolate network communication
30 data of each of the first and second secured wireless network connections from all other network communications data passing through the Internet access point.

142. The computer readable medium of claim 141, wherein the network security rules provide a firewall.

143. The computer readable medium of claim 141, wherein the network security rules provide a sandbox.

5 144. The computer readable medium of claim 141, wherein the network security rules provide a jail.

145. The computer readable medium of claim 141, wherein the network security rules provide a VPN protocol.

10 146. The computer readable medium of claim 145, wherein the VPN protocol is L2TP, PPTP or SSTP.

147. The computer readable medium of any one of claims 136 to 146, further comprising computer readable code for connecting a second wireless network broadcast device to the remote server through a second Internet access point, broadcasting a second open unsecured wireless network connection from the second wireless network broadcast device, and directing the second
15 open unsecured to a unique second web page hosted on the remote server.

148. The computer readable medium of any one of claims 136 to 146, further comprising computer readable code for tracking subscriber usage and recording subscriber usage statistics in a memory of the wireless network broadcast device.

149. The computer readable medium of claim 148, further comprising computer readable code for
20 sending subscriber usage statistics recorded in the memory of the wireless network broadcast device, at a predetermined time interval, to a second remote server configured to maintain subscriber usage records.

150. The computer readable medium of claim 148, wherein subscriber usage is tracked by analyzing header information of data packets sent and received by the wireless network broadcast
25 device.

151. A wireless network broadcast device comprising:

a first wireless adapter to establish password protected secured wireless communications with an Internet access point;

a second wireless adapter to establish a plurality of secured WLANs and an open
30 unsecured WLAN directed to a web page hosted on a remote server and providing information relating to purchase of one of the plurality of secured WLANs; and

a processor communicative with both the first wireless adapter and the second wireless adapter, the processor programmed to execute network security rules to isolate network communications data of each of the plurality of secured WLANs from all other network communications data passing through the first wireless adapter.

5 152. The device of claim 151, wherein the Internet access point is a router connecting to an upstream Internet service provider.

153. The device of claim 152, wherein the information relating to purchase of one of the plurality of secured WLANs includes a data transmission speed of the plurality of secured WLANs, a data amount availability of the plurality of secured WLANs, or any combination thereof.

10 154. The device of claim 153, wherein the information relating to purchase of one of the plurality of secured WLANs includes a cost of purchase, a prompt to confirm a purchase, a prompt to select a network configuration, or any combination thereof.

155. The device of any one of claims 151 to 154, wherein both the first and second wireless adapters are configured to an 802.11 communication standard.

15 156. The device of any one of claims 151 to 155, wherein the network security rules isolate network communication data of each of the plurality of secured WLANs from all other network communications data passing through the Internet access point.

157. The device of any one of claims 151 to 156, wherein the network security rules provide a firewall.

20 158. The device of any one of claims 151 to 156, wherein the network security rules provide a sandbox.

159. The device of any one of claims 151 to 156, wherein the network security rules provide a jail.

25 160. The device of any one of claims 151 to 156, wherein the network security rules provide a VPN protocol.

161. The device of claim 160, wherein the VPN protocol is L2TP, PPTP or SSTP.

162. The device of any one of claims 151 to 161, wherein the unique web page is a captive portal.

163. The device of any one of claims 151 to 162, wherein the processor is configured to track usage of each of the plurality of secured WLANs and record usage statistics in a memory.

30 164. The device of claim 163, wherein usage statistics recorded in the memory of the wireless network broadcast device are communicated at a predetermined time interval to a remote server configured to maintain usage records.

FIGURE 1

1/9

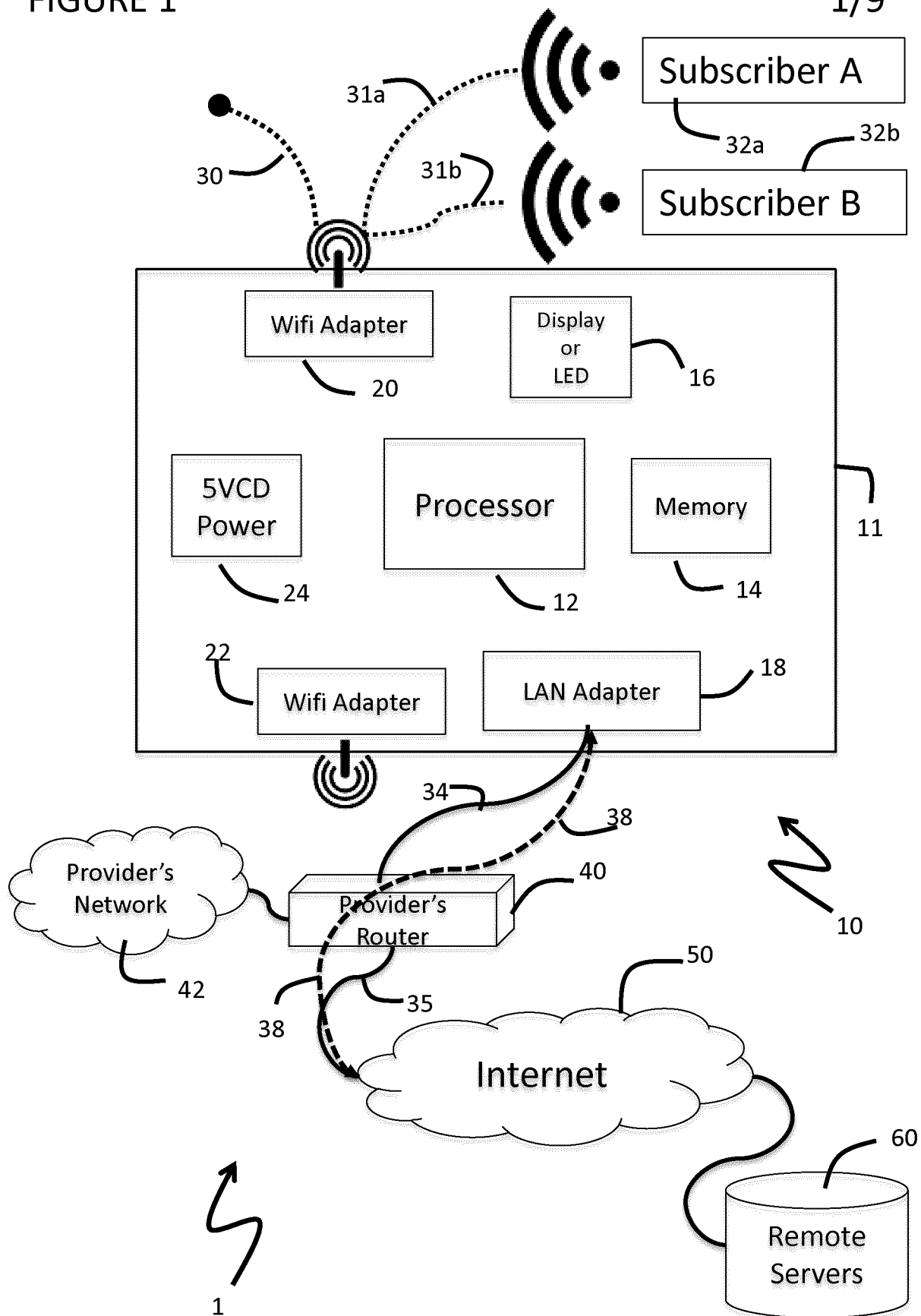


FIGURE 2

2/9

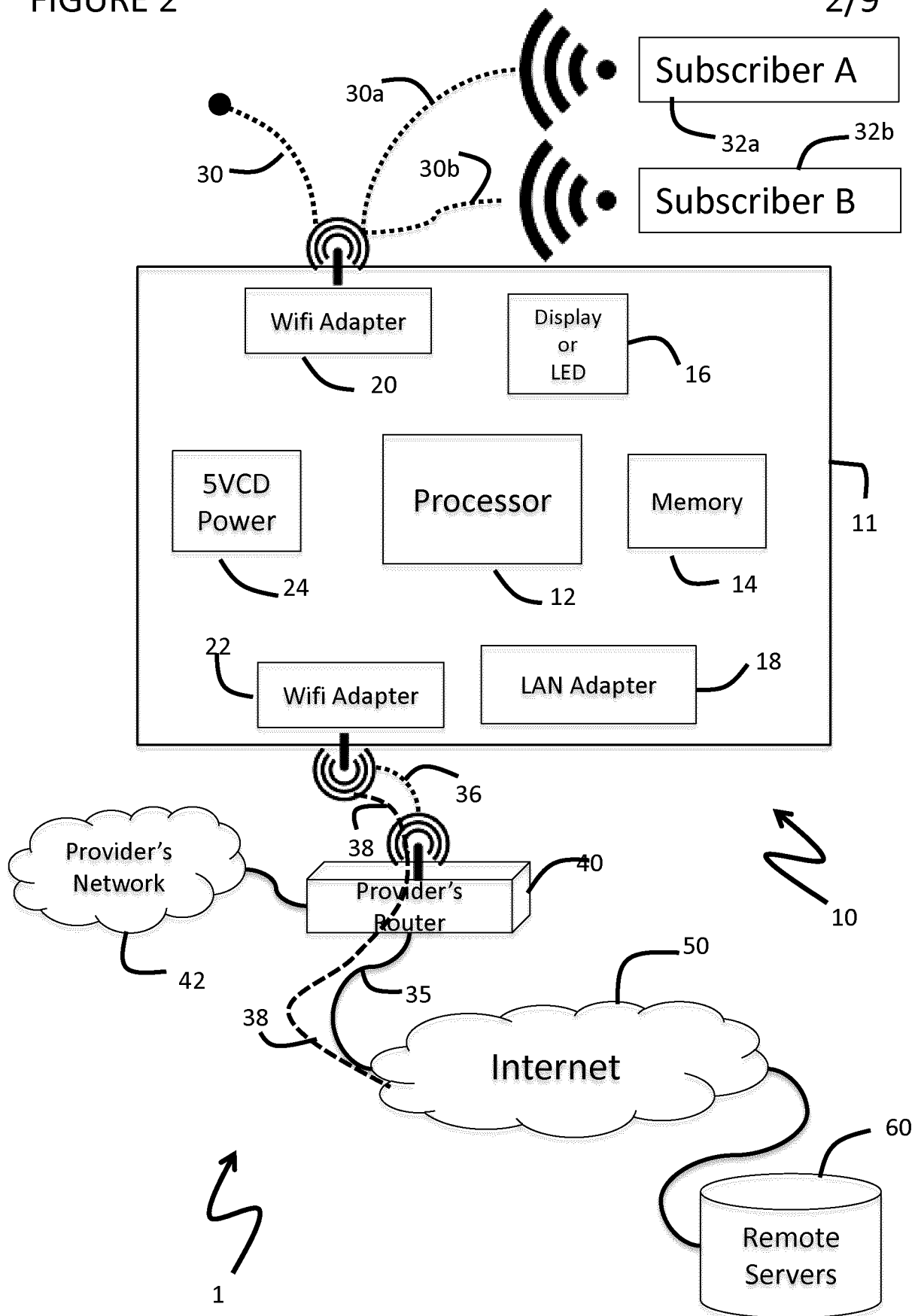


FIGURE 3

3/9

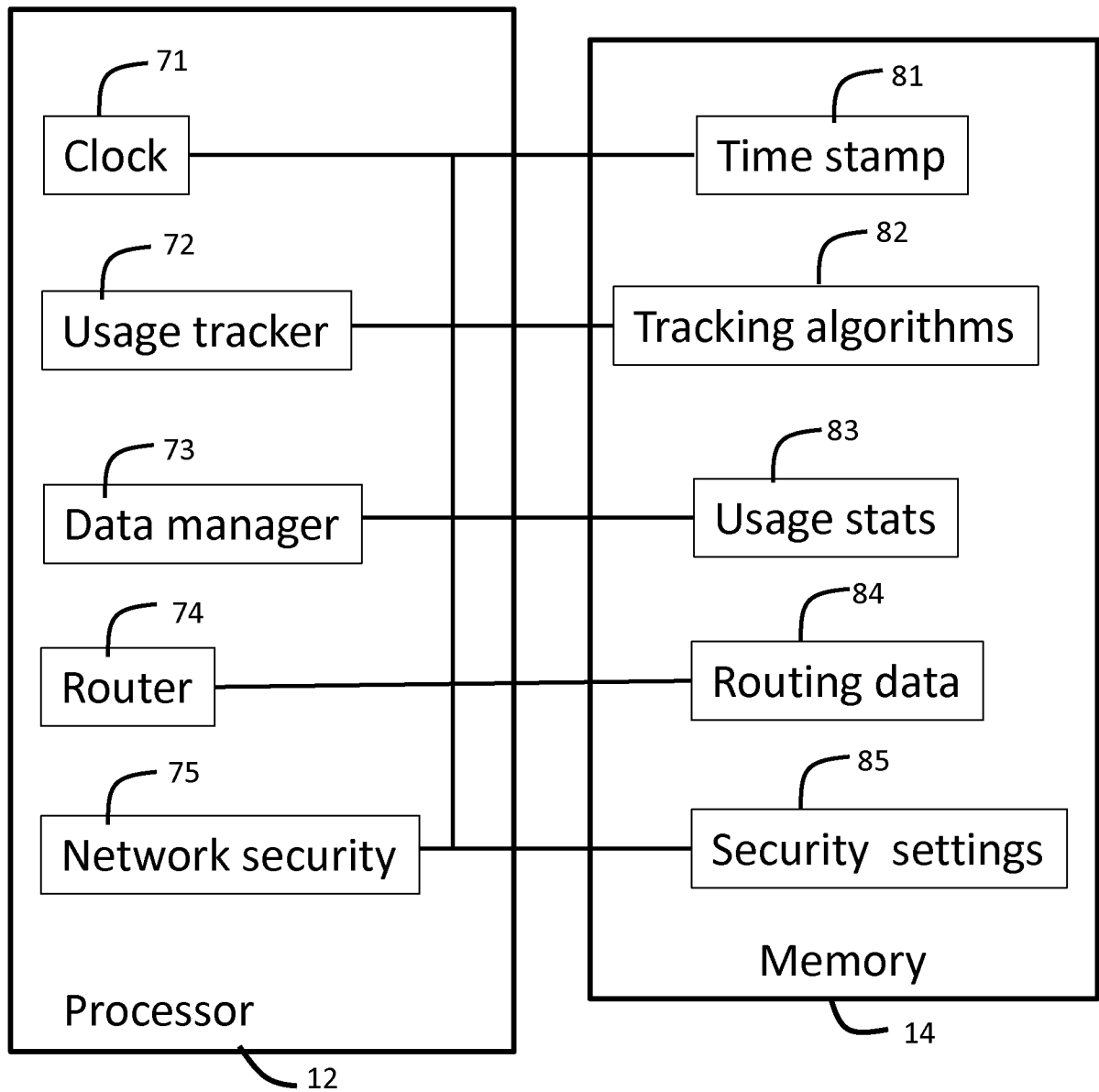


FIGURE 4

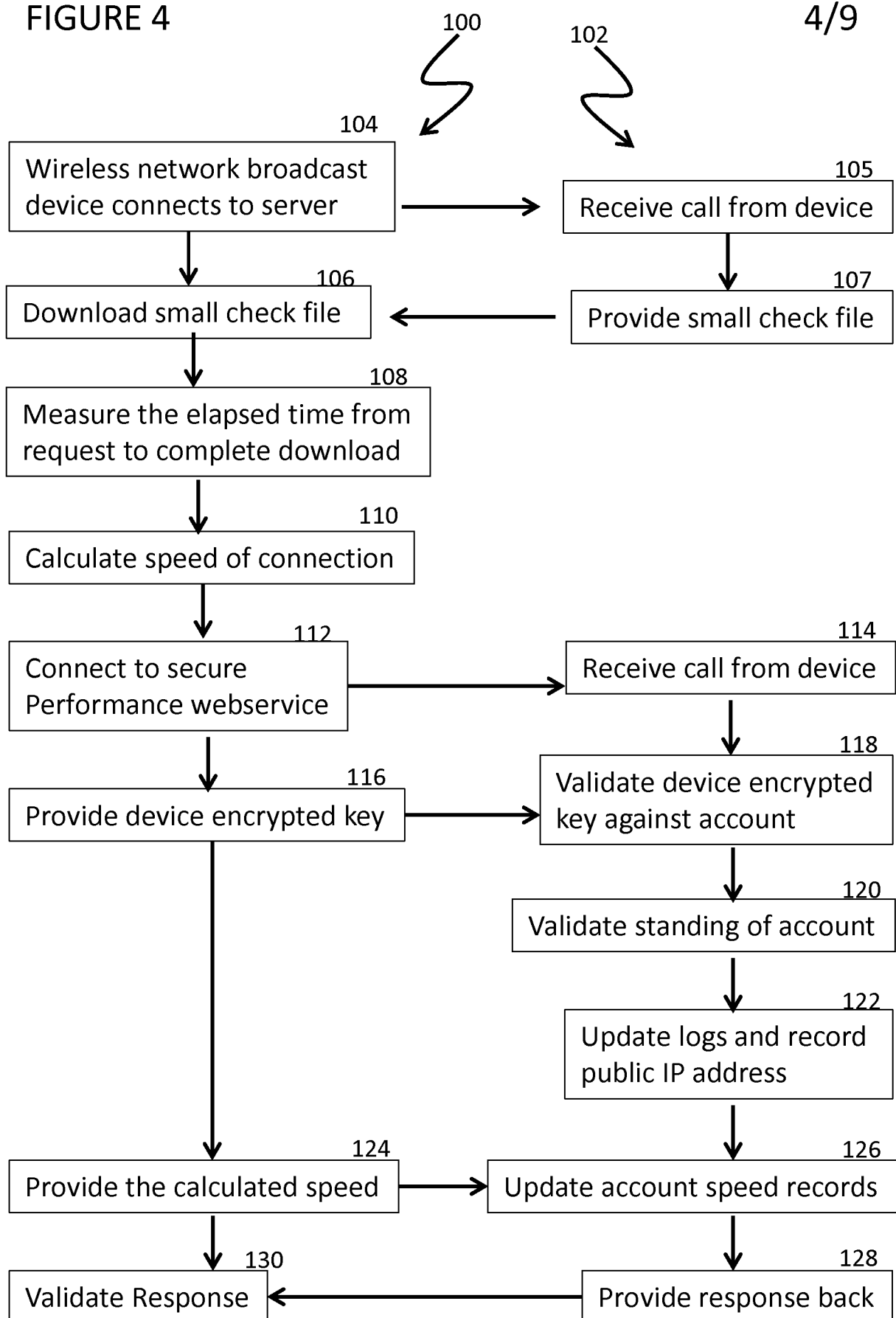


FIGURE 5

5/9

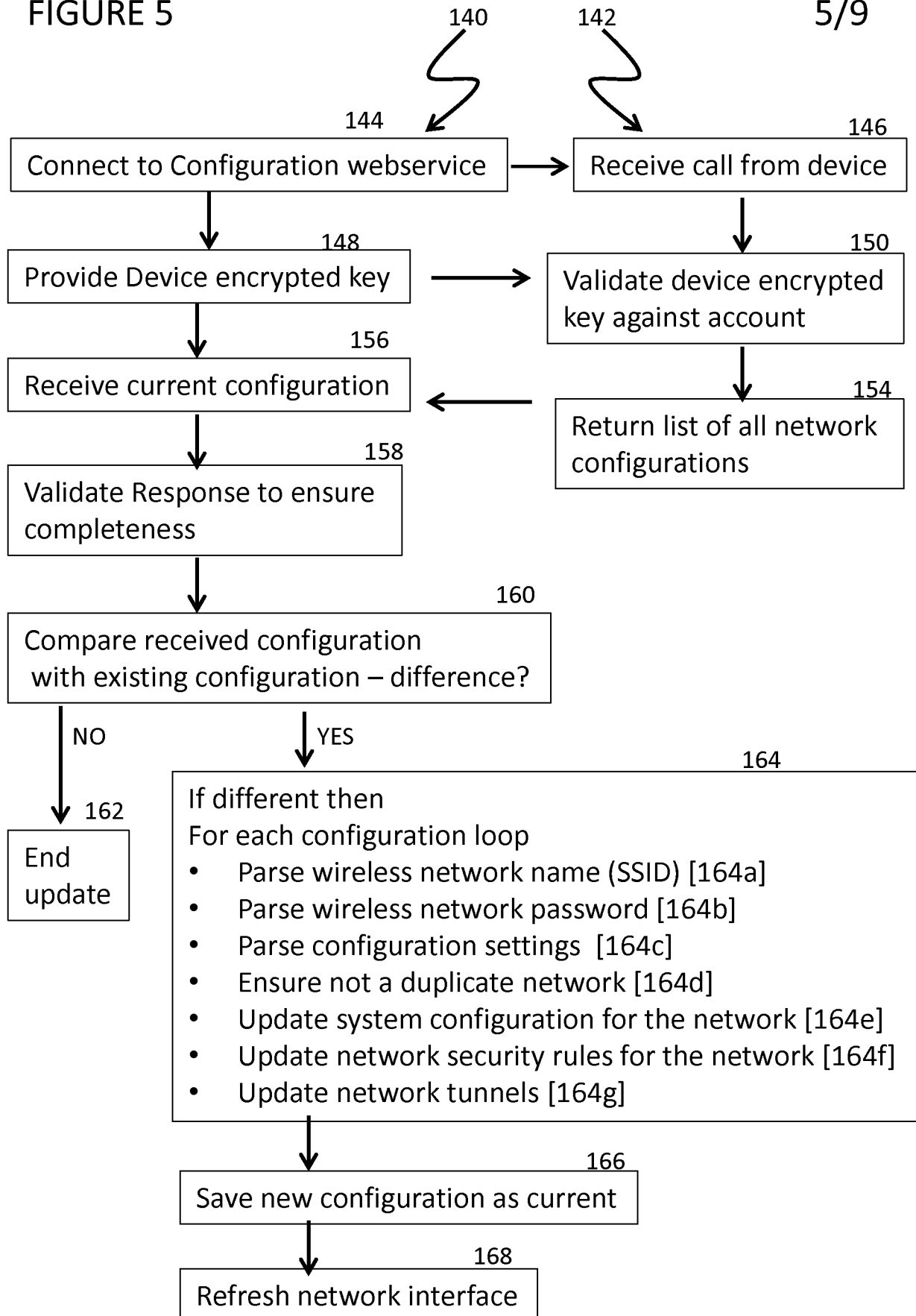


FIGURE 6

6/9

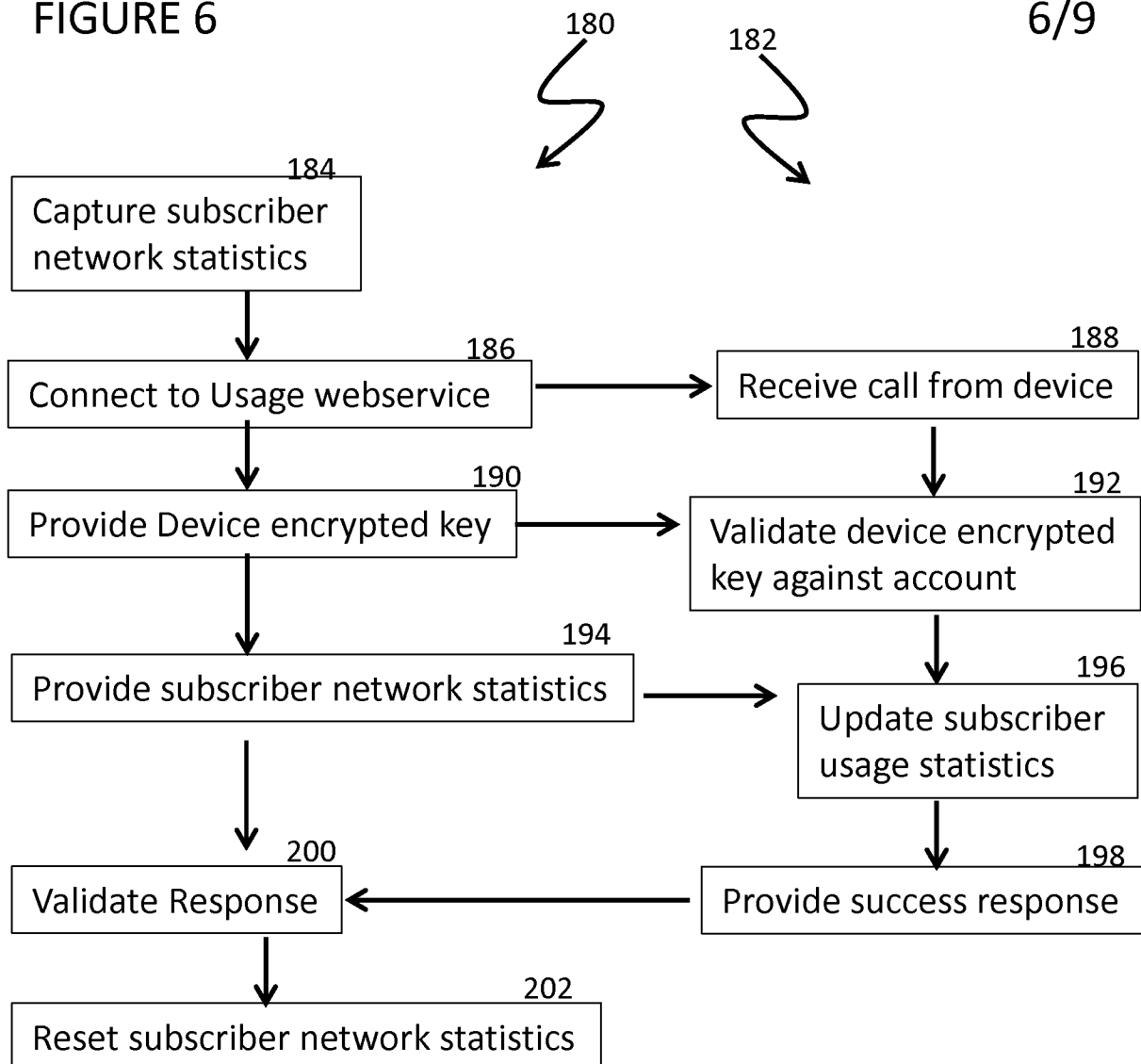


FIGURE 7

7/9

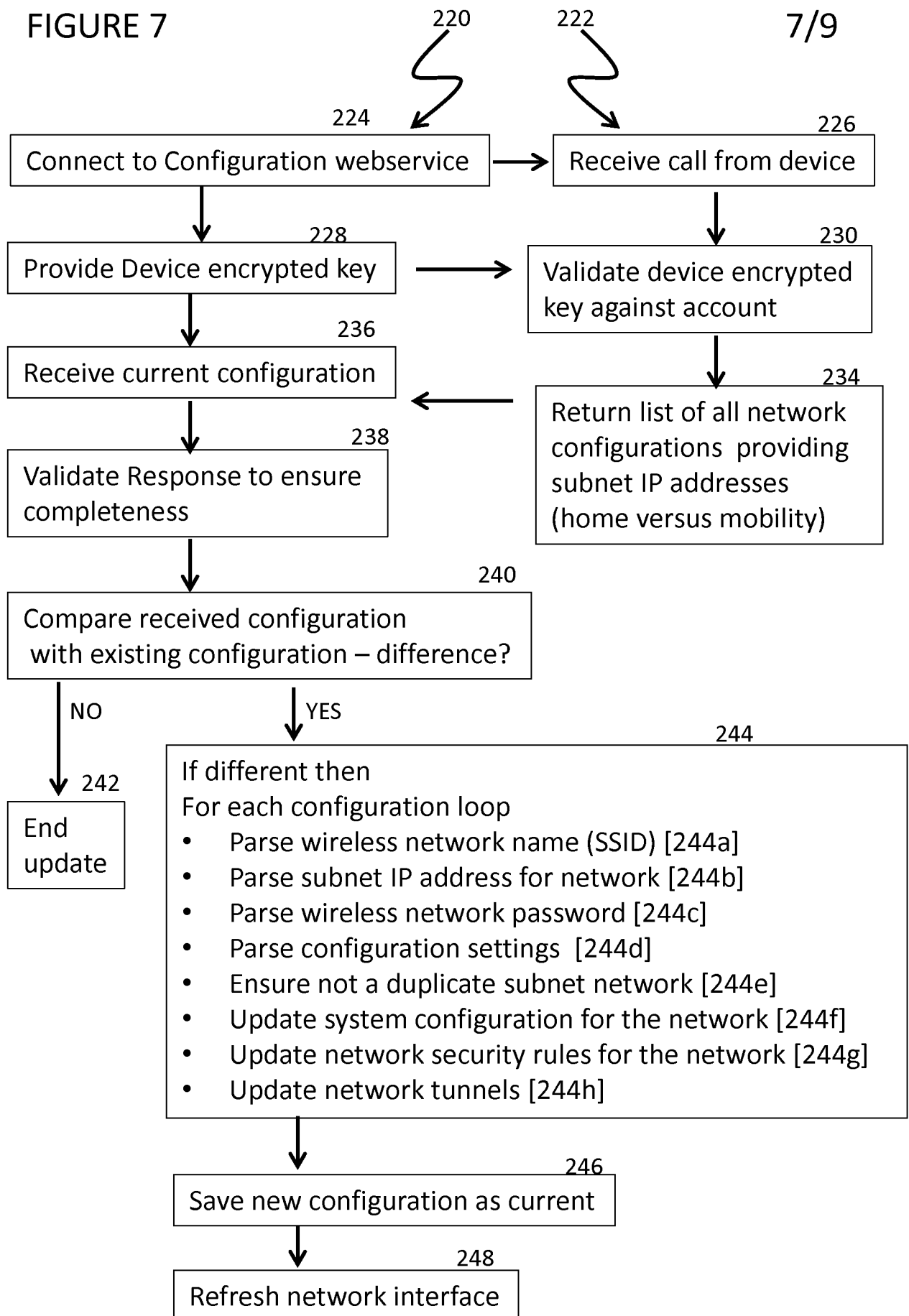


FIGURE 8

8/9

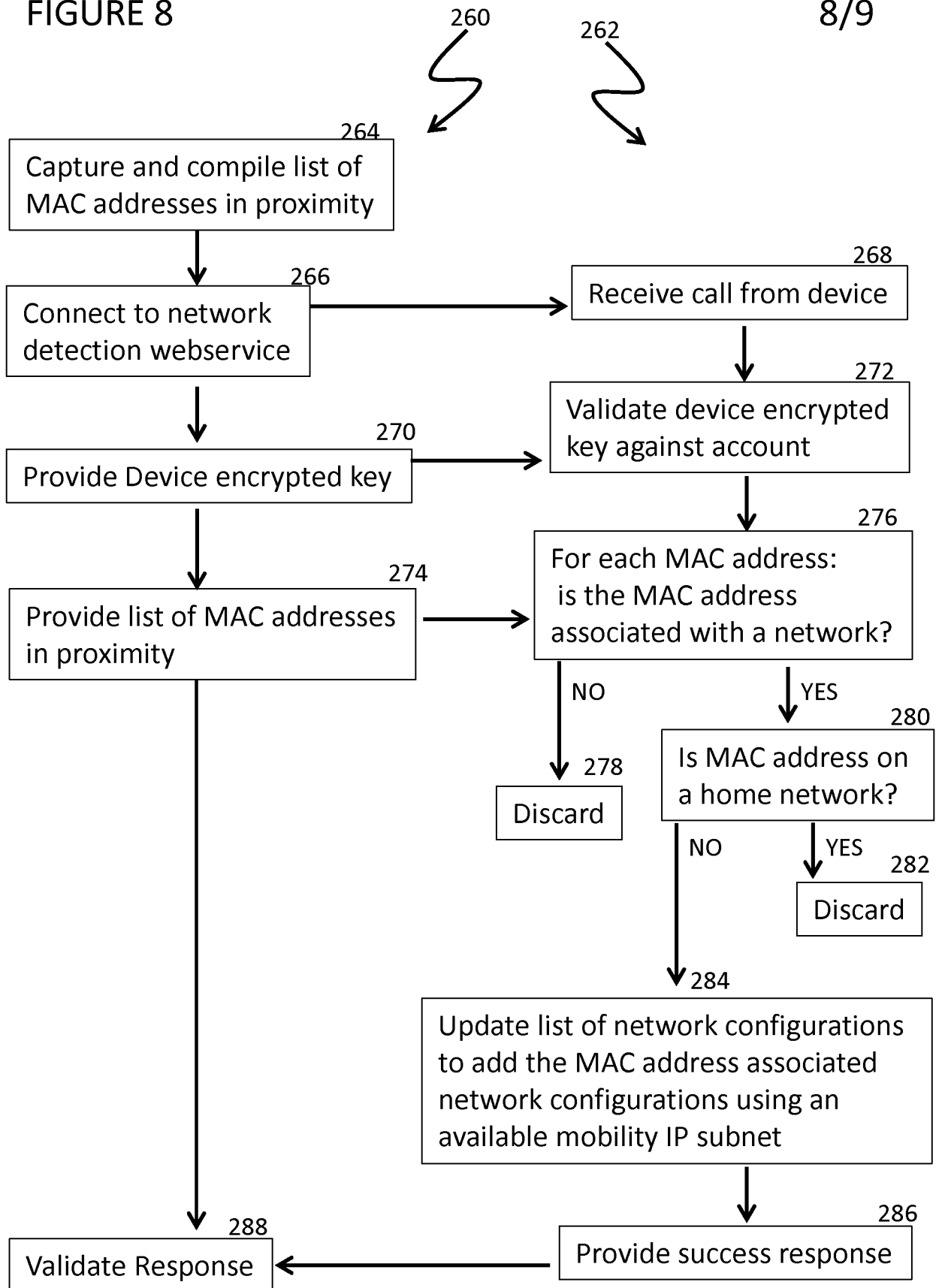
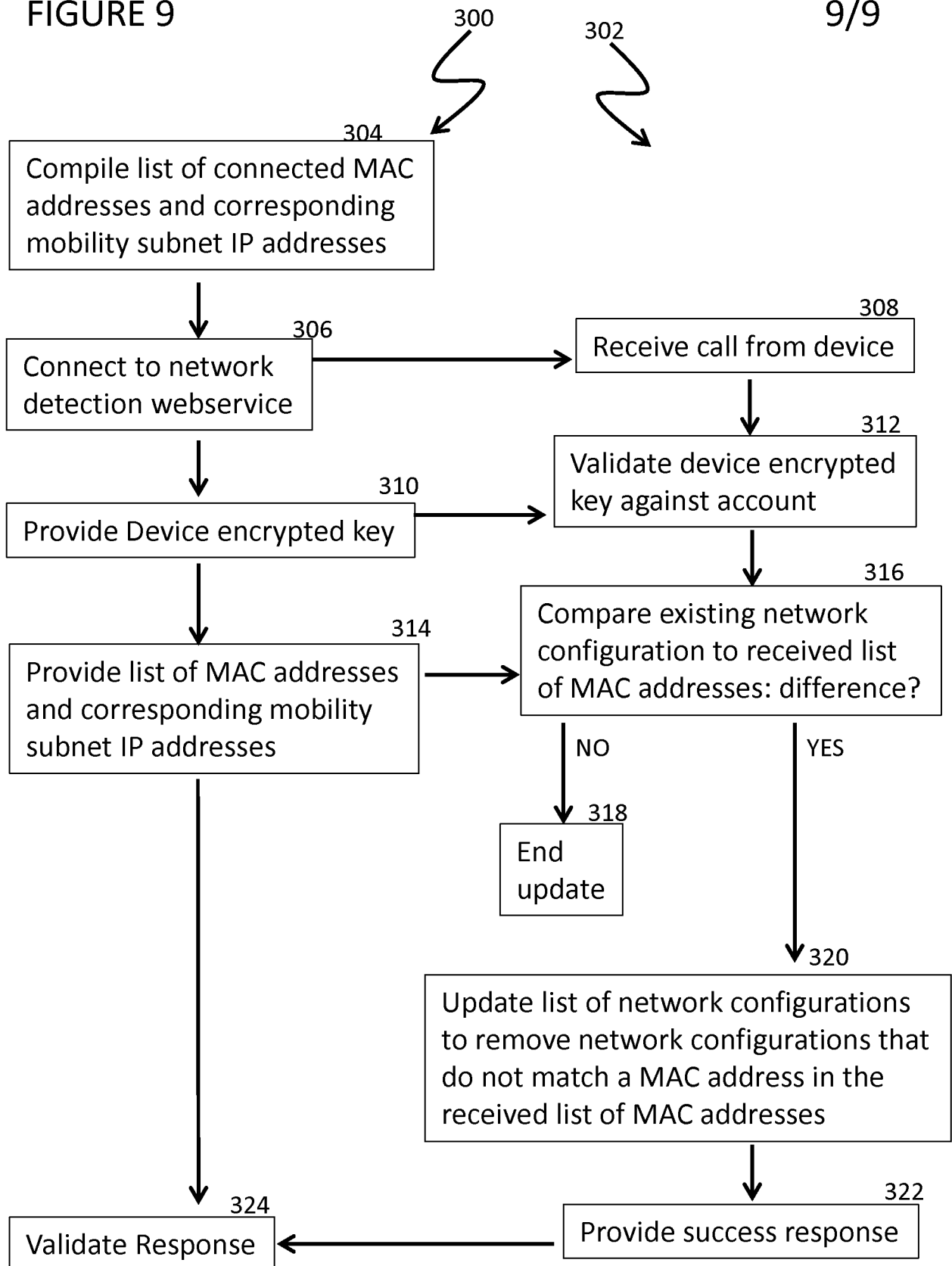


FIGURE 9

9/9



INTERNATIONAL SEARCH REPORT

International application No.

PCT/CA2016/050968

A. CLASSIFICATION OF SUBJECT MATTER

IPC: **H04W 48/18** (2009.01), **H04W 12/08** (2009.01), **H04W 4/26** (2009.01)

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPCs/CPCs: H04W-48/18, H04W-12/08 and H04W-04/26

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

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

Canadian Patent Database and Questel Orbit.com (PlusPat - Biblio, FamPat - Biblio and Full Text, and/or Full Text Databases) - Search terms used: (*see extra sheet page 12*)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Group A GB 2 440 193 A (CARTER) 23 January 2008 (23-01-2008) Abstract Figures 1-14 Page 4, line 2 to page 5, line 27, Page 7, lines 3-23, Page 8, line 3 to page 9, line 24, Page 9, line 29 to page 10, line 25, Page 10, line 26 – page 11, line 4, Page 11, line 16 – page 12, line 19, Page 12, line 20 – page 13, line 16, Page 16, line 20 – page 17, line 15, and Page 30, line 12 – page 31, line 4 Claims 1-22	1-30, 61-105, and 151-164

☒ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* “A” “E” “L” “O” “P”	Special categories of cited documents: document defining the general state of the art which is not considered to be of particular relevance earlier application or patent but published on or after the international filing date document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) document referring to an oral disclosure, use, exhibition or other means document published prior to the international filing date but later than the priority date claimed	“T” “X” “Y” “&”	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art document member of the same patent family
--------------------------------------	--	--------------------------	--

Date of the actual completion of the international search
29 March 2017 (29-03-2017)Date of mailing of the international search report
01 May 2017 (01-05-2017)
 Name and mailing address of the ISA/CA
 Canadian Intellectual Property Office
 Place du Portage I, C114 - 1st Floor, Box PCT
 50 Victoria Street
 Gatineau, Quebec K1A 0C9
 Facsimile No.: 819-953-2476

Authorized officer

Donald Lefebvre (819) 639-8195

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CA2016/050968**Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of the first sheet)**

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

1. ☐ Claim Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claim Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claim Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

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

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

See extra sheet at page 12.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. ☒ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claim Nos.:

Group A – Claims 1-30, 61-105, and 151-164.

Group B – Claims 31-60.
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claim Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- ☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- ☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CA2016/050968

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 9,055,511 (GUPTA et al.) 09 Jun 2015 (09-06-2015) Whole document	1-30, 61-105, and 151-164
A	US 2015/0142623 A1 (FERGUSON et al.) 21 May 2015 (21-05-2015) Whole document	1-30, 61-105, and 151-164
A	US 2007/0083470 A1 (BONNER et al.) 12 April 2007 (12-04-2007) Whole document	1-30, 61-105, and 151-164
=====	=====	=====
	Group B	
X	US 8,792,419 B2 (WOHLERT et al.) 29 July 2014 (29-07-2014) Abstract	31, 35, 39, 41, 45, 49, 51, 55 and 59
-----	Figures 1, 3-46	
Y	Column 2, line 22 – column 4, line 31, Column 9, line 47 – column 11, line 35, Column 16, line 47 – column 17, line 13, Column 17, lines 31-62, Column 18, lines 10-25, Column 44, line 33 – column 45, line 2, Column 45, line 64 – column 46, line 62, Column 53, lines 7-15, Column 58, lines 27-35, and Column 60, lines 38-56	32-40, 42-50 and 52-60
X	US 8,995,318 B2 (ATARIUS et al.) 31 March 2015 (31-03-2015) Abstract Figures 1-19 Column 1, line 52 – column 2, line 41, and Column 18, line 50 – column 19, line 42	31, 41 and 51
Y	GB 2 440 193 A (CARTER) 23 January 2008 (23-01-2008) Abstract Figures 1-14 Page 9, lines 11-18, and Page 11, line 16 – page 12, line 19	32-40, 42-50 and 52-60
A	US 2015/0350870 A1 (HORN et al.) 03 December 2015 (03-12-2015) Whole document	31-60
A	US 8,977,257 B2 (HORN) 10 March 2015 (10-03-2015) Whole document	31-60
A	US 8,953,566 B2 (HEGDE et al.) 10 February 2015 (10-02-2015) Whole document	31-60
A	US 8,681,683 B2 (GIARETTA et al.) 25 March 2014 (25-03-2014) Whole document	31-60
A	US 2013/0142059 A1 (DI GIROLAMO et al.) 06 June 2013 (06-06-2013) Whole document	31-60
A	US 8,379,512 B2 (GOGIC et al.) 19 February 2013 (19-02-2013) Whole document	31-60
A	US 8,023,966 B2 (AALTONEN) 20 September 2011 (20-09-2011) Whole document	31-60
A	US 7,305,229 B2 (FOX et al.) 04 December 2007 (04-12-2007) Whole document	31-60
A	US 7,272,392 B2 (BODA) 18 September 2007 (18-09-2007) Whole document	31-60

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CA2016/050968

Group A

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
GB2440193A	23 January 2008 (23-01-2008)	GB0614354D0	30 August 2006 (30-08-2006)
US9055511B2	09 June 2015 (09-06-2015)	US2009093232A1 AU2008311002A1 AU2008311003A1 AU2008311003B2 AU2008311004A1 AU2008311004B2 BRPI0818609A2 BRPI0818611A2 BRPI0818612A2 CA2701906A1 CA2701924A1 CA2701961A1 CA2881157A1 CN101889419A CN101889420A CN101889420B CN101889464A EP2198585A2 EP2198586A1 EP2198653A2 EP2273755A1 EP2273755B1 EP2273824A2 HK1150482A1 IL204864D0 IL204864A IL204870D0 IL204871D0 IL204871A JP2010541514A JP5248617B2 JP2010541515A JP5290303B2 JP2011501917A JP5623283B2 JP2013153485A JP2014014122A KR20120004534A KR101216086B1 KR20100085095A KR101261347B1 KR20100075628A KR101290186B1 KR20120003957A KR101327456B1 KR20100075627A KR101385612B1 KR20120002611A KR101410371B1 KR20130008627A KR20130016405A MX2010003752A MX2010003753A MX2010003754A MY152239A RU2010118312A RU2459374C2 RU2010118488A RU2475991C2 RU2010118515A RU2488238C2 SG185280A1 SG185282A1	09 April 2009 (09-04-2009) 16 April 2009 (16-04-2009) 16 April 2009 (16-04-2009) 10 January 2013 (10-01-2013) 16 April 2009 (16-04-2009) 01 December 2011 (01-12-2011) 22 April 2015 (22-04-2015) 22 April 2015 (22-04-2015) 07 April 2015 (07-04-2015) 16 April 2009 (16-04-2009) 16 April 2009 (16-04-2009) 16 April 2009 (16-04-2009) 16 April 2009 (16-04-2009) 17 November 2010 (17-11-2010) 17 November 2010 (17-11-2010) 24 July 2013 (24-07-2013) 17 November 2010 (17-11-2010) 23 June 2010 (23-06-2010) 23 June 2010 (23-06-2010) 23 June 2010 (23-06-2010) 12 January 2011 (12-01-2011) 21 September 2016 (21-09-2016) 12 January 2011 (12-01-2011) 28 March 2014 (28-03-2014) 30 November 2010 (30-11-2010) 30 November 2015 (30-11-2015) 30 November 2010 (30-11-2010) 30 November 2010 (30-11-2010) 24 September 2015 (24-09-2015) 24 December 2010 (24-12-2010) 31 July 2013 (31-07-2013) 24 December 2010 (24-12-2010) 18 September 2013 (18-09-2013) 13 January 2011 (13-01-2011) 12 November 2014 (12-11-2014) 08 August 2013 (08-08-2013) 23 January 2014 (23-01-2014) 12 January 2012 (12-01-2012) 27 December 2012 (27-12-2012) 28 July 2010 (28-07-2010) 07 May 2013 (07-05-2013) 02 July 2010 (02-07-2010) 30 July 2013 (30-07-2013) 11 January 2012 (11-01-2012) 11 November 2013 (11-11-2013) 02 July 2010 (02-07-2010) 16 April 2014 (16-04-2014) 06 January 2012 (06-01-2012) 24 June 2014 (24-06-2014) 22 January 2013 (22-01-2013) 14 February 2013 (14-02-2013) 02 July 2010 (02-07-2010) 23 June 2010 (23-06-2010) 23 June 2010 (23-06-2010) 15 September 2014 (15-09-2014) 20 November 2011 (20-11-2011) 20 August 2012 (20-08-2012) 20 November 2011 (20-11-2011) 20 February 2013 (20-02-2013) 20 November 2011 (20-11-2011) 20 July 2013 (20-07-2013) 29 November 2012 (29-11-2012) 29 November 2012 (29-11-2012)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2016/050968**Group A**

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US9055511B2 (continued)		TW200935930A TWI391009B TW200932008A TWI415492B TW200932007A TWI454110B UA97019C2 UA97552C2 UA101337C2 US2009094680A1 US9167505B2 US2009094351A1 WO2009048887A1 WO2009048888A2 WO2009048889A2	16 August 2009 (16-08-2009) 21 March 2013 (21-03-2013) 16 July 2009 (16-07-2009) 11 November 2013 (11-11-2013) 16 July 2009 (16-07-2009) 21 September 2014 (21-09-2014) 26 December 2011 (26-12-2011) 27 February 2012 (27-02-2012) 25 March 2013 (25-03-2013) 09 April 2009 (09-04-2009) 20 October 2015 (20-10-2015) 09 April 2009 (09-04-2009) 16 April 2009 (16-04-2009) 16 April 2009 (16-04-2009) 16 April 2009 (16-04-2009)
US2015142623A1	21 May 2015 (21-05-2015)	AU2007349233A1 AU2007349233A2 AU2007349233B2 AU2010270756A1 AU2010270756B2 BRPI0721466A2 BR112012000373A2 CA2681474A1 CA2681474C CA2752089A1 CA2752090A1 CA2767245A1 CA2767245C CA2794585A1 CA2804455A1 CA2805177A1 CA2823181A1 CA2832545A1 CN102484593A CN102484593B EP2130357A1 EP2130357B1 EP2248295A1 EP2248371A1 EP2281386A1 EP2417755A1 EP2452303A1 EP2452461A2 EP2460114A1 EP2537132A2 EP2537134A2 IL200949D0 IL200949A IN913DEN2012A JP2012533119A JP5830017B2 KR20100015663A KR101490132B1 KR20120062699A KR101625173B1 MX2009009925A MX2012000355A NZ580499A SG177476A1 US2009204457A1 US8116731B2 US2010130165A1 US8280348B2	25 September 2008 (25-09-2008) 10 December 2009 (10-12-2009) 09 February 2012 (09-02-2012) 09 February 2012 (09-02-2012) 27 August 2015 (27-08-2015) 05 August 2014 (05-08-2014) 22 March 2016 (22-03-2016) 25 September 2008 (25-09-2008) 20 December 2016 (20-12-2016) 20 August 2009 (20-08-2009) 20 August 2009 (20-08-2009) 13 January 2011 (13-01-2011) 20 December 2016 (20-12-2016) 14 October 2010 (14-10-2010) 13 January 2011 (13-01-2011) 03 February 2011 (03-02-2011) 25 August 2011 (25-08-2011) 25 August 2011 (25-08-2011) 30 May 2012 (30-05-2012) 03 December 2014 (03-12-2014) 09 December 2009 (09-12-2009) 21 October 2015 (21-10-2015) 10 November 2010 (10-11-2010) 10 November 2010 (10-11-2010) 09 February 2011 (09-02-2011) 15 February 2012 (15-02-2012) 16 May 2012 (16-05-2012) 16 May 2012 (16-05-2012) 06 June 2012 (06-06-2012) 26 December 2012 (26-12-2012) 26 December 2012 (26-12-2012) 17 May 2010 (17-05-2010) 30 June 2014 (30-06-2014) 03 April 2015 (03-04-2015) 20 December 2012 (20-12-2012) 09 December 2015 (09-12-2015) 12 February 2010 (12-02-2010) 05 February 2015 (05-02-2015) 14 June 2012 (14-06-2012) 27 May 2016 (27-05-2016) 28 January 2010 (28-01-2010) 19 April 2012 (19-04-2012) 31 August 2012 (31-08-2012) 28 February 2012 (28-02-2012) 13 August 2009 (13-08-2009) 14 February 2012 (14-02-2012) 27 May 2010 (27-05-2010) 02 October 2012 (02-10-2012)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2016/050968**Group A**

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US2015142623A1 (Continued)		US2008227471A1 US8374634B2 US2012297459A1 US8566912B2 US2012144498A1 US8588748B2 US2012302209A1 US8831564B2 US2011154447A1 US8839394B2 US2014047514A1 US9141773B2 US2014351899A1 US9154952B2 US2009204815A1 US9185123B2 US2013132568A1 US9420448B2 US2014187205A1 US9432845B2 US2016021537A1 US9456348B2 US2015017947A1 US9603023B2 US2011030037A1 US2011202407A1 US2011208601A1 US2012130898A1 US2012131121A1 US2013197998A1 US2013262311A1 US2014040155A1 US2015178715A1 US2016173448A1 US2016227405A1 US2016323709A1 US2016373930A1 WO2008115299A1 WO2009102385A1 WO2009102388A1 WO2009139890A1 WO2010118057A1 WO2011005710A2 WO2011005900A1 WO2011014837A1 WO2011103429A2 WO2011103432A2 WO2013113025A2 WO2013181151A2 ZA201200071B	18 September 2008 (18-09-2008) 12 February 2013 (12-02-2013) 22 November 2012 (22-11-2012) 22 October 2013 (22-10-2013) 07 June 2012 (07-06-2012) 19 November 2013 (19-11-2013) 29 November 2012 (29-11-2012) 09 September 2014 (09-09-2014) 23 June 2011 (23-06-2011) 16 September 2014 (16-09-2014) 13 February 2014 (13-02-2014) 22 September 2015 (22-09-2015) 27 November 2014 (27-11-2014) 06 October 2015 (06-10-2015) 13 August 2009 (13-08-2009) 10 November 2015 (10-11-2015) 23 May 2013 (23-05-2013) 16 August 2016 (16-08-2016) 03 July 2014 (03-07-2014) 30 August 2016 (30-08-2016) 21 January 2016 (21-01-2016) 27 September 2016 (27-09-2016) 15 January 2015 (15-01-2015) 21 March 2017 (21-03-2017) 03 February 2011 (03-02-2011) 18 August 2011 (18-08-2011) 25 August 2011 (25-08-2011) 24 May 2012 (24-05-2012) 24 May 2012 (24-05-2012) 01 August 2013 (01-08-2013) 03 October 2013 (03-10-2013) 06 February 2014 (06-02-2014) 25 June 2015 (25-06-2015) 16 June 2016 (16-06-2016) 04 August 2016 (04-08-2016) 03 November 2016 (03-11-2016) 22 December 2016 (22-12-2016) 25 September 2008 (25-09-2008) 20 August 2009 (20-08-2009) 20 August 2009 (20-08-2009) 19 November 2009 (19-11-2009) 14 October 2010 (14-10-2010) 13 January 2011 (13-01-2011) 13 January 2011 (13-01-2011) 03 February 2011 (03-02-2011) 25 August 2011 (25-08-2011) 25 August 2011 (25-08-2011) 01 August 2013 (01-08-2013) 05 December 2013 (05-12-2013) 26 September 2012 (26-09-2012)
US2007083470A1	12 April 2007 (12-04-2007)	CN101385277A EP1955487A2 JP2009512359A WO2007044969A2	11 March 2009 (11-03-2009) 13 August 2008 (13-08-2008) 19 March 2009 (19-03-2009) 19 April 2007 (19-04-2007)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2016/050968**Group B**

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US8792419B2	29 July 2014 (29-07-2014)	US2011249658A1 US2014287767A1 US9432908B2 US2017013536A1	13 October 2011 (13-10-2011) 25 September 2014 (25-09-2014) 30 August 2016 (30-08-2016) 12 January 2017 (12-01-2017)
US8995318B2	31 March 2015 (31-03-2015)	US2011286389A1 CN102972053A CN102972053B EP2553951A1 EP2553951B1 EP2651155A1 JP2013524651A JP5529333B2 KR20120137499A KR101450831B1 KR20140071449A WO2011123832A1	24 November 2011 (24-11-2011) 13 March 2013 (13-03-2013) 07 October 2015 (07-10-2015) 06 February 2013 (06-02-2013) 20 August 2014 (20-08-2014) 16 October 2013 (16-10-2013) 17 June 2013 (17-06-2013) 25 June 2014 (25-06-2014) 21 December 2012 (21-12-2012) 14 October 2014 (14-10-2014) 11 June 2014 (11-06-2014) 06 October 2011 (06-10-2011)
GB2440193A	23 January 2008 (23-01-2008)	GB0614354D0	30 August 2006 (30-08-2006)
US2015350870A1	03 December 2015 (03-12-2015)	CA2947607A1 CN106416340A EP3152940A1 KR20170013336A TW201601576A WO2015187288A1	10 December 2015 (10-12-2015) 15 February 2017 (15-02-2017) 12 April 2017 (12-04-2017) 06 February 2017 (06-02-2017) 01 January 2016 (01-01-2016) 10 December 2015 (10-12-2015)
US8977257B2	10 March 2015 (10-03-2015)	US2011217978A1 CN102845085A CN102845085B CN102893639A CN104703169A EP2543203A1 EP2543204A2 EP2543204B1 EP2677783A1 EP2677783B1 ES2561757T3 JP2013521745A JP5579878B2 JP2013521746A JP5678104B2 JP2014195300A JP5859603B2 KR20130001728A KR101475431B1 KR20130006646A KR101549891B1 US2012057574A1 WO2011109775A2 WO2011109776A1	08 September 2011 (08-09-2011) 26 December 2012 (26-12-2012) 08 February 2017 (08-02-2017) 23 January 2013 (23-01-2013) 10 June 2015 (10-06-2015) 09 January 2013 (09-01-2013) 09 January 2013 (09-01-2013) 06 May 2015 (06-05-2015) 25 December 2013 (25-12-2013) 04 November 2015 (04-11-2015) 29 February 2016 (29-02-2016) 10 June 2013 (10-06-2013) 27 August 2014 (27-08-2014) 10 June 2013 (10-06-2013) 25 February 2015 (25-02-2015) 09 October 2014 (09-10-2014) 10 February 2016 (10-02-2016) 04 January 2013 (04-01-2013) 22 December 2014 (22-12-2014) 17 January 2013 (17-01-2013) 03 September 2015 (03-09-2015) 08 March 2012 (08-03-2012) 09 September 2011 (09-09-2011) 09 September 2011 (09-09-2011)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CA2016/050968**Group B**

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US8953566B2	10 February 2015 (10-02-2015)	US2010165957A1	01 July 2010 (01-07-2010)
US8681683B2	25 March 2014 (25-03-2014)	US2008304434A1 BRPI0812213A2 CA2689128A1 CA2689128C CN101682637A CN101682637B EP2165501A1 EP2472968A2 EP2472968B1 JP2010531095A JP5323822B2 KR20100018063A KR101143150B1 RU2009149470A RU2448429C2 TW200908588A TWI411252B WO2008154548A1	11 December 2008 (11-12-2008) 16 December 2014 (16-12-2014) 18 December 2008 (18-12-2008) 15 April 2014 (15-04-2014) 24 March 2010 (24-03-2010) 15 October 2014 (15-10-2014) 24 March 2010 (24-03-2010) 04 July 2012 (04-07-2012) 06 May 2015 (06-05-2015) 16 September 2010 (16-09-2010) 23 October 2013 (23-10-2013) 16 February 2010 (16-02-2010) 14 May 2012 (14-05-2012) 20 July 2011 (20-07-2011) 20 April 2012 (20-04-2012) 16 February 2009 (16-02-2009) 01 October 2013 (01-10-2013) 18 December 2008 (18-12-2008)
US2013142059A1	06 June 2013 (06-06-2013)	CA2786596A1 CA2786596C CN102884861A CN102884861B CN105681180A EP2522194A1 EP2522194B1 EP2849531A1 JP2013516912A JP5625069B2 JP2015046887A JP2017055443A KR20120097547A KR101566577B1 KR20140059868A SG182377A1 SG10201500076QA WO20111085073A1	14 July 2011 (14-07-2011) 21 March 2017 (21-03-2017) 16 January 2013 (16-01-2013) 10 February 2016 (10-02-2016) 15 June 2016 (15-06-2016) 14 November 2012 (14-11-2012) 21 May 2014 (21-05-2014) 18 March 2015 (18-03-2015) 13 May 2013 (13-05-2013) 12 November 2014 (12-11-2014) 12 March 2015 (12-03-2015) 16 March 2017 (16-03-2017) 04 September 2012 (04-09-2012) 05 November 2015 (05-11-2015) 16 May 2014 (16-05-2014) 30 August 2012 (30-08-2012) 27 February 2015 (27-02-2015) 14 July 2011 (14-07-2011)
US8379512B2	19 February 2013 (19-02-2013)	US2010067371A1 AU2009293136A1 BRPI0918051A2 CA2736038A1 CN102160405A CN102160417A CN102160417B EP2345282A2 EP2356837A2 IL211359D0 JP2012503438A JP5410530B2 JP2012503439A JP2013158022A KR20130008079A KR101334855B1 KR20110054063A KR101334857B1 KR20110054064A KR20130025437A KR20130025438A MX2011003000A RU2011115050A	18 March 2010 (18-03-2010) 25 March 2010 (25-03-2010) 01 December 2015 (01-12-2015) 25 March 2010 (25-03-2010) 17 August 2011 (17-08-2011) 17 August 2011 (17-08-2011) 01 July 2015 (01-07-2015) 20 July 2011 (20-07-2011) 17 August 2011 (17-08-2011) 31 May 2011 (31-05-2011) 02 February 2012 (02-02-2012) 05 February 2014 (05-02-2014) 02 February 2012 (02-02-2012) 15 August 2013 (15-08-2013) 21 January 2013 (21-01-2013) 02 December 2013 (02-12-2013) 24 May 2011 (24-05-2011) 12 December 2013 (12-12-2013) 24 May 2011 (24-05-2011) 11 March 2013 (11-03-2013) 11 March 2013 (11-03-2013) 26 April 2011 (26-04-2011) 27 October 2012 (27-10-2012)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CA2016/050968**Group B**

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US8379512B2 (continued)		TW201016047A TW201106729A UA101062C2 US2013150046A1 US8760998B2 US2010069072A1 US8886200B2 US2013148632A1 WO2010033729A2 WO2010033730A2	16 April 2010 (16-04-2010) 16 February 2011 (16-02-2011) 25 February 2013 (25-02-2013) 13 June 2013 (13-06-2013) 24 June 2014 (24-06-2014) 18 March 2010 (18-03-2010) 11 November 2014 (11-11-2014) 13 June 2013 (13-06-2013) 25 March 2010 (25-03-2010) 25 March 2010 (25-03-2010)
US8023966B2	20 September 2011 (20-09-2011)	US2006135179A1 EP1831792A2 WO2006067585A2	22 June 2006 (22-06-2006) 12 September 2007 (12-09-2007) 29 June 2006 (29-06-2006)
US7305229B2	04 December 2007 (04-12-2007)	US2006058021A1 EP1617698A2 GB0415759D0 GB2416276A GB2416276B	16 March 2006 (16-03-2006) 18 January 2006 (18-01-2006) 18 August 2004 (18-08-2004) 18 January 2006 (18-01-2006) 17 June 2009 (17-06-2009)
US7272392B2	18 September 2007 (18-09-2007)	US2004142689A1 AT478539T AU2003276288A1 BR0314366A CA2495093A1 CA2495093C CN1711794A CN1711794B DE60333858D1 EP1559294A1 EP1559294B1 ES2347240T3 GB0225888D0 GB2395091A JP2008245292A JP4886727B2 JP2006505205A KR20050067432A KR100726957B1 TW200420096A TWI345408B US2006121904A1 US9338637B2 WO2004043105A1	22 July 2004 (22-07-2004) 15 September 2010 (15-09-2010) 07 June 2004 (07-06-2004) 19 July 2005 (19-07-2005) 21 May 2004 (21-05-2004) 07 June 2011 (07-06-2011) 21 December 2005 (21-12-2005) 23 April 2014 (23-04-2014) 30 September 2010 (30-09-2010) 03 August 2005 (03-08-2005) 18 August 2010 (18-08-2010) 27 October 2010 (27-10-2010) 11 December 2002 (11-12-2002) 12 May 2004 (12-05-2004) 09 October 2008 (09-10-2008) 29 February 2012 (29-02-2012) 09 February 2006 (09-02-2006) 01 July 2005 (01-07-2005) 14 June 2007 (14-06-2007) 01 October 2004 (01-10-2004) 11 July 2011 (11-07-2011) 08 June 2006 (08-06-2006) 10 May 2016 (10-05-2016) 21 May 2004 (21-05-2004)

Continuation of Box No. III, Page 2

The claims are directed to a plurality of inventive concepts as follows:

- Group A** Claims 1-30, 61-105, and 151-164 are directed to a system, method, product and device for providing a plurality of secured wireless network connections over a shared Internet access point and for adding a secured wireless network connection to a wireless network broadcasting device, specifically characterised by the feature of broadcasting a plurality of secured WLANs and an open unsecured WLAN directed to a web page hosted on a remote server and providing information relating to the plurality of secured WLANs and prompts to allow a subscriber to purchase one of the plurality of secured WLANs;
- Group B** Claims 31-60 are directed to a system, method and product for adding a secured wireless network connection for a subscriber in a mobility mode, specifically characterised by the feature of sending a communication from a remote server to a first wireless network broadcasting device to add the mobility mode secured wireless network connection uniquely accessible by a second subscriber in the mobility mode; and
- Group C** Claims 106-150 are directed to a system, method and product for adding a secured wireless network connection to a wireless network broadcasting device, specifically characterised by the feature of broadcasting, from a wireless network broadcast device, a first open unsecured wireless network connection and a first secured wireless network connection uniquely accessible by a first subscriber, the open unsecured wireless network connection directed to a unique first web page providing information relating to purchase of a second secured wireless network connection of the wireless network broadcast device.

Continuation of "FIELDS SEARCHED", Page 4

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

Group A

shared, internet, network, access point, hotspot, wifi, wireless, wlan, *secur*, range, geogra*, subscriber, first, second, inside, within, outside, beyond, comput* device, terminal, computer, client, desktop, laptop, tablet, smart_phone, broadcast*, transmit*, connect*, communicat*, purchas*, web*, web page, prompt, rule, profile, password

Group B

internet, network, access point, hotspot, wireless, wifi, wlan, *secur*, range, geogra*, subscriber, first, second, home, mobility, roaming, traveling, visitor, guest, mode, configuration, setup, remote server, server, broadcast*, transmit*, connect*, communicat*, uniqu* access*