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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 February 2009 (19.02.2009)

PCT

(10) International Publication Number
WO 2009/022052 A1

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/FI2008/050442

(22) International Filing Date: 22 July 2008 (22.07.2008)

(25) Filing Language: Finnish

(26) Publication Language: English

(30) Priority Data:
20075571 15 August 2007 (15.08.2007) FI

(71) Applicant *(for all designated States except US)*: **ELISA OYJ** [FI/FI]; Ratavartijankatu 5, FI-00520 Helsinki (FI).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **JÄRVINEN, Jarkko** [FI/FI]; Malminkatu 24 A 9, FI-00100 Helsinki (FI). **PIRTTILÄ, Veli** [FI/FI]; Kivelänkatu 9 D 78, FI-00260 Helsinki (FI). **LEHTI, Panu** [FI/FI]; Rauhankatu 26 A 14, FI-06100 Porvoo (FI).

(74) Agent: **ESPATENT OY**; Kaivokatu 10 A, FI-00100 Helsinki (FI).

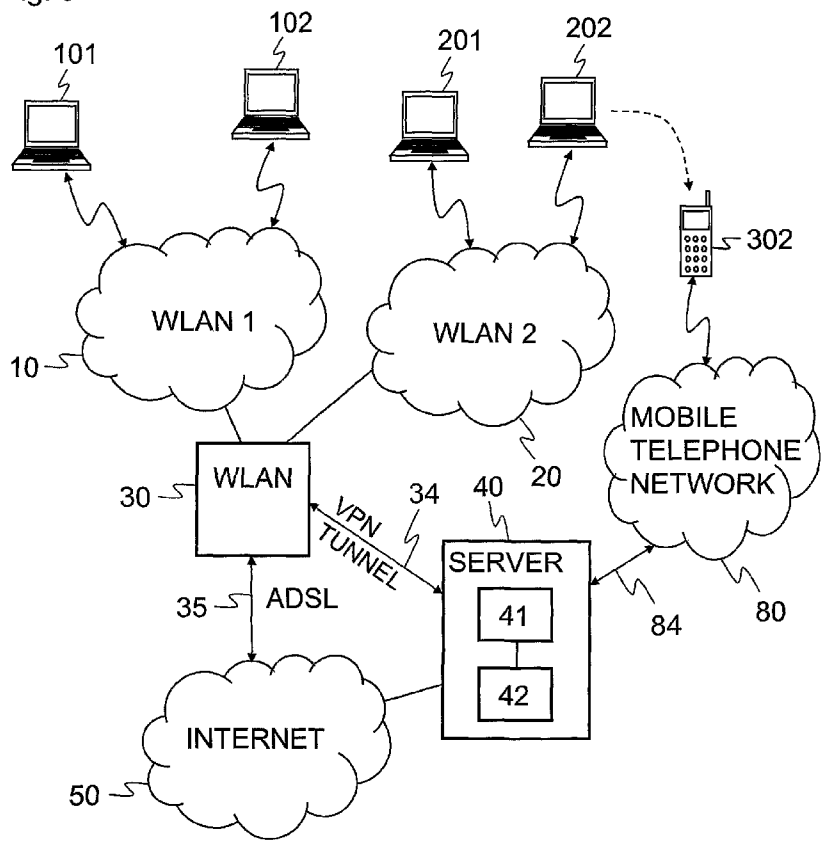
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM,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

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

[Continued on next page]

(54) Title: NETWORK ACCESS FOR A VISITING USER

Fig. 3



(57) Abstract: The invention relates to a method for a visitor (202) in a wireless short-range network to be allowed to access the Internet (50) in a system where the Internet traffic of a holder of a base station (30) of the wireless short-range network is separated from the visitor's traffic. The method comprises intercepting a packet sent by the visiting terminal (202) at a captive portal (42). The packet identifies the sender's address. The method comprises selecting or generating an identifier that pertains or is assigned to said address. Furthermore, the method comprises generating a website on which an identifier is shown to the visitor (202), receiving the identifier from the visitor via a mobile communication network (80) and opening access to the Internet (50) for the address associated with the identifier from the captive portal (42). Furthermore, the invention relates to a captive portal device, system and computer program including corresponding elements.

WO 2009/022052 A1

Published:
— *with international search report*

NETWORK ACCESS FOR A VISITING USER

Generally, the present invention relates to solutions enabling a visiting user to access the Internet on his or her terminal.

For years, Internet access has been possible not only on fixed terminals but also on wireless terminals. Different Internet operators currently provide several different access mechanisms enabling a user to access the Internet.

Figure 1 shows an example. In the figure, wireless terminals (e.g., laptop computers) 101 and 102 of an Internet user are connected to a base station 30 through a wireless local area network (e.g., WLAN). The base station may be in a modem device (e.g., an ADSL modem) that has a connection 35 to the Internet 50.

Wireless local area networks may typically be configured so that registration either requires or does not require some kind of a password. In the latter case, the network is usually called open.

The present invention discloses a novel solution enabling a visiting user to gain access to the Internet through a wireless short-range network.

According to a first aspect of the invention, a method is implemented for a visitor in a wireless short-range network to be allowed to access the Internet in a system where the traffic of a holder of a base station of the wireless short-range network has been separated from the visitor's traffic, comprising:
intercepting a packet sent by a visiting terminal at a captive portal, the packet identifying the sender's address;
selecting or generating an identifier that pertains or is assigned to said address;
generating a website on which the identifier is shown to the visitor;
receiving the identifier from the visitor via a mobile communication network; and
opening access to the Internet for the address associated with the identifier.

Visitors' traffic may be routed in its own network separated in a data secure manner from the device owner's traffic.

In an embodiment of the invention, instructions on where or to which number to send the identifier are also shown in connection with showing the identifier. The visitor may send the identifier to the mobile communication network in a suitable message, e.g., a short message service message (or, more specifically, a text message).

In an embodiment of the invention, a network address translation (NAT) function is performed on the visitor's traffic, whereby a gray IP address of the visiting device is translated into a public IP address.

In an embodiment of the invention, the visitor's traffic is tunneled between said base station of a wireless short-range network and the captive portal, wherein the tunneling may be implemented with, for example, a virtual private network (VPN) connection operating in a NAT traversal operating mode. For example, the IPSec protocol or another suitable tunneling protocol can be used as the tunneling protocol. Tunneling protocols include PPTP/PPP/L2TP, for example.

In an embodiment of the invention, the wireless short-range network is a Wippies WLAN network.

In a method in accordance with an embodiment of the invention, a visiting user may open access to the Internet with a text message (e.g., through a WLAN network). In one such embodiment, an identifier for a "captive portal" is generated for the visitor. The visitor is automatically allowed to communicate with the Internet by sending the identifier to a correct number in a text message. In this case, the user needs no user name or passwords besides the text message, whereby the authentication process becomes significantly easier for the user. The user identification method, as such, is independent of the network, i.e., in principle, the user may be on any mobile telephone operator's network when sending the text message.

In accordance with a second aspect of the invention, a captive portal is implemented for a visitor in a wireless short-range network to be allowed to access the Internet in a system where the traffic of a holder of a base station of the wireless short-range network is separated from the visitor's traffic, comprising:
means for intercepting a packet sent by a visiting terminal, the packet identifying the sender's address;
means for selecting or generating an identifier and assigning the identifier to said address;
means for generating a website on which the identifier is shown to the visitor;
means for receiving the identifier from the visitor via a mobile communication network; and
means for opening Internet access for the address associated with the identifier.

Herein, a "captive portal" refers to a device or server implementing captive portal functionality.

In accordance with a third aspect of the invention, a system according to claim 19 is implemented.

In accordance with a fourth aspect of the invention, a computer program is implemented, comprising a computer-executable program code that, when executed, controls a computerized apparatus to implement captive portal functionality performing a method in accordance with the first aspect.

The computer program in accordance with the fourth aspect may comprise a program code that is executable by any one of the following, for example: a general-purpose processor, a microprocessor, an application-specific integrated circuit, and a digital signal processor. The program code may be executable by a Linux computer, for example.

Some embodiments of the invention have only been or will only be described in connection with some aspects of the invention. However, as a rule, the

corresponding embodiments are also applicable to other aspects as well.

The invention will be described in the following by way of example with reference to the appended drawings, wherein:

Figure 1 shows a prior art system;
Figure 2 shows a system in accordance with an embodiment of the invention;
Figure 3 shows a method and a system for identifying visitors and opening access to the Internet in accordance with an embodiment of the invention; and
Figure 4 is a block diagram of a device comprising captive portal functionality in accordance with an embodiment of the invention.

The same reference numbers are used in the figures to refer to the same subjects or elements. Figure 1 was discussed above in connection with prior art.

Figure 2 shows a system in accordance with an embodiment of the invention. As in Figure 1, wireless terminals (e.g., laptop computers 101 and 102) are connected to a base station 30 through a wireless short-range network (e.g., WLAN) 10. The base station 30 has a permanent connection (e.g., an ADSL connection) 35 to the Internet 50. The base station 30 is located in specific premises, such as the base station owner's home. The base station 30 may provide a plurality of subnetworks. A subnetwork 10 is the base station owner's private subnetwork through which the traffic of the terminals 101 and 102 is routed. In turn, a subnetwork 20 is an open network separate from the subnetwork 10 (different SSID identifiers are used in the subnetworks), enabling other terminals 201 and 202 visiting the area of the base station to have contact with the base station 30. Thus visitors' traffic is routed on their own network separated in a data secure manner from the actual device owner's traffic.

As an example of a service using a system as described above we mention Wippies, where the owner of base station of a wireless local area network (WLAN) may use his or her Internet connection on a number of computers or on any

suitable WLAN device. At the same time, it is possible to share part of the Internet connection with other Wippies users potentially visiting the vicinity.

Wippies provides a data secure way of sharing part of one's own connection with other Wippies users. Wippies is designed so that if the owner needs bandwidth himself or herself, visitors will not prevent the owner from using the connection he or she needs. Visiting Wippies users use their own wireless Wippies LAN (the subnetwork 20) separated from the owner's private network (the subnetwork 10).

In the example shown in Figure 2, the base station owner's (or holder's) terminals 101 and 102 use the connection 35 to communicate with the Internet 50. In contrast, the traffic of visitors connected to the open network 20 is routed from the base station 30 over a virtual connection into a tunnel 34 (e.g., an IPSec VPN tunnel), whose one end point is the base station 30 and the other end point is a server 40 in the network, connected to the Internet 50. However, the tunneled traffic over the virtual connection typically uses the same physical connection as the owner's traffic, albeit separated from the owner's traffic. Server equipment comprises a captive portal 42, which may also be called a traffic capture portal and whose operation will be described below. The server equipment also typically comprises a virtual connection hub, in the VPN case shown in Figure 2, for example, a VPN hub 41 acting as a collector of different VPN connections and as one end point of the virtual connection tunnel. The captive portal 42 and the VPN hub 41 may be implemented in the same or different devices.

Figure 3 shows a method and system for identifying visitors and opening access to the Internet in accordance with an embodiment of the invention. A terminal 202 visiting a subnetwork 20 and a Wippies service are used as a non-limiting example.

When a customer (visitor) and his or her terminal (e.g., a laptop computer, a mobile station, or another WLAN device) enter the area of a Wippies visitor network 20, communication between devices becomes possible. The visitor network is an open network, so typically it is always possible for the terminal 202 to contact it. During contact, the terminal 202 requests a network address (e.g., an

IP address) using a suitable protocol (e.g., the DHCP protocol). A base station 30 issues an IP address to the terminal. The IP address may be one of gray IP addresses distributed by a captive portal 42 to the base station 30 in advance, representing a unique address within a network controlled by the captive portal 42 (the network from the captive portal 42 towards the terminal 202).

When the terminal 202 attempts to communicate with the Internet, the base station opens a VPN tunnel 34 automatically from the user's point of view, whereby all of the visitor's traffic is automatically routed through a VPN hub 41 to the captive portal 42. Thus when the terminal 202 attempts to communicate with the Internet 50 (e.g., tries to open a connection to some WWW service), the captive portal 42 intercepts all transmitted packets and redirects the connection to a login page (the captive portal 42 opens a login page on the terminal 202) and does not allow the customer's traffic to propagate further before login.

Login is carried out using a message sent to a mobile communication network, e.g., a text message or another short message service message (in the following, a text message is used as an example). An identifier is shown to the visitor on the page generated by the captive portal. In addition, brief instructions may be provided on the page, indicating to which number the identifier may be sent, e.g., in a text message. Depending on the implementation, the captive portal 42 may use identifiers in various ways. For example, the captive portal 42 may have a certain number of identifiers in an "identifier pool", from which the captive portal 42 may select the identifier for the login page. Alternatively, the captive portal 42 may generate an identifier as necessary. The identifier may be generated, for example, from the visitor's IP address, on the basis of it, or in some other way. A certain identifier may previously have been linked to correspond to a specific gray IP address in the network controlled by the captive portal. Alternatively, the linking may be performed dynamically when selecting/generating the identifier. Further alternatively, the identifier may be shown to the visitor indirectly. In this case, the actual identifier is not shown in writing to the visitor; rather, only a hint is shown, on the basis of which the visitor will recognize the identifier and know how to send it in a message to a mobile communication network.

Upon receiving the identifier, the visitor sends the identifier in a text message (e.g., on his or her terminal 202 or another terminal (e.g., a cellular telephone/device 302)) to a predetermined number or a number shown on the login page. The text message is passed to a cellular telephone network 80. The cellular telephone network has a connection 84 to a system comprising the captive portal 42. The text message (or, depending on the implementation, only its contents or only information that a correct identifier has been sent to the mobile communication network 80 (even in such cases, the identifier may be considered to be passed to the captive portal 42)) is passed through the connection 84 to the captive portal 42, which will deduce the IP address with which the identifier is associated (this correspondence has previously been stored on the portal 42). Subsequently, the captive portal 42 opens access to the Internet 50 for the IP address in question. The visitor's traffic is routed through the VPN tunnel 34 and a server 40 to the Internet 50. When access to the Internet 50 has been opened, the customer can use the Internet normally on his or her terminal 202. The captive portal 42 typically performs an NAT function for outgoing and incoming packets from/to the terminal 202. In packets moving towards the Internet, the visitor's gray IP address is typically replaced by a public IP address of the captive portal 42. In packets moving in the opposite direction, the public IP address is replaced by the gray IP address. If the virtual connection tunnel has to traverse some other NAT (e.g., an ADSL modem or another firewall device) in the network controlled by the captive portal 42, a NAT Traversal operating method or similar is used for tunneling in accordance with an embodiment.

After a certain period has passed, the captive portal 42 may close the access to the Internet 50 and generate a new identifier on a page, sending which access may be opened again.

Figure 4 shows a block diagram of a captive portal device or a server comprising captive portal functionality. A device 40 comprises a processor 401 for controlling the operation of the device and a memory 402 comprising a computer program/software 403. The computer software 403 may comprise instructions for

the processor to control the device 40, such as an operating system and various applications. In addition, the computer software 403 comprises a program code providing captive portal functionality. Depending on the implementation, the memory 402 comprises a database or a comparable data warehouse 404 for storing identifiers used in certain embodiments and IP addresses corresponding to them.

Furthermore, the device 40 comprises an input/output unit 405 that provides an interface for communication with a cellular mobile communication network. An identifier sent by a visitor to a mobile communication network 80, for example, is received through it. The interface may be a wired connection, for example. The device may also comprise a VPN hub 41 enabling communication in a tunneling manner with a base station 30 in a wireless short-range network.

The description given above provides non-limiting examples of some embodiments of the invention. It is apparent to persons skilled in the art that the invention is not confined to the details presented above, but that the invention may also be implemented in other equivalent ways. For example, it is to be appreciated that, in the above methods, the order of the individual steps of the method may be changed and some steps may be repeated several times or omitted altogether. The protocols presented in the description are also provided as examples. It is also to be appreciated that the terms 'comprise' and 'include' as used in this document are open-ended expressions and not intended to be limiting.

In addition, some features of the embodiments presented may be utilized without employing other features. The above description must be regarded as an explanation describing the principles of the invention and not as limiting the invention. The scope of the invention is only limited by the appended claims.

Claims

1. A method for a visitor in a wireless short-range network to be allowed to access the Internet in a system where the traffic of a holder of a base station of the wireless short-range network is separated from the visitor's traffic, comprising:

intercepting a packet sent by a visiting terminal at a captive portal, the packet identifying the sender's address;

selecting or generating an identifier that pertains or is assigned to said address;

generating a website on which the identifier is shown to the visitor;

receiving the identifier from the visitor via a mobile communication network; and

opening access to the Internet for the address associated with the identifier.

2. A method as claimed in claim 1, wherein instructions on where or to which number to send the identifier are also shown in connection with showing the identifier.

3. A method as claimed in claim 1 or 2, wherein the identifier sent by the visitor is passed to the mobile communication network in a short message service message.

4. A method as claimed in any preceding claim, wherein said visitor's address is a gray IP address of a visiting device.

5. A method as claimed in claim 4, wherein a network address translation (NAT) function is performed on the visitor's traffic, whereby the gray IP address of the visiting device is translated into a public IP address.

6. A method as claimed in any preceding claim, wherein the visitor's traffic is tunneled between said base station of the wireless short-range network and the captive portal.

7. A method as claimed in claim 6, wherein the tunneling is implemented over a VPN connection operating in a NAT traversal operating mode.

8. A method as claimed in claim 6 or 7, wherein the tunneling is implemented with a VPN IPSec tunnel.

9. A method as claimed in any preceding claim, wherein the wireless short-range network is a Wippies WLAN network.

10. A captive portal for a visitor in a wireless short-range network to be allowed to access the Internet in a system where the traffic of a holder of a base station of the wireless short-range network is separated from the visitor's traffic, comprising:

means for intercepting a packet sent by a visiting terminal, the packet identifying the sender's address;

means for selecting or generating an identifier and assigning the identifier to said address;

means for generating a website on which the identifier is shown to the visitor;

means for receiving the identifier from the visitor via a mobile communication network; and

means for opening Internet access for the address associated with the identifier.

11. A captive portal as claimed in claim 10, wherein the captive portal is also configured to show instructions on where or to which number to send the identifier in connection with showing the identifier.

12. A captive portal as claimed in claim 10 or 11, wherein the identifier sent by the visitor is passed to the mobile communication network in a short message service message.

13. A captive portal as claimed in any one of claims 10 to 12, wherein said visitor's address is a gray IP address of a visiting device.

14. A captive portal as claimed in claim 13, wherein the captive portal is also configured to execute a network address translation (NAT) function on the visitor's traffic, whereby the gray IP address of the visiting device is translated into a public IP address.

15. A captive portal as claimed in any one of claims 10 to 14, wherein the captive portal is also configured to tunnel the visitor's traffic between said base station of the short-range network and the captive portal.

16. A captive portal as claimed in claim 15, wherein the tunneling is implemented over a VPN connection operating in a NAT traversal operating mode.

17. A captive portal as claimed in claim 15 or 16, wherein the tunneling is implemented with a VPN IPSec tunnel.

18. A captive portal as claimed in any one of claims 10 to 17, wherein the wireless short-range network is a Wippies WLAN network.

19. A system comprising a base station of a wireless short-range network and a captive portal in accordance with any one of claims 10 to 18.

20. A computer program comprising a computer-executable program code that, when executed, controls a computerized apparatus to carry out captive portal functionality performing a method in accordance with any one of claims 1 to 9.

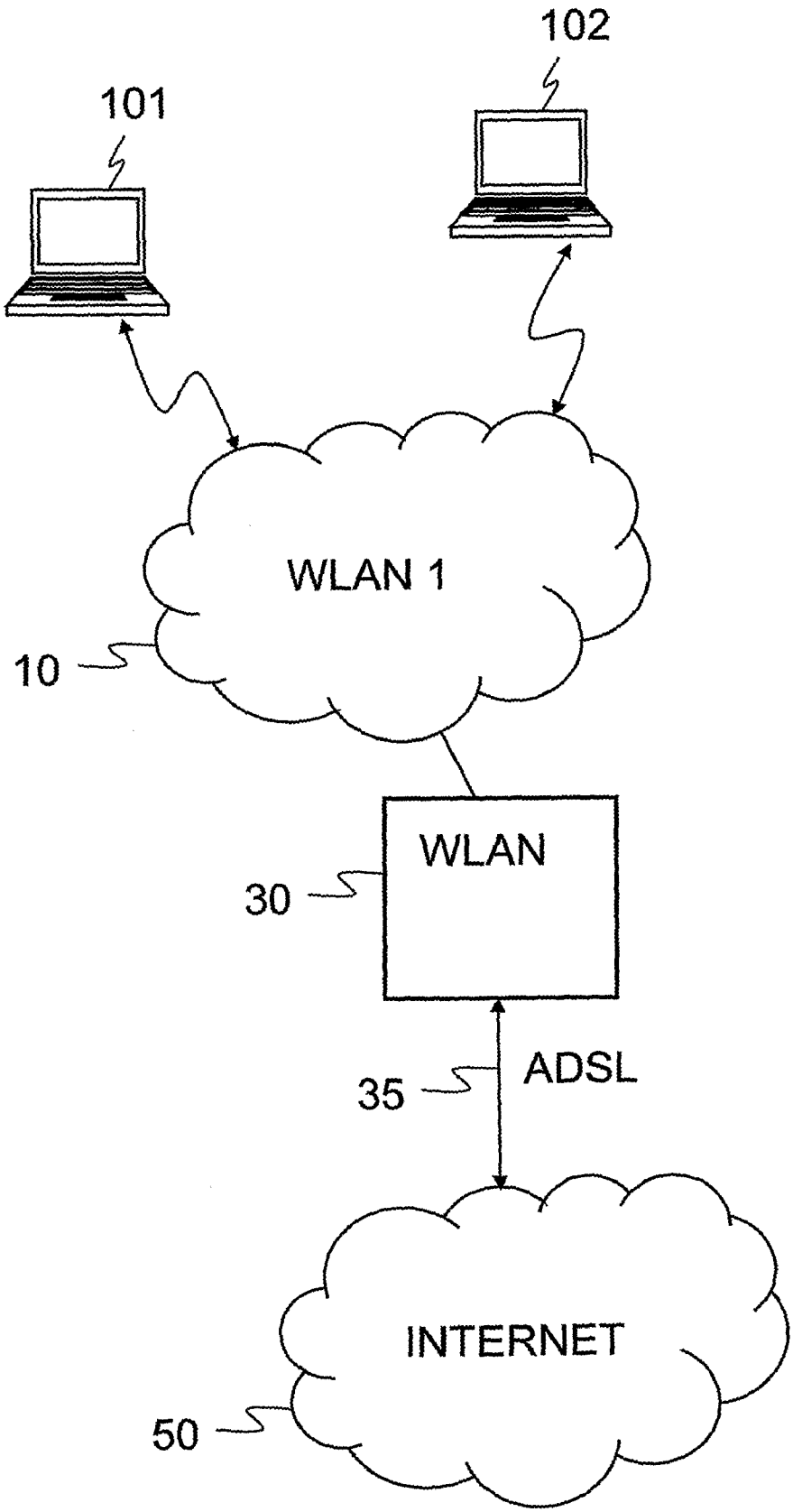


Fig. 1

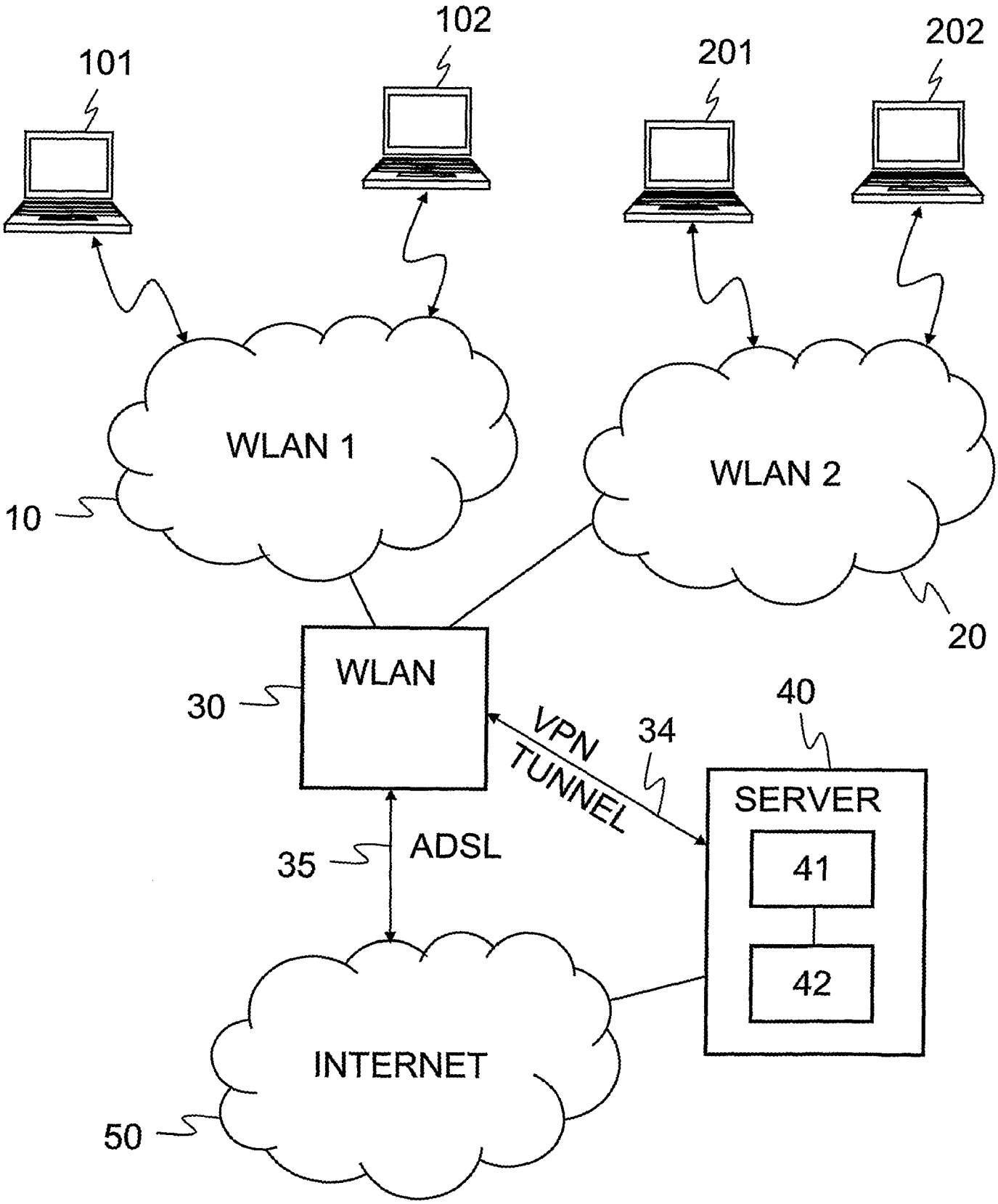

101
102
201
202
WLAN 1
WLAN 2
10
20
WLAN
30
VPN
TUNNEL
34
40
SERVER
41
42
ADSL
35
INTERNET
50

Fig. 2

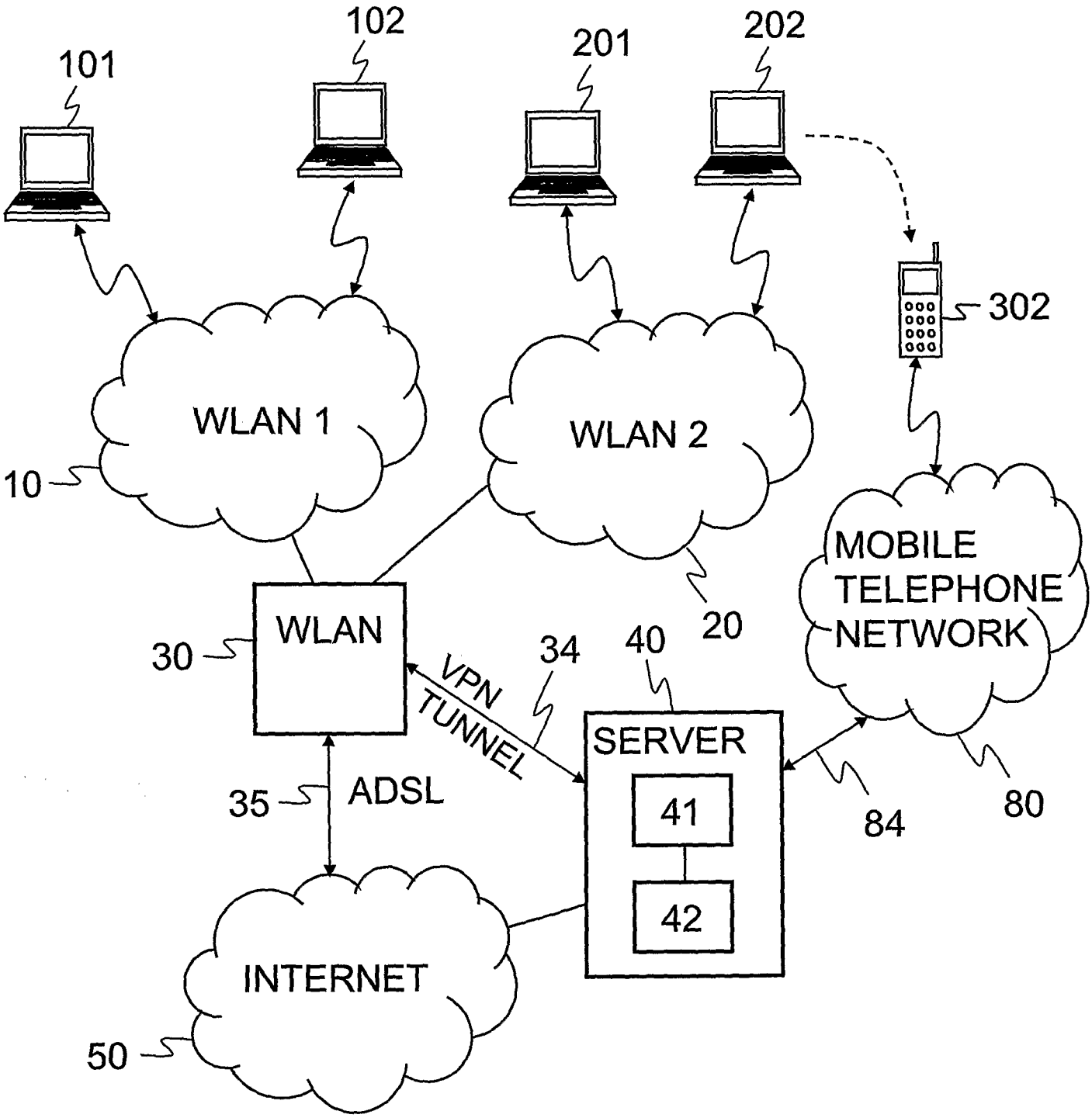

101
102
201
202
302
WLAN 1
WLAN 2
10
20
MOBILE
TELEPHONE
NETWORK
WLAN
30
34
40
VPN
TUNNEL
SERVER
41
42
35
ADSL
84
80
INTERNET
50

Fig. 3

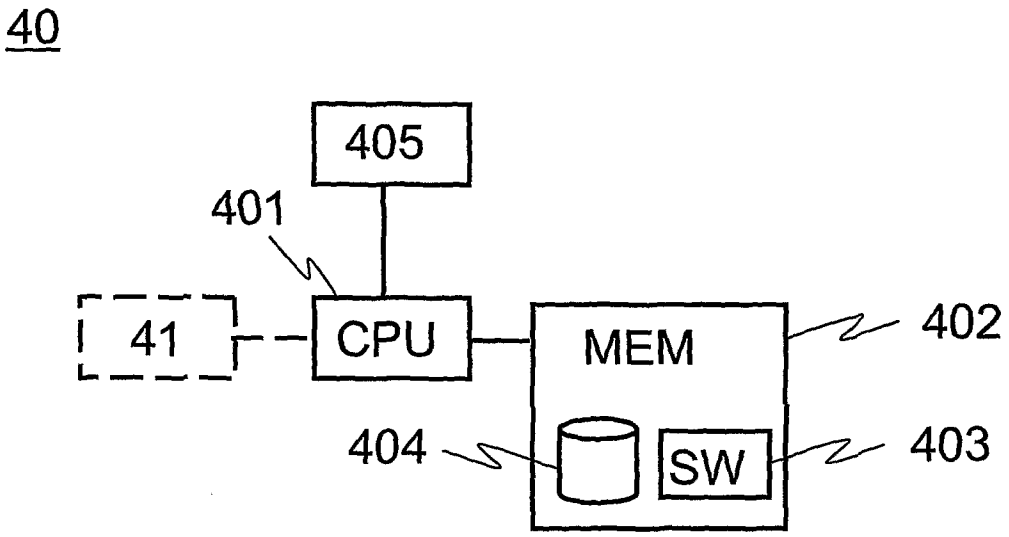


Fig. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2008/050442

A. CLASSIFICATION OF SUBJECT MATTER

See extra sheet

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)

IPC8: H04L29/06

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

FI, SE, NO, DK

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

EPO-Internal, WPI, INSPEC, ETSI, IEEE, Compendex

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2006/0236105 A1 (BROK JACCO et al.) 19 October 2006 (19.10.2006), [0029]-[0032], [0044], [0047]-[0051]; Figs. 1,4,5,6	1-20
Y	WO 02/19593 A2 (ERICSSON TELEFON AB L M) 07 March 2002 (07.03.2002), page 1 lines 5 – 8 and 25 – 31; page 5 line 22 – page 6 line 2; page 6 lines 11 - 13; page 8 lines 20 – 27; page 11 lines 13 – 26; Fig. 2	1-20
A	US 2006/0074814 A1 (LOVELL ROBERT C JR - LOVELL JR ROBERT C) 06 April 2006 (06.04.2006), abstract	

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

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

Date of the actual completion of the international search	Date of mailing of the international search report
31 October 2008 (31.10.2008)	05 November 2008 (05.11.2008)

Name and mailing address of the ISA/FI
National Board of Patents and Registration of Finland
P.O. Box 1160, FI-00101 HELSINKI, Finland
Facsimile No. +358 9 6939 5328

Authorized officer
Jouko Berndtson
Telephone No. +358 9 6939 500

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/FI2008/050442

Patent document cited in search report	Publication date	Patent family members(s)	Publication date
US 2006/0236105 A1	19/10/2006	None	
WO 02/19593 A2	07/03/2002	EP 1314278 A2	28/05/2003
		AU 8279501 A	13/03/2002
US 2006/0074814 A1	06/04/2006	US 2008214144 A1	04/09/2008
		BR PI0516099 A	26/08/2008
		CN 101044746 A	26/09/2007
		EP 1810493 A2	25/07/2007
		CA 2582472 A1	20/04/2006
		WO 2006042213 A2	20/04/2006

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2008/050442

CLASSIFICATION OF SUBJECT MATTER

Int.Cl.
H04L 29/06 (2006.01)