

EX 1004

(21) Application No: **0306975.4**
(22) Date of Filing: **26.03.2003**
(30) Priority Data:
(31) **10113146** (32) **28.03.2002** (33) **US**

(71) Applicant(s):
3Com Corporation
(Incorporated in USA - California)
5400 Bayfront Plaza, Santa Clara,
California 95052-8145,
United States of America

(72) Inventor(s):
Barani Subbiah

(74) Agent and/or Address for Service:
Langner Parry
High Holborn House, 52-54 High Holborn,
LONDON, WC1V 6RR, United Kingdom

(51) INT CL⁷:
H04L 29/06 // H04L 29/06

(52) UK CL (Edition V):
H4L LRADS L205 L215

(56) Documents Cited:
GB 2360914 A **WO 2001/037517 A2**
US 20020022483 A1

(58) Field of Search:
UK CL (Edition V) **G4A, H4L**
INT CL⁷ **G06F, H04L, H04Q**
Other: **On-line: EPODOC, WPI, JAPIO**

(54) Abstract Title: **Network access**

(57) A method for providing communications network access in a public area. The method includes the step 201 of receiving a request to access a communications network from a client. A determination 202 is then made as to whether the request is for access to a first area or a second area of the communications network. The first area can be a local domain of the communications network e.g. a WLAN in an airport or mall. The second area can be the part of the communications network outside the local domain, such as the Internet. In response to receiving a request for access to the first area, access is provided 206 to the services of the first area of the communications network. In response to receiving a request for access to the second area, an authentication process 203 is performed on the client. When the authentication is successful 204, access is provided 205 to the services of the second area of the communications network. The authentication can be performed in accordance with a Web based authentication protocol. The authentication can also be performed in accordance with a basic user registration protocol.

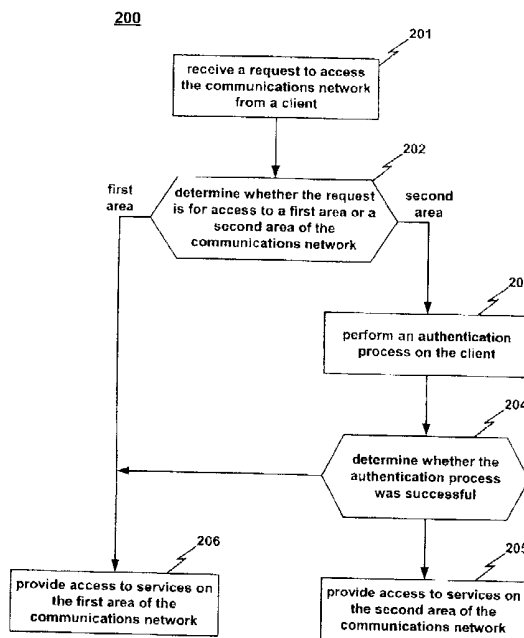


FIG. 2

1/8

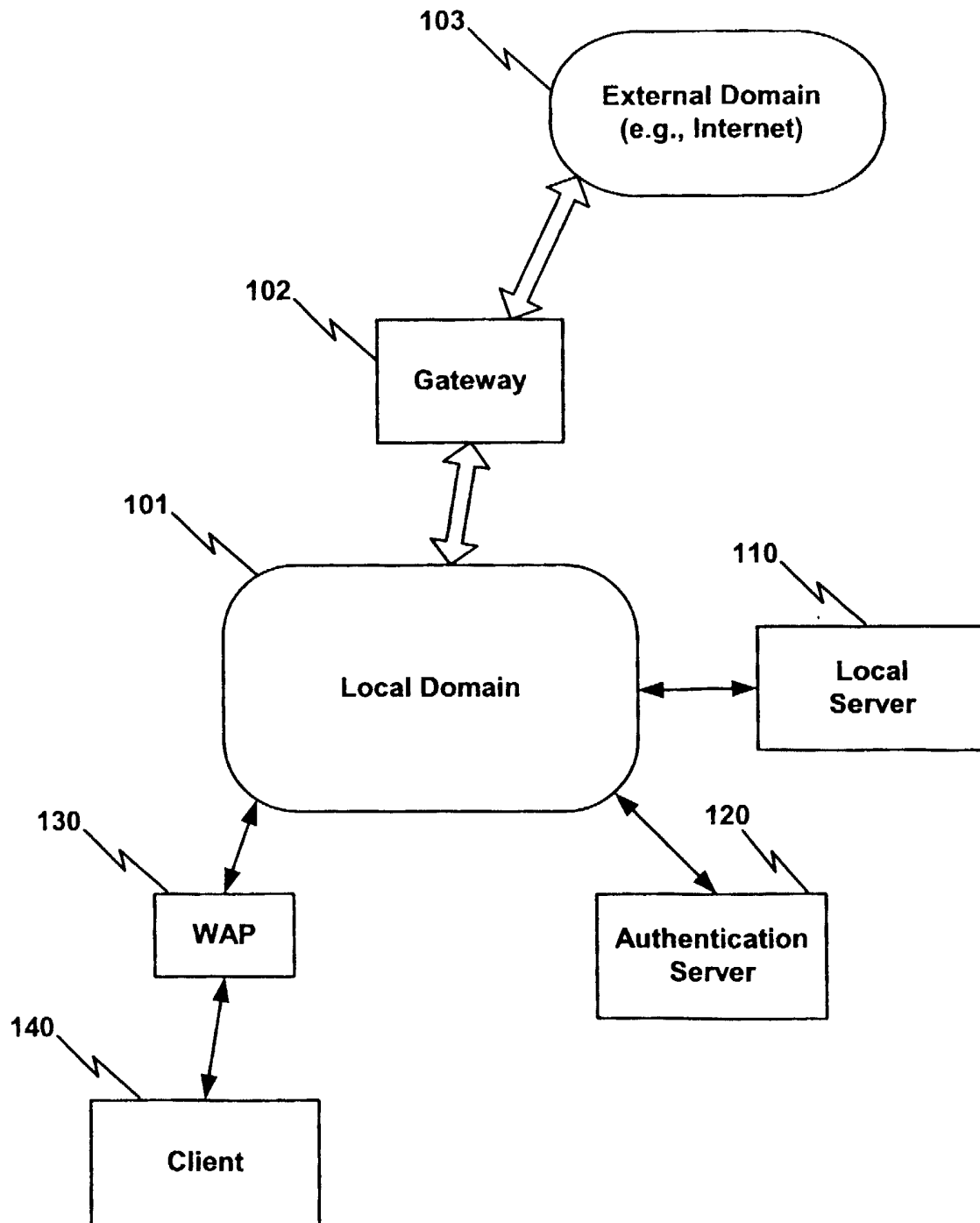


FIG. 1

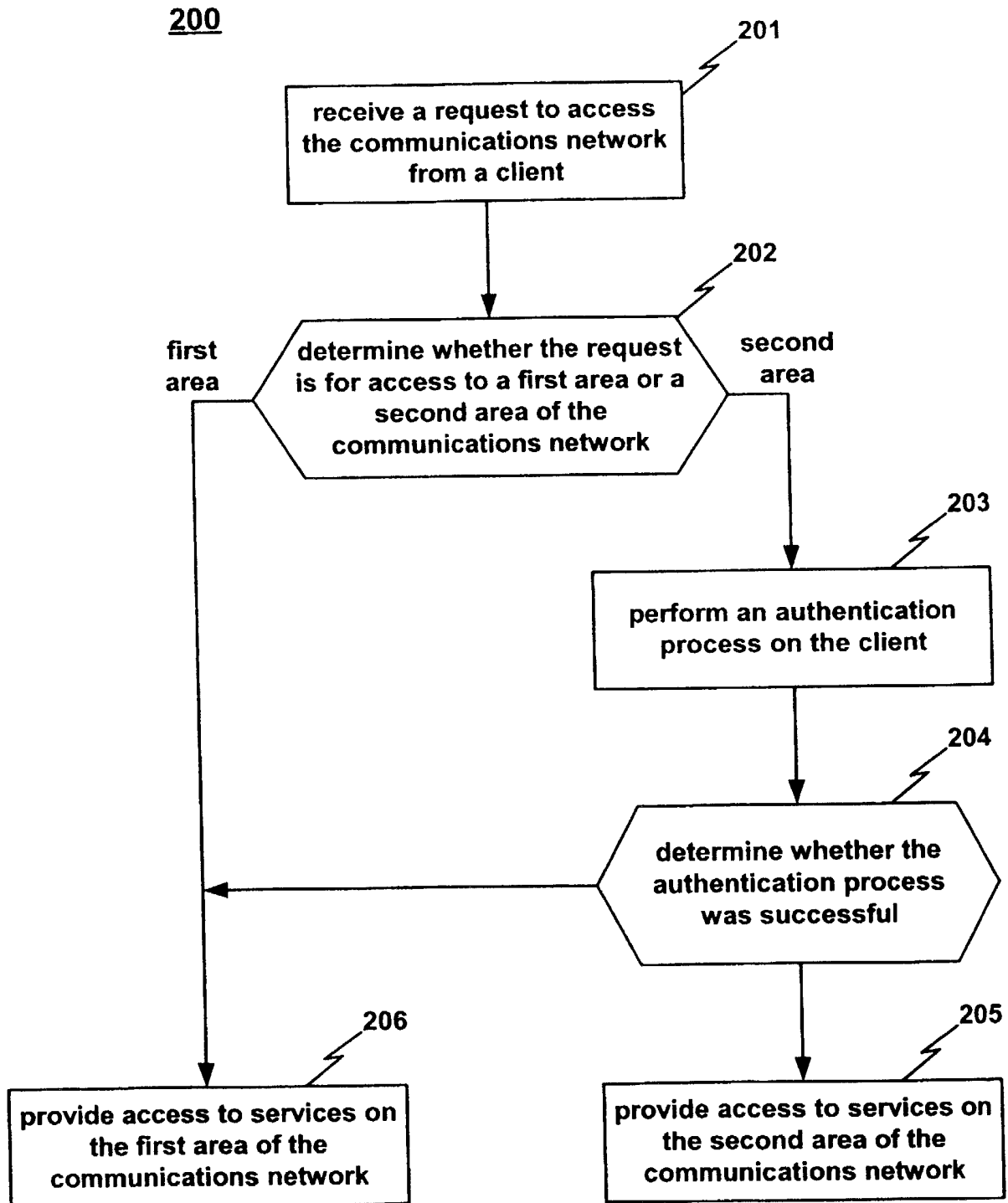


FIG. 2

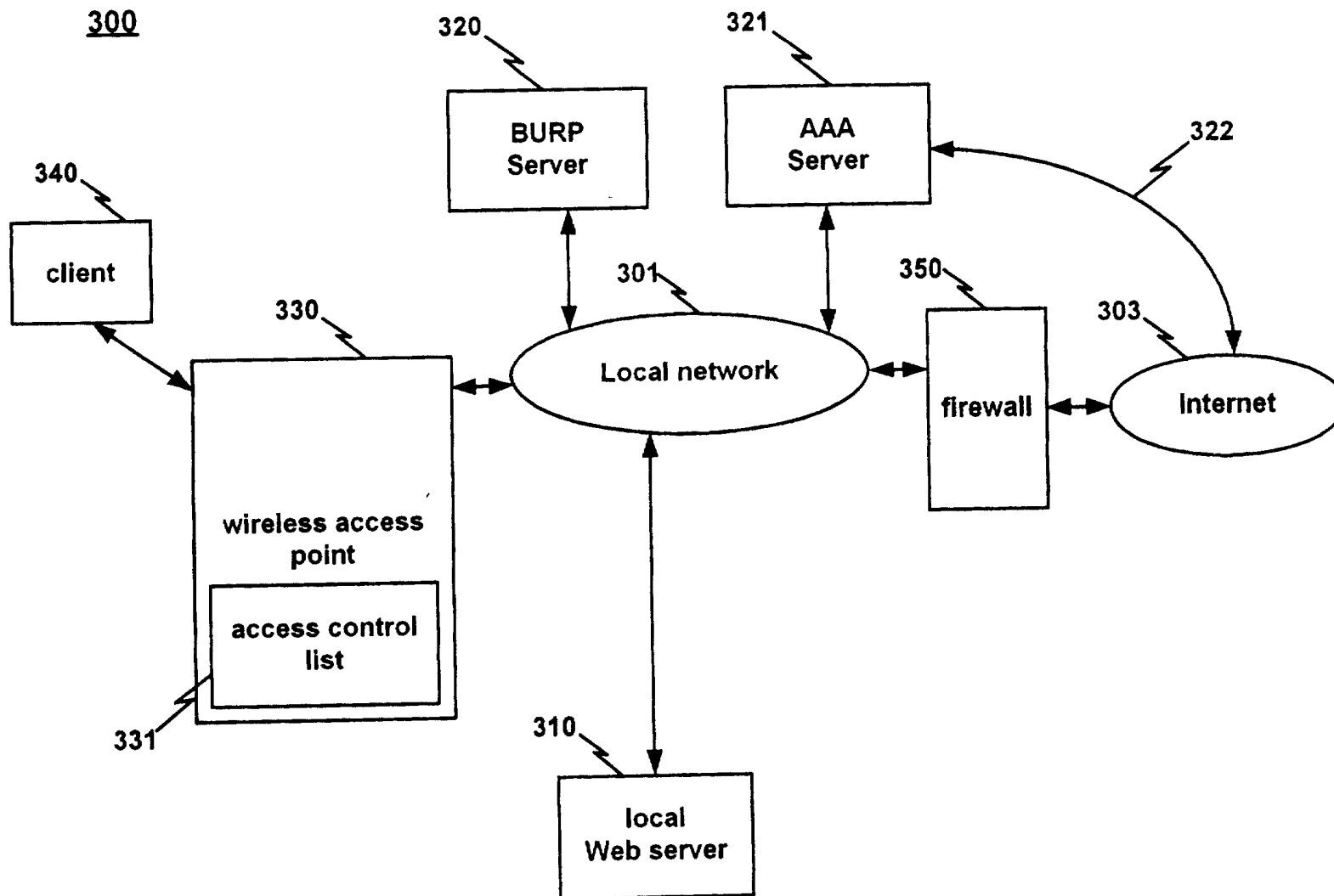
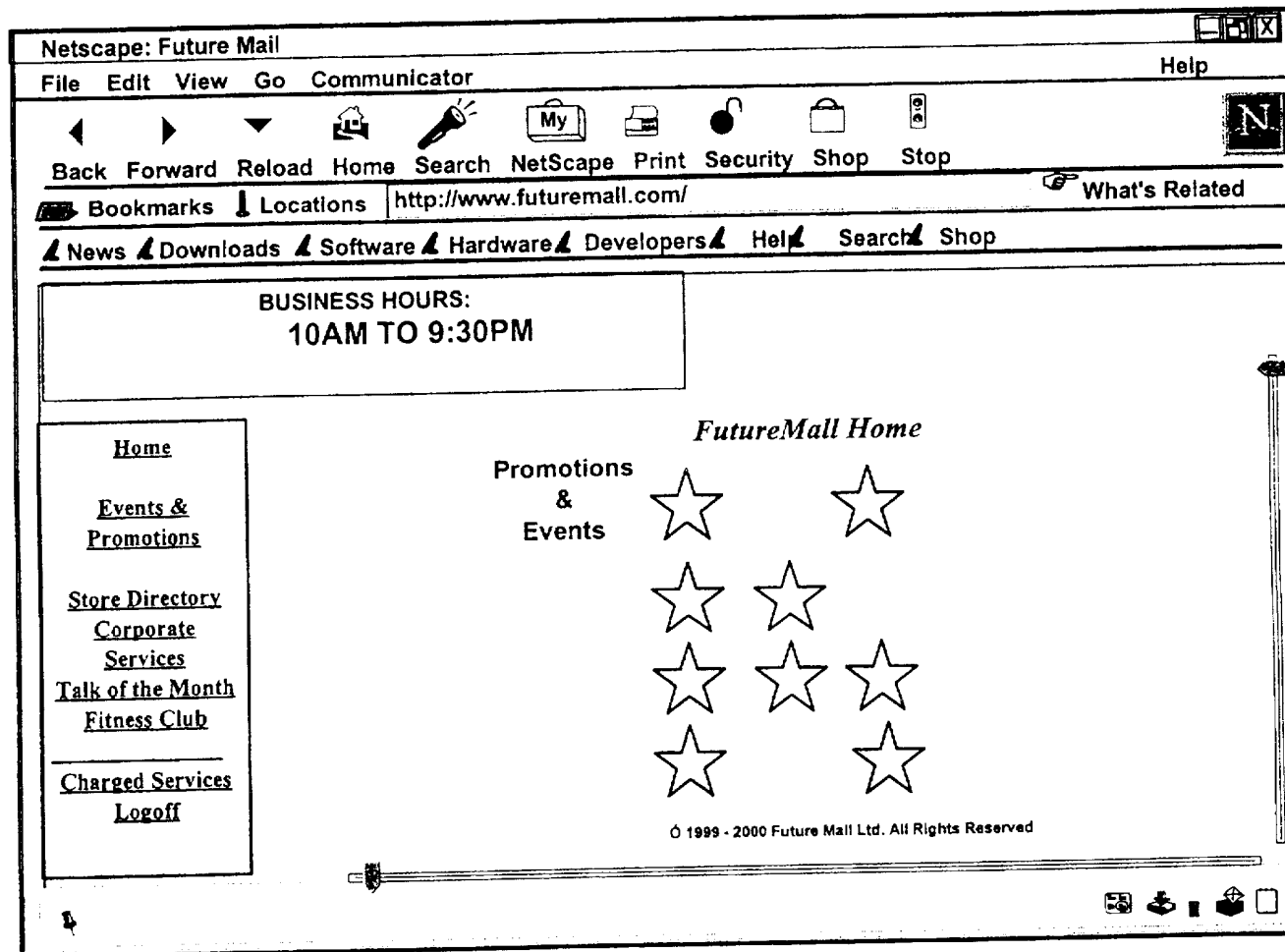


FIG. 3

400



4/8

FIG. 4

500

Netscape Login Form

Login Form

For access of privileged services,

Please fill out this form and submit it. Thank you

LOGIN:

PASSWORD:

CREDIT CARD:

ISP NAME:

LOGIN CODE:

If you came here by accident, click here to go to our home page: [HOME](#)

5/8

FIG. 5

600

login

Login:

Password:

Submit

Cancel

FIG. 6

7/8

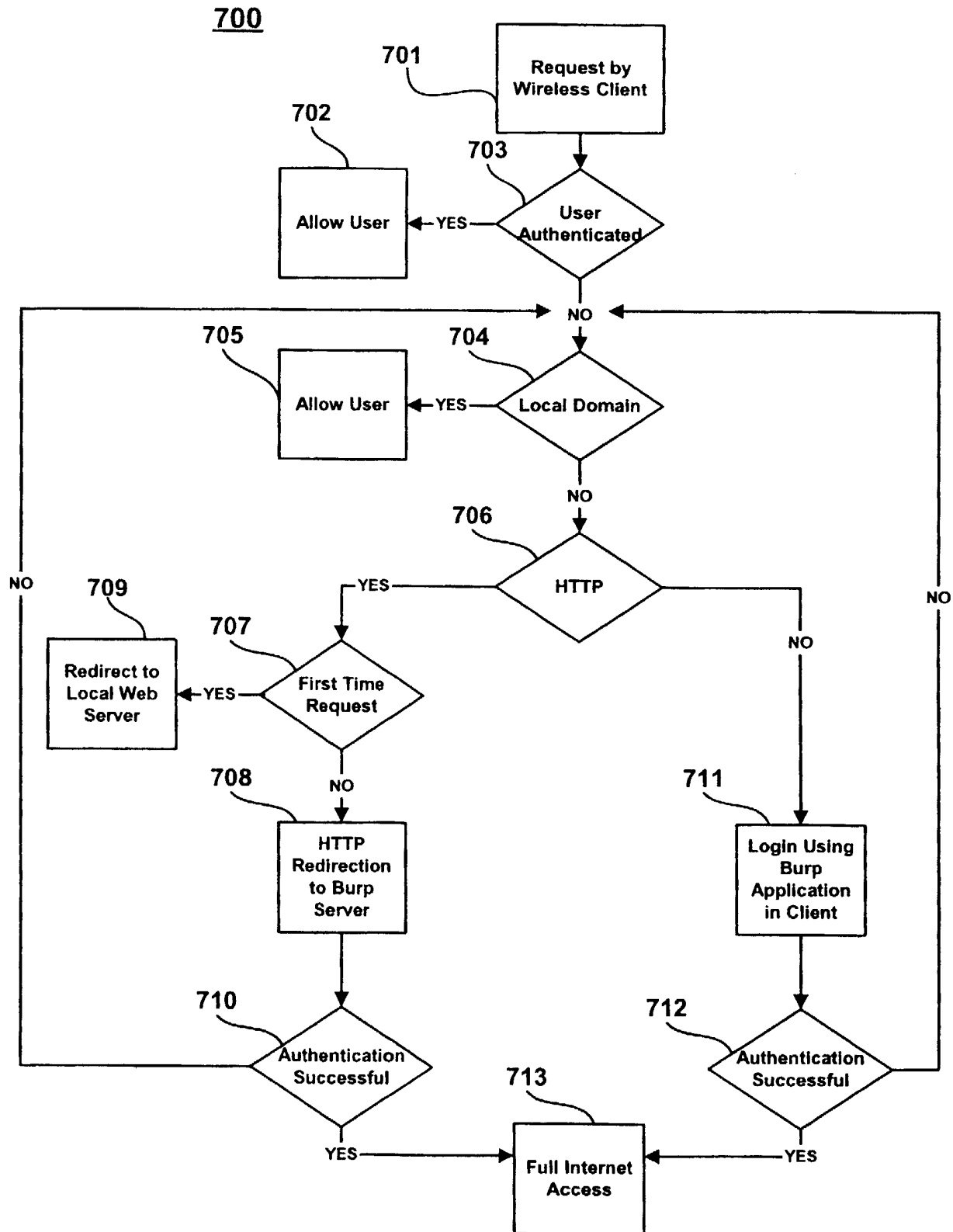
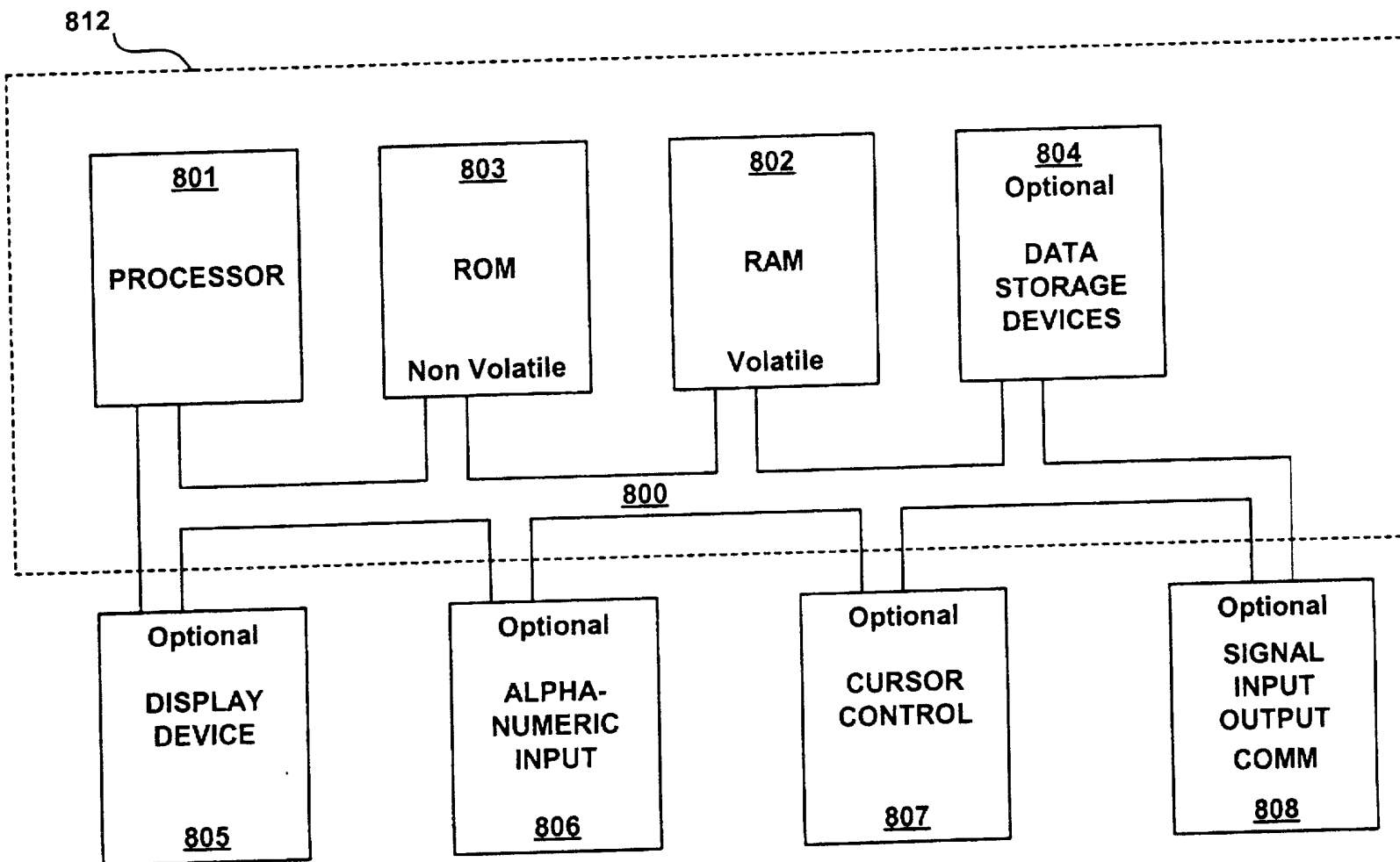


FIG. 7



8/8

FIG. 8

A METHOD AND SYSTEM FOR PROVIDING COMMUNICATIONS5 NETWORK ACCESS AND CONTROL IN A PUBLIC AREATECHNICAL FIELD

The present writing relates generally to accessing information and services via the Internet by using client devices. More specifically, the present invention pertains to a method and system for implementing location sensitive information access and retrieval from the Internet using a variety of different electronic devices.

BACKGROUND ART

15 The use of the Internet for electronic commerce and information retrieval has rapidly proliferated in today's modern world. Thousands of Internet sites and Web portals are constantly accessed by millions of users for obtaining information, news, entertainment, and the like, via the World Wide Web. Many aspects of everyday life are becoming electronically information based, and the access, control, and the use of such electronic information, through the use of various types of electronic devices, is never far from hand. For example, a mobile laptop computer allows access to banking functions (e.g., checking, bill paying, etc.), shopping (e.g., groceries, clothing, etc.), the weather, and other needs from a variety of different locations. A handheld computer device (e.g., a personal

information device such as a palmtop computer, cellphone, or the like) allows such access to be always close at hand. The emergence of wireless communication technologies provides such mobile computer devices with a degree of location independent communication capability. The increasing access to Internet connectivity (e.g., wireless communication, etc.) persuades many users to increasingly relying upon the Internet to fill many of their basic everyday needs.

There exists a number of different mechanisms for managing the access to, and the control of, Internet delivered services and information. Most users are familiar with the prior art methodology of Internet service providers (ISPs). A user pays a fee to an ISP in order to obtain access to the Internet, or more particularly, the World Wide Web. ISPs use a number of different prior art authentication and accounting methodologies in order to verify that the user being connected to the Internet is in fact a paying customer. Such methodologies have become commonly used, and generally function satisfactorily in static, non-mobile, situations. When users endeavor to connect the Internet using mobile technologies, such as, for example, wireless Ethernet, Bluetooth ^(R.T.M.) and the like, prior art methodologies used in static situations have proven inadequate.

Providing Internet access to mobile users has proven problematic. In many situations, it would be advantageous to provide Internet access to a non-static, mobile user. For example, it would be advantageous to provide Internet access to mobile, wireless client equipped passengers (e.g., via wireless PDAs, laptop computers, cellphones, etc.) as they move from place to place within an airport terminal. The Internet access would allow them to, for example, check airline flight times, ground transportation schedules, obtain a list of restaurants, check hotel reservations, or the like. Similarly, wireless Internet access in a

shopping mall or in a downtown business district would allow properly equipped users to obtain information with regard to commercial services, sales, ATM locations, and the like. However, providing the infrastructure to provide such Internet access requires a sizable investment. The prior art provides no
5 convenient, easily used, easily implemented mechanism for spreading the cost of such investment among the users.

There currently exists no mechanism for billing a mobile Internet user for accessing wireless Internet services for brief periods or intermittent periods of
10 time. For example, while a traditional ISP is able to charge a monthly, or yearly, fee for providing Internet access, during the brief time a traveler may require access an airport, there exists no convenient mechanism for billing the traveler for the provided Internet access. Although providing wireless Internet access to users in shopping districts would be advantageous, for example, such access
15 cannot cost effectively be provided, since there exists no convenient and easily implemented method of billing users for such access.

Thus, what is required is a solution that can provide Internet access to mobile, wireless client device equipped, Internet users, while also implementing a
20 convenient, easy-to-use, billing method for such users. What is required is a solution that can authenticate which users are paying, authenticated users, and ensure wireless Internet access is provided to those users. Additionally, what is required is a solution that can implement different levels of wireless Internet access in accordance with different classes of customers. The present invention
25 provides a novel solution to these requirements.

SUMMARY

Embodiments of the present invention comprise a method and system for providing communications network access and control in a public area.

Embodiments of the present invention provide Internet access to mobile, wireless client device equipped, Internet users, while also implementing a convenient, easy-to-use, billing method for such users. Embodiments of the present invention can authenticate which users are paying, authenticated users, and ensure Internet access is provided to those users. Additionally, embodiments of the present invention can implement different levels of Internet access in accordance with different classes of customers.

In one embodiment, the present invention is implemented as a wireless access method for providing communications network access (e.g., Web page browsing, instant messaging, e-mail, etc.) in a public area (e.g., a mall, airport, sports arena, etc.). The method includes the step of receiving a request to access a communications network from a client, such as a PDA, laptop, cellphone, or the like. A determination is then made as to whether the request is for access to a first area or a second area of the communications network. The first area can be a local domain of the communications network, such as, for example, a local Intranet of a shopping mall, airport, or the like. The second area can be the part of the communications network outside the local domain, such as, for example, popular sites or Web pages on the Internet. In response to receiving a request for access to the first area (e.g., local domain), access is provided to the services of the first area of the communications network. In response to receiving a request for access to the second area (e.g., Web pages and/or sites on the Internet), an authentication process is performed on the client. When the authentication is

successful, access is provided to the services of the second area of the communications network.

Depending upon the particular implementation, the authentication can be performed in accordance with standardized Web based authentication protocols or with a basic user registration protocols (BURP). The authentication can provide the mechanism whereby those clients seeking to access content outside the local domain can be charged for costs for providing such access. For example, users surfing the local, or internal, domain can do so freely (e.g., browsing advertisements, informational Web pages, event information, and the like), while those users wanting to view content outside the local domain can be prompted for credit card or other payment information and be notified of any necessary fees prior to having access provided to the external content. The authentication process can ensure those users accessing external content pay for such content, and can be used to provide different levels of Internet access in accordance with different classes of customers.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example and not by way of limitation in the Figures of the accompanying drawings, in which like reference numerals refer to similar elements, and in which:

5

Figure 1 shows a diagram of a system in accordance with one embodiment of the present invention.

10 Figure 2 shows a flow chart of the steps of a process in accordance with one embodiment of the present invention.

Figure 3 shows a diagram of a system in accordance with one embodiment of the present invention.

15 Figure 4 shows a diagram depicting a main, or default, HTML Web page in accordance with one embodiment of the present invention.

20 Figure 5 shows a diagram depicting a login Web page presented to the browser of client by the BURP server in accordance with one embodiment of the present invention.

Figure 6 shows an alternative login interface presentation in accordance with one embodiment of the present invention.

25 Figure 7 shows a flow chart of the steps of a process in accordance with one embodiment of the present invention.

Figure 8 shows a computer system in accordance with one embodiment of the present invention.

DETAILED DESCRIPTION

In the following detailed description of the present invention, a method and system for providing communications network access and control in a public area, numerous specific details are set forth in order to provide a thorough understanding of the present invention. However, it will be obvious to one skilled in the art that the present invention may be practiced without these specific details. In other instances well known methods, procedures, components, and circuits have not been described in detail as not to obscure aspects of the present invention unnecessarily.

10 Notation and Nomenclature:

Some portions of the detailed descriptions which follow are presented in terms of procedures, steps, logic blocks, processing, and other symbolic representations of operations on data bits within a computer memory. These descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. A procedure, computer executed step, logic block, process, etc., is here, and generally, conceived to be a self-consistent sequence of steps or instructions leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated in a computer system. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

25

It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the following discussions, it is appreciated that throughout the present invention, discussions utilizing terms such as "processing" or "computing" or "communicating" or "authenticating" or "registering" or "accessing" or the like, refer to the action and processes of a computer system (e.g., computer system 812 of Figure 8), or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

Description of the Embodiments:

Embodiments of the present invention provide communications network access and control in a public area. Embodiments of the present invention provide Internet access to mobile, wireless client device equipped, Internet users, while also implementing a convenient, easy-to-use, billing method for such users. Embodiments of the present invention can authenticate which users are paying, authenticated users, and ensure wireless Internet access is provided to those users. Additionally, embodiments of the present invention can implement different levels of wireless Internet access in accordance with different classes of customers. Although, embodiments of the present invention are described in the context of providing communications network access via wireless means, wired means of access can also be implemented. Embodiments of the present invention and their benefits are further described below.

Figure 1 shows a diagram of a system 100 in accordance with one embodiment of the present invention. System 100 depicts the basic components of a communications network access and control system in accordance with one embodiment of the present invention. As depicted in Figure 1, system 100 includes a local domain of a communications network 101 coupled to a gateway 102 to an external communications network, shown as external domain 103. A local server 110 and a local authentication server 120 are shown coupled to local domain 101. A client 140 is shown coupled to local domain 101 via a wireless access point (WAP) 130.

System 100 of the present embodiment implements a wireless access method for providing communications network access (e.g., Web page browsing, instant messaging, e-mail, etc.) in a public area (e.g., a mall, airport, sports arena, etc.). System 100 functions in part by receiving and fulfilling requests to access a communications network from clients, such as the client 140, for network based services and information. In this embodiment, client 140 is a digital electronic device, such as a PDA, laptop, cellphone, or the like, equipped for wireless network communication. Client 140 is coupled to the local domain 101 of the communications network via the wireless access point 130.

Upon receiving request for access from client 140, a determination is made as to whether the request is for access to a first area or a second area of the communications network. In this embodiment, the first area is the local domain 101, which is, for example, a local Internet of a shopping mall, airport, or the like. The second area is the part of the communications network outside the local domain 101, in this case external domain 103, comprising, for example, popular sites or Web pages on the Internet. In response to receiving a request for access

to the local domain 101, access is provided to the services of the local domain 101 of the communications network. Such services include, for example, Web pages provided by the local server 110. In response to receiving a request for access to the external domain 103 (e.g., Web pages and/or sites on the Internet), an authentication process is performed on the client 140. The authentication is performed by the authentication server 120. When the authentication is successful, access is provided to the client 140 to the services of the external domain 103 via the gateway 102.

Referring still to the system 100 embodiment of Figure 1, depending upon the particular requirements of the system operator (e.g., network access provider for a mall, airport, etc.), the authentication implemented by authentication server 120 can be performed in accordance with standardized Web based authentication protocols or with a basic user registration protocols (BURP). The authentication process implemented by authentication server 120 provides a mechanism whereby those clients (e.g., client 140) seeking to access content of the external domain 103 (e.g., Web pages or Internet sites on the Internet) can be charged for costs for providing such access. For example, users surfing the local domain 101 can do so freely (e.g., browsing mall advertisements, mall informational Web pages, mall shopping event information, and the like). Those users wanting to view content on the external domain 103 can be prompted for credit card or other payment information by authentication server 120, and be notified of any necessary fees prior to having access provided to the external content. The authentication process can ensure those users accessing external content of the external domain 103 pay for such content, and can be used to provide different levels of network access in accordance with different classes of customers.

(
It should be noted that although the system 100 embodiment is described in the context of providing communications network access via wireless means, wired means of access can also be implemented. For example, a client can gain access to system 100 and the authentication server 120 through a wired Ethernet
5 plug in connection at a network kiosk as opposed to the wireless access point 130.

Figure 2 shows a flow chart of the steps of a process 200 in accordance with one embodiment of the present invention. As depicted in Figure 2, process 200 depicts the operating steps of a communications network access and control
10 process as implemented by a public area network access system in accordance with the present invention (e.g., system 100).

Process 200 begins in step 201, where a request for access to a communications network is received from client (e.g., client 140). As described
15 above, in one embodiment, requests for network access are received wirelessly from clients via a wireless access point (e.g., wireless access point 130) coupled to the network. In another embodiment, requests are received via a wired Ethernet plug-in connection of, for example, an information kiosk.

20 In step 202, a determination is made as to whether the request is for access to a first area (e.g., local domain 101) or a second area (e.g., external domain 103) of the network. As described above, the local domain of the network can include local servers (e.g., local server 110) configured to provide Web pages and information or services tailored for the characteristics of the local area (e.g.,
25 airport, shopping mall, etc.). The external domain can include the servers and other services available on the vast resources of the Internet.

In step 203, when the requests for access to the second area of the network is received, an authentication process is performed on the client. As described above, the authentication process is implemented using an authentication server (e.g., authentication server 120) coupled to the first area of the network.

5

In step 204 and step 205, if the authentication process is successful, access is provided to the services on the second area of of the communications network. Successful authentication can include, for example, receiving credit card information from the user, receiving registration information from the user (e.g., name, address, etc.), network ID and password information, or the like.

10

In step 206, when the request for access to the first area is received as determined in step 202, access is freely provided to the information and services of the first area of the communications network. Alternatively, in the event of an unsuccessful authentication process as determined in step 204, process 200 proceeds to step 206 and provides access to the information and services of the first area.

15

In this manner, process 200 provides Internet access to mobile Internet users, while also implementing a convenient, easy-to-use, billing method for such users. Process 200 can authenticate which users are paying, authenticated users, and ensure Internet access is provided to those users. Additionally, process 200 can implement different levels of Internet access in accordance with different classes of customers.

20

25

Figure 3 shows a diagram of a system 300 in accordance with one embodiment of the present invention. System 300, while being similar to system

100 of Figure 1, shows components of a communications network access and control system embodiment in greater detail. As depicted in Figure 3, system 300 includes a client 340 coupled to a local network 301 via a wireless access point 330. A BURP server 320, a AAA server 321, and a local Web server 310 are
5 coupled to the local network 301. The local network 301 is coupled to the Internet 303 via a firewall 350.

System 300 of the present embodiment functions in a manner substantially similar to system 100 of Figure 1. Access to the local network 301
10 is provided wirelessly, via a wireless access point 330. Local content is served to the client 340 via the local Web server 310. Authentication is performed in accordance with either BURP protocols using BURP server 320 or AAA protocols using AAA server 321.

15 System 300 functions by providing network connectivity and other value added services to wireless clients (e.g., wireless client 340) at public places such as Shopping Malls, Airports, etc., as described above. In this embodiment, wireless access point 330 is configured to provide different levels of access to services, such as partial intranet (e.g., local network 301) access, partial access to certain
20 applications like ftp, web and telnet, full access, etc., to different connected clients. The wireless access point 330 functions with the servers 320 and 321 to authenticate users according to the account they may, or may not, have. In accordance with the results of such authentication, users are allowed/denied services in accordance with their level of subscription.

25 Referring still to Figure 3, in the present embodiment, wireless access point 330 waits for a wireless client (e.g., client 340) to connect to the wired local

network 301. When the client 340 makes a DHCP request, the client 340 will be put onto an access control list 331 with a default status that only allows the client 340 to roam the local network 301, or the local domain. Once the client 340 successfully obtains an IP address, the client 340 can enjoy the free local services offered, for example, by the local Web server 310.

In the present embodiment, when the client 340 tries to access non-local domains such as the Internet 303, the access point 330 will react in the following manner. If the client 340 is using a browser and is downloading a default homepage (e.g., assuming that the Web page resides somewhere in the Internet 303), the wireless access point 330 redirects the browser of client 340 to the local web server 310. The web server 310 then pushes the main, or default, Web page to the client's browser, an example of which is shown in Figure 4 below.

In the present embodiment, the BURP server 320 waits for the IP address of the client 340 from the access point 330. When a request is made by the access point 330 to authenticate a client, the server 320 opens a browser form for the client 340 to authenticate if a browser on client 340 is open. If the client 340 is using an application other than a browser, BURP server 320 authenticates using an authentication application running in the client 340. The server 320 passes the information from the client 340 to the AAA server 321. Depending on the result of the authentication, the server 320 lets the access point 330 know to change its access control list 331 with respect to the client 340.

It should be noted that with respect to the client 340, there are no special applications required if a browser is used to access the local network 301 or Internet 303. The authentication is performed via the browser.

Figure 4 shows a diagram depicting a main, or default, Web page 400 in accordance with one embodiment of the present invention. The main Web page 400 is the Web page to which the browser of client 340 is redirected. The Web page 400 typically functions as the "front page" or "splash page" of the local network 301. In the present embodiment, the access point 330 updates the access control list 331 to make sure that the client 340 is not redirected to the Web page 400 a second time.

10 In the present embodiment, if the client 340 is using a browser and is attempting to access the Internet 303 for the second time, the access point 330 redirects the browser of client 340 to the BURP server 320. The BURP server 320 will then try to authenticate the client 340 through a login Web page, an example of which is shown in Figure 5 below.

15 Figure 5 shows a diagram depicting a login Web page 500 presented to the browser of client 340 by the BURP server 320 in accordance with one embodiment of the present invention. As shown in Figure 5, the login Web page 500 prompts the user for a login identification and password, credit card, ISP
20 information, and login code.

Figure 6 shows an alternative login interface presentation 600 in accordance with one embodiment of the present invention. In the present embodiment, if the client 340 is using other applications besides a Web browser, such as FTP or telnet, the access point 330 sends the IP address of client 340 to the BURP server 320. The BURP server 320 will then try to authenticate the client 340 through a BURP client software process. Once successfully
25

authenticated, the client 340 is allowed to access both the local network 301 and the Internet 303. The access point 330 updates the status of client 340 in the access control list 331 accordingly to allow local and Internet traffic from the authenticated client 340.

5

Figure 7 shows a flow chart of the steps of a process 700 in accordance with one embodiment of the present invention. Process 700 depicts the operating steps as performed by the components of system 300 of Figure 3.

10

Process 700 begins in step 701 when a request from the client 340 is received by the access point 330. In step 703, the wireless access point 330 determines whether the client 340 is authenticated. In step 702, if the user of client 340 has been previously authenticated, full access for the user is allowed. If the user has not been previously authenticated, process 700 proceeds to step 704.

15

In step 704, the wireless access point 330 determines whether the request from the client 340 is for a local domain service. In step 705, if the request is for local domain 301 service, full access to the local service is provided. In step 706, when the request is for an Internet 303 service, a determination is made as to whether the client 340 is using a Web browser or not. If a Web browser is being used, process 700 proceeds to step 707. If a Web browser is not being used, process 700 proceeds to step 711. In step 707, if the request is a first-time request, process 700 proceeds to step 709 where the request is redirected to the local web server 310. Otherwise, process 700 proceeds to step 708, where the request is redirected to the BURP server 320. In step 710, if the authentication is successful, full Internet access is provided in step 713.

25

In step 706, when the client 340 is not using a Web browser, process 700 proceeds to step 711, where the client 340 executes a login process using, for example, a BURP application running within the client 340. In step 712, if the authentication is successful, full Internet access is provided in step 713.

5

Computer System Platform:

With reference now to Figure 8, a computer system 812 in accordance with one embodiment of the present invention is shown. Computer system 812 shows the components of a computer system in accordance with one embodiment of the present invention that provides the execution platform for implementing certain software based functionality of the present invention. As described above, certain processes and steps of the present invention are realized, in one embodiment, as a series of instructions (e.g., software program) that reside within computer readable memory units of a computer system (e.g., system 812) and are executed by the processor(s) of system 812. When executed, the instructions cause the computer system 812 to implement the functionality of the present invention as described above.

In general, computer system 812 shows the basic components of a computer system used to implement "server" machines and "client" machines. Additionally, computer system 812 shows the basic components of an embedded computer system as implemented within a wireless access point, firewall, or gateway. Computer system 812 comprises an address/data bus 800 for communicating information, one or more central processors 801 coupled with the bus 800 for processing information and instructions, a computer readable volatile memory unit 802 (e.g., random access memory, static RAM, dynamic, RAM, etc.) coupled with the bus 800 for storing information and instructions for the central

processor(s) 801, a computer readable non-volatile memory unit (e.g., read only memory, programmable ROM, flash memory, EPROM, EEPROM, etc.) coupled with the bus 800 for storing static information and instructions for the processor(s) 801. System 812 also includes a mass storage computer readable data storage device 804 such as a magnetic or optical disk and disk drive coupled with the bus 800 for storing information and instructions. Optionally, system 812 can include a display device 805 coupled to the bus 800 for displaying information to the computer user, an alphanumeric input device 806 including alphanumeric and function keys coupled to the bus 800 for communicating information and command selections to the central processor(s) 801, a cursor control device 807 coupled to the bus for communicating user input information and command selections to the central processor(s) 801, and a signal generating device 808 coupled to the bus 800 for communicating command selections to the processor(s) 801.

Thus, embodiments herein described provide communications network access and control in a public area. The embodiments provide Internet access to mobile Internet users, while also implementing a convenient, easy-to-use, billing method for such users. The embodiments can authenticate which users are paying, authenticated users, and ensure Internet access is provided to those users. Additionally, embodiments of the present invention can implement different levels of Internet access in accordance with different classes of customers.

In summary, this writing discloses a method for providing communications network access in a public area. The method includes the step of receiving a request to access a communications

network from a client. A determination is then made as to whether the request is for access to a first area or a second area of the communications network. The first area can be a local domain of the communications network. The second area can be the part of the communications network outside the local domain, such as the Internet. In response to receiving a request for access to the first area, access is provided to the services of the first area of the communications network. In response to receiving a request for access to the second area, an authentication process is performed on the client. When the authentication is successful, access is provided to the services of the second area of the communications network. The authentication can be performed in accordance with a Web based authentication protocol. The authentication can also be performed in accordance with a basic user registration protocol.

The foregoing descriptions of specific embodiments have been presented for purposes of illustration and description. They are not intended to be exhaustive or to limit the invention to the precise forms disclosed, and many modifications and variations are possible in light of the above teaching. The embodiments were chosen and described in order best to explain the principles of the invention and its practical application, thereby to enable others skilled in the art best to utilize the invention and various embodiments with various modifications as are suited to the particular use contemplated. It is intended that the scope of the invention be defined by the Claims appended hereto and their equivalents.

CLAIMS:

1. A method for providing communications network access and control in a public area, comprising:
 - 5 receiving a request to access a communications network from a client;
determining whether the request is for access to a first area or a second area of the communications network;
in response to receiving a request for access to the first area, providing access to services on the first area of the communications network;
 - 10 in response to receiving a request for access to the second area, performing an authentication on the client; and
providing access to services on the second area of the communications network when the authentication is successful.
- 15 2. The method of claim 1 wherein the first area is a local domain of the communications network and the second area is outside the local domain of the communications network.
3. The method of claim 2 wherein the second area comprises the
20 Internet.
4. The method of any preceding claim further comprising:
performing a redirect of the request to access the communications network from the client to a server within the local domain; and
25 sending a default Web page to the client from the server.
5. The method of claim 4 further comprising:
performing the authentication on the client in response to receiving a request from the client to access a Web page outside the local domain.

30

6. The method of any preceding claim wherein the request is received via a wireless access point coupled to the communications network.
7. The method of any preceding claim wherein the authentication is performed in accordance with a Web based authentication protocol.
8. The method of any of claims 1 to 6 wherein the authentication is performed in accordance with a basic user registration protocol.
9. A system for providing communications network access and control in a public area, comprising:
a wireless access point for receiving a request to access a communications network from a client, the wireless access point configured to determine whether the request is for access to a first area or a second area of the communications network;
an authentication server coupled to the wireless access point for performing an authentication on the client, wherein the wireless access point provides access to services on the first area of the communications network for requests to access the first area, and wherein access to services on the second area of the communications network is provided when the authentication is successful.
10. The system of claim 9 wherein the wireless access point is coupled to the authentication server via the first area of the communications network.
11. A system for providing communications network access and control in a public area, comprising:
means for receiving a request to access a communications network from a client;
means for determining whether the request is for access to a first area or a second area of the communications network;

in response to receiving a request for access to the first area, means for providing access to services on the first area of the communications network;

- in response to receiving a request for access to the second area,
 5 means for performing an authentication on the client; and
 means for providing access to services on the second area of the communications network when the authentication is successful.

12. The system of claim 11 wherein the request is arranged to be
 10 received via a wireless access point coupled to the communications network.

13. The system of any of claims 9 to 12 wherein the second area comprises the Internet.

15 14. The system of any of claims 9 to 13 wherein the first area is a local domain of the communications network and the second area is outside the local domain of the communications network.

15 15. The system of claim 14 wherein the wireless access point is
 20 configured to perform a redirect of the request to access the communications network from the client to a server within the local domain sent a default Web page to the client from the server.

16. The system of claim 15 wherein the authentication server is
 25 configured to perform the authentication on the client in response to the wireless access point receiving a request from the client to access a Web page outside the local domain.

17. The system of claim 14 further comprising:

means for performing a redirect of the request to access the communications network from the client to a server within the local domain; and

means for sending a default Web page to the client from the server.

5

18. The system of claim 17 further comprising:

means for performing the authentication on the client in response to receiving a request from the client to access a Web page outside the local domain.

10

19. The system of any of claims 9 to 18 wherein the authentication is arranged to be performed in accordance with a Web based authentication protocol.

15

20. The system of any of claims 9 to 18 wherein the authentication is arranged to be performed in accordance with a basic user registration protocol.

20

21. A system for providing communications network access and control in a public area, the system being substantially as described hereinabove with reference to Figures 1 to 5, 7 and 8 optionally as modified in accordance with Figure 6 of the accompanying drawings.

25

22. A method for providing communications network access and control in a public area, the method being substantially as described hereinabove with reference to Figures 1 to 5, 7 and 8 optionally as modified in accordance with Figure 6 of the accompanying drawings

30



INVESTOR IN PEOPLE

Application No: GB 0306975.4
Claims searched: 1-22

25

Examiner: John Betts
Date of search: 17 September 2003

Patents Act 1977 : Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
X	1-2, 6, 9,11-14	GB2360914 A (Psion) see especially p 4. ll.24-27
X	1-2, 6, 9,11-14	WO2001/037517 A2 (Wayport) see particularly p.3 ll.3-11
X	1-2, 6, 9,11-14	US20020022483 A1 (Wayport) see p.3 para 36

Categories:

X Document indicating lack of novelty or inventive step	A Document indicating technological background and/or state of the art.
Y Document indicating lack of inventive step if combined with one or more other documents of same category.	P Document published on or after the declared priority date but before the filing date of this invention.
& Member of the same patent family	E Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC^V:

H4L G4A

Worldwide search of patent documents classified in the following areas of the IPC⁷:

H04Q H04L G06F

The following online and other databases have been used in the preparation of this search report:

EPODOC, WPI, JAPIO