WiFi SMS LOGIN SOLUTION FOR INBOUND (GSM) ROAMERS

FIELD OF INVENTION

The present invention relates to a method and system for wireless network or internet access particularly though not solely for access dependent on cellular roaming subscriptions.

BACKGROUND

The Internet consists of a large number of computers, devices and networks all interconnected via communications links. Users gain access to the Internet via communications service providers, which can be, among others, Internet service providers, wireless Internet service providers, mobile or cellular telephone service providers, or fixed line service providers.

Such communications service providers typically have a limited footprint, that is, they can only provide local access to the Internet in certain areas. For example, a mobile telephone service provider may only provide access to the Internet when the mobile telephone user is within the defined coverage area of the said service provider's mobile network. Another example would be an internet service provider that maintains a national telephone number to deliver Internet access nationwide, but is unable to provide a local access number for a subscriber who travels out of the country of service.

There are a number of access mechanisms for providing roaming local internet access. The most common is via dial-up access, where at least one local access telephone (PSTN) number is provided to travellers to each region. Generally, dial-up roaming access is managed by client software that runs on the guest's computer. This software maintains a searchable database of access numbers for every region and will automatically dial an appropriate local access number based on the guest's indicated current location.

A new and emerging method for providing roaming internet access is the IEEE 802.11 series of Wireless LAN technologies, known as WLAN or WiFi "hot-spots." Because WLAN hotspots do not require the use of a telephone (PSTN) number, access is typically currently managed by having a "walled garden" that allows any user to login to the hotspot, but not go beyond the boundaries of the hotspot. All traffic out of the hotspot is blocked, and all World-

Wide Web (HTTP) requests are redirected to a "landing page" which will allow access to the internet if conditions are met.

One area where such wireless access is becoming popular is airports and other travel access points. One prospect of providing such access is to overseas roamers, also known as inbound roamers (IBR). In prior art systems such as that disclosed in US 6,510,323 to Telefonaktiebolaget LM Ericsson (publ), roamers receive general information depending on the location of the roamer. For example, a welcome message could be sent via the Short Message Service (SMS).

In another prior art system, disclosed in US 6,101,387 to Telefonaktiebolaget LM Ericsson, a roamer is provided with services that are available to that particular network/base station.

Currently in Singapore, SingTel (www.singtel.com) allow inbound roamers to register for wireless internet access by dialing a code "*186" to SingTel. A user identification and password for wireless internet access are provided by return text message.

In order to facilitate global roaming for cellular phones the registration and/or location of mobile telephones that are connected to the system needs to be ascertainable. When a mobile telephone user subscribes to a GSM network for example, subscriber details are stored in a register called the Home Location Register (HLR). As the mobile telephone moves from one Base Station Subsystem (BSS) to another, it reports the change in service to the new BSS. The new BSS then enrols the subscriber in a Visitor Location Register (VLR) associated with the new BSS, which updates and retrieves subscriber information from the HLR. At the same time, subscriber information stored in the old VLR associated the old BSS is deleted. Thus, by inspecting the VLR and/or HLR of a GSM system, it is possible to determine which mobile telephone is associated with or connected to that GSM system.

SUMMARY OF THE INVENTION

It is therefore a object of the present invention to provide a method or system for wireless network or internet access which goes some way to overcoming the above mentioned disadvantages in the prior art or which will at least provide the public with a useful choice.

Accordingly in a first aspect the present invention consists in a system for providing wireless network or internet access comprising:

a monitor configured to detect status of a wireless device associated with a user or in the control of said user,

an access point providing network or internet access dependent on a condition,

means for notifying or alerting a user of any change in said access, said status or said condition.

In a second aspect the present invention may be broadly said to consist in a method of allowing access to a network or the Internet for a user comprising the steps of:

monitoring status of a wireless device associated with said user or in the control of said user,

providing network or Internet access dependant on a condition,

notifying or alerting said user in response to any changes in said status or said access or said condition.

Preferably said condition relates to a predetermined period of access.

Preferably said notification or alert relates to said device not being connected to a predetermined list of networks.

Preferably said condition relates to said status of said device.

Preferably said status relates to the network said device is connected to.

Preferably said method further comprises the step of issuing a user ID and password depending on said status, and adding the same to a list of valid user ID's and passwords.

Preferably said condition relates to entering a user ID and password which match an entry on said valid user ID list.

Preferably said predetermined period expires said user ID and password are removed from said valid user ID list.

To those skilled in the art to which the invention relates, many changes in construction and widely differing embodiments and applications of the invention will suggest themselves without departing from the scope of the invention as defined in the appended claims. The disclosures and the descriptions herein are purely illustrative and are not intended to be in any sense limiting.

The invention consists in the foregoing and also envisages constructions of which the following gives examples.

BRIEF DESCRIPTION OF THE DRAWINGS

The preferred forms of the present invention will now be described with reference to the accompanying drawings in which:

Figure 1 is a functional block diagram of wireless network when connected to a mobile telephone network;

Figure 2 is a diagram illustrating an example connectivity between the wireless network and a mobile telephone network;

Figure 3 is a diagram illustrating the wireless access authentication process;

Figure 4 is a diagram illustrating the wireless network in one embodiment;

Figure 5 is a diagram illustrating an example accounting and billing system for the wireless network;

Figure 6 is a flow chart illustrating the steps involved when wireless access is first requested;

Figure 7 is a flow chart illustrating the steps involved during subsequent requests for wireless access;

Figure 8 is a flow chart illustrating the processes involved in providing the wireless access;

Figure 9 is a flow chart illustrating the monitoring process for monitoring a mobile network;

Figure 10 is an image showing a mobile telephone requesting wireless access;

Figure 11 is a diagram illustrating an example service announcement and an example text message providing wireless access information;

Figure 12 is a diagram illustrating how the wireless access information may be used for wireless access;

Figure 13 is a diagram showing how a message may provided to a user of the wireless network; and

Figure 14 is a diagram showing an example message that is sent when the mobile telephone switches mobile networks.

DETAILED DESCRIPTION

With reference to Figure 1, a wireless network 1, is associated with a further communications network 2, for example a mobile telephone network 2. In this arrangement, a wireless device 3 of a user is monitored, for example is mobile telephone 3.

Other networks or systems that may be connected to the wireless network 1 include a paging network in which the wireless device is a pager, or a Local Area Network (LAN) that may provide authorised users with wireless devices such as laptops and Personal Digital Assistants (PDAs) that have wireless capabilities. In these cases, the status of device e.g. the pager, laptop or PDA may be monitored.

In the arrangement of Figure 1, the access to the wireless network is obtained as follows:

(A) When the user activates or registers the mobile telephone 3 in the vicinity of the mobile telephone network 2 for the first time, a notification is preferably provided to the user. In one form, the notification is a welcome text message, which informs the user that he/she can get free Wireless Internet Access at Wireless Hotspots and may provide details regarding access to the wireless network – such as the duration of the free trial and how to request access e.g. by dialling *WiFi or *9434. The user then sends this access request to the Mobile Switching Centre (MSC) 4 of the mobile network 2 when wireless access is required.

(B) The access request received by the MSC 4 is then forwarded to the mobile-wireless interface system 5. As its name suggests, the mobile-wireless interface system 5 acts as an interface between the mobile telephone network 2 and the wireless network 1.

(C) Details of the mobile phone 3 are retrieved from the Overseas Roaming Partners' Home Location Register (HLR) or the Visitor Location Register (VLR) 6 by the mobile-wireless interface system 5. In one example, the Mobile Station International ISDN Number (MSISDN) of the mobile telephone 3, its International Mobile Subscriber Identity (IMSI) and its VLR information are retrieved. This information are essential for successful delivery of the SMS which is to be explained in (D).

(D) The mobile-wireless interface system 5 generates a user identification and suitable Personal Identification Number (PIN) for access to the wireless network 1. The

user identification could be the mobile telephone's MSISDN or the International Mobile Subscriber Identity (IMSI) of the mobile telephone user and the PIN is generated by a random number generator, or other algorithms as are known in the art. Once generated, both user identification and PIN are stored in a secure database and server, such as a Remote Authentication Dial-In User Service or RADIUS server. The user identification and PIN are also sent to the mobile telephone 3, for example in a text message. For this, the provisions under Signalling System 7- Mobile Application Part (SS7-MAP) may be used. As in known in the art, MAP messages in SS7 protocol may be sent between mobile telephones and databases to support user authentication, equipment identification, and roaming. By using SS7-MAP, the international gateway/toll could be bypassed. In the event if there is no reply from the Overseas Roaming Partners' HLR on the roamer's IMSI and VLR information, the generated user identification and PIN would be forwarded to the 3rd Party SMS Roaming Partner (NILCOM or CITIC) for the delivery of the SMS.

(E) Now that the mobile telephone user has a valid user identification and password, the user may access the wireless network. Where the user wireless access equipment is a laptop 7 having wireless capabilities, the user can log into the wireless network 1 by activating the laptop 7 in the vicinity of a wireless access point or hotspot 8.

(F) Once the login information is submitted, preferably using secure browser, the information is forwarded to the wireless service gateway 9 to authenticate the user identification and PIN combination. For this authentication, the wireless service gateway 9 verifies the submitted user identification-PIN combination with the RADIUS server in the mobile-wireless interface system 5.

(G) If the user identification and PIN combination is successfully verified, the user will be granted accesses to the wireless network 1 via the hotspot 8. In one embodiment, an initial free trial access is given the user to try out the wireless network 1. The free trial could be time-limited, for example a 15-minute free trial. This would encourage the user to at least sample the wireless service that is available.

(H) The user must keep their cellular phone connected to the affiliated network in order to get the full free trial. If the cellular phone does not stay connected a pop up box indicates that free access will not continue unless the cellular phone is connected again.

(I) Once the user logs out of the wireless network 1, or where the free trial period expires, usage data is sent to the mobile-wireless interface system 5. This is then stored in a database to keep track of users that have used the wireless network 1. Such information would be required to later determine which users have exhausted their free trial of the wireless network 1. Alternatively, where the system is a pay-per-use system, usage data will be required to compile an accurate bill.

It will be appreciated by one skilled in the art that other configurations are possible, for example the welcome notification, and registration steps could be combined and/or carried out using other protocols such as Wireless Application Protocal (WAP), bluetooth or the like using an interaction interface. Alternatively an access code could be manually generated using the users' cellular phone number, and even manually provided, e.g. on a slip of paper.

Figure 2 illustrates, the connectivity of the mobile telephone network 2 to the wireless network 1. Three interlinked systems make up the network – the mobile telephone system 2, the wireless access system 10 and the mobile-wireless interface system 5. The wireless network 1 is a combination of the wireless access system 10 and the mobile-wireless interface system 5.

The mobile telephone network 2 comprises the Base Station Subsystem (BSS) 11, the Base Station Controller (BSC) 12, the Mobile Switching Centre (MSC) 4, the Home Location Register/Visitor Location Register (HLR/VLR) 6 and the International Switching Centre (ISC) 14. As is known in the art, this network functions to provide a mobile communication platform for the mobile telephone 3. For the sake of clarity, many interconnections and/or components have been omitted from the diagram. Those skilled in the art will be familiar with these interconnections and/or components, as the preferred form shown bears close resemblance to known GSM systems. If systems other than GSM are employed, equivalent-

functioning components and/or interconnections may take the place of the aforementioned components and/or interconnections.

The wireless access system 10, which provides users with basic wireless network access, comprises the Internet 15 and proxy RADIUS server 16 in communication with a wireless subscriber gateway 9. Connected to this gateway are wireless access points or hotspots 8. In the preferred embodiment, a WiFi system is employed, having WiFi hotspots. As shown in the diagram, user equipment with wireless capabilities such as laptop 7 and Personal Digital Assistants (PDA) 17 can connect to the Internet 15 via this wireless network system. To connect to the wireless network, the users must provide suitable identification that would be verified by the proxy RADIUS server 16.

The mobile-wireless interface system 5 interfaces the mobile telephone system 2 and the wireless access system 10. A detector platform 18 is provided, which detects the entry of the mobile telephone 3 into mobile network 2. This entry occurs when a local roamer enters the BSS 11 and registers in the VLR 6. Also, this could be extended to include overseas roamers, also known as inbound roamers, provided the mobile network 2 is able to handle international roaming. A database 19 connected to the detector platform 18 allows the interface system 5 to record details associated with the mobile telephone 3 such as the MSISDN.

In one embodiment, communication between the mobile telephone 3 and the interface system 5 of the invention is carried out either by a telephone call or via text messages using SMS. However any other communication method is possible also. For the SMS application, a Short Message Switching Centre (SMSC) should be provided. Preferably, the SMSC is incorporated into server 20. The SMSC should be able to access information in the database 19 to retrieve details such as the MSISDN or the IMSI. This is necessary if the MSISDN or IMSI is adopted as the user identification, which would be sent to the user via a text message. Under an SS7 communication, the SMSC is connected to the mobile telephone network 2, in particular to the MSC 4. This allows the SMSC to route text messages to the mobile phone 3 which is connected to the mobile telephone network 2.

Additionally, an interactive server could be provided in the server 20. This portion of the server 20 processes the calls to the wireless request number, such as *WiFi. For this

reason, the interactive server is connected to the mobile network MSC 4. In one embodiment, the interactivity is a voice message that is played over the request call. The voice message would inform the user that a suitable user identification and PIN will be sent to the mobile telephone 3. Once this is complete, the call is terminated and the interactive server proceeds to invoke a PIN generator, which is preferably also incorporated in the server 20. The PIN generator, which is preferably a random number generator, will generate the PIN and store the PIN value in the RADIUS server database 21. The RADIUS server database is connectable to the proxy RADIUS server 16, so that both possess an up-to-date record of valid user identifications and PINs. The PIN generator of the server 20 is in communication with the SMSC, so that once a PIN is generated, it may be sent to the mobile telephone user via a text message.

Figure 3 shows the flow of information in a typical subscriber authentication situation using the RADIUS protocol. As previously shown in Figure 2, the mobile phone 3 requests access to the wireless network via wireless user equipment 7, in this case a laptop, once it is in the vicinity of the wireless access point 8. The access request will include the user authentication details, such as the user identification and PIN. The wireless service gateway 9 then routes the access request to the proxy RADIUS 16.

The proxy RADIUS 16 is a RADIUS server that forwards authentication requests from network access servers, which is the wireless service gateway 9 in this case, to a remote RADIUS server, which is the server 20. The proxy RADIUS 16 also passes replies from the server 20 back to the wireless service gateway 9. Most commonly, this feature enables cooperating Internet service providers (ISPs) to handle dial-in service requests from each other's users. The proxy RADIUS could include a proxy file created in the */etc/raddb* directory on the forwarding server and, if necessary, on the remote server. Each line in the proxy file could contain the hostname or IP address of a remote server, the secret shared between the forwarding server and the remote server, and the realm of the remote server in the proxy chain. Each entry can specify the ports the remote server uses for RADIUS authentication and accounting as well as certain keywords to affect server behavior.

Referring to Figure 4, the connectivity of the main components between the mobile network 2, the wireless network 1 and the mobile-wireless interface system 5 is shown. As previously shown in Figure 2, the main connection between the mobile and wireless networks

is the SS7 link between the MSC 4 and the server 20. In Figure 4, the portion of the server 20 which handles the main connection is shown as a link gateway 22. In the most preferred embodiment, the link gateway 22 is an MEx Link SMS Gateway. The link gateway 22 functions to firstly receive the wireless access request from the user. Upon receipt of the request, the link gateway 22 invokes a request to the PIN generator portion of the server 20 for the generation of a PIN. The link gateway 22 also functions to query the HLR to obtain the user's MSISDN information to be used as user identification (as described in steps C and D in Figure 1). Finally, the link gateway 22 will send the user identification and PIN to the user. In the preferred system employing an MEx Link SMS Gateway, the user identification and PIN incorporated in a text message that is sent to the user's mobile telephone via SMS.

Also as previously shown in Figure 2, the wireless network 1 includes a RADIUS server database 21. Beyond storing the user identification and PIN for authentication purposes, the RADIUS server database 21 can serve the data storage needs of the wireless network 1. It also provides a means for fast-access to critical information such as operational data, system configurations, messaging detail records, service usage and the like.

To provide operation, administration and maintenance (OAM) services for wireless network 1, including the interaction between the wireless network 1 and the mobile network 2, a service provisioning server 23 is included in the wireless network 1. The service provisioning server 23 basically hides the complexity of the proposed network access system by employing user-friendly interfaces. The service provisioning server 23 provides graphical interfaces for systems administrators to administer, control and maintain the system and services. OAM items such as administration of users, resource control, call traffic monitoring and the like can thus be readily accessed. In addition, as this module can be implemented as a client-server and web-based based, system administrations can readily perform OAM activities remotely via a TCP/IP computer network.

In addition, the service provisioning server 23 can also function as a centralised management server for the proposed system. In this configuration, the service provisioning server 23 allows the proposed network access system to integrate with existing centralised management systems for centralised monitoring and administration purposes.

Once the processes involved in interfacing the mobile network 2 with the wireless network 1 is complete, there will exist a communication link between the mobile network 2 and the wireless network 1, specifically via the wireless service gateway 9. Here, management and billing systems 24 could be provided, such as known Network Management Systems (NMS) or Vantive Systems.

Figure 5 shows a flow chart of the processes involved for accessing the wireless network of the invention, where a free trial of the wireless network is provided. As previously mentioned, this free trial is preferably time-limited. The time limit could be, for instance, 15 minutes. It will be appreciated that the requirement of a time-limit and/or the limit value itself will be configurable, dependent on the service provider.

When a user registers a wireless device within the local network, for example a mobile telephone 3 registering in the network VLR 6 and if the user is in the vicinity of a wireless access point, such as a hotspot 8, the wireless network 1 of the invention will notify the user of the wireless access availability. In a highly preferred embodiment, this notification is via a welcome text message. This text message would inform the user of eligibility for wireless access, such as the existence of any free trial, and how to obtain this wireless access, e.g. by dialling *WiFi.

In step 500, the mobile telephone user decides to proceed with the free trial offered and dials the wireless request number *WiFi. When the mobile-wireless interface system 5 receives this request, it firstly determines whether the free trial period for that particular mobile telephone 3 has been exhausted, shown as step 502. This could be done by the interactive server portion of the server 20 appropriately checking the system database 19; in particular for an entry of the mobile telephone MSISDN and a corresponding entry of elapsed free trial time. If the free trial has not elapsed, the mobile-wireless interface system 5 instructs the generation of a PIN in the PIN generator of the server 20. The generated PIN along with the user identification is the transmitted to the mobile telephone 3. As indicated earlier, this is done via a text message, shown in step 504.

In step 506, the user utilises the obtained user identification and PIN to access the wireless network 1. In a preferred system, the user will only need to open a web browser or

equivalent network or Internet accessing software on a wireless device such as a laptop before logging in a walled garden.

Once the user has exhausted the free trial period, shown in step 508, the user is prompted for payment to proceed. In steps 510 and 512, the example payment options are given as mobile payment and credit card payment. If the user selects the mobile payment option, all charges associated with wireless Internet access using the obtained user identification and PIN from that point onwards would be charged out to the user's mobile telephone bill. If the credit card payment option is selected, in step 516, the user only needs to key-in required credit card details over the wireless network to proceed. All charges associated with using the network or Internet under the obtained user identification and PIN from that point onwards would thus be charged out to the user's credit card bill.

If the user decides to discontinue and/or does not respond to the prompted payment request in steps 510 and 512, the user is disconnected in a log-out procedure, shown in step 518. This log-out procedure could be similar if the IBR decides to manually log-out after using the wireless access under the mobile or credit card payment described earlier.

In one preferred embodiment, the usage of the PIN is tracked to ascertain how much to charge the mobile telephone 3 if a mobile payment plan is chosen. To prevent unauthorised use of a PIN which is charged under a mobile payment plan, the preferred system disables the PIN associated to the user/mobile telephone 3 whenever the user logs out of the wireless network. A scenario showing this safety measure is described below.

Assuming that the user attempts to log into the wireless environment using the previously issued user identification and PIN, shown in step 520, the user is prompted by a pop-up message, in step 522. The pop-up message would inform the user regarding the non-acceptance of a previously issued PIN and would preferably inform the IBR that any further access to the Internet via the wireless network will incur access charges. This is because, by this point, all of the free trial period has been used up, which was in step 508. Again, the IBR would be given options for payment that include mobile payment and credit card payment.

If the user wishes to have the access charges billed under the mobile payment plan, the system would seek confirmation regarding the mobile telephone number to which to access is

to be billed. For this reason, the system prompts the user, in step 522, to redial the wireless request number to obtain a new PIN. When this is done, in step 526, the interface system 5 would record the user's mobile telephone number or make appropriate database entries to flag that any future wireless access is to be billed under that mobile number. Of course once the user obtains the new PIN, the log in procedure is repeated as shown in step 528.

Alternatively, if the user chooses the credit card payment plan, in step 524, there is no need to reissue a PIN as there will not be a mobile telephone under which the wireless access charges will be made. The user is then allowed into the wireless network. It will be appreciated that the wireless network 1 may perform credit checks to ensure the credit card details supplied are authentic before the user is granted wireless access.

In summary, when a user has previously exhausted the free trial minutes and attempts to perform a re-login back to the wireless environment using the previous PIN, the user would be prompted whether to pay by mobile bill or by credit card payment. For avoidance of doubts (or possible fraud) the system is designed to re-issue a new PIN so that the user is aware of the chargeable access. For credit card payment, the user is not required to key in any new PIN. Instead, the user has to input the relevant credit card information to purchase a block of duration (e.g. 30/60/120 mins) of wireless access.

Referring now to Figure 6, the process flow when a second or subsequent wireless access request is made after the free trial period has elapsed, for example 15 minutes. It is of course possible to reconfigure this period to suit the particular service provider. This includes charging for any wireless access without provisions for a free trial.

In step 600, the user has dialled the wireless access number to obtain wireless access. In step 602, the mobile-wireless interface system 5 has determined that the 15 minutes of free trial has expired for that user using the particular mobile telephone 3. Here, the mobile-wireless interface system 5 performs a somewhat similar process as it would have if the trial period had not yet expired, that is, it generates a PIN that would be sent to the user's mobile telephone 3 via a text message. This text message however is appended with notification to reflect new conditions for access. In particular, the text message informs the user that the free trial period has been exhausted and that any further wireless access will incur charges. The user must therefore specify a payment option, including either a mobile payment or credit

card payment, before wireless access can be granted. If the user attempts to access the wireless network by opening a web browser in step 606, access will not be granted until either a credit card payment (step 608) is specified or, if the mobile payment plan is chosen (step 608), the user submits a valid user identification and PIN in the walled garden login (step 612).

Referring now to Figure 7, the preferred process flow for a mobile telephone user is shown in Figure 11B. Although the process is detailed in a step-by-step nature, persons skilled in the art will appreciate that various changes by way of modification, addition or deletion that are well known in the art can be made without jeopardising the process flow.

In step 700, mobile telephone user registers with the local mobile network for mobile communication. To inform the user of the availability of a wireless network in the area, the mobile network sends a welcome text message in step 702 via SMS to the user's mobile telephone. Included in the text message are instructions on how to obtain access to the wireless network, such as by dialling a wireless access request number e.g. *WiFi or *9434.

In step 704, the user requests wireless access by following the instructions provided in the welcome text message, that is by making a call to *WiFi in the example given. Once the call is connected to the local mobile network, the wireless system proceeds to retrieve the MSISDN belonging to the user's mobile telephone, as shown in step 706. In the preferred form, the wireless access request call is diverted to the wireless system through the MSC to provide the user with a service related announcement (step 708). If there are no service announcements, or if such a service is not required, step 708 may be omitted completely.

In steps 710 and 712, the wireless system generates a user identification and PIN for wireless access and sends these to the user's mobile telephone in a text message. Preferably, the user identification is the MSISDN of the user's mobile telephone, as this simplifies the allocation of the user identification. Also for a simplified yet robust system, the generated PIN may be a randomly generated number. For system reference and authentication, the user identification and PIN are stored in the system database,(step 714).

When the user decides to utilise the wireless network, shown in step 716, the user ideally opens a web browser which automatically prompts the user for login information

(steps 718 and 720). Clearly, the user must produce a valid user identification and PIN combination to be granted wireless access. An incorrect submission of this combination will result in the system re-prompting the user (steps 722 and 724). For security reasons, there should be a maximum number of retries for the IBR to submit a correct user identification and PIN combination. Although specified in steps 726 and 728 to be "Max retries" and "3 tries" for submission of a wrong user identification and PIN respectively, these values can easily be reconfigured. The chosen values are usually dependent on the level of security the service provider requires, which will be variable from one service provider to another.

In the event that the maximum retries have been exhausted, the user is informed of the failed login attempt (steps 730 and 732). Ideally, the user would be instructed to re-request wireless access to start a new session.

On the other hand, if the login submission is accepted, the user may be provided with confirmation notification. An example of this is shown in step 734. Where a time-limited access is provided, the system should warn the user prior to terminating the access when the time limit is reached, in step 736. This would give the user a chance to consider payment options or, at the very least, to close down or log out of any secure websites that the user might be working in, e.g. an online bank or web-based email services.

Should the user decide to continue using the wireless network, credit card details would be presented in step 738. If the user does not send the required credit card payment details, the wireless access would be terminated. In both cases, it is preferable to inform the user of the outcome in a pop-up message (steps 740 and 742). The process concludes after step 744, once the user logs out of the wireless network and corresponding usage details are recorded.

Figure 8 shows the process flow that is common for all the earlier mentioned processes. This process forms an integral portion of the earlier processes for the reason that it plays the role of the status monitor. For instance, when the wireless device being monitored is a mobile phone, the roaming status of the user on the local mobile network is monitor as described below.

In providing wireless access to roaming mobile telephone user, especially an inbound or overseas roamer, the local mobile network must be sure that the user taking advantage of this access does not defeat the reason for the access, which is to lure the user to remain roaming on said local network. This is particularly important if a free trial of the wireless access is provided. Clearly if the user decides to register with another mobile service provider, in other words roaming under a different provider, the user must be informed that the wireless access would be discontinued unless the user re-registers with the former mobile service provider. This information ensures that the user is provided with the knowledge and time to switch back to the former mobile service provider, in essence luring the user to remain roaming under that mobile network. However, if the user has clearly deregistered with no intention of re-registering in the near future, the wireless access privileges provided by the former mobile service provider should be revoked or terminated.

The preferred form of the system checks the user's roaming status periodically, in step 800. In the most preferred embodiment, the user's roaming status is checked every minute. Checking the user's roaming status requires an HLR query to the mobile network which will increase the signalling traffic. Hence the status checking period is made to be configurable to ensure such traffic can be manageable.

One way in which the local mobile network can determine whether the user is still roaming under its mobile network is to check the MSC for changes to the storage of mobile telephone subscription details. This is because, when a mobile telephone user changes its network, it deregisters from the first network (effectively deregistering from the MSC) before it is completely registered under the new network. By watching for the deregistration of the mobile telephone from the local mobile network, the current system can therefore determine when the roaming user no longer roams under that mobile network.

For the current system, the determination whether the user is still connected to the mobile network 2 is preferably done by having the wireless service gateway 9 in constant communication with the server 20. This way, the wireless service gateway will be able to query the server 20 or the database 19 regarding the status of the user's mobile telephone.

The communication between the wireless service gateway 9 and the server 20 should be over HTTPS (Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL).

HTTPS is a Web protocol developed by Netscape and built into its browser that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS is in fact the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. SSL uses a 40-bit key size for an RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

In step 802, the user is found to be still connected to the local mobile network 2 and is therefore allowed to continue using the wireless network 1. On the other hand, if the determination reveals that the user has left the mobile network 2, the wireless network 1, specifically the mobile-wireless interface system 5, is notified. As described earlier, this notification could by via HTTPS, which is sent through from the wireless network 1 via the Internet to the wireless service gateway 9, shown in step 804.

A message is then sent to notify the user that the system has discovered a deregistration of the mobile telephone. Preferably, this is done via the wireless network in the form displayable on the user equipment (e.g. laptop), such as a pop-up message, Alternatively, the user's web browser could be immediately diverted to a page informing the user of the deregistration. Also, the system may inform the user via the user's mobile telephone, utilising a text message or WAP. Those skilled in the art will be aware of the numerous other ways in which the user could be notified in this regard. The main criterion for the message is that it should inform the user of the deregistration as quickly as possible.

In a highly preferred form, the user is provided with a duration to re-register with the local mobile network before wireless access is discontinued. For example, a 5 minute window could be provided. In the case where a pop-up message is employed, as shown in step 806, the user has a 5-minute period to register back to the local mobile network before access to the wireless network is revoked. If the user fails to comply with this request within the given period, access to the wireless network is accordingly revoked.

In another embodiment, more than one pop-up messages could be provided. Here, a first pop-up would be as described in the previous paragraph, that is to inform the user that a 5-minute window to re-register is provided. If the user still has not re-registered, for example after 3 minutes, another pop-up message could be activated. This time, the user is informed

that only 2 minutes remain for a re-registration to take place to prevent any disruption to the wireless access.

As described earlier, one example application of the current wireless network is in the inbound roamer scenario. It is envisioned that when an inbound roamer (IBR), that is a roamer coming into the current country from overseas, registers in a local mobile network, the IBR could be lured to remain roaming under that local mobile network if a free trial of a wireless network is provided by said local mobile network.

In the specific embodiment shown in Figure 9, the mobile telephone 3 is shown to be connected to the local mobile affiliated network. In accordance with the preferred form of the invention, the user dials *9434, which is also represented by *WiFi, to request access to the wireless system. If the mobile telephone 3 registers for the first time, ideally a welcome text message would be sent informing the IBR of the wireless access facility. However, this is not essential as users may come to know of the wireless access facility and the wireless access number to dial through other means such as non-text-message-based advertisements and/or brochures.

As users of mobile telephones usually expect to receive some voice-based information over the telephone call, a recorded announcement is preferably played to the mobile telephone user once the wireless access call is connected, as shown in Figure 10. This recorded announcement would also help first-time users who may know little about the next step in obtaining wireless access. In the example shown, the voice announcement informs the user that a PIN will be provided shortly. Alternate recoded announcements include known systems, particularly in mobile telephone networks, that allow the user to interactively select options for required information. For instance, the recorded message could include the following - "Please press 1 to hear more about StarHub's wireless network, please press 2 if you would like a PIN sent out to you, please press 3 to find out the balance of your free trial period, or alternatively, please press 0 to speak to a customer service operator".

Once the announcement has been played and a PIN generated, the mobile telephone user receives a text message 100. Included in the text message 100 are the user identification and the PIN for accessing the wireless network. Although the figure shows a certain format for both the user identification and PIN, it is recognised that variations to these formats can

easily be made. For example, instead of a six-digit PIN, service providers requiring higher levels of security could implement a ten-digit PIN.

Figure 11 illustrates the connectivity involved when the IBR attempts to obtain access of the wireless network. As described in the above preferred embodiment, the IBR dials *WiFi of *9434 to request access. Since this number is associated with the server 20 on the mobile-wireless interface system, the IBR call is accordingly diverted by the MSCs 4 to the server 20. Preferably, the interactive server portion of server 20 is activated, where the IBR is able to hear an appropriate announcement.

From the IBR's telephone call, the server 20 is able extract the IBR's mobile telephone number. This number is then used to construct a MAP query, which is sent through the International Switching Centres (ISCs) 14, 14a-c to any of the MSCs of affiliated roaming partners around the world. In the example of Figure 11, the IBR's Home MSC and Home HLR is MSC 4a and HLR 6a. The query effectively asks the Home HLR to provide the server 20 with the IBR's IMSI and VLR information.

For security reasons, the foreign or Home HLRs should only reply to verified requests for IMSI and VLR information. For this, the server 20 is provided with a System Identification, which would be listed in the Routing Access List of foreign HLRs that the server 20 is authorised to query. For the example in Figure 11, the System Identification for server 20 could be a 10-digit number such as 6598540042. Therefore, unless Home HLR 4a lists the System Identification of 6598540042 in its Routing Access List, the MAP query by server 20 will not be replied with the required IMSI and VLR information.

Once the Home HLR 4a checks the Routing Access List and approves a reply to the MAP query, the IBR's IMSI and VLR information is sent back to the server 20. At this point, the IMSI information is set as the user identification for the wireless access. Once a PIN is generated in the PIN generator of the server 20, both user identification and password are sent to the IBR, preferably by text message via SMS.

Figure 12 shows how a user can utilise the information provided in the text message 100 to access the wireless network. In this example, the user has presented a wireless-capable device, such as a laptop in the vicinity of a wireless access point or hotspot. When the user

initiates a web browser 110, the service provider's home webpage is retrieved. From the example shown, the user has initiated the web browser in the vicinity of aaffiliated wireless hotspot, in particular in Changi Airport. In the home webpage, a login form 111 is provided, in which the user should key-in the user identification and PIN provided in the text message 100. When this login form 111 is submitted, and provided the user identification and PIN are verified to be valid, the user will be grated access to the wireless network, including access to the Internet.

Ideally, once connected, connection information is displayed to the user. This is common in the art of providing dial-up Internet access, where a message box indicates, *inter alia*, the speed of connection, duration of connection and total data sent/received. For wireless systems where a time-limited access is provided, such as a 15-minute free trial, it is most preferable to have some duration indication on the user equipment. Such an indication would also be useful for user who are being charged for the wireless access based on duration of use. An example of displayed connection information is shown in Figure 13. In this example, a small web browser window 120 is provided to display connection information. If providing a separate web browser window is not desired, for reason of taskbar congestion, the connection information may be displayed as a small icon in taskbar 121 or as an integral frame in web browser 110.

Referring now to Figure 14, the result of the monitoring feature of the invention is shown. As with the previous examples, the wireless device being monitored is the user's mobile phone. The status of the mobile phone that is monitored is the roaming status. Illustrated in Figure 9, the mobile telephone 3 was initially registered under the affiliated network, which allowed the mobile telephone user to request wireless network access. However, shown in Figure 14 generally by reference numeral 130, the mobile telephone 3 has switched its mobile service provider to a non affiliated network. Since the switch would have involved a deregistration of the mobile telephone 3 from the affiliated mobile network, the mobile-wireless interface system would have detected this switch. This information is then relayed to the wireless network, where a message box 131 is presented to the user. The message box ideally prompts the user to switch back to the original mobile service provider , as the user may not have been aware of the change in service provider. If the user does not comply with the switch request, preferably within a fixed duration, the wireless access privilege is revoke and the user is disconnected.

The foregoing describes the invention including preferred forms thereof. Alterations and modifications as will be obvious to those skilled in the art are intended to be incorporated within the scope hereof.

Glossary

AP	Access Point
APN	Access Point Network
BSC	Base Station Controller
BSS	Base Station Subsystem
DHCP	Dynamic Host Configuration Protocol
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobile communication
GSN	GPRS Support Node
GTP	GPRS Tunneling Protocol
HLR	Home Location Register
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol over Secure Socket Layer
IBR	Inbound Roamer
IMSI	International Mobile Subscriber Identity
ISC	International Switching Centre
ISP	Internet Service Provider
LAN	Local Area Network
LBS	Location Based Service
LDAP	Lightweight Directory Access Protocol
MS	Mobile Station
MSC	Mobile Switching Centre
MSISDN	Mobile Station International ISDN Number
NMS	Network Management System

OAM	Operation, Administration and Maintenance
OMC	Operation & Maintenance Centre
PDA	Personal Digital Assistant
PIN	Personal Identification Number
RADIUS	Remote Authentication Dial-In User Service
SG	Service Gateway
SGSN	Serving GPRS Support Node
SMS	Short Message Service
SMSC	Short Message Switching Centre
SS7	Signalling System 7
SS7-MAP	Signalling System 7 – Mobile Application Part
SSG	Service Selection Gateway
TCP/IP	Transfer Control Protocol/Internet Protocol
VLR	Visitor Location Register
WAP	Wireless Application Protocol
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network
WSG	Wireless Service Gateway

CLAIMS:

1. A method of allowing access to an IP network for a user comprising the steps of:

monitoring status of a wireless device associated with said user or in the control of said user,

providing IP network access dependant on a condition, wherein said condition relates to a predetermined period of access, and

notifying or alerting said user in response to any changes in said status or said access or said condition.

2. A method of allowing access to an IP network as claimed in claim 1 wherein said notification or alert relates to said device not being connected to a predetermined list of networks.

3. A method of allowing access to an IP network as claimed in claim 2 wherein said condition relates to said status of said wireless device.

4. A method of allowing access to an IP network as claimed in any one of claims 1 to 3 wherein said status relates to the network said device is connected to.

5. A method of allowing access to an IP network as claimed in any one of claims 1 to 4 further comprising the step of issuing a user ID and password depending on said status, and adding the same to a list of valid user ID's and passwords.

6. A method of allowing access to an IP network as claimed in claim 5 wherein said condition relates to entering a user ID and password which matches an entry on said valid user ID list.

7. A method of allowing access to an IP network as claimed in claim 5 or claim 6 wherein when said predetermined period expires said user ID and password are

removed from said valid user ID list.

8. A system for providing IP network access comprising:

a monitor configured to detect status of a wireless device associated with a user or in the control of said user,

an access point providing IP network access dependent on a condition, wherein said condition relates to a predetermined period of access, and

means for notifying or alerting a user of any change in said access, said status or said condition.

9. A system for providing IP network access as claimed in claim 8 wherein said notification or alert relates to said device not being connected to a predetermined list of networks.

10. A system for providing IP network access as claimed in claim 9 wherein said condition relates to said status of said wireless device.

11. A system for providing IP network access as claimed in any one of claims 8 to 10 wherein said status relates to the network said wireless device is connected to.

12. A system for providing IP network access as claimed in any one of claims 8 to 11 including means for issuing a user ID and password depending on said status, and adding the same to a list of valid user ID's and passwords.

13. A system for providing IP network access as claimed in claim 12 wherein said condition relates to entering a user ID and password which matches an entry on said valid user ID list.

14. A system for providing IP network access as claimed in claim 12 or claim 13 wherein said system includes means for removing said user ID and password from

said valid user ID list when said predetermined period expires.

15. A method of allowing access to an IP network for a user comprising the steps of:

monitoring the connected network of a wireless device associated with said user or in the control of said user,

providing IP network access dependant on a condition, wherein said condition relates to the connected network of said wireless device, and

notifying or alerting said user in response to any changes in said connected network, said access or said condition.

16. A method of allowing access to an IP network as claimed in claim 15 wherein said wireless device is a mobile telephone and said connected network is a mobile telephone network.

17. A method of allowing access to an IP network as claimed in claim 15 or claim 16 wherein said condition additionally relates to a predetermined period of access.

18. A method of allowing access to an IP network as claimed in any one of claims 15 to 17 wherein said notification or alert relates to said wireless device not being connected to a predetermined list of networks.

19. A method of allowing access to an IP network as claimed in any one of claims 15 to 18 further comprising the step of issuing a user ID and password depending on said connected network, and adding the same to a list of valid user ID's and passwords.

20. A method of allowing access to an IP network as claimed in claim 19 wherein said condition additionally relates to entering a user ID and password which matches an entry on said valid user ID list.

21. A method of allowing access to an IP network as claimed in claim 19 or claim 20 wherein when said predetermined period expires said user ID and password are removed from said valid user ID list.

22. A method of allowing access to an IP network as claimed in any one of claims 15 to 21 wherein said IP network access is provided for a computer or PDA.

23. A system for providing IP network access comprising:

a monitor configured to detect the connected network of a wireless device associated with a user or in the control of said user,

an access point configured to provide IP network access dependant on a condition, wherein said condition relates to the connected network of said wireless device, and

means for notifying or alerting said user in response to any changes in said connected network, said access or said condition.

24. A system for providing IP network access as claimed in claim 23 wherein said wireless device is a mobile telephone and said connected network is a mobile telephone network.

25. A system for providing IP network access as claimed in claim 23 or claim 24 wherein said condition additionally relates to a predetermined period of access.

26. A system for providing IP network access as claimed in any one of claims 23 to 25 wherein said notification or alert relates to said wireless device not being connected to a predetermined list of networks.

27. A system for providing IP network access as claimed in any one of claims 23 to 26 further comprising means for issuing a user ID and password depending on said

connected network, and adding the same to a list of valid user ID's and passwords.

28. A system for providing IP network access as claimed in claim 27 wherein said condition additionally relates to entering a user ID and password which matches an entry on said valid user ID list.

29. A system for providing IP network access as claimed in claim 27 or claim 28 wherein said system includes means for removing said user ID and password from said valid user ID list when said predetermined period expires.

30. A system for providing IP network access as claimed in any one of claims 23 to 29 wherein said IP network access is provided for a computer or PDA.