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

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2619325 C 2015/11/17

(11)(21) **2 619 325**

(12) BREVET CANADIEN / CANADIAN PATENT

(13) **C**

(22) **Date de dépôt/Filing Date:** 2008/01/31

(41) **Mise à la disp. pub./Open to Public Insp.:** 2008/08/05

(45) **Date de délivrance/Issue Date:** 2015/11/17

(30) **Priorités/Priorities:** 2007/02/05 (US11/671,263); 2007/02/05 (EP07101743.8)

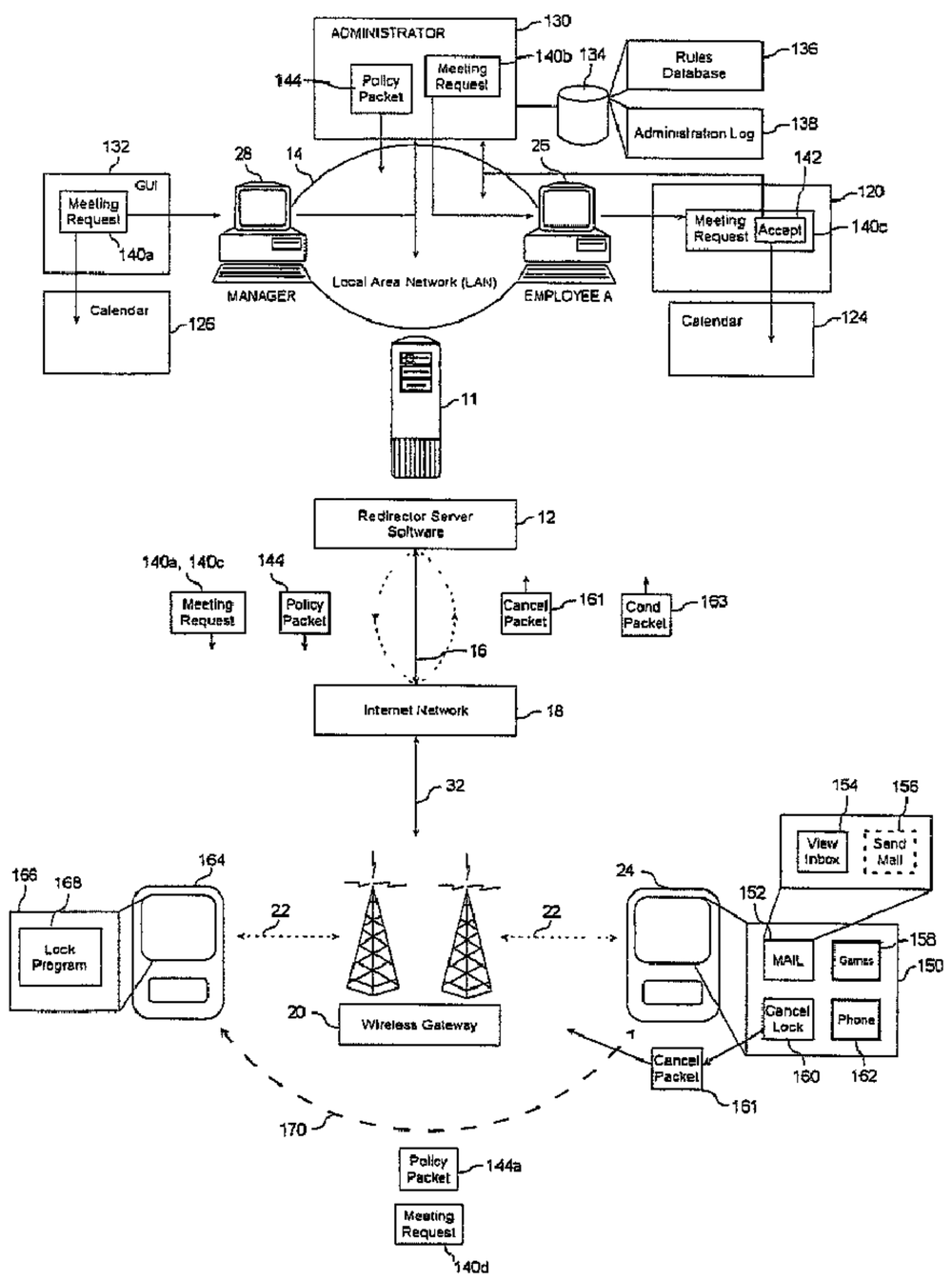
(51) **Cl.Int./Int.Cl.** ***H04W 88/02*** (2009.01)

(72) **Inventeurs/Inventors:**
COSKUN, RISVAN, CA;
MARTIN, DARYL J., CA;
HASSAN, AHMED E., CA;
WILSON, JOHN F., CA

(73) **Propriétaire/Owner:**
BLACKBERRY LIMITED, CA

(74) **Agent:** INTEGRAL IP

(54) **Titre : SYSTEME ET METHODE POUR LA COMMANDE DE L'USAGE D'UN DISPOSITIF**
(54) **Title: SYSTEM AND METHOD FOR CONTROLLING DEVICE USAGE**



(57) **Abrégé/Abstract:**
Mobile device usage may be monitored and restricted by pushing enabling/disabling events from an administrator the device. The events impose a certain set of rules that can "lock" certain features provided by the device, according to permissions and pre-

CA 2619325 C 2015/11/17

(11)(21) **2 619 325**

(13) **C**

(57) **Abrégé(suite)/Abstract(continued):**
established policies, for a certain period of time. Such restricted periods may coincide with meetings or other events in which distractions should be kept to a minimum or be during regular, predetermined time periods. Preferably, the rules include conditional locks that allow a user to use a feature a reasonable number of times before the lock is activated to place the onus on the user for minimizing such distractions, while enabling the user to maintain access to such a vital communication tool. Cancel packets may also be used to not only control but to monitor the application of the rule sets and when certain conditions are breaches, which provides an employer with sufficient information to use in auditing device usage or in reprimanding users for misuse of a privilege such as the use of mobile data communications devices.

ABSTRACT

Mobile device usage may be monitored and restricted by pushing enabling/disabling events from an administrator the device. The events impose a certain set of rules that can "lock" certain features provided by the device, according to permissions and pre-established policies, for a certain period of time. Such restricted periods may coincide with meetings or other events in which distractions should be kept to a minimum or be during regular, predetermined time periods. Preferably, the rules include conditional locks that allow a user to use a feature a reasonable number of times before the lock is activated to place the onus on the user for minimizing such distractions, while enabling the user to maintain access to such a vital communication tool. Cancel packets may also be used to not only control but to monitor the application of the rule sets and when certain conditions are breaches, which provides an employer with sufficient information to use in auditing device usage or in reprimanding users for misuse of a privilege such as the use of mobile data communications devices.

SYSTEM AND METHOD FOR CONTROLLING DEVICE USAGE

TECHNICAL FIELD:

[0001] The following relates to systems and methods for controlling device usage.

DESCRIPTION OF THE PRIOR ART

[0002] Mobile device usage has become widespread amongst both individuals and corporations, and often such users rely heavily, and may even become dependent on, the use of such devices. Mobile devices are often used to conduct business, maintain contact with peers and perform other communication tasks while the user of the device is away from their home or office. Due to their ubiquity, mobile devices, in particular the usage of the devices, have been viewed by many as an interruption to public environments, such as corporate meetings, movie theatres, and public transit.

[0003] In particular, mobile devices have been known to cause interruptions and distractions in a corporate meeting environment, most notably where there are several attendees. For example, in a large meeting, mobile device users may send messages to each other, respond to emails, play games, and even answer telephone calls. Often a presenter or facilitator of such meetings may be distracted by these activities, which can have a negative influence on a presentation, and may cause a user who is participating in the distracting activity to miss or overlook an important point in the presentation.

[0004] In certain scenarios, users do not intend on creating a distraction but merely forget to turn off or silence their device prior to arriving at a meeting. A buzzing or ringing caused by receipt of a message or telephone call could then inadvertently occur which serves to both embarrass the user and possibly result in undesirable consequences.

[0005] In other scenarios, users may bring their mobile device with them while they are away from the office and send and receive emails as if they were actually in their office. The convenience of a mobile device having email capabilities can therefore make it difficult for a company to control attendance.

[0006] It is therefore an object of the following to obviate or mitigate at least one of the above disadvantages.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] Embodiments will now be described by way of example only with reference to the appended drawings wherein:

[0008] Figure 1 is a system diagram showing the redirection of user data items from a user's desktop PC (host system) to the user's mobile device, where the redirector software is operating at the user's desktop PC.

[0009] Figure 2 is a system diagram showing the redirection of user data items from a network server (host system) to the user's mobile device, where the redirector software is operating at the server.

[0010] Figure 3 is a block diagram showing the interaction of the redirector software with other components of the host system in Figure 1 (the user's desktop PC) to enable the pushing of information from the host system to the user's mobile device.

[0011] Figure 4 is a flow chart showing the steps carried out by the redirector software operating at the host system.

[0012] Figure 5 is a flow chart showing the steps carried out by the mobile device to interface with the redirector software operating at the host system.

[0013] Figure 6 is a block diagram showing an embodiment of a system for controlling mobile device usage.

[0014] Figure 7 is a schematic representation of the graphical user interface (GUI) shown in Figure 6.

[0015] Figure 8 is a schematic representation of the rules database shown in Figure 6.

[0016] Figure 9 is a flow chart showing the steps carried out in generating and pushing a policy packet from the administrator to the device in Figure 6.

[0017] Figure 10 is a flow chart showing the steps carried out in triggering the policy packet and applying a rule set for a duration of time to the device in Figure 6.

[0018] Figure 11 is a flow chart showing an alternative method for pushing a policy packet to the device in Figure 6.

[0019] Figure 12 is another embodiment of a system for controlling mobile device usage.

[0020] Figure 13 is a schematic diagram of a mobile device and a display screen therefor.

[0021] Figure 14 is a schematic diagram of another mobile device and a display screen therefor.

[0022] Figure 15 is a schematic block diagram of components of the mobile device of any or both of Figures 13 and 14.

[0023] Figure 16 is a schematic block diagram of the memory shown in Figure 15.

[0024] Figure 17 is a screen shot of a home screen displayed by the mobile device of any or both of Figures 13 and 14.

[0025] Figure 18 is a schematic representation of a category stored in memory in Figure 16.

[0026] Figure 19 is a block diagram showing yet another embodiment of a system for controlling mobile device usage.

DETAILED DESCRIPTION OF THE DRAWINGS

[0027] Referring now to the drawings, Figure 1 is an exemplary system diagram showing the redirection of user data items (such as message A or C) from a user's office PC (host system) 10 to the user's mobile device 24, where the redirector software 12 is operating at the user's PC. Message A in Figure 1 represents an internal message sent from desktop 26 to the user's host

system 10 via LAN 14. Message C in Figure 1 represents an external message from a sender that is not directly connected to LAN 14, such as the user's mobile device 24, some other user's mobile device (not shown), or any user connected to the Internet 18. Message C also represents a command message from the user's mobile device 24 to the host system 10. As described in more detail in Figure 3, the host system 10 preferably includes, along with the typical hardware and software associated with a workstation or desktop computer, the redirector program 12, a TCP/IP subsystem 42, a primary message store 40, an E-mail subsystem 44, a screen saver subsystem 48, and a keyboard subsystem 46.

[0028] In Figure 1, the host system 10 is the user's desktop system, typically located in the user's office. The host system 10 is connected to a LAN 14, which also connects to other computers 26, 28 that may be in the user's office or elsewhere. The LAN 14, in turn, is connected to a wide area network ("WAN") 18, preferably the Internet, which is defined by the use of the Transmission Control Protocol/Internet Protocol ("TCP/IP") to exchange information, but which, alternatively could be any other type of WAN. The connection of the LAN 14 to the WAN 18 is via high bandwidth link 16, typically a T1 or T3 connection. The WAN 18 in turn is connected to a variety of gateways 20, via connections 32. A gateway forms a connection or bridge between the WAN 18 and some other type of network, such as an RF wireless network, cellular network, satellite network, or other synchronous or asynchronous land-line connection.

[0029] In one embodiment, mobile device 24 is a hand-held two-way wireless paging computer, a wirelessly enabled palm-top computer, a mobile telephone with data messaging capabilities, or a wirelessly enabled laptop computer, but could, alternatively be other types of mobile devices capable of sending and receiving messages via a network connection 22. Mobile devices 24 could alternatively not be capable of sending and receiving message via network connection 22. In another embodiment, mobile device 24 is a digital entertainment device, such as an MP3 player or video game device. In yet another embodiment, mobile device 24 is any electronic device which can be used by a user to provide any number of features such as an alarm, email, phone etc.

[0030] In some embodiments, the mobile device 24 includes software program instructions that work in conjunction with the redirector program 12 to enable the seamless, transparent redirection of user-selected data items. Figure 4 describes the basic method steps of the redirector program 12, and Figure 5 describes the steps of the corresponding program operating at the mobile device 24.

[0031] In an alternative embodiment, not explicitly shown in the drawings, the mobile device 24 also includes a redirector program. In this embodiment, user selected data items can be replicated from the host to the mobile device and vice versa. The configuration and operation of the mobile device 24 having a redirector program is similar to that described herein with respect to FIGS. 1-4.

[0032] A user can configure the redirector program 12 to push certain user-selected data items to the user's mobile device 24 when the redirector 12 detects that a particular user-defined event trigger (or trigger point) has taken place. User-selected data items preferably include E-mail messages, calendar events, meeting notifications, address entries, journal entries, personal alerts, alarms, warnings, stock quotes, news bulletins, etc., but could, alternatively, include any other type of message that is transmitted to the host system 10, or that the host system 10 acquires through the use of intelligent agents, such as data that is received after the host system 10 initiates a search of a database or a website or a bulletin board. In some instances, only a portion of the data item is transmitted to the mobile device 24 in order to minimize the amount of data transmitted via the wireless network 22. In these instances, the mobile device 24 can optionally send a command message to the host system to receive more or all of the data item if the user desires to receive it.

[0033] Among the user-defined event triggers that can be detected by the redirector program 12 are, in the preferred embodiment, external events, internal events and networked events. External events preferably include: (1) receiving a command message (such as message C) from the user's mobile device to begin redirection, or to execute some other command at the host, such as a command to enable the preferred list mode, or to add or subtract a particular sender from the preferred list; (2) receiving a similar message from some external computer, and (3) sensing that

the user is no longer in the vicinity of the host system; although, alternatively, an external event can be any other detectable occurrence that is external to the host system. Internal events could be a calendar alarm, screen saver activation, keyboard timeout, programmable timer, or any other user-defined event that is internal to the host system. Networked events are user-defined messages that are transmitted to the host system from another computer coupled to the host system via a network to initiate redirection. These are just some of the events that could be used to initiate replication of the user-selected data items from the host system 10 to the mobile device 24.

[0034] Figure 1 shows an E-mail message A being communicated over LAN 14 from computer 26 to the user's desktop system 10 (also shown in Figure 1 is an external message C, which could be an E-mail message from an Internet user, or could be a command message from the user's mobile device 24). Once the message A (or C) reaches the primary message store of the host system 10, it can be detected and acted upon by the redirection software 12. The redirection software 12 can use many methods of detecting new messages. The preferred method of detecting new messages is using Microsoft's® Messaging API (MAPI), in which programs, such as the redirector program 12, register for notifications or 'advise syncs' when changes to a mailbox take place. Other methods of detecting new messages could also be used.

[0035] Assuming that the redirector program 12 is activated, and has been configured by the user (either through the sensing of an internal, network or external event) to replicate certain user data items (including messages of type A or C) to the mobile device 24, when the message A is received at the host system 10, the redirector program 12 detects its presence and prepares the message for redirection to the mobile device 24. In preparing the message for redirection, the redirector program 12 could compress the original message A, could compress the message header, or could encrypt the entire message A to create a secure link to the mobile device 24.

[0036] Also programmed into the redirector 12 is the address of the user's mobile device 24, the type of device, and whether the device 24 can accept certain types of attachments, such as word processing or voice attachments. If the user's type of mobile device cannot accept these

types of attachments, then the redirector 12 can be programmed to route the attachments to a fax or voice number where the user is located using an attached fax or voice machine 30.

[0037] The redirector may also be programmed with a preferred list mode that is configured by the user either at the host system 10, or remotely from the user's mobile device by transmitting a command message C. The preferred list contains a list of senders (other users) whose messages are to be redirected or a list of message characteristics that determine whether a message is to be redirected. If activated, the preferred list mode causes the redirector program 12 to operate like a filter, only redirecting certain user data items based on whether the data item was sent from a sender on the preferred list or has certain message characteristics that if present will trigger or suppress redirection of the message. In the example of Figure 1, if desktop system 26 was operated by a user on the preferred list of host system 10, and the preferred list option was activated, then message A would be redirected. If, however, desktop 26 was operated by a user not on the host system's preferred list, then message A would not be redirected, even if the user of the host system had configured the redirector to push messages of type A. The user of the host system 10 can configure the preferred list directly from the desktop system, or, alternatively, the user can then send a command message (such as C) from the mobile device 24 to the desktop system 10 to activate the preferred list mode, or to add or delete certain senders or message characteristics from the preferred list that was previously configured. It should be appreciated that a redirection program could combine message characteristics and preferred sender lists to result in a more finely-tuned filter. Messages marked as low priority or that are simple return receipts or message read receipts, for example, could always be suppressed from redirection while messages from a particular sender would always be redirected.

[0038] After the redirector has determined that a particular message should be redirected, and it has prepared the message for redirection, the software 12 then sends the message A to a secondary memory store located in the mobile device 24, using whatever means are necessary. In the preferred embodiment this method is to send the message A back over the LAN 14, WAN 18, and through the wireless gateway 20 to the mobile device 24. In doing so, the redirector preferably repackages message A as an E-mail with an outer envelope B that contains the addressing information of the mobile device 24, although alternative repackaging techniques and

protocols could be used, such as a TCP/IP repackaging and delivery method (most commonly used in the alternative server configuration shown in Figure 2). The wireless gateway 20 requires this outer envelope information B in order to know where to send the redirected message A. Once the message (A in B) is received by the mobile device 24, the outer envelope B is removed and the original message A is placed in the secondary memory store within the mobile device 24. By repackaging and removing the outer envelope in this manner, the mobile computer 24 appears to be at the same physical location as the host system 10, thus creating a transparent system.

[0039] In the case where message C is representative of an external message from a computer on the Internet 18 to the host system 10, and the host 10 has been configured to redirect messages of type C, then in a similar manner to message A, message C would be repackaged with an outer envelope B and transmitted to the user's mobile device 24. In the case where message C is representative of a command message from the user's mobile device 24 to the host system 10, the command message C is not redirected, but is acted upon by the host system 10.

[0040] If the redirected user data item is an E-mail message, as described above, the user at the mobile device 24 sees the original subject, sender's address, destination address, carbon copy and blind carbon copy. When the user replies to this message, or when the user authors a new message, the software operating at the mobile device 24 adds a similar outer envelope to the reply message (or the new message) to cause the message to be routed first to the user's host system 10, which then removes the outer envelope and redirects the message to the final destination, such as back to computer 26. In the preferred embodiment this results in the outgoing redirected message from the user's host system 10 being sent using the E-mail address of the host mailbox, rather than the address of the mobile device, so that it appears to the recipient of the message that the message originated from the user's desktop system 10 rather than the mobile device. Any replies to the redirected message will then be sent to the desktop system 10, which if it is still in redirector mode, will repackage the reply and resend it to the user's mobile data device, as described above.

[0041] Figure 2 is an alternative system diagram showing the redirection of user data items from a network server 11 to the user's mobile device 24, where the redirector software 12 is operating at the server 11. This configuration is particularly advantageous for use with message servers such as Microsoft's® Exchange Server, which is normally operated so that all user messages are kept in one central location or mailbox store on the server instead of in a store within each user's desktop PC. This configuration has the additional advantage of allowing a single system administrator to configure and keep track of all users having messages redirected. If the system includes encryption keys, these too can be kept at one place for management and update purposes.

[0042] In this alternative configuration, server 11 preferably maintains a user profile for each user's desktop system 10, 26, 28, including information such as whether a particular user can have data items redirected, which types of message and information to redirect, what events will trigger redirection, the address of the users' mobile device 24, the type of mobile device, and the user's preferred list, if any. The event triggers are preferably detected at the user's desktop system 10, 26, 28 and can be any of the external, internal or network events listed above. The desktop systems 10, 26, 28 preferably detect these events and then transmit a message to the server computer 11 via LAN 14 to initiate redirection. Although the user data items are preferably stored at the server computer 11 in this embodiment, they could, alternatively, be stored at each user's desktop system 10, 26, 28, which would then transmit them to the server computer 11 after an event has triggered redirection.

[0043] As shown in Figure 2, desktop system 26 generates a message A that is transmitted to and stored at the host system 11, which is the network server operating the redirector program 12. The message A is for desktop system 10, but in this embodiment, user messages are stored at the network server 11. When an event occurs at desktop system 10, an event trigger is generated and transmitted to the network server 11, which then determines who the trigger is from, whether that desktop has redirection capabilities, and if so, the server (operating the redirector program) uses the stored configuration information to redirect message A to the mobile computer 24 associated with the user of desktop system 10.

[0044] As described above with reference to Figure 1, message C could be either a command message from a user's mobile device 24, or it could be a message from an external computer, such as a computer connected to the Internet 18. If the message C is from an Internet computer to the user's desktop system 10, and the user has redirection capabilities, then the server 11 detects the message C, repackages it using electronic envelope B, and redirects the repackaged message (C in B) to the user's mobile device 24. If the message C is a command message from the user's mobile device 24, then the server 11 simply acts upon the command message.

[0045] Turning now to Figure 3, a block diagram showing the interaction of the redirector software 12 with additional components of the host system 10 of Figure 1 (the desktop PC) to enable more fully the pushing of information from the host system 10 to the user's mobile device 24 is set forth. These additional components are illustrative of the type of event-generating systems that can be configured and used with the redirector software 12, and of the type of repackaging systems that can be used to interface with the mobile communication device 24 to make it appear transparent to the user.

[0046] The desktop system 10 is connected to LAN 14, and can send and receive data, messages, signals, event triggers, etc., to and from other systems connected to the LAN 14 and to external networks 18, 22, such as the Internet or a wireless data network, which are also coupled to the LAN 14. In addition to the standard hardware, operating system, and application programs associated with a typical microcomputer or workstation, the desktop system 10 includes the redirector program 12, a TCP/IP sub-system 42, an E-mail sub-system 44, a primary data storage device 40, a screen saver sub-system 48, and a keyboard sub-system 46. The TCP/IP and E-mail subsystems 42, 44 are examples of repackaging systems that can be used to achieve transparency, and the screen saver and keyboard sub-systems 46, 48 are examples of event generating systems that can be configured to generate event messages or signals that trigger redirection of the user selected data items.

[0047] The method steps carried out by the redirector program 12 are described in more detail in Figure 4. The basic functions of this program are: (1) configure and setup the user-defined event trigger points that will start redirection; (2) configure the types of user data items

for redirection and optionally configure a preferred list of senders whose messages are to be redirected; (3) configure the type and capabilities of the user's mobile device; (4) receive messages and signals from the repackaging systems and the event generating systems; and (5) command and control the redirection of the user-selected data items to the mobile device via the repackaging systems. Other functions not specifically enumerated could also be integrated into this program.

[0048] The E-Mail sub-system 44 is the preferred link to repackaging the user-selected data items for transmission to the mobile device 24, and preferably uses industry standard mail protocols, such as SMTP, POP, IMAP, MIME and RFC-822, to name but a few. The E-Mail sub-system 44 can receive messages A from external computers on the LAN 14, or can receive messages C from some external network such as the Internet 18 or a wireless data communication network 22, and stores these messages in the primary data store 40. Assuming that the redirector 12 has been triggered to redirect messages of this type, the redirector detects the presence of any new messages and instructs the E-Mail system 44 to repackage the message by placing an outer wrapper B about the original message A (or C), and by providing the addressing information of the mobile device 24 on the outer wrapper B. As noted above, this outer wrapper B is removed by the mobile device 24, and the original message A (or C) is then recovered, thus making the mobile device 24 appear to be the desktop system 10.

[0049] In addition, the E-Mail sub-system 44 receives messages back from the mobile device 24 having an outer wrapper with the addressing information of the desktop system 10, and strips this information away so that the message can be routed to the proper sender of the original message A (or C). The E-Mail sub-system also receives command messages C from the mobile device 24 that are directed to the desktop system 10 to trigger redirection or to carry out some other function. The functionality of the E-Mail sub-system 44 is controlled by the redirector program 12.

[0050] The TCP/IP sub-system 42 is an alternative repackaging system. It includes all of the functionality of the E-Mail sub-system 44, but instead of repackaging the user-selected data items as standard E-mail messages, this system repackages the data items using special-purpose

TCP/IP packaging techniques. This type of special-purpose sub-system is useful in situations where security and improved speed are important to the user. The provision of a special-purpose wrapper that can only be removed by special software on the mobile device 24 provides the added security, and the bypassing of E-mail store and forward systems can improve speed and real-time delivery.

[0051] As described previously, the system can be triggered to begin redirection upon detecting numerous external, internal and networked events, or trigger points. Examples of external events include: receiving a command message from the user's mobile device 24 to begin redirection; receiving a similar message from some external computer, sensing that the user is no longer in the vicinity of the host system; or any other event that is external to the host system. Internal events could be a calendar alarm, screen saver activation, keyboard timeout, programmable timer, or any other user-defined event that is internal to the host system. Networked events are user-defined messages that are transmitted to the host system from another computer that is connected to the host system via a network to initiate redirection.

[0052] The screen saver and keyboard sub-systems 46, 48 are examples of systems that are capable of generating internal events. Functionally, the redirector program 12 provides the user with the ability to configure the screen saver and keyboard systems so that under certain conditions an event trigger will be generated that can be detected by the redirector 12 to start the redirection process. For example, the screen saver system can be configured so that when the screen saver is activated, after, for example, ten (10) minutes of inactivity on the desktop system, an event trigger is transmitted to the redirector 12, which starts redirecting the previously selected user data items. In a similar manner the keyboard sub-system can be configured to generate event triggers when no key has been depressed for a particular period of time, thus indicating that redirection should commence. These are just two examples of the numerous application programs and hardware systems internal to the host system 10 that can be used to generate internal event triggers.

[0053] Figures 4 and 5, set forth, respectively, flow charts showing the steps carried out by the redirector software 12 operating at the host system 10, and the steps carried out by the mobile

device 24 in order to interface with the host system. Turning first to Figure 4, at step 50, the redirector program 12 is started and initially configured The initial configuration of the redirector 12 includes: (1) defining the event triggers that the user has determined will trigger redirection; (2) selecting the user data items for redirection; (3) selecting the repackaging sub-system, either standard E-Mail, or special-purpose technique; (4) selecting the type of data communication device, indicating whether and what type of attachments the device is capable of receiving and processing, and inputting the address of the mobile device; and (5) configuring the preferred list of user selected senders whose messages are to be redirected.

[0054] Figure 4 sets forth the basic steps of the redirector program 12 assuming it is operating at a desktop system 10, such as shown in Figure 1. If the redirector 12 is operating at a network server 11, as shown in Figure 2, then additional configuration steps may be necessary to enable redirection for a particular desktop system 10, 26, 28 connected to the server, including: (1) setting up a profile for the desktop system indicating its address, events that will trigger redirection, and the data items that are to be redirected upon detecting an event; (2) maintaining a storage area at the server for the data items; and (3) storing the type of data communication device to which the desktop system's data items are to be redirected, whether and what type of attachments the device is capable of receiving and processing, and the address of the mobile device.

[0055] Once the redirector program is configured 50, the trigger points (or event triggers) are enabled at step 52. The program 12 then waits 56 for messages and signals 54 to begin the redirection process. A message could be an E-Mail message or some other user data item that may have been selected for redirection, and a signal could be a trigger signal, or could be some other type of signal that has not been configured as an event trigger. When a message or signal is detected, the program determines 58 whether it is one of the trigger events that has been configured by the user to signal redirection. If so, then at step 60 a trigger flag is set, indicating that subsequently received user data items (in the form of messages) that have been selected for redirection should be pushed to the user's mobile device 24.

[0056] If the message or signal 54 is not a trigger event, the program then determines at steps 62, 68 and 66 whether the message is, respectively, a system alarm 62, an E-Mail message 64, or some other type of information that has been selected for redirection. If the message or signal is none of these three items, then control returns to step 56, where the redirector waits for additional messages 54 to act upon. If, however the message is one of these three types of information, then the program 12 determines, at step 68, whether the trigger flag has been set, indicating that the user wants these items redirected to the mobile device. If the trigger flag is set, then at step 70, the redirector 12 causes the repackaging system (E-Mail or TCP/IP) to add the outer envelope to the user data item, and at step 72 the repackaged data item is then redirected to the user's mobile device 24 via LAN 14, WAN 18, wireless gateway 20 and wireless network 22. Control then returns to step 56 where the program waits for additional messages and signals to act upon. Although not shown explicitly in Figure 4, after step 68, the program could, if operating in the preferred list mode, determine whether the sender of a particular data item is on the preferred list, and if not, then the program would skip over steps 70 and 72 and proceed directly back to step 56. If the sender is on the preferred list, then control would similarly pass to steps 70 and 72 for repackaging and transmission of the message from the preferred list sender.

[0057] Figure 5 sets forth the method steps carried out by the user's mobile device 24 in order to interface to the redirector program 12. At step 80 the mobile software is started and the mobile device 24 is configured to operate with the system, including, for example, storing the address of the user's desktop system 10.

[0058] At step 82, the mobile device waits for messages and signals 84 to be generated or received. Assuming that the redirector software 12 operating at the user's desktop system 10 is configured to redirect upon receiving a message from the user's mobile device 24, at step 86, the user can decide to generate a command message that will start redirection. If the user does so, then at step 88 the redirection message is composed and sent to the desktop system 10 via the wireless network 22, through the wireless gateway 20, via the Internet 18 to the LAN 14, and is finally routed to the desktop machine 10. In this situation where the mobile device 24 is sending a message directly to the desktop system 10, no outer wrapper is added to the message (such as message C in FIGS. 1 and 2). In addition to the redirection signal, the mobile device 24 could

transmit any number of other commands to control the operation of the host system, and in particular the redirector program 12. For example, the mobile 24 could transmit a command to put the host system into the preferred list mode, and then could transmit additional commands to add or subtract certain senders from the preferred list. In this manner, the mobile device 24 can dynamically limit the amount of information being redirected to it by minimizing the number of senders on the preferred list. Other example commands include: (1) a message to change the configuration of the host system to enable the mobile device 24 to receive and process certain attachments; and (2) a message to instruct the host system to redirect an entire data item to the mobile device in the situation where only a portion of a particular data item has been redirected.

[0059] Turning back to Figure 5, if the user signal or message is not a direct message to the desktop system 10 to begin redirection (or some other command), then control is passed to step 90, which determines if a message has been received. If a message is received by the mobile, and it is a message from the user's desktop 10, as determined at step 92, then at step 94 a desktop redirection flag is set "on" for this message, and control passes to step 96 where the outer envelope is removed. Following step 96, or in the situation where the message is not from the user's desktop, as determined at step 92, control passes to step 98, which displays the message for the user on the mobile device's display. The mobile unit 24 then returns to step 82 and waits for additional messages or signals.

[0060] If the mobile device 24 determines that a message has not been received at step 90, then control passes to step 100, where the mobile determines whether there is a message to send. If not, then the mobile unit returns to step 82 and waits for additional messages or signals. If there is at least one message to send, then at step 102 the mobile determines whether it is a reply message to a message that was received by the mobile unit. If the message to send is a reply message, then at step 108, the mobile determines whether the desktop redirection flag is on for this message. If the redirection flag is not on, then at step 106 the reply message is simply transmitted from the mobile device to the destination address via the wireless network 22. If, however, the redirection flag is on, then at step 110 the reply message is repackaged with the outer envelope having the addressing information of the user's desktop system 10, and the repackaged message is then transmitted to the desktop system 10 at step 106. As described

above, the redirector program 12 executing at the desktop system then strips the outer envelope and routes the reply message to the appropriate destination address using the address of the desktop system as the "from" field, so that to the recipient of the redirected message, it appears as though it originated from the user's desktop system rather than the mobile device.

[0061] If, at step 102, the mobile determines that the message is not a reply message, but an original message, then control passes to step 104, where the mobile determines if the user is using the redirector software 12 at the desktop system 10, by checking the mobile unit's configuration. If the user is not using the redirector software 12, then the message is simply transmitted to the destination address at step 106. If, however, the mobile determines that the user is using the redirector software 12 at the desktop system 10, then control passes to step 110, where the outer envelope is added to the message. The repackaged original message is then transmitted to the desktop system 10 at step 106, which, as described previously, strips the outer envelope and routes the message to the correct destination. Following transmission of the message at step 106, control of the mobile returns to step 82 and waits for additional messages or signals.

[0062] Referring now to Figures 13 and 14, one embodiment of a mobile device 24a is shown in Figure 13, and another embodiment of a mobile device 24b is shown in Figure 14. It will be appreciated that the numeral "24" will hereinafter refer to any mobile device 24, including the embodiments 24a and 24b. It will also be appreciated that a similar numbering convention may be used for other general features common between Figures 13 and 14 such as a display 180, a positioning device 182, and a cancel or escape button 184.

[0063] The mobile device 24a shown in Figure 13 comprises a display 180a and the cursor or view positioning device 182 shown in this embodiment is a positioning wheel 182a. Positioning device 182 may serve as another input member and is both rotatable to provide selection inputs to the processor 638 (see Figure 15) and can also be pressed in a direction generally toward housing to provide another selection input to the processor 638. The display 180 may include a selection cursor 750 (see Figure 17) that depicts generally where the next input or selection will be received. The mobile device 24a in Figure 13 also comprises an escape or cancel button

184a and a keyboard 188. In this example, the keyboard 188 is disposed on the front face of the mobile device housing and positioning device 182 and cancel button 184a are disposed at the side of the housing to enable a user to manoeuvre the scroll wheel 182a while holding the mobile device 24 in one hand. The keyboard 188 is in this embodiment a standard QWERTY keyboard.

[0064] The mobile device 24b shown in Figure 14 comprises a display 180b and the positioning device 182 in this embodiment is a trackball 182b. Trackball 182b permits multi-directional positioning of the selection cursor such that the selection cursor can be moved in an upward direction, in a downward direction and, if desired and/or permitted, in any diagonal direction. The trackball 182b is preferably situated on the front face of a housing for mobile device 24b as shown in Figure 14 to enable a user to manoeuvre the trackball 182b while holding the mobile device 24b in one hand. The trackball 182b may serve as another input member (in addition to a directional or positioning member) to provide selection inputs to the processor 638 and can preferably be pressed in a direction towards the housing of the mobile device 24b to provide such a selection input.

[0065] The mobile device 24b also comprises a menu or option button 186 that loads a menu or list of options on display 180b when pressed, and a cancel or escape button 184b to exit, "go back" or otherwise escape from a feature, option, selection or display. The mobile device 24b as illustrated in Figure 7, comprises a reduced QWERTY keyboard 190. In this embodiment, the keyboard 130, positioning device 182, escape button 184b and menu button 186 are disposed on a front face of a mobile device housing.

[0066] The reduced QWERTY keyboard 190 comprises a plurality of multi-functional keys and corresponding indicia including keys associated with alphabetic characters corresponding to a QWERTY array of letters A to Z and an overlaid numeric phone key arrangement. The plurality of keys that comprise alphabetic and/or numeric characters total fewer than twenty-six (26). In the embodiment shown, the number of keys that comprise alphabetic and numeric characters is fourteen (14). In this embodiment, the total number of keys, including other functional keys, is twenty (20). The plurality of keys may comprise four rows and five columns of keys, with the four rows comprising in order a first, second, third and fourth row, and the five

columns comprising in order a first, second, third, fourth, and fifth column. The QWERTY array of letters is associated with three of the four rows and the numeric phone key arrangement is associated with each of the four rows.

[0067] The numeric phone key arrangement is associated with three of the five columns. Specifically, the numeric phone key arrangement may be associated with the second, third and fourth columns. The numeric phone key arrangement may alternatively be associated with keys in the first, second, third, and fourth rows, with keys in the first row including a number "1" in the second column, a number "2" in the third column, and a number "3" in the fourth column. The numeric phone keys associated with keys in the second row include a number "4" in the second column, a number "5" in the third column, and a number "6" in the fourth column. The numeric phone keys associated with keys in the third row include a number "7" in the second column, a number "8" in the third column, and a number "9" in the fourth column. The numeric phone keys associated with keys in the fourth row may include a "*" in the second column, a number "0" in the third column, and a "#" in the fourth column.

[0068] The physical keyboard may also include a function associated with at least one of the plurality of keys. The fourth row of keys may include an "alt" function in the first column, a "next" function in the second column, a "space" function in the third column, a "shift" function in the fourth column, and a "return/enter" function in the fifth column.

[0069] The first row of five keys may comprise keys corresponding in order to letters "QW", "ER", "TY", "UI", and "OP". The second row of five keys may comprise keys corresponding in order to letters "AS", "DF", "GH", "JK", and "L". The third row of five keys may comprise keys corresponding in order to letters "ZX", "CV", "BN", and "M".

[0070] It will be appreciated that for the mobile device 24, a wide range of one or more positioning or cursor/view positioning mechanisms such as a touch pad, a joystick button, a mouse, a touchscreen, set of arrow keys, a tablet, an accelerometer (for sensing orientation and/or movements of the mobile device 24 etc.) or other whether presently known or unknown may be employed. Similarly, any variation of keyboard 188, 190 may be used. It will also be appreciated that the mobile devices 24 shown in Figures 13 and 14 are for illustrative purposes

only and various other mobile devices 24, presently known or unknown are equally applicable to the following examples.

[0071] Figure 15 is a detailed block diagram of a preferred mobile station 602 of the present disclosure. The term "mobile station" will herein refer to the operable components of, e.g. mobile device 24. Mobile station 602 is preferably a two-way communication device having at least voice and advanced data communication capabilities, including the capability to communicate with other computer systems. Depending on the functionality provided by mobile station 602, it may be referred to as a data messaging device, a two-way pager, a cellular telephone with data messaging capabilities, a wireless Internet appliance, or a data communication device (with or without telephony capabilities) – e.g. mobile device 24 shown in Figures 6 and 7. Mobile station 602 may communicate with any one of a plurality of fixed transceiver stations 600 within its geographic coverage area.

[0072] Mobile station 602 will normally incorporate a communication subsystem 611 which includes a receiver 612, a transmitter 614, and associated components such as one or more (preferably embedded or internal) antenna elements 616 and 618, local oscillators (LOs) 613, and a processing module such as a digital signal processor (DSP) 620. As will be apparent to those skilled in field of communications, particular design of communication subsystem 611 depends on the communication network in which mobile station 602 is intended to operate.

[0073] Mobile station 602 may send and receive communication signals over a network after required network registration or activation procedures have been completed. Signals received by antenna 616 through the network are input to receiver 612, which may perform such common receiver functions as signal amplification, frequency down conversion. filtering, channel selection, and like, and in example shown in Figure 15, analog-to-digital (A/D) conversion. A/D conversion of a received signal allows more complex communication functions such as demodulation and decoding to be performed in DSP 620. In a similar manner, signals to be transmitted are processed, including modulation and encoding, for example, by DSP 620. These DSP-processed signals are input to transmitter 614 for digital-to-analog (D/A) conversion, frequency up conversion, filtering, amplification and transmission over communication network

via antenna 618. DSP 620 not only processes communication signals, but also provides for receiver and transmitter control. For example, the gains applied to communication signals in receiver 612 and transmitter 614 may be adaptively controlled through automatic gain control algorithms implemented in DSP 620.

[0074] Network access is associated with a subscriber or user of mobile station 602. In one embodiment, mobile station 602 uses a Subscriber Identity Module or "SIM" card 662 to be inserted in a SIM interface 664 in order to operate in the network. SIM 662 is one type of a conventional "smart card" used to identify an end user (or subscriber) of the mobile station 602 and to personalize the device, among other things. Without SIM 662, the mobile station terminal in such an embodiment is not fully operational for communication through a wireless network. By inserting SIM 662 into mobile station 602, an end user can have access to any and all of his/her subscribed services. SIM 662 generally includes a processor and memory for storing information. Since SIM 662 is coupled to a SIM interface 664, it is coupled to microprocessor 638 through communication lines. In order to identify the subscriber, SIM 662 contains some user parameters such as an International Mobile Subscriber Identity (IMSI). An advantage of using SIM 662 is that end users are not necessarily bound by any single physical mobile station. SIM 662 may store additional user information for the mobile station as well, including datebook (or calendar) information and recent call information. It will be appreciated that mobile station 602 may also be used with other types of network applicable mobile devices 24 such as those being code division multiple access (CDMA) enabled and should not be limited to those using and/or having a SIM card 662.

[0075] Mobile station 602 is a battery-powered device so it also includes a battery interface 654 for receiving one or more rechargeable batteries 656. Such a battery 656 provides electrical power to most if not all electrical circuitry in mobile station 602, and battery interface 654 provides for a mechanical and electrical connection for it. The battery interface 654 is coupled to a regulator (not shown) which provides a regulated voltage V to all of the circuitry.

[0076] Mobile station 602 includes a microprocessor 638 which controls overall operation of mobile station 602. Communication functions, including at least data and voice communications

are performed through communication subsystem 611. Microprocessor 638 also interacts with additional device subsystems such as a display 622, a flash memory 624, a random access memory (RAM) 626, auxiliary input/output subsystems 628, a serial port 630, a keyboard 632, a speaker 634, a microphone 636, a short-range communications subsystem 640, and any other device subsystems generally designated at 642. Some of the subsystems shown in Figure 15 perform communication-related functions, whereas other subsystems may provide "resident" or on-device functions. Notably, some subsystems such as keyboard 632 and display 622, for example, may be used for both communication-related functions, such as entering a text message for transmission over a communication network, and device-resident functions such as a calculator or task list. Operating system software used by microprocessor 638 is preferably stored in a persistent store such as flash memory 624, which may alternatively be a read-only memory (ROM) or similar storage element (not shown). Those skilled in the art will appreciate that the operating system, specific device applications, or parts thereof, may be temporarily loaded into a volatile store such as RAM 626.

[0077] Microprocessor 638, in addition to its operating system functions, preferably enables execution of software applications on mobile station 602. A predetermined set of applications which control basic device operations, including at least data and voice communication applications, as well as the inventive functionality of the present disclosure, will normally be installed on mobile station 602 during its manufacture. A preferred application that may be loaded onto mobile station 602 may be a personal information manager (PIM) application having the ability to organize and manage data items relating to user such as, but not limited to, e-mail, calendar events, voice mails, appointments, and task items. Naturally, one or more memory stores are available on mobile station 602 and SIM 662 to facilitate storage of PIM data items and other information.

[0078] The PIM application preferably has the ability to send and receive data items via the wireless network. In the present disclosure, PIM data items are seamlessly integrated, synchronized, and updated via the wireless network, with the mobile station user's corresponding data items stored and/or associated with a host computer system thereby creating a mirrored host computer on mobile station 602 with respect to such items. This is especially advantageous

where the host computer system is the mobile station user's office computer system. Additional applications may also be loaded onto mobile station 602 through network, an auxiliary subsystem 628, serial port 630, short-range communications subsystem 640, or any other suitable subsystem 642, and installed by a user in RAM 626 or preferably a non-volatile store (not shown) for execution by microprocessor 638. Such flexibility in application installation increases the functionality of mobile station 602 and may provide enhanced on-device functions, communication-related functions, or both. For example, secure communication applications may enable electronic commerce functions and other such financial transactions to be performed using mobile station 602.

[0079] In a data communication mode, a received signal such as a text message, an e-mail message, or web page download will be processed by communication subsystem 611 and input to microprocessor 638. Microprocessor 638 will preferably further process the signal for output to display 622 or alternatively to auxiliary I/O device 628. A user of mobile station 602 may also compose data items, such as e-mail messages, for example, using keyboard 632 in conjunction with display 622 and possibly auxiliary I/O device 628. Keyboard 632 is preferably a complete alphanumeric keyboard and/or telephone-type keypad. These composed items may be transmitted over a communication network through communication subsystem 611.

[0080] For voice communications, the overall operation of mobile station 602 is substantially similar, except that the received signals would be output to speaker 634 and signals for transmission would be generated by microphone 636. Alternative voice or audio I/O subsystems, such as a voice message recording subsystem, may also be implemented on mobile station 602. Although voice or audio signal output is preferably accomplished primarily through speaker 634, display 622 may also be used to provide an indication of the identity of a calling party, duration of a voice call, or other voice call related information, as some examples.

[0081] Serial port 630 in Figure 15 is normally implemented in a personal digital assistant (PDA)-type communication device for which synchronization with a user's desktop computer is a desirable, albeit optional, component. Serial port 630 enables a user to set preferences through an external device or software application and extends the capabilities of mobile station 602 by

providing for information or software downloads to mobile station 602 other than through a wireless communication network. The alternate download path may, for example, be used to load an encryption key onto mobile station 602 through a direct and thus reliable and trusted connection to thereby provide secure device communication.

[0082] Short-range communications subsystem 640 of Figure 15 is an additional optional component which provides for communication between mobile station 602 and different systems or devices, which need not necessarily be similar devices. For example, subsystem 640 may include an infrared device and associated circuits and components, or a Bluetooth™ communication module to provide for communication with similarly enabled systems and devices. Bluetooth™ is a registered trademark of Bluetooth SIG, Inc.

[0083] Turning now to Figure 17, the mobile device 24 displays a home screen 700, which is preferably the active screen when the mobile device 24 is powered up and constitutes the main ribbon application. The home screen 700 generally comprises a status region 702 and a theme background 704, which provides a graphical background for the display 180. The theme background 704 displays a series of icons 706 in a predefined arrangement on a graphical background.

[0084] In some themes, the home screen 700 may limit the number icons 706 shown on the home screen 700 so as to not detract from the theme background 704, particularly where the background 704 is chosen for aesthetic reasons. The theme background 704 shown in Figure 17 provides a grid of icons. In other themes (not shown), a limited list of icons may be displayed in a column (or row) on the home screen along one portion of the display 180. In yet another theme, the entire list of icons may be listed in a continuous row along one side of the home screen on the display 180 enabling the user to scroll through the list while maintaining a limited number of currently visible icons on the display 180. In yet another theme (not shown), metadata may be displayed with each of a limited number of icons shown on the home screen. For example, the next two appointments in the user's calendar may be accessed by the processor 638 and displayed next to the calendar icon. It will be appreciated that preferably several themes are available for the user to select and that any applicable arrangement may be used.

[0085] One or more of the series of icons 706 is typically a folder 708 that itself is capable of organizing any number of applications therewithin.

[0086] The status region 702 in this embodiment comprises a date/time display 710 and an optional service provider logo 712. The theme background 704, in addition to a graphical background and the series of icons 706, also comprises a status bar 714. The status bar 714 provides information to the user based on the location of the selection cursor 750, e.g. by displaying a name for the icon 706 that is currently highlighted.

[0087] An application, such as a profiles application 728 (see Figure 16 described below), may then be initiated (opened or viewed) from display 180 by highlighting a profiles icon 716 using the positioning device 182, and providing a suitable user input to the mobile device 24. For example, profiles application 728 may be initiated by moving the positioning device 182 such that the profiles icon 716 is highlighted as shown in Figure 17, and providing a selection input, e.g. by pressing the trackball 182b.

[0088] Movement, navigation, and/or scrolling with use of a cursor/view positioning device 182 (e.g. trackball 182b or scroll wheel 182a) is beneficial given the relatively large size of visually displayed information and the compact size of display 180, and since information and messages are typically only partially presented in the limited view of display 180 at any given moment. As previously described, positioning device 182 – scroll wheel 182a and trackball 122b, are helpful cursor/view positioning mechanisms to achieve such movement. Positioning device 122, which may be referred to as a scroll wheel or scroll device 182a in one embodiment (Figure 13), specifically includes a circular disc which is rotatable about a fixed axis of housing and may be rotated by the end user's index finger or thumb. As noted above, in another embodiment (Figure 14) the trackball 182b comprises a multi-directional member that enables upward, downward and if desired, diagonal movements. The multi-directional movements afforded, in particular, by the trackball 182b and the presentation of the grid of icons 706 and folders 708 provides the user with flexibility and familiarity of the layout of a traditional desktop computer interface. Also, the positioning device 182 enables movement and selection operations to be executed on the mobile device 24 using one hand. The trackball 182b in particular also

enables both one-handed use and the ability to cause the cursor 182 to traverse the display 180 in more than one direction.

[0001] As shown in Figure 16, memory 624 includes a plurality of applications 726 associated with the series of icons 706 for the processing of data. Applications 726 may be any variety of forms such as, without limitation, software, firmware, and the like. Applications 726 may include, for example, the contacts application 730, electronic mail (e-mail) 732, calendar program 734, memo program 736, messages 738, search 740 etc. In one embodiment, the calendar application 734 stores a trigger 733 for controlling features of the mobile device 24, e.g. for certain calendar events; and stores a category 735 defining a set of rules for the user of that particular mobile device 24, which can be controlled by another entity. An operating system (OS) 742 also resides in memory 624. The mobile devices 24 of the present disclosure are also configured to enable communication between different ones of the applications, e.g. between contacts application 730 and the email application 732. Also, the icons 706 for the applications on the devices 24 can be modified, named, moved, sorted and otherwise interacted with for the purposes of organizing and/or manipulating the visibility of the icons for those applications 726.

[0002] Systems such as that described above with respect to Figures 1-5 often include mobile devices 24 that are purchased, distributed, and administered by an employer, for certain of their employees, as both a communication tool and/or as an incentive. Consequently, in such scenarios, the end user of the device 24 is not the sole owner of the device and, the employer typically has at least some discretion to control usage of the devices which have been purchased for their employees, most notably during working hours.

[0003] Figure 6 shows a schematic diagram of one example of a system for monitoring and controlling mobile device usage. In the example of Figure 6, desktop computer 28 is utilized by a first employee who wishes to schedule a meeting with a second employee, the second employee utilizing desktop 26. It will be appreciated that the example provided herein for scheduling a meeting using desktops 26 and 28 is purely for illustrative purposes only. For example, a meeting may also be scheduled between a wireless device and desktop, e.g., device 164 and desktop 26; between wireless devices, e.g., between devices 24 and 164; between a

desktop and a device, e.g. desktop 28 and device 24, etc. As such, it will be understood that the principles described above in conjunction with Figures 1-5 may be used to schedule meetings with or without accessing a desktop computer.

[0092] In this example, the first employee associated with desktop computer 28 has at least some authority over the second employee associated with desktop computer 26, e.g. supervisor, manager, senior partner, etc. The first employee associated with desktop computer 28 will hereinafter be referred to as a "Manager" and the second employee associated with desktop computer 26 will hereinafter be referred to as "Employee A". Desktops 28, 26 are connected to LAN 14 as described above. The Manager has a first mobile communications device 164 and Employee A has a second mobile communications device 24. It will be appreciated that in this example, both of the Manager and Employee A are employed by the same entity (not shown) and this entity has at least some discretion as to the usage of the devices 24, 164. In this first example, data items are redirected between the desktops 26, 28 and devices 24, 164 respectively through the server 11, redirector software 12, network 18 and gateway 20, using the principles outlined above in conjunction with Figures 1-5. It will be appreciated that, in another example (described below), data items can also be sent locally between devices (e.g. devices 24 and 164), in real-time; without utilizing the server 11, software 12, network 18 and gateway 20.

[0093] Employee A has a mail program running on desktop computer 26, which includes an inbox 120 for sending, receiving and viewing mail and other data items, and a calendar 124 for storing, viewing and organizing appointments and events. The Manager also has a calendar 126, and it will be appreciated that although not shown in Figure 6, the Manager has a mail program similar to Employee A, including an inbox (not shown). Such a mail program is typically provided by the employing entity in which case it runs from a server (e.g. server 11) on the LAN 14. In one example, the Manager interacts with a graphical user interface (GUI) 132 is displayed on desktop 28 for generating a meeting request 140a that includes rules for controlling the usage of Employee A's device 24 by initiating a lock to inhibit features or services provided by device 24 such as phone, email, games etc. It will be appreciated that a meeting request 140a may alternatively be generated using mobile device 164 (or device 24). GUI 132 is typically a

network administered program that runs on a server (e.g. server 11) connected to the LAN 14, and is accessible to the Manager and Employee A over the LAN 14.

[0094] Also connected to the LAN 14 is an administrator 130. The administrator 130 may be used to monitor and control usage of the devices 24, 164 by initiating a lock to inhibit selected ones of features or services provided by devices 24, 164. The administrator 130 includes a data storage device 134 that stores a rules database 136 and an administration log 138. The administrator 130 may alternatively take the form of a program running from any one or all of the desktops 26, 28 and devices 24, 164. In this alternative, the log 138 includes messages that are sent to a meeting coordinator (e.g. Manager) so that they can track device usage without relying on an administrator such as administrator 130. In this example, administrator 130 is shown as a separate entity to illustrate tasks for which it may be responsible.

[0095] The rules database 136 contains rule sets corresponding to selected features that are to be locked, permissions defining other users whose devices can be locked, and time/date information related to meetings or other restricted period for employees of the employing entity such as the Manager and Employee A. The time/date information includes a list of restricted periods that correspond to time periods during which certain features or services provided by the devices 24, 164, are to be disabled, restricted or locked (i.e. inhibited), e.g. during scheduled meetings. The administration log 138 contains time and date information related to such restricted periods and whether or not the rule sets have been complied with by certain employees. The information contained in the administration log 138, when available, is analyzed to enable the administrator 130 or other interested party to monitor the usage of the features or services intended to be locked on the devices 24, 164 during the restricted periods. The administrator 130 initiates the lock for inhibiting features of the devices 24, 164 by pushing policies, in this example policy packets 144, thereto. In general, policy packets 144 include data structures that include enabling/disabling events, and these data structures can alter device configuration to enable and disable features of the devices 24, 164.

[0096] As also shown by way of example in Figure 6, the device 24 includes a display interface 150 for displaying icons enabling a user to select various device features. In Figure 6,

the device 24 provides a mail program 152, a games option 158, an optional cancel lock feature 160 for manually disabling rules imposed by policy packet 144, and a telephone feature 162. The mail program 152 includes an inbox 154 for viewing mail items, and a send mail option 156 for composing and sending mail items.

[0097] If Employee A chooses to select the cancel lock option 160, they are preferably presented with a confirmation dialog (not shown) requesting final confirmation that they wish to disable the administrator imposed lock. In Figure 6, the games option 158 and phone option 162 icons are highlighted, indicating that a lock has been placed on those features, and thus they cannot be used whilst the lock is active. For example, a lock on the phone would typically at least inhibit the device from ringing when an incoming call is received, and may also completely inhibit use of the phone for a restricted period of time. The send mail option 156 is highlighted with a broken border indicating that a conditional lock is being imposed on this feature. A conditional lock allows a user to use this option only a particular, predetermined number of times or under certain conditions. Typically, if this predetermined amount of usage is exceeded, the option is then locked as will be explained in greater detail below.

[0098] The cancel lock option 160 may be configured to only apply to certain features, such as email. For example, a default locking rule may be imposed on the device 24 that forbids Employee A to be able to cancel a lock inhibiting the play of games on the device 24 during a meeting. Such a default locking rule can be imposed at the employing entity's discretion. In another example, the device 24 may be initially configured to have a back-up default lock that will automatically trigger when a meeting starts and especially in the case where a policy packet 144 has not been sent.

[0099] For example, an employee (not shown) enters a meeting without having any prior meeting details. In this case, another attendee (e.g. Employee A) sends meeting details directly to the new attendee via link 170 (explained below), which would then initiate the default locking rules for the new attendee's device (not shown). This option allows for certain features, e.g. games, to be locked in every meeting, whether or not the particular attendee has previously entered the meeting information into their device 24 or desktop 26. In addition, a location

sensing device included in a mobile device, such as a global positioning system (GPS) or radio frequency (RF) identification (ID) can also be used to determine when a mobile device has entered a "meeting zone", which would then automatically trigger the default lock. Therefore, at the employer's discretion, any set of rule guidelines can be implemented to suit their needs or corporate policies.

[00100] The devices 24, 164 typically include a direct, non-network supported link 170 between each other, such as a WiFi, Bluetooth or Infrared (IR) link. In another example described in greater detail below, the link 170 is also used to apply a lock, particularly when access to the wireless gateway 20 is limited or non-existent or to intentionally impose rules for limiting or disabling features of another user's device in real-time. For example, a meeting room below ground may temporarily inhibit the devices 24, 164 from communicating with the wireless gateway 20. In this scenario, the policy packets 144 typically cannot reach the devices 24, 164. Alternatively, the Manager may wish to invoke a locally generated policy packet 144a in real time to lock device 24 during the meeting, in order to disable devices that are being used and have since become a distraction. Policy packet 144a is generated by a lock program 168 accessible through interface 166 provided by device 164. The lock program 168 either pushes a policy packet 144a directly to Employee A, or broadcasts packet 144a within a particular area, thereby locking any device that is being used within that area. It will be appreciated that such options are at the discretion of the employing entity and are typically monitored and controlled by the administrator 130, and would be subject to pre-established permissions and policies.

[00101] As shown in Figure 6, the Manager may schedule a meeting using device 164, producing a meeting request 144d that can be sent directly to device 24 over link 170. The link 170 is particularly useful for scheduling meetings and forwarding policies (e.g. policy packet 144a) during a meeting, or to impose additional rules etc. in real time. For example, a meeting request 140a may be initially generated without imposing any rules. At some other time, or even during the meeting, the Manager may wish to change, update, add or remove certain rules for locking certain devices. Moreover, the Manager can first schedule a meeting and then delegate the responsibility of applying a lock to another employee, e.g. a meeting coordinator or secretary. Therefore, any device used by any entity can be suitably adapted for sending policy packets, e.g.

over link 170, in order to restrict or disable features of the device 24 and need not rely on an administrator 130.

[00102] An exemplary GUI 132 is shown in greater detail in Figure 7. The GUI 132 provides an entry box 200 for entering the name of the organizer of the meeting. The box 200 is populated with the name of the user interacting with the GUI 132 (e.g. the Manager) but may also allow a user to change the name of the organizer, e.g. when scheduled by a secretary or other employee on that user's behalf. An attendee entry box 202 allows a user to enter one or more requested attendees for the meeting (e.g. Employee A). A time/date option 204 allows the user to set the time and date for the meeting. The duration of the meeting will define a "restricted period" which represents a certain period of time where a lock is initiated for inhibiting certain features or services provided by the devices 24 and 164 in order to limit and/or control usage of the devices 24 and 164.

[00103] In the present example, the Manager may, for example, choose to hold a meeting between 2 pm and 5 pm on Monday. Consequently, a three hour restricted period is defined in which a set of rules is imposed on the devices belonging to the attendees of the meeting by initiating a lock. A rule set option 206 allows the Manager to select a pre-defined set of rules (defined by a rule set), or individual rules to impose during the meeting. For example, the Manager may wish to lock distracting features such as telephone and games options, but may allow an attendee to view mail in case an emergency arises. The effects of these rules will be explained in greater detail below. A message box 208 is also provided to enable the Manager to append a message to the meeting request 140a, such as a warning about the rules imposed or an agenda for the meeting. It will be appreciated that the features provided by the GUI 132, shown in Figure 7 are for illustrative purposes only, and any number of variations may exist as desired.

[00104] The above features would typically impose a particular rule or rule set to all attendees listed in the attendee box 202. If the Manager wishes to apply different rule sets to different employees, a customize option 212 may be used instead. The customize option 212 includes a list of the attendees 214 and a rule set selector 216 for each attendee. Typically, the extent to which the rules can be applied is limited by the nature of the user's position within the

employing entity. For example, the Manager may be allowed to impose any lock on Employee A, since Employee A (in this example) reports to the Manager. However, if the Manager was inviting an executive or vice president (not shown) to attend the meeting, e.g., as a speaker, they may not have permission to impose certain (or any) rules on such a user.

[00105] In these types of scenarios, the customize feature 212 allows the Manager to tailor the policy packets 144 to suit not only the nature of the meeting but also to accommodate permissions and any exceptional circumstances. For example, it may be known in advance that Employee A is expecting a very important email that they must acknowledge receipt of. In this case, the Manager can waive rules pertaining to viewing and sending mail, or may impose a conditional lock, which will be explained in greater detail below. Once the data is entered in the GUI 132, the user then chooses a send option 210, which will generate and send the meeting request 144a to the requested attendees. When sending a meeting request 144d over link 170, it will be appreciated that the options provided by GUI 132 are preferably available to the user in the lock program 168.

[00106] An example of the rules database 136 is shown in Figure 8. The rules database 136 generally comprises device related data 228 and user related data 220. For example, the user related data 220 includes records 222 of restricted periods for Employee A, a record 224 of cancelled locks for Employee A, and a list 226 of permissions for Employee A. The permissions include a hierarchical tier indicating Employee A's relative position or seniority within the company. For example, if there are five (5) tiers and Employee A is in tier three (3), Employee A may set rules and thus be able to lock employees in tiers one (1) and two (2) and restrictively in tier three (3). However, in the case where generation of a meeting request 140a is delegated to another employee, there should be an option to enable a user to impose a lock on another user that is in a higher tier.

[00107] The device related data 228 includes a set of predefined rules and/or sets of rules that can be imposed on the devices 24, 164. For example, devices that include games can impose a games lock. Preferably, the administrator 130 governs the establishment of, and discretion for, creating and applying the rules. However, a manifestation of the rules database 136 may also be

included or be accessible to the lock program 168 to enable a user (e.g. the Manager) to select or view the rule sets when generating a meeting request 140d and policy packet 144a.

[00108] The rule sets should be flexible and adaptable depending on the nature of the employing entity and the nature of the restricted period. For example, if a meeting request 140a is used by the Manager to schedule a social function, the rules should be more relaxed than those imposed during a meeting having a specially invited speaker. The rules should also be able to vary in degree throughout a restricted period, and thus different rule sets are applied for certain intervals within the meeting. For example, if a speaker is scheduled for the first 30 minutes, a strict set of rules may be applied for that interval and certain rules relaxed thereafter.

[00109] An exemplary method for pushing a policy packet 144 to device 24 for imposing a set of rules requested by the Manager using GUI 132 is shown in Figure 9, making reference to Figures 6 and 7. In the example shown in Figure 9, the Manager wishes to schedule a meeting with Employee A. The Manager first prepares a meeting request at step 300, by accessing GUI 132 and selecting the preferred criteria. For example, the organizer box 200 would indicate the Manager's name and optionally their title; the attendee box 202 would indicate Employee A and optionally their title; and the time/date option 204 would indicate a day and time for the meeting. Since the meeting includes only one attendee, the rule set option 206 can be used to select a rule set. Preferably, certain rule sets will include a minimum rule set plus other additional rules. For example, all meeting related requests can include a default lock on games 158, a default "silent" setting for phone 162, and other discretionary rules based on the permissions 226. The permissions 226 for the Manager and Employee A are preferably determined by the GUI 132 in order to tailor a rule set for the particular meeting. The rules database 136 is preferably accessed by the GUI 132 in order to obtain the user related data 220 pertinent to the selection of appropriate rules. Alternatively, the employing entity may impose a strict selection of rule sets that are automatically presented to the meeting organizer, based on the permissions 226 and the type of meeting request 140a.

[00110] At step 302, the meeting request 140a is sent to (or sent by) the administrator 130. When the meeting request 140a is sent, the Manager's calendar program 126 is populated with

details of the meeting at step 304 and may include a notice indicating that certain features of the devices 24, 164 will be restricted during the meeting. The meeting request 140b, which represents a copy of the request 140a possessed by the administrator 130, is used by the administrator 130 to update the databases 136 and 138 and to generate a policy packet 144 that will be pushed to the device 24 at step 306.

[00111] In this example, another copy of the request 140c is received by Employee A through inbox 120 at step 308, and Employee A will choose to accept, decline, or tentatively accept the meeting request by making a selection in option 142. The meeting request 140c will preferably indicate to Employee A that certain functionality is restricted during this meeting. For the purpose of this example, Employee A accepts the meeting request 140c, and its calendar program 124 is updated at step 310. An indication that the meeting has been accepted (e.g. an acceptance message) is sent back to the administrator 130 at step 312 and a copy is sent back to the Manager at step 314.

[00112] Details of the meeting request are pushed to the devices 24 and 164 at step 320 using the principles outlined with respect to Figures 1-5 above. The Manager and Employee will then also have the meeting details available to them on their respective devices 164, 24 in order for them to view such details when they are away from their respective desktop computers 28, 26. The meeting details are added to the device calendars at steps 322 and 324. The meeting details will preferably include an indication that certain functionality will be disabled for the duration of the meeting. For example a "lock" icon may be displayed or a note including text that lists the functions that will be disabled. The lock icon may also be presented to the user prior to the time at which the rules are triggered in order to present a "lock reminder" to the user. This reminder is preferably implemented with a conventional calendar reminder that indicates that a meeting is forthcoming.

[00113] Preferably, Employee A and the Manager are provisioned a security key that is only known to them and the server 11. This key can be provided either in the meeting request 140a or 140c, or may be included in an initialization (not shown) that occurs prior to the meeting being scheduled. The security key is used to authenticate the policy packet pushed at step 316 to verify

the validity of the request by the administrator 130 to lock certain features provided by the device 24. The packet 144a may also be validated in this way, thus the packets 144, 144a are preferably medium independent since in this case they are authenticated on the device 24 or 164.

[00114] The administrator 130 then also pushes the policy packet 144 generated in step 306 to the device 24 at step 316. The policy packet 144 is either pushed immediately upon generation of the meeting request, or is pushed at a later time, closer to the start time for the meeting or when Employee A confirms that they will be attending the meeting. Preferably, the policy packet 144 places a trigger 733 (see Figure 16) within the device 24 that will automatically lock features based on the rules imposed when the restricted period begins. The rules carried by the policy packet 144 are preferably stored in a policy/category definition 735 (see Figure 16). The trigger 133 is stored in the device 24 at step 318. Preferably, the device 24 will first authenticate the packet 144 at step 318 to validate that the policies included in the packet come from a recognized entity (e.g. administrator 130 or Manager).

[00115] The device 24 then parses the commands included in the packet 144 which will indicate what features are to be inhibited. The commands may be conveyed in any manner that is suitable to the architecture employed by the device 24. For example, a list of services may be included in the packet with a Boolean "0" or "1" to indicate disable and enable respectively. Alternatively, the device 24 includes pre-existing knowledge of the rule sets 228 and the packet 144 then simply sends a profile identifier indicating which rule set will be applied. The pre-existing knowledge is obtained either when the device 24 is provisioned or at any other suitable time. For example, the commands included in the packet 144 are stored in the trigger 733 in the calendar application 734 as shown in Figure 16, and have respective unique identifiers associated therewith. A timer for the lock stored in the trigger 733, is registered with the operating system 732 that is continually running. The identifier indicates what entry (including a set of commands) in the trigger 733 is linked to a particular execution time. The operating system 732 then provides a call back to check with the timer to see if it is within the restricted period, e.g., every 10ms. If the timer indicates that it is within the restricted period then the commands related to the policy are initiated by having the processor 238 initiate the trigger 733, which in

turn identifies the rules from the stored policy 735 and, when the restricted period finishes, the timer de-registers itself with the operating system 732.

[00116] As noted above, the trigger 733 will preferably include a warning prior to the meeting that certain rules will be imposed, in case Employee A is not attending the meeting and thus a lock on device 24 is not necessary. Such a warning is included in a routine reminder dialog that appears at a certain time prior to the meeting. This dialog allows Employee A to decline the meeting and thus cancel the lock. Also, the device 24 may be synchronized at desktop 26, which indicates that the device cannot be present in the meeting, in which case a lock on the device 24 is either unnecessary or inconsequential. In an alternative embodiment, the policy packet 144 may be sent at the time which the meeting reminder is provided. It will be appreciated that the policy packet 144 is sent at any suitable time prior to the commencement of the meeting and subsequent to the generation of the meeting request 140a.

[00117] In another example, a meeting organized by the Manager, and including Employee A takes place in an area that does not provide wireless coverage, and thus the devices 24 and 164 cannot access wireless gateway 20. It will be appreciated that the following principles are also applicable to generating and imposing policies in real-time and thus any entity may be employed for creating a policy to restrict or disable the usage of a device 24. In this example, the Manager selects only the minimum default lock, namely to lock games and phone during the meeting. If the Manager at some time during the meeting wishes to add a lock (e.g. conditional lock) for mail usage, they send an additional policy packet 144a as shown in Figure 11. The Manager would first access the lock program 168 using their display 166 at step 440. The lock program 168 allows the Manager to push policies to Employee A without the need to synchronize with the desktops 26, 28 since access to the redirector software 12 is unavailable in this scenario. The lock program 168 preferably provides a version of the GUI 132 enabling the Manager to set and/or refine the parameters shown in Figure 11 at step 442.

[00118] The device 164 would then prepare a local policy packet 144a at step 444 and push the packet 144a over link 170 to the device 24 at step 446. The packet 144a will then place a trigger 733 in the device (or immediately trigger 733 if done in real time) as discussed above and

shown in Figure 10. It will be appreciated that preferably, the Manager and Employee A are provisioned with a security key prior to the meeting in order for Employee A to authenticate packet 144a sent by the Manager. The lock program 168 therefore allows the Manager to remove, apply or revise the rule sets in real time during a meeting. This feature is applicable whether or not service is available to the devices 24, 164. Preferably, the packets 144a are able to be broadcast to multiple attendees at the same time, within a certain range of the device 164. Preferably, the devices 164 and 24 are also able to authenticate each other using cryptographic or other secure measures, e.g., certificates, digital signatures, etc.

[00119] In a variation of the above example, the Manager and Employee A spontaneously schedules a meeting without sending a prior meeting request. In this case, the Manager generates a meeting request 140d, which includes the opportunity to apply certain rules at that time. Alternatively, the Manager accesses the lock program 68 and proceeds with the steps set forth in Figure 11.

[00120] An exemplary method for implementing a policy trigger 733 on device 24 is shown in Figure 10. As indicated above, preferably, the policy packet 144 is triggered in the device 24 at the time of the meeting. However, prior to triggering, a locking reminder is preferably presented to Employee A. At step 400, a warning dialog is presented on the display 150 for Employee A to confirm their attendance. If Employee A indicates that they are still planning to attend the meeting, the rules are applied at step 402. As shown in Figure 6 and mentioned above, the games 158 and phone 162 features are locked for the duration of the meeting, and a conditional lock is placed on the send mail option 156.

[00121] In this example, the Manager has chosen a rule set that allows Employee A to send mail messages a limited number of times in order to allow Employee A to respond to a certain number of messages. As also shown in Figure 6, Employee A preferably has unrestricted access to their inbox 154 (i.e. no lock has been placed on inbox 154). The conditional lock on the send mail option 156 allows the organizer of the meeting (e.g. the Manager) to place the onus on the attendee for triggering a lock on certain features of device 24. This allows the Manager to

portray a sense of trust towards Employee A and allow for certain discretions in the case of important emails, but also to ensure that distracting behaviour can be limited or inhibited.

[00122] For example, during a two hour meeting, it would be reasonable to allow attendees to view their inbox and respond to a few (e.g. five or six) emails over the course of the meeting. In this case, a conditional lock allows the organizer to provide some flexibility, while restricting frequent messaging. Preferably, if a conditional lock is breached then a conditional breach packet 163 is pushed by the device 24 back to the administrator 130 to update the administration log 138.

[00123] At step 404, the rules imposed by the policy packet 144 are active for the duration of the meeting. However, as shown in Figure 10, step 406 allows Employee A to use features within the defined conditional rules. The conditional rules would also typically include unlimited use of features that are not locked, such as the inbox 154 in this example. During conditional usage, the device 24 continually checks to see if any conditions have been breached at step 408. If use of the conditional feature is below a pre-determined threshold defined by the conditions, then the conditional usage resumes. However, if a conditional lock is breached, an additional lock is added at step 409 and step 404 continues. The additional lock would typically change the conditional restriction on the feature (e.g. send mail) to a full lock thus restricting any further use.

[00124] During step 404, another option is permitted, namely an option to cancel the lock 160. If the cancel option 160 is not selected, the rules 404 are maintained in force for the duration of the meeting. If the cancel option 160 is selected at step 410, a cancel indicator, such as cancel packet 161 is prepared at step 412 and the cancel packet 161 is pushed to the administrator 130 at step 414. It will be understood that the cancel option 160 should only apply to those features that can be unlocked according to the policies set by the employing entity. If default rules are implemented, certain features, e.g. games or cell phone, should remain locked despite any attempt to cancel the lock during a restricted period.

[00125] For example, Employee A may wish to step out of the meeting, leave early, or a break may occur. In such scenarios, Employee A continually has the option to cancel the lock and

resume use of all functions offered by the device 24. As mentioned above, by selecting the cancel lock option 160, a cancel packet 161 is pushed back to the administrator 130. Certain cancel packets 161 may be expected during scheduled breaks, and may also be required during exceptional circumstances. In any case, the cancel packet 161 indicates to the administrator 130 that the lock was removed, and allows the administrator 130 to investigate further if necessary. Alternatively, a lock that has been triggered, relinquishes at certain predetermined intervals to accommodate scheduled breaks, e.g., lunch periods. The policy packets 144 may be tailored to offer such flexibility so as to minimize disruptions in service to the attendees while also minimizing distractions during the meeting.

[00126] Therefore, device usage can be monitored and the use of certain services or features restricted by pushing policy packets 144 from an administrator 130 to the device 24. The policy packets 144 impose a certain set of rules that "lock" certain features provided by the device, according to permissions and pre-established policies, for a certain period of time. Such restricted periods coincide with meetings or other events in which distractions should be kept to a minimum. Preferably, the rules include conditional locks that allow a user to use a feature a reasonable number of times before the lock is activated to place the onus on the user for minimizing such distractions, while enabling the user to maintain access to an often important communication tool. Moreover, the use of cancel packets 161, conditional packets 163, and the administration log 138 allows an administrator 130 to not only control but to monitor the application of the rule sets and when certain conditions are breached, which provides an employer with sufficient information to use in auditing device usage or in reprimanding users for misuse of a privilege such as the use of a mobile data communications device 24, 164.

[00127] A further embodiment shown in Figure 12 enables a service provider to restrict access to a service during restricted periods. In the embodiment shown in Figure 12, users access a service through a network and the service provider controls access to and limits and/or monitors the period of time during which the service is provided. An Internet service is provided to a campus network 500, such as that provided at a university. The network 500 is embodied as a LAN and includes a first user operating a first computer 502 (hereinafter User A) and a second user operating a second computer 504 (hereinafter User B). Typically, the network 500 includes

wireless access for laptops and other portable computing devices, and thus the computers 502, 504 are preferably laptop computers that may be used by User A and User B respectively when in the range of the wireless service. A campus Internet service provider 508 operates a server 506 for providing access to the Internet and other network resources. The provider 508 also controls access to the Internet. The provider 508 includes a data storage device 510 that includes a timetable database 512 that outlines restricted periods for User A and User B.

[00128] Typically, a student such as User A, has designated lecture periods, and has the option to use their laptop 502 for taking notes etc. However, often if a wireless network is present, User A is able to use instant messaging or browse the Internet during a lecture, which is often distracting to other participants in the same environment. Since the Internet service is provided to User A, is usually free of charge, the provider 508 often has the discretion to restrict Internet access during lecture periods. In order to do so, the provider 508 will typically have access to the timetable database 512. Certain measures should be taken to ensure privacy, e.g. by associating a timetable with a user ID that does not reveal the student's name. As shown in Figure 12, when User A wishes to access the Internet, a connection attempt 514 is made with the server 506. The provider 508 consults the database 516 when a connection attempt 514 is made to determine if User A is scheduled to be in a lecture. If they are, the provider denies access 518 during that period.

[00129] In some cases, User A may be connected prior to the lecture, and thus could maintain their connection during the lecture. In such cases, the provider conducts a regular poll in order to determine if connections do exist, and then disconnects users during restricted periods. In other cases, User A that does not attend a lecture in order to work on another project may need Internet access in a lab or other room. Preferably, users will be able to exercise a cancel lock option (not shown) similar to that described with reference to Figure 6. Alternatively, a user's location within the network 500 may be detectable through RF ID or through other detection means at local network access points, in which case a user's access may only be restricted if they are trying to connect to the network 500 from within the expected location of the lecture. Accordingly, rule sets are defined that can be exercised by the provider 508 to minimize unnecessary service interruption while also minimizing distractions and disruptions.

[00130] In another scenario, User A and User B are logged onto PCs 502 and 504 respectively in a computer lab. In this scenario the location of the PCs 502 and 504 is fixed, and, Internet usage as well as the use of other programs such as games can be inhibited in a manner similar to that described above with respect to Figure 12. Accordingly, e.g., when User A is logged on during a schedule lab period, the service provider 508 is able to inhibit distracting behaviour by controlling the use of certain programs that are likely to cause a distraction.

[00131] In another embodiment, the devices 24 and 164 includes a GPS or other suitable location determining feature (not shown) for engaging and disengaging a lock that is imposed on the devices 24 and 164. For example, when Employee A enters a meeting room during a scheduled meeting, the device 24 (or a network connected detector, not shown) detects the presence of Employee A in the meeting and then initiates a policy packet 144. If the policy packet originates from the network 14, the packet is pushed through the redirector server software 12 as described above. If the device 24 itself triggers the lock, the device 24 imposes a default lock as also described above. In this example, when Employee A enters the meeting, features such as games and phone are disabled until they exit the meeting.

[00132] Likewise, if Employee A leaves a meeting prior to completion, such a change in location could be tracked in order to automatically disengage the lock without requiring Employee A to manually choose the cancel lock 160 option.

[00133] Accordingly, various implementations of the principles discussed above may be incorporated to include any suitable level of sophistication as desired by the employing entity. In the result, device usage may be controlled by any entity with the appropriate permissions to do so, for inhibiting distracting behaviour and to encourage only necessary usage of the device during particular restricted time periods.

[00134] In yet another embodiment, shown in Figure 19, the principles discussed above for controlling use of the mobile device 24 can be extended to control the mobile device 24 during any predetermined period of time, in addition to, or rather than, as dictated by calendar appointments.

[00135] In the example shown in Figure 19, an administrator 130 having a data storage device 14 storing a rules database 136 and administration log 138, controls the use of the mobile device 24, similar to the embodiment shown in Figure 6. In the embodiment of Figure 19, the administrator 130 pushes or sends a specific type of policy packet, in this example, a category packet 760 to the mobile device 24 in a manner similar to that described above with respect to Figure 6. The category packet 760 may be a modified policy packet 144 or may comprise its own configuration. The category packet 760 is received by the processor 638 and stored in memory 624, e.g. in the calendar application 734 as a category definition 735 with associated trigger 733. It will be appreciated that the category definition 735 may be stored in any portion of memory 624 and is shown stored in the calendar application 734 for illustrative purposes only.

[00136] The category definition 735 is shown in Figure 18, and comprises generally one or more feature restrictions 752, one or more time restrictions 754 and one or more exemptions 756 if applicable. The category definition 735 is associated with the mobile device's internal clock, similar to the trigger 733, however, the time restrictions 754 are predefined and are not associated with a particular calendar event as is the policy packet 144 shown in Figure 6.

[00137] For example, the time restrictions 754 may cause the trigger 733 to restrict certain features (i.e. implement feature restrictions 752) for predefined blocks of the day, such as during working hours. For example, where the administrator 130 wishes to control use of email, games, phone etc. while Employee A is supposed to be at work, the category definition 735 can be imposed on the mobile device 24 by pushing the category packet 760 to the mobile device 24. Similar to the calendar-associated policy packets 144, a cancel packet 161 can be generated for emergency or urgent purposes to "unlock" the features. The exemptions 756 may include information related to vacation days, statutory holidays or special circumstances where the trigger 733 should not be implemented.

[00138] The administrator 130 can apply a single category to each user over which it has control, or may provide multiple category levels for varying permissions. For example, a normal user, e.g. Employee A, may be restricted from sending emails, web surfing and playing games during the hours of 9 am to 5 pm but those features released after work hours. In this way, the

administrator 130 can inhibit Employee A from pretending to be in the office when they are not by virtue of the connectivity provided by the mobile device 24. However, if Employee A needs to leave work for an emergency, or for an external meeting away from their desk, they can select the cancel lock 160 using a suitable input mechanism, and a cancel packet 161 is created and sent back to the administrator 130 to log the event in the administration log 138. In this way, Employee A can get access to features when appropriate, but if done repeatedly, this behaviour can be audited by the administrator 130, and appropriate action taken if necessary.

[00139] Another category level, e.g. for Manager, may have no restrictions on email but only for games and web surfing. Similarly, an executive, owner etc. may have absolutely no restrictions and thus the category definition 735 would comprise an empty entry in the time restrictions 754 or an empty entry in the feature restrictions 752, thereby avoiding implementation of the trigger 733 at any time (unless a policy packet 160 is appropriately applied). For users having no restrictions, the category definition 735 may instead be blocked by the mobile device 24 or the administrator 130 may be unable to create the category packet 760.

[00140] It will be appreciated that the category definition 735 may be stored in the mobile device 24 at the time of manufacture, stored during a provisioning or set up procedure or may be empty initially and have to be set using the category packet 760. Preferably, the category packet 760 can be used to dynamically change the category definition 735 as desired, e.g. when a user's status in the company changes. Similarly, category packets 760 can be used to update the exemptions 756 for holidays etc. such that the trigger 733 can be suppressed at appropriate times.

[00141] It can therefore be seen that mobile device usage can also be restricted on a regular basis according to predefined time intervals to limit the use of the mobile device 24 when appropriate. In this way, a user can be profiled based on the nature of their job to inhibit unaccounted absences made available through the connectivity provided by the mobile device 24. The administration log 138 may also be used to keep track of deviations from the restrictions, e.g. when a cancel packet 161 is initiated for auditing and/or to track suspect behaviour. It will be appreciated that the category packet 760 may be created and pushed to the

mobile device 24 by any other entity and may even be another mobile device 24, similar to the communication link 170 shown in Figure 6 and described above.

[00142] Similarly, it will be appreciated that the conditional packets 163 are equally applicable to the embodiment shown in Figure 19 and thus may also be used to enable controlled conditional access to certain features during the predetermined restricted periods, e.g. during the work day.

[00143] It will be appreciated that the particular options, outcomes, applications, screen shots and icons shown in the figures and described above are for illustrative purposes only and many other variations can be used according to the principles described.

[00144] Although the above has been described with reference to certain specific embodiments, various modifications thereof will be apparent to those skilled in the art as outlined in the appended claims.

Claims:

1. A method for controlling usage of features provided by a first mobile device in a communication system, said method comprising:

receiving a set of rules at said first mobile device from a second device, said set of rules having been selected from a user interface on said second mobile device and having been broadcast by said second mobile device to a plurality of mobile devices for controlling usage of particular features on said plurality of mobile devices, said set of rules comprising one or more feature restrictions and one or more time restrictions for restricting usage of said particular features during one or more predetermined restricted periods, said set of rules being selected on said second device from a plurality of rules, wherein which of said plurality of rules can be assigned to said plurality of mobile devices is limited by permissions to impose particular rules;

storing said set of rules on said first mobile device; and

applying said feature restrictions for the duration of said one or more predetermined restricted periods according to said set of rules.

2. The method according to claim 1, further comprising upon receiving a policy packet comprising a change to the set of rules, applying one or more changes to at least one of said one or more feature restrictions and said one or more time restrictions in said set of rules on said first device, to thereby dynamically change said set of rules on said first mobile device to accommodate a change in a category level or enable a temporary exemption.

3. The method according to claim 1 or claim 2, further comprising said first mobile device authenticating said set of rules to validate an origin of said set of rules.

4. The method according to any one of claims 1 to 3 wherein said feature restrictions are implemented on a regular basis.

5. The method according to claim 4 wherein said regular basis comprises one or more predefined blocks of a day.

6. The method according to any one of claims 1 to 5 further comprising, during said one or more restricted periods, providing an option to cancel one or more of said feature restrictions to thereby enable one or more features that have been inhibited by said set of rules.

7. The method according to claim 6 wherein upon selection of said option, said first mobile device generates a cancel indicator and sends said cancel indicator to said second mobile device for monitoring usage.

8. The method according to any one of claims 1 to 7 wherein said set of rules comprises at least one conditional rule, said conditional rule allowing a conditional feature to be used a predetermined number of times during said restricted period, wherein if said predetermined number of times is exceeded, said conditional feature is disabled thereafter and a conditional indicator is provided to said second mobile device for monitoring said usage.

9. The method according to any one of claims 1 to 8 wherein said set of rules is chosen from multiple category levels for varying permissions.

10. The method according to any one of claims 1 to 9, wherein said set of rules further comprises one or more exemptions related to circumstances where triggering said feature restrictions should not be implemented.

11. The method according to any one of claims 1 to 10, wherein said set of rules is received from said second mobile device via a direct non-network supported link.

12. A first mobile device for a communications network in which usage of features provided by the first mobile device is controllable, the first mobile device comprising:

a processor; and

a memory for storing computer readable instructions executable by the processor for causing the first mobile device to implement the method of any one of claims 1 to 11.

13. A computer readable medium storing computer readable instructions executable by a processor of a first mobile device for causing said first mobile device to implement the method of any one of claims 1 to 11.

14. A method of controlling usage of features provided by a plurality of first mobile devices in a communication system, said method comprising a second mobile device:

detecting in a user interface on the second mobile device, selection of a set of rules from a plurality of rules to be broadcast to said plurality of first mobile devices, wherein which of said plurality of rules can be assigned to said plurality of first devices is limited by permissions to impose particular rules, said set of rules comprising one or more feature restrictions and one or more time restrictions for restricting usage of said particular features during one or more predetermined restricted periods; and

broadcasting said set of rules to said plurality of first mobile devices to have said set of rules stored on respective ones of said plurality of first mobile devices.

15. The method according to claim 14, further comprising sending a policy packet to said plurality of first mobile devices, said policy packet comprising a change to said set of rules for applying one or more changes to at least one of said one or more feature restrictions and said one or more time restrictions in said set of rules on said plurality of first mobile devices to thereby change said set of rules on said plurality of first mobile devices to accommodate a change in a category level or enable a temporary exemption.

16. The method according to claim 14 or claim 15, further comprising using a security key to enable said second mobile device to authenticate said set of rules.

17. The method according to any one of claims 14 to 16, wherein said feature restrictions are implemented on a regular basis.

18. The method according to claim 17 wherein said regular basis comprises one or more predefined blocks of a day.

19. The method according to any one of claims 14 to 18, further comprising providing an option to cancel one or more of said feature restrictions inhibited by said set of rules.

20. The method according to claim 19, further comprising receiving a cancel indicator from at least one of said plurality of first mobile devices indicative of selection of said option.

21. The method according to any one of claims 14 to 20, wherein said set of rules further comprises at least one conditional rule, said conditional rule allowing a conditional feature to be used a predetermined number of times during said restricted period, wherein if said predetermined number of times is exceeded, said conditional feature is disabled thereafter and a conditional indicator is received by said second mobile device for monitoring said usage.

22. The method according to any one of claims 14 to 21 further comprising selecting said set of rules from a plurality of rule sets contained in a rules database.

23. The method according to any one of claims 14 to 22 further comprising monitoring usage by updating an administration log.

24. The method according to any one of claims 14 to 23 wherein which of said plurality of rules is selected is dictated by an organizational structure.

25. The method according to any one of claims 14 to 24, wherein said set of rules is broadcast by the second mobile device via a direct non-network supported link.

26. A second mobile device in a communications network for controlling usage of features provided by a plurality of first mobile devices, the second mobile device comprising:

a processor; and

a memory for storing computer readable instructions executable by the processor for causing the second mobile device to implement the method of any one of claims 14 to 25.

27. A computer readable medium storing computer readable instructions executable by a processor of a second mobile device for causing said second mobile device to implement the method of any one of claims 14 to 25.

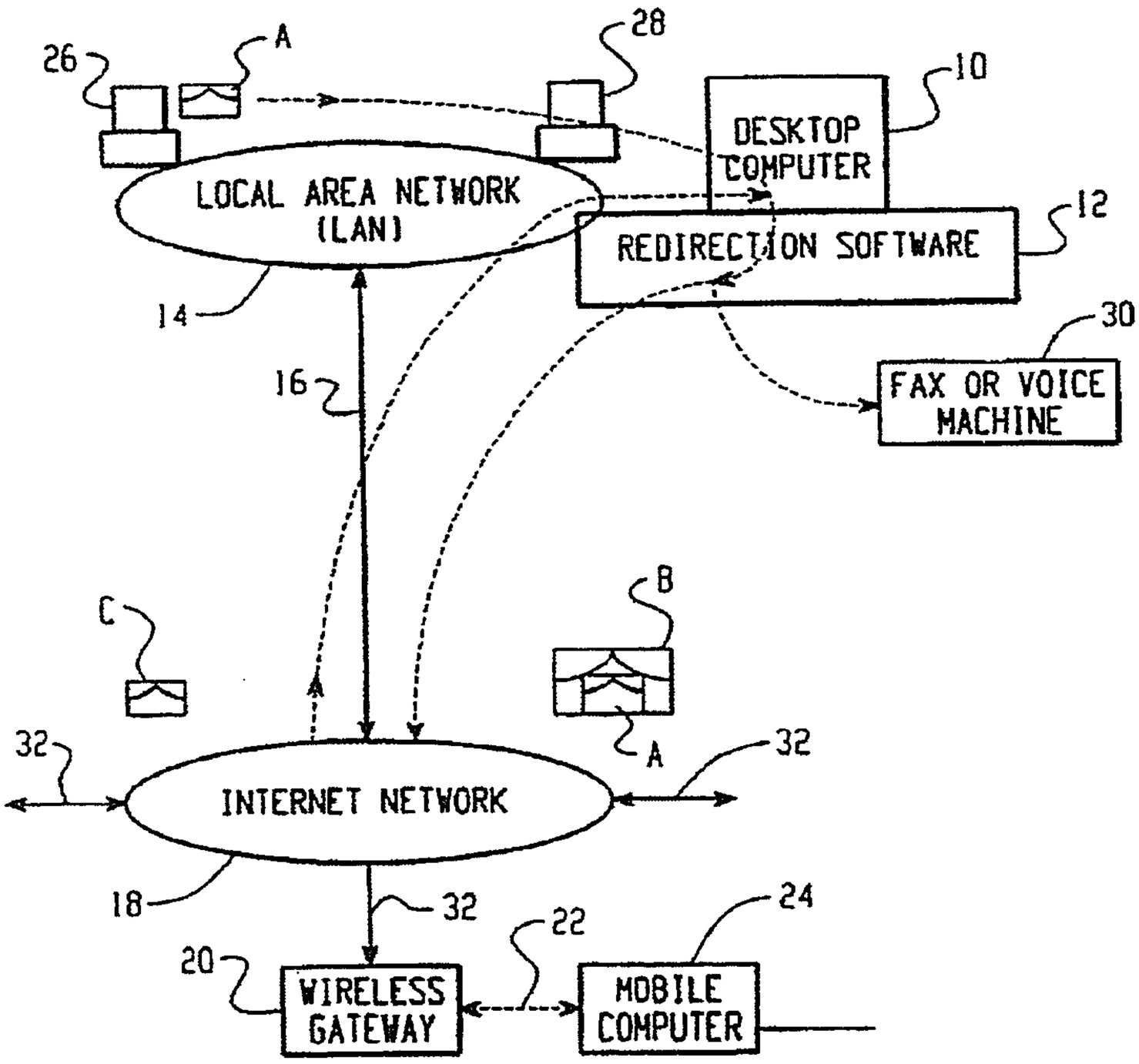

26
A
28
10
DESKTOP COMPUTER
LOCAL AREA NETWORK (LAN)
12
REDIRECTION SOFTWARE
14
30
16
FAX OR VOICE MACHINE
C
B
A
32
INTERNET NETWORK
32
32
18
32
24
22
20
WIRELESS GATEWAY
MOBILE COMPUTER

Fig. 1

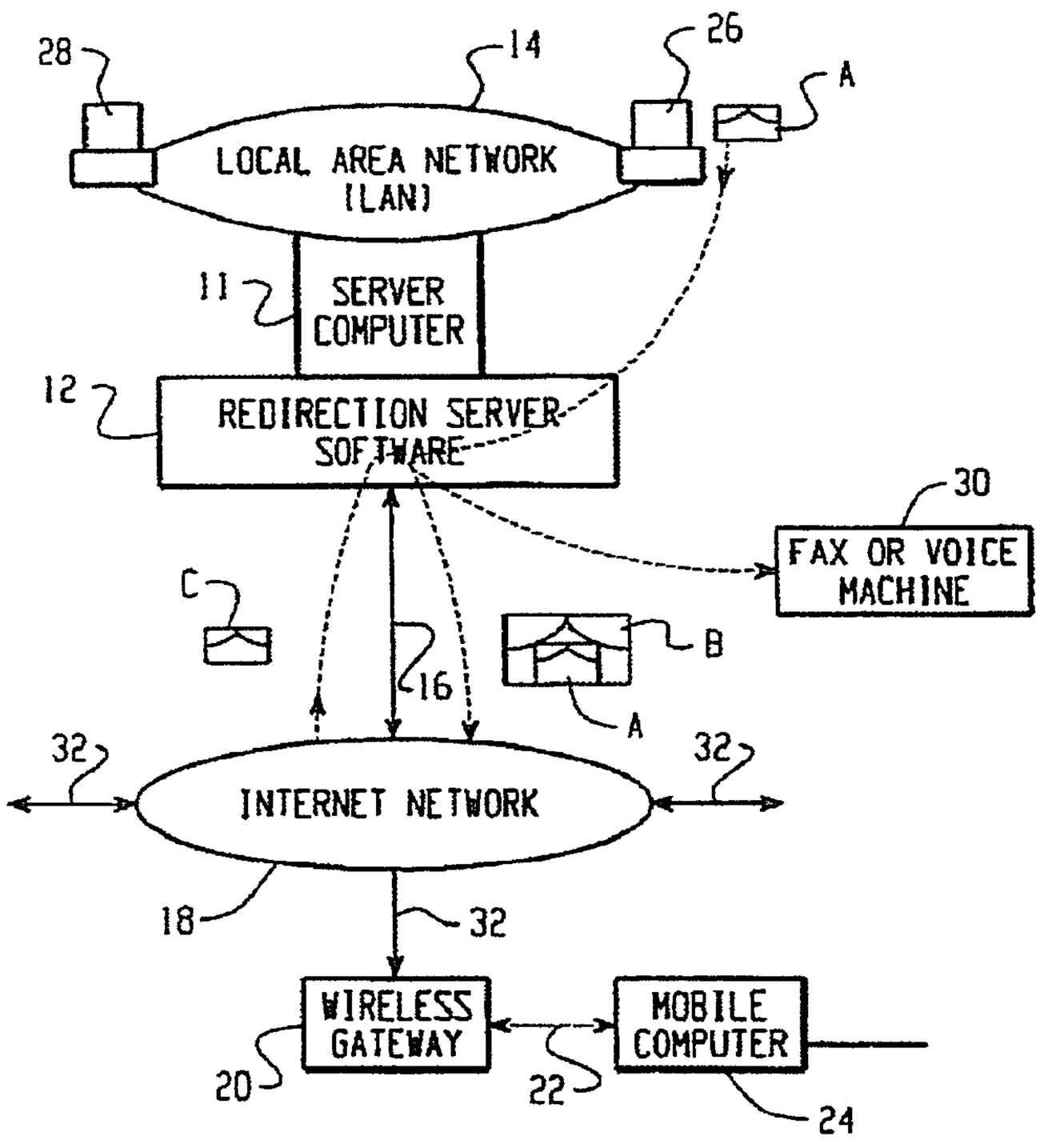

28
14
26
A
LOCAL AREA NETWORK
(LAN)
11
SERVER
COMPUTER
12
REDIRECTION SERVER
SOFTWARE
30
FAX OR VOICE
MACHINE
C
16
B
A
32
32
INTERNET NETWORK
18
32
WIRELESS
GATEWAY
MOBILE
COMPUTER
20
22
24

Fig. 2

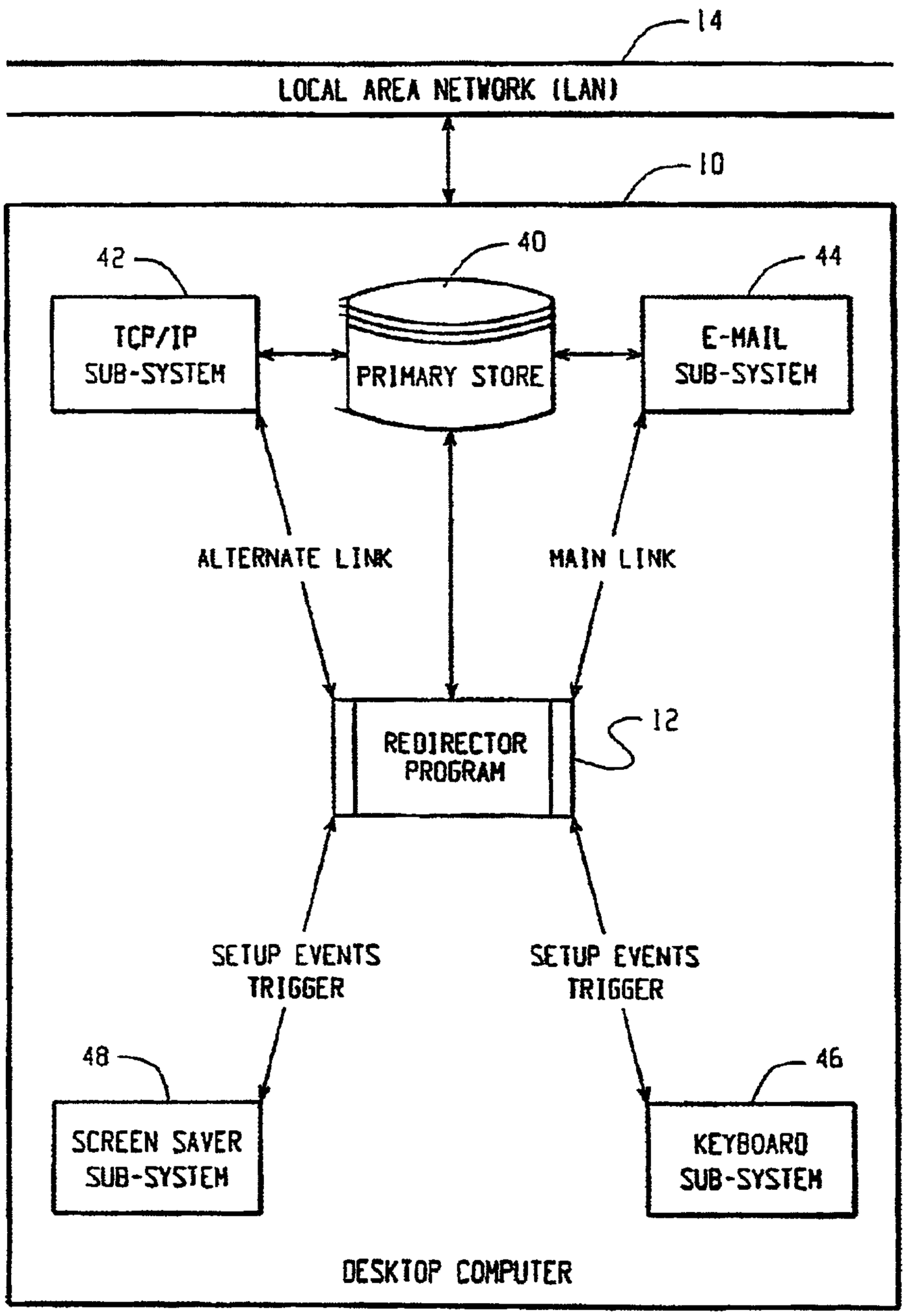

14
LOCAL AREA NETWORK (LAN)
10
42
40
44
TCP/IP SUB-SYSTEM
PRIMARY STORE
E-MAIL SUB-SYSTEM
ALTERNATE LINK
MAIN LINK
REDIRECTOR PROGRAM
12
SETUP EVENTS TRIGGER
SETUP EVENTS TRIGGER
48
46
SCREEN SAVER SUB-SYSTEM
KEYBOARD SUB-SYSTEM
DESKTOP COMPUTER

Fig. 3

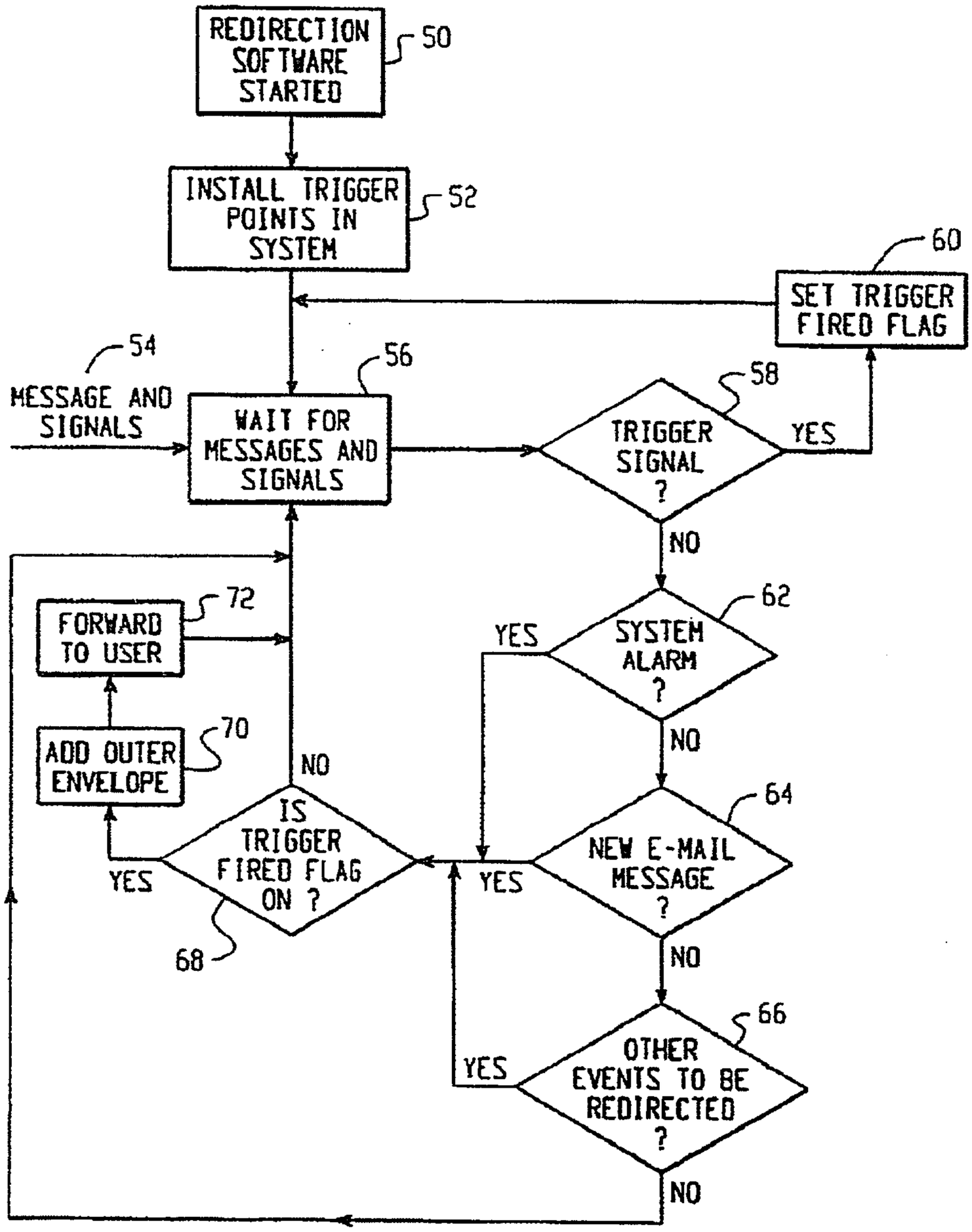

REDIRECTION SOFTWARE STARTED
50
INSTALL TRIGGER POINTS IN SYSTEM
52
60
SET TRIGGER FIRED FLAG
54
MESSAGE AND SIGNALS
56
WAIT FOR MESSAGES AND SIGNALS
58
TRIGGER SIGNAL ?
YES
NO
62
SYSTEM ALARM ?
YES
NO
64
NEW E-MAIL MESSAGE ?
YES
NO
66
OTHER EVENTS TO BE REDIRECTED ?
YES
NO
72
FORWARD TO USER
70
ADD OUTER ENVELOPE
IS TRIGGER FIRED FLAG ON ?
YES
NO
68

Fig. 4

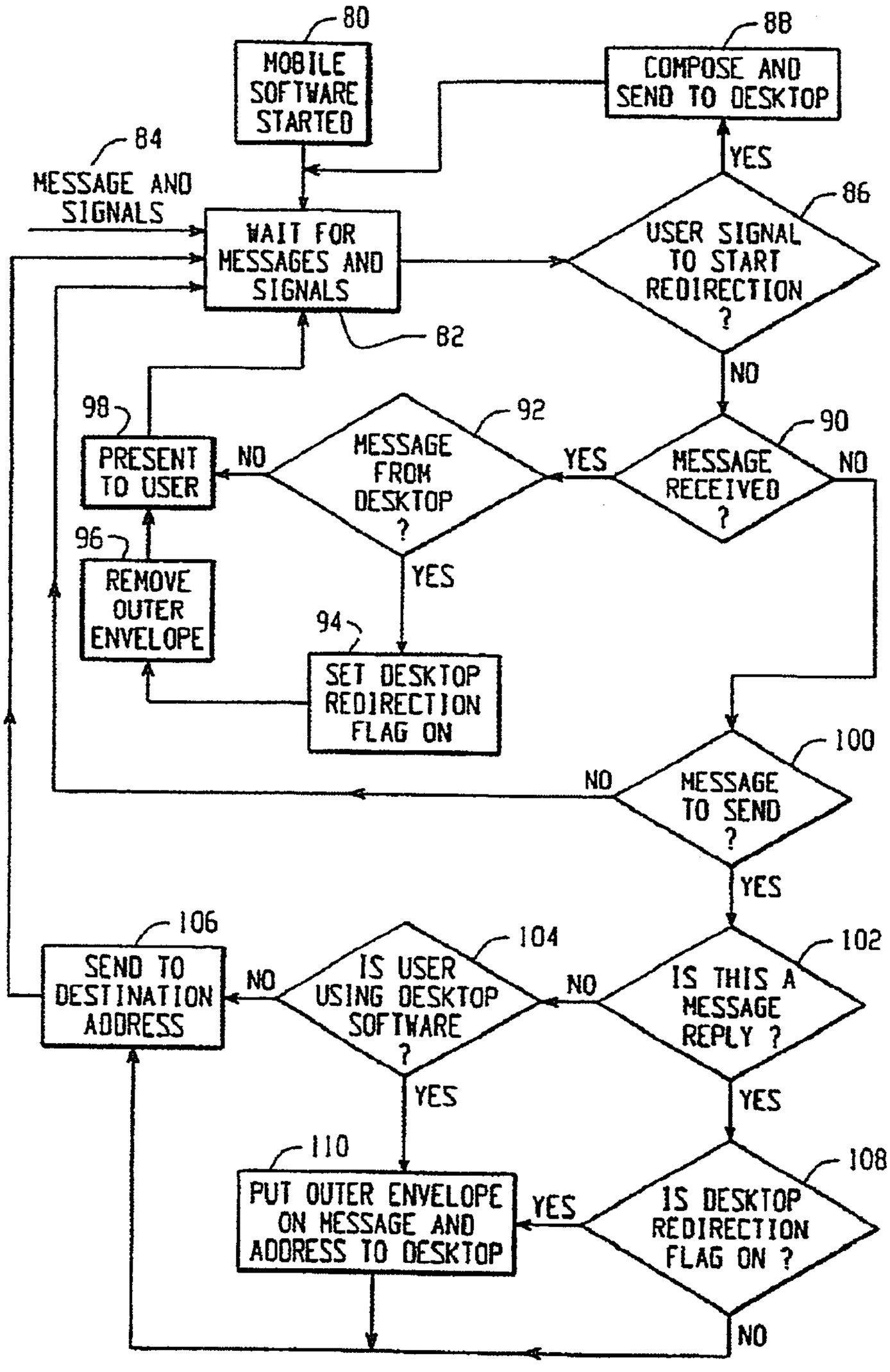

80
MOBILE SOFTWARE STARTED
88
COMPOSE AND SEND TO DESKTOP
84
MESSAGE AND SIGNALS
WAIT FOR MESSAGES AND SIGNALS
82
86
USER SIGNAL TO START REDIRECTION ?
YES
NO
98
PRESENT TO USER
NO
92
MESSAGE FROM DESKTOP ?
YES
90
MESSAGE RECEIVED ?
NO
96
REMOVE OUTER ENVELOPE
YES
94
SET DESKTOP REDIRECTION FLAG ON
100
NO
MESSAGE TO SEND ?
YES
106
SEND TO DESTINATION ADDRESS
NO
104
IS USER USING DESKTOP SOFTWARE ?
NO
102
IS THIS A MESSAGE REPLY ?
YES
YES
110
PUT OUTER ENVELOPE ON MESSAGE AND ADDRESS TO DESKTOP
YES
108
IS DESKTOP REDIRECTION FLAG ON ?
NO

Fig. 5

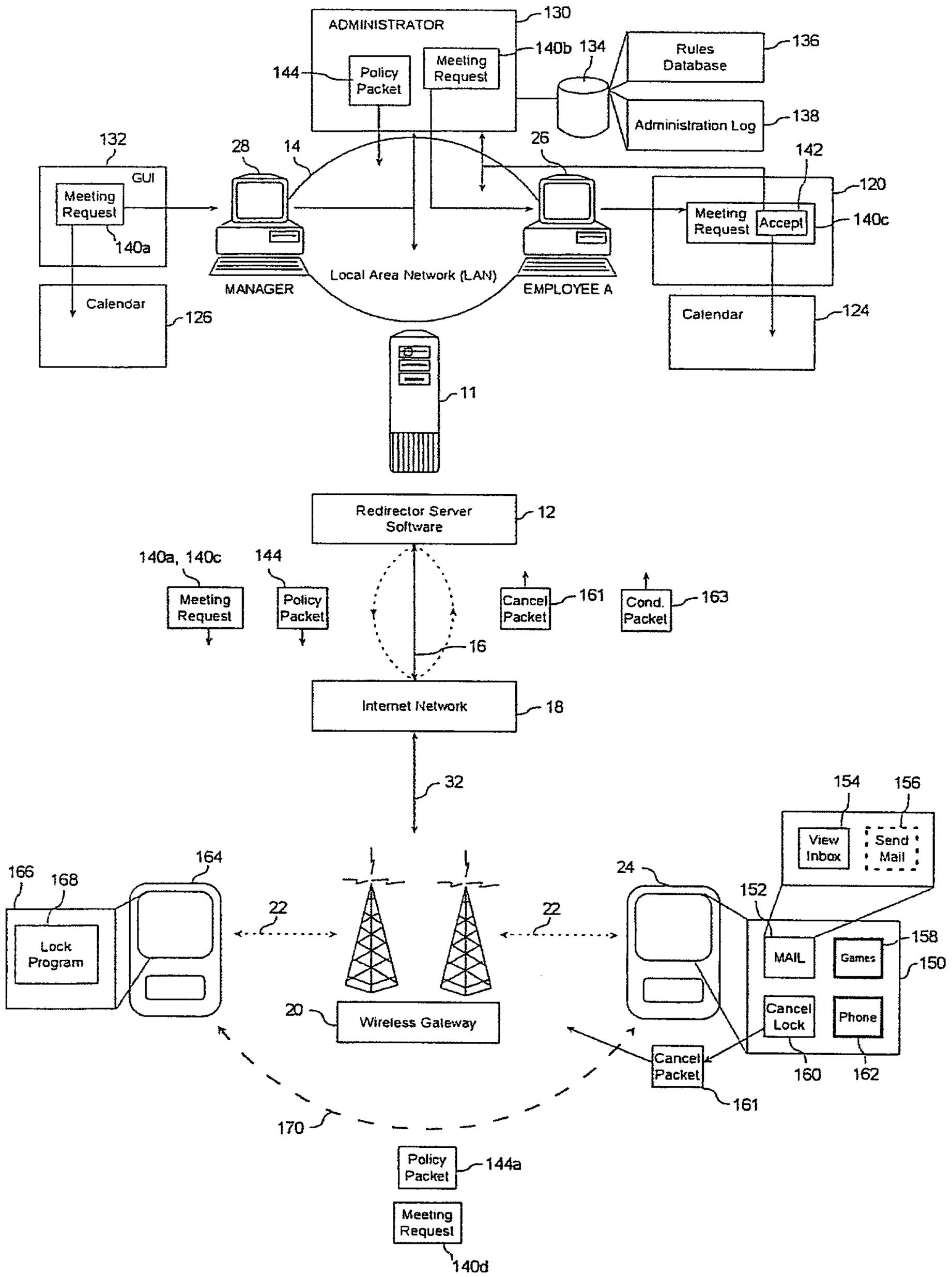

ADMINISTRATOR
130
Policy Packet
144
Meeting Request
140b
134
Rules Database
136
Administration Log
138
132
GUI
Meeting Request
140a
28
14
26
142
120
Meeting Request
Accept
140c
MANAGER
Local Area Network (LAN)
EMPLOYEE A
Calendar
126
Calendar
124
11
Redirector Server Software
12
140a, 140c
144
Meeting Request
Policy Packet
Cancel Packet
161
Cond. Packet
163
16
Internet Network
18
32
154
156
View Inbox
Send Mail
164
166
168
24
152
Lock Program
22
22
MAIL
Games
158
150
Cancel Lock
Phone
20
Wireless Gateway
Cancel Packet
160
162
161
170
Policy Packet
144a
Meeting Request
140d

Fig. 6

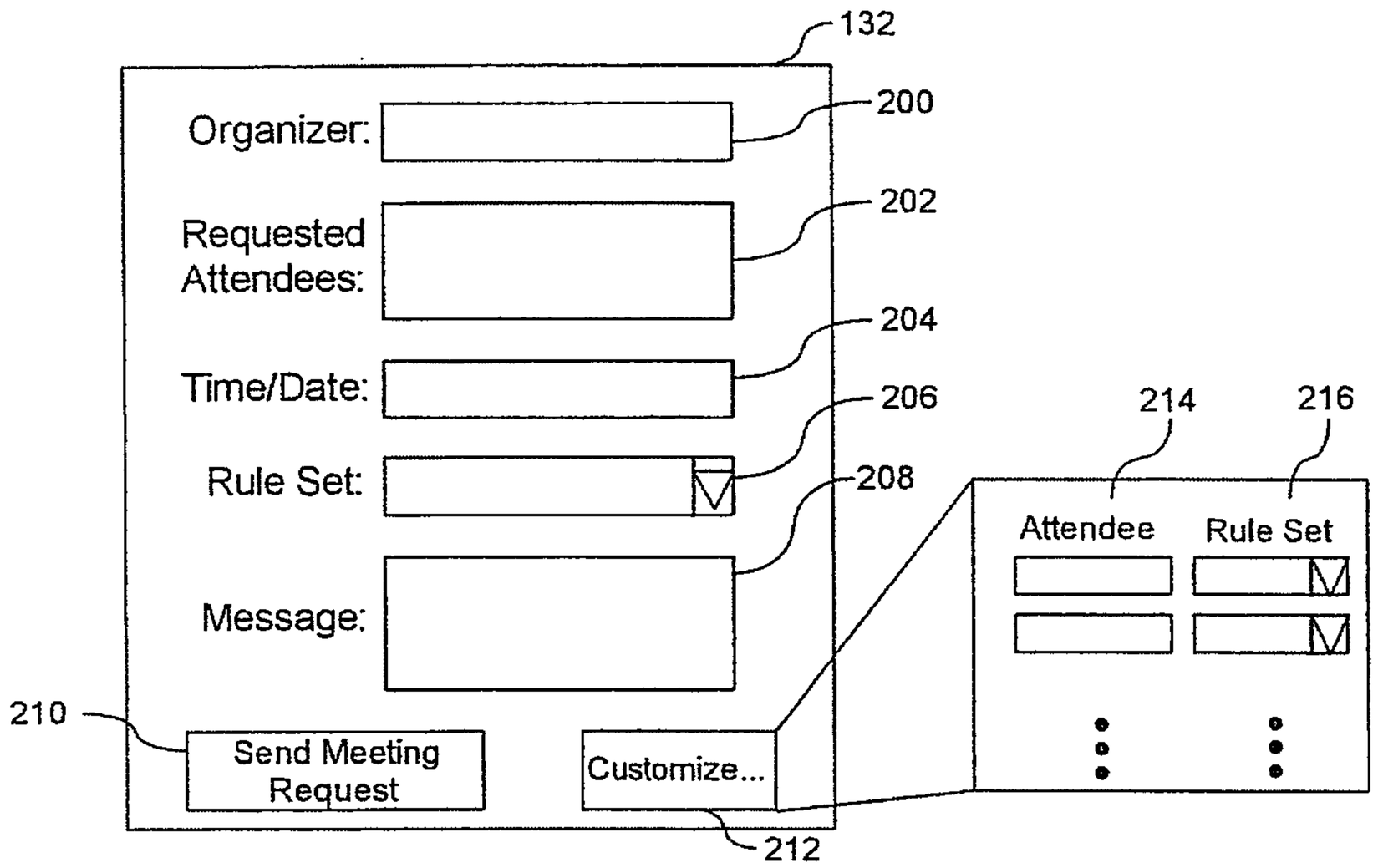

132
Organizer:
200
Requested Attendees:
202
204
Time/Date:
206
Rule Set:
214
216
Attendee
Rule Set
208
Message:
210
Send Meeting Request
Customize...
212

Fig. 7

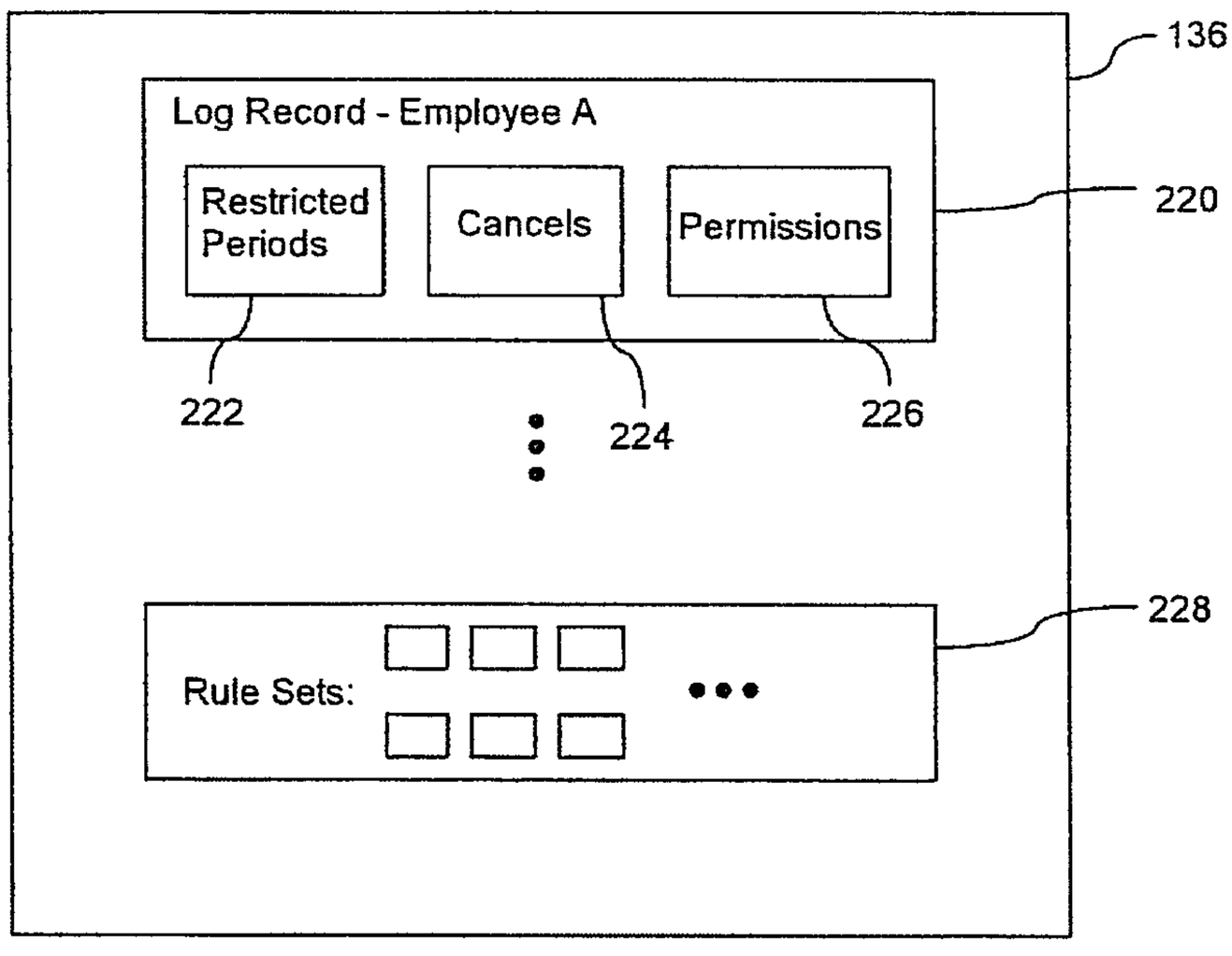

136
Log Record - Employee A
Restricted Periods
Cancels
Permissions
220
222
224
226
Rule Sets:
228

Fig. 8

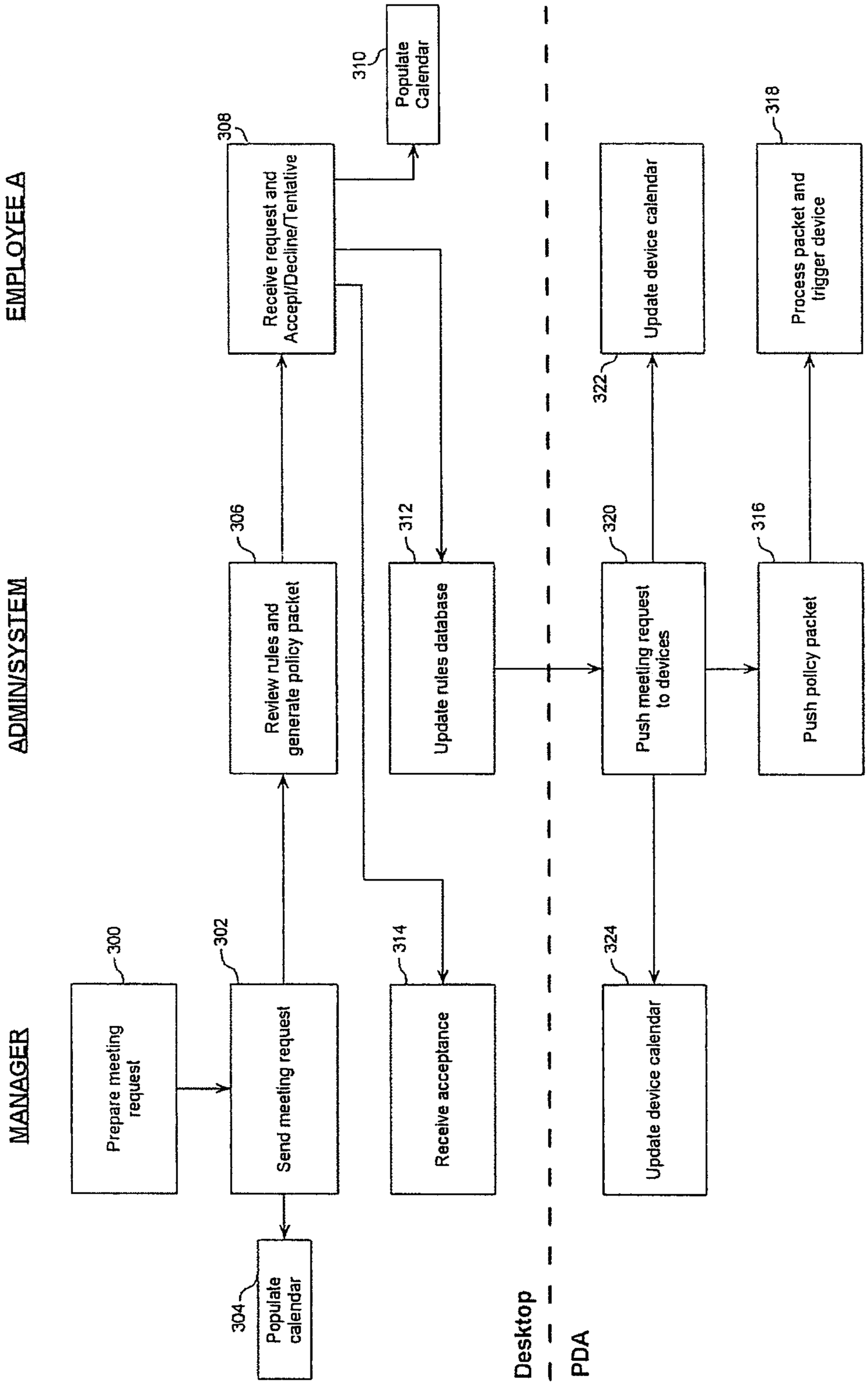

EMPLOYEE A
ADMIN/SYSTEM
MANAGER
Desktop
PDA
Prepare meeting request
300
Send meeting request
302
Populate calendar
304
Review rules and generate policy packet
306
Receive request and Accept/Decline/Tentative
308
Populate Calendar
310
Update rules database
312
Receive acceptance
314
Push policy packet
316
Process packet and trigger device
318
Push meeting request to devices
320
Update device calendar
322
Update device calendar
324

Fig. 9

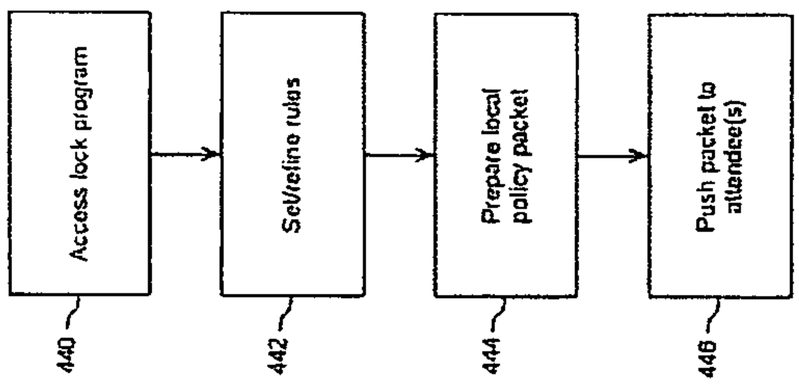

Access lock program
440
Set/refine rules
442
Prepare local policy packet
444
Push packet to attendee(s)
446

Fig. 11

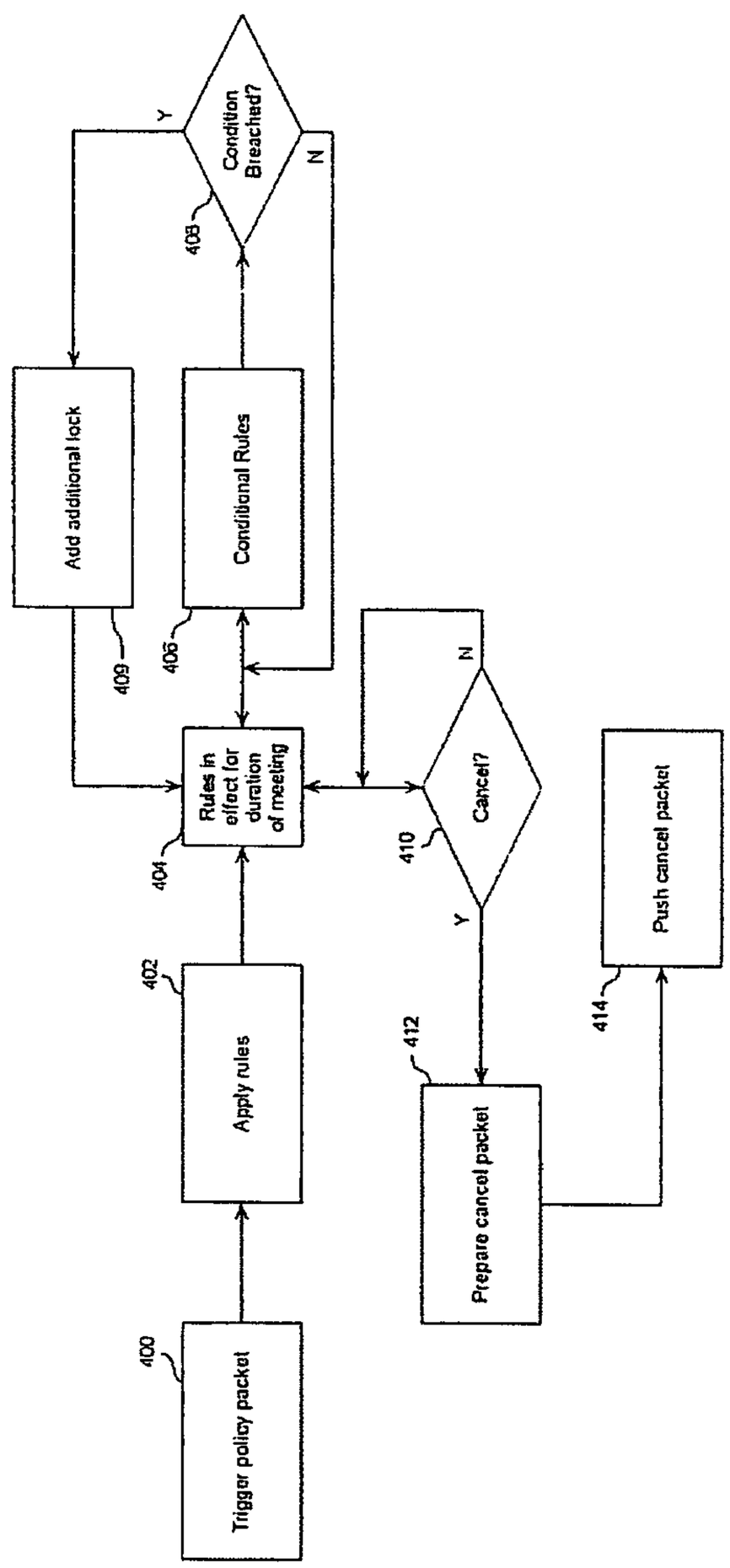

Trigger policy packet
400
Apply rules
402
Rules in effect for duration of meeting
404
Conditional Rules
406
Add additional lock
409
Condition Breached?
408
Y
N
Cancel?
410
Y
N
Prepare cancel packet
412
Push cancel packet
414

Fig. 10

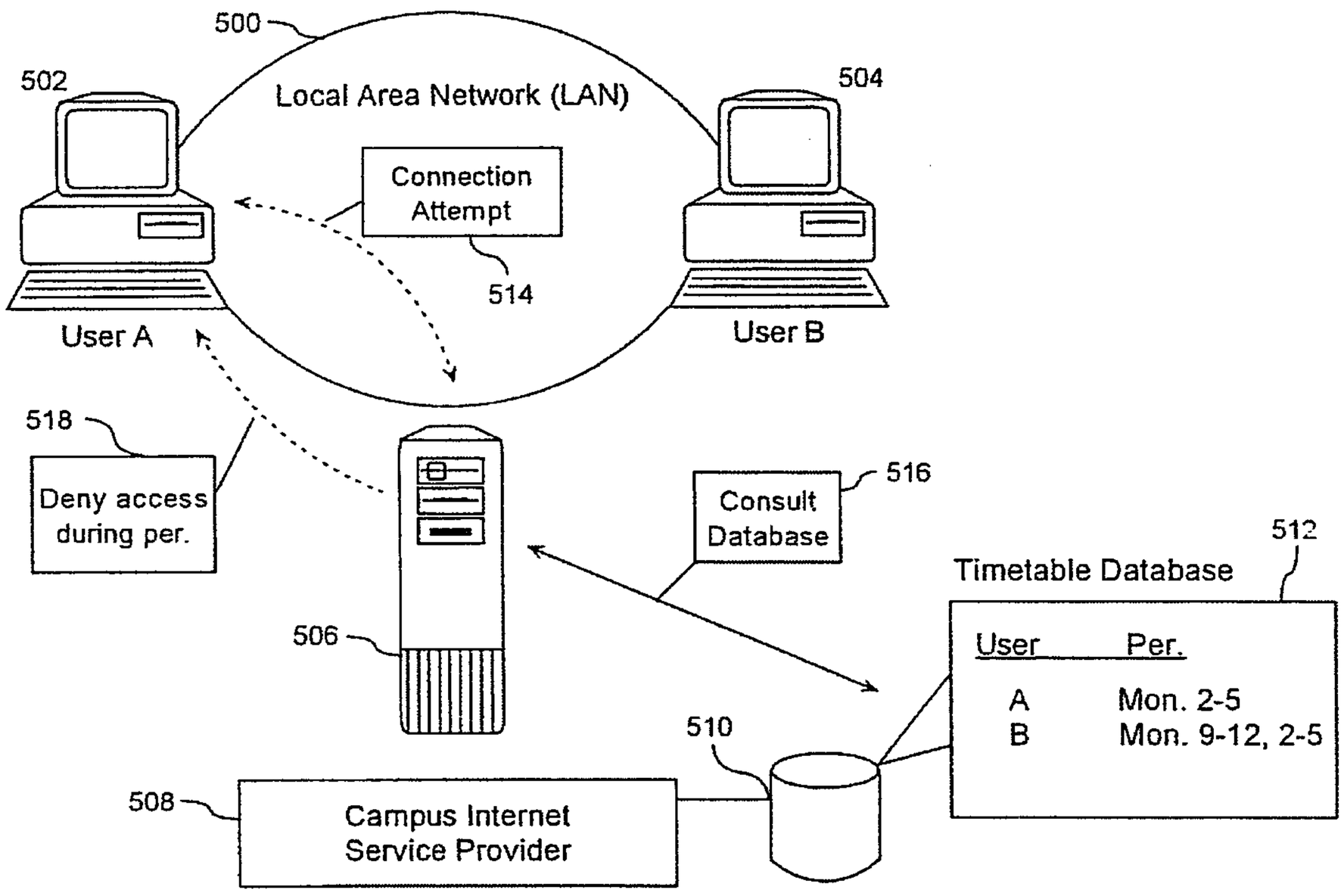

500
Local Area Network (LAN)
502
504
Connection Attempt
514
User A
User B
518
Deny access during per.
516
Consult Database
512
Timetable Database
User Per.
A Mon. 2-5
B Mon. 9-12, 2-5
506
510
508
Campus Internet Service Provider

Fig. 12

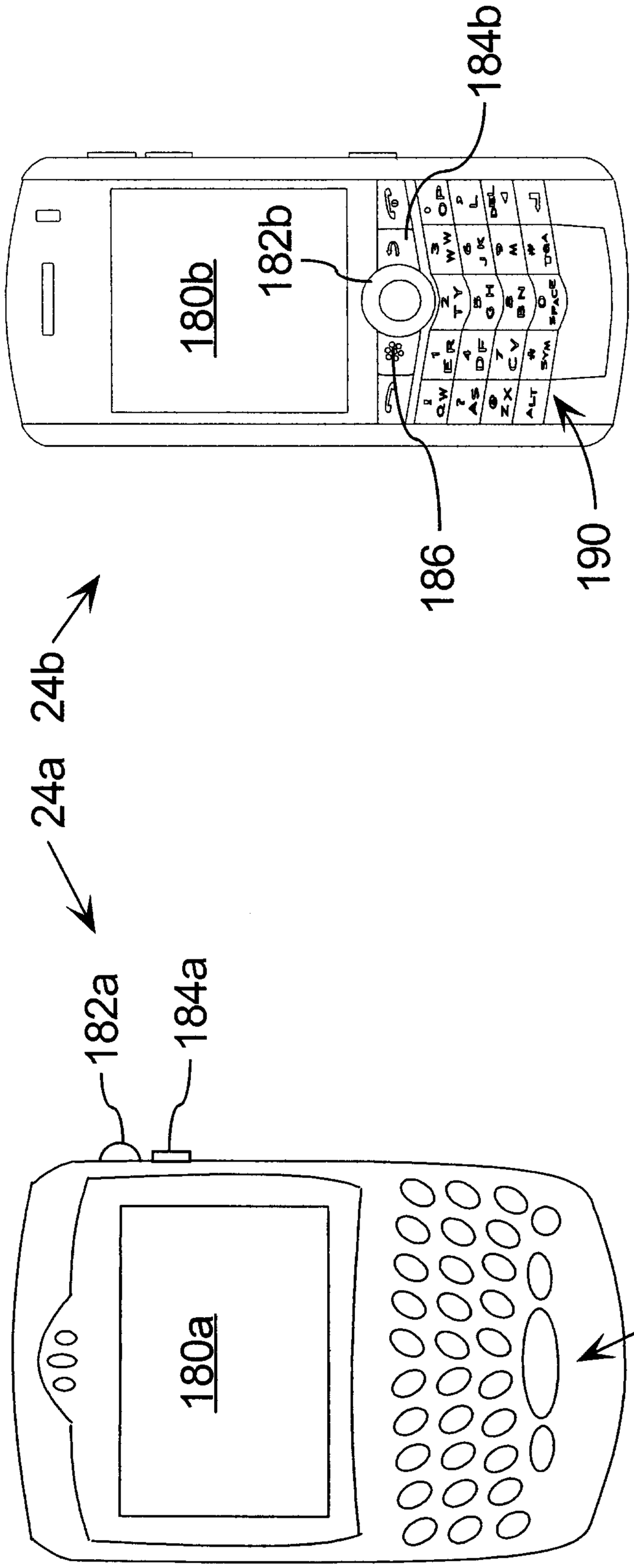


Figure 13

Figure 14

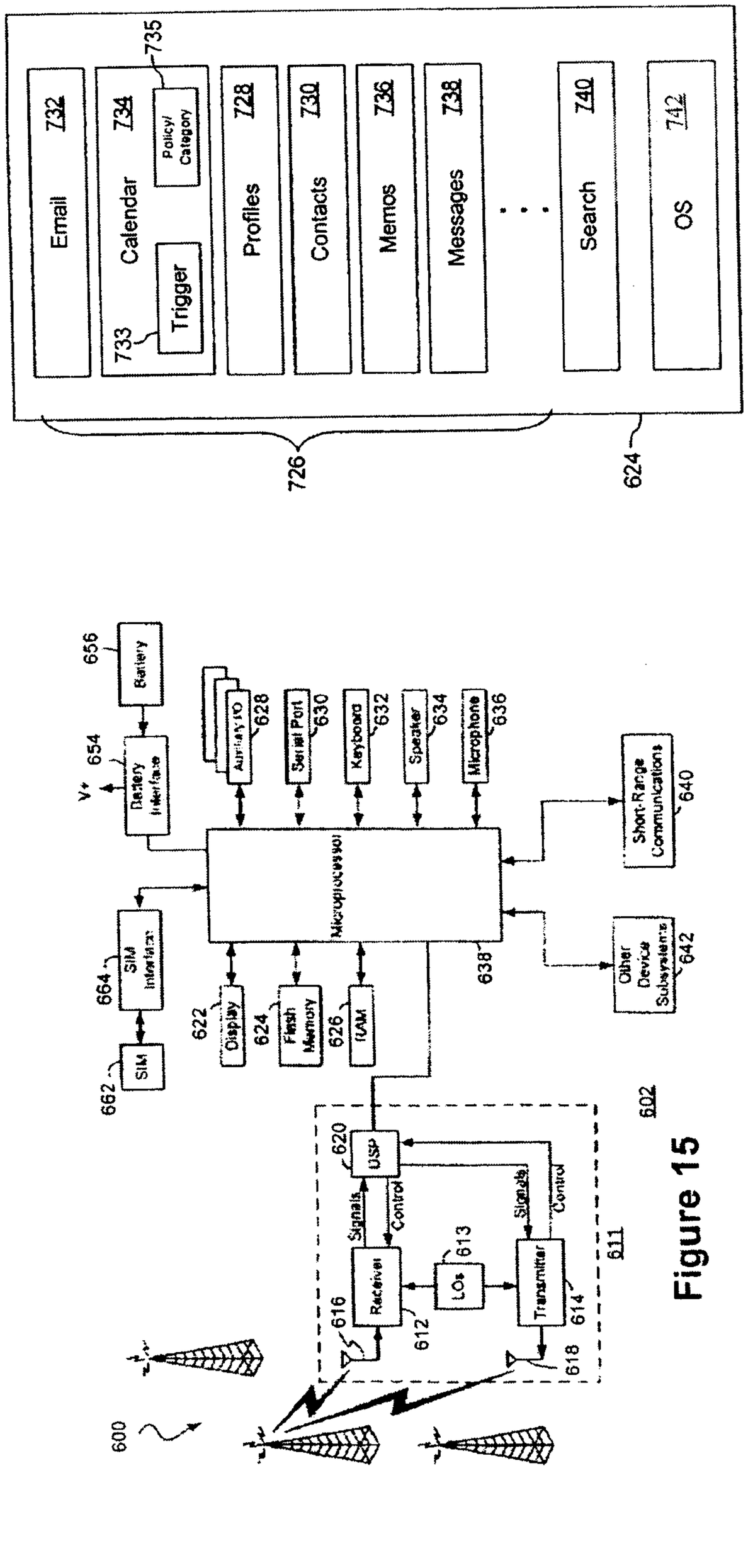


Figure 16

Figure 15

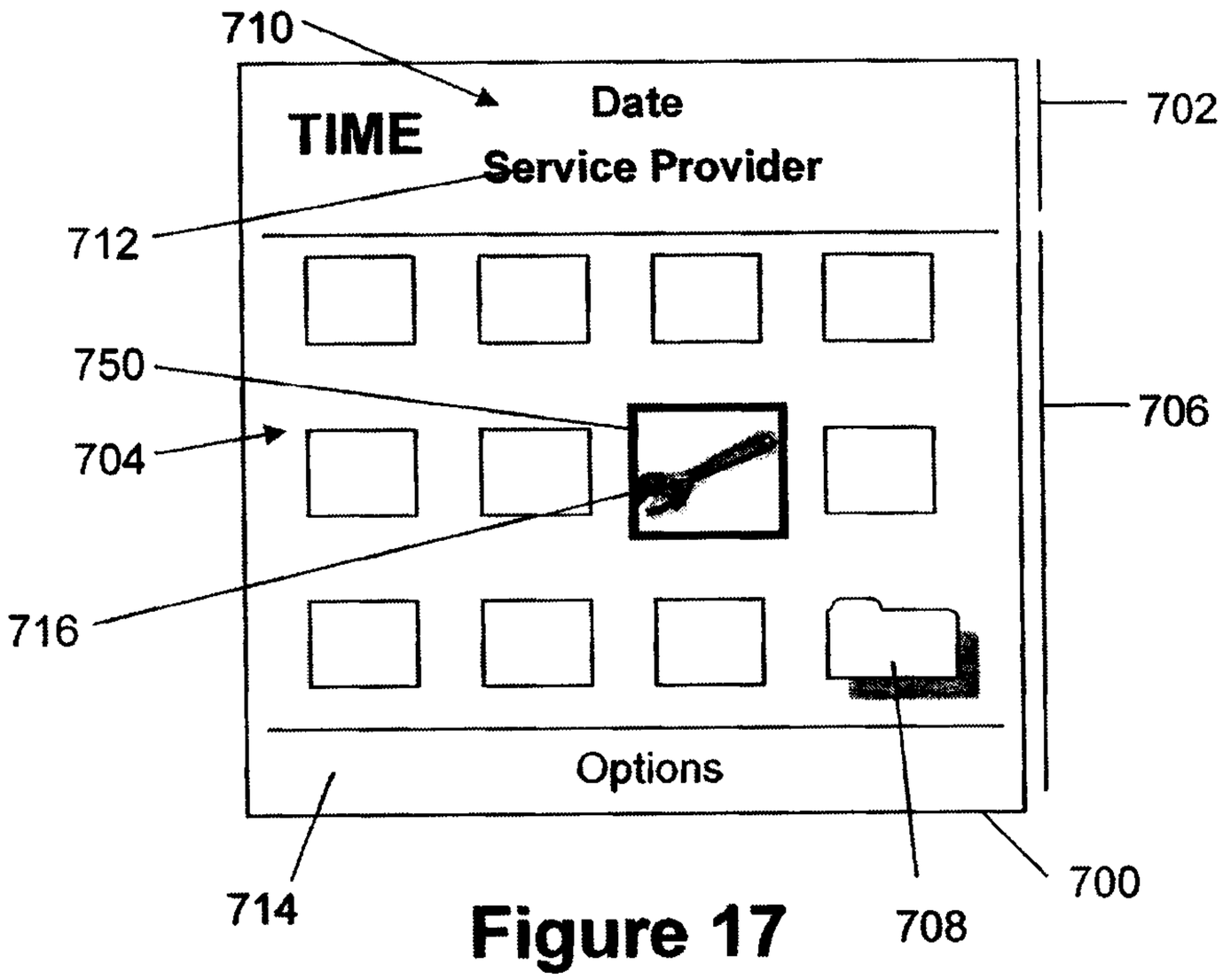


Figure 17

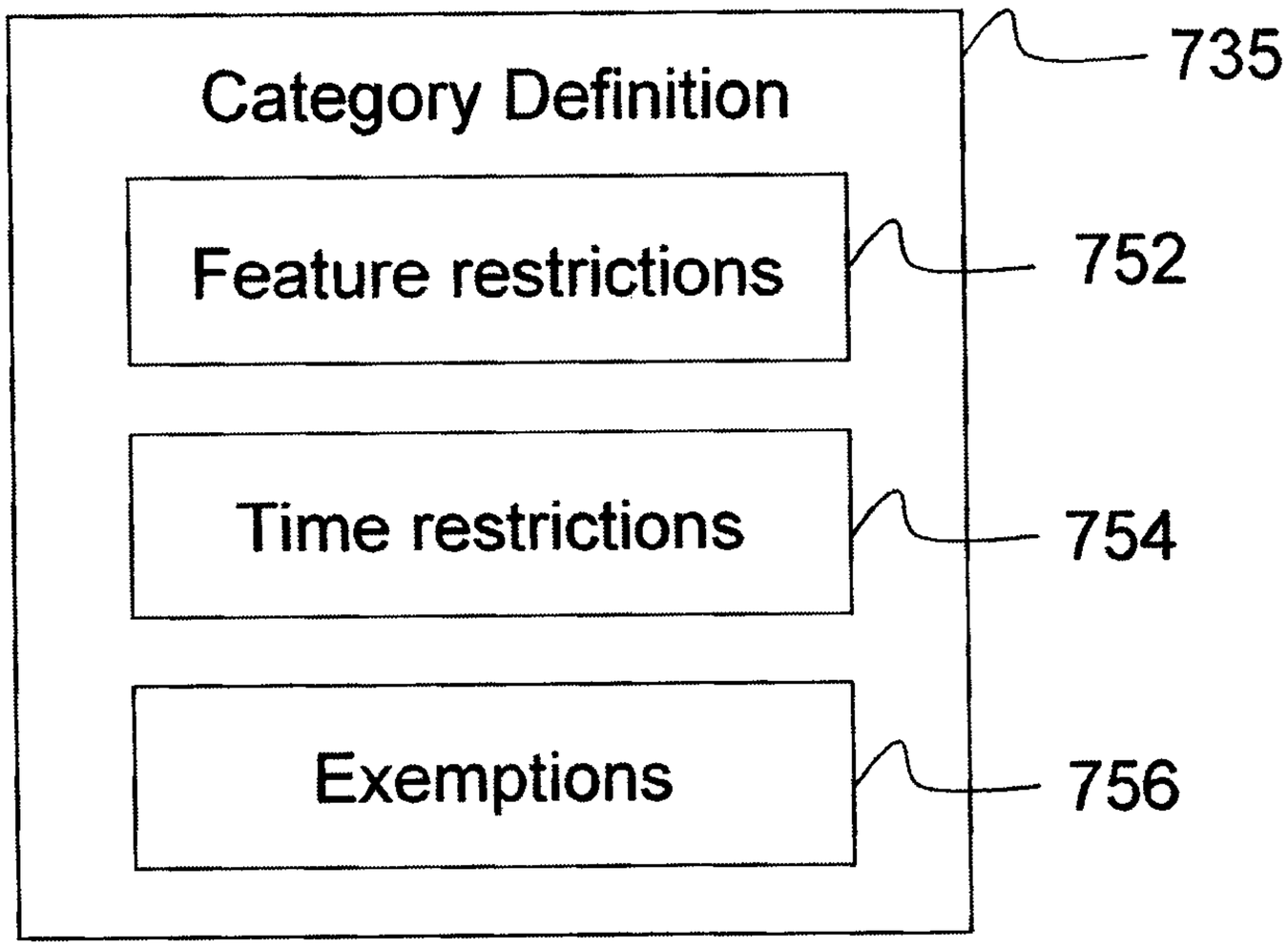


Figure 18

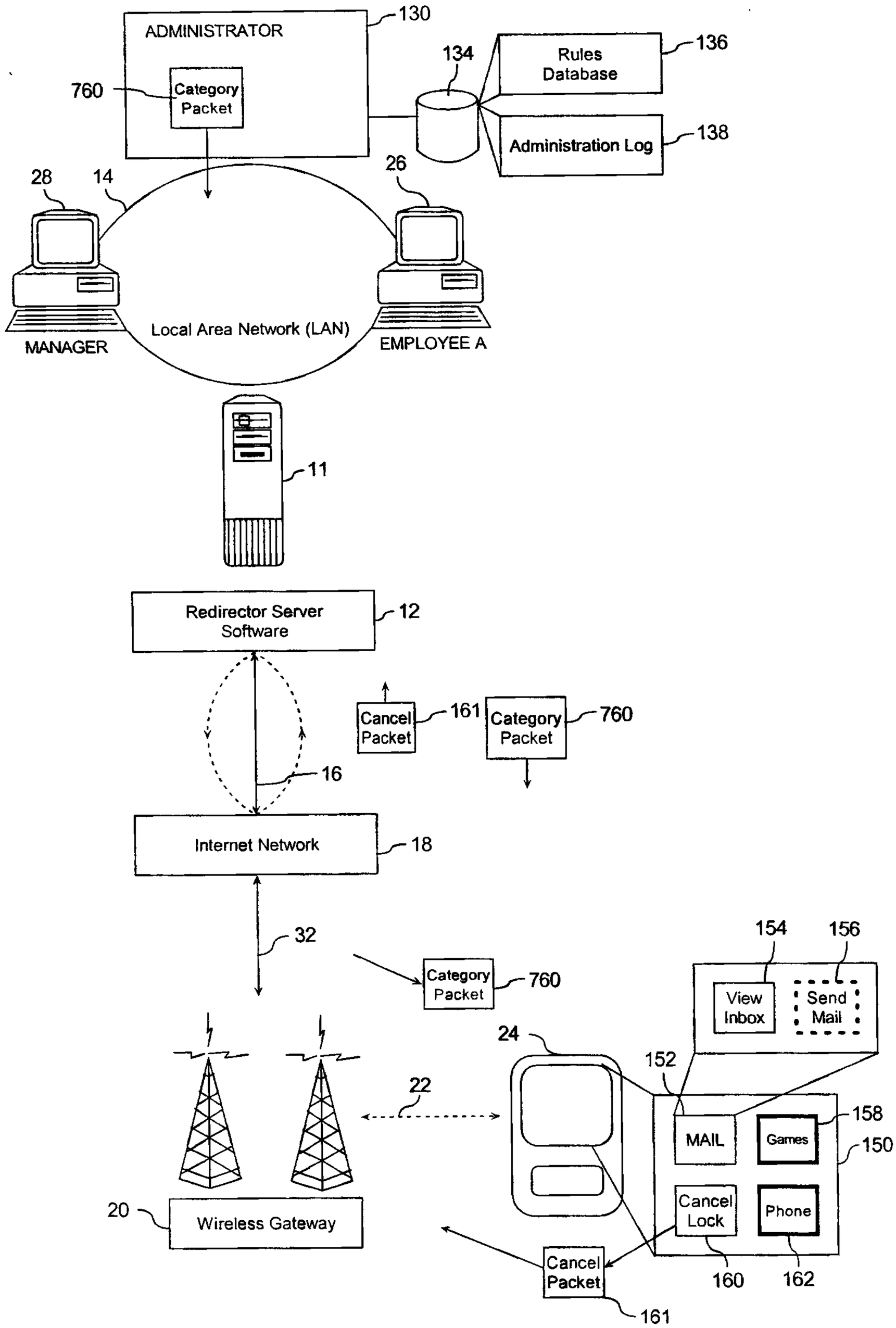
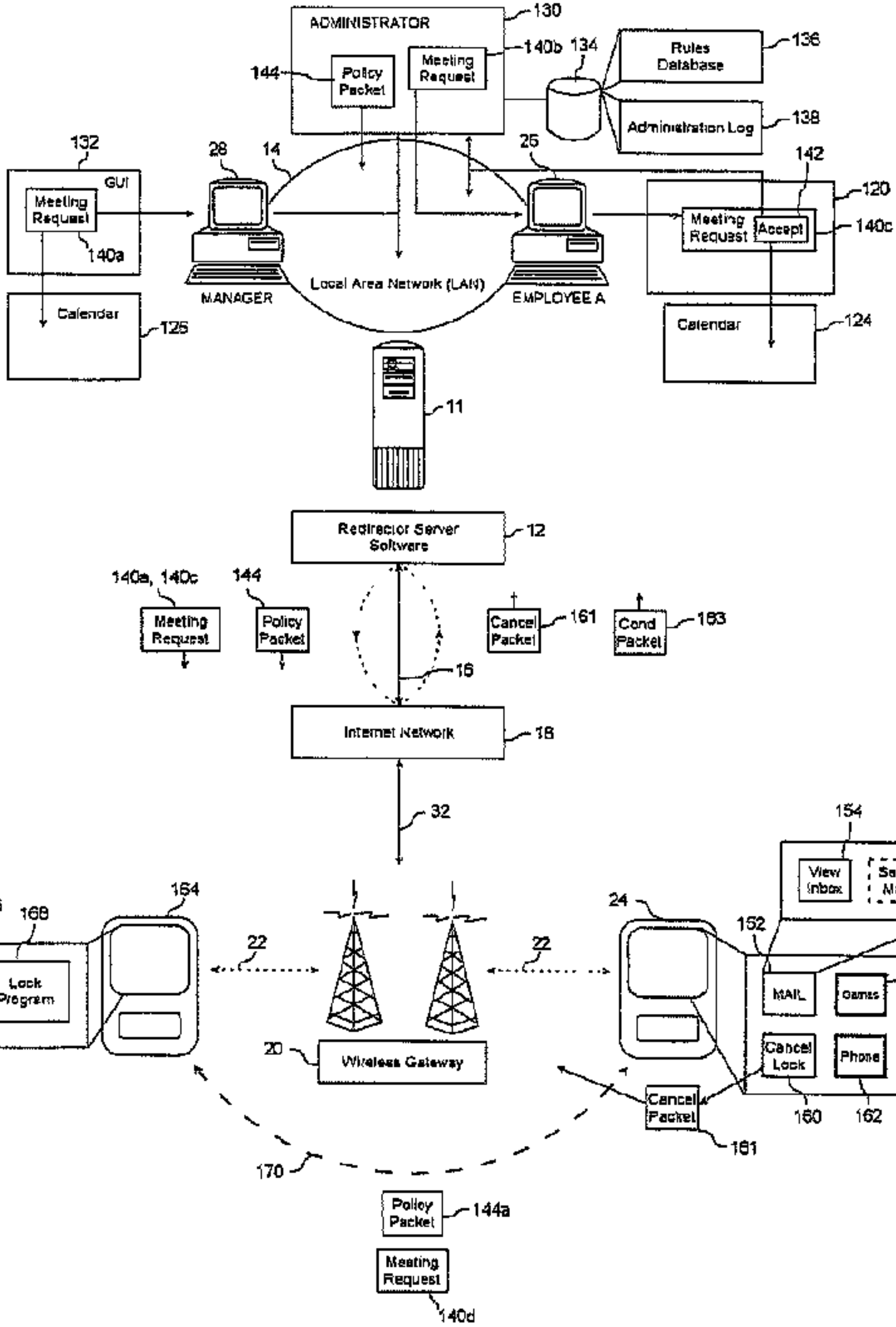

ADMINISTRATOR
130
760
Category Packet
134
Rules Database
136
Administration Log
138
28
14
26
Local Area Network (LAN)
MANAGER
EMPLOYEE A
11
Redirector Server Software
12
Cancel Packet
161
Category Packet
760
16
Internet Network
18
32
Category Packet
760
154
156
View Inbox
Send Mail
24
152
158
MAIL
Games
150
Cancel Lock
Phone
22
20
Wireless Gateway
Cancel Packet
160
162
161

Fig. 19


ADMINISTRATOR
130
140b
134
144
Policy Packet
Meeting Request
Rules Database
136
Administration Log
138
132
GUI
Meeting Request
140a
28
14
25
142
120
Meeting Request
Accept
140c
Local Area Network (LAN)
MANAGER
EMPLOYEE A
Calendar
125
Calendar
124
11
Redirector Server Software
12
140a, 140c
144
Meeting Request
Policy Packet
Cancel Packet
161
Cond Packet
163
16
Internet Network
18
32
154
156
View Inbox
Send Mail
24
152
164
166
168
Lock Program
22
22
MAIL
Games
158
150
Cancel Lock
Phone
20
Wireless Gateway
Cancel Packet
160
162
161
170
Policy Packet
144a
Meeting Request
140d