

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
24 January 2002 (24.01.2002)

PCT

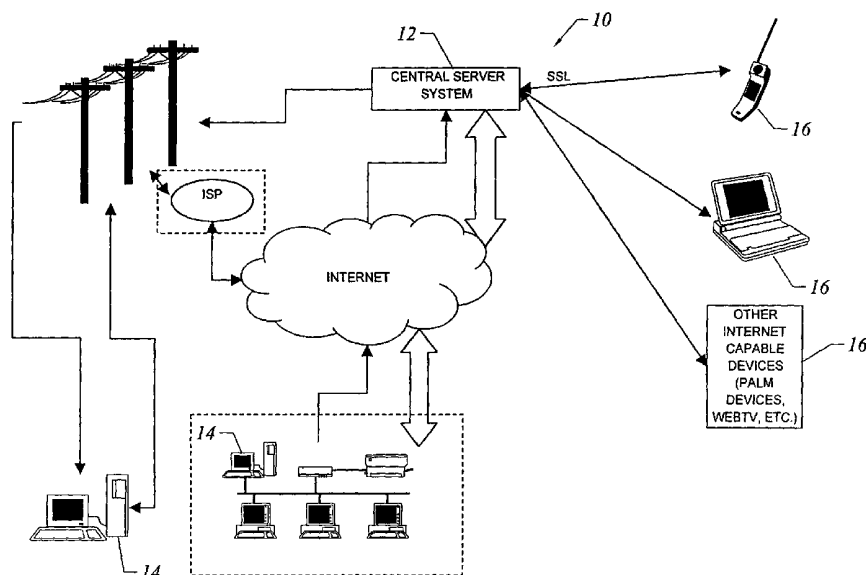
(10) International Publication Number
WO 02/06963 A1

- (51) International Patent Classification⁷: G06F 13/00
- (21) International Application Number: PCT/US01/22824
- (22) International Filing Date: 19 July 2001 (19.07.2001)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data: 09/618,956 19 July 2000 (19.07.2000) US
- (71) Applicant: FUSIONONE, INC. [US/US]; 55 Almaden Boulevard, Suite 800, San Jose, CA 95113 (US).
- (72) Inventors: TU, Edgar, Allan; 6881 Sunnyslope Avenue, Castro Valley, CA 94552 (US). PANG, Eric; 288 South Bernardo Avenue, Sunnyvale, CA 94086 (US).
- (74) Agent: VIERRA, Larry, E.; Vierra Magen Marcus Harmon & DeNiro LLP, Suite 540, 685 Market Street, San Francisco, CA 94105-4206 (US).
- (81) Designated State (national): JP.
- (84) Designated States (regional): European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: REMOTE ACCESS COMMUNICATION ARCHITECTURE APPARATUS AND METHOD



(57) Abstract: Disclosed herein is a system and method for communicating data from a base computer (14) to a remote device (16) via central server system (12) without the necessity of specialty software on the remote device (16). Remote devices (16) such as laptop computers and cellular telephones communicate with the central server system (12), while the central server system (12) likewise communicates with base computers (14). Communications between the central server system (12) and the base computers are facilitated by an intermittent query from base computers to the central server system in a manner which allows communications even in a firewall-contained environment. The system and method provides a means for facilitating both persistent connections and dialup communications between the base computers and the central server system.

WO 02/06963 A1

- 1 -

S P E C I F I C A T I O N5 REMOTE ACCESS COMMUNICATION ARCHITECTURE
 APPRATUS AND METHODBACKGROUND OF THE INVENTION1. Field of the Invention

10 The present invention relates generally to remote access systems. More particularly, the present invention relates to an apparatus and method for implementing a communication architecture for remotely accessing a computer by means of a remote device without the need for special software applications on the remote device.

15 2. The Prior Art

 In general, remote access systems allow a "remote" user (from a remote computer) to connect to and access resources on another computer. For example, a user on a mobile computer may connect to and access resources on a home computer via conventional remote access
20 systems. However, prior art remote access systems require special application software to be supplied to both the remote system and the base system. Due to this shortcoming, most prior art remote access systems are limited to devices including substantial computing capabilities in the remote computer. Also, access to another computer
25 via a remote access system is provided using conventional data connection means, typically through a PSTN (public switched telephone

- 2 -

network) connection. That is, a direct connection from the remote computer to the base computer is typically required for security reasons.

Remote access systems can generally be categorized into two types of systems. The first system is generally referred to as a remote access server (RAS) system. A RAS system usually comprises server RAS software residing on a RAS server and client RAS software residing on a "remote" computer. The RAS server is coupled to resources (e.g., printers, files, other nodes) which are remotely accessed by a user of the system. In operation, a user of the remote computer connects to the RAS server via a dial-in telephone connection. Upon connection, the RAS server queries for the user's access credentials (e.g., user name and password). Upon authentication of the user's access credentials, the user is granted access to resources on the RAS server and/or resources on other nodes connected to the RAS server to which the user is authorized access. The RAS software manages the connection process, the authentication process, the access privileges, and the data transfers between the RAS server and the remote computer. RAS systems are also used by commercial service providers, such as Internet Access Providers (ISPs) to allow their customers access into their network resources.

In another implementation, RAS systems may be used in conjunction with an Internet connection. In this scheme, a user is able to access a RAS server indirectly via the Internet, rather than directly

- 3 -

via a point to point telephone connection. These RAS systems are generally referred to as virtual private networks (VPNs), because a secure channel is provided via the normally unsecured Internet. In VPNs, a remote user having a computer operatively coupled to the VPN, is able to access resources on another computer via the Internet using Internet protocols.

The other type of remote access system is generally referred to as a remote control system (RCS). RCSs allow a remote user to not only access resources on another "host" computer, but also allow the user to control the host computer. RCSs typically display on the remote computer what would normally be displayed on the host computer (known as screen emulation). In this way, the user is able to control the host computer from the remote computer as if the user was directly accessing the host computer. An example of a commercially available RCS product is PC Anywhere™ by Symantec Corp.™. Like RAS systems, RCS allows a remote user to connect via a conventional means, including a telephone connection and via the Internet. Again, special software is required on both nodes.

There are several disadvantages with RAS and RCS systems. In RAS systems, file synchronization poses a common problem, particularly with respect to email applications. For example, where a remote user downloads email to the remote computer it may be stored on the remote

- 4 -

computer. Thus, when the user gets back to the local computer, that email is not accessible on the remote computer, but must somehow be transferred from the remote computer or disregarded. This can become quite frustrating to the user.

5 In addition, in RAS implementations certain files may be unusable without the original application. For example, with certain email applications, the messages associated with the email application are commonly stored in a proprietary file format. Without the original email application, the file would be unusable to the remote user if the
10 original application is not installed on the remote computer accessed by the user.

RCS, on the other hand, typically requires proprietary software to be installed on both the server (host) and client (remote) computers. Proprietary software limits the ability of a remote user to access the
15 host computer, because such proprietary software may not be readily accessible.

In addition, often the setup and administration of RAS and RCS systems are cumbersome or otherwise overwhelming for the home or corporate users. Setup normally involves the assistance of a network
20 system administrator and is usually complicated further by the fact that each user may have different remote computers and different host computers. Each setup then becomes unique and difficult.

- 5 -

BRIEF DESCRIPTION OF THE INVENTION

Accordingly, there is a need for a method and apparatus which provides for remote and secure access to a host or base computer, and which further provides an open application standard for client access to the host computer. The present
5 invention satisfies these needs, as well as others, and generally overcomes the deficiencies found in the background art.

Thus, it is desirable to have an open application standard (such as a conventional world wide web (web) browser), particularly on the client side, whereby a mobile user may access a plurality of data
10 processing means (computers, Internet terminals, PDAs, mobile telephones, etc.).

To overcome the above described and other shortcomings of the prior art, disclosed herein is an apparatus and method for remotely accessing a base computer. The remote access device may be any device
15 capable of accessing the internet and does not require the installation of specialty software thereon. The base computer operates by means of an agent that communicates with a central server system.

A user of the system may access a base computer from a remote device such as a laptop computer, cellular telephone, palm pilot, or any
20 other device capable of accessing the internet. A browser interface on a laptop computer for example is all that would be required for a laptop computer. The laptop user would then access the central server system

- 6 -

web site and be provided with one or more tasks that the user may desire to perform. Such tasks may include checking email on the base computer, obtaining files from the base computer, copying files from the remote computer to the base computer, or accessing an address book on
5 the base computer.

The base computer intermittently contacts the central server system to determine whether the central server system has established a session with a remote user. When a session has been established between a remote user and the central server system, the central server
10 system replies to the base computers next intermittent request with an IP address and port number for the base computer to establish a socket connection. The IP address and port number correspond to a server in the central server system handling the particular session task requests. That socket connection will be maintained between the base computer
15 and the server until the server ends the session or a predefined timeout period expires.

While the socket connection is maintained, the base computer “listens” for tasks from the server. It should be noted that because of the intermittent initial contacts from the base computer to the central
20 server system, operation of this system will be allowed, even in the presence of a firewall (i.e. a firewall between the base computer and the internet is intended to preclude a signal from an outside source coming

- 7 -

through the firewall unless requested, but will allow outgoing signals; thus, a message sent from a base computer to a web server would be allowed through a firewall along with any response to said message). Likewise, since the base computer establishes the continuous connection
5 with the IP socket and port number of the server in question after being informed of same from the central server system in response to one of the intermittent contacts, a firewall is not a problem. Thus, once a task is selected by a remote user, the central server system via the connected server (to the base computer) transmits the task request to the base
10 computer and the base computer provides the data and/or files necessary to fulfill that request in response back to the central server system.

The central server system then, in turn, presents the requested data to the remote user in an internet readable form. For instance, in
15 the laptop computer example, the information is presented in a browser readable format such as HTML. For a cellular device on the other hand, a WAP (Wireless Application Protocol) would be used to present such information to the cellular device user via the cellular device display (HDML, WML, etc.). Additionally, the communications between the
20 remote device and the central server system are preferably conducted via a secure sockets layer (SSL) for security purposes, and the communications between the base computer and the central server

- 8 -

system are preferably conducted via a proprietary protocol utilizing encryption as well to also ensure security.

Therefore, it is a first object of the present invention to provide a system for remotely accessing a base computer without the necessity of
5 specialty software on the remote device.

It is another object of the present invention to provide a system for remotely accessing a base computer wherein the remote device communicates solely with an internet server system and the base computer communicates solely with the internet server system.

10 It is yet another object of the present invention to provide a system for remotely accessing a base computer via the internet in a manner that is highly secure.

It is yet another object of the present invention to provide a method for both remotely accessing a base computer that is continuously
15 connected to the internet and one which is not continuously connected to the internet.

It is yet another object of the present invention to provide a remote access system that will work even though the base computer may reside behind a firewall.

20 Viewed from a first vantage point a method for remotely accessing a base computer from internet-enabled remote devices wherein the remote devices do not include remote access software is

- 9 -

disclosed, comprising in combination, establishing a remote access session with one of the remote devices at an internet central server system, presenting a task list to the remote device from said central server system, receiving a task selection at said central server system
5 from the remote device, establishing a persistent connection between said central server system and a base computer in response to intermittent contact from said base computer to said central server system, transmitting said task from said central server system to the
10 base computer via said connection between said central server system and said base computer, receiving at said central server system task data from the base computer responsive to said transmitted task, and presenting from said central server system a task response compiled from said task data to the remote device.

Viewed from another vantage point a remote access system is
15 disclosed comprising in combination a central server system in operative communication with the internet, an internet server for communicating with remote devices, the internet server comprising one server within the central server system, a task transmitter within the central server system for transmitting tasks to base computers; and a task data
20 receiver within the central server system for receiving task data from base computers.

- 10 -

BRIEF DESCRIPTION OF THE DRAWING FIGURES

FIG. 1 is a schematic diagram of an overview of the present invention.

FIG. 2 is a schematic diagram of the present invention in a
5 continuous connection environment.

FIG. 3 is a schematic diagram of the present invention in a non-continuous connection environment.

FIG. 4 is a flowchart of the present invention in a continuous connection environment.

10 FIG. 5 is a flowchart of the present invention in a non-continuous connection environment.

DETAILED DESCRIPTION OF THE INVENTION

Persons of ordinary skill in the art will realize that the following
15 description of the present invention is illustrative only and not in any way limiting. Other embodiments of the invention will readily suggest themselves to such skilled persons having the benefit of this disclosure.

Referring to the drawing figures, wherein like numerals denote like parts throughout the various drawing figures, Figure 1 is directed
20 to the remote access system 10 of the present invention. Generally, the remote access system 10 includes a central server system 12 that may be in operative communication with a remote device 16. Additionally, a

- 11 -

base computer 14 may be continuously or non-continuously in operative communication with central server system 12. Furthermore, the central server system 12 may consist of one or more servers. A multiple server configuration would allow for the handling of certain discreet operations
5 by different servers and is preferred. For instance, one server may be configured as a web site server, while another may be configured to communicate in a manner understood by cellular phones, and yet another for PDA's, and so forth.

The essence of the system is to enable a remote device 16 to
10 retrieve data from, or provide data to, a base computer 14 with the assistance of central server system 12. No special software is installed on the remote device 16. To the contrary, remote device 16 may be any device capable of accessing the internet which includes a readable interface such as a computer, mobile telephone, palm device, webTV, or
15 any other such device.

A remote user using a remote device 16 may connect to the central server system 12 as the user might connect to any other internet site. Once connected (and authenticated), that user will then be presented with task options by the central server system in an internet
20 readable format (HTML for mobile computer user using a browser for instance) by the device being used. The user will then select the task

- 12 -

desired at which time the central server system 12 will transmit the task to base computer 14.

The base computer 14, via an agent installed thereon, will contact the central server 12 from time to time to determine if a remote user session has been established. Copending application entitled AGENT
5 SYSTEM FOR A SECURE REMOTE ACCESS SYSTEM, filed July 19, 2000, having attorney docket number MONG-00-003, describes more fully this method, system, and apparatus of implementing the agent and is expressly incorporated herein by reference. Thus, the base computer
10 14 intermittently contacts the central server system 12 to determine whether the central server system 12 has established a session with a remote user. When a session has been established between a remote device 16 and the central server system 12, the central server system 12 replies to the base computers next intermittent contact with an IP
15 address and port number for the base computer 14 to establish a socket connection with a server in the central server system 12. The IP address and port number correspond to a server in the central server system 12 handling the particular session task requests. That socket connection will be maintained between the base computer 14 and the server until
20 the server ends the session or a predefined timeout period expires.

While the socket connection is maintained, the base computer 14 "listens" for tasks from the server. It should be noted that because of the

- 13 -

intermittent initial contacts from the base computer 14 to the central server system 12, operation of this system will be allowed, even in the presence of a firewall (i.e. a firewall between the base computer 14 and the internet is intended to preclude a signal from an outside source
5 coming through the firewall unless requested, but will allow outgoing signals; thus, a message sent from a base computer 14 to a web server would be allowed through a firewall along with any response to said message). Likewise, since the base computer 14 establishes the continuous connection with the IP address and port number of the
10 server in question after being informed of same from the central server system 12 in response to one of the intermittent contacts, a firewall is not a problem.

Thus, once a task is selected by a remote user via remote device 16, the central server system 12 via the connected server (to the base
15 computer) transmits the task request to the base computer 14 and the base computer 14 provides the data and/or files necessary to fulfill that request in response back to the central server system 12. Then, the central server system will present the task information/data to the remote device 16 in a manner readable by remote device 16.

20 More specifically, and referring now to Figures 2 and 4, a continuous connection remote access system and method are depicted. Figure 2 is intended to be a graphical representation of the system,

- 14 -

while Figure 4 is intended to provide a flowchart of the system method. A "continuous connection" includes, but is not limited to such on demand or persistent connection means such as T1, T3, ADSL, ISDN or other similar types of connectivity as opposed to dial-up connections.

5 As shown in Figure 2, a base computer 14 resides on a network with a plurality of other devices as is common in an office setting. That network resides behind firewall 15 which is intended to prevent unwanted access to the network from outside sources (hackers, etc.). A message may pass from within the firewall to outside sources such as
10 internet 18 web servers as will be appreciated by those skilled in the art. Likewise, responses to such outgoing signals are allowed back through the firewall as they are deemed wanted since a device within the firewall requested them. The communication media is continuously available to users as is known and common in large group settings such
15 as offices. That is, access does not require any additional level of effort by base computer 14, as would be the case for dial-up connections. Thus, Figure 2 depicts one embodiment of the invention where the environment includes a continuous open connection between base computer 14 and central server system 12 via internet 18 preferably in
20 an encrypted manner.

On the other hand, mobile devices 16 are also capable of connecting to central server system 12 as they would any other internet

- 15 -

resource. Central server system 12 includes the necessary server subsystems for communicating appropriately with each such remote device. Co-pending application entitled METHOD AND APPARATUS FOR A SECURE REMOTE ACCESS SYSTEM, filed July 19, 2000, 5 having attorney docket number MONG-00-002, describes more fully this method, system, and apparatus of implementing the server subsystems within the central server system and is expressly incorporated herein by reference. For instance, one server within central server system 12 may communicate to WAP (wireless application protocol) enabled devices 16, 10 cellular telephones for instance, while another may communicate to IP (internet protocol) enabled devices 16, laptop computers for instance. The communication between remote devices 16 and central server system 12 is preferably accomplished in a secure and authenticated manner, such as by secure sockets layer (SSL) and passwords.

15 Software installed on the base computer 14, an agent as described in U.S. Patent Serial Number XX/XXXX, attorney docket number MONG-00-003 incorporated herein by reference, provides the capability of receiving tasks from central server system 12. It is also capable of performing those tasks on data within base computer 14. For 20 instance, if the agent within base computer 14 receives a task from central server system 12 and central server system 12 transmits the task of getting a file directory from the base computer, the agent

- 16 -

responds by providing the base computer 14 directory structure in a manner understandable by central computer system 12. Furthermore, in this continuous connection environment, the agent in base computer 14 "listens" (since a persistent socket connection has been established)
5 for new tasks from central server 12.

Thus, and referring now especially to Figure 4, the base computer 14 will intermittently contact central server system 12 to determine if a remote session has been established (i.e. a session between a remote device 16 and central server system 12). If a remote session has been
10 established, central server system 12 replies to base computer 14 with an IP address and port number for the base computer 14 to connect with to receive tasks. Base computer 14 then establishes the specified socket connection and awaits ("listens" for) tasks. In this manner, complications associated with firewalls as described above, may be
15 avoided. That is, the connection originates with the base computer 14 and is allowed to go out to central server system 12. Furthermore, the reply transmitted from central server system 12 to base computer 14 is likewise allowed as will be understood by those individuals familiar with firewalls.

20 However, before any communication between central server system 12 and the agent of base computer 14 may take place, a user must have registered with central server system 12. Registration

- 17 -

includes the providing of typical user information such as name, address, telephone number, and so forth and will likewise include an associated password for authentication purposes. The authentication is necessary to establish whether remote users are who they purport to be.

5 Thus, once a user account is established and a record thereof created in the central server system 12 database, a user may then remotely access the base computer 14 with a remote device 16 as follows. From a remote device 16, the user attempts to contact central server system 12 to initiate a remote access session. Central server
10 system 12 enables an SSL session (if remote device 16 is able to communicate via SSL) and requests a username and password from the remote user. The remote user provides a username and password that is verified against the central server system database record discussed above. If the central server system 14 cannot verify the remote
15 username and password provided (one or more attempts may be allowed, but a limited number of attempts is preferred for security reasons), then the session is terminated by the central server system.

On the other hand, if the remote user is authenticated (username and password provided by remote user match central server system
20 database record), then a list of tasks is presented to the remote used to choose amongst. The list may include such tasks as "check email", "get directory list", "upload files to base computer", "download files from base

- 18 -

computer”, “get address book”, and other like tasks. This list may be presented as text or as icons or both depending on the remote device protocol limitations or capabilities. The user will then select a task from the list.

5 Upon receipt of the user task selection form remote device 16, the central server system 12 then transmits that task to the connected base computer 14. Then, upon receipt of the task request, base computer 14 performs the task in accordance with the agent-defined instruction set. For instance, if the task is to provide a directory listing, the agent will
10 provide the necessary directory tree information to the central server system 12.

 Thereafter, the central server system 12, upon receipt of the data from base computer 14, presents the information to the remote device in a manner viewable by the remote device (HTML for a remote computer
15 using a browser for instance). The presented information, will also include other tasks or subtasks that may be selected by the remote user (subdirectories of the directory may be needed in a next step). The remote user will continue selecting tasks or subtasks until wishing to end the session at which time the end session task will be selected. The
20 session is then terminated by the user and central server system 12. Of course, after a period of no selections or activity on the part of the remote user, the session may be terminated by the central server system

- 19 -

as well as will be appreciated by those skilled in the art now informed by this disclosure.

In an alternate embodiment, namely a non-continuous connection environment for the base device, and referring now to Figures 3 and 5, 5 the present invention is likewise depicted. In this environment, non-continuous connection means a connection between the base computer 14 and the central server system 12 in which the connection is not persistent, such as a dial-up or PSTN connection. That is, many home computers are capable of connecting to the internet only by way of a 10 dial-up connection via a local ISP 20. Typically, that ISP resides behind a firewall. Therefore, it is desirable to enable such home users constrained by dial-up connections to access the home computer 14 when away from the home computer 14 with a remote device 16.

As will be understood by those familiar with connecting to an ISP 15 from a home computer via a dial-up connection, the base or home computer 14 must first establish a connection via a PSTN ("POTS") 22 with the ISP by dialing into one or more predefined telephone numbers. If the ISP verifies the user appropriately, such as by a username and password, then the connection is allowed to continue until the user logs 20 off or some other event terminates the session. Also important, but not typically an issue for a dial-up ISP user, is that a firewall typically precludes unwanted incoming traffic from other internet sources to the

- 20 -

ISP. Thus, connected users can send messages from the ISP to other internet sources and receive responses, however, unsolicited incoming traffic is generally precluded by the ISPs firewall 15 to prevent unwanted attacks (or hacks) on the ISP servers and system devices.

5 A remote user having a remote device 16 may connect to the central server system 12 as described above for a continuous connection (i.e. SST, password, authentication, etc.), but in this non-continuous connection environment the base computer 14 may either not be on or at least not connected to the internet. Thus, making it impossible for the
10 base computer to intermittently contact the central server system 12 as described above. However, the central server system 12 can record the telephone number of the base computer's modem upon registration by requiring the user to provide such information upon registering. Having this information then, when the central server system 12 is contacted by
15 a remote device 16, central server system 12 will, via one or more available modems (i.e. a modem bank), dial the base computer modem line telephone number to attempt a connection therewith.

As will be appreciated by those familiar with modern modems, the base computer 14, if not already on, may turn itself on when the
20 modem therewith is called upon by the central server system 12 and a connection established. Thus, once "awakened," the agent within the base computer 14 may initiate contact processes as follows. First, the

- 21 -

connection is terminated with central server system 12, thus minimizing costs associated with the central server system 12 having to dial into the base computer 14. Then, the base computer 14 can establish an internet connection by dialing into ISP 20 via PSTN 22. Once connected to the internet in this manner, base computer 14 via the agent may begin
5 intermittently contacting the central server system 12 to determine if a remote session has been established, not unlike the process described above for the continuous connection environment. On the other hand, if upon attempting to establish a connection with base computer 14,
10 central server system 12 encounters a "busy" signal, then the session with the remote device is terminated.

More specifically, and referring now especially to Figure 5, a user having a remote device will attempt to login to central server system 12 and central server system 12 will establish (if possible) a SSL
15 connection. A username (or number) and password are then requested of the remote user by central server system 12. If authenticated, a task list is presented to the remote user by the central server system 12 on remote device 16. If authentication fails, the session is terminated. If authentication succeeds, central server system 12 initiates a call to base
20 computer 14's modem.

If the base computer 14 modem is not busy, then the agent therein disconnects the line and establishes a connection with the user's

SUBSTITUTE SHEET (RULE 26)

- 22 -

ISP 20 (as described above). Once the connection with the ISP 20 is established, the agent will begin intermittently contacting central server system 12 to determine if a remote session has been established. If a remote session has indeed been established, the central server system 5 12 will send an IP address and port number of the server processing tasks for the session to the base computer 14. Then the base computer 14 establishes a connection at the specified IP address and port number and begins "listening" for tasks on the established socket connection. Once a task is selected on the remote device 16 by a remote user, the 10 central server system 12 will transmit that task request to the base computer via the established socket connection. Then, as with the continuous connection environment, the base computer will perform the task by supplying the data necessary to fulfill the task to the central server system 12. This process will continue until the session is 15 terminated by the central server system (via selection of a termination task request by a remote user or the expiration of a predefined time-out period).

While embodiments and applications of this invention have been shown and described, it would be apparent to those skilled in the art 20 that many more modifications than mentioned above are possible without departing from the inventive concepts herein. The invention,

SUBSTITUTE SHEET (RULE 26)

- 23 -

therefore, is not to be restricted except in the spirit of the appended claims.

- 24 -

What is claimed is:

1. A method for remotely accessing a base computer from internet-enabled remote devices wherein the remote devices do not include remote access software, comprising in combination:
 - 5 establishing a remote access session with one of the remote devices at an internet central server system;
presenting a task list to the remote device from said central server system;
receiving a task selection at said central server system from the
10 remote device;
establishing a persistent connection between said central server system and a base computer in response to intermittent contact from said base computer to said central server system;
transmitting said task from said central server system to the
15 base computer via said connection between said central server system and said base computer;
receiving at said central server system task data from the base computer responsive to said transmitted task; and
presenting from said central server system a task response
20 compiled from said task data to the remote device.

- 25 -

2. The method of claim 1 further comprising terminating said remote access session by said central server system.
3. The method of claim 2 further comprising communicating said task response via a protocol compatible with the remote device.
4. The method of claim 3 wherein said protocol is TCP/IP for remote devices configured as computers.
5. The method of claim 3 wherein said protocol is WAP for remote devices configured as wireless communication devices.
6. The method of claim 1 further comprising authenticating the user of the remote device while establishing the remote access session.
7. The method of claim 6 further comprising providing a secure communication means while establishing the remote access session and continuing said secure communication between said central server system and the remote device until said session is terminated.

20

- 26 -

8. The method of claim 7 further comprising encrypting the communications between said central server system and the base computer.
- 5 9. The method of claim 8 further comprising establishing a communication link between the base computer and the central server system when the base computer is not already connected to the internet.
- 10 10. The method of claim 9 further comprising dialing up a base computer modem by the central server system to wake up the base computer to establish said communication link.
- 15 11. The method of claim 10 further comprising disconnecting from the dial up connection by the base computer and then reestablishing the communication link via the internet between said central server system and said base computer.
12. A remote access system, comprising in combination:
a central server system in operative communication with the
20 internet;
an internet server for communicating with remote devices, said internet server comprising one server within said central server system;

SUBSTITUTE SHEET (RULE 26)

- 27 -

a task transmitter within said central server system for transmitting tasks to base computers; and

a task data receiver within said central server system for receiving task data from base computers.

5

13. The remote access system of claim 12 further comprising security services enabled between said central server system and remote devices, and between said central server system and base computers.

10 14. The remote access system of claim 13 wherein said security services between said central server system and remote devices include means for authenticating the user of the remote device.

15 15. The remote access system of claim 14 wherein said security services between said central server system and base computers includes encryption.

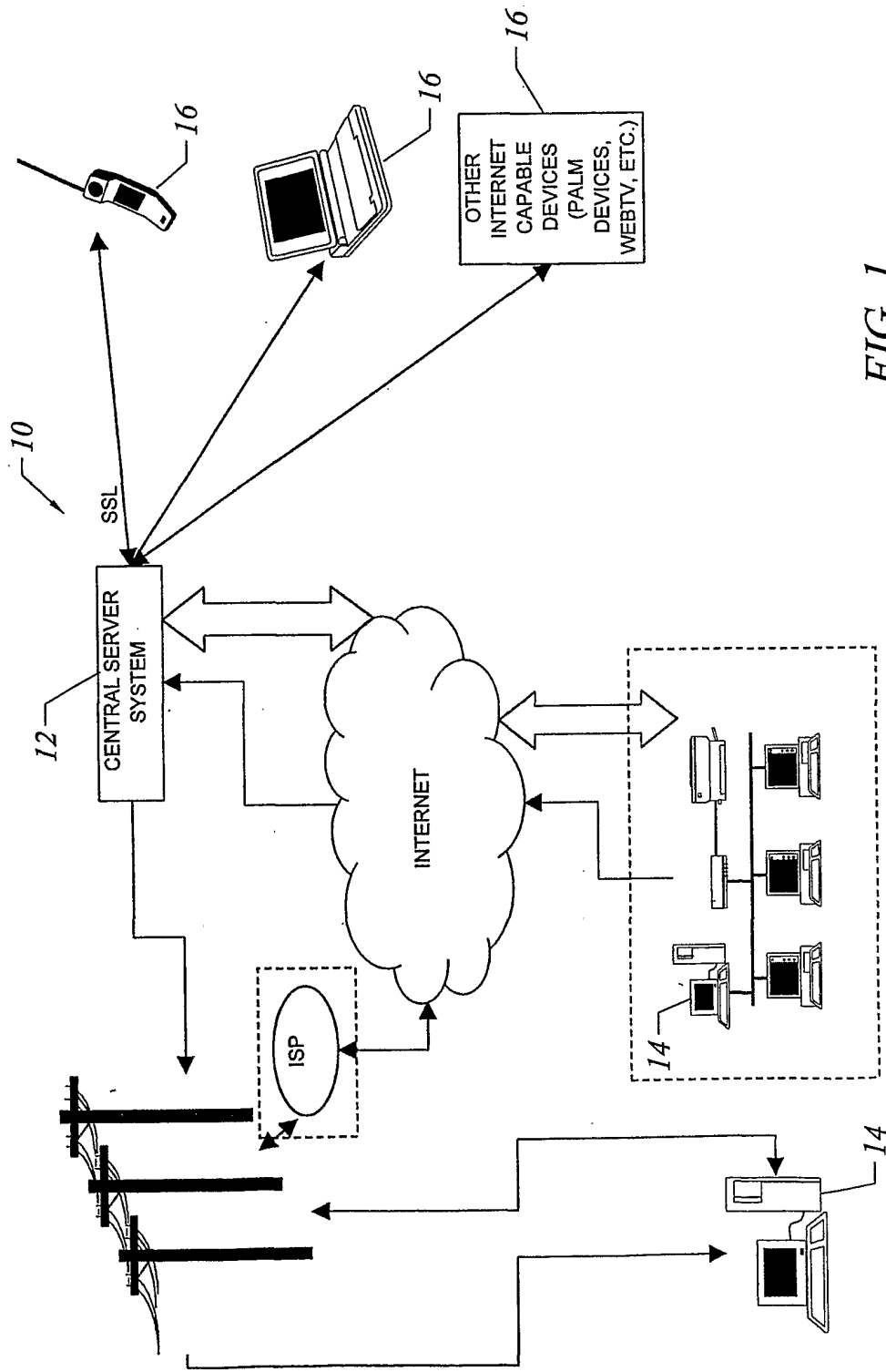


FIG. 1

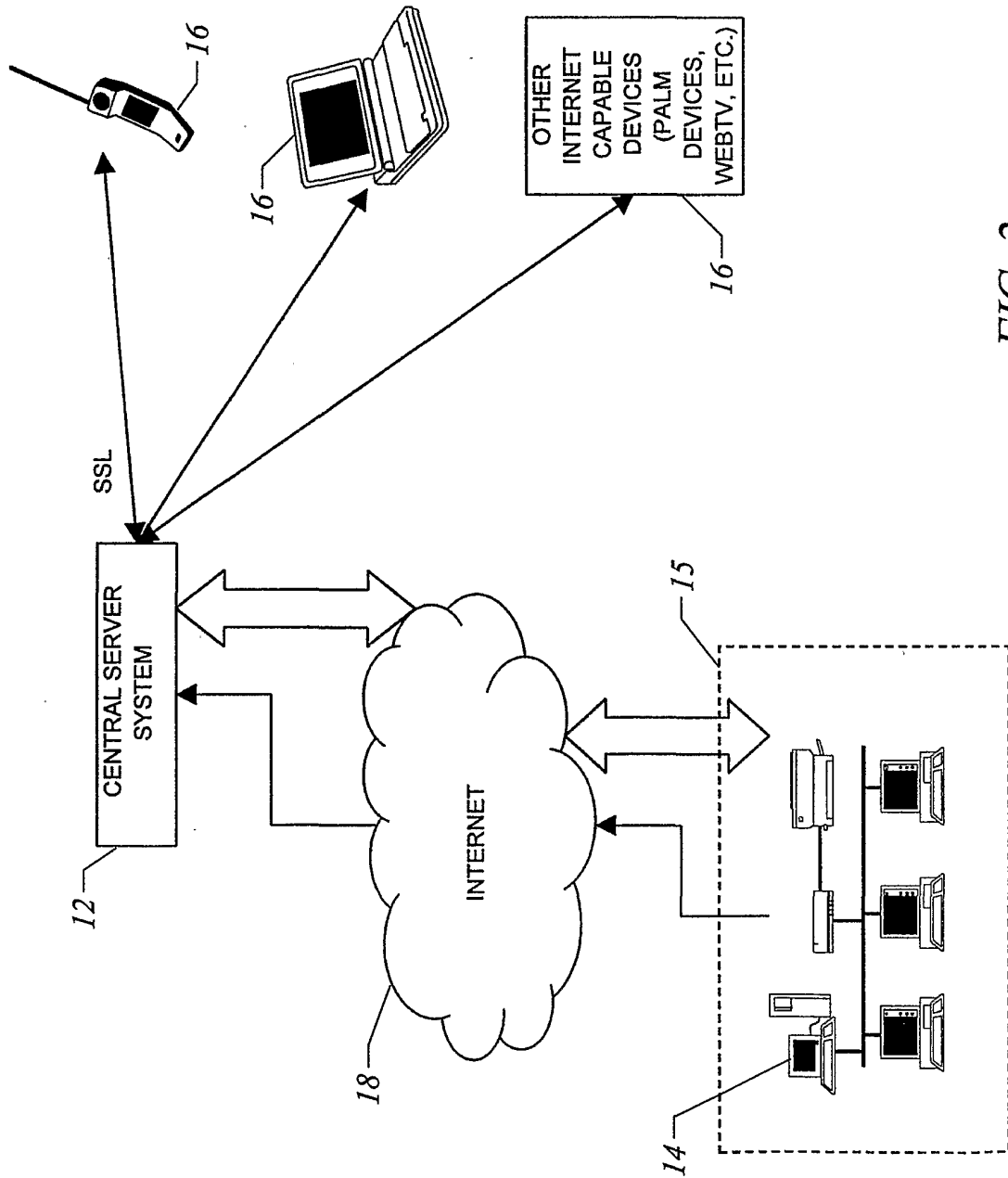


FIG. 2

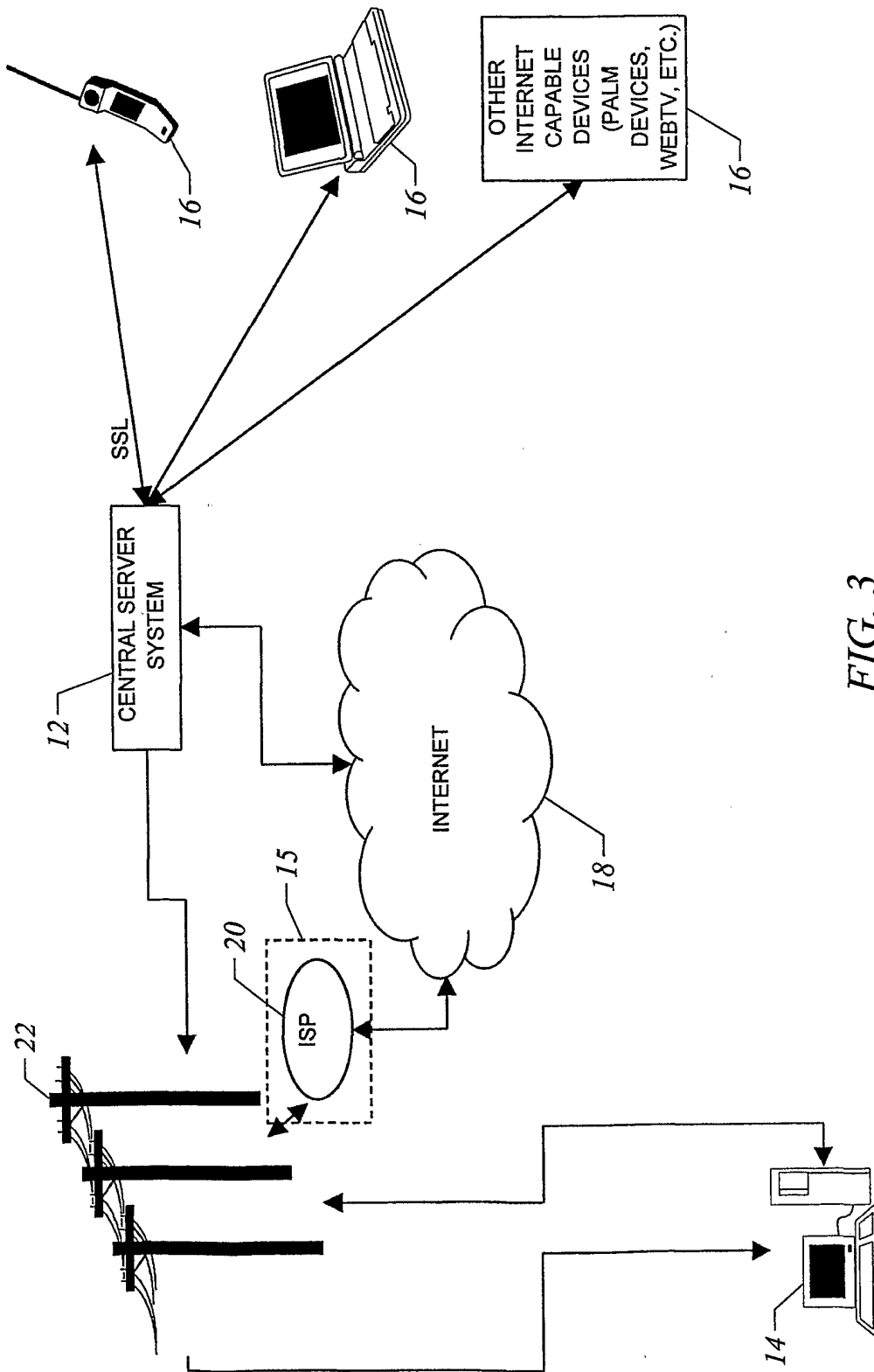


FIG. 3

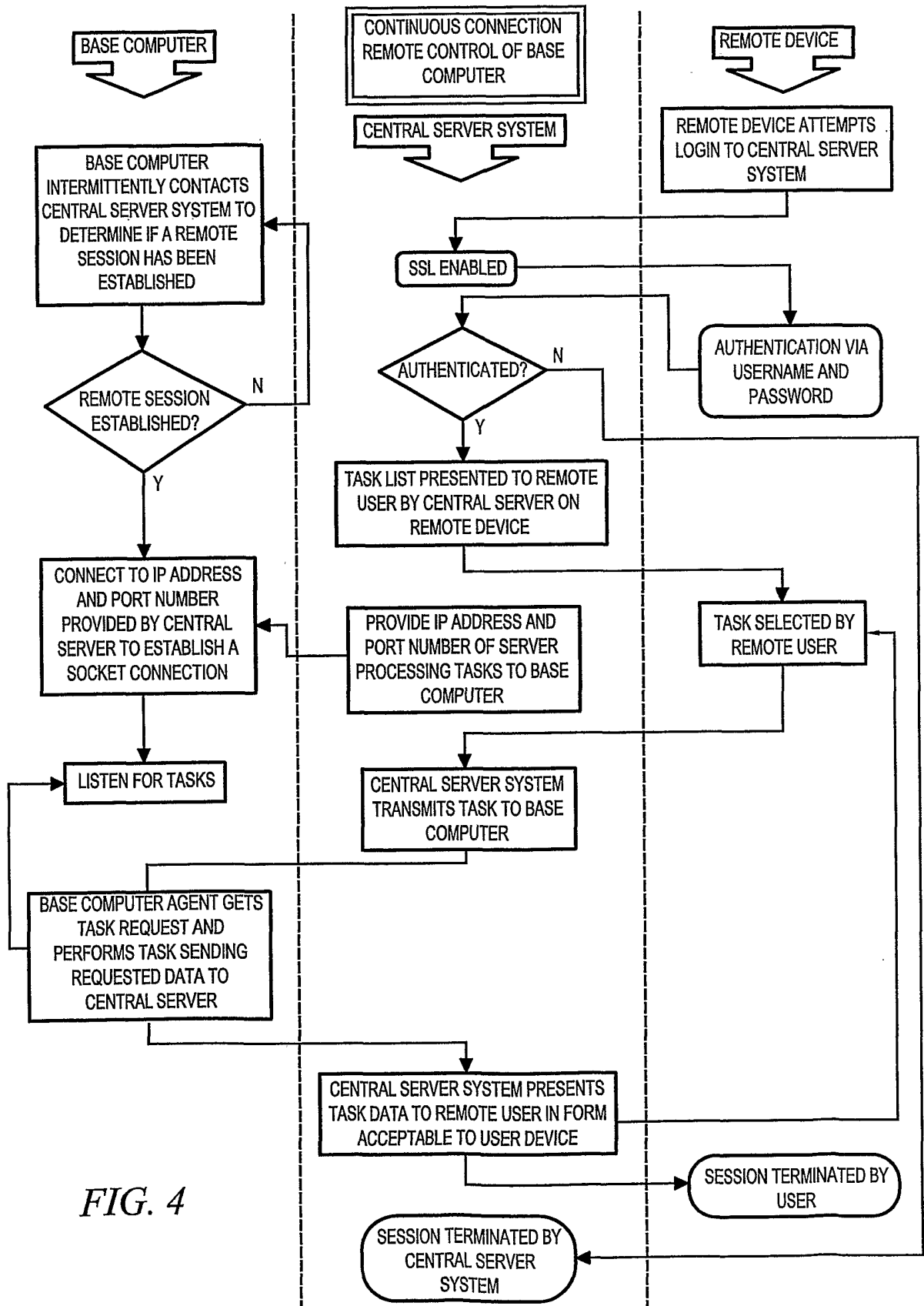
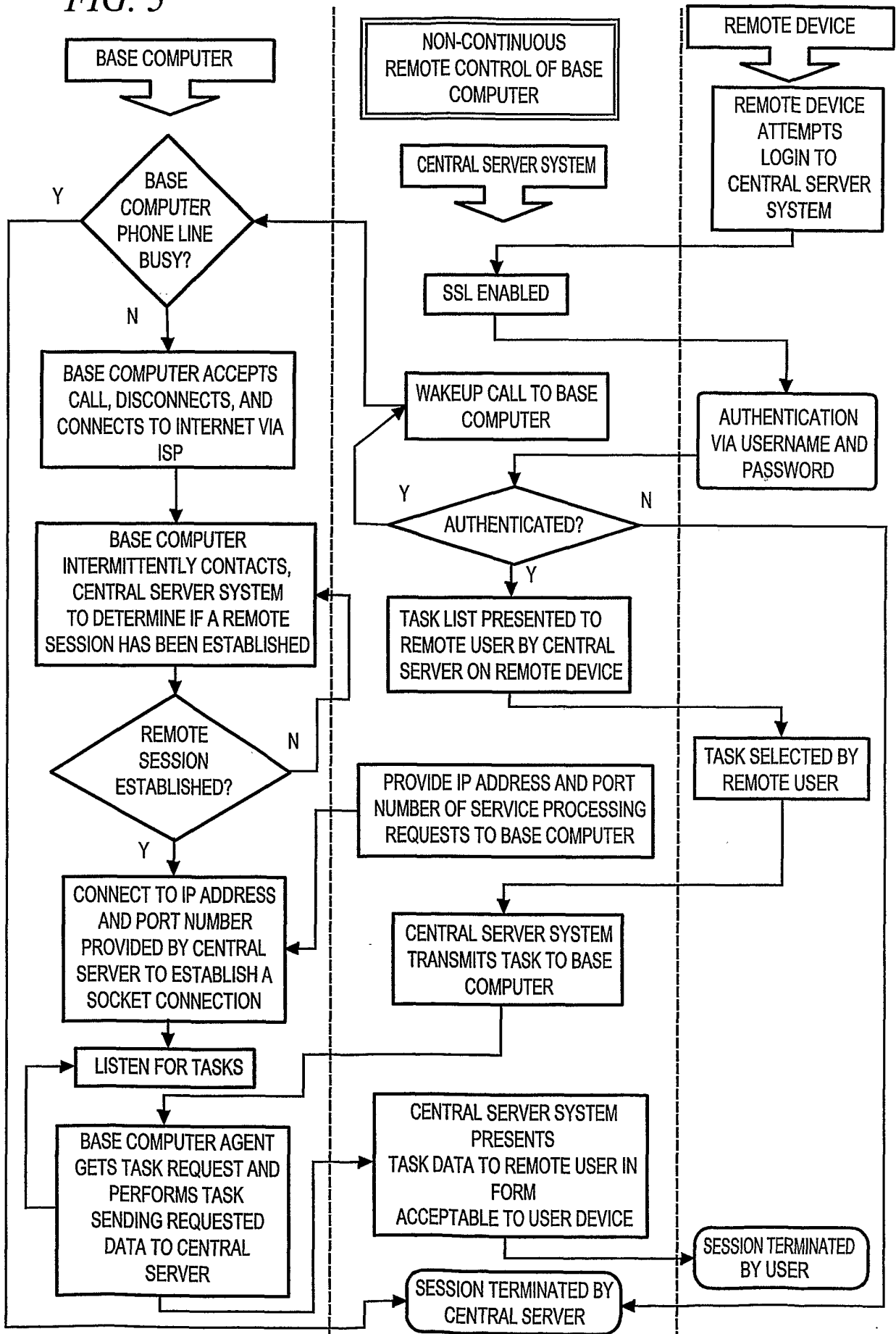


FIG. 4

FIG. 5

5/5



INTERNATIONAL SEARCH REPORT

International application No. .
PCT/US01/22824

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06F 13/00
US CL :709/203, 100, 200

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 709/203, 100, 200

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

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

WEST: USPT

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,012,088 A (LI et al.) 04 January 2000; Abstract; Figs. 4,8,11A	1-15
A,P	US 6,247,048 B1 (GREER et al.) 12 June 2001	

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

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

Date of the actual completion of the international search

30 SEPTEMBER 2001

Date of mailing of the international search report

30 OCT 2001

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

KENNETH R. GOUTER

Telephone No. (703) 305-8447