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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 December 2001 (27.12.2001)

PCT

(10) International Publication Number
WO 01/98947 A1

(51) International Patent Classification[7]: G06F 17/30

(21) International Application Number: PCT/US00/32925

(22) International Filing Date: 4 December 2000 (04.12.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/594,409 16 June 2000 (16.06.2000) US

(71) Applicant: **N2H2, INC.** [US/US]; Suite 3400, 900 4th Avenue, Seattle, WA 98164 (US).

(72) Inventors: **IRWIN, James, M.**; 1904 - 239th Place SE, Bothell, WA 98021 (US). **HOTOPP, Mark, R.**; 3315 - 133rd Street SW, Unit 104, Lynnwood, WA 98037 (US). **MOHAZZABFAR, Amir, F.**; 7620 NE 24th, Medina, WA 98039 (US).

(74) Agent: **HOPE, Leonard, J.**; Christensen O'Connor Johnson & Kindness PLLC, Suite 2800, 1420 Fifth Avenue, Seattle, WA 98101 (US).

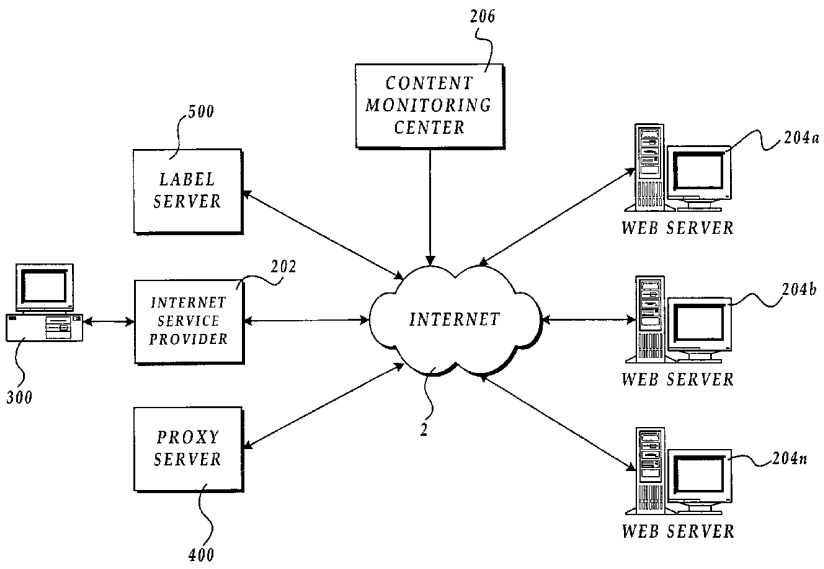
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR FILTERING CONTENT AVAILABLE THROUGH A DISTRIBUTED COMPUTING NETWORK



(57) Abstract: A client computer, proxy server computer, label server computer, and a content monitoring center are provided for filtering network content. When a request is received at the client computer for a network resource, the client computer requests the resource from either the proxy or label server computer. If the request is made to the proxy server, the proxy server searches a block database and an allow database to determine if the client computer is blocked from retrieving the resource. If the client computer is blocked from retrieving the resource, the proxy server computer returns an error message to the client computer. If the client computer is not blocked from retrieving the resource, the proxy server computer retrieves the resource on behalf of the client computer and transmits the requested resource to the client computer. The requested resource may then be displayed at the client computer. If the request is made to the label server, the label server searches a block database and an allow database and returns the search results to the client computer. The client computer receives the search results and displays an error message if the client computer is blocked from retrieving the requested resource. If the client computer is not blocked from retrieving the requested network resource, the client computer retrieves the requested resource directly from a server computer hosting the resource. The requested resource may then be displayed at the client computer. A content monitoring center monitors available network resources to identify those resources that the client computer should not be permitted to retrieve. The content monitoring center then utilizes this data to update the block and allow databases utilzed by the proxy and label servers.

WO 01/98947 A1

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.

METHOD AND SYSTEM FOR FILTERING CONTENT AVAILABLE THROUGH A DISTRIBUTED COMPUTING NETWORK

Field of the Invention

This invention generally relates to the field of network computing and, more specifically, to a method and system for filtering content that is available through a distributed computing network.

Background of the Invention

With the advent and explosion of the Internet, literally millions of World Wide Web ("WWW" or "Web") sites have been created. Web sites exist today that provide information in virtually every known subject area, like news, weather, stocks and other business information, hobbies, technology, and more. The content provided by these Web sites is typically available to anyone using a standard personal computer connected to the Internet and that has a Web browser application program. The large body of information available through these types of Web sites is of great value to researchers, employees, hobbyists, and students of all ages.

Along with the explosion in the number of Web sites available on the Internet has come a similar explosion in the number of available Web sites dealing with information that may be illegal or considered offensive. For instance, Web sites exist today that provide child pornography, information on racism, hate groups, graphic violence, and other content that may be objectionable. While appreciated by some, these types of Web sites are particularly offensive to many adults, and especially offensive and even potentially harmful to children. Moreover, these types of Web

sites may be accessed through computers located in places where it would be considered inappropriate to access such Web sites, such as an office setting.

With the proliferation of potentially offensive Web sites, the likelihood that these Web sites will be encountered while utilizing the WWW has increased dramatically. A simple keyword search for non-objectionable material is likely to produce search results that include Web links to potentially offensive content. Once such search results have been displayed to the user, the user is only one mouse click away from the potentially harmful Web sites. An unsupervised child or an employee working on a company computer can then easily access these Web sites, and may even do so inadvertently through an erroneous selection. In response to this, methods and systems for filtering Internet content have been created to filter and restrict the Web sites that a particular computer may access. However, the previous methods and systems for filtering network content suffer from several drawbacks.

One type of system for filtering Internet content utilizes a database located at the client computer executing the Web browser to identify "blocked" Web sites. When a request is received for a Web site, a check of the block database is made to determine if access to the Web site has been blocked. If the Web site is listed in the database, access to the Web site is blocked and the Web browser is not permitted to access the requested Web site. If the Web site is not blocked, the Web browser is permitted to connect to the requested Web site. While this type of system produces acceptable results, the main drawback of this system is that the user must manually update the contents of the block database or manually request an update of the database from the provider of the filtering system. If the user does not update the database, a user of the computer may be permitted access to objectionable Web sites that are not listed in an outdated database. Moreover, even if the database could be automatically updated on the client computer, the typically large size of such databases and the slow speeds of most Internet connections make updating such a database located on a client computer impracticable.

Another type of system for filtering Internet content relies on a proxy server computer to filter content for a group of computers connected to a LAN ("Local Area Network"). When a request for a Web site is received from one of the computers connected to the LAN at the proxy server, the proxy server checks a database of blocked sites to determine if the sited has been blocked. If the site has not been blocked, the proxy server connects to the requested Web site on behalf of the requesting computer and provides the requested Web page to the computer. If the

site has been blocked, an error message is provided to the requesting computer. This type of system works exceptionally well in an office environment or a school setting where many computers connect to the Internet through a proxy server. However, this type of filtering system is impracticable in a home setting where a single computer may access the Internet without the use of a proxy server. A proxy server simply cannot be required in a home setting to provide content filtering for a single client computer.

Therefore, in light of these problems, there is a need for a method and system for filtering content available through a distributed computing network that does not require a user to manually update a database of blocked Web sites or store a large database of blocked sites at the client computer. Furthermore, there is a need for a method and system for filtering content available through a distributed computing network that does not require the use of a proxy server computer for each individual client computer.

Summary of the Invention

The present invention solves the above described problems by providing a method and system for filtering content available through a distributed computing network, like the Internet. According to one actual embodiment of the invention, a method and system for filtering network content is provided that does not require manual updating of a block database stored at the client computer, and does not require the storage of a large block database at the client computer. Moreover, the present invention provides a method and system for filtering network content that may be utilized by a single client computer without the use of a proxy server located proximate to the client computer.

Generally described, the present invention provides a system for filtering network content. According to one actual embodiment of the present invention, a client computer, proxy server computer, and a content monitoring center are provided. The client computer comprises a standard personal computer executing a Web browser application program. The client computer also comprises application software that intercepts requests for network resources, such as Web sites, and redirects these requests to the proxy server. Therefore, when a request is received at the client computer for a network resource, such as a Web site, the client computer requests the resource from the proxy server computer instead of requesting the resource directly from the server computer hosting the network resource.

The proxy server computer is connected to the Internet via a very high-speed connection and receives requests for network resources from the client computer. The proxy server computer maintains a "block" database that identifies network resources that the client computer is not permitted to access. Additionally, the proxy server computer may maintain an "allow" database identifying network resources that the client computer is explicitly permitted to access. The proxy server computer receives requests for network resources from the client computer and, in response, searches its block and allow databases to determine if the client computer is blocked from retrieving the requested network resource. If the client computer is blocked from retrieving the requested network resource, the proxy server computer returns an error message to the client computer. If the client computer is not blocked from retrieving the requested network resource, the proxy server computer retrieves the network resource on behalf of the client computer and transmits the requested resource to the client computer. The requested resource may then be displayed at the client computer.

According to an embodiment of the present invention, a content monitoring center is also provided. The content monitoring center monitors resources available on the network, such as Web sites, to identify resources that the client computer should not be permitted to retrieve. The content monitoring center then utilizes this data to maintain the block and allow databases utilized by the proxy server. Like the proxy server, the content monitoring center is connected to the Internet via a very high-speed Internet connection. Utilizing the high-speed connection, the content monitoring center can continually update the block and allow databases located at the proxy server, even if these databases grow very large. By updating these databases frequently, offensive network resources may be blocked almost immediately after they are created and go "live" on the Internet. Moreover, because the block database is located at the proxy server and updated by the content monitoring center, the user of the client computer does not have to manually update a database.

According to an embodiment of the present invention, the client computer also maintains a "block" database identifying network resources to be blocked. Such a database may be searched by the client computer prior to contacting the proxy server computer to determine if the requested resource has been blocked. If the requested resource has been blocked, an error message will be generated at the client computer and the client computer will not be permitted to access the requested resource. Likewise, the client computer may also maintain an "allow" database to

override the inclusion of a resource in the proxy server block database that blocks a particular site. The client computer may also search the allow database prior to contacting the proxy server. If a requested resource is identified in the allow database, the client computer is explicitly allowed to retrieve the resource, so therefore the proxy server is not contacted. If a requested resource is not identified in the allow database or the block database, the proxy server is utilized as described above. By maintaining block and allow databases at the client computer, a user of the client computer can block or explicitly allow network resources that are not identified in the block and allow databases maintained by the proxy server.

According to another actual embodiment of the present invention, a client computer, a label server computer, and a content monitoring center are provided for filtering network content. When a request for a network resource is received at the client computer, a request to validate the network resource is transmitted to the label server computer. The label server computer is connected to the Internet via a high-speed connection. The label server computer receives the request to validate the network resource from the client computer and, in response, searches a block database and an allow database to determine if the requested resource is identified in either of these databases. The label server then returns the search results to the client computer.

The client computer receives the search results from the label server and determines whether the search results indicate that the client computer is permitted to retrieve the requested network resource. If the client computer is permitted to retrieve the requested network resource, the client computer retrieves the network resource directly from the server computer hosting the requested network resource. If the client computer is not permitted to retrieve the network resource, an error message is displayed at the client computer. As in the proxy server embodiment, the client computer may also search block and allow databases located at the client computer prior to contacting the label server to override the block and allow databases located at the label server. Additionally, as in the proxy server embodiment, the block and allow databases stored at the label server may be updated by a content monitoring center.

In accordance with yet other aspects of the invention, a method, a computer-controlled apparatus, and a computer-readable medium containing instructions are also provided for filtering network content.

Brief Description of the Drawings

The foregoing aspects and many of the attendant advantages of this invention will become more readily appreciated as the same become better understood by reference to the following detailed description, when taken in conjunction with the accompanying drawings, wherein:

FIGURE 1 is a block diagram illustrating an exemplary operating environment for aspects of the present invention.

FIGURE 2 is a block diagram illustrating an actual embodiment of the present invention for filtering network content available over a distributed computing network.

FIGURE 3 is a block diagram showing an illustrative client computer utilized in an embodiment of the present invention.

FIGURE 4 is a block diagram showing an illustrative proxy server computer utilized in an actual embodiment of the present invention.

FIGURE 5 is a block diagram showing an illustrative label server computer utilized in an actual embodiment of the present invention.

FIGURE 6A is a flow diagram illustrating the operation of a client computer utilizing a proxy server to filter network content in an actual embodiment of the present invention.

FIGURE 6B is a flow diagram illustrating the operation of a client computer utilizing a label server to filter network content in an actual embodiment of the present invention.

FIGURE 7 is a flow diagram illustrating the operation of a proxy server computer for filtering network content in an actual embodiment of the present invention.

FIGURE 8 is a flow diagram illustrating the operation of a label server computer for filtering network content in an actual embodiment of the present invention.

Detailed Description of An Illustrative Embodiment

The present invention provides a method, system for filtering content available through a distributed computing network. Aspects of the present invention are embodied in one or more server computers and other system components accessible through, and utilizing, the Internet. As is well known to those skilled in the art, the term "Internet" refers to the collection of networks and routers that use the

Transmission Control Protocol/Internet Protocol ("TCP/IP") to communicate with one another. A representative section of the Internet 2 is shown in FIGURE 1, in which a plurality of local area networks ("LANs") 102 and a wide area network ("WAN") 106 are interconnected by routers 104. The routers are special purpose computers used to interface one LAN or WAN to another. Communication links within the LANs may be twisted wire pair, or coaxial cable, while communication links between networks may utilize 56 Kbps analog telephone lines, 1 Mbps digital T-1 lines, 45 Mbps T-3 lines or other types of high-speed communications links known to those skilled in the art. Furthermore, computers, such as client computer 300, and other related electronic devices can be remotely connected to either the LANs 102 or the WAN 106 via a modem and temporary telephone link, or other type of network connection. It will be appreciated that the Internet 2 comprises a vast number of such interconnected networks, computers, and routers and that only a small, representative section of the Internet is shown in FIGURE 1.

Communication over the Internet typically take place based upon an information exchange between client computers and server computers. Each client computer and server computer is assigned an Internet Protocol ("IP") address that uniquely identifies the computer on the Internet. The IP addresses of server computers may also be mapped to domain names using a series of name server computers also accessible over the Internet. As will be described in more detail below, the IP address of a server computer may be utilized to filter network resources available from the server computer.

As the Internet has grown, so has the number of network resources available to users of the Internet. Network resources are files and other data available on the Internet and, in particular, through the WWW. Network resources available over the Internet are typically identified using a Uniform Resource Locator ("URL"), such as "http://www.n2h2.com/index.html." A URL has two parts: (1) a scheme and (2) a scheme-specific part. The scheme identifies the high-level protocol through which the resource is to be transferred. The scheme-specific part contains additional information useful in establishing a connection between a client and a server. The phrase "http" is the scheme for network resources available via the Web. This indicates that the Internet address specified communicates using HTTP. The remainder of the URL following the colon is the scheme-specific part. Generally, this portion of the URL identifies a host HTTP server name and the file system path to the network resource to be transferred. As will be described in more detail below,

the URL of a network resource may be utilized to filter the network resource. Those skilled in the art should appreciate that while the described embodiment of the present invention filters network resources available over the WWW, network resources available via any other transmission protocol may be similarly filtered. For instance, network resources available via the File Transfer Protocol ("FTP"), Gopher, or other type of Wide Area Information Server may be filtered in a similar manner.

As is appreciated by those skilled in the art, the WWW is a vast collection of interconnected or "hypertext" documents written in the HyperText Markup Language ("HTML"), or another standard markup language, and that are electronically stored at "Web sites" throughout the Internet. A Web site is a server computer connected to the Internet that has mass storage facilities for storing hypertext documents and that runs administrative software for handling requests for those stored hypertext documents. As is known to those skilled in the art, a Web server may also include facilities for storing and transmitting application programs, such as application programs written in the JAVA® programming language from Sun Microsystems, for execution on a remote computer. Likewise, a Web server may also include facilities for executing scripts and other application programs on the Web server itself. In general, Web servers are stateless with respect to client transactions. The stateless nature of the Web simplifies the server and client architectures.

A client computer may retrieve network resources from the Web by utilizing a Web browser application program. A Web browser, such as Netscape's NAVIGATOR® or Microsoft's INTERNET EXPLORER®, is a software application program for providing displaying network resources available on the Web. Generally, when a request is made by a user to retrieve a network resource, the Web browser transmits a request for the network resource to the server computer identified in the URL of the network resource. In response to the request, the server computer hosting the network resource transmits the resource to the client computer. When the requested resource is received at the client computer, the Web browser uses the contents of the resource to construct and display its contents. Typically, a network resource, such as an HTML file, contains various commands for displaying text, graphics, controls, background colors, and other types of display features. The resource may contain the URL addresses of other network resources that should be included in the visual representation of the resource, such as graphics, sounds, animation files, or hyperlinks.

Referring now to FIGURE 2, several embodiments of the present invention will be described. According to one actual embodiment of the present invention, a client computer 300, a proxy server computer 400, and a content monitoring center 206 are provided that are connected to the Internet 2. The client computer 300 comprises a standard personal computer executing a Web browser application program. The client computer 300 also comprises application software that intercepts requests for network resources, such as Web sites, and redirects these requests to the proxy server 400. When a request is received at the client computer for a network resource, such as a Web site hosted by one of Web servers 204A-204N, the client computer 300 requests the resource from the proxy server computer 400 rather than requesting the resource directly from the server computer hosting the network resource. The client computer 300 will be described in greater detail below with reference to FIGURES 3, 6A, and 6B.

The proxy server 400 computer is connected to the Internet 2 via a high-speed connection, such as a T-3 or an OC-3 connection known to those skilled in the art. The proxy server 400 is located at a separate location from the client computer 300 and is accessible to many client computers. The proxy server computer 400 receives requests for network resources from the client computer 300 over the Internet 2. The proxy server computer 400 also maintains a "block" database that identifies network resources that the client computer is "blocked" from retrieving. Additionally, the proxy server computer 400 may maintain an "allow" database that contains the identity of network resources that the client computer 300 is explicitly permitted to retrieve.

The proxy server computer 400 receives requests for network resources from the client computer 300 and, in response, searches its block and allow databases to determine if the client computer 300 is blocked from retrieving the requested network resource. If the client computer 300 is blocked from retrieving the requested network resource, the proxy server computer 400 returns an error message to the client computer 300. If the client computer 300 is not blocked from retrieving the requested network resource, the proxy server computer 400 retrieves the network resource on behalf of the client computer 300 and transmits the requested resource to the client computer300. The requested resource may then be displayed at the client computer 300. Additional aspects of the proxy server computer 400 are described below with respect to FIGURES 4 and 7.

According to another actual embodiment of the present invention, a client computer 300, a label server computer 500, and a content monitoring center 206 are provided that are connected to the Internet 2. When a request is received at the client computer 300 for a network resource such as a Web site served by one of Web server computers 204A-204N, a request to validate the network resource is transmitted to the label server computer 500. Like the proxy server computer, the label server computer 500 is also connected to the Internet 2 via a high-speed connection. The label server computer 500 receives the request to validate the network resource from the client computer 300 and, in response, searches a block database and an allow database to determine if the requested resource is identified in either of these databases. The label server computer 500 then returns the search results to the client computer. The label server computer 500 will be described in more detail below with respect to FIGURES 5 and 8.

The client computer 300 receives the search results from the label server and determines whether the search results indicate that the client computer 300 is permitted to retrieve the requested network resource. If the client computer 300 is permitted to retrieve the requested network resource, the client computer 300 retrieves the network resource directly from the server computer hosting the requested network resource without the aid of the label server computer 500. If the client computer 300 is not permitted to retrieve the network resource, an error message is displayed at the client computer 300.

According to an embodiment of the present invention, a content monitoring center 206 is also provided. The content monitoring center 206 monitors resources available on the network, such as Web sites served by Web server computers 204A-204N, and identifies resources that the client computer 300 should not be permitted to retrieve. Typically, network resources that the client computer 300 is not permitted to receive are identified by IP address or by a specific URL at which the resource is located. The content monitoring center 206 then transmits this data to the proxy server computer 400 or label server computer 500 so that the data can be used to update the block and allow databases. The content monitoring center 206 is also connected to the Internet via a very high-speed Internet connection. Utilizing the high-speed connection, the content monitoring center 206 can periodically update the block and allow databases located at the proxy server computer 400 and the label server computer 500.

Referring now to FIGURE 3 a client computer 300 utilized in an embodiment of the present invention will be described. Those of ordinary skill in the art will appreciate that the client computer 300 includes many more components than those shown in FIGURE 3. However, it is not necessary that all of these generally conventional components be shown in order to disclose an illustrative embodiment for practicing the present invention. The client computer 300 includes a network interface unit (not shown) for providing a communications connection 334 for connecting to the Internet or other type of distributed computing network. Those of ordinary skill in the art will appreciate that such a network interface unit includes the necessary circuitry for such a connection, and is also constructed for use with the TCP/IP protocol, the particular network configuration of the LAN, WAN, or Internet Service Provider it is connecting to the Internet through, and a particular type of coupling medium. The client computer 300 may also be equipped with a network interface unit capable of communicating with an Internet Service Provider through a point to point protocol ("PPP") connection or a Serial Line Interface Protocol ("SLIP") connection as known to those skilled in the art.

The client computer 300 also includes a ROM BIOS 310, central processing unit 302, and a system memory 304. The system memory 304 generally comprises a random access memory ("RAM") 306, a read-only memory ("ROM") 308 and a permanent mass storage device 314, such as a disk drive. The system memory 304 typically stores an operating system (not shown) for controlling the operation of the client computer 300, and may also store application programs. The storage device 314 and system memory 304 also includes a WWW browser application program 316, such as Netscape's NAVIGATOR® or Microsoft's INTERNET EXPLORER® browsers, for accessing the WWW. It will be appreciated that these components may be stored on a computer-readable medium and loaded into the system memory 304 of the client computer 300 using a drive mechanism associated with the computer-readable medium, such as a floppy drive, CD-ROM/DVD-ROM drive, or hard disk drive (not shown). An input interface (not shown) may also be provided for receiving input from input devices 330, such as a mouse or keyboard. Likewise, an output interface (not shown) may also be provided for outputting information to the communications connection 334, a video display adapter, speakers, printers, and the like. The system memory 304, communications connection 334, input devices 332, and output devices 330 are all connected to the central processing unit 302 via

system bus 312. Other peripherals may also be connected to the central processing unit 302 in a similar manner.

The storage device 314 also includes a configuration application program 322. The configuration application 322 may be utilized by a user of the client computer 300 to specify configuration settings, such as the level of network content that should be filtered for a particular user of the client computer 300. For instance, a user may choose between a "safe haven," where the highest level of potentially offensive network content is filtered, a "protected surfing" level, where a lower level of network content is filtered, or a "free ride" level, where no filtering takes place. These configuration settings would then be saved by the configuration application 322 in the configuration database 320.

The configuration application 322 may also allow a user of the client computer 300 to input the URL or IP address of network resources that the client computer should be blocked from retrieving, or that the client computer should be explicitly permitted to retrieve. The identities of these "blocked" or "allowed" sites are then stored in the local block database 326 or the local allow database 328, respectively. As will be described in greater detail below with respect to FIGURES 6A and 6B, the local block database 326 and the local allow database 328 may be queried prior to contacting either the proxy server or the label server to determine if the requested network resource should be blocked or allowed. By checking these databases prior to contacting a label or proxy server, the client computer 300 can override the block and allow databases maintained at the label or proxy server. In this manner, a user of the client computer 300 can explicitly allow or block the retrieval of a network resource.

The storage device 314 also maintains an administrative control dynamically linked library ("DLL") 318. According to an embodiment of the invention, the administrative control DLL 318 intercepts requests for network resources before they are transmitted over the Internet. To accomplish this, the administrative control DLL 318 interfaces with Layered Service Provider 324 or through another socket interface as known to those skilled in the art. The administrative control DLL 318 may then cause a search to be made of the local block database 326 and the local allow database 328 for the requested network resource. If the requested network resource is identified in the local allow database 328, the administrative control DLL may transmit a request for the requested network resource through the layered service provider 324. If the requested network resource is identified in the local block

database 328, the administrative control DLL 318 may generate an error message to be displayed by the WWW browser application program 316. If the requested network resource is not identified in either the local block database 326 or the local allow database 328, the administrative control DLL 318 will make a request to a label server or a proxy server for the requested resource. The operation of such a request to a proxy server or a label server is described below with respect to FIGURES 6A and 6B, respectively. Those skilled in the art should appreciate that the administrative control DLL 318 may also utilize the configuration database 320 to identify the filtering level for the current user of the client computer 300. The administrative control DLL 318 may then use this information to determine whether the user of the client computer 300 is permitted to retrieve the requested network resource according to their assigned filtering level.

Those skilled in the art should appreciate that while the client computer 300 is described as a conventional personal computer, the invention described herein may be utilized in connection with other types of computing devices capable of receiving network content. For instance, the invention may be utilized to filter content delivered to a cellular phone, a personal digital assistant, a set-top box, or other similar computing devices known to those skilled in the art.

Referring now to FIGURE 4 a proxy server computer 400 utilized in an embodiment of the present invention will be described. Those of ordinary skill in the art will appreciate that the proxy server computer 400 includes many more components then those shown in FIGURE 4. However, it is not necessary that all of these generally conventional components be shown in order to disclose an illustrative embodiment for practicing the present invention. The proxy server computer 400 includes a network interface unit (not shown) for providing a communications connection 434 for connecting to the Internet or other type of distributed computing network. Those of ordinary skill in the art will appreciate that such a network interface unit includes the necessary circuitry for such a connection, and is also constructed for use with the TCP/IP protocol, the particular network configuration of the LAN or WAN it is connecting through, and a particular type of coupling medium.

The proxy server computer 400 also includes conventional components such as a ROM BIOS 410, central processing unit 402, and a system memory 404. The system memory 404 generally comprises a random access memory ("RAM") 406, a read-only memory ("ROM") 408 and a permanent mass storage device 414, such as a disk drive. The system memory 404 typically stores an operating system 416 for

controlling the operation of the proxy server computer 400, such as UNIX, Linux, or Windows NT or 2000 provided by Microsoft Corporation. The storage device 414 and system memory 304 also includes software components such as the proxy application program 418 and the database update application program 428. It will be appreciated that these components may be stored on a computer-readable medium and loaded into the system memory 404 of the proxy server computer 400 using a drive mechanism associated with the computer-readable medium, such as a floppy drive, CD-ROM/DVD-ROM drive, or hard disk drive. An input interface (not shown) may also be provided for receiving input from input devices 430, such as a mouse or keyboard. Likewise, an output interface (not shown) may also be provided for outputting information to the communications connection 434, a video display adapter, printers, and other output devices known to those skilled in the art. The system memory 404, communications connection 434, input devices 432, and output devices 430 are all connected to the central processing unit 402 via system bus 412. Other peripherals may also be connected to the central processing unit 402 in a similar manner.

The storage device 414 also maintains a block database 422 and an allow database 426. The block database 422 comprises the identity of network resources that a client computer is not permitted to retrieve. The allow database 426 comprises the identity of network resources that a client computer is explicitly permitted to retrieve. More particularly, the block database 422 may comprise an Internet Protocol address identifying one or more blocked network resources 436 or a URL identifying one or more blocked resources 420. Those skilled in the art should appreciate that a network resource may similarly be blocked based upon objectionable words contained within the URL or based upon other terms or parameters attached to or associated with a URL. Similarly, the allow database 426 may comprise an Internet Protocol address identifying one or more allowed network resources 438, or a URL identifying one or more allowed network resources 424.

As mentioned briefly above, the storage device 414 maintains a database update application program 428. The database update application program 428 is operative to periodically receive database updates to the block database 420 and the allow database 426 from a content monitoring center. The database updates may be periodically requested from the content monitoring center by the database update application 428, or may be "pushed" from the content monitoring center to the proxy server computer 400 as known to those skilled in the art.

As also mentioned briefly above, the storage device 414 maintains a proxy application program 418. The proxy application 418 receives requests for network resources from client computers. Based on these requests, the proxy application 418 searches the block database 422 and the allow database 426 to determine if the requesting client computer is permitted to retrieve the requested network resource. If the client computer is not permitted to retrieve the requested resource, an error message is returned to the client computer. If the client computer is permitted to retrieve the requested network resource, the proxy application 418 connects to a server computer hosting the requested network resource and retrieves the resource on behalf of the client computer. The proxy application 418 then provides the resource to the client computer. Operation of the proxy application program 418 is described in greater detail below with reference to FIGURE 7.

Referring now to FIGURE 5, a label server computer 500 utilized in an embodiment of the present invention will be described. Those of ordinary skill in the art will appreciate that the label server computer 500 includes many more components then those shown in FIGURE 5. However, it is not necessary that all of these generally conventional components be shown in order to disclose an illustrative embodiment for practicing the present invention. The label server computer 500 includes a network interface unit for providing a communications connection 532 for connecting to the Internet or other type of distributed computing network. Those of ordinary skill in the art will appreciate that such a network interface unit includes the necessary circuitry for such a connection, and is also constructed for use with the TCP/IP protocol, the particular network configuration of the LAN or WAN it is connecting through, and a particular type of coupling medium.

The label server computer 500 also includes conventional components such as a ROM BIOS 510, central processing unit 502, and a system memory 504. The system memory 504 generally comprises a random access memory ("RAM") 506, a read-only memory ("ROM") 508 and a permanent mass storage device 514, such as a disk drive. The system memory 504 typically stores an operating system 516 for controlling the operation of the proxy server computer 400, such as UNIX, Linux, or Windows NT or 2000 provided by Microsoft Corporation. The storage device 514 and system memory 504 also includes software components such as the label server application program 518 and the database update application program 526. It will be appreciated that these components may be stored on a computer-readable medium and loaded into the system memory 504 of the label server computer 500 using a

drive mechanism associated with the computer-readable medium, such as a floppy drive, CD-ROM/DVD-ROM drive, or hard disk drive. An input interface may also be provided for receiving input from input devices 530, such as a mouse or keyboard. Likewise, an output interface (not shown) may also be provided for outputting information to the communications connection 532, a video display adapter, printers, and other output devices known to those skilled in the art. The system memory 504, communications connection 532, input devices 530, and output devices 528 are all connected to the central processing unit 502 via system bus 512. Other peripherals may also be connected to the central processing unit 502 in a similar manner.

The storage device 514 also maintains a block database 518 and an allow database 522. The block database comprises the identity of network resources that a client computer is not permitted to retrieve. The allow database comprises the identity of network resources that a client computer is explicitly permitted to retrieve. More particularly, the block database 518 may comprise an Internet Protocol address identifying one or more blocked network resources 534 or a URL identifying one or more blocked resources 520. Similarly, the allow database 522 may comprise an Internet Protocol address identifying one or more allowed network resources 536, or a URL identifying one or more allowed network resources 524.

As mentioned briefly above, the storage device 514 maintains a database update application program 526. As with the proxy server, the database update application program 526 is operative to periodically receive database updates to the block database 518 and the allow database 522 from a content monitoring center. The database updates may be periodically requested from the content monitoring center by the database update application 526, or may be "pushed" from the content monitoring center to the label server computer 500 as known to those skilled in the art.

The storage device 514 also maintains a label server application program 517. The label server application 517 receives requests to validate network resources from client computers. Based on these requests, the label server application 517 searches the block database 518 and the allow database 522 for the requested network resource. The label server application 517 then provides the results of its search to the client computer. Operation of the label server application program 517 is described in greater detail below with reference to FIGURE 8.

Referring now to FIGURE 6A, an illustrative Routine 600 for the operation of a client computer utilizing a proxy server to filter network content will be described.

Routine 600 begins at block 602, where a request is received at the client computer for a network resource. Typically, the request will take the form of an HTTP address provided at the client computer by a user. From block 602, Routine 600 continues to block 604 where a search of the block and allow databases located at the client computer is performed. As described above, the block and allow databases located at the client computer may be updated by a user of the client computer and allow the user to override the block and allow databases located at the proxy server.

From block 604, Routine 600 continues to block 606, where a determination is made as to whether the client computer is explicitly allowed to retrieve the requested network resource. In particular, if the URL or the IP address of the requested network resource is identified in the allow database, then the client computer is explicitly permitted to retrieve the requested resource. If it is determined that the client computer is allowed to retrieve the requested network resource, the Routine 600 branches to block 608, where the client computer connects directly to the server computer hosting the requested resource and retrieves the requested resource. The requested resource may then be displayed by the client computer.

If, at block 606, it is determined that the client computer is not explicitly allowed to retrieve the requested network resource, Routine 600 continues to block 610. A determination is made at block 610 as to whether the client computer is explicitly blocked from retrieving the requested network resource. In particular, a determination is made as to whether the URL or IP address of the requested network resource is identified in the block database located at the client computer. If the requested network resource is identified in the block database, the Routine 600 branches to block 616, where an error message is displayed at the client computer. The Routine 600 then continues from block 616 to block 602. If the requested network resource is not identified in the block database, the Routine 600 continues to block 612.

At block 612, the client computer transmits a request for the network resource to a proxy server computer. The format of the request may comprise an HTTP packet including the IP address of the client computer and the URL and IP address of the requested network resource. As described below with respect to FIGURE 7, the proxy server computer is operative to receive the request from the client computer and to determine whether the client computer may retrieve the requested network resource. The proxy server computer then transmits a response to the client computer indicating whether or not the client computer may retrieve the requested

network resource. Accordingly, Routine 600 continues from block 612 to block 614, where a determination is made as to whether the proxy server computer has permitted the client computer to retrieve the requested resource. If the proxy server computer does not permit the client computer to retrieve the requested resource, Routine 600 branches to block 616, where an error message is displayed at the client computer.

If, at block 614, it is determined the proxy server computer has permitted the client computer to retrieve the requested resource, Routine 600 continues to block 618. At block 618, the requested network resource is retrieved through the proxy server and the network resource is displayed at the client computer. Routine 600 then continues from block 618 to block 602, where another request to retrieve a network resource may be processed.

Referring now to FIGURE 6B, an illustrative Routine 650 for the operation of a client computer utilizing a label server to filter network content will be described. Routine 650 begins at block 652, where a request is received at the client computer for a network resource. As described above, the request typically takes the form of an HTTP address provided at the client computer by a user but may take another form known to those skilled in the art. From block 652, Routine 650 continues to block 654 where a search of the block and allow databases located at the client computer is performed. Those skilled in the art should appreciate that the label server may be utilized to filter network content without the use of the block and allow databases located at the client computer.

From block 654, Routine 650 continues to block 656, where a determination is made as to whether the client computer is explicitly allowed to retrieve the requested network resource. As described above, if the URL or IP address of the requested network resource is identified in the allow database, then the client computer is explicitly permitted to retrieve the requested resource. If it is determined that the client computer is allowed to retrieve the requested network resource, the Routine 650 branches to block 658, where the client computer connects directly to the server computer hosting the requested resource and retrieves the requested resource. The requested resource may then be displayed at the client computer.

If, at block 656, it is determined that the client computer is not explicitly allowed to retrieve the requested network resource, Routine 650 continues to block 660. A determination is made at block 660 as to whether the client computer is explicitly blocked from retrieving the requested network resource. If the requested network resource is identified in the block database, the Routine 650 branches to

block 668, where an error message is displayed at the client computer. The Routine 650 then continues from block 668 to block 652. If the requested network resource is not identified in the block database, the Routine 650 continues to block 662.

At block 662, the client computer transmits a request to validate the network resource to a label server computer. As with the proxy server, the format of the request may comprise an HTTP packet including the IP address of the client computer and the URL and IP address of the requested network resource. As described in more detail below with respect to FIGURE 8, the label server computer is operative to receive the request from the client computer, and to search a block and allow database located at the label server computer. The label server computer then transmits a response to the client computer in the form of search results indicating whether or not the requested network resource was identified in its block or allow databases. Therefore, Routine 650 continues from block 662 to block 664, where the client computer receives the search results produced by the label server computer.

From block 664, the Routine 600 continues to block 666, where a determination is made as to whether the search results received from the label server computer indicate that the client computer is allowed to retrieve the requested network resource. If the requested network resource was identified in the allow database located at the label server, or was not identified in the block database located at the label server, the client computer will be permitted to retrieve the requested network resource. If the client computer is not permitted retrieve the requested resource, Routine 650 branches to block 668, where an error message is displayed at the client computer. If, at block 666, it is determined that the client computer may retrieve the requested resource, Routine 650 continues to block 670. At block 670, the requested network resource is retrieved by the client computer directly from the server computer hosting the requested network resource. The client computer does not utilize the label server to retrieve the requested network resource. From block 670, Routine 600 continues to block 652, where another request to retrieve a network resource may be processed in a similar manner.

Referring now to FIGURE 7, an illustrative Routine 700 for filtering network content at a proxy server will be described. Routine 700 begins at block 702, where a request for a network resource is received at from a client computer. As described above with respect to FIGURE 5 and 6, the request comprises an HTTP packet including the IP address of the client computer and the URL or IP address of the requested network resource. From block 702, the Routine 700 continues to block

704, where the block and allow data bases are searched for the URL or IP address of the requested network resource. Methods for searching a database are well known to those skilled in the art.

From block 704, Routine 700 continues to block 706, where a determination is made as to whether the requested network resource is blocked. The network resource will be blocked if the URL or IP address of the requested network resource is identified in the block database and are not identified in the allow database. If the URL or IP address of the requested network resource is not identified in either database, access to the network resource will be permitted. If, at block 706, it is determined that the URL or IP address of the requested network resource is blocked, the Routine 700 branches to block 708 where an error message is returned to the client computer from the proxy server computer. The Routine 700 then returns to block 702, where additional requests may be received by the proxy server computer and processed in a similar fashion.

If, at block 706, it is determined that the URL or IP address of the requested network resource is not blocked, Routine 700 will continue to block 710. At block 710, the proxy server computer connects to the server computer hosting the requested network resource on behalf of the client computer. Routine 700 then continues to block 712 where the requested network resource is retrieved by the proxy server computer. At block 714, a script file may be inserted into the requested network resource. According to an actual embodiment of the invention, a script written in JavaScript from Sun Microsystems is inserted into the URL. The script causes the Web browser executing on the client computer to display a banner associated with a provider of the filtering system. Those skilled in the art should appreciate that such a script may be utilized to display other information or provide other types of functionality.

From block 714, Routine 700 continues to block 716 where the requested network resource is returned to the client computer. The client computer may then display the requested network resource utilizing a Web browser or may utilize the requested network resource for another purpose. The Routine 700 then continues from block 716 to block 702, where another request for a network resource is received and processed in a similar fashion.

Turning now to FIGURE 8, an illustrative Routine 800 for filtering network content utilizing a label server will be described. Routine 800 begins at block 802, where a request is received to validate a URL or IP address from the client computer.

Typically, the request will comprise the URL or IP address corresponding to the requested URL and the IP address of the client computer. Routine 800 then continues from block 802 to block 804, where the label server computer searches its block and allow databases for the specified URL or IP address. From block 804, the Routine 800 continues to block 806, where the results of the search are returned to the client computer. The routine 800 then continues to block 808, where it ends.

In light of the above, it should be appreciated by those skilled in the art that the present invention provides a method, system, computer-controlled apparatus, and computer-readable medium for filtering network content. While an actual embodiment of the invention has been illustrated and described, it will be appreciated that various changes can be made therein without departing from the spirit and scope of the invention.

The embodiments of the invention in which an exclusive property or privilege is claimed are defined as follows:

1. A method for filtering network content comprising:

receiving a request for a network resource at a client computer;

in response to the request, searching the database located at the client computer to determine if the client computer is blocked from receiving the network resource;

transmitting a request to retrieve the requested network resource to a proxy server in response to determining that the requested network resource is not blocked;

determining whether the proxy server permits the client computer to retrieve the requested network resource; and

in response to determining that the proxy server permits the client computer to retrieve the requested network resource, retrieving the requested network resource through the proxy server.

2. The method of Claim 1, further comprising:

searching a database located at the client computer in response to the request for a network resource to determine if the client computer is explicitly allowed to retrieve the network resource; and

in response to determining that the client computer is allowed to retrieve the network resource, retrieving the network resource at the client computer without utilizing the proxy server.

3. The method of Claim 2, further comprising:

in response to determining that the client computer is blocked from retrieving the network resource, not permitting the client computer to retrieve the network resource and displaying an error message at the client computer.

4. The method of Claim 3, wherein the network resource comprises a file created in a standard page markup language.

5. The method of Claim 4, wherein the database located at the client computer comprises a network address or a uniform resource locator corresponding to a network resource that the client computer is blocked from retrieving.

6. The method of Claim 5, wherein the database located at the client computer further comprises a network address or a uniform resource locator corresponding to at least one network resource that the client computer may retrieve.

7. A computer-readable medium comprising instructions which, when executed by a computer, cause the computer to perform the method of Claims 1,2,3,4,5, or 6.

8. A method for filtering network content comprising:

receiving a request for a network resource at a client computer;

in response to the request, searching a database located at the client computer to determine if the client computer is blocked from retrieving the network resource;

transmitting a request to a label server to retrieve the requested network resource in response to determining that the requested network resource is not blocked;

receiving search results from the label server in response to the request;

determining whether the search results indicate that the client computer may retrieve the network resource; and

in response to determining that the client computer may retrieve the requested network resource, retrieving the requested network resource from a server computer hosting the requested resource.

9. The method of Claim 8, further comprising:

searching a database located at the client computer in response to the request for a network resource to determine if the client computer is explicitly allowed to retrieve the network resource; and

in response to determining that the client computer is allowed to retrieve the network resource, retrieving the network resource at the client computer without contacting the label server.

10. The method of Claim 9, further comprising:

in response to determining that the client computer is blocked from retrieving the network resource, not permitting the client computer to retrieve the network resource and displaying an error message at the client computer.

11. The method of Claim 10, wherein the network resource comprises a file created in a standard page markup language.

12. The method of Claim 11, wherein the database located at the client computer comprises a network address or a uniform resource locator for at least one network resource that the client computer is allowed to retrieve.

13. The method of Claim 12, wherein the database located at the client computer further comprises a network address or a uniform resource locator for at least one network resource that the client computer is allowed to retrieve.

14. A computer-readable medium comprising instructions which, when executed by a computer, cause the computer to perform the method of Claims 8,9,10,11,12, or 13.

15. A method for filtering network content comprising:

receiving a request from a client computer for a network resource at a proxy server;

in response to the request, searching a database located at the proxy server to determine if the client computer is blocked from retrieving the requested network resource;

connecting to a server computer hosting the requested network resource and retrieving the requested network resource in response to determining that the client computer is not blocked from retrieving the network resource; and

returning the network resource to the client computer.

16. A method of Claim 15, further comprising:

inserting a script into the requested network resource to create a modified network resource.

17. The method of Claim 15, further comprising:

searching a database located at the proxy server to determine if the client computer is explicitly allowed to retrieve the requested network resource; and

in response to determining that the client computer is allowed to retrieve the network resource;

retrieving the network resource on behalf of the client computer, and transmitting the network resource to the client computer.

18. The method of Claim 17, further comprising:

in response to determining that the client computer is blocked from retrieving the requested network resource, returning an error message to the client computer.

19. The method of Claim 18, wherein the network resource comprises a file created in a standard page markup language.

20. The method of Claim 19, wherein the database located at the proxy server comprises a network address or a uniform resource locator for a network resource that the client computer is blocked from retrieving.

21. The method of Claim 20, wherein the database located at the proxy server further comprises a network address or a uniform resource locator for at least one network resource that the client computer is allowed to retrieve.

22. The method of Claim 20, wherein the database located at the proxy server is updated from a content monitoring center.

23. A computer-readable medium comprising instructions which, when executed by a computer, cause the computer to perform the method of Claims 15,16,17,18,19,20,21 or 22.

24. A method for filtering network content comprising:

receiving a request from a client computer to validate a network resource at a label server;

in response to the request, searching a database located at the label server to determine if the requested network resource is identified in a list of blocked network resources; and

returning the results of searching the database to the client computer.

25. The method of Claim 24, further comprising:

searching a database located at the label server to determine if the requested network resource is identified in a list of allowable network resources.

26. The method of Claim 25, wherein the network resource comprises a file created in a standard page markup language.

27. The method of Claim 26, wherein the database located at the label server comprises a network address or a uniform resource locator for a network resource that the client computer is blocked from retrieving.

28. The method of Claim 27, wherein the database located at the label server comprises a network address or a uniform resource locator for at least one network resource that the client computer is allowed to retrieve.

29. The method of Claim 27, wherein the database is updated from a content monitoring center.

30. A computer-controlled apparatus capable of performing the method of Claims 1, 8, 15, or 24.

31. A system for filtering network content comprising:

a proxy server,

a client computer capable of connecting to the proxy server via a distributed computing network,

and a network resource available on the distributed computing network, and wherein the client computer is operative to:

receive a request for the network resource,

search a database located at the client computer to determine if the client computer is blocked from retrieving the network resource,

transmit a request to the proxy server to retrieve the network resource, and

in response to receiving authorization from the proxy server, retrieve the network resource through the proxy server.

32. The system of Claim 31, wherein the client computer is further operative to:

search a database located at the client computer to determine if the client computer is allowed to retrieve the network resource; and

in response to determining that the client computer is allowed to retrieve the network resource, retrieving the network resource at the client computer without utilizing the proxy server.

33. The system of Claim 31, wherein the proxy server is operative to:

receive a request from the client computer for the network resource;

in response to the request, searching a database located at the proxy server to determine if the client computer is blocked from retrieving the requested network resource;

connecting the proxy server to a server computer hosting the requested network resource to retrieve the network resource in response to determining that the network resource is not blocked; and

transmitting the network resource to the client computer.

34. The system of Claim 33, wherein the proxy server is further operative to:

search a database located at the proxy server to determine if the client computer is explicitly allowed to retrieve the requested network resource.

35. The system of Claim 34, wherein the proxy server is further operative to:

receive an update to the database located at the proxy server from a content monitoring center.

36. A system for filtering network content comprising:

a label server,

a client computer capable of connecting to the label server via a distributed computing network,

and a network resource available on the distributed computing network, and wherein the client computer is operative to:

receive a request for the network resource;

search a database located at the client computer to determine if the client computer is blocked from retrieving the network resource;

in response to determining that the client computer is not blocked from retrieving the network resource, transmitting a request to the label server to retrieve the network resource;

receive search results from the label server;

determine whether the search results permit the client computer to retrieve the network resource; and

in response to determining that the search results permit the client computer to retrieve the network resource, retrieving the network resource.

37. The system of Claim 36, wherein the client computer is further operative to:

search a database located at the client computer to determine if the client computer is allowed to retrieve the network resource; and

in response to determining that the client computer is allowed to retrieve the network resource, retrieving the network resource at the client computer without contacting the label server.

38. The system of Claim 36, wherein the label server is operative to:

receive a request from a client computer to validate a network resource;

in response to the request, searching a database located at the label server to determine if the client computer is blocked from retrieving the requested network resource; and

returning the search results to the client computer.

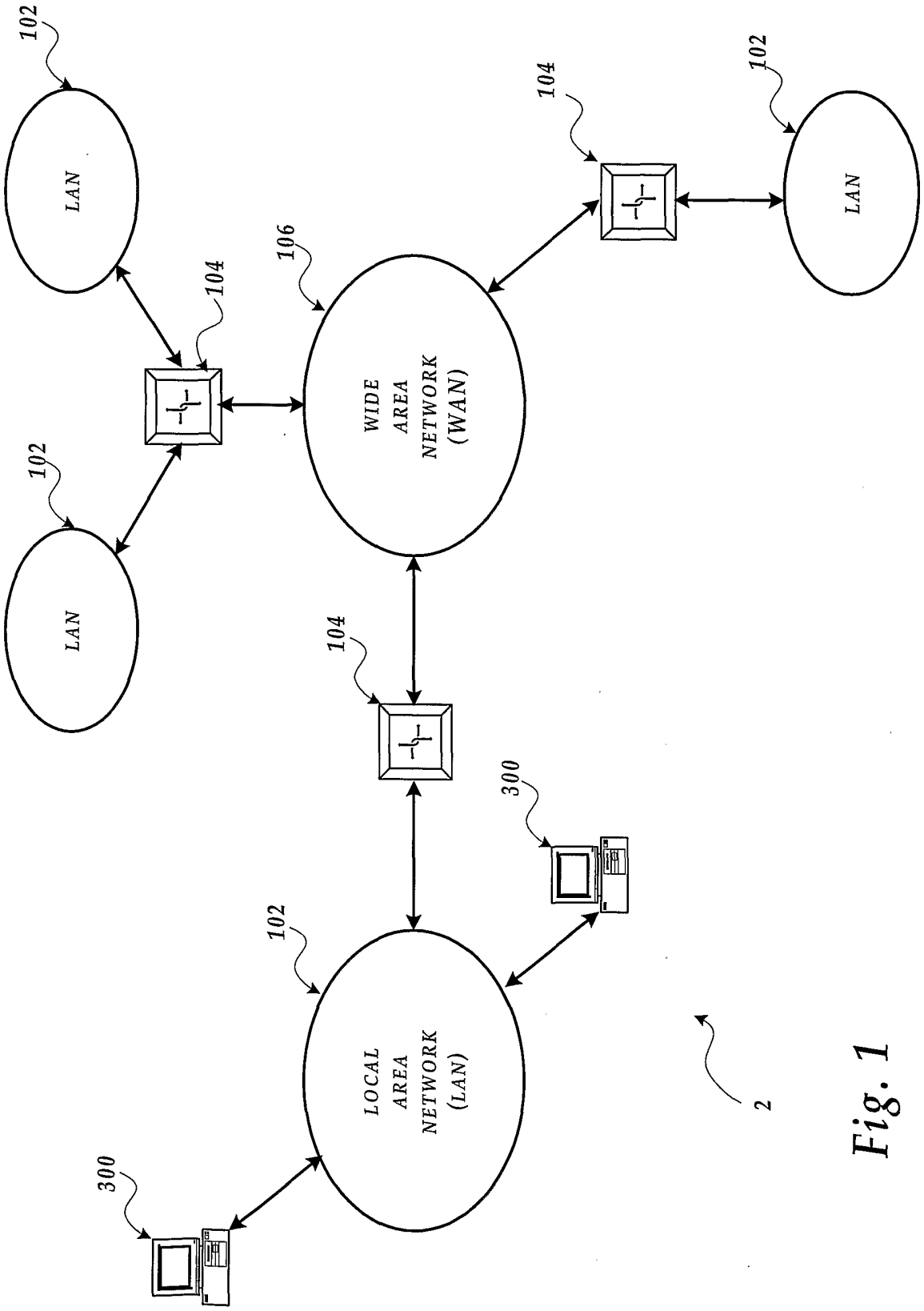

102
LAN
104
106
WIDE AREA NETWORK (WAN)
102
LAN
104
102
LAN
104
300
102
LOCAL AREA NETWORK (LAN)
300
2

Fig. 1

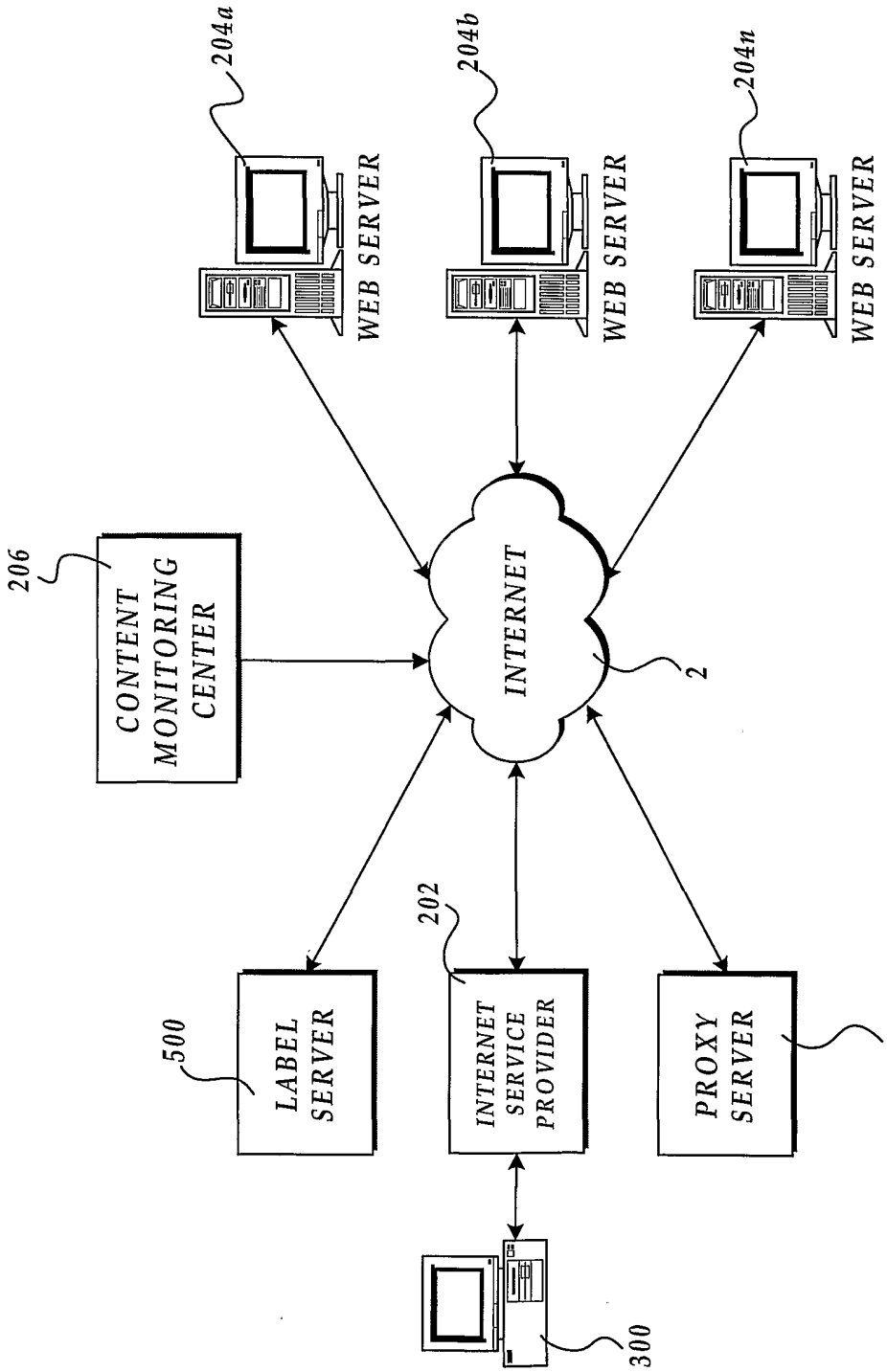

204a
WEB SERVER
204b
WEB SERVER
204n
WEB SERVER
206
CONTENT MONITORING CENTER
INTERNET
2
202
500
LABEL SERVER
INTERNET SERVICE PROVIDER
PROXY SERVER
400
300

Fig.2

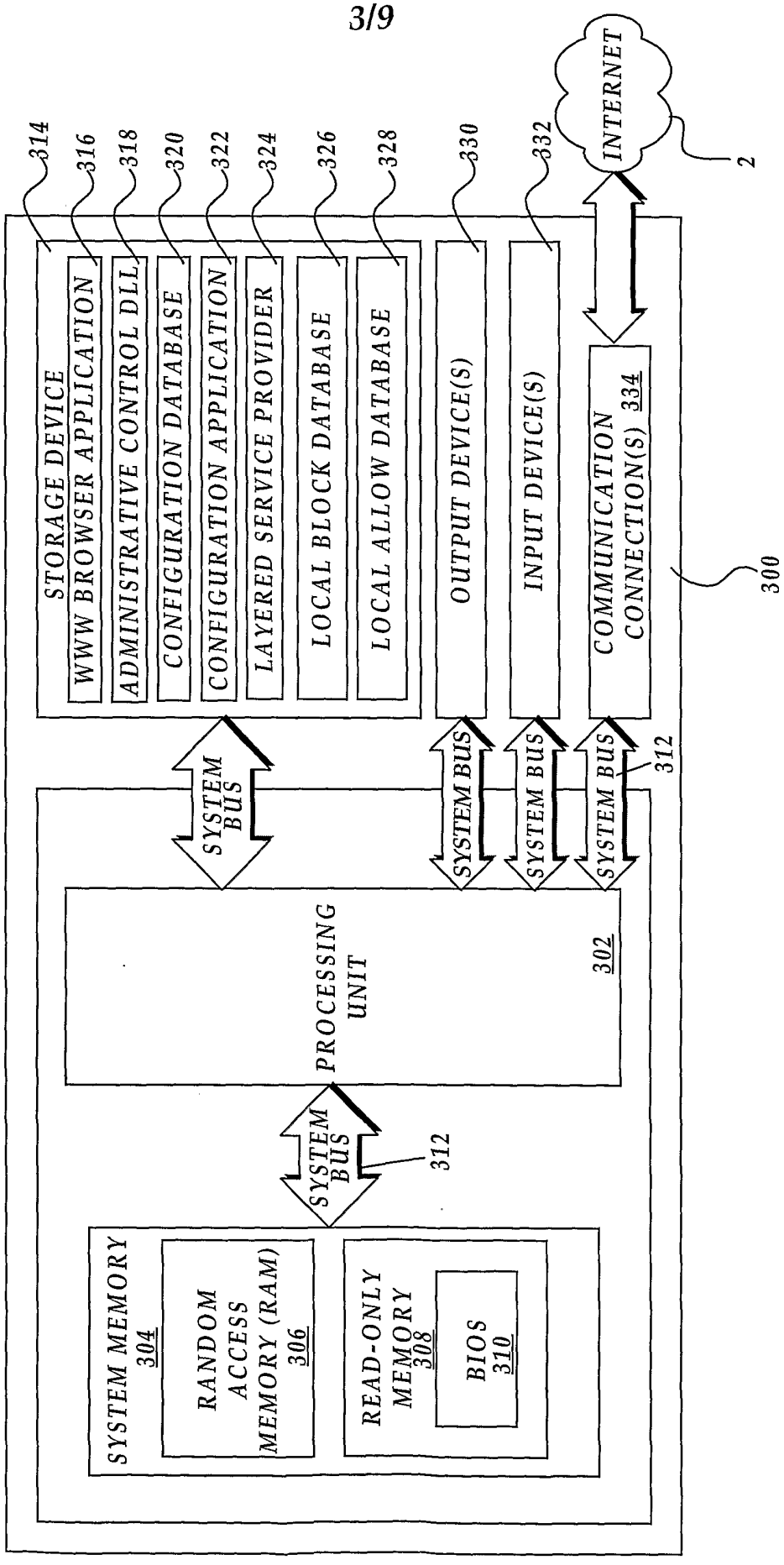

INTERNET
2
314
316
318
320
322
324
326
328
330
332
STORAGE DEVICE
WWW BROWSER APPLICATION
ADMINISTRATIVE CONTROL DLL
CONFIGURATION DATABASE
CONFIGURATION APPLICATION
LAYERED SERVICE PROVIDER
LOCAL BLOCK DATABASE
LOCAL ALLOW DATABASE
OUTPUT DEVICE(S)
INPUT DEVICE(S)
COMMUNICATION CONNECTION(S) 334
300
SYSTEM BUS
SYSTEM BUS
SYSTEM BUS
SYSTEM BUS
312
312
PROCESSING UNIT
302
SYSTEM MEMORY 304
RANDOM ACCESS MEMORY (RAM) 306
READ-ONLY MEMORY 308
BIOS 310

Fig.3

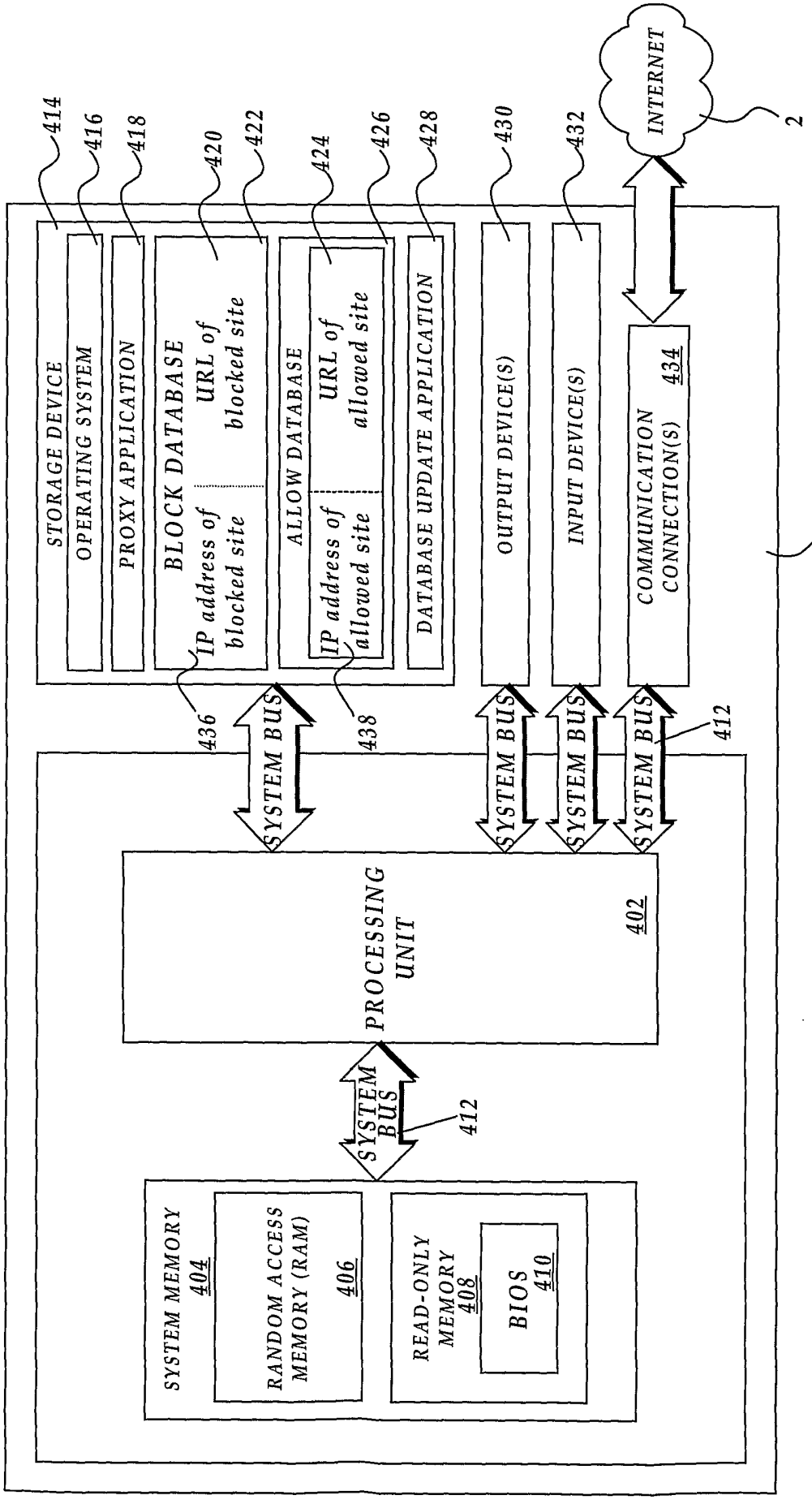

INTERNET
2
414
416
418
420
422
424
426
428
430
432
STORAGE DEVICE
OPERATING SYSTEM
PROXY APPLICATION
BLOCK DATABASE
IP address of blocked site
URL of blocked site
ALLOW DATABASE
IP address of allowed site
URL of allowed site
DATABASE UPDATE APPLICATION
OUTPUT DEVICE(S)
INPUT DEVICE(S)
COMMUNICATION CONNECTION(S) 434
400
436
438
412
SYSTEM BUS
PROCESSING UNIT
402
SYSTEM MEMORY 404
RANDOM ACCESS MEMORY (RAM) 406
READ-ONLY MEMORY 408
BIOS 410

Fig.4

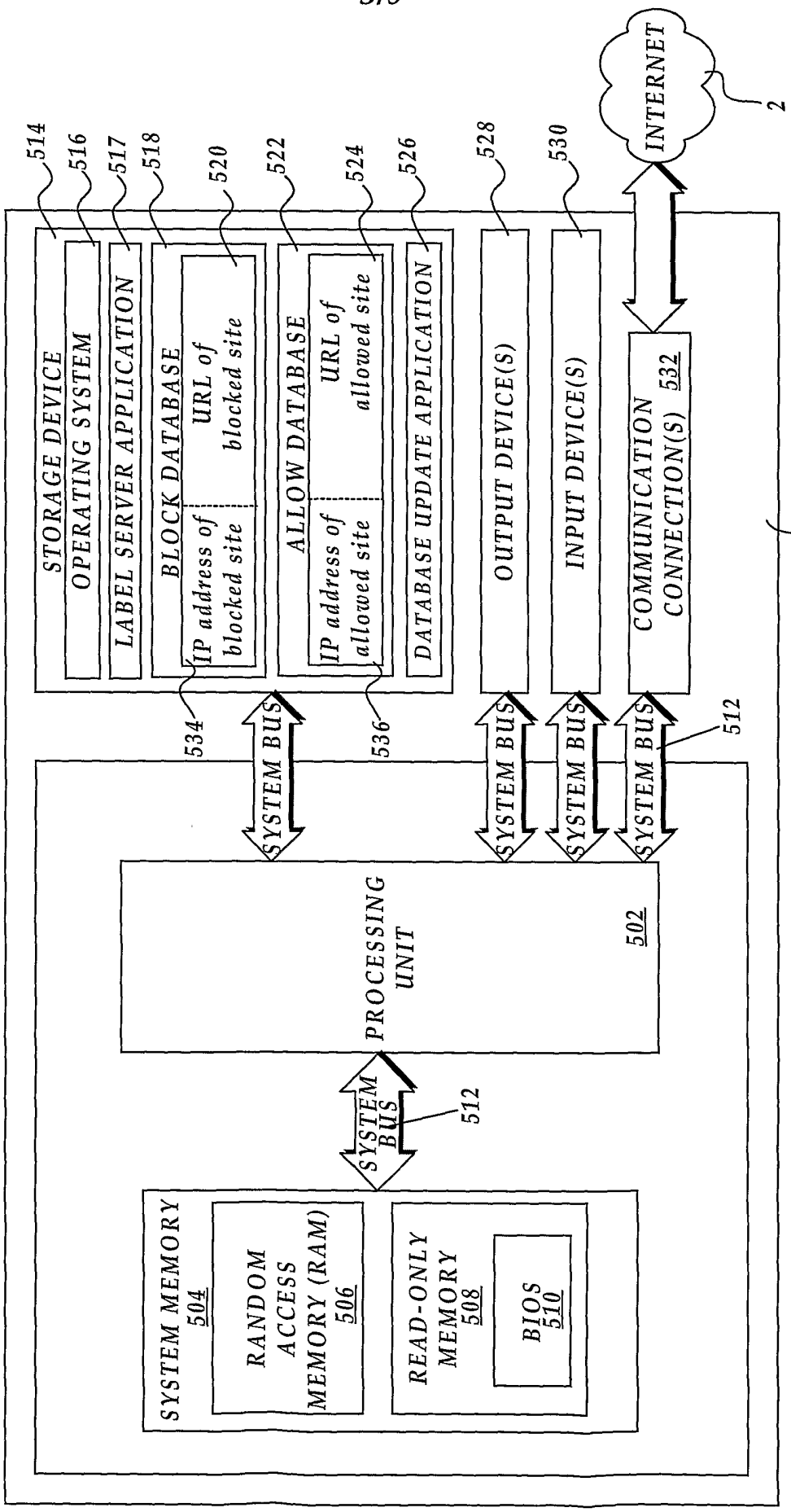

INTERNET
2
514
516
517
518
520
522
524
526
528
530
STORAGE DEVICE
OPERATING SYSTEM
LABEL SERVER APPLICATION
BLOCK DATABASE
IP address of blocked site
URL of blocked site
ALLOW DATABASE
IP address of allowed site
URL of allowed site
DATABASE UPDATE APPLICATION
OUTPUT DEVICE(S)
INPUT DEVICE(S)
COMMUNICATION CONNECTION(S) 532
500
534
536
512
SYSTEM BUS
PROCESSING UNIT
502
SYSTEM MEMORY 504
RANDOM ACCESS MEMORY (RAM) 506
READ-ONLY MEMORY 508
BIOS 510

Fig.5

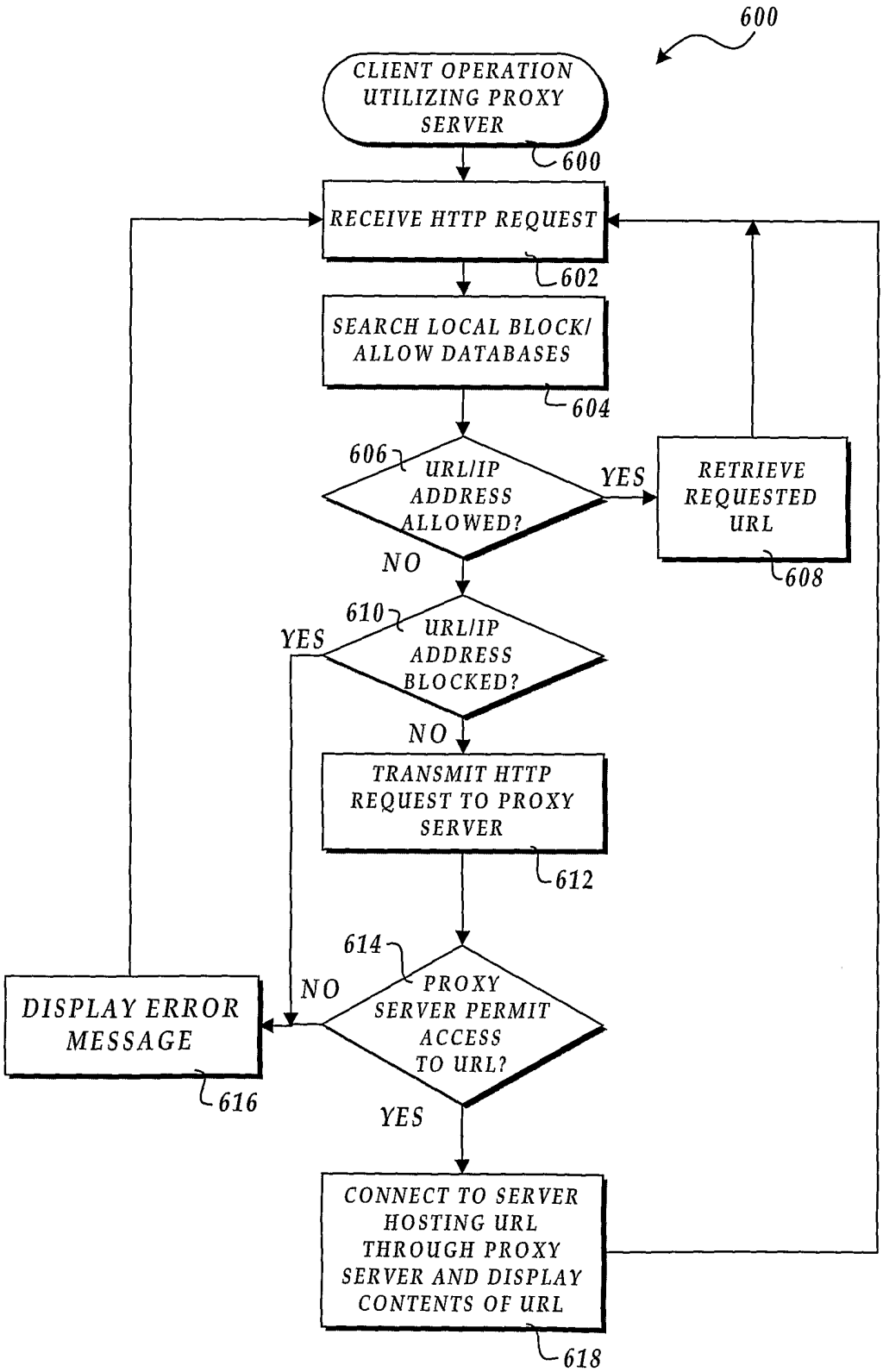

600
CLIENT OPERATION UTILIZING PROXY SERVER
600
RECEIVE HTTP REQUEST
602
SEARCH LOCAL BLOCK/ ALLOW DATABASES
604
606
URL/IP ADDRESS ALLOWED?
YES
RETRIEVE REQUESTED URL
608
NO
610
URL/IP ADDRESS BLOCKED?
YES
NO
TRANSMIT HTTP REQUEST TO PROXY SERVER
612
614
PROXY SERVER PERMIT ACCESS TO URL?
NO
DISPLAY ERROR MESSAGE
616
YES
CONNECT TO SERVER HOSTING URL THROUGH PROXY SERVER AND DISPLAY CONTENTS OF URL
618

Fig.6A

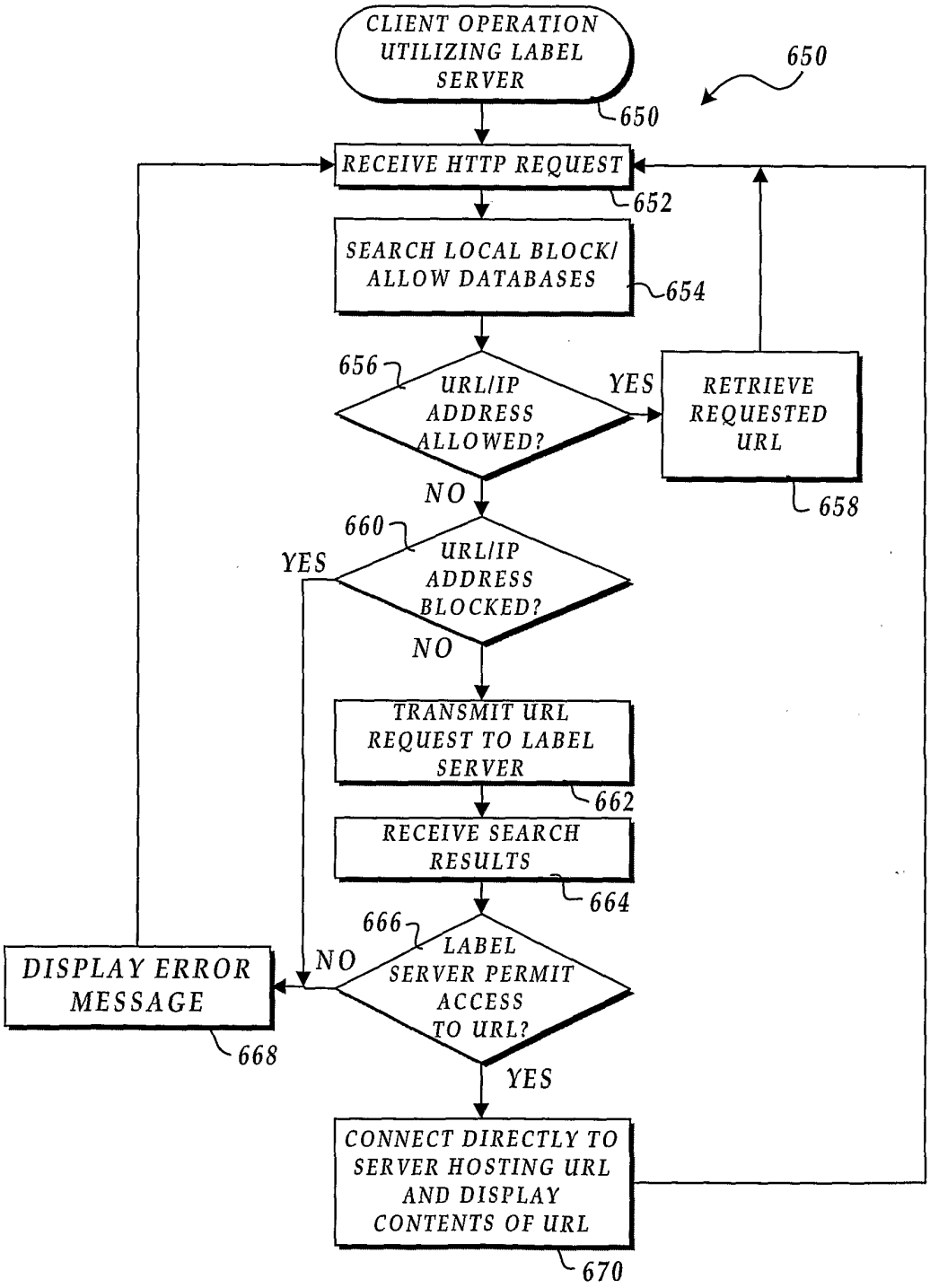

CLIENT OPERATION UTILIZING LABEL SERVER
650
650
RECEIVE HTTP REQUEST
652
SEARCH LOCAL BLOCK/ ALLOW DATABASES
654
656
URL/IP ADDRESS ALLOWED?
YES
RETRIEVE REQUESTED URL
658
NO
660
URL/IP ADDRESS BLOCKED?
YES
NO
TRANSMIT URL REQUEST TO LABEL SERVER
662
RECEIVE SEARCH RESULTS
664
666
LABEL SERVER PERMIT ACCESS TO URL?
NO
DISPLAY ERROR MESSAGE
668
YES
CONNECT DIRECTLY TO SERVER HOSTING URL AND DISPLAY CONTENTS OF URL
670

Fig.6B

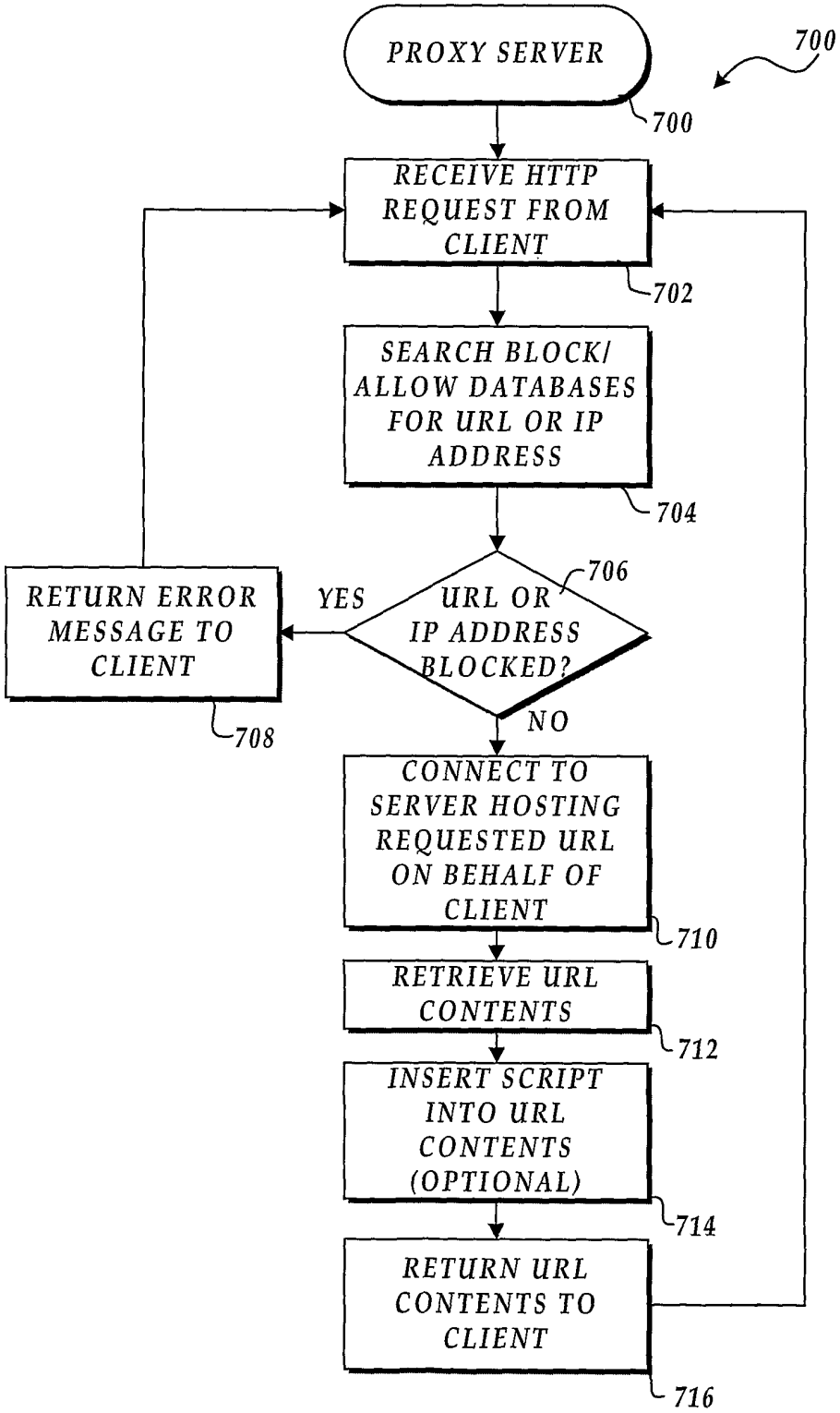

PROXY SERVER
700
700
RECEIVE HTTP REQUEST FROM CLIENT
702
SEARCH BLOCK/ ALLOW DATABASES FOR URL OR IP ADDRESS
704
706
URL OR IP ADDRESS BLOCKED?
YES
RETURN ERROR MESSAGE TO CLIENT
708
NO
CONNECT TO SERVER HOSTING REQUESTED URL ON BEHALF OF CLIENT
710
RETRIEVE URL CONTENTS
712
INSERT SCRIPT INTO URL CONTENTS (OPTIONAL)
714
RETURN URL CONTENTS TO CLIENT
716

Fig.7

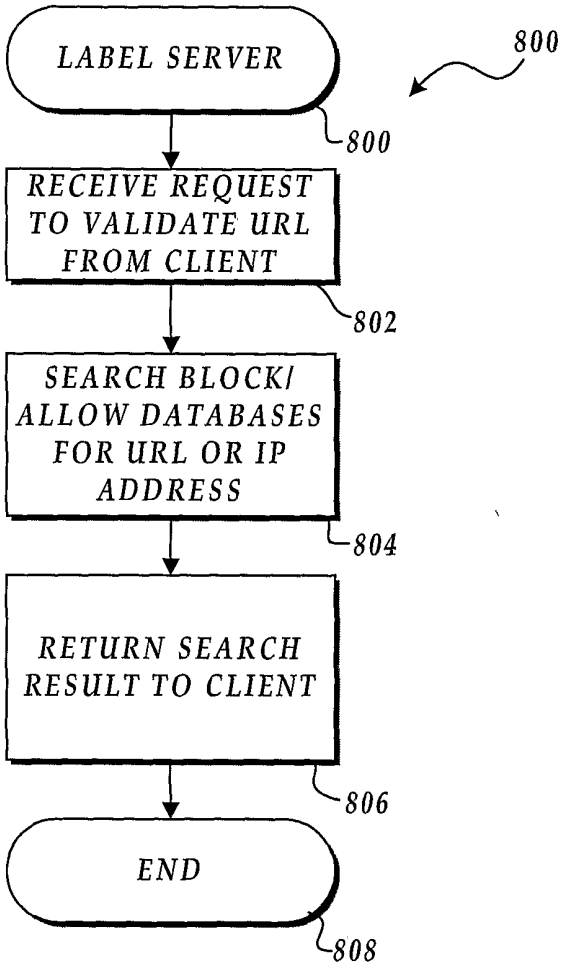

LABEL SERVER
800
800
RECEIVE REQUEST TO VALIDATE URL FROM CLIENT
802
SEARCH BLOCK/ ALLOW DATABASES FOR URL OR IP ADDRESS
804
RETURN SEARCH RESULT TO CLIENT
806
END
808

Fig.8

INTERNATIONAL SEARCH REPORT

Interr ıal Application No
PCT/US 00/32925

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F17/30

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)
IPC 7 G06F H04L

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 practical, search terms used)

EPO-Internal, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 884 033 A (KENDALL MATTHEW ET AL) 16 March 1999 (1999-03-16)	1-7, 15-23, 31-35
Y	column 1, line 31 -column 1, line 64 column 3, line 64 -column 4, line 64 column 7, line 16 -column 8, line 38 figure 1	8-14, 24-30, 36-38

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 January 2001	01/02/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Abbing, R

INTERNATIONAL SEARCH REPORT

Interr al Application No
PCT/US 00/32925

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98 41913 A (DEROSA ROBERT ;CIRASOLE PETER (US); FOX ROBERT (US); BASCOM GLOBAL) 24 September 1998 (1998-09-24)	1-7, 15-23, 31-35
Y		8-14, 24-30, 36-38
	page 3, line 8 -page 7, line 11 figures 4-8 page 10, line 9 -page 10, line 25 page 14, line 16 -page 17, line 3 ---	
X	US 5 706 507 A (SCHLOSS ROBERT JEFFREY) 6 January 1998 (1998-01-06)	8-14, 24-30, 36-38
A		1-7, 15-23, 31-35
	abstract column 4, line 57 -column 6, line 11 ---	
A	EP 0 748 095 A (AT & T CORP) 11 December 1996 (1996-12-11) the whole document ---	1-38
A	US 5 991 810 A (SUBRAMANIAM ANAND ET AL) 23 November 1999 (1999-11-23) abstract -----	1,15,31

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter ial Application No
PCT/US 00/32925

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5884033 A	16-03-1999	NONE	
WO 9841913 A	24-09-1998	US 5987606 A	16-11-1999
		AU 6564898 A	12-10-1998
US 5706507 A	06-01-1998	NONE	
EP 0748095 A	11-12-1996	US 5678041 A	14-10-1997
		CA 2176775 A	07-12-1996
		CN 1145489 A	19-03-1997
		JP 9026975 A	28-01-1997
US 5991810 A	23-11-1999	NONE	