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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 May 2009 (07.05.2009)

PCT

(10) International Publication Number
WO 2009/058668 A1

(51) International Patent Classification:
G06F 7/00 (2006.01)

(21) International Application Number:
PCT/US2008/081019

(22) International Filing Date: 23 October 2008 (23.10.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/982,495 2 November 2007 (02.11.2007) US

(71) Applicant *(for all designated States except US)*: **PAGLO LABS INC.** [US/US]; 1804 Embarcadero Road, Suite 201, Palo Alto, CA 94303 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **WATERS, Christopher** [NZ/US]; 609 Arboleda Drive, Los Altos, CA 94024 (US). **DE HAAFF, Brian** [US/US]; 20 Gloria Circle, Menlo Park, CA 94025 (US). **LOCKHART, Andrew** [US/US]; 359 Knobcone Drive, #204, Loveland, CO 80538 (US).

(74) Agents: **VINCENT, Lester, J.** et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 1279 Oakmead Parkway, Sunnyvale, CA 94085-4040 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(54) **Title:** HOSTED SEARCHING OF PRIVATE LOCAL AREA NETWORK INFORMATION WITH SUPPORT FOR ADD-ON APPLICATIONS

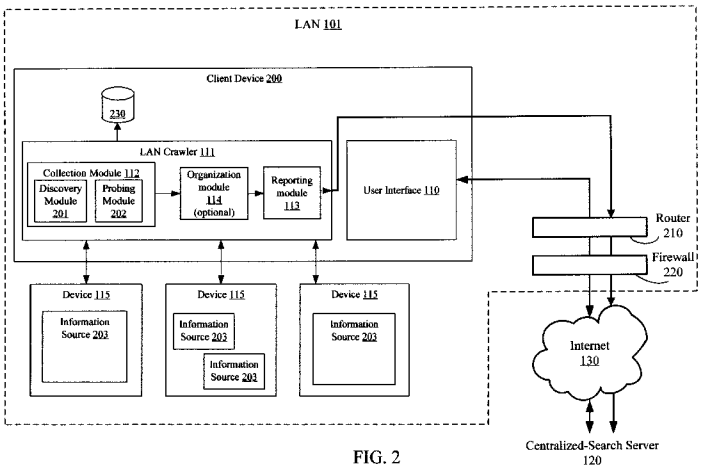


FIG. 2

(57) **Abstract:** Hosted searching of private LAN information is described. The apparatus includes a LAN crawler to automatically and repeatedly crawl a LAN having multiple devices, using a discovery module to discover the devices, a generic- probing module to attempt to collect the descriptive information according to a first set of probing requirements, and multiple specific-probing plug-ins each of which attempt to collect the descriptive information according to a second set of specific probing requirements. In another embodiment, the apparatus also includes a hosted on-demand search system including a centralized- search server to create and synchronize a private search database. The centralized-search server includes an application interface to receive a request to access the private search database from a third-party add-on application, to provide the accessed information to the third-party add-on application, and to receive from the third-party add-on application an application rendered component to be displayed on the user interface.

WO 2009/058668 A1

HOSTED SEARCHING OF PRIVATE LOCAL AREA NETWORK INFORMATION WITH SUPPORT FOR ADD-ON APPLICATIONS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] Not Applicable.

BACKGROUND

Field

[0002] Embodiments of the invention relate to the field of hosted searching; and more specifically, to the hosted searching of private local area network (LAN) information.

Background

[0003] One method of searching is performed over the World Wide Web (WWW). This type of searching is commonly referred to as web searching and is normally performed by a search engine. The term search engine is used to refer to an information retrieval system designed to help find information stored on a computer system. Search engines help to minimize the time required to find information and the amount of information which is subsequently consulted. One type of conventional search engines are Web search engines that search for information on the public WWW. Other types of conventional search engines may include enterprise search engines that search on private intranets, personal search engines, and mobile search engines. Typically, search engines provide an interface to enable users to specify criteria about an item of interest and have the engine find the matching items within the stored information. The items of interest of interest are typically documents and the criteria are the words or concepts that the document may contain. A document, as used herein, is a bounded physical representation of a body of information designed with the capacity to communicate information. Documents may be digital files in various formats, including web pages, word processing documents, images, or the like.

[0004] One prior art technique of Web search engine is to use a Web crawler. A web crawler, also known as a web spider, web robot or web bot, is a program or automated script which browses the WWW in a methodical, automated manner.

This process is called web crawling or spidering. Many search engines uses spidering as a means of providing up-to-date data. Web crawlers are mainly used to create a copy of all the visited pages for later processing by the search engine that will index the downloaded pages to provide fast searches. A web crawler typically starts with a list of Uniform Resource Locator (URL), and upon visiting these URLs, the web crawler identifies all hyperlinks in the page and adds them to the list of URLs to visit. These URLs can be recursively visited according to a set of policies. By indexing collected documents, or metadata about the documents, the search engine can provide a set of matching items quickly. For example, a library search engine may determine the author of each book automatically and add the author name to a description of each book. Users can then search for books by the author's name. The metadata collected about each item (e.g., document) is typically stored in the form of an index. The index provides a way for the search engine to calculate the relevance, or similarity, between the search query and the set of items.

[0005] A limitation of this prior art method is that the collected information is a copy of the entire document, and the index is organized according to the collected documents, such as by the metadata that corresponds to the document. As a result, this prior art method has the disadvantages of processing the entire collected documents, such as to extract or generate metadata related to the collected documents, and organizing the document information (e.g., metadata) according to documents, not according to the items of interest.

[0006] Another prior art technique of a personal search engine is to use a desktop search tool. A desktop search tool is a tool that searches the contents of a user's own computer files, rather than searching other computers, or searching the Internet. These tools are designed to find information about documents on the user's computer, including web browser histories, e-mail archives, text documents, audio files, images, video, or the like. The search index for the desktop search tool resides on the user's computer. The search index is also organized according to the documents, not according to the items of interest.

[0007] A limitation of this prior art method is that the desktop search tool only collects information from a user's computer, not other computers. Another

limitation of this prior art method is that the desktop search tool only collects information on the user's computer and does not discover other devices from which to collect information. As a result, this prior art method has the disadvantage of being limited in the types of information sources from which to collect information and the types of information that can be collected.

BRIEF SUMMARY

[0008] A method and apparatus for hosted searching of different LAN information is described. In one embodiment, an apparatus for hosted searching of different private LAN information includes a LAN crawler to automatically and repeatedly crawl a LAN having multiple devices. The LAN crawler includes a collection module to attempt to collect, from across multiple disparate information sources stored in the multiple devices, only the parts of the disparate information sources that include descriptive information of a first set of one or more items of interest. The collection module includes a discovery module to discover the devices of the private LAN, a generic-probing module to attempt to collect the descriptive information according to a first set of probing requirements, and multiple specific-probing plug-ins each of which attempt to collect the descriptive information according to a second set of probing requirements that are specific to each of the specific-probing plug-ins. In one embodiment, one of the specific-probing plug-ins is configured to attempt to collect the descriptive information according to one or more probing requirements that are specific to an add-on application. The LAN crawler also includes a reporting module to automatically report the collected information organized according to the first set of items of interest out of a firewall of the private LAN being crawled and over the Internet.

[0009] In another embodiment, the apparatus for hosted searching of different private LAN information includes a hosted on-demand search system including a set of one or more centralized-search servers. The set of one or more centralized-search servers includes a crawler interface to receive the reports of different instances of the LAN crawler deployed on the multiple private LANs, at least some of which are operated by different entities, and a database interface to create and synchronize a separate private search database for each of the private LANs based on the received

reports. Each of the private search databases includes the collected information that is not organized by documents located on the private LANs, by the first set of items of interest. The set of one or more centralized-search servers also includes a server user interface module to provide a user interface over the Internet to the private LAN, to perform private searches of the private search database, and to provide an application rendered component as part of the user interface. The set of one or more centralized-search servers also includes an application interface to receive a request to access the collected information stored in the private search database from a third-party add-on application, to provide the accessed information to the third-party add-on application, and to receive from the third-party add-on application an application rendered component to be displayed on the user interface.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] The invention may best be understood by referring to the following description and accompanying drawings that are used to illustrate embodiments of the invention. In the drawings:

[0011] Figure 1 illustrates an exemplary hosted on-demand search system coupled to multiple private LANs over a network according to one embodiment of the invention;

[0012] Figure 2 illustrates an exemplary private LAN having a LAN crawler deployed on a client device according to one embodiment of the invention;

[0013] Figure 3 illustrates exemplary information sources stored on the multiple devices of the private LAN according to one embodiment of the invention;

[0014] Figure 4 illustrates an exemplary reorganization module of the centralized-search server according to one embodiment of the invention;

[0015] Figure 5 illustrates an exemplary flow diagram of the LAN crawler of the client device according to one embodiment of the invention;

[0016] Figure 6 illustrate an exemplary flow diagram of a private search according to one embodiment of the invention;

[0017] Figure 7 illustrates an exemplary flow chart of operations between the client device and the hosted on-demand search system according to one embodiment of the invention;

[0018] Figure 8 illustrates exemplary user interface pages of the user interface on the client device according to one embodiment of the invention;

[0019] Figure 9 illustrates an exemplary embodiment of a private search database that is a hierarchical database that stores the collected information in a tree structure according to one embodiment of the invention;

[0020] Figure 10 illustrates exemplary search syntaxes for searching a hierarchical database according to one embodiment of the invention;

[0021] Figure 11 illustrates an exemplary hosted on-demand search system coupled to multiple private LANs and to one or more hosted application services.

[0022] Figure 12 illustrates an exemplary hosted on-demand search system coupled to a private LANs over a network with support for add-on applications according to one embodiment of the invention;

[0023] Figure 13 illustrates an exemplary extensible LAN crawler according to one embodiment of the invention;

[0024] Figure 14 illustrates an exemplary hosted application service;

[0025] Figure 15 illustrates an exemplary flow diagram of an application search according to one embodiment of the invention;

[0026] Figure 16 illustrates an exemplary user interface page of the user interface including an application panel according to one embodiment of the invention;

[0027] Figure 17 illustrates an exemplary dashboard page according to one embodiment of the invention.

DETAILED DESCRIPTION

[0028] The following description describes methods and apparatus for hosted searching of different private LAN information. In the following description, numerous specific details such as logic implementations, opcodes, operations, hardware of software modules, code, and types and interrelationships of system components are set forth in order to provide a more thorough understanding of the present invention. It will be appreciated, however, by one skilled in the art that the invention may be practiced without such specific details. In other instances, control structures, gate level circuits and full software instruction sequences have not been shown in detail in order not to obscure the invention. Those of ordinary skill in the

art, with the included descriptions, will be able to implement appropriate functionality without undue experimentation.

[0029] References in the specification to "one embodiment", "an embodiment", "an example embodiment", etc., indicate that the embodiment described may include a particular feature, structure, or characteristic, but every embodiment may not necessarily include the particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an embodiment, it is submitted that it is within the knowledge of one skilled in the art to affect such feature, structure, or characteristic in connection with other embodiments whether or not explicitly described.

[0030] In the following description and claims, the terms "coupled" and "connected," along with their derivatives, may be used. It should be understood that these terms are not intended as synonyms for each other. Rather, in particular embodiments, "connected" may be used to indicate that two or more elements are in direct physical or electrical contact with each other. "Coupled" may mean that two or more elements are in direct physical or electrical contact. However, "coupled" may also mean that two or more elements are not in direct contact with each other, but yet still co-operate or interact with each other.

[0031] A method and apparatus for hosted searching of private LAN information is described. In one embodiment, an apparatus for hosted searching of private LAN information includes a LAN crawler to automatically and repeatedly crawl a LAN having multiple devices, and a hosted on-demand search system including a set of one or more centralized-search servers. The LAN crawler includes a collection module to attempt to collect, from across multiple disparate information sources stored in the multiple devices, only the parts of the disparate information sources that include descriptive information of a first set of one or more items of interest. In one embodiment, the collection module includes a discovery module to discover the devices of the private LAN, a generic-probing module to attempt to collect the descriptive information according to a first set of probing requirements, and multiple specific-probing plug-ins each of which attempt to collect the descriptive

information according to a second set of probing requirements that are specific to each of the specific-probing plug-ins. In one embodiment, one of the specific-probing plug-ins is configured to attempt to collect the descriptive information according to one or more probing requirements that are specific to an add-on application. In another embodiment, the LAN crawler includes a reporting module to automatically report the collected information organized according to the first set of items of interest out of a firewall of the private LAN being crawled and over the Internet. In another embodiment, the LAN crawler includes an organization module to automatically organize the collected information according to the first set of items of interest.

[0032] In another embodiment, the set of one or more centralized-search servers includes a crawler interface to receive the reports of the LAN crawler deployed on the private LAN, and a database interface to create and synchronize a private search database for the private LAN based on the received reports. The private search database includes the collected information that is not organized by documents located on the private LAN, but by the first set of items of interest. In another embodiment, the set of one or more centralized-search servers also includes a server user interface module to provide a user interface over the Internet to the private LAN, to perform private searches of the private search database, and to provide an application rendered component as part of the user interface. In another embodiment, the set of one or more centralized-search servers also includes an application interface to receive a request to access the collected information stored in the private search database from a third-party add-on application, to provide the accessed information to the third-party add-on application, and to receive from the third-party add-on application an application rendered component to be displayed on the user interface.

Hosted On-Demand Search System

[0033] Figure 1 illustrates an exemplary hosted on-demand search system 100 coupled to multiple private LANs 101, 102, and 103 over a network 130 according to one embodiment of the invention. The hosted on-demand search system 100 is coupled to private LANs 101, 102, and 103 over the network 130, for example, the

Internet. The private LANs may be owned and operated by different entities, such as different users, organizations, companies, or the like. For example, LAN 101 may be owned by a first company, and the LANs 102 and 103 are owned by a separate company, or alternatively, the LANs 101 may all be owned by separate companies. Each of the private LANs 101, 103, and 103 includes user interfaces (UI) 110(1), 110(2), and 110(3), respectively, and multiple devices 115 (only illustrated in private LAN 101 for ease of illustration). In one embodiment, the user interfaces 110(1), 110(2), and 110(3) are browser-based UIs that allow a user to retrieve the information from the corresponding private search databases 121(1), 121(2), and 121(3), respectively. The private search databases 121(1), 121(2), and 121(3) are data repositories that store the information collected by the LAN crawlers 111(1), 111(2), and 111(3), respectively. Using the user interfaces 110(1), 110(2), and 110(3), users can query the collected information stored in the private search databases 121(1), 121(2), and 121(3), respectively, to get search results. The user interfaces 110(1), 110(2), and 110(3) can display the search results in tree, chart, list, table, formats, as well as other types of formats.

[0034] The multiple devices 115 may include a server, a directory server, a workstation, a network printer, a switch, a router, or other electronic devices that can be part of a private LAN. Also, deployed on the private LANs 101, 102, and 103, are LAN crawlers 111(1), 111(2), 111(3), respectively. A LAN crawler is an automated script which explores the devices 115 of each of the private LANs in a methodical, automated manner. The LAN crawler automatically and repeatedly crawls the devices 115 of the private LAN to collect, from across multiple disparate information sources stored on the devices 115, descriptive information of items of interest. The LAN crawler collects from multiple disparate information sources, only those parts of the disparate information sources that include descriptive information of the first set of items of interest, instead of copying the entire information source. The LAN crawler of each of the private LAN may be deployed on a client device, such as a client workstation. Alternatively, the LAN crawler may be deployed on one of the devices 115 of the private LAN. In one embodiment, the LAN crawler and the UI for each of the private LANs resides on the same client

device. Alternatively, the LAN crawler and UI for each of the private LANs may reside on separate devices. It should be noted that the LAN crawler is different from a web crawler (also referred to as a web spider, web robot, or web bot), which is a program or automated script which browses the World Wide Web in a methodical, automated manner in order to create a copy of all the visited pages for later processing by a search engine that indexes the downloaded pages.

[0035] Although only illustrated in the LAN crawler 111(1), each of the LAN crawlers 111(1), 111(2), and 111(3) includes a collection module 112 and a reporting module 113. The collection module 112 attempts to collect, from across each of the disparate information sources, the descriptive information of the items of interest. In one embodiment, the descriptive information is collected from a single information source. In another embodiment, the descriptive information is collected from multiple information sources. The reporting module 113 automatically reports the collected information. In one embodiment, the reporting module 113 automatically reports the collected information organized according to the items of interest out of a firewall of the private LAN being called and over the Internet. In one embodiment, the reporting module 113 is configured to send the reports periodically over the Internet. In another embodiment, the reporting module 113 is configured to send the information once collected. Alternatively, the reporting module 113 may be configured to send the report on a scheduled basis. In one embodiment, the reports include corresponding time-stamped data with the collected information to indicate the time at which the information is collected. Alternatively, the reports do not include time-stamped data.

[0036] In another embodiment, each of the LAN crawlers also includes an organization module 114. The organization module 114 automatically organizes the collected information according to the items of interest. In one embodiment, the collection module 112 attempts to collect the descriptive information through a set of one or more organize questions to the devices 115 of the private LAN being crawled. In response to the set of one or more organize questions the collection module 112 receives values from the devices 115, including the descriptive information of the items of interest. In one embodiment, the organized questions

are request inquiries with defined names that extract values that correspond to the defined names. The defined names and corresponding values are name-value pairs that can be stored in the private search database 121. When the collection module 112 asks the questions in an organized manner, the collected information is implicitly organized for the reports that are sent by the reporting module 113. For example, it may be important to know the different between a computer named "Tetris" and installed software name "Tetris." Because the LAN crawler 111 knows how it collected the information for each item (e.g., using the organized questions), including how to identify the computer which has the name, the network to which that computer belongs, and the identity of the computer which has the software installed, the two items similarly named items can be distinguished by its organization in the collected information. Similarly, the collected information may be stored in the private search database using this organization. In another embodiment, the collection module 112 collects information that is not implicitly organized, and sends the unorganized information to the organization module 114 to be organized for the reports that are sent by the reporting module 113. In either case, the reporting module 113 generates one or more reports to send to the collected information to the hosted on-demand search system 100.

[0037] The hosted on-demand search system 100, which is coupled to the network 130 (e.g., Internet), includes a set of one or more centralized-search servers 120 (one centralized-search server has been illustrated. The centralized-search server 120 includes a private search database that corresponds to each of the private LANs. For example, the centralized-search server 120 includes private search databases 121(1), 121(2), and 121(3), which correspond to private LANs 101, 102, and 103, respectively. A search database is a collection of records or data that is stored in a data repository of a computer system so that a computer program or person using a search query language can consult it to answer search queries. The centralized-search server 120 includes a database interface 122 which creates and synchronize the separate private search databases 121(1), 121(2), and 121(3) for each of the private LANs 101, 102, and 103, respectively.

[0038] In one embodiment, the database interface 122 is a database management system (DBMS), which is used to manage and query the search database. In one embodiment, the database interface 122 is implemented in code. The central concept of a database is that of a collection of records, or pieces of information. Typically, for a given database, there is a structural description of the type of pieces of information held in that database; this description is known as a schema. The schema describes the objects that are represented in the database, and the relationships among them. There are a number of different ways of organizing a schema, that is, of modeling the database structure; these are known as database models. There are various types of database models, such as, for example, relational models, flat models, hierarchical models, network models, object-relational models, object models, entity-relationship models, associative models, concept-oriented models, entity-attribute-value models, semi-structured models, extensible markup language (XML) database models, or the like. The model in most common use is the relational model, which represents all information in the form of multiple related tables, each including rows, and columns. This model represents relationships by the use of values common to more than one table. Other models such as the hierarchical model and the network model use a more explicit representation of relationships. The hierarchical model is organized into a tree-like structure. The structure allows repeating information using parent/child relationships: each parent can have many children but each child only has one parent. In one embodiment, the private search databases 121(1), 121(2), and 121(3) is a hierarchical database, as described in more detail below. Alternatively, in other embodiments, the private search databases 121(1), 121(2), and 121(3), are other types of databases.

[0039] Each of the private search databases 121(1), 121(2), and 121(3) includes the collected information, which is collected from across the disparate information sources of a private LAN being crawled. The collected information in each of the private search databases 121(1), 121(2), and 121(3) is organized according to the items of interest, and not by documents located on the private LANs. It should be

noted conventional search engines organize the collected information according to the collected documents, not the items of interest.

[0040] The centralized-search server 120 also includes a crawler interface 123 that receives the reports from the reporting module 113 of the different instances of the LAN crawler (e.g., 111(1), 111(2), and 111(3)) deployed on the different private LANs 101, 102, and 103. The crawler interface 123 distinguishes the reports from the different instances of the LAN crawler deployed on the different private LANs to identify in which private search database a particular report is to be stored, and sends the distinguish reports to the database interface 122 to be stored in the identified search database (e.g., search databases 121(1), 121(2), and 121(3)). In one embodiment, the crawler interface 123 distinguishes the reports by sending an identifier of the received report to a configuration database 125, and receives the identified search database that corresponds to the identifier from the configuration database 125. The identifier identifies the entity that operates the particular LAN from which the report was received. The identifiers for each of the private LANs may be inserted into the reports by the respective LAN crawler.

[0041] The centralized-search server 120 also includes a server user interface (UI) module 124 that is coupled to the database interface 122, crawler interface 123, and configuration database 125. The server UI module 124 is configured to provide a user interface 110 over the Internet to each of the private LANs 101, 102, and 103, to allow users to perform private searches of their corresponding private search database 121(1), 121(2), and 121(3), respectively. In one embodiment, the server UI module 124 receives a search query from a user of the private LAN 101 to perform a private search of the corresponding private search database 121(1). These servers UI module 124 performs a search in the search database 121(1) through the database interface 122 using the search query. In one embodiment, the server UI module 124 is configured to store the search query in the configuration database 125 for later retrieval by the user. The user may designate the search query as being shareable. When the search query is designated as shareable, the server UI module 124 stores the search query, but not the search results of the private search, and designates the saved search query as shareable, allowing for display and selection of

the shareable search query on the user interfaces 110(1), 110(2), and 110(3) of the private LANs 101, 102, and 103, respectively. However, when the search query is not designated as shareable, the server UI module 124 stores a search query and only allows for display and selection of the stored search query on the user interface 110(1) of the private LAN 101 from which the search query originated.

[0042] The centralized-search server 120 also includes the configuration database 125 that is coupled to the crawler interface 123 and the server user interface module 124. In addition to storing the search queries as described above, the configuration database 125 may also store authentication information for access by the user interfaces 110(1), 110(2), and 110(3). The configuration database 125 also stores the identifiers to identify the source of the received reports in order to distinguish each of the reports for each of the private LANs from which the reports originated. Table 1 includes exemplary types of information that are stored in the configuration database 125.

TABLE 1

Type of Information	**Description of Information**
Users	User authentication information
Companies	Companies which to which the users belong
Demographics	Demographic information collected from users
Crawlers	Information about crawler operation
Dashboards	A dashboard is a collection of dashboard panels each of which display information from saved search queries
Saved Search Queries	A search query which has been saved by a user and optionally designated as shareable
Search Histories	Search history for each user

The exemplary types of information of Table 1 include users, demographics, LAN crawlers, dashboards, saved search queries, and search histories. The user-type

information may include user authentication information that is used to authenticate the user, such as when the user requests the user interface 110(1) from the server user UI module 124. The demographic-type information may include demographic information collected from each of the users of the private LANs 101, 102, and 103, respectively. The crawler-type information may include information about the crawler operations on the particular LAN crawlers of each of the private LANs 101, 102, and 103. The dashboard-type information includes information regarding a collection of dashboard panels. A dashboard is a graphical user interface (GUI) widget that can be part of the user interface 110(1), and can be configured and saved by the user to display search results in various forms for saved search queries. For example, the user interface 110(1) may include a page that displays various components, as well as the dashboard. Alternatively, the page may include a dashboard that includes one or more dashboard panels. Each of the dashboard panels may include updated search results for separate saved search queries. For example, a user may have separate dashboard panel for displaying search results in the form of a list, a chart, or a table, as described in more detail below. The collection of dashboard panels may include saved configurations of the dashboard on each of the user interfaces 110(1), 110(2), and 110(3). For example, the user may save the configuration of a dashboard with a saved search query so that when the user logs in, the dashboard may be displayed with updated search results for the saved search query without having to manually enter the search query again.

[0043] Also, the configuration database 125 may also store other types of information, such as saved search queries and search histories. The saved search query may be saved by a user and optionally designated as shareable to be shared with other users of other private LANs. It should be noted that although a search query is designated as shareable, only the saved search queries are shared, not the search results from the saved search queries. The search history type information includes search histories for each of the users. It should be noted that Table 1 includes exemplary types of information that may be stored in the configuration database 125, but in other embodiments, the database 125 may store other types of information.

[0044] In another embodiment, the hosted on-demand search system 100 includes a classification server 140 coupled to a classification database 141. The classification server 140 may attempt to identify devices 115 that are discovered on the private LANs 101, 102, and 103. The classification server 141 is configured to compare the collected information of the private search databases 121(1), 121(2), and 121(3) against predetermined characteristics of own devices stored in the classification database 141, and to compute a classification metric for the multiple devices 115 of the private LAN 101, 102, and 103. For example, the classification server 140 may evaluate the collected information by comparing the collected information against "fingerprints" of known devices stored in the classification database 141, comparing the media access control (MAC) address (of the collected information) to ranges of MAC addresses for known devices stored in the classification database 141, or the like. Then using either the fingerprint comparison or the MAC address lookup, or both, classification server 140 determines a classification for the discovered devices of the private LANs 101, 102, and 103. The classification server 140 can evaluate the collected information and determine a classification for the discovered devices and notify the administrator of the private LAN of the device classification, or modify the collected information in the private search database 121 to include the device classification. By using the classification server 140 and classification database 141, it is possible to collect information from many different networks, and thus a large set of different devices. It is also possible to classify an unknown, discovered device 115 on the private LAN; especially, when the LAN crawler deployed on the private LAN is unable to report certain classification information (e.g., vendor, model, or the like) to the hosted on-demand search server 120. In one embodiment, the classification server 140 and classification database 141 are the classification server and classification database, developed by Network Chemistry of Palo Alto, California. The classification server and classification database developed by Network Chemistry may be implemented according to the various embodiments described in U.S. Patent Application Serial No. 11/803,004, filed May 10, 2007, entitled "Collaborative Device Classification." Alternatively, the classification server 140 and

classification database 141 are other types of classification servers and classification databases. The distribution module 127 is configured to distribute copies of the LAN crawler to be installed on devices. For example, through the user interface, a user visiting a website hosted by the company or organization that manages the hosted on-demand search system 100, may click on a link to download the LAN crawler to the user's computer to be installed and executed.

[0045] Figure 2 illustrates an exemplary private LAN 101 having a LAN crawler deployed on a client device 200 according to one embodiment of the invention. The LAN crawler 111 of the client device 200 automatically and repeatedly collects information from multiple devices 115 of the private LAN 101 out of a firewall 220 of the private LAN 101 being crawled and over the Internet 130 to the centralized-search server 120. In particular, the LAN crawler 111 automatically and repeatedly collects information from disparate information sources 203 that are stored on the multiple devices 115. Each of the devices 115 may store one or more information sources 203. As described above, the reporting module 113 automatically records the collected information, which is organized according to the items of interest, out of the firewall 220. In one embodiment, the reporting module 113 communicates with the crawler interface 123 over the Internet through a router 210 and the firewall 220. A router is a computer networking device that interconnects separate logical subnets. A router is a computer whose software and hardware are usually tailored to the tasks of routing and forwarding, generally containing a specialized operating system (e.g. Cisco's IOS or Juniper Networks JunOS or Extreme Networks XOS), RAM, NVRAM, flash memory, and one or more processors. A router may also manage a pool of Internet Protocol (IP) addresses and may have information about client configuration parameters such as the default gateway, the domain name, the Domain name system (DNS) servers, other servers, or the like. A firewall is a hardware or software device which is configured to permit, deny, or proxy data through a computer network which has different levels of trust. Routers and firewalls of private LANs are known to those of ordinary skill in the art, and accordingly, a detailed description regarding routers and firewalls has not been included so as to not obscure the embodiments of the present invention. It should

also be noted at the user interface 110 communicates with the server UI module 124 of the centralized-search server 120 over the Internet 130 through the router 210 and firewall 220.

[0046] In one embodiment, the collection module 112 of the LAN crawler 111 includes a discovery module 201, and a probing module 202. The discovery module 201 automatically discovers the devices 115 of the private LAN 101 being crawled by the LAN crawler 111. The probing module 202 attempts to collect data on each of the information sources 203 stored in the discovered devices 115 of the private LAN 101. The probing module 202 may be configured to collect data from information sources 203 according to a set of probing requirements. The set of probing requirements may include a set of one or more organized questions. The collection module 112 asks the set of one or more questions of the information sources 203 of the devices 115, and receives values in response to the set of organized questions from the information sources 203. The values include descriptive information regarding the items of interest. In another embodiment, the set of probing requirements may include other types of requests to collect information from the devices 115. As described above, when the collection module asks organized questions, the LAN crawler 111 may not need an organization module to organize the collected information according to the items of interest, since the collected information is implicitly organized by the use of organized questions. Alternatively, the LAN crawler 111 may include an organization module 114 that organizes the collected information according to the items of interest before being reported over the Internet 130 by the reporting module 113.

[0047] In one embodiment, the LAN crawler 111 is coupled to a data store 230 (e.g., a memory, a database, or the like) in which the LAN crawler 111 stores configuration information for the particular LAN crawler 111. In one embodiment, the configuration information may include the set of probing requirements for the LAN crawler 111, such as a set of one or more organized questions. Alternatively, the configuration information stored in the data store 230 includes additional LAN crawler configuration information. In another embodiment, the LAN crawler

configuration for each of the LAN crawlers is stored in the configuration database 125.

[0048] In general, the LAN crawler 111 discovers devices 115 on the private LAN 101 and collects information from the discovered devices 115. The LAN crawler 111 collects, from across multiple disparate information sources 203 stored in the devices 115, only those parts of the disparate information sources 203 that include descriptive information of the first set of items of interest. In one embodiment, for at least one item of interest, the parts are collected from multiple disparate information sources. In one embodiment, the LAN crawler 111 is deployed on the client device 200. For example, the LAN crawler 111 can be software operating on a processor of the client device 200.

[0049] In one embodiment, the descriptive information of the first set of items of interest include, in general, technical information regarding the private LANs 101, 102, and 103, user of the private LANs 101, 102, and 103, and the multiple devices 115 of each of the private LANs 101, 102, and 103. Each of the LAN crawlers 111(1), 111(2), and 111(3), is configured to collect values of the technical information from the multiple information sources 203 stored on the devices 115 through a set of one or more organized questions to the devices 115 of the private LAN being crawled.

[0050] Information Technology (IT) or Information and Communications Technology (ICT), as defined by the Information Technology Association of America (ITAA), is the study, design, development, implementation, and support or management of computer-based information system, particularly software applications and computer hardware. IT deals with the use of electronic computers and computer software to convert, store, protect, process, transmit, and retrieve information, securely. IT professionals, such as network administrators, perform a variety of duties that range from installing applications to designing complex computer networks and information databases, such as data management, networking, engineering computer hardware, database and software design, as well and the management and administration of entire systems or networks. In one embodiment, the technical information is IT information that is used by an IT

professional in performing a variety of duties, such as those described above, for the study, design, development, implementation, and support or management of computer-based information systems, particularly software applications and computer hardware. Some examples of descriptive IT information include, but are not limited to, information in configuration files in routers, switches, firewalls, asset lists, information in Lightweight Directory Access Protocol (LDAP) servers (described below), personal computer configuration information in a registry, a Windows Management Instrumentation (WMI) database (described below), and/or a directory, physical and logical network topology information, flow information, raw packet contents, log information from all devices, networks, and systems. Alternatively, the descriptive information of the first set of items of interest may include other types of information other than technical information, such as financial information, enterprise information, or the like.

[0051] Network and host security solutions and network management applications are specialized repositories of information that operate independently and without information sharing. More advanced technology leads to more specialization, which makes it even more difficult to share information between systems or devices. Attempts to integrate this information, such as security information managers (SIM), or configuration management databases (CMDB), lead to even more specialization as they limit the resolution of information that they will receive and process—e.g., only receiving alerts from support intrusion detection systems (IDSs), which detects unwanted manipulations to systems, or only parsing configuration from supported routers. The embodiments described herein may allow a user to more easily find technical information, such as network management information and relationships within and between disparate systems or devices, which may help the user to solve network management and security problems. The embodiments described herein may also allow a user to find related items of interest, even when the items of interest originate from disparate information sources, such as devices employing different data models. A data model is an abstract model that describes how data is represented and used.

[0052] More specifically, in other embodiments, the technical information may include information regarding existence of the devices 115 within each of the private LANs 101, 102, and 103. The devices 115 may include one or more routers, one or more switches, one or more servers, one or more directory servers, one or more workstations, or the like. The technical information may also include information regarding existence of multiple hardware modules within each of the devices 115, states of the hardware modules, properties of the hardware modules, configuration of the hardware modules, history of the hardware modules. The technical information may also include information regarding existence of any peripherals coupled with the devices 115, states of the peripherals, properties of the peripherals, configuration of the peripherals, history of the peripherals. The technical information may also include information regarding existence of at least one operating system operating within each of the devices 115, state of the operating systems, properties of the operating systems, configuration of the operating systems, history of the operating systems. The technical information may also include information regarding existence of software within each of the devices 115, state of the software, properties of the software, configuration of the software, history of the software. The technical information may also include information regarding presence of users using each of the devices 115, an inventory of users that are authorized to use each of the devices 115, policies assigned to the users for each of the devices 115, and history of each user's actions regarding each of the devices 115.

[0053] For example in one embodiment of the invention the data stored in the private search database includes information regarding substantially all devices within a private LAN, a list of software installed on those devices, and a list of users authorized to use those devices. Additionally, the data stored may include information regarding the operating system version installed on substantially all devices within the private LAN, the software which is running on substantially all devices within the private LAN, and a configuration file from at least one router, switch, or firewall within the private LAN. The devices may include substantially all workstations within a private LAN, substantially all routers within the private

LAN, substantially all switches within the private LAN, substantially all servers within the private LAN, substantially all firewalls within the private LAN, and substantially all directory servers within the private LAN.

[0054] The disparate information sources 203 may include, for example, a routing table of a router, a router configuration file of a router, an ARP table of a switch, a bridging table of a switch, a switch configuration table of a switch, a software configuration file of a server, a resource utilization counter of a server, a log file of a server, custom application file of a server, user information of a directory server, group information of a directory server, a software configuration file of a workstation, a registry of a workstation, an operating system interface database of a workstation, a directory of a workstation, a resource utilization counter of a workstation, a log file of a workstation, a configuration file of a network printer, or the like. Alternatively, other technical information may be collected from other types of information sources than those listed above.

[0055] In another embodiment, the technical information is collected from the registry of a device running the WINDOWS® operating system, available from Microsoft®. In another embodiment, the technical information is collected from a WMI database of a device running Microsoft WINDOWS. In another embodiment, the technical information is collected from the "/proc directory" of a device running a UNIX-like operating system (e.g., Linux). In another embodiment, the technical information is collected from a directory service (e.g., residing on a directory server) using LDAP. LDAP is an application protocol for querying and modifying directory services, running over Transmission Control Protocol and Internet Protocol (TCP/IP). LDAP tends to use DNS names for structuring the objects of the directory service. In another embodiment, the technical information is collected from a networking device, for example, a router or a switch, using the Simple Network Management Protocol (SNMP), Telnet, Secure Shell (SSH) protocols, or the like. In another embodiment, the technical information is collected from a network printer using SNMP or the like. Alternatively, the technical information may be collected from other devices that are part of the private LAN.

[0056] In one embodiment, the technical information is collected by the LAN crawler 111 asking a set of one or more organized questions of the disparate information sources 203, described above, which are stored in the devices 115 of the private LAN being crawled. In response to the set of organized questions, the LAN crawler 111 receives values of the technical information from the disparate information sources stored on the devices 115.

[0057] There are several techniques that may be employed to discover the devices 115 on the private LAN. These techniques fall generally into two main categories: passive traffic collection, and active scanning.

[0058] Passive traffic collection entails operating in a promiscuous mode in order to observe all broadcast and non-broadcast network traffic, such as Ethernet traffic. In this technique, device MAC addresses are gathered and the source IP address is recorded if the packet in question is an IP or address resolution protocol (ARP) packet. For active scanning the following techniques can be used: 1) ARP Scanning, 2) Ping Scanning, and 3) CAM Table Scanning.

[0059] In ARP Scanning, the local network segment is probed by issuing ARP requests to each possible IP address within the system's broadcast domain. The upper and lower bounds for the addresses to query are determined by examining the network and broadcast addresses of the network adapter used by the LAN crawler 111 to perform the scanning activity. If an ARP reply is received, then a device at the queried IP address exists.

[0060] Ping Scanning involves sending an Internet Control Message Protocol (ICMP) echo request (a *Ping* packet) to a single IP address or a range of addresses. If a device is utilizing one of the IP addresses to which a Ping was sent, the device responds with an ICMP echo reply packet. Thus it can be determined if a device 115 exists at an arbitrary IP address.

[0061] Cam Table Scanning involves interrogating the network's switching infrastructure for the MAC addresses of the devices connected to it. This may be done via SNMP. This enables the LAN crawler 111 to quickly gather MAC addresses for all devices 115 on the private LAN without the need for the LAN crawler 111 to be on the same network segment. As described above, the

classification server 140 is configured to classify the devices 115. For example, the organizationally unique identifiers (OUIs) which form the first 24-bits of the MAC address can be compared against those that belong to a particular manufacture. For example, the OUI of the MAC address can be compared with those that belong to a manufacture of wireless or wired access points (APs).

[0062] Some other techniques that can be used to collect information about the devices 115 of the private LAN are, for example:

1) Passive operating system detection: A device's operating system can be determined remotely by observing key fields in the TCP/IP packets that it emits.
2) TCP & UDP port scanning: APs often run at least a handful of remotely accessible services. By cataloging the services found on a particular model of AP it is possible to determine what devices appear similar to it.
3) IP protocol scanning: Even if a different revision of an AP model uses the same operating system it may support different IP protocols.
4) Service interrogation: Many APs provide services used to configure them. This technique involves interrogating the services an AP may be running in order to gather information that may differentiate it from another device.
5) SNMP queries: Some APs provide SNMP management capabilities. SNMP queries are used to glean any information that may uniquely identify a device.
6) Promiscuous mode detection: If the device is in promiscuous mode then it may be a network bridge. APs may be network bridges.
7) NAT (Network Address Translation) device detection: If the device is performing NAT, then it may be an AP/router. Wireless AP/routers act as NAT gateways for the hosts connected to them.
8) Dynamic Host Configuration Protocol (DHCP) Client Identification: This identifies default hostnames and options that are unique to the DHCP client implementations used in off-the-shelf wireless AP/routers.

[0063] Additionally, the device's manufacturer may be determined by the OUI of its MAC address. This information is gathered during normal network communication with the device 115.

[0064] In one embodiment, the LAN crawler 111 is configured to collect the same information as described in the U.S. Patent Application Serial No. 11/803,004, filed May 11, 2006, entitled "Collaborative Device Classification." In another embodiment, the LAN crawler 111 is configured to collect the same, similar, and/or dissimilar information than the information described in the U.S. Patent Application Serial No. 11/803,004. For example, in addition to, or in place of, the information collected by the scan agent, the LAN crawler 111 is configured to attempt to collect information from other types of information sources, such as a WMI database.

[0065] A WMI database is a type of operating system interface database. WMI specifically is a set of extension to the WINDOWS Driver Model that provides an operating system interface through which instrumented components provide information and notification. WMI allows scripting languages like VBScript or WINDOWS POWERSHELL®, available from Microsoft, to manage personal computers and servers that are running WINDOWS, both locally and remotely. The contents of the WMI database may include make and model information for the hardware of the device, hardware configuration of the device, technical support ID information, list of installed programs, information about logged in users, information about running programs, and/or resource utilization information (e.g., CPU, memory, and disk utilization).

[0066] In addition to collecting information from a WMI database, the LAN crawler 111 is configured to collect information from other operating system interface databases, such as Web-Based Enterprise Management (WBEM) and Common Information Model (CIM) standards, available from the Distributed Management Task Force (DMTF).

[0067] Figure 3 illustrates exemplary information sources 300 stored on the multiple devices 115 of the private LAN according to one embodiment of the invention. The multiple private LAN devices 115 include the client device 200 that is running the instance of the LAN crawler 111 (e.g., workstation), the router 210, a

switch 310, a server 320, a directory server 330, a first workstation 340, a network printer 350, and a second workstation 360. The information sources 300 are disparate information sources (e.g., 301-326) that are stored on the LAN devices 115. In this embodiment, the router 210 includes a routing table 301 and a routing configuration 302. The routing table 301, also referred to as a Routing Information Base (RIB), is an electronic table (e.g., stored in a file) or database type object that is stored in the router 210. The routing table 301 stores the routes (and in some cases, metrics associated with those routes) to particular network destinations. The routing table 301 may also include information regarding the topology of the private LAN. The routing configuration 302 is an electronic table (e.g., stored in a file) or database type object that is stored in the router 210. The routing configuration 302 may include router configuration information, such as how to automate assignment of IP addresses, subnet masks, default gateway, and other IP parameters, such as firewall rules, or the like. It should be noted that the format of the routing configuration 302 depends on the manufacturer of the router 210. For example, in a router developed by Cisco Systems Inc., the routing configuration 302 is expressed as a series of commands; a new router can be set up with the same configuration by entering the series of commands into a command line interface of the new router. As such, the routing configuration 302 in the Cisco Systems' router may be more like a file. In other embodiments, the routing configuration 302 is available through SNMP. In these embodiments, the routing configuration 302 is stored more like a database.

[0068] In one embodiment, the LAN crawler 111 collects descriptive information from the router 210 using SNMP. Alternatively, the LAN crawler 111 may collect the descriptive information from the router 210 using other protocols, such as Telnet, SSH protocols, or the like.

[0069] In this embodiment, the switch 310 includes an Address Resolution Protocol (ARP) table 303, a bridging table 304, and switch configuration 305. A switch, also referred to as a network switch, is a computer networking device that connects network segments. Network switches are capable of inspecting data packets as they are received, determining the source and destination device of that

packet, and appropriately forwarding the packet to the intended connected device. Switches of private LANs are known to those of ordinary skill in the art, and accordingly, a detailed description regarding switches has not been included so as to not obscure the embodiments of the present invention. The ARP table 303 is a table used for finding a host's hardware address when only the host's network layer address is known. ARP is a standard method for resolving many different network-layer protocol addresses to hardware addresses, and may be used to translate IP addresses to MAC addresses. The ARP table 303 may also include information regarding Token Rings, Fiber Distribution Date Interface (FDDI), IEEE 802.11, IP over ATM, or the like. The switch configuration 305 may store other configuration information related to the switch 310.

[0070] In one embodiment, the LAN crawler 111 collects descriptive information from the switch 310 using SNMP. Alternatively, the LAN crawler 111 may collect the descriptive information from the switch 310 using other protocols, such as Telnet, Secure Shell (SSH) protocols, or the like.

[0071] In this embodiment, the server 320 includes various disparate information sources, such as software configuration files 306, resource utilization counters 307, log files 308, and custom application files 309. The software configuration files 306 may include information regarding the software that is installed and/or running on server 320, for example, the type and version of the operating system, and/or the types and versions of other types of software. It should be noted that the software configuration information may be stored in other information sources than software configuration files.

[0072] The resource utilization counters 307 may include the actual resource utilization values of the server 320. The resource utilization may include, for example, central processing unit (CPU) performance of one or more processors, input-output (I/O) performance, memory performance, or the like. The resource utilization counters 307 may be hardware performance counters (also referred to as hardware counters), which are a set of special-purpose registers of a processor to store the counts of hardware-related activities within the computer system. Alternatively, the resource utilization counters 307 may be software performance

counters that read the values from set of special-purpose registers of the processor. Alternatively, the resource utilization values may be stored in log files, WMI database, or in other types of files stored on the sever 320.

[0073] The log files 308 may include time-based log information of the server 320. The time-based log information may be sequentially or chronologically recorded in the log files 308. The log files 308 may include recorded events to provide an audit trail that can be used to diagnose problems. For example, some operating systems provide a "syslog" service, which allows the filtering and recording of log message to be performed by a separate dedicated subsystem, rather than each application recording log message. "Syslog" is a standard for forwarding log message in an IP network. The "syslog" service can be used to integrate log data from many different types of systems into a central repository.

[0074] The custom application files 309 may include information regarding applications that are currently installed and/or running on the server 320. In one embodiment, custom applications can be developed for exclusive use by the server 320. The custom application file 309 may include information that is specific to custom applications. For example, a Manufacturing Resource Planning (MRP) application may provide the number of transactions per section it is processing through an application interface (API). The LAN crawler 111 could collect specific information, such as transactions per second, from the MRP application through an API.

[0075] In one embodiment, the LAN crawler 111 collects descriptive information from the server 320 using Hypertext transfer protocol (HTTP). Alternatively, the LAN crawler 111 may collect the descriptive information from the server 320 using other protocols, such as Representational State Transfer (REST), Remote Procedure Call (RPC), Simple Object Access Protocol (SOAP), SNMP, SSH, WMI, COBRA, Distributed Component Object Model (DCOM), or the like.

[0076] In this embodiment, the directory server 330 is an information source that includes user information 311 and/or group information 312. The directory server 330 may be a device that executes one or more software applications that store and organize information about users, groups of users, and/or network resources. The

directory server 330 may be used by a network administrator to manage users' access to the resources. The directory server 330 may also store a directory database that holds information about names to objects that are managed in the directory service. The directory server 303 may store such information as, for example, names of users, names of groups of users, permission sets associated with the users, permission sets associated with the groups of users, or the like. The directory service may be a shared information infrastructure for locating, managing, administrating, and organizing common items and network resources, which can include volumes, folders, files, printers, users, groups, devices, telephone numbers, and other objects. For example, the directory service may be used to obtain a list of available computers and the information for accessing them. The directory server 303 may also define the namespace for the network. A namespace a namespace in this context is the term that is used to hold one or more objects as named entries. The directory service has a set of rules that determine how network resources are named and identified. The rules specify that the names be unique and unambiguous. The name is called the distinguished name (DN) and is used to refer to a collection of attributes, such as relative distinguished names, which make up the name of a directory entry.

[0077] In one embodiment, the LAN crawler 111 collects descriptive information from the directory service on the directory server 330 using LDAP. Alternatively, the LAN crawler 111 collects descriptive information from the directory server 330 using other protocols, such as protocols used in Active Directory, Remote Authentication Dial In User Service (RADIUS), or the like. Active Directory is an implementation of directory services for use with devices running WINDOWS operating system. Active Directory may provide central authentication and authorization services for WINDOW-based computers, and may allow administrators to assign policies, deploy software, and apply updates to an organization. Active Directory stores information and settings in a central database. The RADIUS protocol is an authentication, authorization, and accounting protocol for applications such as network access or IP mobility.

[0078] In this embodiment, the first workstation 340 includes various information sources, such as software configuration files 313, resource utilization counters 314, log files 315, directories 316 (e.g., "/proc directory) of the first workstation 340. The first workstation 340 is a device that is running a UNIX or UNIX-like operating system, such as Linux. A UNIX-like operating system is one that behaves in a manner similar to a UNIX system, while not necessarily conforming to or being certified to any version of the Single UNIX specification. The software configuration files 313 may include information regarding the software that is installed and/or running on first workstation 340, for example, the type and version of the operating system (e.g., Linux), and/or the types and versions of other types of software, as described above with respect to the software configuration files 306. The resource utilization counters 314 may include the actual resource utilization values of the first workstation 340, as described above with respect to the resource utilization counters 307. The log files 315 may include time-based log information of the first workstation 340, as described above with respect to the log files 308.

[0079] The directories 316 may include, for example, the "/proc directory." The "/proc directory" is a file or a directory of files containing information about all the CPUs and memories in the system, such as the numbers used to identify each logical CPU, the vender identifications used to identify the CPU manufacturer, the numbers given to identify the CPU family or manufacturing process, information about the current state of the system's computer memory (including virtual memory and the cache), or the like. On workstations that are running Linux, the "/proc directory" may substitute or compliment information contained in the resource utilization counters 314.

[0080] In one embodiment, the LAN crawler 111 collects descriptive information from the first workstation 340 using SSH. Alternatively, the LAN crawler 111 may collect the descriptive information from the first workstation 340 using other protocols, such as telnet, SNMP, syslog, HTTP, or the like.

[0081] In this embodiment, the network printer 350 includes various information sources, such as a configuration file 317, software configuration files 318, resource utilization counters 319, log files 321, or the like. The software configuration files

318, resource utilization counters 319, log files 321 are similar to those described above with respect to the server 320 and first workstation 340. The configuration file 317 includes information about the network printer, such as the name of the network printer 350, the IP address of the network printer 350, configuration settings of the network printer 350, or the like.

[0082] In one embodiment, the LAN crawler 111 collects descriptive information from the network printer 350 using SNMP. Alternatively, the LAN crawler 111 may collect the descriptive information from the network printer 350 using other protocols, such as HTTP, Telnet, or the like.

[0083] In this embodiment, the second workstation 360 includes various information sources, including registry 322, WMI database 323, software configuration files 324, resource utilization counters 325, and log files 326. Registry 322 is a directory which stores setting and options for the operating system. The registry 322 may contain information and settings for all the hardware, operating system software, most non-operating system software, users, preferences of the device (e.g., personal computer (PC)), or the like. For example, registry 322 is the Microsoft Registry for the WINDOWS operating system. Whenever a user makes changes to settings, file associations, system policies, or installed software, the changes are reflected and stored in the registry 322. The registry 322 also provides a window into the operation of the kernel, exposing runtime information such as performance counters and currently active hardware. In another embodiment, the information that is obtained from the registry may also be obtained from other non-Windows mechanisms, such as Sysfs and procfs, which expose runtime information through the file system.

[0084] As described above, the WMI database 323 is a type of operating system interface database. The contents of the WMI database 323 may include make and model information for the hardware of the device, hardware configuration of the device, technical support ID information, list of installed programs, information about logged in users, information about running programs, and/or resource utilization information (e.g., CPU, memory, and disk utilization).

[0085] In another embodiment, the WMI database 323 may be other operating system interface databases, such as Web-Based Enterprise Management (WBEM) and Common Information Model (CIM) standards, from the Distributed Management Task Force (DMTF), or the like.

[0086] The software configuration files 324 may include information regarding the software that is installed and/or running on second workstation 360, for example, the type and version of the operating system (e.g., WINDOWS), and/or the types and versions of other types of software, as described above with respect to the software configuration files 306. The resource utilization counters 325 may include the actual resource utilization values of the second workstation 360, as described above with respect to the resource utilization counters 307. The log files 326 may include time-based log information of the second workstation 360, as described above with respect to the log files 308.

[0087] In one embodiment, the LAN crawler 111 collects descriptive information from the second workstation 360 using WMI. Alternatively, the LAN crawler 111 may collect the descriptive information from the second workstation 360 using other protocols, such as server message block (SMB), DCOM, SNMP, or the like.

[0088] TABLE 2 includes exemplary information sources, and the corresponding first set of items of interest.

TABLE 2

Information Sources:	**First set of items of Interest:**
For each Private LAN	List of all device connected to a network
For each network device information like:	
	IP address
	MAC Address
	Open TCP and UDP ports
	Responses to probes on TCP and User Datagram Protocol (UDP) ports
	Dynamic Host Configuration Protocol (DHCP) request contents

	Domain Name System (DNS) names of the devices
For each devices running Microsoft Windows operating system, collected information like:	
	List of installed programs (content of the Window registry)
	Installed program configuration (content of the Window's registry)
	Operating System Configuration (content of the Window's registry)
	Names of users who have logged into the device (content of the Window's registry)
	Invalid Configurations which might have been created by spyware, adware or malicious programs (content of the Window's registry)
	Hardware Configuration of the device (content from Windows Management Instrumentation (WMI))
	Make and model information for the hardware (content from WMI)
	Technical support ID information (content from WMI)
	List of installed programs (content from WMI)
	Information about logged in users (content from WMI)
	Information about running programs (content from WMI)

	Resource utilization information including, e.g., CPU, memory, and disk utilization (content from WMI)
	Resource utilization information including, e.g., CPU, memory, and disk utilization (from performance counters)
For each devices running Unix-like operating system, collected information like:	
	Resource utilization information including, e.g., CPU, memory, and disk utilization (e.g., content from /proc directory, performance counters, etc)
	List of installed programs
	Installed program configuration
	Information about logged in users
	Information about running programs
For each devices supporting SNMP (e.g., switches and routers), collected information like:	
	Interface utilization statistics
	ARP tables
	Bridging Tables
	Routing Tables
	Other information contained in SNMP Management Information Bases (MIBs)
For each devices supporting telnet or SSH interfaces with command line interfaces (e.g., Cisco IOS based devices), collected information like:	
	Detailed device configuration files

	Bridging tables
	Routing tables
For each directory server (e.g., devices using protocols such as LDAP or Active Directory), collected information like:	
	List of users and groups in the network
	Contact information for users
	Group membership information for users
	Login history information for users
	List of other resources in network, such as servers and databases
For each device, log information, saved to log files or forwarded using syslog, like:	
	User login history
	Firewall log information
	Mail server history
	Application error logs
For each web server, collected information like:	
	The number of hits to the website
	Number of sales, click-through rate, or other sales metrics
For each device, collected information from other internal systems (e.g., Customer Relationship Management (CRM) Systems), like:	
	Number of meetings scheduled
	Pipeline value
For each application on a device, collected information like:	

	Up-time of the application
	Number of transactions processed
	Number of active connections
	Average transaction time

[0089] Figure 4 illustrates an exemplary reorganization module 126 of the centralized-search server 120 according to one embodiment of the invention. In this embodiment, the database interface 122 includes the reorganization module 126. The reorganization module 126 is configured to reorganize the collected information by adding items of interest to the collected information stored in the corresponding search database 121, to reorganize the existing items of interest stored in the corresponding search database 121, to rename existing items of interests stored in the corresponding search database 121, or the like. In one embodiment, the reorganization module 126 is part of the database interface 122. Alternatively, the reorganization module 126 may be implemented in a separate module, or in other modules of the hosted on-demand search system 100.

[0090] The reorganization module 126 includes a report scanning module 401, an integration module 402, and a renaming module 403. The report scanning module 401 is configured to attempt to collect, from across the disparate reports received from the private LAN being crawled, descriptive information of other items of interest (also referred to as second set of one or more items of interest). The integration module 402 is configured to integrate the collected descriptive information that is organized according to the second set of items of interest into the corresponding private search database 121. The integration module 402 can extract descriptive information of the second set of items of interest from the reports that include the descriptive information of the first set of items of interest, and integrate the extracted information into the private search database 121 to be organized according to the second set of items of interest in addition to, or in place of, the descriptive information that is organized according to the first set of items of interest when received from the crawler interface 123. For example, TABLE 3

includes exemplary second set of items of interest that can be created from the first set of items of interest received in the reports from the LAN crawlers.

TABLE 3

Second Set of Items of Interest	**Description of How Created**
Network topology information	Interconnection of devices 115 on the private LAN deduced from the information in routing and bridging information collected by the LAN crawler 111
Estimated device vendor and model for devices which do not report this information	Device vendor and model for devices 115 deduced from classification server 140
Security Audit	Information reported by the LAN crawler 111 is analyzed for security of configuration and for security incidents and the security posture of the private LAN is summarized in a report
Software License Audit	Information about installation applications is summarized so it can be compared with the number of licenses owned for each software application
Threshold Alerting	Resource utilization information, such as disk usage, is compared with thresholds and if the thresholds are exceeded then the user is notified

[0091] In other embodiments, other types of second set of items of interest can be created from the first set of items of interest received in the reports from the LAN crawlers.

[0092] In another embodiment, the report scanning module 401 and the integration module 402 are used to reorganize the collected information according

to a different organization, such as organized according to the created items of interest that are derived from the first set of items of interest.

[0093] The renaming module 403 is configured to rename similar items having different terminology to have a common terminology for searching purposes. The report scanning module 401 attempts to identify from among the first set of items of interest, received in the reports, similar items having different terminology. The renaming module 403 renames the similar items to have the common terminology. The integration module 402 integrates the collected information of the reports and the renamed similar items into the corresponding search database 121. For example, a workstation running WINDOWS may include a "network adapter" to communicate with other devices 115, while a workstation running Linux may include a "network interface" to communicate with other devices. When searching the private search database 121, a user may provide a search query for all "network interfaces" of the private LAN to be displayed to show the available network interfaces or network adapters that communicate with other devices. Without reorganizing the collected information using the renaming module 403, the search results may not include the "network adapters," even though the user intended the search query to include the "network adapters." The renaming module 403 can rename the collected "network adapter" information to be named as "network interfaces," or vice versa. Also, in other embodiments, the renaming module 403 does not replace the name of the collected information, but adds additional information to the collected information. So for the example above, the "network interface" and "network interface" objects can be modified to include both values as "network interface" and "network interface." Alternatively, the renaming module 403 may rename the collected information to include a class identifier that identifies, for example, both "network interface" and "network interface." Alternatively, the report scanning module 401, integration module 402, and renaming module 403 may be used to otherwise reorganize the collected information to be separately stored in the private search database 121, or in place of the collected information in the private search database 121.

[0094] In another embodiment, the report scanning module 401, the integration module 402, and renaming module 403 are used to reorganize the collected information as described above, such as according to the first set of items of interests and/or according to the second set of items of interest; however, the reorganized information of this embodiment may include common terminology for similar items of the disparate information sources 203 having different terminologies.

[0095] In one embodiment, in order to create network topology information, information is collected from bridging tables from switches of the private LAN 101. For example, the LAN crawler 111 is configured to access the bridging table 304 of the switch 310, illustrated in Figure 3. The LAN crawler 111 can access the bridging table 304 using SNMP, SSH protocol, or the like. In addition, the LAN crawler 111 can access information from the routing tables of the routers of the private LAN, for example, from the routing table 310 of router 201, illustrated in Figure 3. Using the information from the bridging tables and/or routing tables, information about the network topology can be created and integrated into the collected information stored in the private search database 121. The network topology information may be separately stored in the private search database 121 for later retrieval by the user when the user wishes to analyze the network topology of the private LAN. In addition to obtaining the information from the bridging and routing tables, in another embodiment, device names may be retrieved form the DNS server using reverse DNS lookups using the IP addresses. As such, the IP addresses can be linked to the device names. The device names may also be stored in addition to, or in place of, the previously collected information stored in the private search database 121. In another embodiment, information regarding the device types can be obtained, for example, by receiving responses to probes to open ports. Alternatively, other types of information may be collected to create the network topology information.

[0096] The operations of this and other flow diagrams will be described with reference to the exemplary embodiments of the other diagrams. However, it should be understood that the operations of the flow diagrams can be performed by

embodiments of the invention other than those discussed with reference to these other diagrams, and the embodiments of the invention discussed with reference these other diagrams can perform operations different than those discussed with reference to the flow diagrams.

[0097] The techniques shown in the figures can be implemented using code and data stored and executed on one or more computers. Such computers store and communicate (internally and with other computers over a network) code and data using machine-readable media, such as machine storage media (e.g., magnetic disks; optical disks; random access memory; read only memory; flash memory devices) and machine communication media (e.g., electrical, optical, acoustical or other form of propagated signals – such as carrier waves, infrared signals, digital signals, etc.). In addition, such computers typically include a set of one or more processors coupled to one or more other components, such as a storage device, a number of user input/output devices (e.g., a keyboard and a display), and a network connection. The coupling of the set of processors and other components is typically through one or more busses and bridges (also termed as bus controllers). The storage device and network traffic respectively represent one or more machine storage media and machine communication media. Thus, the storage device of a given computer system typically stores code and data for execution on the set of one or more processors of that computer. Of course, one or more parts of an embodiment of the invention may be implemented using different combinations of software, firmware, and/or hardware.

[0098] Figure 5 illustrates an exemplary flow diagram 500 of the LAN crawler 111 of the client device 200 according to one embodiment of the invention. As described above, the LAN crawler 111 is configured to attempt to collect the descriptive information from the multiple disparate information sources 203 through a set of one or more organized questions to the devices 115 of the private LAN being crawled. In particular, the collection module 112 receives values, including descriptive information of the first set of items of interest, in response to the set of organized questions from the disparate information sources 203. As depicted in Figure 5, as part of the flow diagram 500, the LAN crawler 111 of the client device

200 asks a first organized question 501 of a particular LAN device 115. The LAN device 115 responds to the first organized question 501 with a first response value 502. The LAN crawler 111 of the client device 200 then asks a second organized question 503 of the same LAN device 115 or a different LAN device 115. The LAN device 115 response to the second organized questions 503 with a second response value 504. The LAN crawler 111 then integrates the collected information (e.g., organized questions and corresponding response values) into a report, operation 505, and sends the report with the collected information to the hosted on-demand search system 100, operation 506. As described above, the collected information in the report is implicitly organized by nature of asking organized questions and receiving the corresponding response values in response to the organized questions. In another embodiment, the LAN crawler 111 collects information in a non-organized fashion and organizes the collected information before integrating the collected information into the report at operation 505. Also, as described above, the collected information may later be reorganized by the hosted on-demand search server 100 (e.g., reorganization module 126).

[0099] In the embodiment above, two organized questions 501 and 503 were asked of one or more LAN devices 115. In other embodiments, more or less organized questions may be asked of one or more LAN devices 115. The reports may include one or more organized questions and corresponding value(s). In one embodiment, the reports are sent periodically over the Internet to the hosted on-demand search system 100. In another embodiment, the reports are sent once they are integrated with a set of one or more organized questions and corresponding values. Alternatively, the reports may be sent on a scheduled basis. The collected information may be stored temporarily and independently of, or as part of the report, in memory before sending the report to the hosted on-demand search system 100, such as in the data store 230.

[00100] Figure 6 illustrate an exemplary flow diagram 600 of a private search according to one embodiment of the invention. As described above, the server user interface module 124 of the hosted on-demand search system 100 is configured to receive a search query from a user of the private LAN 101 to perform a private

search of the corresponding private search database 121. As part of the flow diagram 600, the user interface 110 of the client device sends an authentication request 601 to the server user interface module 124 of the hosted on-demand search system 100. The server user interface module 124 performs the authentication, in response to receiving the authentication request 601, operation 602. The server user interface module 124, for example, may authenticate the user by looking up user's authentication information stored in the configuration database 125. The authentication information stored in the configuration database 125 may be compared against the user authentication information sent in the authentication request 601. If the user is not authenticated, the server user interface module 124 may send a response to the client device 200 to indicate that authentication failed (not illustrated). However, if the user is authenticated in operation 602, the server user interface module 124 responds to the client device 200 to indicate that the authentication is granted 603. The authentication process may occur every time a user submits a search query, or alternatively, the authentication process may occur when the user first logs on to the hosted on-demand search system 100 using the user interface 110, for example, for each session. Although the authentication process is not necessary to receive a search query from a user, the authentication process may add additional security to the hosted on-demand search system 100.

[00101] Once the user has been authenticated, the user interface 110 can receive a search query from the user, operation 604. Figure 8 illustrates a search GUI 801 of a user interface page 800 on the user interface 110 that includes a first interface widget 802 to receive a search query 803 from the user, operation 604. Once the user has typed in the search query 803, the user may then select, or otherwise activate, a second interface widget 804, to send the search query 803 to the hosted on-demand search system 100, operation 605. The server user interface module 124 receives the search query 803 and processes the search query, operation 606. The operation 606 may include sending the search query 803 to the database interface 122 to perform a private search in the corresponding search database 121 that corresponds to the private LAN from which the user originated the search request. The database interface 122 returns the search results to the server user interface

module 124. The server user interface module 124 may generate the user interface page 800, including include the search results 805, for the search GUI 801. The server user interface module 124 sends the generated user interface page 800, including the search results 805, to the client device 200 to be displayed, operation 607. The client device 200 then displays the user interface page 800, including the search results 805, as part of the search GUI 801, operation 608. In one embodiment, the search results 805 are displayed to look like search results from typical web search engines, such as with a small snippet of information including the context for the matching fields. Alternatively, the search results 805 may be displayed in other ways.

[00102] In one embodiment, the search query 803 is used to retrieve aggregate values, such as the number of devices 115 which are in a wireless access point class (e.g., "wifi_ap"). In another embodiment, the search query 803 is used to retrieve exact matches based on structure, for example, finding all devices on which a particular software application has been installed. This may be useful in knowing how many licenses of the particular software applications are being used on the private LAN, such as for software licensing audits, or the like. In another embodiment, the search query is used to retrieve matches of similar items that use different terminology. In another embodiment, the search query can be modified to refine a search, such as by clicking on aspects of a search result to refine the search, or to focus on the detailed information about the resource found.

[00103] In one embodiment, the search query 803 can be designated as shareable with other users, even users outside of the private LAN in which the user is conducting the private search. As illustrated in Figure 8, the search GUI 801 includes a third interface widget 806 that allows a user to designate the search query 803 as shareable. Once the user has designated the search query 803 as shareable, when the user selects, or otherwise activates the second interface widget, the designation information is sent with the search query 803 to the server user interface module 124. The server user interface module 124 stores the saved search query 803 in the configuration database 125 for later retrieval by the user or by other uses in, or outside, the private LAN. It should be noted that the server user interface

module 124 is configured to store the search query 803 when designated as shareable, but not the search results 805. By designating the search query 803 as shareable, the server user interface module 124 is able to allow display and selection of the stored search query 803 by another user, for example, users of a different private LAN. In another embodiment, additional interface widgets may be used, such as, for example, one to designate a search query as shareable with the user's colleagues, another to designate a search query as shareable with a community, and another to designate a search query as shareable with the public. Once the interface widgets have been selected, another interface widget can be selected to save the search query or queries.

[00104] Although the embodiment above describes sending the search query 803 that is received from the user in operation 604, alternatively, the search query that is sent in operation 605 may also be a saved search query that is stored on the client device 200. Alternatively, instead of sending the search query 803 in operation 605, the client device 200 may send a request to perform a private search based on a saved search query that is stored on the hosted on-demand search system 100.

[00105] In one embodiment, as illustrated in Figure 8, the user interface 110 may display a user interface page 850 that includes a dashboard GUI 851. As described above, a dashboard is a GUI widget that can be part of the user interface page 850, and can be configured and saved by the user to display search results in various forms for saved search queries. For example, the user interface page 850 includes three dashboard panels 860, 870, and 880. The first panel 860 includes the saved search query 861, and displays the updated search results 862 in the form of a list when the dashboard GUI 851 is refreshed (e.g., when the user first accesses the dashboard and/or periodically thereafter). The second panel 870 includes the saved search query 871, and displays the updated search results 872 in the form of a chart when the dashboard GUI 851 is refreshed. The third panel 880 includes the saved search query 881, and displays the updated search results 882 in the form of a table when the dashboard GUI 851 is refreshed. Each of the dashboard panels 860, 870, and 880 may include updated search results for separate saved search queries, or alternatively, for the same search queries.

[00106] As described above, the collection of dashboard panels 860, 870, and 880 may include saved configurations of the dashboard (e.g., search queries, such as the placement on the dashboard panels on the dashboard GUI, the number of search results to display, the form to display the search results, or the like). These configurations may be stored for each user on the multiple private LANs. In one embodiment, the dashboard configuration of the dashboard GUI 851 can be designated as shareable to be shared with users of the same or different private LANs. For example, the dashboard GUI 851 may include an interface widget 852, which when selected, or otherwise activated, designates the dashboard to be shareable. The dashboard configuration may be saved locally on the client device 200 (e.g., in data store 230), and/or sent to the hosted on-demand search system 100 to be stored in the configuration database 125 for later retrieval by the user and/or users of the same or different private LANs. In one embodiment, the user may save the dashboard configuration with a saved search query so that when the user logs in, the dashboard GUI 851 is displayed with updated search results for the saved search query without having to manually enter the search query again.

[00107] Although the embodiment above includes a single interface widget 852 to designate the dashboard configuration of the dashboard GUI 851, in other embodiments, the configurations of the dashboard panels 860, 870, and 880, can be individually or collectively saved for later retrieval by the user and/or other users of the same private LAN or different private LANs.

[00108] Figure 7 illustrates an exemplary flow chart of a method 700 of operations between the client device 200 and the hosted on-demand search system 100 according to one embodiment of the invention. The method 700 may start with a user on the client device 200 requesting the LAN crawler 111 from the hosted on-demand search system 100. This request may be made by the user through an Internet browser, or otherwise, to the distribution module 127 of the server user interface module 124. For example, the user, visiting a website hosted by the company or organization that manages the hosted on-demand search system 100, may click on a link to download the LAN crawler 111 to the client device 200. The

LAN crawler 111 may also be provided in other forms, such as on a compact disc, or the like.

[00109] On the client side, the user then installs the LAN crawler 111 on the client device 200 of the private LAN 101, operation 701. As described above, the LAN crawler 111 automatically and repeatedly collects private data stored on the devices 115 of the private LAN 101 using the LAN crawler 111, operation 702; automatically organizes the collected information, operation 703; and automatically reports the organized information to the hosted on-demand search system 100, operation 704. As described above, the LAN crawler 111 may collect from multiple disparate information sources, only those parts of the disparate information sources that include descriptive information of the first set of items of interest. These items of interests may be collected from the multiple disparate information sources 203. Also, the LAN crawler 111 may be configured to organize the collected information by using organized questions. The LAN crawler 111 may also organize the collected information using the organization module 114. After the user has installed the LAN crawler 111 and the LAN crawler 111 has started to report the collected information to the hosted on-demand search system 100, the user requests the user interface 110 from the hosted on-demand search system 100, operation 705. This may be done by the user accessing a website and logging into an account using a username and password. Alternatively, the user may request the user interface 110 in other ways, such as launching an application that requests and displays the user interface 110.

[00110] On the server side, the hosted on-demand search system 100 receives the reports from the client device 200, operation 706. Based on the received reports, the hosted on-demand search system 100 creates and synchronizes a private search database 121, operation 707. The hosted on-demand search system 100, upon request (e.g. operation 705), provides the user interface 1110, such as the search GUI 801, to the client device 200, operation 708. The user interface 110 allows the user to perform one or more private searches of the private search database 121.

[00111] In one embodiment, once the LAN crawler 111 has been installed, the operations 702-704 on the client side, and operation 706 and 707 on the server side

may be performed automatically and repeatedly. For example, the LAN crawler 111 may be configured to automatically and repeatedly collect the private data from devices 115 of the private LAN 101. This may be configured to be periodic at scheduled intervals, to be continuous, to be only in response to discovery of new devices 115 on the private LAN, or the like. In another embodiment, once the LAN crawler 111 has been installed, the operations 702-704 may be performed manually in response to a user request.

[00112] On the client side, using the provided user interface 110, the client device 200 receives a search query from a user, operation 709. For example, the user may type in a search query 803 in the first interface widget 802. Alternatively, the user may select a saved search query 803, such as from a drop-down list of saved searches. The drop-down list may include search queries that are already included in the hosted on-demand search system 100, search queries that the user has previously saved, search queries that user's colleagues has previously saved, search queries that have been previously saved by the community, or the like. The user may designate the search query as shareable to be shared with other users, including users of other private LANs, operation 710. The user may designate the search query 803 by selecting the third interface widget 806, which may be a check box, a radio button, or the like. Alternatively, the user may chose to not designate the search query 803 as shareable, keeping the search query 803 private to the private LAN 101. The user then selects, or otherwise activates, the second interface widget 804, which sends the search query to the hosted on-demand search system 100, operation 711.

[00113] On the server side, the hosted on-demand search system 100 receives the search query from the client device 200 to search the private search database, operation 712. The hosted on-demand search system 100 performs a private search in the corresponding private search database 121 using the search query, operation 713. The hosted on-demand search system 100 returns the search results of the private search to the client device 200 in a user interface page, operation 714. For example, the hosted on-demand search system 100 generates the user interface page 800 that includes the search results 805 and sends the generated page to the client

device 200 to be displayed. The hosted on-demand search system 100 also stores the search query, for example, in the configuration database 125, operation 715.

[00114] On the client side, the client device 200 receives the generated user interface page with the search results and displays the user interface page to the user, operation 716. The user may then review the search results, modify the search query to perform an additional search, search for additional items within the search results, type in another search query, save the search query, or the like. The user may also designate the search query as shareable after the user has received the search results. For example, the user may select the third interface widget 806 to designate the search query 803 as shareable. The user interface may send a request to the hosted on-demand search system 100 to modify the saved search query 803, which was previously stored in the configuration database 125, to be designated as shareable, instead of private.

[00115] Although the operations of Figure 7 have been described and illustrated as performing a private search in response to a search query received from a user, in other embodiments, private searches may be performed in response to saved search queries, such as saved search queries of a dashboard GUI. For example, upon launching the dashboard GUI 851, the client device 200 sends the saved search queries 861, 871, and 881 to the hosed on-demand search system 100, performs the corresponding private searches using the search queries 861, 871, and 881, returning the updated search results 862, 872, and 882 to be displayed in the dashboard panels 860, 870, and 880, respectively. Also, the dashboard panels 860, 870, and 880 or the dashboard GUI 851 may be designated as shareable (e.g., selecting the interface widget 852). The user interface may send a request to the hosted on-demand search system 100 to save, and designated as shareable, the dashboard configurations in the configuration database 125 for later retrieval by the user and other uses, including users of other private LANs. The configuration of the dashboard panels 860, 870, and 880 or the dashboard GUI 851 may be modified before or after the private searches have been performed. If performed after the private searches have been performed, an additional request may be sent to designate the previously saved dashboard configuration as shareable.

[00116] Figure 9 illustrates an exemplary embodiment of a private search database that is a hierarchical database that stores the collected information in a tree structure according to one embodiment of the invention. In Figure 9, the data of hierarchical database 110 is organized into a tree structure. Each data element (i.e., not a value) on the tree is a node of the tree. Each node on the tree has a corresponding unique identifier (e.g., a node identifier). For example, network node 902 has a unique identifier of two. At the top of the tree structure is the root node 900 of the tree, which is represented by the symbol `/`. The node can be described by a unique path, where each branch of the tree corresponds to a slash (/) in the path. For example, the path may be `/network/device/interface/name`. Directly below the root node exists two child nodes, network 902 and directory 972. A child node is a node, not a value, that itself descends from a node (e.g., a parent node or root node). Each parent node can have many child nodes, but each child node only has one parent. A child node may also be a parent node. For example, network 902 and directory 972 each are parent nodes in addition to being child nodes because they include one or more child nodes.

[00117] In addition, network 902 and directory 972 are each root nodes of a sub-tree. A sub-tree is a subset of the tree. A sub-tree includes information starting at the sub-tree root node and traversing through each child node of the sub-tree root node and ending with at least one value. Any node on the tree that itself has nodes below it (e.g., a parent node) can be referred to as a sub-tree root node. Thus, each sub-tree may include other sub-trees (i.e., the sub-trees may be nested within a sub-tree). There are many sub-trees in Figure 9. For example as previously described, a sub-tree where network 902 is the sub-tree root node includes all the information, including values, from the nodes device 904, device 906 (which includes the node manufacturer 928), and device 908. As an example of a nested sub-tree, device 904 is a sub-tree root node for the sub-tree that includes all the information, including values, from the nodes manufacturer 910, interface 912, and interface 914. The interface 912 node includes the MAC Address 916, Name 918, Status 920, and the interface 914 node includes MAC Address 922, name 924, and Status 926. As another example of a nested sub-tree, device 908 is a sub-tree root node for the sub-

tree that includes all the information, including values, from the nodes interface 930, interface 936, manufacturer 944, names 932, 934, 938, and status 940. As another example of a nested sub-tree, the directory 972 includes the nodes users 974 and users 976, which include the nodes name 978 and names 980, respectively.

[00118] Values are associated with leaf nodes. For example, the node manufacturer 910 is a leaf node because it is associated with the value 910 'Dell Corporation'. While in one embodiment of the invention values are only associated with leaf nodes, in alternative embodiments of the invention any node in the hierarchy can have values associated with that node.

[00119] In one embodiment, the LAN crawler 111 collects information about the private LAN being crawled (e.g., network assets) and sends it to the hosted on-demand search system to be stored in the private search database, which stores the data in a tree-structured format. As illustrated in Figure 9, the collected information is visually represented in an inverted tree structure with the root at the top, and each data element as a node on the tree. The hierarchical database is useful because it provides the flexibility to scale and the ability to group related information and display the relationships.

[00120] The hierarchical database provides the ability to provide quantitative answers to questions, such as questions regarding IT information of a private LAN. The LAN crawler 111 collects information in an organized manner that lends itself to be stored in a tree structure. The hierarchical database may maintain the organization or structure of the information collected by the LAN crawler 111. For example, if you search the private search database for 'Tetris', a full-text search algorithm finds every instance of 'Tetris', including a computer named 'Tetris' and a software program named 'Tetris.' Because the LAN crawler knows how it collected the information for each, including how to identify the computer which has the name, and the network to which that computer belongs, and the identity of the computer which has the software installed, this organization can be maintained in the private search database using a hierarchical database. Using the hierarchical database, the hosted on-demand search system can know the difference between the

computer named 'Tetris' and a software program named 'Tetris,' because of the relationships between the computer and the software in the hierarchical database.

[00121] As many database users are familiar with SQL, according to one embodiment of the invention the hierarchical database is searched with a query syntax that is familiar to SQL uses. For example, Figure 10 illustrates exemplary search syntaxes for searching a hierarchical database according to one embodiment of the invention. For example a simple hierarchical database search query syntax may take the form of `SELECT * FROM /Network`. Similarly to SQL, the `SELECT` clause in the query is used to specify the data returned subject to the `FROM` clause. In the above simple example, the asterisk indicates that everything in the hierarchical database is to be returned subject to the `FROM` clause (e.g., the network node). In the case of a tree, everything in the tree will be returned subject to the `FROM` clause. Also similar to SQL, the `FROM` clause describes from where in the database information should be returned. In the case of a tree, the `FROM` clause represents which sub-tree the data will be searched from. Also similar to SQL, a `WHERE` clause may be used to specify the selection. In other words, the `WHERE` clause restricts or filters the data returned. An example of a search query with a `WHERE` clause is `SELECT * FROM /Network/Device WHERE Interface/Name = 'eth0'`. It should be understood that the above search syntaxes are exemplary and that many other syntaxes as known in the art to search a hierarchical database may be used.

[00122] According to another embodiment of the invention, the private search database illustrated as a hierarchical database in Figure 9 also may be used to generate data in an unstructured database (e.g., an inverted index, a forward index, a trie, a vector space model, etc.). For example, virtual documents may be created from the hierarchical database. A virtual document is used to refer to representation of data as textual data that may be indexed into an unstructured database. Referring to Figure 9, the virtual documents that are created are represented by the dashed lines. Once virtual documents are created, the unstructured database and the hierarchical database may be searched with a single search query to allow keyword based searching of the unstructured database while retaining the searching of the

hierarchical database. For example, the single search query may take the form of `SELECT * FROM %Dell%` where the unstructured search string `%Dell%` is used to search the unstructured database (e.g., the virtual documents within the unstructured database) for the string 'dell'. As there are two virtual documents that include the term 'Dell', both of the sub-trees representing those virtual documents are returned as a result.

[00123] For example in one embodiment of the invention the data stored in a hierarchical database includes information regarding substantially all devices within a private LAN, a list of software installed on those devices, and a list of users authorized to use those devices. Additionally, the data stored may include information regarding the operating system version installed on substantially all devices within the private LAN, the software which is running on substantially all devices within the private LAN, and a configuration file from at least one router, switch, or firewall within the private LAN. The devices may include substantially all workstations within a private LAN, substantially all routers within the private LAN, substantially all switches within the private LAN, substantially all servers within the private LAN, substantially all firewalls within the private LAN, and substantially all directory servers within the private LAN.

[00124] Figure 11 illustrates an exemplary hosted on-demand search system 1100 coupled to the multiple private LANs 101, 102, and 103 and to one or more hosted application services 1120. The hosted on-demand search system 1100 is similar to the hosted on-demand search system 100 described above, except the hosted on-demand search system 1100 includes support for hosted application services 1120. As illustrated in Figure 11, users 1101 of the private LAN 101 interacts with the hosted on-demand search system 1100 through the user interface 1103 (e.g., the user interface 110(1)) to access the private search databases 1121 (e.g., 121(1)) on the set of one or more centralized-search server 1120 (only one illustrated for ease of illustration). Similarly, other users 1102 of other private LANs, such as private LANs 102 and 103, interact with the hosted on-demand search system 1100 through the user interface 1103 (e.g., user interfaces 110(2) and 110(3)) to access the private search databases 1121 (e.g., 121(2), and 121(3)). Since the hosted on-demand

search system 1100 includes support for add-on applications, one or more applications providers 1104 can also interact with the hosted on-demand search system 1100 through an application interface (API) 1105. Add-on applications of the application providers 1104 can be created by an entity that operates and hosts the hosted on-demand search system 1100, or alternatively, by third-party entities. The add-on applications may be used to extend the functionality of the hosted on-demand search system 1110, by adding specific functionality through the user interfaces. For example, one add-on application, as described above, collects network topology information and generates a network topology map to be displayed to the user. The network topology map provides, for example, a visual representation of the devices 115 of the private LAN and the interconnections between the devices 115.

[00125] The add-on applications of the application providers 1104 may be local add-on applications that reside on the hosted on-demand search system 1100, or alternatively, remote add-on applications that reside on a remote server or on a device of the private LAN. For example, if the add-on application is created by a third party, then the application logic may be run on a remote server. The add-on applications of the application providers 1104 can include application logic to query information in the private search databases 1121. The add-on applications of the application providers 1104 can also include application logic to add information to the private search databases 1121, such as inserting additional data to be stored within, or in place of the collected information stored in the private search databases 1121. In another embodiment, the add-on applications reside on a client device of the private LAN. In this embodiment, the add-on applications access the collected information on the hosted on-demand search system 1100 using an API, like the API 1105 described herein. For example, the user 1101 may generate an add-on application, and/or a specific plug-in for the LAN crawler, and run the add-on application on the client device to access the collected information that has been collected and privately stored in the private search database 1121. This is different than a private search engine that collect information from only the client device, because the specific plug-in for the LAN crawler can collect information not only

from the client device, but from other devices of the private LAN. Also, the private search engine stores the collected information on the client device, where the add-on application would access collected information that is hosted by the hosted on-demand search system 1100.

[00126] In one embodiment, the user interface 1103 provides user interface pages with an application view, such as in an application panel. The user interface 1103 can request the application view from the on-demand search system 1100, which interacts with the applications via the API 1105 to generate the content to display in the application view to the user. The add-on applications, using the API 1105, access the collected information to generate the content for the application view. The application view can be a dashboard GUI that is part of a user interface page, a user interface page, or the like. The add-on applications may be used to provide visualization of the collected information. It should be noted that the add-on application can perform specific queries to access the collected information stored in the private search database, as well as perform searches of the collected information using search queries, and can render an application component that is representative of the search results, or alternatively, an application component that is not related to the search results. For example, an add-on application can render the current temperature of a zip code specified by a user, or the add-on application can render a network topology map, which is based of the accessed information. In one embodiment, the add-on application reads data from the private search database 1121, using specific queries or search queries, processes the returned data, and renders a result to the user that includes the processed data. In one embodiment, the result is a graphical representation of the processed data. Alternatively, the result is not a graphical representation, but merely the data in a list, a table, or the like.

[00127] Also, as described below, the hosted on-demand search system 1100 includes support to allow the add-on applications of the application providers 1104 to affect how the LAN crawler collects information from the private LAN being crawled. In one embodiment, the LAN crawler is an extensible crawler, as described below. The hosted on-demand search system 1100 may allow the LAN crawler to be extended to include specific plug-ins that attempt to collect additional

descriptive information that may be used by the add-on applications. The add-on applications may provide the additionally collected information to the user and/or provide visualization of the additionally collected information to the user. As such, the specific plug-ins can be used to collect specific information that is used by the add-on applications. For example, an add-on application that processes Netflow data may add a specific-plug-in to the LAN crawler to collect NetFlow information from routers. NetFlow is an open, but proprietary network protocol, developed by Cisco Systems to run on Cisco Internetwork Operating System (IOS)-enabled equipment for collecting IP traffic information.

[00128] According to one embodiment of the invention, a private search database that is a hierarchical database is extended for an add-on application. Once traditional relational databases based on tables have been set up, the relational databases often tend to be rigid and hard to extend. Hierarchical databases that store the collected information in a tree structure, however, are more flexible than the relational databases and can be easily extended.

[00129] As previously described, the LAN crawler 111 may be extended by specific-probing plug-ins that collect the descriptive information according to one or more probing requirements that are specific to add-on applications of application providers. These add-on applications may provide additionally collected information to the user and/or provide visualization of the additionally collected information to the user. In the case of a hierarchical database, the hierarchy of the tree is extended by adding a sub-tree corresponding to the application provider and the add-on application. For example, in one embodiment of the invention, a new sub-tree from the root of the tree is added for each application provider in the private search database. In one embodiment, the application providers can extend the tree under an 'enterprise' node, using their reversed domain name to uniquely identify the new sub-tree. For example, the Acme Corp extends the tree under: `/enterprise/com/acme`. The information that is collected from the specific-probing plug-in that corresponds to the application provider's add-on application is stored under this new sub-tree. If an application provider has more than one add-on application, each add-on application may have its own sub-tree branching from the

sub-tree that corresponds to the application provider. For example, for an add-on application that processes Netflow data, the hierarchy of the tree is extended by adding a sub-tree corresponding to the application provider that created this add-on application.

[00130] Figure 12 illustrates an exemplary hosted on-demand search system 1100 coupled to a private LANs over a network with support for add-on applications according to one embodiment of the invention. The components of the hosted on-demand search system 1100 are similar to the components of the hosted on-demand search system 100 as indicated by similar reference numbers. Descriptions of these components have not been included in the present embodiments. It should also be noted that the embodiments above are described with respect to multiple private LANs, where the embodiment described below are described with respect to a single private LAN 101. Although described with respect to a single private LAN, the embodiments may also be implemented with a hosted on-demand search system that interacts with multiple LANs.

[00131] As described above, the add-on applications can be local add-on applications, such as local add-on applications 1228 that are run on the centralized-search server 1120, or remote add-on applications, such as remote add-on applications 1241 that run on the remote server(s) 1240. As noted above, the remote add-on applications may also be run on a client device of the private LAN 101, but hereinafter, the remote add-on applications are described as running on the remote server(s) 1240. Both the local add-on applications 1228 and the remote add-on applications 1241 access the collected information stored in the private search database 1121 through an API 1221. In one embodiment, the add-on applications (1228 or 1241) are third-party add-on applications. The third-party add-on application is executed by the remote server 1240 and the third-party add-on application communicates with the server user interface module 1224 through the API 1221. In one embodiment, a third-party add-on application is configured to submit additional data to the API 1221 to be stored in the private search database 1121. In another embodiment, a third-party add-on application is configured to access information from the private search database 1121 through the API 1221.

The third-party add-on application may also perform searches in the private search database 1121 through the API 1221. As such, the API 1221 facilitates access to the collected information stored in the private search database 1121 for the add-on applications 1228 and 1241.

[00132] The API 1221 is also used as an interface between the database interface 122, the configuration database 125, the server user interface 1224, and the local and remote add-on applications 1228 and 1241. As described above, the database interface 122 creates and synchronizes the private search database 1121 for the private LAN 101 based on the reports received at the crawler interface 123 from the LAN crawler 111. The private search database 1121 stores the collected information from across the multiple disparate information sources 203 stored on the devices 115 of the private LAN 101. It should be noted that the collected information is not organized according to the documents located on the devices 115, but is organized according to the first set and/or second set of items of interest. The server user interface module 1224 provides a user interface 1210 over the network 130 (e.g., Internet) to the private LAN 101, and provides an application rendered component, such as application panel 1212 of a dashboard GUI 1211, as part of the user interface 1210.

[00133] In one embodiment, the server user interface module 1224 includes an application rendering module 1227 and a user interface rendering module 1226. The application rendering module 1227 is configured to render an application rendered component, generated by the add-on application, to be displayed in the user interface 1210. In one embodiment, the application rendered component represents the search results of a private search by the add-on application (1228 or 1241). The user interface rendering module 1226 is configured to generate a user interface page including the application rendered component to be displayed in the user interface 1210. The user interface rendering module 1226 may include logic to generate the user interface page, such as view logic, controller logic, and model logic. Alternatively, other types of logic may be used to generate the user interface page. The various types of logic used in generating user interface pages are known

to those of ordinary skill in the art, and the detailed description regarding their operations has not been included so as to not obscure the present embodiments.

[00134] In one embodiment, the configuration database 125 is configured to store authentication information for access via the remote add-on application 1241 (e.g., third-party add-on application. In another embodiment, the configuration database 125 is configured to store a configuration of the application rendered component, including the corresponding search query for later retrieval by the user 1101 or other users 1102 of other private LANs. Alternatively, the configuration database 125 may also store search queries, application configurations for particular users, user authentication information, or the like.

[00135] In another embodiment, a hosted on-demand search system 1100 includes a classification server (e.g., a classification server 140) is coupled to the centralized-search server 1120 and a classification database (not illustrated in Figure 12). As described above, or the classification server is configured to compare the collected information of the private search database 1121 against predetermined characteristics of known devices, and to compute a classification metric for each of the devices 115 of the private LAN 101.

[00136] Figure 13 illustrates an exemplary extensible LAN crawler 1310 according to one embodiment of the invention. The extensible LAN crawler 1310 includes similar components as the LAN crawler 111, as described above, except the LAN crawler 1310 is extensible in that it can include specific-probing plug-ins 1310 to collected additional descriptive information according to a set of probing requirements that are specific to each of the specific probing plug-ins 1310. Like the collection module 112 described above, the collection module 1312 is configured to attempt to collect from across each of the disparate information sources 203 stored in the devices 115, only those parts of the disparate information sources that include descriptive information of a first set of items of interest. The collection module 1312 also includes a discovery module to discover the existing devices 115, as described above, and new devices 1315 of the private LAN 101, and a generic probing module 1302, to attempt to collect the descriptive information from the disparate information sources 203 stored on the device 115 and new

devices 1315 according to a first set of probing requirements. For example, the discovery module 1301 discovers the new devices 1315, such as by scanning network traffic as described above, and sends a request to the generic probing module 1302 to start collecting information from the new devices 1315 according to the first set of probing requirements. The first set of probing requirements may include one or more organized questions to be asked of the new devices 1315, such as name of device, type of device, or the like. The first set of probing requirements includes generic requirements that are not specific to any particular device.

[00137] The specific-probing plug-ins 1310 are each coupled to the collection module 1312, and attempt to collect descriptive information from the disparate information sources 203 stored on the device is 115 (including the new devices 1315) of the private LAN 101. Each of the specific-probing plug-ins 1310 attempts to collect the descriptive information according to a second set of probing requirements that are specific to each of the specific probing plug-ins 1310. In one embodiment, one of the specific-probing plug-ins 1310 attempts to collect descriptive information according to one or more probing requirements that are specific to the local or remote add-on applications 1228 and 1241.

[00138] The specific probing plug-ins 1310 may be one of three types of plug-ins, namely periodic plug-ins 1311, device plug-ins 1312, or hybrid plug-ins 1313. The periodic plug-ins 1311 attempt to collect the descriptive information from at least one of the devices 115 of the private LAN 101 periodically. For example, the plug-in 1321 is configured to collect specific information from the directory server 330, such as using LDAP periodically. In this example, the plug-in 1321 only periodically collects information from the single information source, but in other embodiments, the periodic plug-ins 1311 are configured to collect information from one or more information sources periodically. The device plug-ins 1312 attempt to collect the descriptive information from at least one of the devices 115 of the private LAN 101. In one embodiment, the device plug-ins 1312 are configured to collect information from newly discovered devices, such as the new device 1315. For example, when a new device is discovered by the discovery module 1301, each of the device plug-ins 1312 are configured to attempt to collect information from the

new device 1315 according to each of their specific probing requirements. For example, a plug-in 1323 attempts to collect information from the WMI database 323 on the new device 1315. If the new device 1315 does not include the WMI database 323 the plug-in 1323 does not collect information from the new device 1315. However, if the new device 1315 includes the WMI database 323, then the plug-in 1323 collects information from the WMI database 323 of the new device 1315. In another embodiment, the device plug-in 1324 attempts to collect information from the registry 322 of the new device 1315, when the new device 1315 has been discovered by the discovery module 1301. Similarly the device plug-in 1325 attempts to collect information from the directory 316 of the new device 1315, when the new device 1315 has been discovered by the discovery module 1301. If the new device 1315 does not include registry 322 or the directory 316, the plug-ins 1324 and 1325 do not collect information from the new device 1315; however, if the new device 1315 includes one or the other, or both, the registry 322 and the directory 316, the plug-ins 1324 and 1325 collect information from the registry 322 and/or the directory 316 of the new device 1315.

[00139] In another embodiment, the device plug-ins 1312 attempt to repeatedly collect information from already existing devices 115 of the private LAN 101. In another embodiment, the device plug-ins 1312 attempt to collect information from devices that have been identified as a specific type of device according to a set of one or more probing requirements that are specific to the identified device. In another embodiment, the device plug-ins 1312 attempt to collect information from at least one of the devices 115 according to specific probing requirements of a specified type of information source, such as a directory server, a WMI database, a registry, a directory, a router, or the like.

[00140] The hybrid plug-ins 1313 may be configured to collect the descriptive information from the devices 115 both as a periodic plug-in and as a device plug-in, as described above. For example, the plug-in 1322 may be configured to collect information from the router 210 as a device plug-in when the router 210 has been discovered by the discovery module 1301. The plug-in 1322 may also collect information periodically from the router 210. In one embodiment, the plug-in 1322

is configured to collect firewall configuration settings from the router 210. This may be done initially as a device plug-in, and subsequently as a periodic plug-in. Alternatively, the device plug-ins 1323, 1324, and 1325 may also be configured to be hybrid plug-ins 1313 or periodic plug-ins 1311, and the periodic plug-in 1321 may also be configured to be a hybrid plug-ins 1313 or a device plug-in 1312.

[00141] Once the information has been collected by each of the specific-probing plug-ins 1310, the collected information is sent to the reporting module 113 to be sent in reports out of the firewall of the private LAN and over the Internet 130 to the centralized-search server 1120. In one embodiment, the collected information is organized by the organizing module 114. In another embodiment, the information is collected in an organized manner, such as using organized questions, and does not need to be organized by the organizing module 114, as described above.

[00142] In one embodiment, the specific-probing plug-ins 1310 include specific probing requirements that are specific to an add-on application (e.g., local or remote add-on applications 1228 and 1241). The specific-probing plug-ins 1310 collect additional information that can be used by the add-on application. This may improve the hosted application services 1120.

[00143] Figure 14 illustrates an exemplary hosted application service 1120. In this embodiment, a firewall rule plug-in 1401 is configured to collect information regarding the firewall configuration settings of the private LAN 101, as a firewall rule collector. In one embodiment, the firewall rule plug-in 1401 is the hybrid plug-in 1322 of Figure 13. Alternatively, the firewall rule plug-in 1401 may be a periodic plug 1311 or a device plug-in 1312 as described above. The collected information is reported to the private search database 1121 on the hosted on-demand search system 1110. The collected information can then be accessed by an add-on application that includes a firewall rule checker 1402. The firewall rule checker 1402 may be a remote add-on application 1241, or alternatively, a local add-on application 1228. Alternatively the hosted application services 1120 may include other types of add-on applications, and other types of specific probing plug-ins that collect information that is specific to the other types of add-on applications.

[00144] Figure 15 illustrates an exemplary flow diagram 1500 of an application search according to one embodiment of the invention. As described above, the server user interface module 1124 of the hosted on-demand search system 1100 is configured to receive a search query from an add-on application to perform a private search of the private search database 1121. In one embodiment of the application search, the client device 200 requests that the hosted on-demand search system 1100 shows the dashboard GUI 1211, including the application panel 1212, on the user interface 1210, operation 1501. In response, the host on-demand search system 1100 requests that the remote server 1240 render the application panel 1212, operation 1502. In order to render the application panel 1212, the remote server 1241 sends an API request to the hosted on-demand search system 1100 to perform a database fetch in the private search database 1121, operation 1503. The API request in operation 1503 may include a search query, or alternatively, a specific query to fetch specific information from the private search database 1121. The API 1221 sends the API request to the database interface 1121 to perform the database fetch in order to obtain the requested information from the private search database 1121. In one embodiment, the hosted on-demand search system 1100 authorizes the API request before performing the database fetch, for example, by accessing authorization information in the configuration database 125. The API request may include third-party authorization information that is compared to the authorization information stored in the configuration database 125. If the third-party authorization information matches the authorization information stored in the configuration database 125, the API request is authorized, and the database fetch is performed, operation 1504. Once the API 1221 receives the database fetch results. The database fetch results are sent to the add-on application of the remote server 1240, operation 1505. Using the database fetch results, the add-on application generates application panel 1212, operation 1506, and sends the application panel 1212 to the hosted on-demand search system 1100 to be rendered in the user interface, operation 1507. Subsequently, the hosted on-demand search system 1100 generates the user interface page with the application panel 1212, operation 1508, and sends the user interface page to the client device 200 to be displayed, operation

1509. The client device 200 then displays the user interface page with the application panel 1212.

[00145] In one embodiment, the add-on application is configured to send the search request to the API 1221 to perform a private search of the private search database 1121 to extract LAN-centric network topology information for the private LAN 101. Using the LAN-centric network topology information, the add-on application creates a network topology map to be displayed on the user interface 1210, such as the network topology map 1611 of Figure 16 in the application panel 1210. The network topology map 1611 is a visual representation of the collected LAN-centric network topology information. The add-on application sends the network topology map 1611 to the server user interface module 1124 to render the network topology map 1611 as part of the application rendered component in the user interface 1210. The server user interface module 1124 generates the user interface page, such as the user interface page 1600, which includes the dashboard GUI 1211. The user interface page 1600 includes the three dashboard panels 860, 870, and 880, as described above, and the application panel 1210. The user interface page 1600 may also include the interface widget 852 to designate the dashboard as shareable, as well as another interface widget 1652 to save the dashboard. As described above, when the interface widget 1652 or 852 are selected, or otherwise activated, the user interface 1210 sends the dashboard to the hosted on-demand search system 1110 to be saved in the configuration database 125, and/or to be designated as shareable or not.

[00146] In one embodiment of displaying the network topology map 1611, the hosted on-demand search system 1110 receives a first request from the private LAN 101 to display the network topology map 1611 to be displayed on the user interface 1212. The hosted on-demand search system 1110 sends a second request to the add-on application (e.g., local add-on application 1228 or remote add-on application 1241) to generate the application rendered component that includes the network topology map 1611. The hosted on-demand search system 1110 receives one or more requests from the add-on application to perform one or more queries to the private search database 1121 for LAN-centric network topology information. The

hosted on-demand search system 1110 authorizes the one or more queries using application authorization information stored in the configuration database 125. The hosted on-demand search system 1110 sends the query results to the add-on application, and the add-on application generates the network topology map 1611 based on the collected LAN-centric network topology information. The network topology map 1611 is then sent to the hosted on-demand search system 1110 and the hosted on-demand search system 1110 generates the page with the network topology map 1611 as part of the user interface provided to the private LAN 101.

[00147] In another embodiment, the network topology map 1611 is generated based on other collected information than LAN-centric network topology information, such as non-LAN-centric information.

[00148] Although the embodiments above described generating the network topology map 1611 as the application rendered component, alternatively, the application rendered component can be any type of rendered component by the add-on application, such as text, charts, tables, graphs, diagrams, or the like. The rendered component can be related to, or unrelated to, the collected information that is stored in the private search database 1121.

[00149] Figure 17 illustrates an exemplary dashboard page 1700 according to one embodiment of the invention. The dashboard page 1700 includes a browser-based user interface page that includes multiple dashboard panels 1701, 1702, and 1703. The dashboard page 1700 displays the network topology map 1611 in the dashboard panel 1701. As described above, the network topology map 1611 represents LAN-centric network topology information that is stored in the private search database 1121. The dashboard panel 1701 may be configured to allow the user to change the view of the network topology map 1611, such as zooming in and out, changing the field of view of the network topology map 1611, highlighting objects in the network topology map 1611 to display additional information about the object, such as name of a device, IP address of the device, or the like. The dashboard page 1700 also displays the recent memory use of the private LAN 101 in dashboard 1702, and the supporting IDs in the dashboard panel 1703. The recent memory use may be generated from a saved search query associated with the dashboard panel 1702, as

described above with respect to Figure 8. For example, upon opening the dashboard page 1700, the user interface sends the saved search query for the recent memory usage to the hosted on-demand search system 1100, and the hosted on-demand search system 1100 generates the dashboard panel 1702 using the search results of the saved search query. In other embodiments, the dashboard page 1700 is configured to display other types of information in the dashboard panels 1701, 1702, and 1703.

Another Embodiment of the Invention

[00150] Having described embodiment(s) of the invention, alternative embodiment(s) will now be described. Like the previous embodiment(s), these alternative embodiment(s) allow for hosted searching of information with support for add-on applications and/or extensible crawling. However, unlike the previous embodiment(s), these embodiment(s) allow for hosted searching information for information that is not limited to private LAN information, as described above but may include other types of information, such as financial information, enterprise information, traffic statistics from web-sites, transaction statistics from a database system, trading volumes from a stock trading application, resource usage and resource availability in a MRP system or a Enterprise Resource Planning (ERP) system, sales forecast information from a customer relationship management (CRM) system, or the like.

Alternative Embodiments

[00151] While embodiments of the invention has been described in relation to collecting private LAN information stored on devices of a private LAN, such as technical information from devices of the private LAN, other embodiments may include collecting other types of information, as described above, from other types of information sources on devices of public networks, private and public networks, or the like. Therefore, embodiments of the invention are not limited to collecting private LAN information. In addition, while embodiments of the invention have been described in relation to technical information stored in devices of the private LAN, alternative embodiments could be implemented such that other types of information may be collected from information sources of devices of public

networks, private and public networks, or the like. Such an embodiment could be implemented by having the LAN crawler ask one or more questions of the devices to collect the other types of information. This may be done using one or more specific-probing plug-ins as described herein.

[00152] For example, while the flow diagrams in the figures show a particular order of operations performed by certain embodiments of the invention, it should be understood that such order is exemplary (e.g., alternative embodiments may perform the operations in a different order, combine certain operations, overlap certain operations, etc.)

[00153] While the invention has been described in terms of several embodiments, those skilled in the art will recognize that the invention is not limited to the embodiments described, can be practiced with modification and alteration within the spirit and scope of the appended claims. The description is thus to be regarded as illustrative instead of limiting.

CLAIMS

What is claimed is:

1. An apparatus for hosted searching of private local area network (LAN) information comprising:

a LAN crawler to automatically and repeatedly crawl a LAN having a plurality of devices, said LAN crawler including,

a collection module to attempt to collect, from across each of a plurality of disparate information sources stored in the plurality of devices, only those parts of the disparate information sources that include descriptive information of a first plurality of items of interest, wherein for at least one of the plurality items of interest, the parts include technical information regarding the private LAN, users of the private LAN, and the plurality of devices of the private LAN, and

a reporting module to automatically report the collected information organized according to the plurality of items out of a firewall of the private LAN being crawled and over the Internet; and

a hosted on-demand search system to be coupled to the Internet including, a set of one or more centralized-search servers including,

a crawler interface to receive the reports from the LAN crawler deployed on the private LAN,

a database interface to create and synchronize a private search database for the private LAN based on the received reports, wherein the private search database includes the collected information collected from across the disparate information sources of that private LAN organized by the first plurality of items of interest, and wherein the private search database is not organized by documents located on the plurality of devices of the private LAN,

a server user interface module to provide a user interface over the Internet to the private LAN, to perform private searches of the private search database, and to provide an application rendered component as part of the user interface, and

an application interface to receive a request to access the collected information stored in the private search database from a third-party add-on application, to provide the accessed information to the third-party add-on application, and to receive from the third-party add-on application the application rendered component to be displayed on the user interface.

2. The apparatus of claim 1, wherein the third-party add-on application is executed by a remote server and the third-party add-on application communicates with the server user interface module through the application interface.

3. The apparatus of claim 1, wherein the plurality of disparate information sources include a routing table of a router, a router configuration file of a router, an address resolution protocol (ARP) table of a switch, a bridging table of a switch, a switch configuration table of a switch, a software configuration file of a server, a resource utilization counter of a server, a log file of a server, custom application file of a server, user information of a directory server, group information of a directory server, a software configuration file of a workstation, a registry of a workstation, an operating system interface database of a workstation, a directory of a workstation, a resource utilization counter of a workstation, a log file of a workstation, and a configuration file of a network printer.

4. The apparatus of claim 1, wherein the LAN crawler is deployed on one of the plurality of devices in each of the plurality of different private LANs, the LAN crawler to collect values of the technical information from the plurality of disparate information sources stored on the plurality of devices of the LAN being crawled

through a set of one or more organized questions to the plurality of devices of the private LAN being crawled.

5. The apparatus of claim 1, wherein the set of one or more centralized-search servers further includes a configuration database coupled to the server user interface module to store authentication information for access by the third-party add-on application and search queries.

6. The apparatus of claim 1, wherein the server user interface module comprises:

an application rendering module to render an application rendered component to be displayed in the user interface, wherein the application rendered component represents the search results of the private search by the third-party add-on application; and

a user interface rendering module to generate a user interface page including the application rendered component to be displayed in the user interface.

7. The apparatus of claim 1, wherein the LAN crawler further includes an organization module to automatically organize the collected information according to the first plurality of items of interest.

8. The apparatus of claim 1, wherein the collection module is configured to attempt to collect the technical information from the plurality of disparate information sources through a set of one or more organized questions to the plurality of devices of the private LAN being crawled, the collection module receiving values in response to the set of organized questions from the plurality of disparate information sources, wherein the values, received in response to the set of organized questions, include the descriptive information of the first plurality of items of interest.

9. The apparatus of claim 1, wherein at least some of the private search databases are each a hierarchical database, wherein the hierarchical database includes one or more sub-trees branching from a tree root node, wherein each sub-tree includes one or more nodes starting at a sub-tree root node, and wherein each node has a unique identifier, and wherein each hierarchical database is searched with a search query that includes a SELECT clause and a FROM clause, wherein the SELECT clause includes syntax to identify a path in the hierarchical database starting at a root of the hierarchy, and wherein the FROM clause describes from where in the hierarchical database information should be returned.

10. The apparatus of claim 9, wherein the hierarchical database is extended for the third-party add-on application by creating a new sub-tree from the tree root node that corresponds to that third-party add-on application's application provider, wherein information in that new sub-tree can be accessed only through that third-party add-on application.

11. The apparatus of claim 1, wherein the set of centralized-search servers comprises a reorganization module to reorganize the collected information received in the reports, the reorganization module including,

a report scanning module to attempt to collect, from across the reports, descriptive information of a second plurality of items of interest, wherein the descriptive information of the second plurality of items of interest include LAN-centric network topology information; and

an integration module to integrate the collected descriptive information of the second plurality of items of interest organized according to the second plurality of items of interest into the corresponding private search database.

12 The apparatus of claim 11, wherein the third-party add-on application is configured to send the search request to the application interface to perform the private search of the private search database to extract the LAN-centric network

topology information for the private LAN, create a network topology map to be displayed on the user interface based on the LAN-centric network topology information, and to send the network topology map to the server user interface module to provide the network topology map as part of the application rendered component in the user interface.

13. The apparatus of claim 1, wherein the third-party add-on application is configured to submit additional data to the application interface to be stored in the private search database.

14. The apparatus of claim 1, wherein the hosted on-demand search system further comprises a classification server coupled to a classification database and the set of centralized-search servers, the classification server to compare the collected information of the private search databases against predetermined characteristics of known devices, and to compute a classification metric for each of the plurality of devices of the private LAN.

15. A method for hosted searching of private local area network (LAN) information, comprising:

automatically and repeatedly crawling a private LAN having a plurality of devices to collect, from across each of a plurality of disparate information sources stored in the plurality of devices of the private LAN, only those parts of the disparate information sources that include descriptive information of a first plurality of items of interest, wherein for at least one of the plurality items of interest, the parts include technical information regarding the private LAN, users of the private LAN, and the plurality of devices of the private LAN;

automatically reporting the collected information organized according to the first plurality of items of interest out of a firewall of the private LAN being crawled and over the Internet to a hosted on-demand search system;

receiving the reports from the private LAN being crawled at the hosted on-demand search system;

creating and synchronizing a private search database for the private LAN based on the received reports, wherein the private search database includes the descriptive information collected from across the disparate information sources of that private LAN organized by the first plurality of items of interest, and wherein the private search database is not organized by documents located on the private LAN;

receiving a request to access the collected information stored in the private search database from a third-party add-on application;

providing the accessed information to the third-party add-on application.

16. The method of claim 15, wherein the plurality of disparate information sources include a routing table of a router, a router configuration file of a router, an address resolution protocol (ARP) table of a switch, a bridging table of a switch, a switch configuration table of a switch, a software configuration file of a server, a resource utilization counter of a server, a log file of a server, custom application file of a server, user information of a directory server, group information of a directory server, a software configuration file of a workstation, a registry of a workstation, an operating system interface database of a workstation, a directory of a workstation, a resource utilization counter of a workstation, a log file of a workstation, and a configuration file of a network printer.

17. The method of claim 16, wherein said automatically and repeatedly crawling that private LAN to collect descriptive information comprises:

asking a set of one or more organized questions of the plurality of disparate information sources stored in the plurality of devices of the private LAN being crawled; and

receiving values of the technical information from the plurality of disparate information sources in response to the set of organized questions.

18. The method of claim 15, further comprising:

receiving from the third-party add-on application an application rendered component to be displayed on the user interface; and

providing a user interface over the Internet to the private LAN that includes the application rendered component.

19. The method of claim 15, further comprising:

storing a configuration of the application rendered component, including the search query, in a configuration database for later retrieval; and

allowing display and selection of the stored configuration of the application rendered component, but not the search results of the private search by the third-party add-on application, through the user interface when the stored search query is designated as shareable.

20. The method of claim 15, further comprising:

organizing the collected information according to the first plurality of items of interest before reporting the collected information out of the firewall; and

integrating the organized information into the corresponding private search databases.

21. The method of claim 15, further comprising:

receiving at the hosted on-demand search system a first request from the private LAN to display the user interface with the application rendered component;

sending a second request to the third-party add-on application to generate the application rendered component;

receiving from the third-party add-on application a third request to perform one or more private searches for the descriptive information of the first plurality of items of interest in the private search database;

authorizing one or more private searches using a configuration database;

sending search results of the one or more private searches to the third-party add-on application;

generating the application rendered component to represent the search results of the one or more private searches;

generating a page for the user interface that includes the application rendered component that represent the search results of the one or more private searches; and

sending the generated page, including the application rendered component, to the user interface to be displayed.

22. The method of claim 15, further comprising:

collecting from across the reports descriptive information of a second plurality of items of interest;

organizing the collected descriptive information of the second plurality of items of interest according to the second plurality of items of interest; and

integrating the collected descriptive information of the second plurality of items of interest organized according to the second plurality of items of interest into the corresponding private search database reorganized information into the corresponding private search databases.

23. The method of claim 22, wherein the descriptive information of the second plurality of items of interest include LAN-centric network topology information, wherein the method further comprises:

receiving at the hosted on-demand search system a first request from the private LAN to display a network topology map to be displayed on the user interface as part of the application rendered component;

sending a second request to the third-party add-on application to generate the application rendered component that includes the network topology map;

receiving from the third-party add-on application a third request to perform one or more private searches for LAN-centric network topology information in the private search database;

authorizing the one or more private searches using a configuration database;

sending search results of the one or more private searches to the third-party add-on application;

generating the network topology map as part of the application rendered component based on the search results of the one or more private searches;

generating a page for the user interface that includes the application rendered component and the network topology map; and

sending the generated page, including the network topology map, to the user interface to be displayed.

24. The method of claim 15, wherein automatically and repeatedly crawling the private LAN to collect descriptive information comprises:

asking a set of one or more organized questions to the plurality of devices of the private LAN being crawled; and

receiving values in response to the set of organized questions from the plurality of disparate information sources, wherein the received values are the descriptive information of the first plurality of items of interest.

25. The method of claim 15, further comprising:

comparing the collected information of the private search database against predetermined characteristics of known devices; and

computing a classification metric for each of the plurality of devices of the private LAN.

26. An apparatus for hosted searching of private local area network (LAN) information comprising:

a LAN crawler to automatically and repeatedly crawl a LAN having a plurality of devices, said LAN crawler including,

a collection module to attempt to collect, from across each of a plurality of disparate information sources stored in the plurality of devices, only those parts of the disparate information sources that include descriptive information of a first plurality of items of interest, wherein for at least one of the first plurality items of interest, the parts are collected from multiple ones of the plurality of disparate information sources, wherein the collection module comprises:

a discovery module to discover the plurality of devices of the private LAN; and

a generic-probing module to attempt to collect the descriptive information from the disparate information sources stored on the plurality of devices of the private LAN according to a first set of probing requirements;

a plurality of specific-probing plug-ins that are coupled to the collection module to attempt to collect the descriptive information from the disparate information sources stored on the plurality of devices of the private LAN, each of the plurality of specific-probing plug-ins to attempt to collect the descriptive information according to a second set of probing requirements that are specific to each of the plurality of specific-probing plug-ins, wherein at least one of the plurality of specific-probing plug-ins is configured to attempt to collect the descriptive information from the disparate information sources stored on the plurality of devices of the private LAN according to one or more probing requirements that are specific to an add-on application; and

a reporting module to automatically report the collected information organized by the first plurality of items of interest out of a

firewall of the private LAN being crawled and over the Internet; and

a hosted on-demand search system to be coupled to the Internet including, a

set of one or more centralized-search servers including,

a crawler interface to receive the reports from the LAN crawler deployed on the private LAN,

a database interface to create and synchronize a private search database for the private LAN based on the received reports, wherein the private search database includes the collected information collected from across the disparate information sources of that private LAN organized by the first plurality of items of interest, and wherein the private search database is not organized by documents located on the plurality of devices of the private LAN,

a server user interface module to provide a user interface over the Internet to the private LAN, to perform private searches of the private search database, and to provide an application rendered component as part of the user interface, and

an application interface to receive a search request to perform a private search of the private search database from the add-on application, to provide search results of the private search to the add-on application, and to receive from the add-on application the application rendered component, representing the search results, to be displayed on the user interface.

27. The apparatus of claim 26, wherein the add-on application is configured to submit additional data to the application interface to be stored in the private search database.

28. The apparatus of claim 26, wherein the set of one or more centralized-search servers further includes a configuration database coupled to the server user interface

module to store authentication information for access by the add-on application and search queries.

29. The apparatus of claim 26, wherein the LAN crawler further includes an organization module to automatically organize the collected information according to the first plurality of items of interest, wherein the first plurality of items of interest include LAN-centric network topology information, and wherein the plurality of disparate information sources include a routing table.

30. The apparatus of claim 26, wherein the collection module is configured to attempt to collect the technical information from the plurality of disparate information sources through a set of one or more organized questions to the plurality of devices of the private LAN being crawled, the collection module receiving values in response to the set of organized questions from the plurality of disparate information sources, and wherein the values, received in response to the set of organized questions, include the descriptive information of the first plurality of items of interest.

31. The apparatus of claim 26, wherein at least some of the private search databases are each a hierarchical database, wherein the hierarchical database includes one or more sub-trees branching from a tree root node, wherein each sub-tree includes one or more nodes starting at a sub-tree root node, and wherein each node has a unique identifier, and wherein each hierarchical database is searched with a search query that includes a SELECT clause and a FROM clause, wherein the SELECT clause includes syntax to identify a path in the hierarchical database starting at a root of the hierarchy, and wherein the FROM clause describes from where in the hierarchical database information should be returned.

32. The apparatus of claim 31, wherein the hierarchical database is extended for the third-party add-on application by creating a new sub-tree from the tree root node that corresponds to that third-party add-on application's application provider,

wherein information in that new sub-tree can be accessed only through that third-party add-on application.

33. The apparatus of claim 26, wherein the hosted on-demand search system further comprises a classification server coupled to a classification database and the set of one or more centralized-search servers, the classification server to compare the collected information of the private search database against predetermined characteristics of known devices, and to compute a classification metric for each of the plurality of devices of the private LAN.

34. The apparatus of claim 26, wherein the descriptive information of the first plurality of items of interest includes technical information regarding the private LAN, users of the private LAN, and the plurality of devices of the private LAN.

35. The apparatus of claim 26, wherein the plurality of disparate information sources include a routing table of a router, a router configuration file of a router, an address resolution protocol (ARP) table of a switch, a bridging table of a switch, a switch configuration table of a switch, a software configuration file of a server, a resource utilization counter of a server, a log file of a server, custom application file of a server, user information of a directory server, group information of a directory server, a software configuration file of a workstation, a registry of a workstation, an operating system interface database of a workstation, a directory of a workstation, a resource utilization counter of a workstation, a log file of a workstation, and a configuration file of a network printer.

36. The apparatus of claim 26, wherein at least one of the plurality of specific-probing plug-ins is a periodic plug-in that attempts to collect the descriptive information from the plurality of devices of the private LAN periodically.

37. The apparatus of claim 26, wherein at least one of the plurality of specific-probing plug-ins is a device plug-in that attempts to collect the descriptive

information from the plurality of devices of the private LAN that are a specified type of device according to a set of one or more probing requirements that are specific to the specified type of device.

38. The apparatus of claim 26, wherein at least one of the plurality of specific-probing plug-ins is a hybrid plug-in that operates as either:

a periodic plug-in that that attempts to collect the descriptive information from at least one of the plurality of devices of the private LAN periodically; or

a device plug-in that attempts to collect the descriptive information from the at least one device of the plurality of devices of the private LAN according to specific probing requirements of a specified type of information source.

39. A method for hosted searching of private local area network (LAN) information, comprising:

automatically and repeatedly crawling a private LAN having a plurality of devices to collect, from across each of a plurality of disparate information sources stored in the plurality of devices of the private LAN, only those parts of the disparate information sources that include descriptive information of a first plurality of items of interest, wherein for at least one of the plurality items of interest, wherein for at least one of the first plurality items of interest, the parts are collected from multiple ones of the plurality of disparate information sources, wherein said automatically and repeatedly crawling comprises:

discovering the plurality of devices of the private LAN;

collecting the descriptive information from the disparate information sources stored on the plurality of devices of the private LAN according to a first set of probing requirements; and

collecting the descriptive information according to a second set of probing requirements, wherein said collecting the descriptive information according to the second set comprises collecting the descriptive information according to one or more probing requirements that are specific to an add-on application;

automatically reporting the collected information organized according to the first plurality of items of interest out of a firewall of the private LAN being crawled and over the Internet to a hosted on-demand search system;

receiving the reports from the private LAN being crawled at the hosted on-demand search system;

creating and synchronizing a private search database for the private LAN based on the received reports, wherein the private search database includes the descriptive information collected from across the disparate information sources of that private LAN organized by the first plurality of items of interest, and wherein the private search database is not organized by documents located on the private LAN;

receiving a search request to perform a private search of the private search database from the add-on application; and

providing search results of the private search to the add-on application.

40. The method of claim 39, wherein the descriptive information of the first plurality of items of interest include technical information regarding the plurality of private LANs, users of the plurality of private LANs, and the plurality of devices of the plurality of private LANs.

41. The method of claim 40, wherein the plurality of disparate information sources include a routing table of a router, a router configuration file of a router, an address resolution protocol (ARP) table of a switch, a bridging table of a switch, a switch configuration table of a switch, a software configuration file of a server, a resource utilization counter of a server, a log file of a server, custom application file

of a server, user information of a directory server, group information of a directory server, a software configuration file of a workstation, a registry of a workstation, an operating system interface database of a workstation, a directory of a workstation, a resource utilization counter of a workstation, a log file of a workstation, and a configuration file of a network printer.

42. The method of claim 41, wherein said automatically and repeatedly crawling that private LAN to collect descriptive information comprises:

asking a set of one or more organized questions of the plurality of disparate information sources stored in the plurality of devices of the private LAN being crawled; and

receiving values of the technical information from the plurality of disparate information sources in response to the set of organized questions.

43. The method of claim 39, further comprising:

receiving from the add-on application an application rendered component that represents the search results to be displayed on the user interface; and

providing a user interface over the Internet to the private LAN that includes the application rendered component.

44. The method of claim 39, further comprising:

receiving at the hosted on-demand search system a first request from the private LAN to display the user interface with an application rendered component;

sending a second request to the add-on application to generate the application rendered component;

receiving from the add-on application a third request to perform one or more private searches for the descriptive information of the first plurality of items of interest in the private search database;

authorizing one or more private searches using a configuration database;

sending search results of the one or more private searches to the add-on application;

generating the application rendered component to represent the search results of the one or more private searches;

generating a page for the user interface that includes the application rendered component that represent the search results of the one or more private searches; and

sending the generated page, including the application rendered component, to the user interface to be displayed.

45. The method of claim 39, wherein said collecting the descriptive information according to the second set of probing requirements comprises collecting the descriptive information from at least one of the plurality of devices of the private LAN periodically.

46. The method of claim 39, further comprising organizing the collected descriptive information of the second plurality of items of interest according to the first plurality of items of interest, wherein the first plurality of items of interest include LAN-centric network topology information, and wherein the plurality of disparate information sources include a routing table.

47. The method of claim 39, wherein said collecting the descriptive information according to the second set of probing requirements comprises collecting the descriptive information from the plurality of devices of the private LAN according to a set of one or more probing requirements that are specific to a specified type of information source.

48. The method of claim 39, further comprising:

collecting from across the reports descriptive information of a second plurality of items of interest;

organizing the collected descriptive information of the second plurality of items of interest according to the second plurality of items of interest; and

integrating the collected descriptive information of the second plurality of items of interest organized according to the second plurality of items of interest into the corresponding private search database reorganized information into the corresponding private search databases.

49. The method of claim 48, wherein the descriptive information of the second plurality of items of interest include LAN-centric network topology information, wherein the method further comprises:

receiving at the hosted on-demand search system a first request from the private LAN to display a network topology map to be displayed on the user interface as part of the application rendered component;

sending a second request to the add-on application to generate the application rendered component that includes the network topology map;

receiving from the add-on application a third request to perform one or more private searches for LAN-centric network topology information in the private search database;

authorizing the one or more private searches using a configuration database;

sending search results of the one or more private searches to the add-on application;

generating the network topology map as part of the application rendered component based on the search results of the one or more private searches;

generating a page for the user interface that includes the application rendered component and the network topology map; and

sending the generated page, including the network topology map, to the user interface to be displayed.

50. The method of claim 39, further comprising:

comparing the collected information of the private search database against predetermined characteristics of known devices; and

computing a classification metric for each of the plurality of devices of the private LAN.

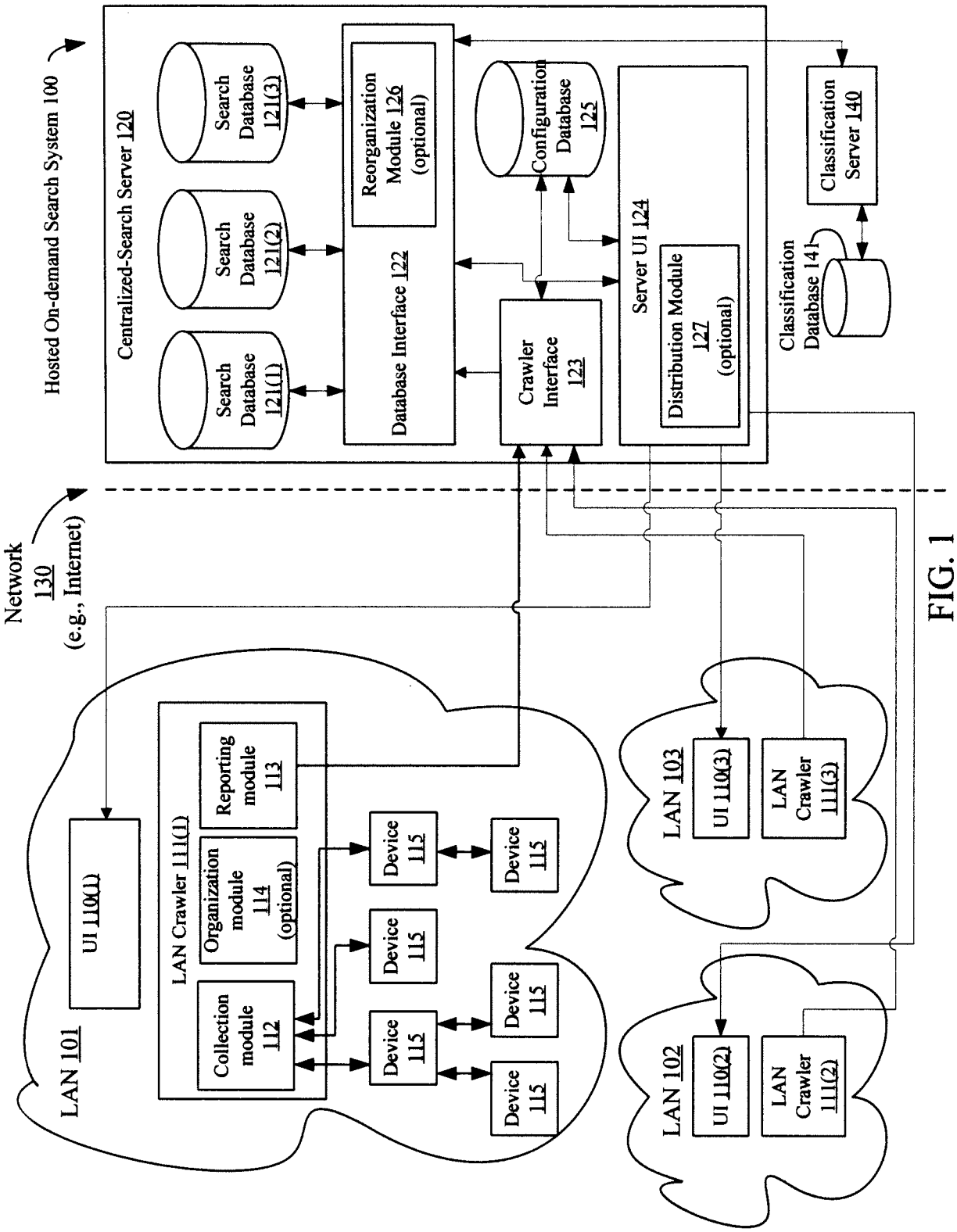

Hosted On-demand Search System 100
Centralized-Search Server 120
Search Database 121(1)
Search Database 121(2)
Search Database 121(3)
Database Interface 122
Reorganization Module 126 (optional)
Configuration Database 125
Crawler Interface 123
Server UI 124
Distribution Module 127 (optional)
Classification Server 140
Classification Database 141
Network 130 (e.g., Internet)
LAN 101
UI 110(1)
LAN Crawler 111(1)
Collection module 112
Organization module 114 (optional)
Reporting module 113
Device 115
LAN 103
UI 110(3)
LAN Crawler 111(3)
LAN 102
UI 110(2)
LAN Crawler 111(2)

FIG. 1

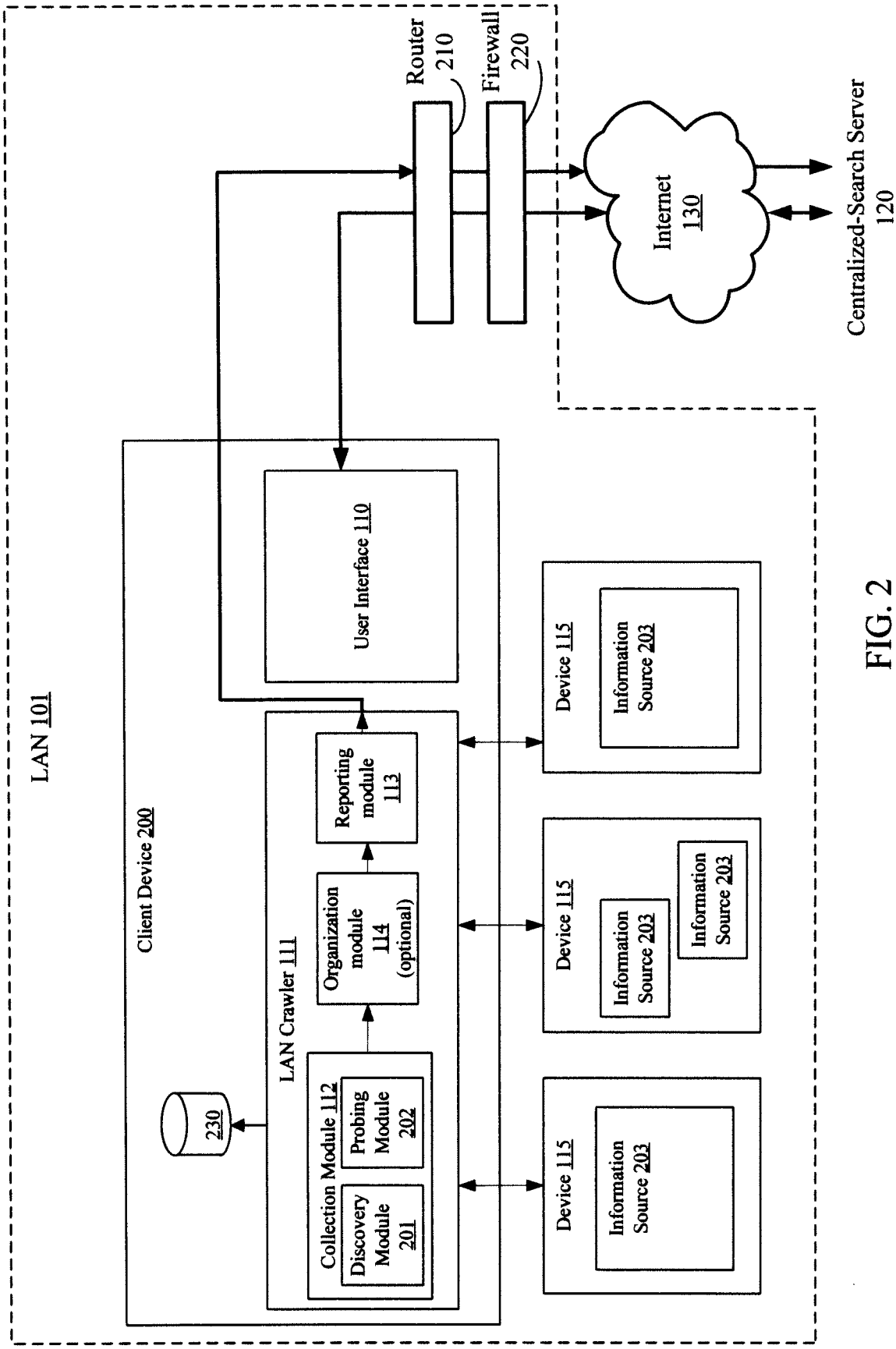

LAN 101
Client Device 200
User Interface 110
LAN Crawler 111
Collection Module 112
Discovery Module 201
Probing Module 202
Organization module 114 (optional)
Reporting module 113
230
Router 210
Firewall 220
Internet 130
Centralized-Search Server 120
Device 115
Information Source 203
Device 115
Information Source 203
Information Source 203
Device 115
Information Source 203

FIG. 2

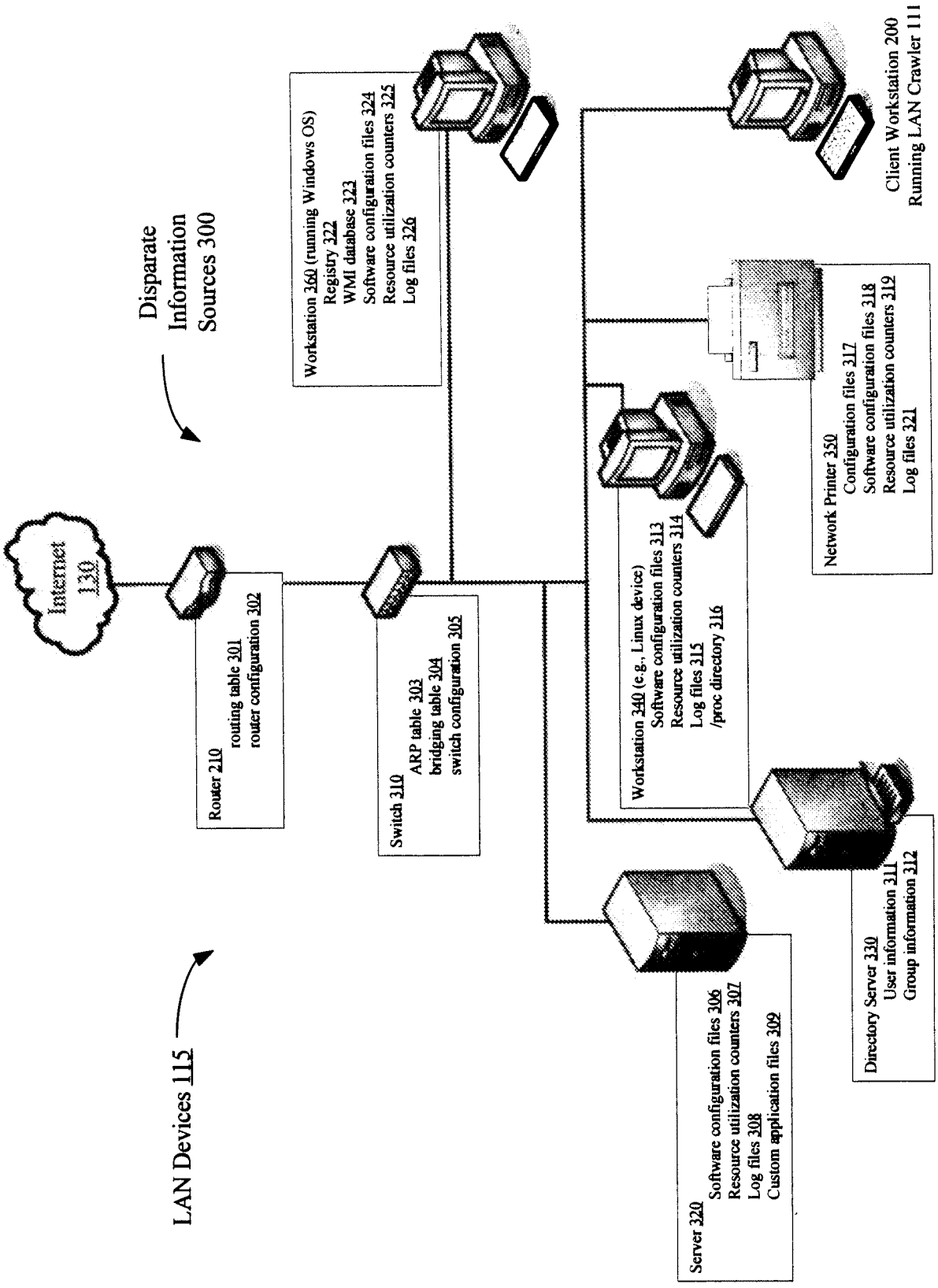

Disparate Information Sources 300
LAN Devices 115
Internet 130
Router 210
routing table 301
router configuration 302
Switch 310
ARP table 303
bridging table 304
switch configuration 305
Workstation 360 (running Windows OS)
Registry 322
WMI database 323
Software configuration files 324
Resource utilization counters 325
Log files 326
Workstation 340 (e.g., Linux device)
Software configuration files 313
Resource utilization counters 314
Log files 315
/proc directory 316
Network Printer 350
Configuration files 317
Software configuration files 318
Resource utilization counters 319
Log files 321
Client Workstation 200
Running LAN Crawler 111
Server 320
Software configuration files 306
Resource utilization counters 307
Log files 308
Custom application files 309
Directory Server 330
User information 311
Group information 312

FIG. 3

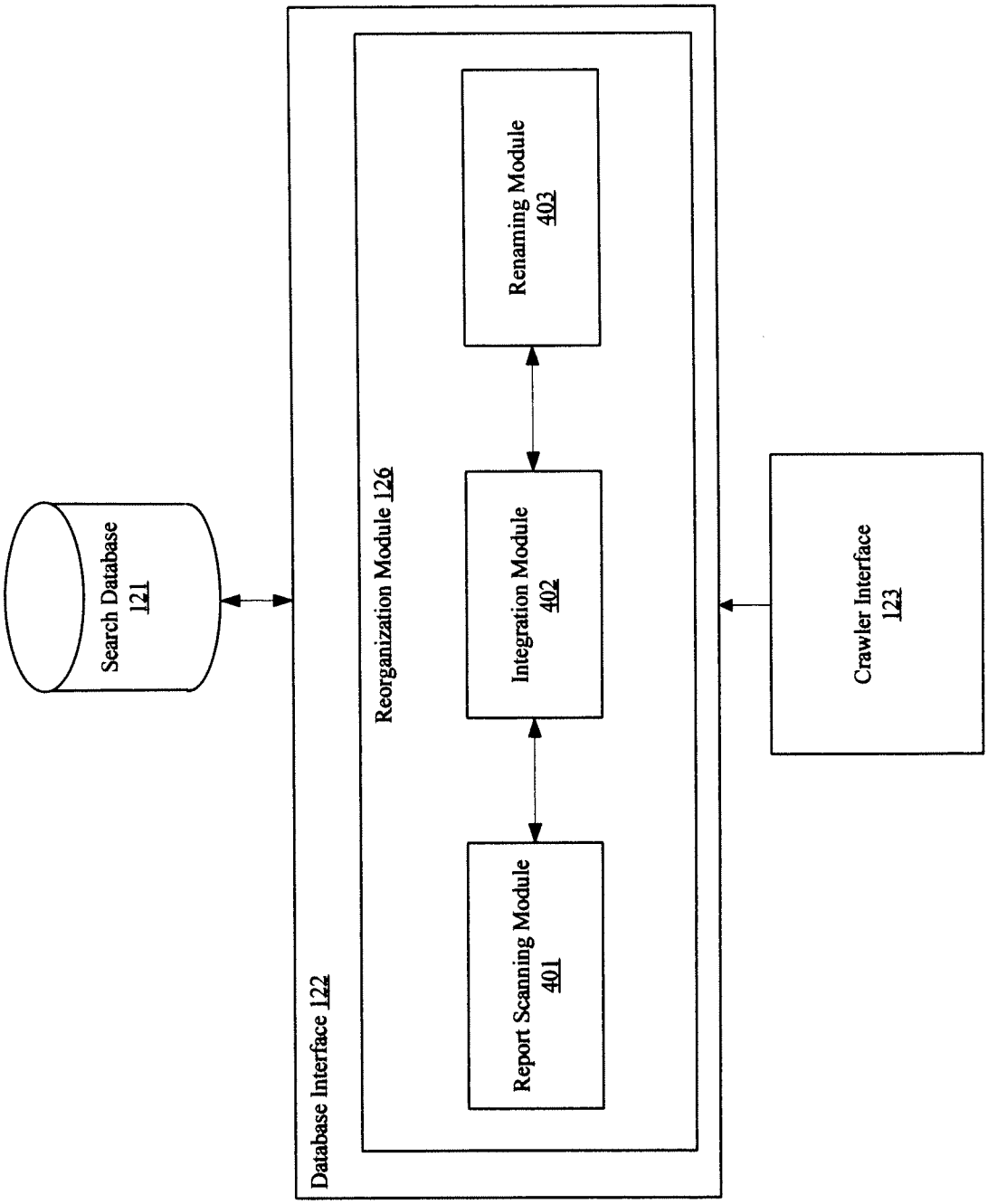

Search Database
121
Database Interface 122
Reorganization Module 126
Renaming Module
403
Integration Module
402
Report Scanning Module
401
Crawler Interface
123

FIG. 4

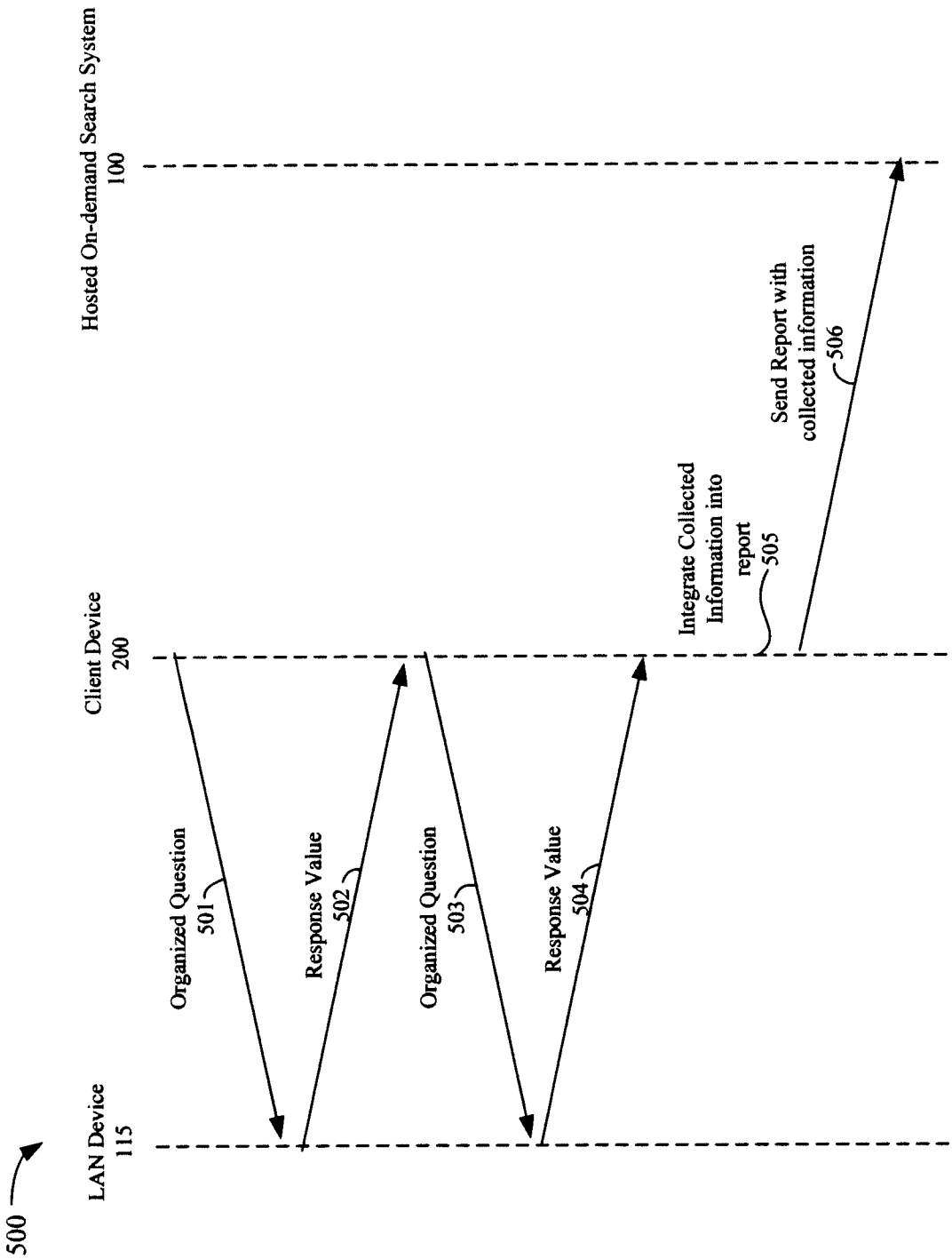

500
LAN Device
115
Client Device
200
Hosted On-demand Search System
100
Organized Question
501
Response Value
502
Organized Question
503
Response Value
504
Integrate Collected Information into report
505
Send Report with collected information
506

FIG. 5

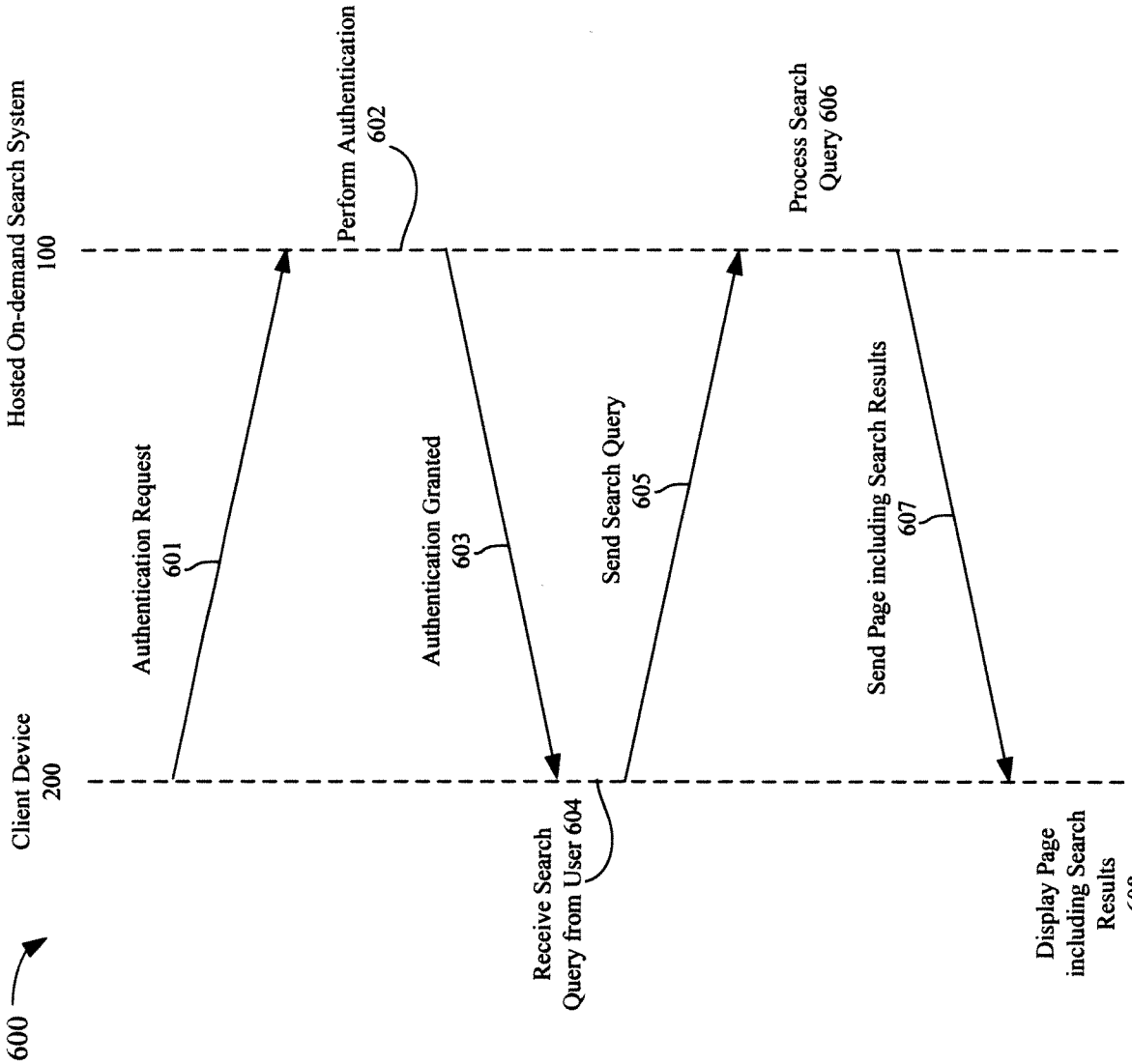

600
Client Device
200
Hosted On-demand Search System
100
Authentication Request
601
Perform Authentication
602
Authentication Granted
603
Receive Search
Query from User 604
Send Search Query
605
Process Search
Query 606
Send Page including Search Results
607
Display Page
including Search
Results
608

FIG. 6

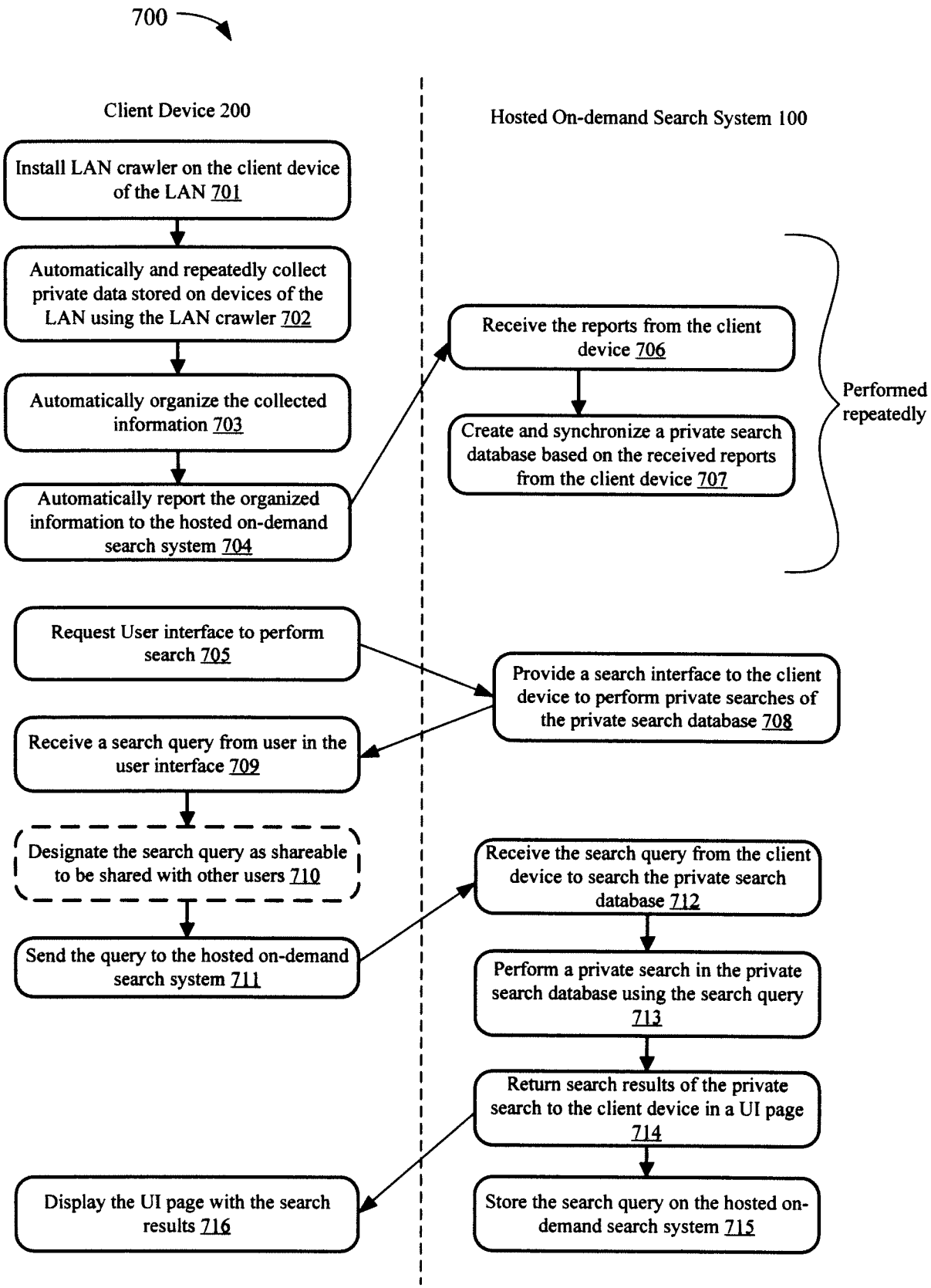

700
Client Device 200
Hosted On-demand Search System 100
Install LAN crawler on the client device of the LAN 701
Automatically and repeatedly collect private data stored on devices of the LAN using the LAN crawler 702
Automatically organize the collected information 703
Automatically report the organized information to the hosted on-demand search system 704
Receive the reports from the client device 706
Create and synchronize a private search database based on the received reports from the client device 707
Performed repeatedly
Request User interface to perform search 705
Provide a search interface to the client device to perform private searches of the private search database 708
Receive a search query from user in the user interface 709
Designate the search query as shareable to be shared with other users 710
Send the query to the hosted on-demand search system 711
Receive the search query from the client device to search the private search database 712
Perform a private search in the private search database using the search query 713
Return search results of the private search to the client device in a UI page 714
Store the search query on the hosted on-demand search system 715
Display the UI page with the search results 716

FIG. 7

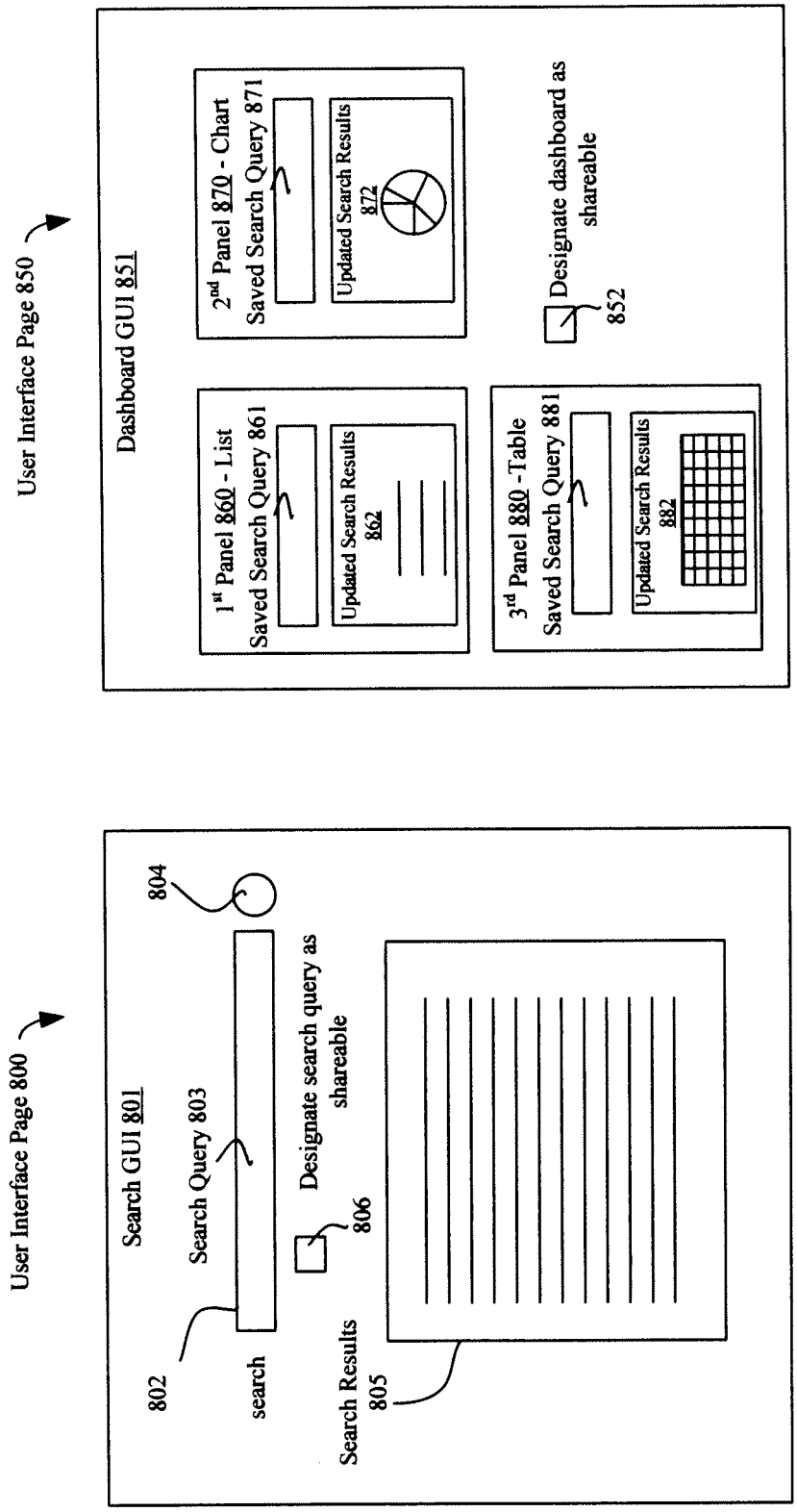

User Interface Page 850
Dashboard GUI 851
1st Panel 860 - List
Saved Search Query 861
Updated Search Results 862
2nd Panel 870 - Chart
Saved Search Query 871
Updated Search Results 872
Designate dashboard as shareable
852
3rd Panel 880 -Table
Saved Search Query 881
Updated Search Results 882
User Interface Page 800
Search GUI 801
Search Query 803
804
802
search
Designate search query as shareable
806
Search Results
805

FIG. 8

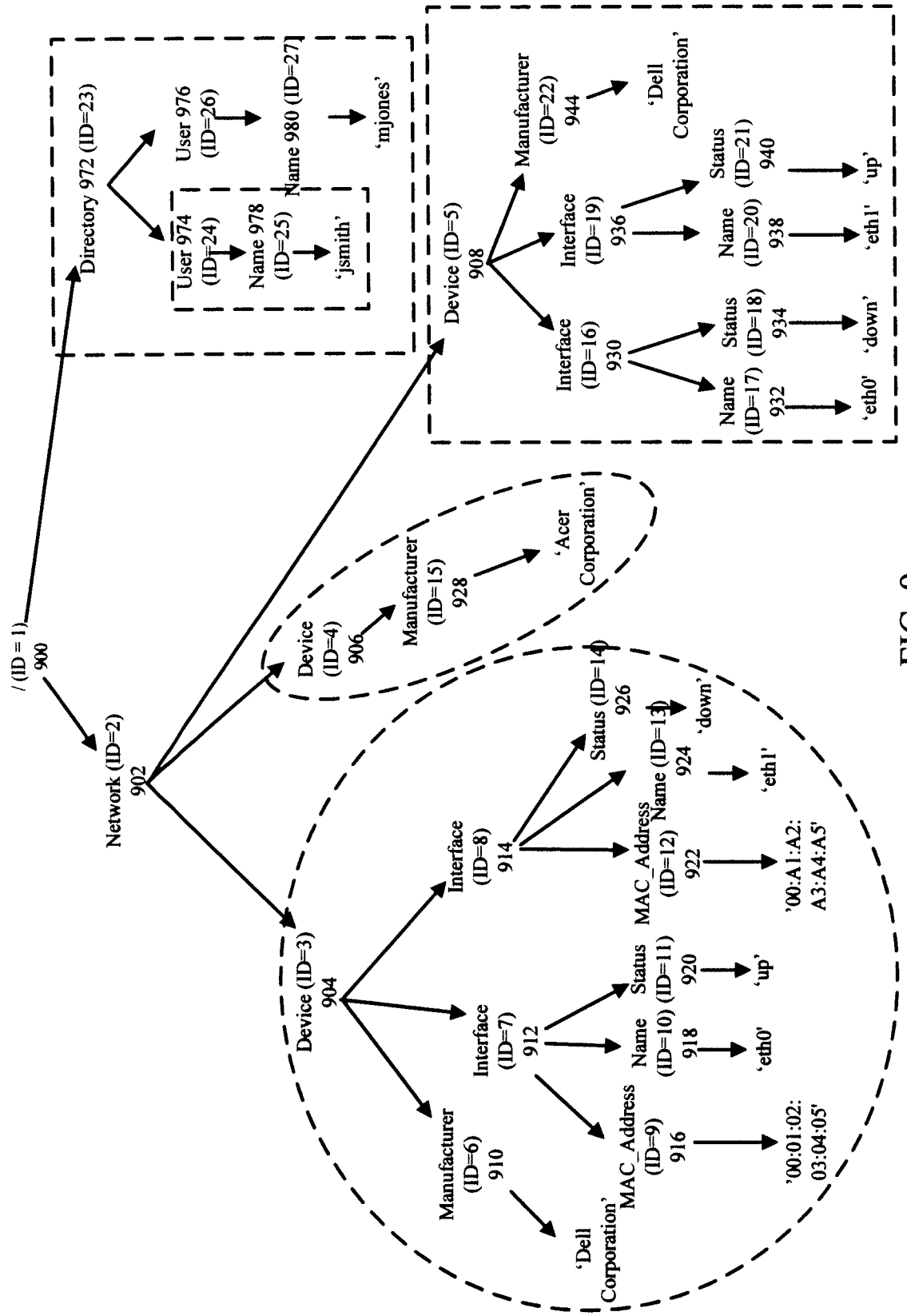
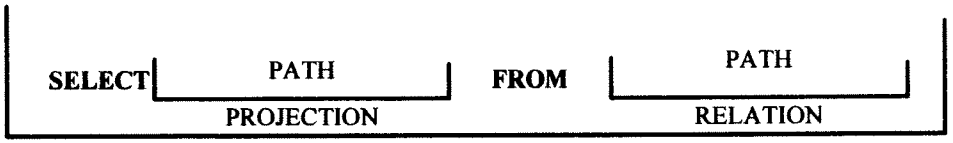
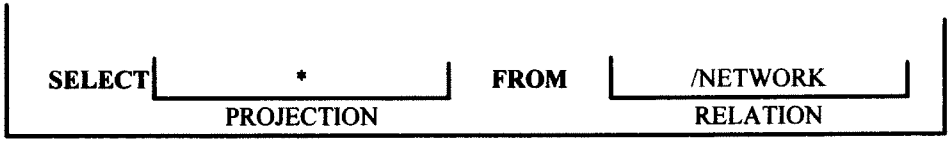

/ (ID = 1)
900
Network (ID=2)
902
Directory 972 (ID=23)
User 974 (ID=24)
Name 978 (ID=25)
'jsmith'
User 976 (ID=26)
Name 980 (ID=27)
'mjones'
Device (ID=5)
908
Manufacturer (ID=22)
944
'Dell Corporation'
Interface (ID=19)
936
Status (ID=21)
940
Name (ID=20)
938
'eth1'
'up'
Interface (ID=16)
930
Status (ID=18)
934
'down'
Name (ID=17)
932
'eth0'
Device (ID=4)
906
Manufacturer (ID=15)
928
'Acer Corporation'
Device (ID=3)
904
Interface (ID=8)
914
Status (ID=14)
926
'down'
MAC_Address (ID=12)
922
Name (ID=13)
924
'eth1'
'00:A1:A2: A3:A4:A5'
Interface (ID=7)
912
Status (ID=11)
920
'up'
Name (ID=10)
918
'eth0'
Manufacturer (ID=6)
910
'Dell Corporation'
MAC_Address (ID=9)
916
'00:01:02: 03:04:05'

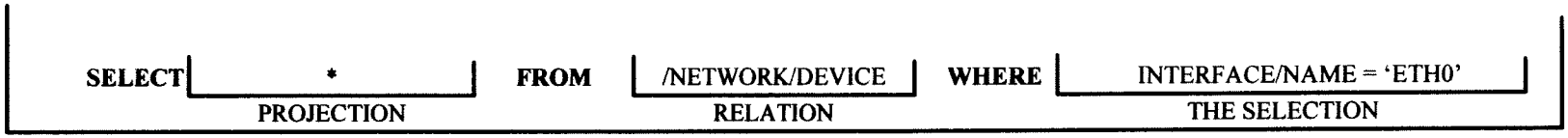
FIG. 9



HIERARCHICAL DATABASE SEARCH
QUERY SYNTAX



HIERARCHICAL DATABASE SEARCH QUERY
EXAMPLE



HIERARCHICAL DATABASE SEARCH QUERY
EXAMPLE
THAT INCLUDES A WHERE CLAUSE

FIG. 10

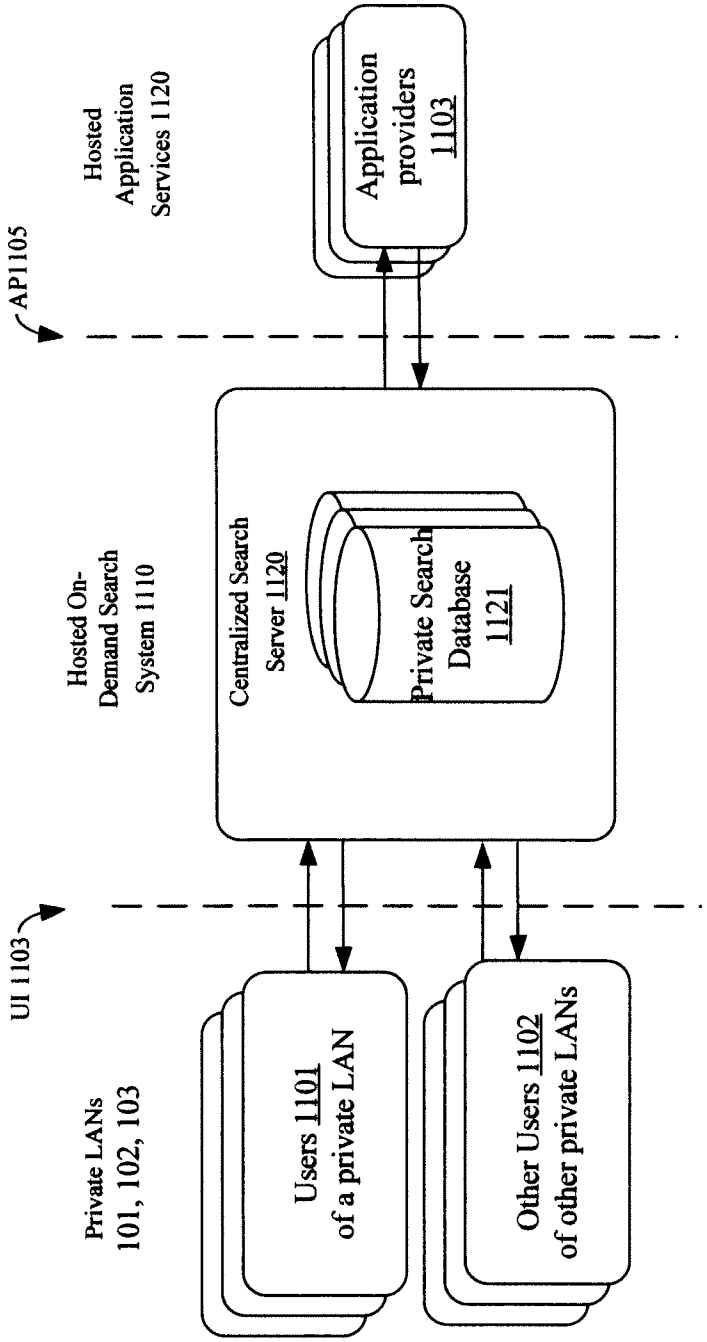

Application providers 1103
Hosted Application Services 1120
AP1105
Hosted On-Demand Search System 1110
Centralized Search Server 1120
Private Search Database 1121
UI 1103
Private LANs 101, 102, 103
Users 1101 of a private LAN
Other Users 1102 of other private LANs

FIG. 11

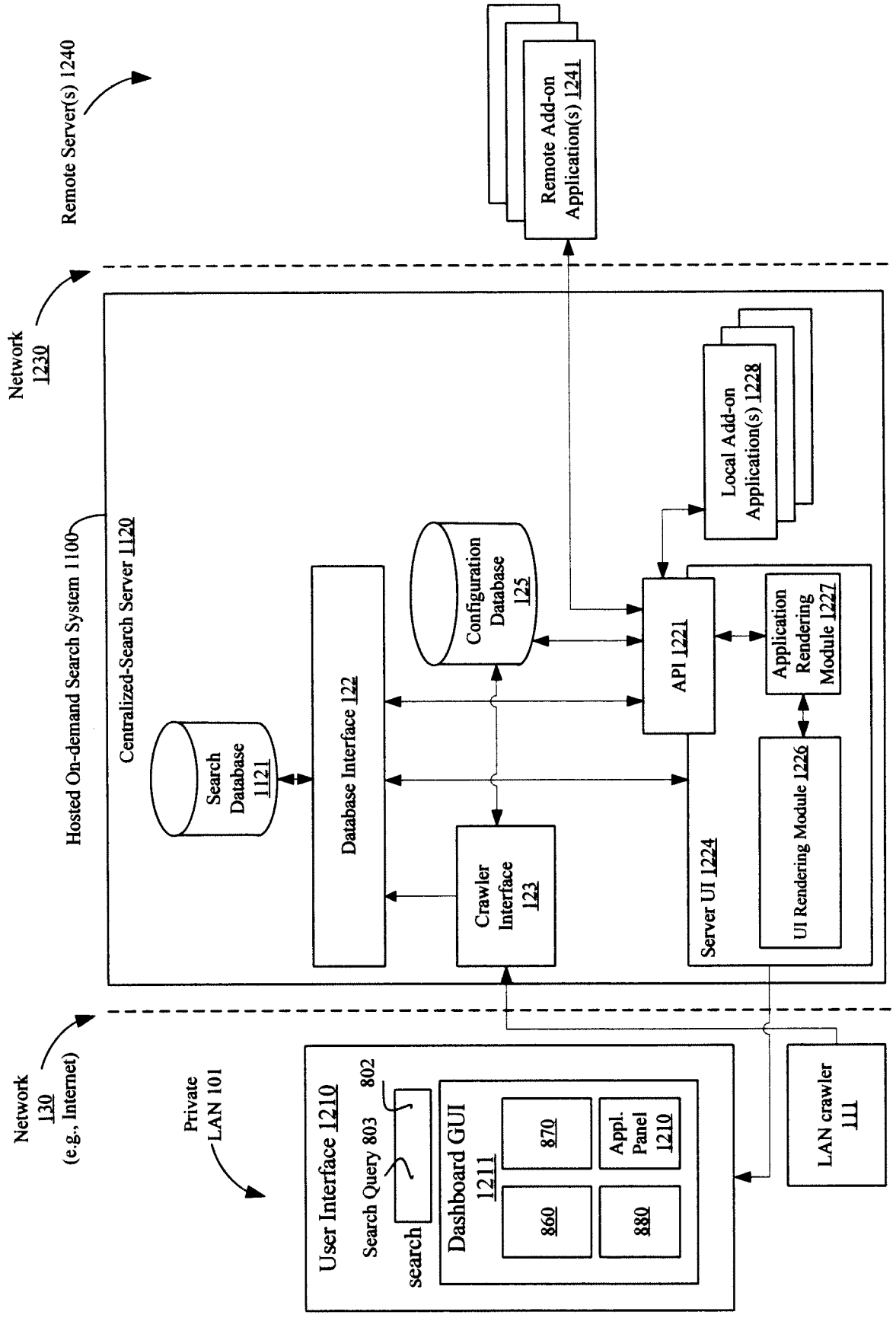

Remote Server(s) 1240
Remote Add-on Application(s) 1241
Network 1230
Hosted On-demand Search System 1100
Centralized-Search Server 1120
Local Add-on Application(s) 1228
Configuration Database 125
Search Database 1121
Database Interface 122
API 1221
Application Rendering Module 1227
Crawler Interface 123
Server UI 1224
UI Rendering Module 1226
Network 130 (e.g., Internet)
Private LAN 101
User Interface 1210
Search Query 803
802
search
Dashboard GUI 1211
870
Appl. Panel 1210
860
880
LAN crawler 111

FIG. 12

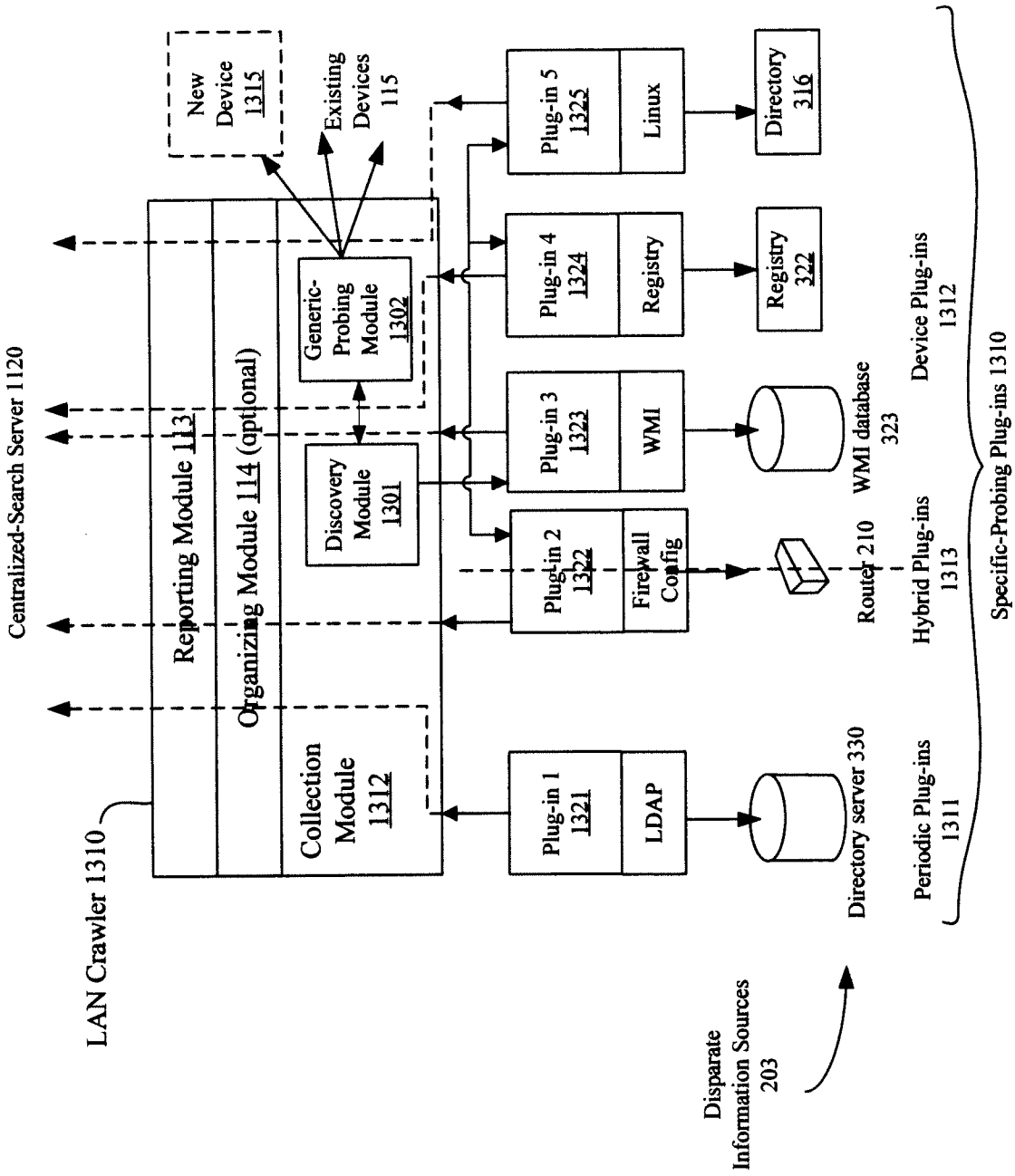

Centralized-Search Server 1120
LAN Crawler 1310
Reporting Module 113
Organizing Module 114 (optional)
Collection Module 1312
Discovery Module 1301
Generic-Probing Module 1302
New Device 1315
Existing Devices 115
Plug-in 1 1321
LDAP
Plug-in 2 1322
Firewall Config
Plug-in 3 1323
WMI
Plug-in 4 1324
Registry
Plug-in 5 1325
Linux
Directory 316
Registry 322
WMI database 323
Router 210
Directory server 330
Disparate Information Sources 203
Periodic Plug-ins 1311
Hybrid Plug-ins 1313
Device Plug-ins 1312
Specific-Probing Plug-ins 1310

FIG. 13

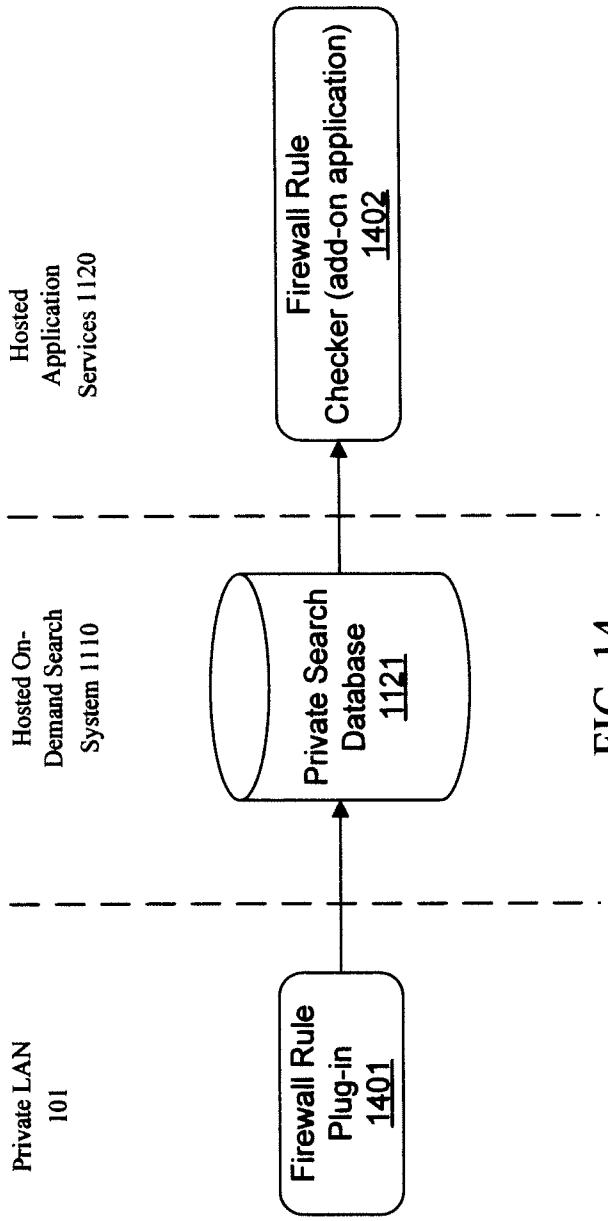

Hosted Application Services 1120
Firewall Rule Checker (add-on application) 1402
Hosted On-Demand Search System 1110
Private Search Database 1121
Private LAN 101
Firewall Rule Plug-in 1401

FIG. 14

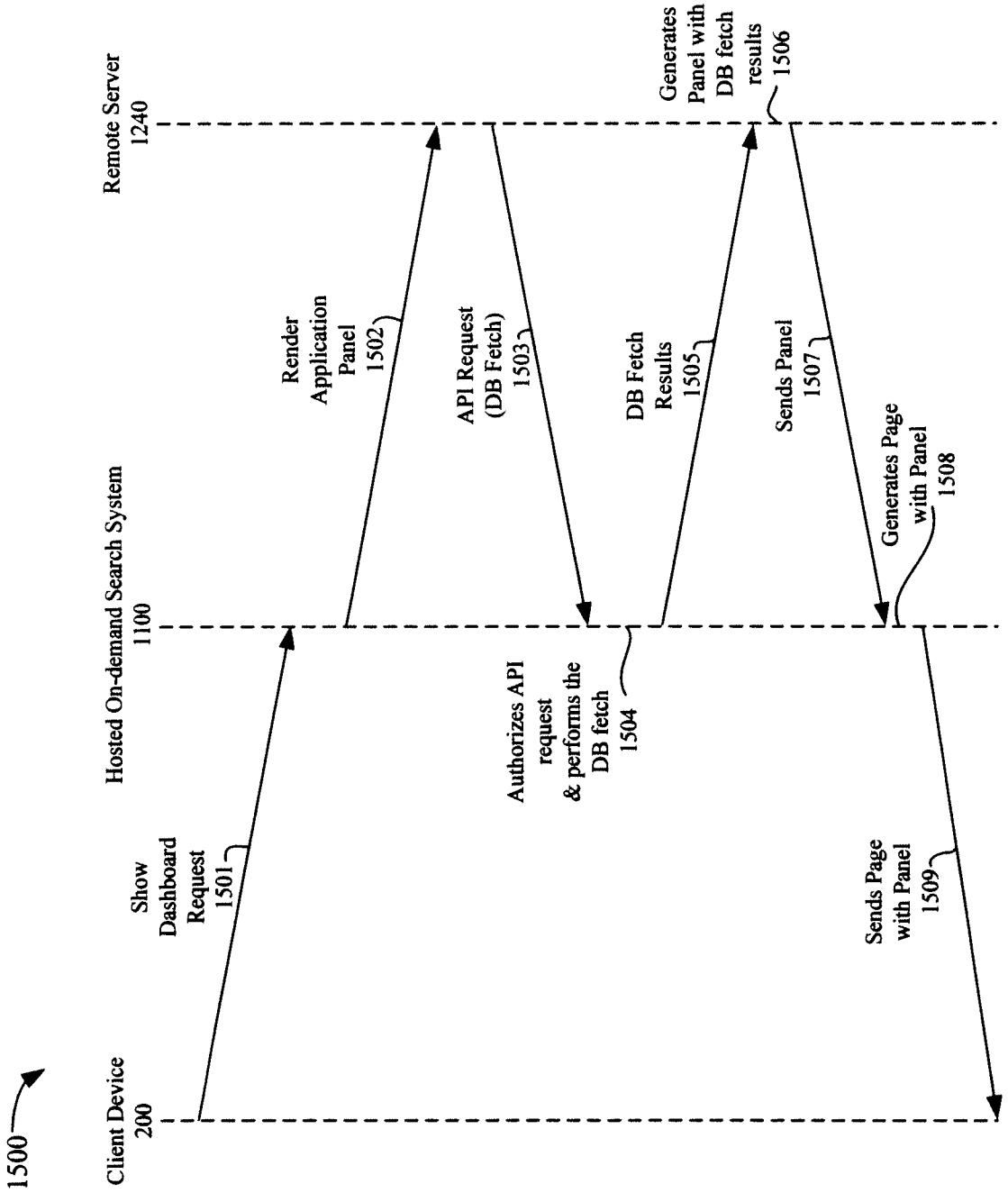

1500
Client Device 200
Hosted On-demand Search System 1100
Remote Server 1240
Show Dashboard Request 1501
Render Application Panel 1502
API Request (DB Fetch) 1503
Authorizes API request & performs the DB fetch 1504
DB Fetch Results 1505
Generates Panel with DB fetch results 1506
Sends Panel 1507
Generates Page with Panel 1508
Sends Page with Panel 1509

FIG. 15

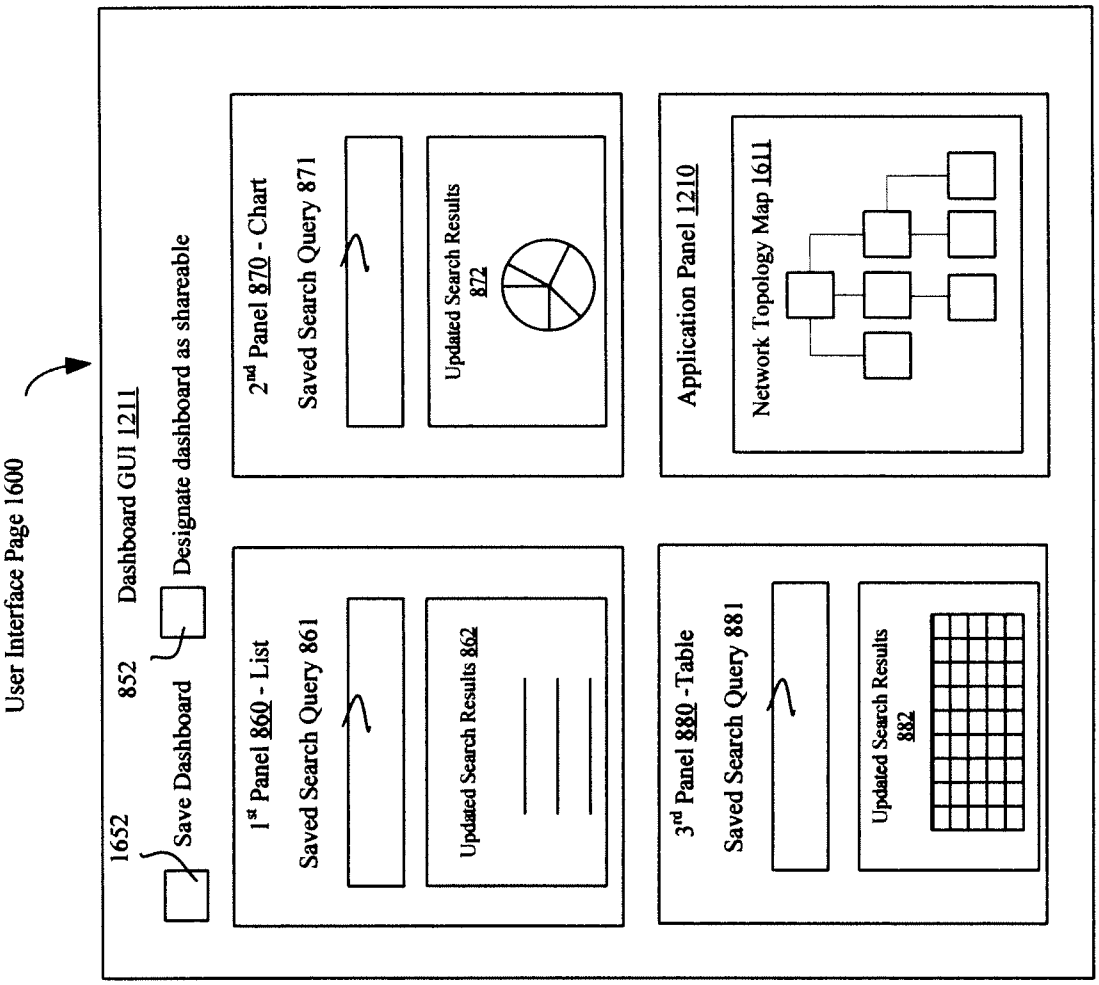

User Interface Page 1600
Dashboard GUI 1211
1652
Save Dashboard
852
Designate dashboard as shareable
1st Panel 860 - List
Saved Search Query 861
Updated Search Results 862
2nd Panel 870 - Chart
Saved Search Query 871
Updated Search Results 872
3rd Panel 880 -Table
Saved Search Query 881
Updated Search Results 882
Application Panel 1210
Network Topology Map 1611

FIG. 16

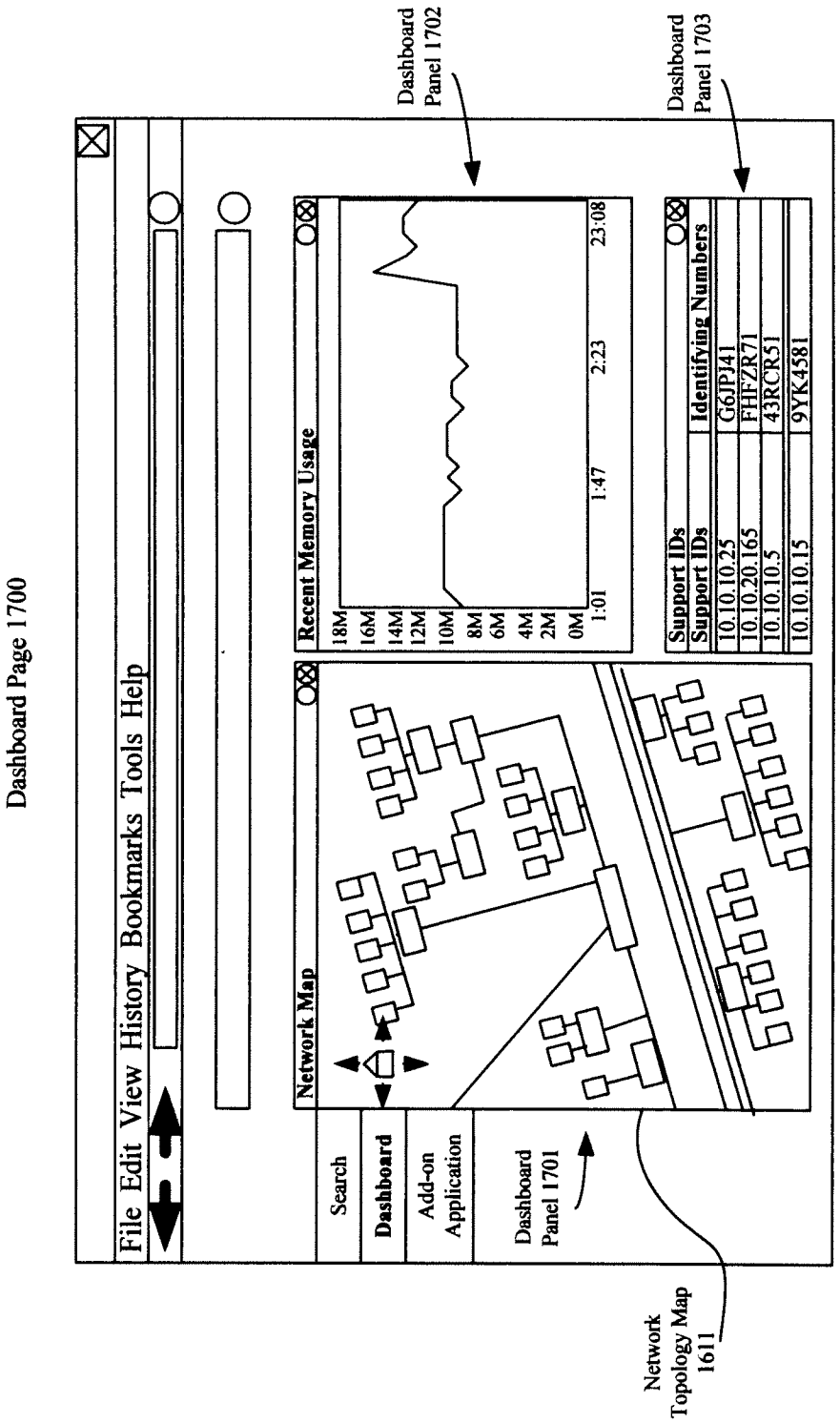

Dashboard Page 1700
File Edit View History Bookmarks Tools Help
Dashboard Panel 1702
Dashboard Panel 1703
Recent Memory Usage
18M
16M
14M
12M
10M
8M
6M
4M
2M
0M
1:01
1:47
2:23
23:08
Support IDs
Support IDs
Identifying Numbers
10.10.10.25
G6JPJ41
10.10.20.165
FHFZR71
10.10.10.5
43RCR51
10.10.10.15
9YK4581
Network Map
Search
Dashboard
Add-on Application
Dashboard Panel 1701
Network Topology Map 1611

FIG. 17

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 08/81019

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 7/00 (2008.04)
USPC - 707/3
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)
USPC 707/3

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC 707/1,101,102,204 709/217,218,224 715/968

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PubWEST(USPT,PGPB,EPAB,JPAB); DialogPRO(Patents);Google Scholar
Search Terms: crawl, LAN, probe, database, third party

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6,463,430 B1 (Brady et al) 08 October 2002 (08.10.2002), entire document especially Figs 2,4,5,6 and col 5, ln 3-18; col 6, ln 1-15; col 7, ln 11-26; col 11, ln 44-67; col 15, ln 59-66; col 18, ln 1-8; col 19, ln 2-10; col 20, ln 4-28; col 23, ln 15-26; col 24, ln 13-24,31-37; col 25, ln 61-67.	1-50
Y	US 2007/0203869 A1 (Ramsey et al.) 30 August 2007 (30.08.2007), entire document especially Fig 4,6 and para [0034], [0036]-[0038], [0043], [0046]-[0048], [0063], [0066], [0070], [0074], [0087]-[0089], [0100], [0104], [0105], [0110], [0113], [0114], [0116], [0117], [0119], [0121], [0123], [0124], [0132]-[0135], [0137], [0138], [0140].	1-50

☐ Further documents are listed in the continuation of Box C. ☐

* 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 application or patent 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
03 December 2008 (03.12.2008)	29DEC 2008
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (April 2007)