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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 July 2003 (24.07.2003)

PCT

(10) International Publication Number
WO 03/060744 A1

(51) International Patent Classification⁷: G06F 15/173, H04L 9/00

(21) International Application Number: PCT/US02/30630

(22) International Filing Date: 26 September 2002 (26.09.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/347,060	8 January 2002 (08.01.2002)	US
10/127,938	22 April 2002 (22.04.2002)	US

(71) Applicant: **AVAYA TECHNOLOGY CORP.** [US/US]; 211 Mount Airy Road, Basking Ridge, NJ 07920 (US).

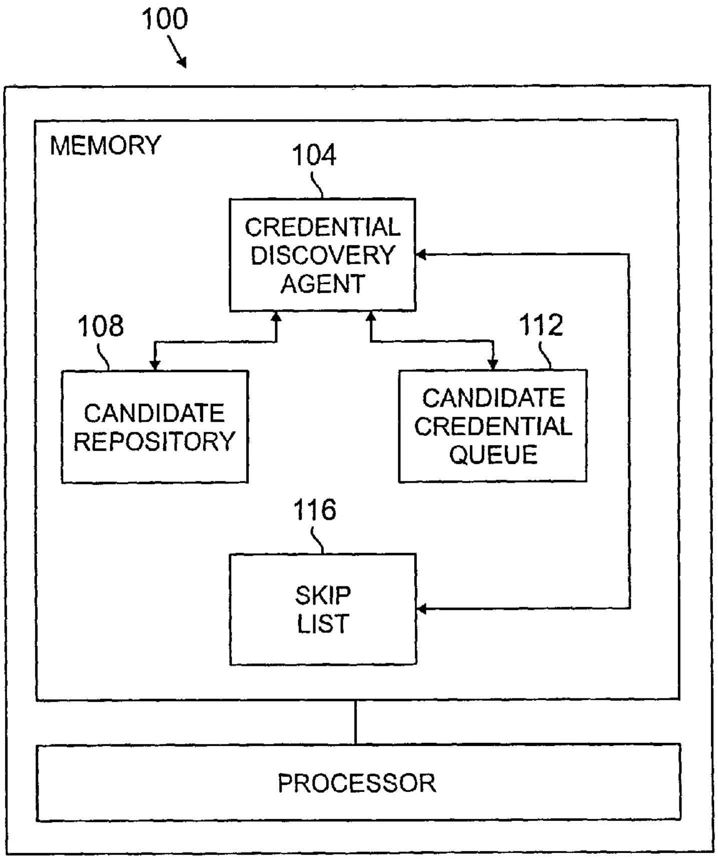
(72) Inventors: **GORINGE, Christopher, M.**; 24 Caird Place, Seven Hills, NSW 2147 (AU). **KRUMM-HELLER, Alex, M.**; 44 Monash Road, Gladesville, NSW 2111 (AU). **SCHREUDER, James, D.**; 4 Nowraine Street, Summer Hill, NSW 2130 (AU). **MINHAZUDDIN, Muneyb**; 18 Sciarra Cresent, Acacia Gardens, Quakers Hill, NSW 2763 (AU). **SMITH, Melanie**; 45 Nelson Street, Rozelle, NSW 2039 (AU). **RANKINE, Alastair, J.**; 1544 Harrison Avenue, Boulder, CO 80303 (US).

(74) Agents: **SWARTZ, Douglas, W.** et al.; Sheridan Ross P.C., Suite 1200, 1560 Broadway, Denver, CO 80202-5141 (US).

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

[Continued on next page]

(54) Title: CREDENTIAL MANAGEMENT AND NETWORK QUERYING



(57) Abstract: The present invention is directed to a system and method for determining one or more credentials of a network device. The system and method select a first network device from among a plurality of network devices, access a credential repository (108), contact the first network device, and test the validity of the first set of credentials. The credential repository (108) comprises a first set of credentials corresponding to the first network device. If user provides invalid or no credentials, a candidate credential queue (112) can be used to guess a valid second set of credentials when the first set of credentials is not valid.

SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

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

Published:

— *with international search report*

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

CREDENTIAL MANAGEMENT AND NETWORK QUERYING

FIELD OF THE INVENTION

The present invention is related generally to authentication in data networks and specifically to determining credentials for computational components in data networks.

BACKGROUND OF THE INVENTION

In computational networks, it is common to have one or more automated network management system (NMS) devices for collecting data to ascertain levels of performance (*e.g.*, BER, loss of synchronization, *etc.*), equipment, module, subassembly, and card failures, circuit outages, levels of traffic, and network usage. NMS devices typically interrogate network components, such as routers, ethernet switches, and other hosts for stored information. As will be appreciated, a network device or component is a computational component that may or may not have a physical counterpart, *e.g.*, the component may be a virtual computational component such as an interface. Examples of proprietary network management systems include Hewlett-Packard's OPENVIEW™, IBM's NETVIEW™, and Digital Equipment Corporation's EMA™. To permit such network management systems in distributed processing networks to communicate with hosts for monitoring and controlling the enterprise network, network management communication protocols have been developed, such as the Simple Network Management Protocol or SNMP and the Common Management Information Protocol or CMIP.

During interrogation, NMS devices interact with authentication systems present in network devices, such as routers. Authentication systems are an essential part of network security. Typically, a user is able to access information in certain network devices only by entering one or more credentials. As used herein, a "credential" refers to a set of information (e.g., a character or string of characters) which must be provided to a computational component for access to information in the computational component to be provided. Examples of credentials for version 1 of SNMP include a community string, for version 3 of SNMP User-Based/Security Model or include USM mode, user name, authentication method, authentication password, privacy method, and privacy password, and for TELNET include a user login, password, router type, and prompt. As will be appreciated, different credentials can be required for differing levels of information access, *e.g.* read-only access and supervisor levels.

When a new NMS system device is connected to a network, the NMS device must learn the various forms of authentication used to be able to interrogate network devices. The learning process typically involves a user manually setting credentials before using the tool on the network. This is not only a slow task but also fails to easily allow for dynamic changes of authentication during use. For example, some network security schemes require a credential to be periodically changed to maintain a high level of network security.

Network management personnel typically compromise network security for ease of credential configuration in NMS devices. For example, some network management systems rely on the credential being set to a default credential (generally public level access credentials) on all components in the network. In some applications, the varying access levels to the network components are compromised by using a common default credential. This practice unnecessarily restricts the type of authentication to a type of default credential and can restrict with what type of equipment the network management system can be used and also compromises network security. Other network management systems do permit a limited number of passwords to be entered before the network management system performs interrogation but fail to allow for dynamic changes in authentication during use.

SUMMARY OF THE INVENTION

These and other needs are addressed by the various embodiments and configurations of the present invention. The credential discovery agent of the present invention determines credentials of network devices by maintaining a credential repository, which typically is a historical record of credentials used in the network, and/or a candidate credential queue, which typically is a listing of credentials ordered based on the likelihood that the credentials are in current use by the network devices of interest. In one architecture, the agent, repository, and queue consider that network management personnel reuse credentials over time and, at any given time, reuse the same credential for different network devices.

In one embodiment, the credential discovery agent determines one or more credentials of a network device by performing the steps of:

(a) selecting a first network device from among a plurality of network devices;

(b) accessing the credential repository, the credential repository comprising a first set of credentials corresponding to the first network device;

(c) contacting the first network device; and

(d) testing the validity of the first set of credentials.

The credential repository holds credentials that have been learned (e.g., from the user, by a successful guess, etc.). The repository is used to save the credentials between executions and can have things removed or added to it during agent operation. Between runs the repository allows the credentials to be stored so they can be used on subsequent runs of the agent.

The credential repository can include a number of variables associated with the first network device. These variables can include a corresponding credential state, a corresponding protocol identifier, a corresponding (IP) address, a total number of instances of use of at least one credential in the first set of credentials, a corresponding candidate credential frequency counter associated with at least one credential in the first set of credentials, a recency of use of at least one credential in the first set of credentials, and the administrative locality of at least one credential in the first set of credentials. The protocol identifier is indicative of the protocol defining or associated with the credentials and/or the authentication system used to communicate with the network device.

If the agent is unable to determine the valid credentials using the repository, the agent can prompt the user for additional credentials to test. In this manner, the user can provide input into the operation of the agent. The user is typically prompted for credentials as the agent contacts differing types of network devices. The user fills in the required credential(s) and the agent then verifies that the inputted credential(s) are correct by using the inputted credential(s) to contact the network device. When the credential(s) is valid, it is copied into the repository.

In another embodiment, the agent determines at least one credential of a network device when previously used credentials are invalid or unsuccessfully validated by performing the steps of:

(a) selecting one or more credential from a candidate credential queue;

(b) contacting a network device;

(c) testing the validity of the credential(s); and

(d) assigning a priority value or ranking to the tested credential based on whether or not the credential(s) is valid.

The priority value is used to determine an order in which to test corresponding credentials when it is necessary to guess the credential in use by the network device. In one configuration, the priority value is used to order the listing of credentials in the candidate credential queue. In another configuration, the priority value is determined based on one or more of a candidate credential frequency counter, a recency of use counter, and an administrative locality associated with the corresponding set of credentials.

In one configuration, the agent attempts to guess the credential before prompting the user for a credential. These guesses may include standard defaults, credentials which have been used or tried elsewhere in the network, or credentials which have been provided by the user up-front.

The agent, credential repository, and candidate credential queue can have a number of advantages. First, the agent can dynamically and automatically maintain the repository and candidate over time. Conventional tools allow for a limited number of credentials to be entered before the tool is used, but such tools do not allow for dynamically adding more credentials during use of the tool. In contrast, the agent updates the repository and queue during and/or after each run of the credential discovery agent. Second, the agent can be convenient to use and determine credentials in significantly less time than conventional techniques. Third, the agent can reduce the amount of user interaction by making educated guesses at the credential before prompting the user. In some configurations, the agent speculatively tests credentials on any new network devices detected to reduce the requirement for user interaction. Fourth, the agent can obviate the need for the user to manually input an extensive list of credentials before the agent is run. Fifth, the agent can make network management systems more flexible in dealing with unknown credentials by prompting the user and also storing known credentials in the repository for later use. These and other advantages will be apparent from the disclosure of the invention(s) contained herein.

The above-described embodiments and configurations are neither complete nor exhaustive. As will be appreciated, other embodiments of the invention are possible utilizing, alone or in combination, one or more of the features set forth above or described in detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram of a computational architecture according to a first embodiment of the present invention and

Figs. 2A and 2B depict a flow schematic of the credential discovery agent.

DETAILED DESCRIPTION

Fig. 1 depicts a computational architecture 100 according to a first embodiment of the present invention. The architecture 100 comprises a credential discovery agent 104 configured to determine one or more valid credentials for selected network devices or components, a credential repository 108 mapping credentials to IP addresses and containing other information, a candidate credential queue 112 listing credentials in order of priority for credential guessing by the credential discovery agent 104, and a skip list 116 listing IP addresses for which credential determination was not performed at the request of the user.

The credential repository 108, which is typically encrypted, is loaded at runtime of the agent 104 to provide an initial population of credentials for IP addresses of network components. The repository can include a number of fields for each IP address including one or more credentials, a credential state, a protocol identifier, and protocol access level for credential and/or for each credential a protocol identifier, corresponding IP addresses, the total number of instances of use of the credential by the listed IP addresses, a priority of use of the credential, a candidate credential frequency counter to reflect the frequency of use of the credential in the network (or in the credential repository), recency of use of the (valid) credential in the network (or recency of use as determined by the agent 104), the administrative locality of the credential, and other information that can be used to assign a priority value to the credential in the candidate credential queue 112. During operation of the agent 104, the credential repository 108 is updated by the agent 104, such as after each IP address is considered and/or after all of the IP addresses are considered. As will be appreciated, a unique network component identifier other than IP address can be employed, depending upon the protocol associated with the network component.

The candidate credential queue 112 provides a listing of credentials, each of which has a corresponding priority and protocol identifier. When guessing, the agent 104 tests the credentials in order of each credential's corresponding priority value. In one implementation for version 1 of SNMP, the queue 112 is initially populated with a credential containing the community string "public". During any individual discovery task, each credential, which is successfully validated by the credential repository is also added to the queue 112, though with a lower priority than that of the "public" credential. As will be appreciated, the priority can be assigned based on any one of or combination of factors including the candidate credential frequency counter to reflect the frequency of use of the credential in the network (or in the credential repository), the recency of use of the (valid) credential in the network (or the recency of use as determined by the agent 104), and/or the administrative locality of the credential relative to the IP address under consideration (*e.g.*, if the network component under consideration is associated with or connected to another network component which has a corresponding credential the corresponding credential is first used as a test credential).

The skip list 116 is simply a listing of network component IP addresses for which the agent 104 will not perform a credential determination.

The operation of the credential discovery agent 104 is depicted in Figs. 2A and 2B. Referring to Fig. 2A, the agent 104 is created in step 200.

In step 204, the agent 104 determines if the credential repository 108 is populated with one or more IP addresses. If the credential repository 108 is empty or nonexistent, the agent 104 initializes the repository and proceeds to step 208. If the credential repository is not empty, the repository is loaded by the agent in step 212. Initially, all credentials in the credential repository 108 are assumed to be untested or not yet successfully validated. The agent 104 then proceeds to step 208.

In decision diamond 208, the agent determines whether the user has requested to stop discovery. If the user has so requested, the agent 104 proceeds to step 216 and returns with an error code (STOP_CRED) indicating the request. If the user has not so requested, the agent proceeds to step 220.

In step 220, the agent selects an initial IP address for credential determination. The initial IP address is typically selected from a network access list of one or more IP addresses provided by the user. This network access list can be generated by the user manually or automatically using a network topology discovery algorithm such as described in U.S. Patent Applications entitled "Topology Discovery by Partitioning Multiple Discovery Techniques" and "Using Link State Information to Discover IP Network Topology", both by Goringe, et al., filed concurrently herewith and incorporated herein by this reference. The network access list typically includes a list of network component identifiers (*e.g.*, IP addresses) and a corresponding credential state field for each identifier.

The agent then proceeds to step 224 where the agent determines if the selected IP address is on the skip list 116.

If the selected IP address is on the skip list 116, the agent 104 sets the credential state for the IP address in the network access list as NO CREDENTIAL in step 228 and proceeds to decision diamond 232 where the agent determines if there is another IP address on the network access list. The NO CREDENTIAL state means that no valid credential was obtained for the corresponding IP address. The corresponding IP address entry in the credential repository 108 (if any) is typically not removed from the repository if the IP address is skipped. If a next IP address is available, the agent 104 gets the next IP address in step 236 and repeats step 224. If a next IP address is unavailable, the agent 104 saves the updated credential repository and terminates operation in step 216.

If the IP address is not on the skip list, the agent 104 next determines in decision diamond 240 whether there is in the credential repository 108 an IP address entry matching the selected IP address. In other words, the agent 104 determines whether the repository 108 contains a credential corresponding to the selected IP address.

When a corresponding credential exists, the agent in step 244 tests the validity of the credential by known techniques. The techniques, of course, depend upon the protocol being used by the network component corresponding to the IP address.

When the credential is valid in step 248, the agent 104 proceeds to step 252 where the credential is added to the candidate credential queue 112 and then to step 256 where the corresponding entry in the network access list (and/or credential repository) is assigned the credential state of FOUND CREDENTIAL. This state means that the credential was validated. The credential is stored in the appropriate out-parameter corresponding to the IP address. The agent 104 may increment a candidate credential frequency counter and/or otherwise adjust the priority of the credential in the candidate credential queue 112. The agent 104 then returns to step 232 discussed above.

When the credential is invalid in step 248, the agent 104 must determine the reason why the credential was not successfully validated. The unsuccessful validation could be due to an invalid credential or to the network component being uncontactable at the time. Accordingly, the agent 104 in step 260 pings the device and in decision diamond 264 determines whether a response is received from the component within a selected time interval. The ping step 260 can be done using an Internet Control Message Protocol or ICMP echo request.

In any event, if a response is not received, the agent 104 in step 268 assigns a credential state of UNCONTACTABLE to the corresponding entry in the network access list (and/or credential repository) and returns to step 232 above. As will be appreciated, the credential state of UNCONTACTABLE indicates that the network component was unresponsive to the ping. The corresponding IP address entry in the credential repository is not removed when the credential state is UNCONTACTABLE.

If a response is received, the agent 104 in step 272 removes the entry corresponding to the IP address from the credential repository 108, updates the entry corresponding to the credential in the credential repository 108, and adjusts the candidate credential queue 112 when the credential is listed in the candidate credential queue. As noted, the priority of the credentials in the queue 112 can be based on any number of factors, including usage of the credential. When the credential is no longer in use by a network component, the priority often requires adjustment downward to reflect the nonuse. Typically, the candidate credential frequency counter is decremented.

The agent next proceeds to step 276 where the agent 104 attempts to guess the credential from the credentials listed in the queue 112. When guessing, the agent 104 tries all of the credentials in the queue 112 in order of priority. As shown in steps 280, 284, and 288, each credential is retrieved sequentially and an attempt is made to validate it.

When a credential is successfully validated in steps 276, 280, 284 and 288, the credential is stored in the appropriate out-parameter corresponding to the IP address in step 292 and the corresponding entry in the network access list (and/or credential repository) is assigned the credential state of FOUND CREDENTIAL in step 256. The agent 104 may increment a candidate credential frequency counter and/or otherwise adjust the priority of the credential in the candidate credential queue 112. The agent 104 then returns to step 232 which is discussed above.

When a credential is unsuccessfully validated in steps 276, 280, 284 and 288, the agent 104 in step 296 checks the user's preferences regarding whether or not the user is to be prompted for further instructions regarding the IP address. This preference is indicated by using a flag state. If no credentials that can be used to access the remote network component are found or if none of the found credentials work, the user may be prompted for a new set of credentials. The user is prompted only if the existence of the remote network component has earlier been confirmed by pinging as noted above and the flag to not prompt the user is not set (or vice versa).

In decision diamond 300, the agent 104 determines whether to prompt the user. When the prompt flag is set(*i.e.*, the user does not want to be prompted) then the agent 104 in step 304 marks the IP address for which no credential can be found as through the user had responded with a skip command. In other words, the IP address is added to the skip list 116. The corresponding entry in the network access list (and/or credential repository) is then assigned in step 308 a credential state of NO CREDENTIAL. The agent 104 then returns to step 232 discussed above.

When the prompt flag is not set(*i.e.*, the user wants to be prompted), then the agent 104 in step 312 prompts the user. The user can respond in five different ways. First, the user can respond by entering a credential as shown by decision diamond 316. When a credential is entered, the agent 104 tests the validity of the credential in step 320. When in step 324 the credential is valid, the agent proceeds to step 292 discussed above. When in step 324 the credential is invalid, the agent returns to step 312 and again prompts the user. Second, the user can respond by instructing the agent 104 to skip the IP address. This is shown in step 328. When the agent 104 receives this response, the agent 104 proceeds to step 304 discussed previously. Third, the user can respond by instructing the agent 104 to stop. This is shown in step 332. In that event, the agent 104 sets the prompt flag to stop in step 336, adds the address to the skip list 116 in step 340, saves the updated credential table and terminates operation in step 344. Fourth, the user can respond by instructing the agent 104 to no prompt. This is shown by step 348. In that event, the agent 104 sets the prompt flag to no prompt in step 352 and proceeds to step 304 discussed above. Finally, the user can provide an unintelligible or unrecognized response. In that event, the agent 104 returns to step 312 and again prompts the user.

Returning to decision diamond 240, when a corresponding credential is not in the credential repository the agent 104 in step 356 pings the device as discussed above to determine if the network component is contactable. The agent 104 in decision diamond 360 determines whether or not a response is timely received. When a timely response is received, the agent 104 proceeds to step 276 discussed above. When no timely response is received, the agent 104 proceeds to step 268 also discussed above.

A number of variations and modifications of the invention can be used. It would be possible to provide for some features of the invention without providing others. For example in one alternative embodiment, the architecture discussed above supports other versions of SNMP, such as version 3 of SNMP, and/or protocols other than SNMP, such as TELNET and CMIP. In this embodiment, the credential object would be defined in way(s) to support one or more different protocols. For example, the architecture can support multiple protocols at the same time. A protocol identifier is then used in the credential repository to identify the protocol corresponding to the network component and the credential object accorded a number of alternative definitions depending upon the corresponding protocol. In this embodiment, the credentials in the candidate credential frequency queue 112 would only be used in the credential guessing routine for the network component corresponding to the IP address under consideration when the network component used the protocol corresponding to the credential (as shown by the corresponding protocol identifier). In another alternative embodiment, a unique network component identifier other than IP address is used in the credential repository. For example, the identifier could be a component id as defined by the OSPF protocol, and/or credentials preconfigured by the user to be used as candidates for guessing. In another alternative embodiment, credentials in the repository that are not successfully validated are not removed from the respository but are marked with an appropriate flag indicating this fact. The credential may still be used by the network at a subsequent time or be concurrently used by a network component that is not listed in the credential repository. These credentials are eligible for inclusion in the candidate credential queue 112. As will be appreciated, some network security schemes rotate use of or periodically reuse credentials. In yet another alternative embodiment, the candidate credential queue can include credentials from sources other than the network itself. For example, the queue can include credentials that are in common or widespread use in the industry, default credentials in use when a device is initially acquired from a supplier or manufacturer, and/or credentials that are provided by the user in advance.

The present invention, in various embodiments, includes components, methods, processes, systems and/or apparatus substantially as depicted and described herein, including various embodiments, subcombinations, and subsets thereof. Those of skill in the art will understand how to make and use the present invention after understanding the present disclosure. The present invention, in various embodiments, includes providing devices and processes in the absence of items not depicted and/or described herein or in various embodiments hereof, including in the absence of such items as may have been used in previous devices or processes, e.g. for improving performance, achieving ease and\or reducing cost of implementation.

In one alternative embodiment, the credential discovery agent is implemented in whole or part as an application specific integrated circuit or other type of logic circuit.

The foregoing discussion of the invention has been presented for purposes of illustration and description. The foregoing is not intended to limit the invention to the form or forms disclosed herein. Although the description of the invention has included description of one or more embodiments and certain variations and modifications, other variations and modifications are within the scope of the invention, e.g. as may be within the skill and knowledge of those in the art, after understanding the present disclosure. It is intended to obtain rights which include alternative embodiments to the extent permitted, including alternate, interchangeable and/or equivalent structures, functions, ranges or steps to those claimed, whether or not such alternate, interchangeable and/or equivalent structures, functions, ranges or steps are disclosed herein, and without intending to publicly dedicate any patentable subject matter.

What is claimed is:

1. A method for determining one or more credentials of a network device, comprising:

selecting a first network device from among a plurality of network devices;

accessing a credential repository, the credential repository comprising a first set of credentials corresponding to the first network device;

contacting the first network device; and

testing the validity of the first set of credentials.

2. The method of Claim 1, wherein the credential repository further comprises, for the first network device, a plurality of a corresponding credential state, a corresponding protocol identifier, a corresponding address, a total number of instances of use of at least one credential in the first set of credentials, a corresponding candidate credential frequency counter associated with at least one credential in the first set of credentials, a recency of use of at least one credential in the first set of credentials, and the administrative locality of at least one credential in the first set of credentials.

3. The method of Claim 1, further comprising:

assigning a credential state to at least one credential in the first set of credentials.

4. The method of Claim 1, further comprising, when at least one credential in the first set of credentials is valid:

adding the at least one credential to a candidate credential queue.

5. The method of Claim 1, further comprising, when at least one credential in the first set of credentials is not valid:

pinging the first network device to determine whether the first network device is contactable.

6. The method of Claim 1, further comprising, when at least one credential in the first set of credentials is not valid:

selecting a second set of credentials from a candidate credential queue; and

testing the validity of the second set of credentials.

7. The method of Claim 6, further comprising, when at least one credential in the second set of credentials is not valid:

prompting a user for a third set of credentials; and when the third set of credentials is received from the user, testing the validity of the third set of credentials.

8. The method of Claim 1, wherein the plurality of network devices comprises a second network device, each of the first and second network devices has an associated protocol identifier indicative of a protocol used by the network device, and the first and second protocol identifiers are different.

9. The method of Claim 6, further comprising:

comparing a protocol associated with the first network device with a protocol identifier associated with the second set of credentials.

10. The method of Claim 9, wherein, when the protocol associated with the first network device is different from the protocol associated with the protocol identifier, the testing step is not performed.

11. A credential repository for a network, comprising:

a plurality of network device identifiers, at least first and second network devices in the plurality of network devices using different protocols;

for each of the plurality of network devices, the credential repository further comprises, for the first and second network devices, a corresponding protocol identifier; and

for each of the plurality of network devices, a corresponding set of credentials configured for the protocol associated with the corresponding protocol identifier.

12. The credential repository of Claim 11, comprising, for each of the plurality of network device identifiers, a plurality of a corresponding credential state, a corresponding address, a total number of instances of use of at least one credential in the corresponding set of credentials, a corresponding candidate credential frequency counter associated with at least one credential in the corresponding set of credentials, a recency of use of at least one credential in the first set of credentials, and an administrative locality of at least one credential in the corresponding set of credentials.

13. A system for determining one or more credentials of a network device, comprising:

means for selecting a first network device from among a plurality of network devices;

a credential repository comprising a first set of credentials corresponding to the first network device;

means for accessing the credential repository;

means for contacting the first network device; and

means for testing the validity of the first set of credentials.

14. The system of Claim 13, wherein the credential repository further comprises, for the first network device, a plurality of a corresponding credential state, a corresponding protocol identifier, a corresponding address, a total number of instances of use of at least one credential in the first set of credentials, a corresponding candidate credential frequency counter associated with at least one credential in the first set of credentials, a recency of use of at least one credential in the first set of credentials, and the administrative locality of at least one credential in the first set of credentials.

15. The system of Claim 13, further comprising:

means for assigning a credential state to at least one credential in the first set of credentials.

16. The system of Claim 13, further comprising, when at least one credential in the first set of credentials is valid:

means for adding the at least one credential to a candidate credential queue.

17. The system of Claim 13, further comprising, when at least one credential in the first set of credentials is not valid:

means for pinging the first network device to determine whether the first network device is contactable.

18. The system of Claim 13, further comprising, when at least one credential in the first set of credentials is not valid:

second means for selecting a second set of credentials from a candidate credential queue; and

second means for testing the validity of the second set of credentials.

19. The system of Claim 18, further comprising, when at least one credential in the second set of credentials is not valid:

means for prompting a user for a third set of credentials; and

when the third set of credentials is received from the user, third means for testing the validity of the third set of credentials.

20. A system for determining one or more credentials of a network device, comprising:

a credential repository comprising a first set of credentials corresponding to a first network device; and

a credential discovery agent configured to select the first network device from among a plurality of network devices, access the credential repository, contact the first network device, and test the validity of the first set of credentials.

21. The system of Claim 20, wherein the credential repository further comprises, for the first network device, a plurality of a corresponding credential state, a corresponding protocol identifier, a corresponding address, a total number of instances of use of at least one credential in the first set of credentials, a corresponding candidate credential frequency counter associated with at least one credential in the first set of credentials, a recency of use of at least one credential in the first set of credentials, and the administrative locality of at least one credential in the first set of credentials.

22. The system of Claim 20, wherein the credential discovery agent is further configured to assign a credential state to at least one credential in the first set of credentials.

23. The system of Claim 20, wherein the credential discovery agent is further configured, when at least one credential in the first set of credentials is valid, to add the at least one credential to a candidate credential queue.

24. The system of Claim 20, wherein the credential discovery agent is further configured, when at least one credential in the first set of credentials is not valid, to ping the first network device to determine whether the first network device is contactable.

25. The system of Claim 20, wherein the credential discovery agent is further configured, when at least one credential in the first set of credentials is not valid, to select a second set of credentials from a candidate credential queue and test the validity of the second set of credentials.

26. The system of Claim 25, wherein the credential discovery agent is further configured, when at least one credential in the second set of credentials is not valid, to prompt a user for a third set of credentials and, when the third set of credentials is received from the user, to test the validity of the third set of credentials.

27. A candidate credential queue for determining a credential of a network device, comprising:

a plurality of sets of credentials, each of the plurality of sets of credentials having a corresponding ranking indicative of a probability that the plurality of sets of credentials is currently in use by the network device.

28. The candidate credential queue of Claim 27, wherein the ranking is determined based on at least one of a candidate credential frequency counter, a recency of use counter, an administrative locality associated with the corresponding set of credentials, preferences of the user, a user configured priority, and an ordering of validation of at least one set of credentials on another network device.

29. A method for determining at least one credential of a network device, comprising:

selecting at least one credential;

contacting a network device;

testing the validity of the at least one credential; and

assigning a ranking to the at least one credential based on whether or not the at least one credential is valid.

30. The method of Claim 29, wherein the ranking reflects a probability that the at least one credential is in current use in the network associated with the network device.

31. A system for determining at least one credential of a network device, comprising:

a credential discovery agent configured to assign a rank to at least one credential based on whether or not the at least one credential is valid.

32. The system of Claim 31, wherein the rank reflects a probability that the at least one credential is in current use in the network associated with the network device.

33. The system of Claim 31, wherein the credential discovery agent is further configured to select at least one credential from a candidate credential queue, test the validity of the at least one credential, and assign the rank to the at least one credential based on whether or not the at least one credential is valid.

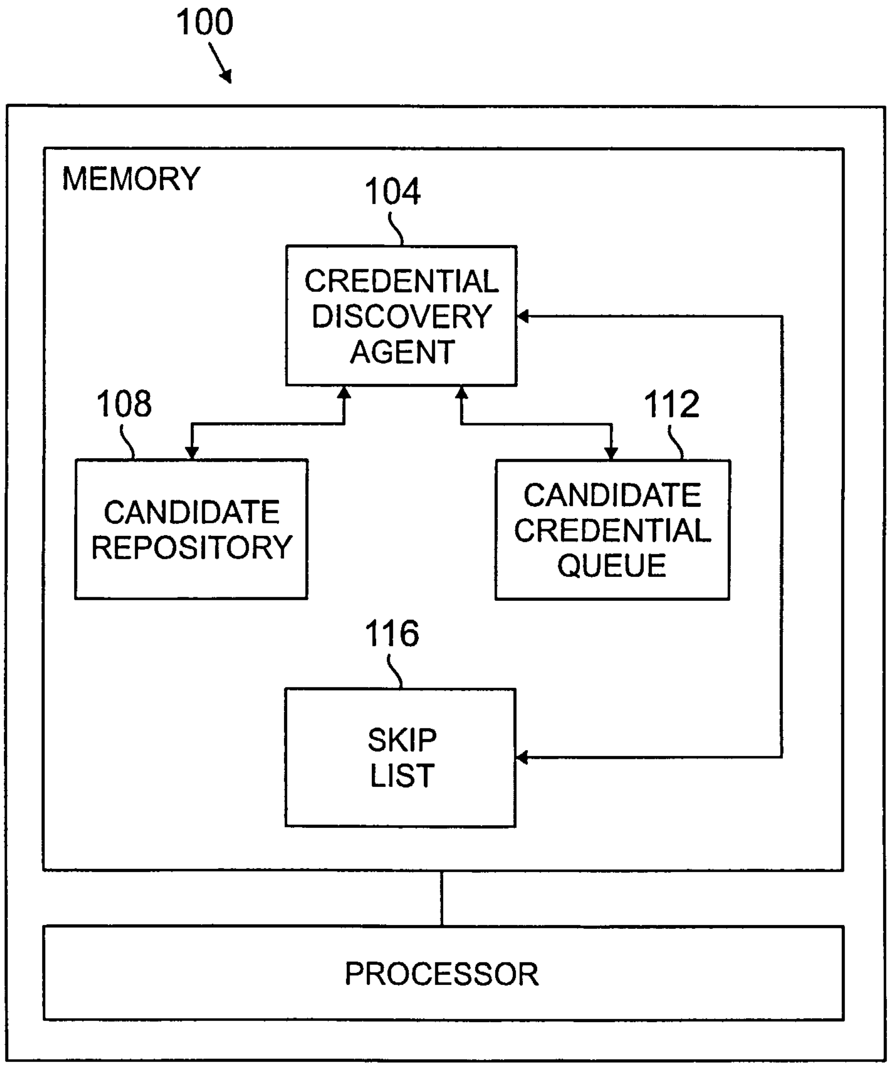

100
MEMORY
104
CREDENTIAL DISCOVERY AGENT
108
CANDIDATE REPOSITORY
112
CANDIDATE CREDENTIAL QUEUE
116
SKIP LIST
PROCESSOR

FIG. 1

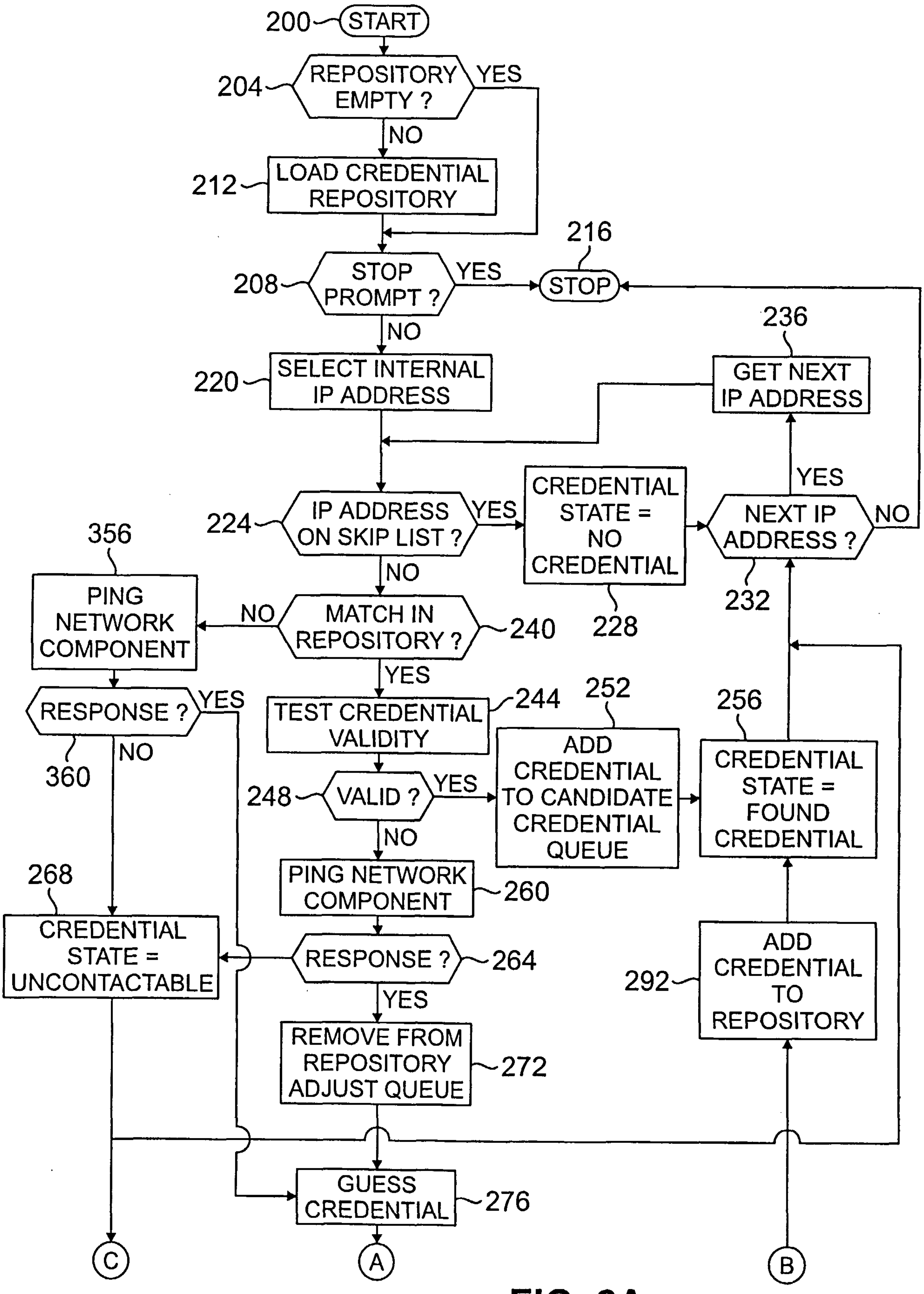

200
START
204
REPOSITORY EMPTY ?
YES
NO
212
LOAD CREDENTIAL REPOSITORY
216
208
STOP PROMPT ?
YES
STOP
NO
236
GET NEXT IP ADDRESS
220
SELECT INTERNAL IP ADDRESS
YES
224
IP ADDRESS ON SKIP LIST ?
YES
CREDENTIAL STATE = NO CREDENTIAL
NEXT IP ADDRESS ?
NO
356
NO
232
PING NETWORK COMPONENT
NO
MATCH IN REPOSITORY ?
240
228
YES
RESPONSE ?
YES
TEST CREDENTIAL VALIDITY
244
252
256
360
NO
ADD CREDENTIAL TO CANDIDATE CREDENTIAL QUEUE
CREDENTIAL STATE = FOUND CREDENTIAL
248
VALID ?
YES
NO
268
PING NETWORK COMPONENT
260
CREDENTIAL STATE = UNCONTACTABLE
RESPONSE ?
264
292
ADD CREDENTIAL TO REPOSITORY
YES
REMOVE FROM REPOSITORY ADJUST QUEUE
272
GUESS CREDENTIAL
276
C
A
B

FIG. 2A

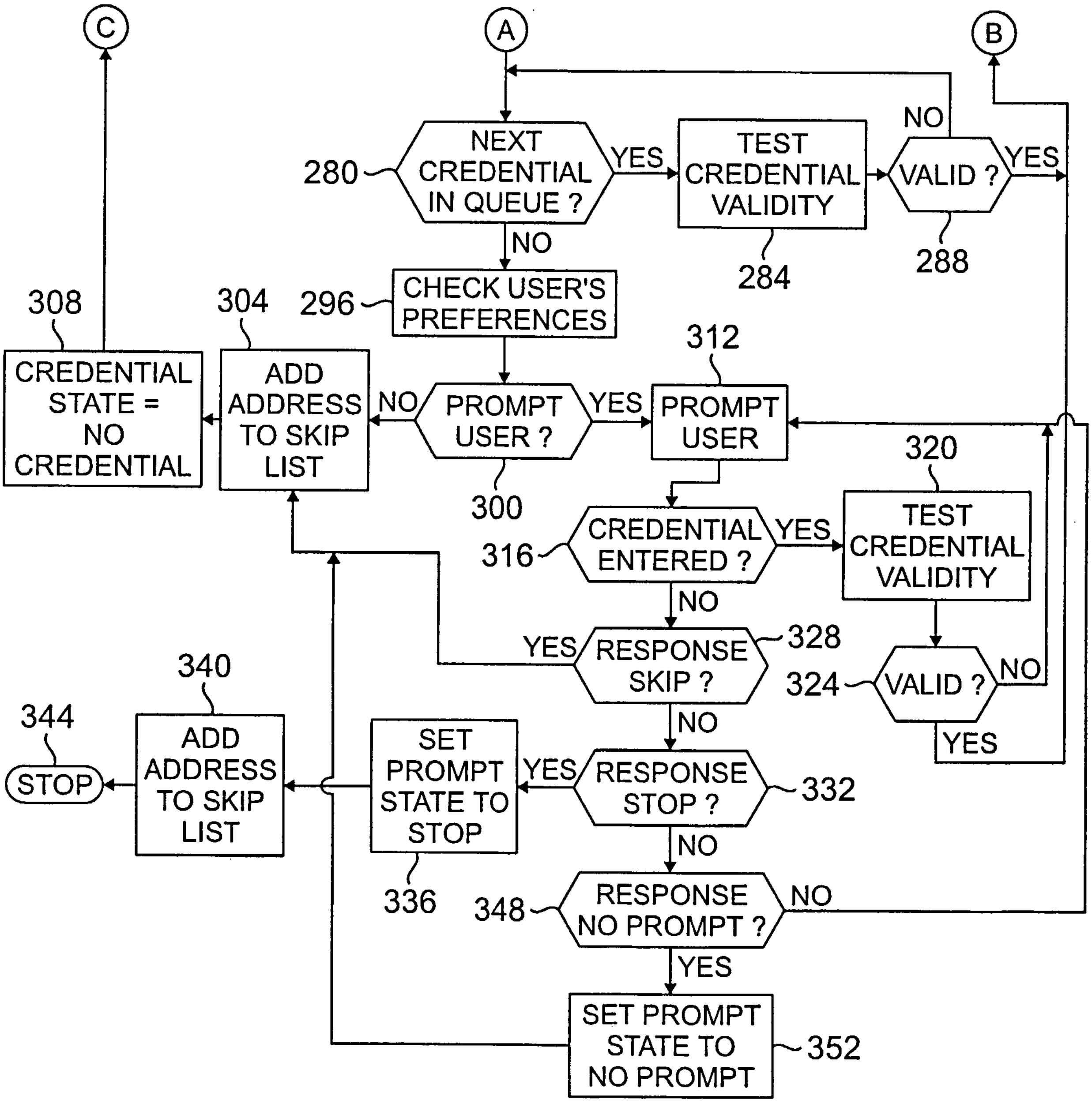

C
A
B
NEXT CREDENTIAL IN QUEUE ?
280
YES
NO
TEST CREDENTIAL VALIDITY
284
VALID ?
288
NO
YES
CHECK USER'S PREFERENCES
296
PROMPT USER ?
300
NO
YES
ADD ADDRESS TO SKIP LIST
304
CREDENTIAL STATE = NO CREDENTIAL
308
PROMPT USER
312
CREDENTIAL ENTERED ?
316
YES
NO
TEST CREDENTIAL VALIDITY
320
VALID ?
324
NO
YES
RESPONSE SKIP ?
328
YES
NO
RESPONSE STOP ?
332
YES
NO
SET PROMPT STATE TO STOP
336
ADD ADDRESS TO SKIP LIST
340
STOP
344
RESPONSE NO PROMPT ?
348
NO
YES
SET PROMPT STATE TO NO PROMPT
352

FIG. 2B

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US02/30630

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 15/173; H06L 9/00
US CL : 709/224, 225, 226; 713/155,156,201

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 709/224, 225, 226; 713/155,156,201

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	NOVOTNEY, J et al. "An Online Credential Repository for the Grid: MYProxy" from High Performance Distributed Computing, 2001 Proceedings. Lawrence Berkely Lab. Berkely, CA USA pages 104-111 7-9 Aug. 2001. see pages 107-110 sections 4-6.	1
Y,P	US2002/00116647 A1 (MONT et al.) 22 August 2002 (22.08.2002), pages 5-7 paragraphs 85-140	2-33
Y,P	US2002/0144149 A1 (HANNA et al.) 03 October 2002 (03.10.2002), pages 4, 5 paragraphs 38-50	2-33
Y	US2002/0112062 A1 (BROWN et al.) 15 August 2002 (15.08.2002), pages 1 paragraphs 6-10, pages 2-3 paragraphs 26-47	1, 18, 19, 20
A	US 2001/0049786 A1 (HARRISON et al.) 06 December 2001 (06.12.2001), pages 3-6 paragraphs 37-77	1, 6, 13, 18, 20, 25, 26
A,P	US 2002/0087704 A1 (CHENAIS et al) 04 July 2002 (04.07.2002), pages 2-3 paragraphs 30-36	8-11
A,P	US 2002/0161591 A1 (DANNEELS et al.) 31 October 2002 (31.10.2002), figure 1, paragraphs 18-25	1-33

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

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier application or patent 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)	"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
"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	"&"	document member of the same patent family

Date of the actual completion of the international search

12 November 2002 (12.11.2002)

Date of mailing of the international search report

03 JAN 2003

Name and mailing address of the ISA/US

Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703)305-3230

Authorized officer

Glenton Burgess for

Telephone No. (703) 305-3900

INTERNATIONAL SEARCH REPORT

PCT/US02/30630

Continuation of B. FIELDS SEARCHED Item 3:
IEEE
credental <near/1> (repository <or> database <or> set <or> list)

ACM
"credential repository"