METHOD AND SYSTEM FOR INTERROGATING THE INTERNET

DESCRIPTION OF THE INVENTION

THIS INVENTION relates to a method and system for interrogating the Internet to identify a server to which a user at a remote location belongs but which the user is unable to specify.

It is often desired for an Internet user travelling on business or at leisure to be able to establish a connection at a remote location with a server to which the user belongs, for example in order to retrieve electronic mail.

Software systems, known as remote access mail clients, for retrieving mail for a user located remotely from the user's electronic mail server already known. However, these known remote access mail clients require the user to specify the electronic mail server concerned by supplying the server name and the numerical Internet Provider (IP) address.

If the user is unable to specify the server in this way, the user will be unable to retrieve the electronic mail at the remote location. The user is thus obliged to carry the relevant information with him and, since the information is not of the kind which can be readily memorised, the user may have to carry the information in written form.

If the information is carried in the user's memory, it may be forgotten or imperfectly recalled and, if it is carried in the form of a written list, it may be lost or misplaced and risk falling into the wrong hands.

Moreover, many users of the Internet are not technically sophisticated and do not have a complete knowledge or understanding of the technical terms and information associated with the Internet.

It is therefore an object of the present invention to provide a method and system enabling the identification of a server to which a user at a remote location belongs whilst only requiring the user to provide basic, easily remembered information.

Accordingly, in one aspect, the invention provides a method of identifying a server to which a user at a remote location belongs but which the user is unable to specify, including the steps of: providing an access database containing records of servers supporting a specified electronic mail protocol or protocols; requiring from the user the electronic mail address and log-in password of the user; parsing the mail address to identify and remove the user identifier from the mail address and thereby obtain a presumed domain name of the user's server; interrogating the access database to determine whether it contains a record of a server corresponding to the presumed domain name; and retrieving the record of any correspondence server thus identified as the server to which the user belongs.

In the event that the access database contains no corresponding server record, the method may include the further steps of: assuming that the domain name is the user's server; checking the domain name for the user's mail; and identifying the domain name as the user's server if the domain name responds positively.

In the event that the access database contains no corresponding server record and the domain name responds negatively, the method may include the further steps of: sending out a Mail Exchange (MX) record enquiry to the Internet Domain Name System (DNS) database regarding the presumed domain name; listing the responses received from the DNS database; checking the responses in turn to determine whether a predetermined port or ports associated with the predetermined protocol or protocols is or are open or closed; and identifying a response having an open port or ports as the user's server.

The method may further include the further steps of; obtaining the IP address of the MX record; checking the open or closed status of the predetermined port or ports for a predetermined block of host IP addresses; writing all those IP addresses having the predetermined port or ports open into the access database; interrogating each IP address on the temporary database with the user's address and password; and identifying a successful IP address as the user's server.

In the event that the user's server is not identified from amongst the responses from the DNS database, the method may include the further steps of: requesting the full list of host names for the presumed domain name by DNS zone transfer; checking the open or closed status of the predetermined ports of the listed host names in turn; and identifying a host having open port status as the user's server.

In the event that the previous steps of the method have failed to identify the user's server, the method may include the further steps of: retrieving the IP address block which has been allocated to the presumed domain name by the Networked Information Centre (NIC); checking the open or closed status of the predetermined port or ports of the IP addresses in the block; storing all of the IP addresses having open port status in the access database; interrogating the stored IP addresses in turn with the user's address and password; and identifying a successful IP address as the user's server.

Advantageously, the method includes the steps of updating the access database with a record of a previously unrecorded server identified as the user's server or identified as supporting the predetermined protocol or protocols.

A preferred embodiment of the method includes the steps of retrieving the user's electronic mail from a server identified as the user's server and directing the mail to the user at the remote location.

In another aspect, the invention provides a system for identifying a server to which a user at a remote location belongs but which the user is unable to specify, including: an access database containing records of servers supporting a predetermined electronic mail protocol or protocols; and a remote access mail client associated with the database and having access to the Internet Domain Name System (DNS) database and to a search engine associated with the protocol or protocols; in which system the remote access mail client is arranged to require from the user the user's electronic mail address and password, to parse the mail address to identify and remove the user identity from the mail address and thereby obtain a presumed domain name of the user's server, to interrogate the access database to determine whether it contains a record of a server corresponding to the presumed domain name, and to retrieve the record of any corresponding server thus identified as the server to which the user belongs.

Preferably, the remote access mail client is arranged to assume that the presumed domain name is the user's server in the event that the access database contains no corresponding server record, to check the domain name for the user's mail and to identify the domain name as the user's server if the domain name responds positively.

If the database contains no corresponding server record and the presumed domain name responds negatively, the remote access mail client is arranged to send out a Mail Exchange (MX) record enquiry to the DNS database regarding the presumed domain name, to list the responses from the DNS database, to check the responses in turn to determine whether a predetermined port or ports associated with the protocol or protocols is or are open or closed, and to identify a response having an open port or ports as the user's server.

The remote access mail client may further be arranged to obtain the IP

This Sheet Has Been Replaced



address of the MX record, to check the open or closed status of the predetermined port or ports for a predetermined block of host IP addresses, to store all of the IP addresses having open port status in the access database interrogating the stored IP addresses in turn with the user's address and password, and to identify a successful IP address as the user's server.

If the user's server is not identified from amongst the responses from the DNS database the remote access mail client is arranged to request the full list of host names for the presumed domain name by DNS zone transfer, to check the open or closed status of the predetermined listed host names in turn and to identify a host having open port status as the user's server.

If the previous actions of the remote access mail client have failed to identify the user's server the remote access mail client is arranged to retrieve the IP address block which has been allocated to the presumed domain name by the Networked Information Centre (NIC), to check the open or closed status of the predetermined port or ports, to store all of the IP addresses having open port status in the access database, to interrogate the stored IP addresses in turn with the user's address and password, and to identify a successful IP address as the user's server.

Advantageously, the remote access mail client is arranged to write in the access database a record of any previously unrecorded server identified as the user's server.

In a preferred embodiment of the system, the remote access mail client is arranged to retrieve the user's mail from any server identified as the user's server and to direct it to the user at the remote location.

In order that the invention may be more readily understood, an embodiment

thereof will now be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 is a schematic diagram of a system embodying the invention for retrieving electronic mail for a user located remotely from the user's electronic mail server;

Figure 2 shows the form of a database included in the Figure 1 system; and

Figures 3A and 3B together form a flow chart illustrating the method of electronic mail retrieval implemented by the system of Figure 1.

Referring firstly to Figure 1, a system embodying the invention for retrieving electronic mail for a user at a location remote from the user's electronic mail server comprises a web-based electronic mail software application or remote access mail client 1, the operation of which will be described in more detail hereinafter. Associated with the remote access mail client 1 is a dynamic access database 2 containing records of servers which support a specified electronic mail protocol or protocols, in the present case the Post Office Protocol (POP3) and the Internet Message Access Protocol (IMAP4).

The remote access mail client 1 also has access to the Internet generally and, in particular to the Domain Name System (DNS) database 3 which correlates domain names and numerical IP addresses, to the WHOIS server 4 holding the IP address blocks allocated to domains, organisations and companies and to the POP3/IMAP4 search engine 5.

It is assumed that the user who wishes to retrieve his electronic mail has available at the remote location a computer 6 with Internet access and a browser 7

through which the user can gain access to the remote access mail client 1. The computer 6 may, for example, be any suitable computer served by any Internet Service Provider (ISP) local to a hotel or office to which the user has travelled.

The user's electronic mail server 8 which supports POP3/IMAP4 and which is to be identified and contacted by the remote access mail client 1 is shown in phantom lines in Figure 1.

Figure 2 illustrates the database 2 of the system embodying the invention. As will be seen the database 2 is divided into first and second Tables T1 and T2. The first Table T1 contains a series of user records each having three entries, namely the electronic mail address of a user who subscribes to the system, the identity (IP address) of the POP3/IMAP4 server to which the user belongs and an error flag number which may have the values 0-6 and the purpose of which will appear from the following description.

The second Table T2 contains domain records each having two entries, that is, the name of a domain and the identities (IP addresses) of the electronic mail servers associated with that domain.

In Figure 2, each Table T1, T2 contains a single entry exemplifying the user and domain records.

The method implemented by the system of figure 1 in identifying the user's server 8 and retrieving the user's electronic mail will first be described in outline and then in more detail with reference to Figures 3A and 3B.

In outline, the method requires the user first to log into the Internet Service Provider (ISP) at the computer 6 and then access the remote access mail client 1 via

the browser 7. On contracting the remote access mail client 1, the user is invited by the homepage of the system to type in merely the user's electronic mail address and log-in password and then to press ENTER. Thereupon, the remote access mail client initiates a sequence of actions in stages in order to attempt to identify a subscribing user's server from the minimal information provided by the user. Upon identifying the user's server, the remote access mail client 1 provides the server with the user's new address and password to retrieve the user's mail and deliver it to the user at the computer 6.

The method comprises three basic phases which are carried out in sequence to the extent necessary.

In a first stage of a first phase, the remote access mail client 1 parses the electronic mail address provided by the user and strips out the user identity from the address, working on the assumption that the user identity in the address is the same as the user's log-in password, thereby obtaining a presumed domain name of the user's server. The remote access mail client 1 then interrogates the access database 2 to determine whether the user is an existing user with a user record indicating the user's server and, if not, whether the database contains a domain record that corresponds to the presumed domain name of the user's server.

If there is such a record, the record is retrieved from the access database and the user's details are sent to the thus identified server to retrieve the user's mail and direct it to him at the computer 6.

By way of example, assume that the user enters the electronic mail address "userid@aztech.com.sg". After checking whether there is a user record corresponding to this address, the remote access mail client 1 strips out the user identity "userid" and checks the access database 2 to see if it contains a domain

record that corresponds to the domain name "aztech.com.sg". If there is such a record, it identifies the user's server and his mail can be retrieved and sent to the computer 6.

In a second stage of the first phase, the remote access mail client assumes that the domain name is the user's server and checks the domain name for the user's mail, identifying the domain name as the user's server if the user's mail is retrieved and writing a record of the domain name into the access database 2.

If there is a negative response from the domain name, then the remote access mail client 1 sends out a DNS enquiry to check for the MX record. The responses received from the DNS database 3 are listed in sequential order by the remote access mail client 1, the basic assumption being that one of these might be the user's POP3/IMAP4 server since most of the electronic mail servers now support POP3/IMAP4 protocols and a mail exchange server would also be the POP3/IMAP4 server. Each response is checked to see if port 110 and/or port 143, the ports associated with the POP3/IMAP4 protocols, is/are open or closed. The user's identify and log-in password is sent to any response having one of these ports open to retrieve the user's mail and a record of any successful response is written into the access database 2. This ends the first phase of operation.

If the first phase of the method fails to identify the user's server, the remote access mail client 1 initiates a second phase of the method, in a first stage of which IP addresses are first enumerated. This involves the remote access mail client 1 obtaining the IP address of the MX record and checking the open or closed status of the ports 110 and 143 of the host IP addresses 2 to 254 (for example, addresses 203.120.164.2 to 203.120.164.254). All those IP addresses with open ports 110 and/or 143 are subsequently checked for the user's mail with a record of any successful host being then written into the access database 2.

If the enumeration of IP addresses fails to identify the user's server, the remote access mail client initiates a second stage of the second phase of the method, in which the entire list of names CANME and/or HOST is requested for the presumed domain name by zone transfer from the DNS database. The host names on the list are checked for open ports 110 and 143 and the host names having open port status are written into the access database 2 and checked for the user's mail, a record of any successful host being written into the access database 2.

If the second phase of the method fails to identify the user's server, the remote access mail client 1 initiates a third and final phase, in which the system retrieves from the WHOIS server the IP address block, INETNUM, NETNUMBER OR NETBLOCK, which has been allocated to the domain organisation or company by the Networked Information Centre (NIC) and scans the ports 110 and 143 of the addresses in the block. Again, all IP addresses having open port status are used to check for the user's mail with a record of the successful host being written into the access database 2.

The entering of a record of the user's server in the access database 2 when and if the server is located, means that the system would not have to go through the same procedure again for a user with the same presumed domain name, since the user's server would be identified in the first stage of the first phase and access would be almost instantaneous.

Referring now to Figure 2, which illustrates the detailed operation of the system, the following steps are carried out:

S1 As invited by the homepage, the user enters his electronic mail address and password at the computer 6.

S2 Table 1 of the database 2 is checked to see if there is an existing user record. If there is such a record, the user is identified as an existing subscriber with the electronic mail server identified in his record and the method proceeds to step 3. If not, then the method proceeds to step S4.

S3 In this step, the subscribing user's electronic mail is checked and, if retrieved, passed to the user at the remote location, the error flag being set to O and the procedure then being complete. If the user's mail is not retrieved, e.g. because the record is incorrect, then the method proceeds to step S5. The user's record may be incorrect, for example, because the identity of the user's server has changed.

S4 This step presents a user, who is not already a subscriber to the system, with the terms and conditions of the system. If the user accepts, his electronic mail address is written to Table T1 in writing step W1 to establish a record for that user and the method proceeds to step S6. If the user does not accept the terms and conditions, the user is returned R1 to the homepage of the system at step S1.

S5 In this step, the error flag in the subscribing user's record in T1 is increased by 1. If the error flag then has a value of less than or equal to 6, the method proceeds to step S6. If the error flag value is greater than 6, the method goes to step S7.

S6 This step strips the user identity from the user's electronic mail address from either step S5 or W1 to obtain the presumed domain name which is then checked against the domain records in table T2 to see if there is a corresponding domain record. If there is a corresponding domain record, the method proceeds to step S8. If not, the method goes to step S10.

S7 In this step, the administrator is notified of the fact that there have been six

failed attempts to retrieve the user's electronic mail and the method proceeds to step S10.

S8 The user's electronic mail is checked using the server details contained in Table 2 for the user's presumed domain. If the mail is retrieved, the details of the corresponding server are written to Tables 1 and 2 and the procedure is completed. If not, then the method goes to step S9.

S9 Table 1 of the database is updated with the user's error flag being increased by 1 and the message PLEASE TRY AGAIN LATER is displayed. If the error flag has a value of greater than 6, the method notifies the administrator through step S7.

S10 This step initiates an interrogation of the Internet to determine the as yet unknown POP3/IMAP4 server to which the user belongs and first initiates step S11.

S11 This step assumes that the presumed domain name is the server and checks it for the user's mail. If the attempt is successful, a record of the server is written into both the user record and the domain database records and the procedure terminates in writing step W2 in Tables 1 and 2. If the attempt is unsuccessful the DNS MX record is checked. If this identifies the user's server, a record of the server is written into both the Tables 1 and 2 in writing step W3 and the procedure terminates. If neither the presumed domain name check nor the DNS MX record check identifies the user's server, but the servers checked nevertheless support POP3/IMAP4, details of the servers are written into the domain record in Table 2 in writing step W4. The method then goes to step S12.

S12 This step obtains the IP address of the MX record, passes the user's identity and password and triggers a first scanning step S13.

S13 In this step, the MX IP address scanning is carried out. If this identifies the user's server, a record of the server is written into both the user and domain records in Tables 1 and 2 in writing step W5 and the procedure terminates. If the scan is without success, records of the failed addresses, which nevertheless support POP3/IMAP4, are written in the Table 2 in writing step W6 and the method proceeds to step S14.

S14 This step requests DNS zone transfer of all the host names of the domain. If the request is successful, the method progresses to step S15. If unsuccessful, the method proceeds to step S16.

S15 If the requested zone transfer is executed, the host names thus obtained are scanned and checked for the user's mail. If one of the scanned hosts proves to be the user's server, a record to the server is written in both the user and domain records in Tables 1 and 2 in writing step W1. If not, a record of the unsuccessful hosts, which nevertheless support POP3/IMAP4, is written in the database Table 2 in writing step W8.

S16 Failure to identify the user's server in step S14 leads to initiation of this step which gets the IP address block for the domain from the WHOIS server, scans the addresses and selects those which support the POP3/IMAP4 protocols and then initiates step S17.

S17 This step checks the addresses selected in step S16 for the user's mail and a record of any successful host is written into both the user and domain records of the database Tables 1 and 2 in writing step W9. A record of unsuccessful hosts, which nevertheless support POP3/IMAP4, are written into the domain record in Table 2 of the database in writing step W10.

S18 The final step of the method terminates this search for user's server, even if step S17 has still failed to produce success, and sends an electronic mail to notify the administrator of the system.

In the above described method, the remote access mail client 1 performs the parsing of the input user address and password, the POP3/IMAP4 search engine performs the searching and the access database (SQL server) triggers the POP3/IMAP4 search and update.

It is envisaged that the described methodology of the present invention will find applications other than the remote access of electronic mail for a user. However, the described system and method embodying the invention has particular advantages for the remote retrieval of electronic mail, namely: a user need not carry all the technical information with him when travelling; there is no danger of such information falling into the wrong hands; most users can reliably remember their own electronic mail address and password, so that nothing needs to be written down; and users are not troubled by the need to supply the complex information that the known POP3/IMAP4 remote access mail clients normally require in order to provide material of a user's mail at a remote location.

The convenience and ease of using a system embodying the invention will thus enable travelling executives to keep in touch, even if they are not technically very knowledgeable or have lost or forgotten the cryptic list of server name and IP address that is required in order to set up a mail access at a remote location using one of the known remote access mail clients.

It is further clear that the establishment of the POP3/IMAP4 server database within a system embodying the invention will enable efficient use of the resources of the system and the Internet.

Finally, it is noted that the system embodying the invention may fail to identify the user's server entirely if: the user's e-mail server does not support POP3/IMAP4 mail but this would also preclude the use of known remote access mail clients, such as EUDORA and INTERNETMAIL; the mail address or password input by the user is incorrect; or the user does not have right of access.

CLAIMS



1. A method of identifying an electronic mail server to which a user at a remote location belongs but which the user is unable to specify, including the steps of: providing an access database containing records of servers supporting a specified electronic mail protocol or protocols; requiring from the user the electronic mail address and log-in password of the user; parsing the mail address to identify and remove the user identifier from the mail address and thereby obtain a presumed domain name of the user's server; interrogating the access database to determine whether it contains a record of a server corresponding to the presumed domain name; and retrieving the record of any corresponding server thus identified as the server to which the user belongs.

2. A method according to Claim 1, including the steps of: assuming that the domain name is the server in the event that the access database contains no corresponding server record; checking the domain name for the user's mail; and identifying the domain name as the user's server if the domain name responds positively.

3. A method according to Claim 2, including the following steps in the event that the access database contains no corresponding server record and the domain name responds negatively: sending out a Mail Exchange (MX) record enquiry to the Internet Domain Name System (DNS) database regarding the presumed domain name; listing the responses received from the DNS database; checking the responses in turn to determine whether a predetermined port or ports associated with the predetermined protocol or protocols is or are open or closed; and identifying a response having an open port or ports as the user's server.

4. A method according to Claim 3, including: obtaining the Internet Provider

This Sheet Has Been Replaced





(IP) address of the MX record; checking the open or closed status of the predetermined port or ports for a predetermined block of host IP addresses; storing all of the IP addresses having open port status in the access database; interrogating the stored IP addresses with the user's address and password; and identifying a successful IP address as the user's server.

5. A method according to claim 3, including the following steps in the event that the user's server is not identified from amongst the responses from the DNS database: requesting the full list of host names for the presumed domain name by DNS zone transfer; checking the open or closed status of the predetermined ports of the listed host names in turn; and identifying a host having open port status as the user's server.

6. A method according to Claim 5, including the following steps in the event that the DNS database does not allow zone transfer: retrieving the IP address block which has been allocated to the presumed domain by the Networked Information Centre (NIC); checking the open or closed status of the predetermined port or ports of the IP addresses in the block; storing all of the IP addresses having open port status in the access database; interrogating each of the stored IP addresses with the user's address and password; and identifying a successful IP address as the user's server.

7. A method according to any one of Claims 2 to 6, including the step of updating the access database with a record of a previously unrecorded server identified as the user's server or identified as supporting the predetermined protocol or protocols.

8. A method according to any preceding claim, including the step of retrieving the user's electronic mail from a server identified as the user's server and directing

This Sheet Has Been Replaced



the mail to the user at the remote location.

9. A method according to any preceding claim, in which the database is divided into first and second tables and including the steps of: entering records of users' mail addresses and the addresses of servers identified as corresponding servers in the first table; and entering records of domain names and the addresses of any servers identified as corresponding servers in the second table.

10. A method according to any preceding claim in which the predetermined protocol or protocols is or are the Post Office Protocol (POP3) and/or the Internet Message Access Protocol (IMAP4).

11. A system for identifying a server to which a user at a remote location belongs but which the user is unable to specify, including: an access database containing records of servers supporting a predetermined electronic mail protocol or protocols; and a remote access mail client associated with the database and having access to the Internet Domain Name System (DNS) database and to a search engine associated with the protocol or protocols; in which system the remote access mail client is arranged to require from the user the user's electronic mail address and password, to parse the mail address to identify and remove the user identity from the mail address and thereby obtain a presumed domain name of the user's server, to interrogate the access database to determine whether it contains a record of a server corresponding to the presumed domain name, and to retrieve the record of any corresponding server thus identified as the server to which the user belongs.

12. A system according to Claim 11, in which the remote access mail client is arranged to assume that the presumed domain name is the user's server in the event that the access database contains no corresponding server record, to check the domain name for the user's mail and to identify the domain name as the user's

server if the domain name responds positively.

13. A system according to claim 12, in which the remote access mail client is arranged to send out Mail Exchange (MX) record enquiry to the DNS database regarding the presumed domain name, to list the responses from the DNS database, to check the responses in turn to determine whether a predetermined port or ports associated with the protocol or protocols is or are open or closed, and to identify a response having an open port or ports as the user's server.

14. A system according to claim 13, in which the remote access mail client is arranged to obtain the IP address of the MX record, to check the open or closed status of the predetermined port or ports for a predetermined block of host IP addresses, store all of the IP addresses having open port status, to interrogate the stored addresses in turn with the user's address and password, and to identify a successful IP address as the user's server.

15. A system according to Claim 14, in which the remote access mail client is arranged to request the full list of host names for the presumed domain name by DNS zone transfer, to check the open or closed status of the predetermined ports of the listed host names and to identify a host having an open port status as the user's server.

16. A system according to Claim 15, in which the remote access mail client is arranged to retrieve the IP address block which has been allocated to the presumed domain name by the Networked Information Centre (NIC), to check the open or closed status of the predetermined port or ports, to store all of the IP addresses having open port status in the access database, to interrogate the IP addresses having open port status in turn and to identify a successful IP address as the user's server.

This Sheet Has Been Replaced



17. A system according to any one of Claims 11 to 16, in which the remote access mail client is arranged to write in the access database a record of any previously unrecorded server identified as the user's server identified as supporting the predetermined protocol or protocols.

18. A system according to any one of claims 11 to 17, in which the remote access mail client is arranged to retrieve the user's mail from any server identified as the user's server and to direct it to the user at the remote location.

19. A system according to any one of Claims 11 to 18, in which the database is divided into first and second tables, records of users' mail addresses and their corresponding servers being entered in the first table and records of domain names and their corresponding servers being entered in the second table.

20. A system according to any one of Claims 11 to 19, in which the predetermined protocol or protocols is or are the Post Office Protocol (POP3) and/or the Internet Message Access Protocol (IMAP4).

This Sheet Has Been Replaced

