A decentralized name services embodied in a system/method that communicates periodically name/identifier information of a host (100, 104) from a root name server (310) to a first (300) and second (302) local virtual name servers. The first server (300) receives a machine name from an originating host (100) and resolves the machine name into a machine identifier for the second server (302) and a destination host (104). In the event that the resolved machine identifier is for the second server (302), the second server (302) resolves the machine name for the destination host (104). Alternatively, the first server (300) may receive the machine name from the originating host (100) and they both are on a same subnet. The first server (300) resolves the machine name into the machine identifier for the second server (302) and the destination host (104). However, if the resolved machine identifier is intended for the second server (302), the second server (302) will resolve the machine name into the machine identifier for the destination host (104).
<table>
<thead>
<tr>
<th>Code</th>
<th>Country</th>
<th>Code</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>AL</td>
<td>Albania</td>
<td>ES</td>
<td>Spain</td>
</tr>
<tr>
<td>AM</td>
<td>Armenia</td>
<td>FT</td>
<td>Finland</td>
</tr>
<tr>
<td>AT</td>
<td>Austria</td>
<td>FR</td>
<td>France</td>
</tr>
<tr>
<td>AU</td>
<td>Australia</td>
<td>GA</td>
<td>Gabon</td>
</tr>
<tr>
<td>AZ</td>
<td>Azerbaijan</td>
<td>GB</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>BA</td>
<td>Bosnia and Herzegovina</td>
<td>GE</td>
<td>Georgia</td>
</tr>
<tr>
<td>BB</td>
<td>Barbados</td>
<td>GH</td>
<td>Ghana</td>
</tr>
<tr>
<td>BE</td>
<td>Belgium</td>
<td>GN</td>
<td>Guinea</td>
</tr>
<tr>
<td>BF</td>
<td>Burkina Faso</td>
<td>GR</td>
<td>Greece</td>
</tr>
<tr>
<td>BG</td>
<td>Bulgaria</td>
<td>HU</td>
<td>Hungary</td>
</tr>
<tr>
<td>BI</td>
<td>Benin</td>
<td>IE</td>
<td>Ireland</td>
</tr>
<tr>
<td>BR</td>
<td>Brazil</td>
<td>IL</td>
<td>Israel</td>
</tr>
<tr>
<td>BY</td>
<td>Belarus</td>
<td>IS</td>
<td>Iceland</td>
</tr>
<tr>
<td>CA</td>
<td>Canada</td>
<td>IT</td>
<td>Italy</td>
</tr>
<tr>
<td>CF</td>
<td>Central African Republic</td>
<td>JP</td>
<td>Japan</td>
</tr>
<tr>
<td>CG</td>
<td>Congo</td>
<td>KE</td>
<td>Kenya</td>
</tr>
<tr>
<td>CH</td>
<td>Switzerland</td>
<td>KG</td>
<td>Kyrgyzstan</td>
</tr>
<tr>
<td>CI</td>
<td>Côte d'Ivoire</td>
<td>KP</td>
<td>Democratic People's</td>
</tr>
<tr>
<td>CM</td>
<td>Cameroon</td>
<td>KR</td>
<td>Republic of Korea</td>
</tr>
<tr>
<td>CN</td>
<td>China</td>
<td>KZ</td>
<td>Kazakhstan</td>
</tr>
<tr>
<td>CZ</td>
<td>Czech Republic</td>
<td>LC</td>
<td>Saint Lucia</td>
</tr>
<tr>
<td>DE</td>
<td>Germany</td>
<td>LI</td>
<td>Liechtenstein</td>
</tr>
<tr>
<td>DK</td>
<td>Denmark</td>
<td>LK</td>
<td>Sri Lanka</td>
</tr>
<tr>
<td>EE</td>
<td>Estonia</td>
<td>LR</td>
<td>Liberia</td>
</tr>
<tr>
<td>LS</td>
<td>Lesotho</td>
<td>LT</td>
<td>Lithuania</td>
</tr>
<tr>
<td>LU</td>
<td>Luxembourg</td>
<td>LV</td>
<td>Latvia</td>
</tr>
<tr>
<td>MC</td>
<td>Monaco</td>
<td>MD</td>
<td>Republic of Moldova</td>
</tr>
<tr>
<td>MG</td>
<td>Madagascar</td>
<td>MK</td>
<td>The former Yugoslavia</td>
</tr>
<tr>
<td>ML</td>
<td>Mali</td>
<td>MN</td>
<td>Mongolia</td>
</tr>
<tr>
<td>MR</td>
<td>Mauritania</td>
<td>MW</td>
<td>Malawi</td>
</tr>
<tr>
<td>NE</td>
<td>Niger</td>
<td>NL</td>
<td>Netherlands</td>
</tr>
<tr>
<td>NO</td>
<td>Norway</td>
<td>NZ</td>
<td>New Zealand</td>
</tr>
<tr>
<td>PL</td>
<td>Poland</td>
<td>PT</td>
<td>Portugal</td>
</tr>
<tr>
<td>RO</td>
<td>Romania</td>
<td>RU</td>
<td>Russian Federation</td>
</tr>
<tr>
<td>SD</td>
<td>Sudan</td>
<td>SE</td>
<td>Sweden</td>
</tr>
<tr>
<td>SG</td>
<td>Singapore</td>
<td>SI</td>
<td>Slovenia</td>
</tr>
<tr>
<td>SK</td>
<td>Slovakia</td>
<td>SN</td>
<td>Senegal</td>
</tr>
<tr>
<td>SZ</td>
<td>Swaziland</td>
<td>TD</td>
<td>Chad</td>
</tr>
<tr>
<td>TG</td>
<td>Togo</td>
<td>TJ</td>
<td>Tajikistan</td>
</tr>
<tr>
<td>TM</td>
<td>Turkmenistan</td>
<td>TR</td>
<td>Turkey</td>
</tr>
<tr>
<td>TT</td>
<td>Trinidad and Tobago</td>
<td>UA</td>
<td>Ukraine</td>
</tr>
<tr>
<td>TG</td>
<td>Uganda</td>
<td>US</td>
<td>United States of America</td>
</tr>
<tr>
<td>UZ</td>
<td>Uzbekistan</td>
<td>VN</td>
<td>Viet Nam</td>
</tr>
<tr>
<td>YU</td>
<td>Yugoslavia</td>
<td>ZW</td>
<td>Zimbabwe</td>
</tr>
</tbody>
</table>
DECENTRALIZED NAME SERVICES

BACKGROUND OF THE INVENTION

The present invention relates network services, and more particularly to name services. Even more particularly, the present invention relates to a system and method for reducing bandwidth usage in the provision of name services in a highly distributed network environment, such as the Internet.

The Internet presents significant challenges and opportunities to providers of traditional network services including name services, such as domain name services, or other such services used to resolve machine names. The number of Internet users is growing rapidly, stimulating network traffic and in turn demand for new services.

One result of this Internet "boom" has been a shortage of available bandwidth, particularly at routers (gateways) at critical junctions throughout the Internet. These shortages of bandwidth cause "bottlenecks" that slow the movement of data across the routers. Such "bottlenecks" are due to the fact that, frequently, more traffic (in terms of bandwidth) needs to pass through a particular router than the particular router has capacity (in terms of bandwidth). These bandwidth "bottlenecks" frequently result in slow throughput during peak usage periods, leading to less than desirable performance.

Recently, studies have been conducted confirming that approximately 17% of all Internet traffic is due to what is referred to as domain name lookups. A service referred to as Domain Name Services (or DNS) is the culprit.

Each host on the Internet is assigned an Internet protocol, or IP, address. These IP addresses take the form of four numbers, each between 0 and 255, separated by periods, and are used to uniquely identify each host on the Internet. An example of an IP address
is 204.216.142.198. IP addresses are inherently "unfriendly" in that they are "machine-like" and "numerical" in nature and are thus difficult for users to remember.

As a result, a system of domain names has been developed in which textual names are associated with a host's IP address in order to identify the host by a textual name. An example of a domain name is emke.com.

Because, however, the use of domain names is not integral to the underlying protocol used on the Internet (Internet Protocol or IP), these domain names must be "looked up" each time they are used, so that the underlying IP address can be determined.

Referring to FIGS. 1 and 2, when an originating host 100 connected to the Internet 102 uses a domain name to attempt access of a destination host 104 on the Internet 102, the originating host 100 first queries its local domain name server 106 or DNS (maintained by its Internet service provider or, ISP, which may be a commercial online service provider, a company network service provider, or other DNS provider) by sending the domain name of the destination host 104 with which the originating host 100 seeks to communicate to the local domain name server 106, in hopes that the local domain name server 106 has cached information regarding the IP address corresponding to the domain name of the destination host 104.

In the event this local domain server 106 does not have information regarding the IP address of the destination host 104, the local domain name server 106 queries a root domain name server 108 for this IP address. Currently, there are thirteen root domain servers worldwide, almost all of which are located in the United States.

The root domain name server 108 may redirect the local domain name server's request to a generic top level domain, or gTLD, server 110 associated with a
particular generic top level domain for which an IP address is sought. For example, if a ".com" domain is sought, the root domain server 108 may redirect the local domain name server’s request to a gTLD server 110 for the " .com" domain. The gTLD server 110 is generally located proximate to the root domain server 108, both of which are generally located remotely from the originating host 100. Each root domain name server 108 has its own set of gTLD servers 110.

The root domain name server 108, or gTLD server 110, may provide the local domain name server 106 with the IP address of the destination host 104, however, it may also redirect the local domain name server 106 to another local domain name server 112 that provides domain name services for the destination host 104 domain name.

The other local domain name server 112 provides the originating host’s local domain name server 106 with the IP address of the destination host 104, and the local domain name server 106 provides the IP address of the destination host 104 to the originating host 100. The originating host 100 then can communicate directly with the destination host 104 using the destination host’s 104 address. Thus, two long distance communications, i.e., that between the local domain name server 106 and the root domain name server 108, and that between the local domain name server 106 and the generic gTLD server 110 take place before direct communication between the originating host’s local domain server 106 and the destination host’s local domain name server can occur

These communications may, depending on the location of the originating host 100 and its local domain name server 106, require a pair or intercontinental communications 114, 116 (between the originating host’s local domain name server 106 and the root domain name server 108, and between the originating host’s local domain name server 106 and the gTLD server 110), which at
this time for foreign (i.e., non-U.S.) users can present significant a communications "bottleneck", not to mention the significant additional traffic this creates on the Internet 102.

The present invention advantageously addresses the above and other needs.

SUMMARY OF THE INVENTION

The present invention advantageously addresses the needs above as well as other needs by providing a decentralized name services approach suited particularly for provision of name services in a highly distributed environment.

One embodiment of the present invention can be characterized as a method of resolving a machine name into a machine identifier. The method has steps of communicating periodically machine name/machine identifier information from a root name server to a first local virtual name server; receiving, in the first local virtual name server, a machine name from an originating host; resolving, within the first local virtual name server, the machine name into a machine identifier for one of a second local virtual name server and a destination host; and resolving, within the second local virtual name server, in the event the machine identifier into which the machine name is resolved by the first local virtual name server is a machine identifier for the second local virtual name server, the machine name into a machine identifier for the destination host.

Another embodiment of the present invention can be characterized as a method of resolving a machine name into a machine identifier, having steps of receiving, in a first local virtual name server, a machine name from an originating host, the originating host and the first local virtual name server being in a first subnet; resolving, within the first local virtual name server, the machine name into a machine identifier for one of a
second local virtual name server and a destination host; and resolving, within the second local virtual name server, in the event the machine identifier into which the machine name is resolved by the first local virtual name server, the machine name into a machine identifier for the destination host.

Yet another embodiment of the present invention can be characterized as a system for resolving a machine name into a machine identifier. The system employs an originating host initiating communication with a destination host by transmitting a machine name of the destination host to a first virtual name server; the first virtual name server receiving the machine name and resulting the machine name into a machine identifier or one of a second virtual name server or the destination host; and initiating communication with the second virtual name server in the event the machine identifier into which the machine name is resolved is a machine identifier for the second virtual name server, transmitting the machine name of the destination host to the second virtual name server; and the second virtual name server receiving the machine name from the first virtual name server and resolving the machine name into the machine identifier of the destination host, and transmitting the machine identifier of the destination host to the fast virtual name server, the first virtual name server transmitting the machine identifier of the destination host, whether resolved in the first virtual name server or the second virtual name server, to the originating host.

BRIEF DESCRIPTION OF THE DRAWINGS

The above and other aspects, features and advantages of the present invention will be more apparent from the following more particular description thereof, presented in conjunction with the following drawings wherein:
FIG. 1 is a block diagram illustrating an originating host, the originating host's local domain name server, a root domain name server, a gTLD server, a destination host's local domain name server, and the destination host, with arrows illustrating traffic generated between these hosts as a result of a domain name lookup (worst case, i.e., non-cached, etc.) in accordance with the prior art;

FIG. 2 is a signal diagram illustrating data signals traveling between the originating host, the originating host's local domain name server, the root domain name server, the gTLD server, the destination host's local domain name server, and the destination host of FIG. 1 in accordance with the prior art;

FIG. 3 illustrates an originating host, the originating host's local virtual gTLD server, a destination host's local virtual gTLD server, and the destination host, with arrows illustrating traffic generated between these hosts as a result of a domain name lookup in accordance with one embodiment of the present invention; and

FIG. 4 is a signal diagram illustrating data signals traveling between the originating host, the originating host's local virtual gTLD server, the destination host's local virtual gTLD server, and the destination host of FIG. 3 in accordance with one embodiment of the present invention.

Corresponding reference characters indicate corresponding components throughout the several views of the drawings.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The following description of the presently contemplated best mode of practicing the invention is not to be taken in a limiting sense, but is made merely for the purpose of describing the general principles of the
invention. The scope of the invention should be
determined with reference to the claims.

Referring to FIGS. 1 and 2, a block diagram and
a signal diagram are shown of a current (prior art)
approach to domain name lookup in an Internet
environment. Shown is an originating host 100, the
originating host's domain name server 106, a root domain
name server 108, a generic top level domain (gTLD) server
110, a destination host's local domain name server 112
and the destination host 104.

As explained above, the architecture
illustrated dictates that up to five communications 114,
116, 118, 120, 122 occur in order for the originating
host 100 to contact the destination host 104, two of
which (114 and 116) are potentially intercontinental
communications even when both the originating host 100
and the destination host 104 are in the same foreign,
i.e., non-U.S., country. Furthermore, even in a purely
U.S. communication a great deal of network traffic occurs
outside the originating host's subnet in order to resolve
(i.e., look up) a domain name. As explained above, this
arrangement is highly undesirable in that a great deal of
communication occurs unnecessarily, thus wasting the
precious little bandwidth available in many areas of the
Internet, such as at routers providing intercontinental
connections.

Referring to FIGS. 3 and 4, a block diagram and
a signal diagram are shown illustrating an approach in
accordance with one embodiment of the present invention.

This alternative approach eliminates both the root domain
name server (at least in the sense employed by the prior
art approach of FIGS. 1 and 2) and the gTLD server from
the structure and method required by the prior art for
resolution of a domain name into an IP address in a
network transaction (i.e., from a single communication
between the originating host 100 and the destination host
104), leaving only the originating host 100, a local
virtual gTLD server 300, a remote virtual gTLD server 302, and the destination host 104.

By way of example, comparing the approach presented in FIGS. 3 and 4 with the currently known approach of FIGS. 1 and 2, as currently used on the Internet, if a user were in Australia and wished to access a destination host in Australia, in accordance with the prior art approach of FIGS. 1 and 2, he/she would potentially have to initiate two intercontinental communications 114, 116 (one 114 to the root domain name server 108 and another 116 to the gTLD server 110) in order to locate the destination host 104 within his/her own country. This is clearly quite inefficient and borders on abusive in view of the bandwidth "bottlenecks" that presently exist on portions of the Internet, such as at some routers.

Applying the approach of FIGS. 3 and 4, all domain name information is maintained locally by the originating host’s local virtual gTLD server 300 (typically the local virtual gTLD server 300 would be maintained by an Internet service provider, or by a company having its own subnet), and therefore no need to access a root domain server or other gTLD server 300 exists. If the Australian originating host wishes to access an Australian destination host, the originating host accesses its local virtual gTLD server 300 at which information regarding the IP address (or, in other embodiments, another such machine identifier) of the destination host 104 is stored. This IP address information may be in the form of an IP address (or other machine identifier) for the remote virtual gTLD server 302 at the destination host 104, in which case a query is sent by the originating host’s local virtual gTLD server 300 to the destination hosts’s local virtual gTLD server 302, the response to which is the IP address (or other machine identifier) for the destination host 104; or this IP address information may be in the form of an IP
address (or other machine identifier) for the destination host 104.

Next, the originating host 100 communicates directly with the destination host 104 using its IP address as provided by the respective virtual gTLD server 300 or 302. Thus, three communications 304, 306, 308 are required in order for the originating host 100 to communicate with the destination host 104, instead of five, as with the prior art approach of FIGS. 1 and 2.

In addition, in the case of the present example, i.e., a foreign originating host and a foreign destination host 104, none of the three communications are intercontinental.

A database of domain names and corresponding ID addresses is maintained on the local and remote gTLD servers 300, 302, and the local and remote virtual gTLD servers 300, 302 are maintained by a root domain name server 310, much like the root domain name server 108 in FIG. 1, on a periodic basis, such as daily, however, rather than on a per-transaction basis. An entire database of domain names and corresponding IP addresses need not be downloaded to each virtual gTLD server on the Internet periodically. Instead, a delta file containing only the additions, changes and deletions to the root domain name server’s databases since the last update of the virtual gTLD server, need be sent on the periodic basis. This delta file requires minimum bandwidth, and only a single interchange between the root domain name server 310 and the virtual gTLD servers 300, 302 need take place. This delta file can be compressed using any number of widely known compression approaches in order to further improve bandwidth efficiency.

This interchange between the virtual gTLD servers 300, 302 and the root domain name server 310 can be initiated by the virtual gTLD servers 300, 302, via a request or, alternatively, can be initiated by the root domain name server 310 by a "pusher". A hybrid
environment, in which regular updates are requested periodically by the virtual gTLD servers 300, 302, such as daily, with "emergency" updates being delivered by the "pusher" at the root domain name server 310 in the event a corrupt or otherwise flawed delta file is distributed by the root domain name server 310, is considered a preferred operating mode.

This "pusher" can also be used in the event the root domain name server 310 has need to expire or otherwise change a domain name's status, and assure that all virtual gTLD servers throughout the Internet are updated. The "pusher" is simply an additional process executing in the root domain name server 310.

One additional benefit of the present approach is that domain name server updates are highly managed and centrally administered, yet the need for constant access to and communication with the root domain name server 310, on a per transaction basis, is not required.

Changes to domain names may be initiated by the virtual gTLD server 300 or 302 that "hosts" the changed domain name. When a change is made to a domain name managed by a particular virtual gTLD server 300 or 302, the virtual gTLD server 300 or 302 creates its own delta file to be transmitted to the root domain name server 310 during its next transaction with the root domain name server 310, or immediately. This delta file assures that the root domain name server 310 is updated quickly after changes are made at the virtual gTLD server 300 or 302 to the hosted domain name, and that these changes will soon be propagated throughout the Internet within one update cycle to each other virtual gTLD server 300 or 302 on the Internet.

One side benefit that the present embodiment offers is that all domain name server lookup activity for any given originating host, and for that matter, for any given group of originating hosts, or any given subnet, is conducted through a single virtual gTLD server. This
means that this virtual gTLD server is aware of all domain name lookup activity by the originating host or originating hosts that use the virtual gTLD server, and therefore can maintain logs of domain name server activity by such originating host. As a result, companies or government entities maintaining their own virtual gTLD servers can monitor activities by employees and others on their subnet simply by viewing (or otherwise auditing) their virtual gTLD server logs. This advantage of the present embodiment may prove highly desirable to some companies or government entities that wish to maintain a watch over their employees' Internet activities.

Furthermore, each virtual gTLD server can be programmed to deny domain name services to particular destination domains (i.e., hosts) as determined by their administrators. Thus, companies or government entities wishing to block domain name server servicing for certain domain names need simply configure their virtual gTLD server to deny domain name lookup services to originating hosts within their network. This can be done on a per-originating-host basis, on the basis of a group of originating hosts, or on the basis of an entire subnet. Likewise, domain name services can be denied altogether for certain originating hosts in the event, for example, the originating host is to be denied access to servers outside a particular subnet or group of hosts.

While the invention herein disclosed has been described by means of specific embodiments and applications thereof, numerous modifications and variations could be made thereto by those skilled in the art without departing from the scope of the invention set forth in the claims. For example, the present invention has application outside the Internet, such as for example, on internets or other TCP/IP networks, or subnetworks.
By way of further example, the inventors envision that the present invention does not dictate that the entire Internet adopt teachings of the embodiment described above. Individual Internet service providers (ISP's) or company subnets could adopt an approach in accordance with the embodiment described above, while others continue to operate in accordance with the teachings of the prior art, as also described above.

By way of yet a further example, the inventors contemplate that the present invention can easily be applied to other network topologies employing machine name lookup and machine identifiers analogous to IP addresses.
CLAIMS

What is claimed is:

1. A method of resolving a machine name into a machine identifier comprising:
   communicating periodically machine name/machine identifier information from a root name server to a first local virtual name server;
   receiving, in the first local virtual name server, a machine name from an originating host resolving, within the first local virtual name server, the machine name into a machine identifier for one of a second local virtual name server and a destination host; and
   resolving, within the second local virtual name server, in the event the machine identifier into which the machine name is resolved by the first local virtual name server is a machine identifier for the second local virtual name server, the machine name into a machine identifier for the destination host.

2. The method of Claim 1 further comprising: transmitting information from the originating host to the destination host using the machine identifier for the destination host.

3. The method of Claim 1 wherein said communicating periodically said machine name/machine identifier information comprises communicating an entire database of machine name/machine identifier information from the root name server to the first local virtual name server.

4. The method of Claim 1 wherein said communicating periodically said machine name/machine identifier information comprises:
communicating, at the expiration of a first period, a delta database of changed machine name/machine identifier information from the root name server to the first local virtual name server; and

communicating, at the expiration of a second period, an entire database of machine name/machine identifier information from the root name server to the first local virtual name server at the expiration of a second period.

5. The method of Claim 1 wherein said communicating periodically said machine name/machine identifier information comprises communicating a portion of an entire database of machine name/machine identifier information from the root name server to the first local virtual name server.

6. The method of Claim 1 wherein said communicating periodically said machine name/machine identifier information comprises:

transmitting periodically an update request from the first local virtual name server to the root name server; and

communicating, in response thereto, said machine name/machine identifier information from the root name server to the first local virtual name server.

7. The method of Claim 6 wherein transmitting periodically an update request comprises transmitting an entire database request, and said communicating, in response thereto, said machine name/machine identifier information comprises communicating an entire database of machine name/machine identifier information from the root name server to the first local virtual name server.

35
8. The method of Claim 7 wherein transmitting periodically an update request comprises transmitting a delta database request, and said communicating in response thereto said machine name/machine identifier information comprises communicating a delta database of changed machine name/machine identifier information from the root name server to the first local virtual name server.

9. A method of resolving a machine name into a machine identifier comprising:
   receiving, in a first local virtual name server, a machine name from an originating host, the originating host and the first local virtual name server being in a first subnet;
   resolving, within the first local virtual name server, the machine name into a machine identifier for one of a second local virtual name server and a destination host; and
   resolving, within the second local virtual name server, in the event the machine identifier into which the machine name is resolved by the first local virtual name server, the machine name into a machine identifier for the destination host.

10. The method of Claim 9 further comprising: transmitting information from the originating host to the destination host, the destination host being in a different subnet than the subnet in which the originating host and first virtual name server are.

11. A system for resolving a machine name into a machine identifier comprising:
   an originating host initiating communication with a destination host by transmitting a machine name of the destination host to a first virtual name server;
the first virtual name server receiving the machine name and resulting the machine name into a machine identifier or one of a second virtual name server or the destination host; and initiating communication with the second virtual name server in the event the machine identifier into which the machine name is resolved is a machine identifier for the second virtual name server, transmitting the machine name of the destination host to the second virtual name server; and

the second virtual name server receiving the machine name from the first virtual name server and resolving the machine name into the machine identifier of the destination host, and transmitting the machine identifier of the destination host to the first virtual name server, the first virtual name server transmitting the machine identifier of the destination host, whether resolved in the first virtual name server or the second virtual name server, to the originating host.

12. The system of Claim 11 further comprising: the destination host.

13. The system of Claim 12 further comprising: a root name server periodically transmitting at least a portion of a name database to the first virtual name server.

14. The system of Claim 13 wherein said first virtual name server includes means for transmitting a request to the root name server, the request comprising an update request; said root server further comprising means for responding to the request by transmitting said at least a portion of the name database.
15. The system of Claim 12 further comprising: said first virtual name server including means for transmitting a request to a root name server; the root name server transmitting at least a portion of a name database to the first virtual name server in response to the request.

16. The system of Claim 12 further comprising: a root name server transmitting at least a portion of a name database to the first name server in response to chances in the name database since a previous transmission to the root name server.
INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) : H04L 12/00, 12/26; G06F 1/00

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)


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)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category*</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X, P</td>
<td>US 5,898,830 A (WESINGER, JR. ET AL.) 27 APRIL 1999 (27/04/1999), see FIGs. 1-3, col. 8, line 55 to col. 10, line 65</td>
<td>1-16</td>
</tr>
<tr>
<td>X, P</td>
<td>US 5,777,989 A (MCGARVEY) 07 JULY 1998 (07/07/1998), see FIGs. 1-3, col. 3, line 60 to col. 5, line 37.</td>
<td>1-16</td>
</tr>
</tbody>
</table>

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

* Special categories of cited documents:
  "A" document defining the general state of the art which is not considered to be of particular relevance
  "B" earlier document published on or after the international filing date
  "L" document which may throw doubt 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

"I" 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
"A" document member of the same patent family

Date of the actual completion of the international search
06 AUGUST 1999

Date of mailing of the international search report
01 NOV 1999

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
DUONG, FRANK
Telephone No. (703) 308-5428

Form PCT/ISA/210 (second sheet) (July 1992)