MULTISERVER FOR PROVIDING INTEGRATED COMPUTER SERVICES

A multiserver for providing file sharing service, print services, fax services and Internet hosting services is disclosed. The various services are implemented using publicly available software packages, the configuration of which has been integrated by means of a unified configuration management interface. The configuration management interface automatically configures the underlying packages in response to information entered by an administrator. The underlying software packages may be changed without changing the appearance of the configuration management interface, allowing the system to be upgraded without requiring the administrator to learn how to configure the new packages.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>AL</td>
<td>Albania</td>
<td>ES</td>
<td>Spain</td>
<td>LS</td>
<td>Lesotho</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AM</td>
<td>Armenia</td>
<td>FI</td>
<td>Finland</td>
<td>LT</td>
<td>Lithuania</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AT</td>
<td>Austria</td>
<td>FR</td>
<td>France</td>
<td>LU</td>
<td>Luxembourg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AU</td>
<td>Australia</td>
<td>GA</td>
<td>Gabon</td>
<td>LV</td>
<td>Latvia</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AZ</td>
<td>Azerbaijan</td>
<td>GB</td>
<td>United Kingdom</td>
<td>MC</td>
<td>Monaco</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BA</td>
<td>Bosnia and Herzegovina</td>
<td>GE</td>
<td>Georgia</td>
<td>MD</td>
<td>Republic of Moldova</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BB</td>
<td>Barbados</td>
<td>GH</td>
<td>Ghana</td>
<td>MG</td>
<td>Madagascar</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BE</td>
<td>Belgium</td>
<td>GN</td>
<td>Guinea</td>
<td>MK</td>
<td>The former Yugoslav Republic of Macedonia</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BF</td>
<td>Burkina Faso</td>
<td>GR</td>
<td>Greece</td>
<td>ML</td>
<td>Mali</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BG</td>
<td>Bulgaria</td>
<td>HU</td>
<td>Hungary</td>
<td>MN</td>
<td>Mongolia</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BJ</td>
<td>Benin</td>
<td>IE</td>
<td>Ireland</td>
<td>MR</td>
<td>Mauritania</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BR</td>
<td>Brazil</td>
<td>IL</td>
<td>Israel</td>
<td>MW</td>
<td>Malawi</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BY</td>
<td>Belarus</td>
<td>IS</td>
<td>Iceland</td>
<td>MX</td>
<td>Mexico</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CA</td>
<td>Canada</td>
<td>IT</td>
<td>Italy</td>
<td>NE</td>
<td>Niger</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CF</td>
<td>Central African Republic</td>
<td>JP</td>
<td>Japan</td>
<td>NL</td>
<td>Netherlands</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CG</td>
<td>Congo</td>
<td>KE</td>
<td>Kenya</td>
<td>NO</td>
<td>Norway</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CH</td>
<td>Switzerland</td>
<td>KG</td>
<td>Kyrgyzstan</td>
<td>NZ</td>
<td>New Zealand</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CI</td>
<td>Côte d'Ivoire</td>
<td>KP</td>
<td>Democratic People's Republic of Korea</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CM</td>
<td>Cameroon</td>
<td>KR</td>
<td>Republic of Korea</td>
<td>PL</td>
<td>Poland</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CN</td>
<td>China</td>
<td>KZ</td>
<td>Kazakhstan</td>
<td>PT</td>
<td>Portugal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CU</td>
<td>Cuba</td>
<td>LC</td>
<td>Saint Lucia</td>
<td>RO</td>
<td>Romania</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CZ</td>
<td>Czech Republic</td>
<td>LJ</td>
<td>Liechtenstein</td>
<td>RU</td>
<td>Russian Federation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DE</td>
<td>Germany</td>
<td>LK</td>
<td>Sri Lanka</td>
<td>SD</td>
<td>Sudan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DK</td>
<td>Denmark</td>
<td>LR</td>
<td>Liberia</td>
<td>SE</td>
<td>Sweden</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EE</td>
<td>Estonia</td>
<td></td>
<td></td>
<td>SG</td>
<td>Singapore</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SI</td>
<td>Slovenia</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SK</td>
<td>Slovakia</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SN</td>
<td>Senegal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SZ</td>
<td>Swaziland</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TD</td>
<td>Chad</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TG</td>
<td>Togo</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TJ</td>
<td>Tajikistan</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TM</td>
<td>Turkmenistan</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TR</td>
<td>Turkey</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TT</td>
<td>Trinidad and Tobago</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UA</td>
<td>Ukraine</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UG</td>
<td>Uganda</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>US</td>
<td>United States of America</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UZ</td>
<td>Uzbekistan</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VN</td>
<td>Viet Nam</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>YU</td>
<td>Yugoslavia</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ZW</td>
<td>Zimbabwe</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Title: Multiserver for Providing Integrated Computer Services

FIELD OF THE INVENTION

This invention relates to computer servers and more particularly to servers capable of providing a number of computer services.

BACKGROUND OF THE INVENTION

Modern business practices require substantial use of computers for both internal activities, such as document development (using both local and remote computer terminals), and external activity, such as advertising using an internet website and sending and receiving communications via electronic mail or fax. The increasing need to interconnect computers, both within a local office environment and externally to suppliers, clients and the general public has created a need for a simplified computer system which can be configured to provide these services more conveniently and cost effectively. Increasingly, these needs are being felt by companies and individual users.

The variety of computer services required by business enterprises have traditionally been provided by selecting appropriate computer hardware, operating system software (computer hardware and the associated operating system software are often referred to collectively as a “platform”) and a group of software application packages (which provide the desired computer services) designed to operate on the computer platform. Each software application is then independently configured for the needs of the business. Among the disadvantages of this method is the need for technically skilled personnel to select, configure and maintain the platform and applications software.

The provision of the necessary computer services is further complicated when a business has already selected several incompatible platforms. This situation often arises when a company merges with another, when a decision is made to change from one platform to another or when the differing needs of a business require the use of incompatible platforms for different purposes.

Accordingly, there is a need for a system which provides computer services required by a typical business enterprise in a single package. Such a system will provide file management services, printing management services and e-mail services. Each of these services is preferably linked together by a cohesive interface which allows an administrator to configure each of the services simultaneously. It is preferable if the system further provides fax management services, internet hosting services and provides security services, including a firewall mechanism to control unauthorized access to the system. Such a system will be an assembly of a group of “servers”, each of which will be dedicated to the provision of one or more of these services. In the specification and claims such a system will be referred to as a “multiserver”.
More generally, there is a need for a multiserver that provides a number of computer services, all of which can be simultaneously configured to operate compatibly with one another using a cohesive configuration interface.

**SUMMARY OF THE INVENTION**

The present invention provides a multiserver which meets this need. One embodiment of a multiserver according to the present invention includes a group of servers which provide various computer services required by a typical business enterprise. Each of the servers consists of a pre-existing software package which is publicly available. The servers are configured using a configuration management interface. The configuration management interface presents a series of configuration screens which allow an administrator to enter all data required to configure each server in a single environment. As this data is entered, each of the servers is updated to reflect it. The configuration management interface reduces the need for the administrator to individually configure each server and reduces the likelihood that inconsistent configuration of the different servers will lead to incompatibilities between them.

The use of a configuration management interface to configure the servers allows the servers themselves to be changed as new server products become available. All that is required in this case is to modify the configuration management interface to configure the new server, generally without modifying the appearance of the configuration management interface. Even if new servers are added to the multiserver to provide new computer services, the configuration management interface may retain its appearance. If all information required to configure the new servers may already be collected using the existing configuration management interface, then no change to the configuration management interface is required. If some additional information is required, the configuration management interface may be modified to collect this additional information and to configure the new server using it. However, the administrator need only provide this additional information. The administrator will not be required to learn how to configure the new server.

As the multiserver is improved by modifying the specific servers used to provide various functions, the administrator may be not be aware of any change to the multiserver, except for having the advantage of the new features offered by the new server. This allows the multiserver to be improved and modified in a manner transparent to the administrator and other users of the system and reduces the need for highly qualified technical personnel to configure and operate the multiserver.

Although the multiserver described below is intended for use in a business environment, other embodiments of multiservers according to the present invention may be intended for use in other environments. For example, a multiserver designed for use in a research development environment may include a number of servers which provide data gathering and analysis services. As another example, a multiserver designed for
residential use may include servers which provide word processing, spreadsheet internet, security and home automation and networking services.

Furthermore, a multiserver may be implemented using a variety of computer platforms. The multiserver described below implements the well known Linux operating system and utilizes a number of well known, publicly available software packages to implement the various servers required to provide the desired computer services. One skilled in the art will recognize that a multiserver may include a different operating system or different software packages.

In a first embodiment of the present invention, there is provided a configuration management interface for configuring a plurality of computer services, said computer services installed on a computer system, said configuration management interface comprising: configuration definition means for allowing characteristics of each of said computer services to be defined by an administrator; and configuration implementation means for configuring the plurality of said computer services to correspond to said characteristics.

According to a second embodiment of the present invention, there is provided a configuration management interface for configuring a plurality of computer services, said configuration management interface being embodied in a computer readable medium, and said configuration management interface comprising: configuration definition means for allowing characteristics of each of said computer services to be defined by an administrator; and configuration implementation means for configuring the plurality of said computer services to correspond to said characteristics.

According to a third embodiment of the present invention, there is provided a multiserver for providing a plurality of computer services to a plurality of users, said multiserver being capable of installation and execution on a computer system, said multiserver comprising: a file server for providing file storage and retrieval services to at least some of said users; a print server for providing print services to at least some of said users; a mail server for providing e-mail services to at least some of said users; and a configuration management interface, said configuration management interface including configuration definition means for allowing an administrator to define: characteristics of said users; characteristics of said file storage and retrieval services, print services and e-mail services; and characteristics of the use of said file storage and retrieval services, print services and e-mail services by each of said users, and said configuration management interface including configuration implementation means for configuring said file server, said print server and said mail server to correspond to the characteristics defined by said administrator.

Another aspect of the present invention provides a method of sending a fax transmission comprising the steps of: providing a fax server capable of making a fax transmission; providing a fax control file including fields for identifying one or more fax source files to be faxed and identifying a destination telephone number to which the fax is to be sent; providing one or more documents corresponding to said fax source files;
ensuring that said fax control file has not been modified for a first selected period of time; ensuring that each of said documents has not been modified for a second selected period of time; assembling a fax document consisting of said documents; and instructing said fax server to send said fax document to said destination telephone number.

Another aspect of the present invention provides a method of relaying a piece of electronic mail transmitted from a transmitting computer to a receiving computer through a host computer, said method comprising the steps of: recording a user name and password for a user; establishing a list of computers for which said host computer will relay electronic mail; waiting for said user to establish a communication link between said transmitting computer and said host computer and to enter said user name and said password; adding said transmitting computer to said list of computers; receiving said electronic mail from said transmitting computer; and relaying said electronic mail to said receiving computer.

BRIEF DESCRIPTION OF THE DRAWINGS

An exemplary preferred embodiment of the present invention will now be described with reference to the drawings, in which:

Figure 1 is a block drawing showing interconnections between elements of an exemplary preferred embodiment of a multiserver according to the present invention;

Figure 2 is a block diagram showing a security model of the multiserver of Figure 1;

Figure 3 shows a status screen 100 of the configuration management interface 20 of the multiserver of Figure 1;

Figure 4 shows an administration locks subscreen of the configuration management interface 20 of the multiserver of Figure 1;

Figure 5 shows an administration miscellaneous subscreen of the configuration management interface 20 of the multiserver of Figure 1;

Figure 6 shows an administration backup subscreen of the configuration management interface 20 of the multiserver of Figure 1;

Figure 7 shows an administration remote subscreen of the configuration management interface 20 of the multiserver of Figure 1;

Figure 8 shows an administration DNS subscreen of the configuration management interface 20 of the multiserver of Figure 1;

Figure 9 shows a networks screen of the configuration management interface 20 of the multiserver of Figure 1;

Figure 10 shows a users and groups screen of the configuration management interface 20 of the multiserver of Figure 1;

Figure 11 shows a file server screen of the configuration management interface 20 of the multiserver of Figure 1;

Figure 12 shows a print server screen of the configuration management interface 20 of the multiserver of Figure 1;
Figure 13 shows a fax server screen of the configuration management interface 20 of the multiserver of Figure 1;

Figure 14 shows a fax routing screen of the configuration management interface 20 of the multiserver of Figure 1;

Figure 15 shows a domain server screen of the configuration management interface 20 of the multiserver of Figure 1;

Figure 16 shows a FTP server screen of the configuration management interface 20 of the multiserver of Figure 1;

Figure 17 shows a web server screen of the configuration management interface 20 of the multiserver of Figure 1; and

Figure 18 shows a mail server screen of the configuration management interface 20 of the multiserver of Figure 1; and

Figure 19 shows a firewall screen of the configuration management interface 20 of the multiserver of Figure 1.

**DETAILED DESCRIPTION OF THE INVENTION**

The structure and operation of an exemplary preferred embodiment of a multiserver will now be explained with reference to the Figures.

Figure 1 shows a multiserver 10 according to the present invention. Multiserver 10 comprises a configuration management interface 20, a file server 22, a print server 24, a web server 26, a File Transfer Protocol (FTP) server 28, a time server 29, a telnet server 30, a mail server 32, a fax server 34, a phone connection 36, a domain name server 38, and an internet connection 40. Multiserver 10 is connected to a plurality of LAN workstations 42 through a local area network (LAN) 50.

Each of the servers referred to above is designed to provide one or more computer services. For example, file server 22 provides file storage and retrieval services. Computer services services provided by other servers are described below in the discussion of each server. Certain computer services may be provided by more than one server. For example, fax server 34 and mail server 32 cooperate to provide the fax relaying services described below.

As will be appreciated, multiserver 10 will be installed on a computer (not shown). This computer is referred to hereinafter as the multiserver computer. In the preferred embodiment of multiserver 10, a Linux based operating system has been installed on the multiserver computer prior to the installation of software packages which comprise components of multiserver 10.

Linux is one of a number of unix operating systems and will be familiar to one skilled in the art. Although a Linux based operating system is installed on the multiserver computer of the preferred embodiment, one skilled in the art will recognize that other unix based operating systems and non-unix based operating systems may be used as the operating system of a multiserver and will be capable of adapting the present invention for use with such operating systems.
In the preferred embodiment, LAN workstations 42 may be unix platform, Windows platform or Macintosh platform computers. One skilled in the art will appreciate that computers using other platforms, such as PalmOS, used by the PalmPilot handheld computers, may be added as LAN workstations and will be capable of doing so.

As will be described in further detail below, the configuration of multiserver 10 is normally controlled by an administrator.

In the preferred embodiment of multiserver 10, domain name server 38 hosts a primary domain, which is accessible through the internet. The primary domain serves as an incoming mail service. In the preferred embodiment, the primary domain has at least five additional hosted services: a private web site, a public web site, an FTP site, an outgoing mail service and a fax service. A person skilled in the art will recognize that, in a different embodiment of a multiserver according to the present invention, the primary domain may not have all of these hosted services or may have additional hosted services.

Domain name server 38 may also host a number of virtual domains, each of which may have a domain name entirely distinct from the domain name of the primary domain. A virtual domain name serves as an incoming mail service for each virtual domain. Like the primary domain, each virtual domain may have a number of hosted services. In the preferred embodiment of multiserver 10, each virtual domain has at least three additional hosted services: a private web site, a public web site and an outgoing mail service. If a virtual domain administrator has been designated for the virtual domain (described below), the virtual domain administrator will have FTP access to the private and public web sites.

In addition, a number of sub-domains may be created under the primary domain. Sub-domain names must consist of a name prepended to the primary domain name. For example, if the primary domain name is ntk.com, a valid sub-domain name is testing.ntk.com. The sub-domain serves as an incoming mail service for the sub-domain. In the preferred embodiment, each sub-domain has at least three additional hosted services: a private web site, a public web site and an outgoing mail service. If a virtual domain administrator has been designated for the sub-domain (described below), the virtual domain administrator will have FTP access to the private and public web sites.

Additional hosted services may be added to the primary domain, virtual domains and sub-domains in the manner described below.

Multiserver 10 may be used by several groups of users. The first group of users are LAN users, who are given password protected access to multiserver 10 services from LAN workstations 42 connected to multiserver 10 by means of LAN 50. LAN users include users who connect to multiserver 10 by any communication means, such as a point to point protocol (PPP) connection, which is a part of LAN 50. LAN users are given an e-mail account on the primary domain of multiserver 10, allowing them to use the incoming and outgoing mail services of the primary domain. A home directory is also created in the file system of the multiserver 10 for each LAN user, however, LAN users may or may not be given access to this home directory, depending on the
configuration of multiserver 10. LAN users may be given authorized FTP access to their home directory. LAN users who are members of an admin group (described below) are the only users permitted to access multiserver 10 via telnet.

A second group of users are web surfers, who may be permitted to access, without entering a password, the public web sites of the primary domain, sub-domains and virtual domains.

A third group of users are guests, who are given password protected access to specific private web sites of the primary domain, specific sub-domains or specific virtual domains.

A fourth group of users are virtual domain administrators, who have the authority to modify the content of the public and private web sites of their respective sub-domains or virtual domains via authorized FTP access.

A fifth group of users are virtual domain e-mail account users, who are given an e-mail account on a sub-domain or virtual domain, allowing them to use the incoming and outgoing mail services of that domain.

A sixth group of users are FTP surfers. FTP surfers may be given access to the public anonymous FTP site of the primary domain.

As noted above, LAN users and virtual domain administrators are the only users that may have authorized FTP access to the file system of multiserver 10.

Figure 2 shows a security model of multiserver 10. File server 22, print server 24, fax server 34 and a LAN workstation 42 are shown connected to one another by means of LAN 50. Multiserver 10 may be connected to a plurality of LAN workstations 42 in known manner by means of LAN 50.

File server 22, print server 24 and fax server 34 are further connected to internet firewall 60. Domain name server 38, web server 26, mail server 32, FTP server 28, time server 29 and telnet server 30 are connected between internet firewall 60 and LAN firewall 62.

LAN firewall 62 is connected to internet connection 40. Internet connection 40 is coupled to the internet (not shown) to allow web surfers to access the web sites of the primary domain, specific sub-domains or specific virtual domains and to allow LAN users to access internet and web sites located on the internet.

File server 22, print server 24, fax server 34 and LAN workstations 42 may be described as being “outside the internet firewall” and this is indicated by dashed box 64. Time server 29, domain name server 38, web server 26, mail server 32, FTP server 28 and telnet server 30 may be described as being “on the firewall” and this is indicated by dashed box 66. Internet connection 40 and the internet (not shown) may be described as being “outside the LAN firewall” and this is indicated by dashed box 68.

All LAN users will normally have access to elements of the multiserver 10 which are outside the internet firewall or on the firewall (boxes 64 and 66), although access to specific services may be restricted by the administrator. LAN Users may be given access to the internet, which is outside the LAN firewall 62, if desired by the administrator.
Conversely, web surfers will normally be able to access components of the multiserver 10 which are on the firewall and outside the LAN firewall (boxes 66 and 68). In the preferred embodiment, web surfers cannot access components of multiserver 10 which are outside the internet firewall (box 64). This cannot be varied by the administrator.

Configuration management interface 20 (Figure 1) uses a colour coding scheme to identify the location of specific components of multiserver 10 relative to the internet firewall 60 and the LAN firewall 62. Components which are outside the internet firewall (box 64) are displayed to the user with a green background, indicating that they are considered safe from web surfers. Components which are outside the LAN firewall (box 68) are displayed with a red background, indicating that they are accessible to web surfers. Components which are on the firewall (box 66) are displayed with a red or yellow background. Components which are accessible to web surfers, such as the domain name server 38, web server 26 and FTP server 28 are displayed with a red background. Components which may be accessible to web surfers, depending on options selected by the administrator using configuration management interface 20 are displayed, such as mail server 32, are displayed with a yellow background. One skilled in the art will recognize that any set of colours may be selected and the implementation of this invention is not restricted to the use of colour on configuration management interface 20.

The preferred embodiment of multiserver 10 will now be described in further details in two steps. Part One below describes the various servers and components of multiserver 10 by setting out the software packages and other elements which comprise the servers and components. Most elements of the multiserver 10, other than configuration management interface 20, are software package available pursuant to the well-known GNU License. The use of these software packages will be known to persons skilled in the art. Part Two describes the configuration of multiserver 10 using configuration management interface 20. Part Three describes a fax scanner which is part of a fax server described in Parts Two.

PART ONE: ARCHITECTURE OF MULTISERVER 10

Authentication and Access Control Services

Various components of multiserver 10 require authentication to permit users to access various services. For example, a LAN user must enter a password to access services such as e-mail. To provide authentication services, the standard unix module PAM (Pluggable Authentication Module) has been implemented. A person skilled in the art will understand how to implement PAM or another authentication utility to provide the necessary authentication services.

In addition, accessibility to various services by the various users may be restricted based on the location from which the user has access multiserver 10 and other criteria. In the preferred embodiment of multiserver 10, the well-known TCP Wrappers package has
been implemented to provide access control. For example, the TCP Wrappers package is used to control the access available to LAN users to their home directories through telnet server 30.

**File server 22**

File server 22 provides file storage and retrieval services for LAN users connected to the multiserver 10 via LAN connection 50.

File server 22 is implemented using the following packages, which are available pursuant to the GNU license:

(i) Samba for Windows file services;

(ii) Netatalk for Macintosh file services; and

(iii) NFS for unix compatible file services.

**Print Server 24**

Print server 24 provides printing services to LAN workstations 42. Print server 42 allows LAN users to print a document from LAN workstations 42 to configured printers.

Print server 24 is implemented using the following software packages, which are available pursuant to the GNU license:

(i) Samba for Windows printer services;

(ii) Netatalk for Macintosh printer services; and

(iii) lpd for unix compatible printer services.

Print server 24 is also implemented using the following software package, which is available pursuant to the Alladin Free Public License, for making all configured non-postscript printers compatible with postscript:

(i) Ghostscript.

**Web Server 26**

Web server 26 provides web site internet services. Web server 26 is connected to the internet. This connection may be via an ISDN device, analog telephone modem or another device, which will be known to the person skilled in the art.

Web server 26 is implemented using the following package, which is available pursuant to the GNU license:

(i) Apache.

**Fax Server 34**

Fax server 34 permits authorized users of the multiserver 10 to send and receive documents via facsimile devices connected to multiserver 10.

Fax server 34 is implemented using the following package, which is available from Silicon Graphics, Inc.:

(i) Hylafax.
The Hylafax software package receives faxes and converts them into graphic image files in a TIFF format. Hylafax program file faxrcvd stores these TIFF files in a received fax queue.

In the preferred embodiment, Hylafax program file faxrcvd has been replaced. The new faxrcvd program is written in the Tcl/TK programming language, which will be familiar to persons skilled in the art. In the preferred embodiment, the new faxrcvd is used to convert the TIFF files created by Hylafax into Adobe Acrobat compatible PDF format graphic files and to implement an automatic e-mail delivery system for received faxes.

The administrator of multiserver 10 may specify auto-delivery rules for received faxes based on the station ID of the sending fax station. These rules create a one-to-many link between a particular station ID and one or more recipients identified by their e-mail addresses, which need not be e-mail addresses in domains hosted on multiserver 10. These autodelivery rules are recorded in a Tcl/TK language program file /var/spool/fax/etc/delivery, which has the following format:

```
switch -- "$SEND" {
    station_ID [ set SENDTO recipients ; set infaxfs infax? ]
.
.
    default [ set SENDTO default_recipients ; set infaxfs infax? ]
}
```

where

- `station_ID`: the station_ID of the sending fax station
- `recipients`: a comma delimited list of e-mail addresses to which a fax received from the the sending fax station will be sent in PDF format
- `infax?`: 0 - indicates that the PDF format file will not be copied to an infax file share volume (The infax file share volume is used to store incoming faxes. It is further described below in the description of file share volumes) 1 - indicates that the PDF format file will be copied to the infax file share volume
- `default_recipients`: a comma delimited list of e-mail addresses to which a PDF format file for a fax received from a station
whose station_ID is not specified in any of the auto-delivery rules above will be sent. If this list is left empty, any fax which is not auto-delivered according to the earlier rules will be stored in the infax file share volume.

After a fax is received and has been converted into TIFF format, Hylafax daemon hfaxd calls the modified faxrcvd script, which then takes the following steps:

1. Hylafax function faxinfo is used to obtain the following information about the received fax:

   - TIFF file name
   - sending fax station station_ID
   - number of pages in the fax
   - resolution of the fax (normal or high)
   - page size of received fax
   - date and time fax received
   - time taken to receive fax
   - data rate of fax transmission
   - received fax status (OK or error message)

2. The file name for the pdf file to be created is determined. This filename has the following format:

   DateFaxrefModemref.pdf

   where

   Date is the system clock date in MMDDYYYY format

   Faxref is a unique three character reference for each fax received on a particular modem on a particular day. The first fax received on each modem on a particular day is given Faxref AAA, the next fax is given Faxref AAB, etc.

   Modemref a unique two character reference assigned to each modem in a manner described below.

   For example, the fourth fax received on fax modem FC on March 29, 1999 will have the file name 03291999AADFC.pdf.
3. The /var/spool/fax/etc/delivery file is used to determine whether the station_ID matches an auto-delivery rule and if so, which e-mail addresses the PDF format file will be sent to and if it will be stored in the infax file share volume. If not, the default rule is used to determine which e-mail addresses the PDF format file will be sent to and whether it will be stored in the infax file share volume.

4. If an error occurred during fax reception, then the error message is sent to the specified e-mail addresses. If the default auto delivery rule was used to determine the specified recipient, and no recipient was specified, the error message is sent to the members of the infax group (described below).

5. If the fax was received at normal resolution, then the Hylafax TIFF file is converted into a postscript format file using unix utility tiff2ps. The postscript file is converted into a PDF format file using the unix utility ps2pdf. This PDF file is given the file name determined in step 2.

6. If the fax was received at high resolution, the Hylafax TIFF file is converted directly into a PDF format file using a function named convert. This PDF file is given the file name determined in step 2. (The convert function is part of a graphic manipulation package named Image Magick, which is available pursuant to the GNU license.)

7. The PDF is converted into a base 64 encoded e-mail compatible file attachment using a program called uuenview, which is available in the public domain.

8. The base 64 encoded e-mail compatible file attachment is file is e-mailed to the specified recipients using Sendmail, along with the information about the fax determined in step 1.

9. If specified in var/spool/fax/etc/delivery, the PDF file is moved to the infax file share volume.

Domain Name Server 38

Domain Name Server 38 provides IP address information in response to queries from the internet regarding domains hosted by multiserver 10.

Domain Name Server 38 is implemented using the following package, which is available pursuant to the GNU license:

(i) BIND.

Mail Server 32

Mail server 32 provides internet e-mail services for LAN user, virtual domain administrator and virtual domain e-mail account users. Mail server 32 is also used by other components of multiserver 10, such as fax server 34 to communicate with LAN users.

Mail server 32 is implemented using the following software packages, which are available pursuant to the GNU license:

(i) Sendmail, for relaying outbound e-mail and accepting incoming e-mail;
(ii) Procmail, for further processing incoming mail (for example, sending received mail to a fax machine); and
(iii) Fetchmail, for consolidating multiple external e-mail accounts into a single LAN user account.

5 FTP Server 28

FTP server 28 provides remote file access to LAN users and virtual domain administrators via the internet using the File Transfer Protocol.

FTP server 28 is implemented using the following package, which is available pursuant to the GNU license:

(i) WU-FTPD.

Telnet Server 30

Telnet server 30 provides LAN users in the admin group with remote access to multiserver 10 via the internet using the DARPA telnet protocol.

Telnet server 30 is implemented using the following package, which is available pursuant to the GNU license:

(i) TELNET.

Time Server 29

Time server 29 provides time synchronization services to LAN workstations and to the internet using the Network Time Protocol.

Time server 29 is implemented using the following package, which is available pursuant to the GNU license:

(i) XNTP.

Internet Firewall 60 and LAN Firewall 62

One of the purposes of multiserver 10 is to allow the administrator to securely administer internet domains while reducing the exposure of multiserver 10 to malicious public users. At the same time, the administrator may wish to allow LAN users to access the internet while limiting the web sites to which LAN users are able to connect. These security services are provided in multiserver 10 by means of an Internet firewall 60 and a LAN firewall 62, shown in Figure 2.

30 The purpose of internet firewall 60 is to protect multiserver 10 and the LAN from the internet (i.e. from web surfers and guests). The purpose of LAN firewall 62 is to control the use of the internet from LAN workstations 42.

The well known Unix kernel-level firewall rule-set administration utility, IP chains, is used to configure the acceptance or rejection of packets through the internet and LAN firewalls 60, 62.

35 The policy used to configure both the internet and LAN firewalls 60, 62 may be stated as “That which is not expressly permitted is denied.”
Internet firewall 60 and LAN firewall 62 are sequentially configured by executing two scripts. The first configures internet firewall 60, which is fixed and cannot be varied by changing the configuration of multiserver 10. The second script configures LAN firewall 62, which will be configured depending on the internet access policy assigned to specific LAN workstation 42 (described below).

**Internet Firewall Configuration Script**

The rules for the internet firewall are put into effect before the network layer of the multiserver computer is enabled. This prevents the security risk known as a race condition from arising.

In the preferred embodiment of multiserver 10, the internet firewall is configured by taking the following steps, using IP chains:

1. Disallow all packets from all sources, whether from the LAN or the internet.
2. Trap all packets which are ultimately passed for bandwidth usage accounting.
3. Allow the mail server functions from the LAN or the internet.
4. Allow the fax server to communicate with itself via a loopback address.
5. Disallow packets that originate from the internet which claim to originate from the LAN.
6. Allow packets that originate from the LAN that are destined for the LAN to pass.
7. Allow packets originating from the internet or the LAN for preapproved services hosted on multiserver 10 to pass. In the preferred embodiment, these services include web server, mail server, FTP server, telnet server, and time server.

**LAN Firewall Configuration Script**

Each of the LAN workstations 42 may be assigned one of four internet access policies:

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>the LAN workstation is not permitted any access to the internet</td>
</tr>
<tr>
<td>Approved</td>
<td>the LAN workstation is permitted access only to pre-approved internet hosts</td>
</tr>
<tr>
<td>Restricted</td>
<td>the LAN workstation is permitted access to all internet hosts except those in a restricted list</td>
</tr>
<tr>
<td>Full</td>
<td>the LAN workstation is permitted access to all internet hosts</td>
</tr>
</tbody>
</table>

The LAN firewall 62 is configured by taking the following steps:

1. For every LAN workstation 42 assigned an internet access policy of none, nothing is done.
2. For every LAN workstation 42 assigned an internet access policy of approved, packets are only allowed from approved sites.
3. For every LAN workstation 42 assigned an internet access policy of restricted:
   (i) Packets are disallowed from restricted sites;
(ii) All other packets are allowed.

4. For every LAN workstation assigned an internet access policy of full, packets are allowed from any site.

Configuration Management Interface 20

Configuration management interface 20 provides the administrator of multiserver 10 with a convenient, efficient and centralized means for configuring the various components of multiserver 10. The configuration management interface 20 consists of a number of screens which allow multiserver 10 to be configured to operate as desired by the administrator.

The description of configuration management interface 20 is broken into two parts. Configuration management interface 20 maintains a set of data files to record the configuration selected by the administrator for multiserver 10. These data files are described in this section. The use and operation of configuration management interface 20 is described below in Part Two.

The data files maintained by configuration management interface 20 are, in general, stored in a directory /root/MSconfig/dat and are described here, organized by the server to which they are related and the functions they serve. These data files are used by configuration management interface 20 for several purposes. First, they are used when the configuration of multiserver 10 is changed to ensure that only valid changes are made. Second, these files may be used to restore the configuration of various components of multiserver 10 to the desired condition after a malfunction has occurred. One skilled in the art will recognize that these data files are not the configuration files for the public domain software packages described above.

In the description below, the use of capital letters in the name of a file generally indicates that, in the preferred embodiment, the capital letters should be replaced with the equivalent information to determine the actual file name. For example, if reference is made to the file /root/MSconfig/dat/VIRTUALDOMAIN.dat, then a real file name may be /root/MSconfig/dat/bubba.com.dat, where bubba is the name of a virtual domain added to domain name server 38.

GROUPS

LAN Users who have been given access to workstations 42 are organized into various groups. The names of these groups are stored in a file named /root/MSconfig/dat/groups.dat, which comprises a lists of group names. When multiserver 10 is initially configured, /root/MSConfig/dat/groups.dat has the following contents:

*admin
*faxblast
*infax
*users
Each of the initial groups listed above is prefixed with an asterisk (*) to indicate that the group cannot be deleted. The initial groups required for various operations of multiserver 10 are:

<table>
<thead>
<tr>
<th>Group</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>members are given administrator permissions, allowing them to log directly in to multiserver 10, as opposed to non-admin LAN users, who may access multiserver 10 resources (i.e. may mount file share volumes or connect to printers, etc.) but may not log in to the multiserver 10 directly</td>
</tr>
<tr>
<td>faxblast</td>
<td>LAN users must be a member to send a fax</td>
</tr>
<tr>
<td>infax users</td>
<td>LAN users must be a member to access the file share volume in which incoming faxes are stored by default group includes all LAN users but does not include other types of users such as virtual domain administrators</td>
</tr>
<tr>
<td>vadmin</td>
<td>group includes all virtual domain administrators.</td>
</tr>
<tr>
<td>virtualmail</td>
<td>used as the primary group for virtual users added for e-mail enabled groups, as described below.</td>
</tr>
<tr>
<td>web</td>
<td>members are given write access to the web_server file share volume, allowing them to modify all web sites</td>
</tr>
</tbody>
</table>

When the administrator adds a group to multiserver 10, the name of the group is added to data file /root/MSconfig/dat/groups.dat (without an asterisk).

The administrator may configure a group to be “e-mail enabled”. A group which is e-mail enabled is added to multiserver 10 as a virtual LAN user. This virtual LAN user is given an e-mail account on the primary domain of multiserver 10. The e-mail address of members of the e-mail enabled group is placed in a .forward file within the home directory of the virtual user. This .forward file is used in known manner by the Sendmail software package to forward mail sent to the virtual LAN user to all members of the e-mail enabled group. The virtual LAN user exists only for the purpose of forwarding e-mail messages to group members and does not have any other attributes of a LAN user.

A file entitled /root/MSconfig/dat/grpMail/GROUPNAME.dat is created for every e-mail enabled group. This file contains a list of the users who are members of the group.
USERS

When a LAN user is added to multiserver 10, the LAN user is assigned a LAN user name, password, given a home directory in the file system of the multiserver computer, is added to the users group, may be added to other groups and is provided an e-mail account on the primary domain of multiserver 10. The LAN user's e-mail may be forwarded to another e-mail address, to a fax machine or it may be processed by a custom script. For each LAN user, this information is recorded in a file named /root/MSconfig/dat/usersList.dat, each record having the following format:

USERNAME /home/USERNAME /bin/SHELL GROUP(S) FORWARDING

where:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USERNAME</td>
<td>LAN user's name</td>
</tr>
<tr>
<td>/home/USERNAME</td>
<td>path of the LAN user's home directory</td>
</tr>
<tr>
<td>/bin/SHELL</td>
<td>SHELL will be /bin/bash if user is in the admin group; otherwise /bin/false</td>
</tr>
<tr>
<td>GROUP(S)</td>
<td>comma separated list of groups to which LAN user belongs</td>
</tr>
<tr>
<td>FORWARDING</td>
<td>DON'T if e-mail is not forwarded; comma separated list of e-mail addresses; fax machine telephone number; or CUSTOM if a custom .procmailrc script is used</td>
</tr>
</tbody>
</table>

When a new user is added, a record is added to data file /root/MSconfig/dat/usersList.dat.

FILE SHARE VOLUMES

File share volumes are used by multiserver 10 for various purposes. For example, file share volumes may be created and assigned to LAN users or groups, allowing all members of the group to access the file share volume.

In addition, a file share volume is created for some of the initial groups created when multiserver 10 is initially configured.

group  file share volume  Description
admin  admin              used to store administrative scripts and the network trash folder; members of the admin group are given access to this file share volume
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHAREVOLUME</td>
<td>Name of the file share volume</td>
</tr>
<tr>
<td>PRIMARYOWNER(GROUP)</td>
<td>Name of the user or group which owns the file share volume</td>
</tr>
<tr>
<td>PRIMARYGROUPACCESS</td>
<td>Access privileges of the primary user or group</td>
</tr>
<tr>
<td>OTHERGROUPACCESS</td>
<td>Access privileges of users or groups other than the primary user or group</td>
</tr>
</tbody>
</table>

Information about each file share volume is recorded in a file named /root/MSconfig/dat/fShareList.dat, each record having the following format:

```
SHAREVOLUME PRIMARYOWNER(GROUP) PRIMARYGROUPACCESS OTHERGROUPACCESS
```

As described above certain groups are created when multiserver 10 is initially configured. File /root/MSconfig/dat/fShareList.dat will initially have the following contents:

```
*admin admin ReadWrite None
```
*cdrom users ReadOnly ReadOnly
*fax_blast faxblast ReadWrite None
*infax infax ReadWrite None
*pftp N/A None None
5 *web_server web ReadWrite ReadOnly

PRINTERS

Information about all printers which have been added to print server 24 is stored an a file named /root/MSconfig/dat/printersList.dat, each record having the following format:

PRINTERNAME PORT PRINTERTYPE NETWORK

where:

Field Description
PRINTERNAME Name of printer
PORT Port on which printer is connected
PRINTERTYPE Identifies the printer driver to be used with the printer
NETWORK Identifies whether the printer is a network printer. If it is, then the network type (for example, ethtalk or token ring) is entered in this field. This must match the type of LAN used with multiserver 10.

FAX

Fax server 34 sends and receives faxes using one or more modems connected to multiserver 10. As modems are added to fax server 34, each modem is assigned a unique two character code used by fax server 34 to distinguish between faxes received on different modems. The data required to configure fax server 34 to perform these functions is stored in several data files used by configuration management interface 20.

Information about modems connected to multiserver 10 is recorded in a file named /root/MSconfig/dat/modems.dat, each record having the following format:

STATIONID MODEMREFERENCE AREACODE FAXNUMBER PORT

where:

Field Description
STATIONID Station ID of the modem
MODEMREFERENCE Two character modem reference assigned when the modem is added to fax server 34
AREACODE Area code of the modem’s telephone connection
FAXNUMBER      Telephone number of the modem’s telephone connection

PORT    Port on which the modem is connected to multiserver 10

The modem reference of the last modem added to fax server 34 is recorded in a
file named /root/MSconfig/dat/modemref.dat. When a new modem is added, the modem
reference assigned is incremented, stored in this file and is recorded in
/data/MSconfig/dat/modems.dat as the reference number of the new modem. In the
preferred embodiment, modem references comprise a two letter alphabetic code. The
first modem added to fax server 34 is assigned modem reference FA; the next modem
added is assigned modem reference FB.

The port and modem reference for each modem are also stored in a data file
named /var/spool/fax/modems.dat, each record having the following format:

PORT  MODEMREFERENCE

Data file /var/spool/fax/modems.dat is used by Hylafax to create unique file names
for PDF format files in which received faxes are stored.

Information regarding the redirection of incoming faxes received from a
specified station ID to one or more users or groups is recorded in a file named
/root/MSconfig/dat/inFaxIDs.dat, each record having the following format:

INCOMINGSTATIONID  FORWARDTO  INFA;

where:

Field                Description

INCOMINGSTATIONID    Station ID of sending fax machine

FORWARDTO            A comma separated list which may include:
usersnames of LAN users; internet e-mail
addresses; or names of mail enabled groups.

INFAX_FSV            Yes/No; Are faxes delivered according to this
auto-delivery rule also stored in the infax file
share volume?

The /root/MS Config/dat/inFax IDs.dat file is used to create the /var/spool/fax/etc/
delivery file.

The destination of incoming faxes which are not delivered according to an auto-
delivery rule set out in /root/MSconfig/dat/inFaxIDs.dat is set out in a file named
/root/MSconfig/dat/inFaxRcvrs.dat, which contains a comma separated list of: user names
of LAN users; internet e-mail addresses; or the names of mail enabled groups. These incoming faxes are delivered to each user, address, or group identified.

**DOMAIN NAMES**

A list of the domains hosted by multiserver 10, their associated hosted services and the IP address of the computer to which each domain or host service will resolve is stored in a file named /root/MSconfig/dat/dnsmap.dat, which has the following format:

<table>
<thead>
<tr>
<th>PRIMARYDOMAIN</th>
<th>PRIMARY</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUB.PRIMARYDOMAIN</td>
<td>SERVERIPADDRESS</td>
</tr>
<tr>
<td>AUTH.PRIMARYDOMAIN</td>
<td>SERVERIPADDRESS</td>
</tr>
<tr>
<td>FAXSERVERNAME.PRIMARYDOMAIN</td>
<td>SERVERIPADDRESS</td>
</tr>
<tr>
<td>FTPSERVERNAME.PRIMARYDOMAIN</td>
<td>SERVERIPADDRESS</td>
</tr>
<tr>
<td>MAILSERVERNAME.PRIMARYDOMAIN</td>
<td>SERVERIPADDRESS</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SUBDOMAIN</th>
<th>SERVERIPADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUB.SUBDOMAIN</td>
<td>SERVERIPADDRESS</td>
</tr>
<tr>
<td>AUTH.SUBDOMAIN</td>
<td>SERVERIPADDRESS</td>
</tr>
<tr>
<td>mail.SUBDOMAIN</td>
<td>SERVERIPADDRESS</td>
</tr>
</tbody>
</table>

<list additional sub-domains of the primary domain>

<table>
<thead>
<tr>
<th>VIRTUALDOMAIN</th>
<th>SERVERIPADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUB.VIRTUALDOMAIN</td>
<td>SERVERIPADDRESS</td>
</tr>
<tr>
<td>AUTH.VIRTUALDOMAIN</td>
<td>SERVERIPADDRESS</td>
</tr>
<tr>
<td>mail.VIRTUALDOMAIN</td>
<td>SERVERIPADDRESS</td>
</tr>
</tbody>
</table>

<list additional virtual domains>

As an example, if multiserver 10 is configured with ntk.com as its primary domain, alpha.ntk.com and fun.ntk.com as sub-domains and beta.com and gamma.net as virtual domains, then data file /root/MSconfig/dat/dnsmap.dat may have the following contents:

<table>
<thead>
<tr>
<th>ntk.com</th>
<th>PRIMARY</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.ntk.com">www.ntk.com</a></td>
<td>ntk.com</td>
</tr>
<tr>
<td>auth.ntk.com</td>
<td>ntk.com</td>
</tr>
<tr>
<td>fax.ntk.com</td>
<td>ntk.com</td>
</tr>
<tr>
<td>ftp.ntk.com</td>
<td>ntk.com</td>
</tr>
<tr>
<td>mail.ntk.com</td>
<td>ntk.com</td>
</tr>
<tr>
<td>alpha.ntk.com</td>
<td>ntk.com</td>
</tr>
<tr>
<td><a href="http://www.alpha.ntk.com">www.alpha.ntk.com</a></td>
<td>ntk.com</td>
</tr>
</tbody>
</table>
When a domain is added to domain name server 38, two web sites are created. The first is a public web site which will be accessible to web surfers. The second is a private web site which will only be accessible to guests of the domain. The names of the public and private web sites are used as a prefix to the name of the domain to identify the two web sites to users.

When a domain is created, files relating to the domain are stored in a directory within the web_server file share volume described above under the heading "File Share Volumes". In the preferred embodiment of multiserver 10, this directory is given a name called a domain reference. The first domain created is given domain reference A; the second domain is given domain reference B. The directory name is incremented for each subsequent domain added to domain name server and more than one character will be used if necessary. This naming convention is used to allow domain names longer than 8+3 character file names permitted by Windows 3.11 workstations. For virtual domains and sub-domains, this information is stored in a file named /root/MConfig/dat/domainList.dat, each record having the following format:

```plaintext
DOMAINNAME PUBLICPREFIX AUTHPREFIX DOMAINREF
```

where:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAINNAME</td>
<td>Name of the virtual domain or sub-domain</td>
</tr>
<tr>
<td>PUBLICPREFIX</td>
<td>Prefix of public web server of domain</td>
</tr>
<tr>
<td>AUTHPREFIX</td>
<td>Prefix of private web server of domain</td>
</tr>
<tr>
<td>DOMAINREF</td>
<td>Domain reference</td>
</tr>
</tbody>
</table>
This information is mirrored in a file named /home/httpd/legend.txt. This file is stored in the web_server file share volume, and is therefore accessible to members of the web group. Data file /root/MSconfig/dat/domainList.dat will not normally be accessible to these users.

For the primary domain, this information is stored in a file named /root/MSconfig/dat/screens.dat (explained below under the heading “Screen Options”).

The file /root/MSconfig/dat/vDomRefCounter.dat contains the last domain reference assigned to a domain and is used to ensure that domains are given unique sequential domain references.

MAIL SERVER

Mail server 32 provides incoming and outgoing internet e-mail services for LAN users and e-mail account users.

Mail server 32 may be configured to relay e-mail from any IP address, from specific IP addresses only, from the LAN only or from no IP address. The configuration of these options is described below. If e-mail relaying from specific IP addresses is selected, the permitted IP addresses are listed in a file named /root/MSconfig/dat/ipallow.dat, which is used by the sendmail software package in known manner.

Each domain may have e-mail accounts and aliases to those accounts.

For the primary domain, this information is stored in a data file named /root/msconfig/dat/aliasmail.primary, each record having the following format:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALIAS</td>
<td>alias for the e-mail address</td>
</tr>
<tr>
<td>ACCOUNT</td>
<td>e-mail account to which the alias is linked</td>
</tr>
</tbody>
</table>

For sub-domains and virtual domains, this information relating to these e-mail accounts and the associated aliases are stored in a file named /root/MSconfig/dat/aliasmail.DOMAINNAME, where DOMAINNAME is the name of the domain. The file /root/MSconfig/dat/aliasmail.DOMAINNAME may contain two types of records, account records and alias records, which may appear in any order.

Account records have the following format:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCOUNT</td>
<td>e-mail account name address</td>
</tr>
</tbody>
</table>

where
empty field (dash is required)

Alias records have the following format:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALIAS ACCOUNT</td>
<td>e-mail account to which the alias is linked</td>
</tr>
</tbody>
</table>

Each sub-domain and virtual domain may have a single virtual domain administrator, who is given authority to access the public and private web sites of the domain and modify them. If a virtual domain administrator is defined, the e-mail account name for the virtual domain administrator is stored in a file named /root/MSconfig/dat/siteAdmin/DOMAINNAME, which has the following format:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SITEADMINISTRATOR</td>
<td>virtual domain administrator’s e-mail account name</td>
</tr>
</tbody>
</table>

The virtual domain administrator’s e-mail account on the sub-domain or virtual domain is not listed in the file /root/MSconfig/dat/aliasmail.DOMAINNAME. Aliases to the virtual domain administrator’s e-mail account will be listed in that file.

Mail server 32 may be configured to refuse mail sent from a specific e-mail address or from an entire internet domain. Information relating to such blocked addresses or domains is recorded in a file named /root/MSconfig/dat/mailList.dat, each record having the following format:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BLOCKEDADDRESS/DOMAIN</td>
<td>originating e-mail address or internet domain from which e-mail will be rejected</td>
</tr>
<tr>
<td>MESSAGE</td>
<td>message which will be returned with rejected message to originating e-mail address or internet domain</td>
</tr>
</tbody>
</table>
WEB SERVER

The names and passwords of guests of the private web sites of each domain are stored in a data file named /root/MSconfig/vDomains/DOMAINNAME.guests. For example, the file name for the private web site is /root/MSconfig/vDomains/primary.guests. Each of these files has the following format:

GUESTNAME PASSWORD

where

Field Description
Guestname Name of the guest of the private web site of the domain
Password Password of the guest

ADMINISTRATION - LOCKS

Multiserver 10 is configured to be administered at two levels: management level and administration level. Access to the administration screens of configuration management interface 20 may be at either level, both of which require password authorization.

Information relating to the screens which are accessible when configuration management interface 20 is in a locked state is stored in a file named /root/MSconfig/dat/lockConfig.dat. (The locked and unlocked states of the configuration management interface 20 are explained below in Part Two.) This information is divided into two sections: the Administration locks section and the Management locks section.

Administration locks section

This section of data file /root/MSconfig/dat/lockConfig.dat contains a 0 or 1 for each of the following screens, indicating that the administrator has respectively, denied or permitted access to that particular screen, when the configuration management interface 20 is in a locked state.

Users & Groups
File Server
Print Server
Fax Server
Domain Server
Web Server
FTP Server
Mail Server
Firewall
Networks

Management locks section
This section of data file /root/MSconfig/dat/lockConfig.dat contains a 0 or 1 for each of the following screens, indicating that the manager has, respectively, denied or permitted access to that particular screen when the configuration management interface is in a locked state. As described below, management locks override administrator locks.

Users & Groups
File Server
Print Server
Fax Server
Domain Server
Web Server
FTP Server
Mail Server
Firewall
Networks
Miscellaneous sub-screen
Backup sub-screen
Locks sub-screen
Remote sub-screen
DNS sub-screen

The administration password is stored in a file named /root/MSconfig/dat/adminpass.dat in an encrypted format. The management password is stored in an encrypted format in a file named /root/MSconfig/dat/mgmtpass.dat.

ADMINISTRATION - FIREWALL
LAN users may be permitted to access the internet from specific LAN workstations 42. Information relating to these LAN workstations 42 is recorded in a file named /root/MSconfig/dat/registry.dat, each record having the following format:

LANMACHINEIP EXPIRYTIME ACCESS

where

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LANMACHINEIP</td>
<td>IP address of the LAN Workstation 42</td>
</tr>
<tr>
<td>EXPIRYTIME</td>
<td>Expiry time of registration of LAN Workstation 42</td>
</tr>
</tbody>
</table>
ACCESS

Type of access permitted from LAN Workstation 42

Three types of access permitted for a LAN Workstation are Full, Approved or Restricted. If Full access is permitted, a LAN user accessing from the specified LAN workstation 42 may access any internet site. If Approved access is permitted, the LAN user may access only internet sites listed in a data file named /root/MSconfig/dat/approved.dat. If Restricted access is permitted, the LAN user may access any internet site except those listed in a file named /root/MSConfig/dat/restricted.dat. These files are used to modify the LAN Firewall configuration script to achieve the specified level of accessibility for each LAN workstation 42.

SCREEN OPTIONS

Configuration management interface 20 is comprised of a number of configuration screens, each of which displays the configuration of various elements of multiserver 10 and allow the administrator to modify the configuration. Some of the information entered by the administrator on these configuration screens is recorded in a file named /root/MSconfig/dat/screens.dat. This file has a fixed number of records, each of which is on a separate line of the file. The records are organized in a number of sections, as described below:

<table>
<thead>
<tr>
<th>Record</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File sharing section</strong></td>
<td></td>
</tr>
<tr>
<td>File Sharing</td>
<td>on - file sharing services are on</td>
</tr>
<tr>
<td></td>
<td>off - file sharing services are off</td>
</tr>
<tr>
<td><strong>Fax Server section</strong></td>
<td></td>
</tr>
<tr>
<td>Fax Server</td>
<td>on - fax services are on</td>
</tr>
<tr>
<td></td>
<td>off - fax services are off</td>
</tr>
<tr>
<td><strong>Administration section</strong></td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>Locked - configuration management interface 20 is locked</td>
</tr>
<tr>
<td></td>
<td>Unlocked - configuration management interface 20 is unlocked</td>
</tr>
<tr>
<td>CD</td>
<td>Mounted - CD-ROM drive is mounted on multiserver 10</td>
</tr>
<tr>
<td></td>
<td>Unmounted - CD-ROM drive is not mounted on multiserver 10</td>
</tr>
</tbody>
</table>
System Administrator

        System Administrator
        LAN user name of system administrator

5

Backups Sections

This section contains two records for each day of the week, respectively indicating (1) whether a backup of the designated sections of the multiserver 10 file system will be done; (2) the time at which the backup will be done on the selected days.

As an example, the records for Monday may have the following values:

Backup on Monday
0 - no backup will be done on Mondays
1 - backup will be done at the designated time each Monday

Monday Backup time
  time designated for backups to be done on Mondays

The backups sections also contains records indicating which sections of the multiserver 10 file system will be backed up:

Backup Users Section
0 - user’s home directories (in the /home file share volume) are not backed up
1 - user’s home directories are backed up

Backup Web Server Section
0 - web_server (/home/httpd) file share volume is not backed up
1 - web_server file share volume is backed up

Backup File Sharing Section
0 - /usr/filesharing directory is backed up
1 - /usr/filesharing directory is not backed up

Backup Operating System
0 - system files in the /etc, /var and other directories are not backed up (a person skilled in the art will be able to determine which files are included in the expression "operating system files")

1 - system file are backed up

Remote Administration Section

FTP Accessibility

LAN - FTP server 28 of the primary domain is accessible only to LAN users accessing from a LAN workstation

Specific - FTP server 28 of the primary domain is accessible to FTP surfers connecting from specified IP addresses

Internet - FTP server 28 of the primary domain is accessible to FTP surfers connecting from any IP address

If specific FTP accessibility is selected, the IP addresses from which an FTP connection will be accepted are listed /root/MScnfig/dat/specFTP.dat.

Remote Login

No External Login - no user may telnet into multiserver 10

LAN - LAN users in the admin group may telnet to multiserver 10 from a LAN workstation

Specific - LAN users in the admin group may telnet into multiserver 10 from a specified IP address

Internet - LAN users in the admin group may telnet into multiserver 10 from any IP address

If specific remote login accessibility is selected, the IP addresses from which a telnet connection will be accepted are listed /root/MScnfig/dat/specRemote.dat.

Time servers section

Multiserver 10 may be configured to maintain correct time based on a signal from one or more time servers. The names of the selected time servers is included in /root/MScnfig/dat/screens.dat.
Primary Time Server  IP address of a primary time server
Secondary Time Server  IP address of a secondary time server
Tertiary Time Server  IP address of a tertiary time server

Primary domain server section
Information relating to the primary domain hosted by multiserver 10 is stored in a series of records in /root/MSconfig/dat/screens.dat containing the following information:

Primary Domain Name
Primary Domain's Public Web Site Name Prefix (eg. www)
Primary Domain's Protected Web Site Name Prefix (eg. auth)
Primary Domain's Server Name
Primary Domain's FTP Server Name Prefix (eg. FTP)
Primary Domain's Mail Server Name Prefix (eg. mail)
Primary Domain's Primary Name Server (always same as Primary Domain Name)
Primary Domain's Secondary Name Server
Primary Domain's Secondary Name Server IP Address (may be different from the Primary Domain Name)

Web server section
Web Server  Off - Web server 26 not will serve web sites to web surfers and guests
            On - Web server 26 will serve web sites to web surfers and guests

LAN User access to Primary Domain's Protected Web Site
0 - LAN users cannot access the private web site of the primary domain
1 - LAN users can access the private web site of the primary domain

Primary domain FTP server section
FTP Server  Off - FTP server 28 will not permit any FTP access to multiserver 10
           On - FTP server 28 will permit FTP access to multiserver 10
FTP Private Section Setting

No access - FTP surfers are denied any access to the primary domain anonymous FTP site

Read only - FTP surfers are permitted read only access to the primary domain anonymous FTP site

Read & Write - FTP surfers are permitted read and write access to the primary domain anonymous FTP site

Write only - FTP surfers are permitted write only access to the primary domain anonymous FTP site

FTP Authorized Section Setting

No access - LAN users and virtual domain administrators are denied FTP access to multiserver 10

Read & Write - LAN users and virtual domain administrators are permitted access to their designated private area in the file system of multiserver 10

For LAN users, the designated private area in the file system of multiserver 10 is the LAN user's home directory. In the case of virtual domain administrators, the designated private area is the directory in which the public and private web sites for the domain are stored.

Mail server section

Outgoing Mail Relay

None - mail server 26 will not relay e-mail originating from any IP address

LAN - mail server 26 will relay e-mail originating from LAN workstations

Specific - mail server 26 will relay e-mail originating from IP addresses specified in a file named /root/MSconfig/dat/ipallow.dat

Internet - mail server 26 will relay e-mail originating from any IP address
Relay Outgoing Mail For All Password Authenticated IP Numbers

Off - mail server 26 will only relay mail according to the rule set in the Outgoing Mail Relay record

On - if Outgoing Mail Relay setting is not Internet, then mailer server 26 will relay e-mail originating from an IP address from which a LAN user has connected and correctly entered his Lan user name and password within the previous 15 minutes

Firewall section

Allow LAN users access to Internet

Off - LAN users cannot access the internet from any LAN workstation 42

On - LAN users may access the internet from specified LAN workstations 42, subject to the internet access policy defined for each specific LAN workstation 42 in a file named /root/MSconfig/dat/registry.dat (described below).

Network (External connection) section

IP Type

Fixed - the IP address of multiserver 10 is fixed

Dynamic - the IP address of multiserver 10 is dynamically assigned

External IP

IP address of multiserver 10 (used only if IP type is fixed)

External Subnet IP

Subnet IP address of multiserver 10 (used only if IP type is fixed)
External Network IP  Network IP address of multiserver 10
(used only if IP type is fixed)

External Broadcast IP

Broadcast IP address of multiserver 10
(used only if IP type is fixed)

External Connection Type

connection type between multiserver 10 and the inter

External Location

physical or logical location on the
multiserver 10 of the internet connection

External Connection Policy

Permanent - connection between
multiserver 10 and internet is maintained
continuously
Dial-on-demand - connection between
multiserver 10 and internet is
established when required and
subsequently terminated

Dial-on-Demand Disconnection

Idle time until Dial-on-demand internet
connection is terminated

External Gateway IP  Gateway IP address of the internet
connection

Network (Internal Connection) section

Internal IP  IP address of LAN connection
Internal Subnet IP  Subnet IP address of LAN connection
Internal Network IP  Network IP address of LAN connection
Internal Broadcast IP  Broadcast IP address of LAN connection

Network (Authorization) section

This information is required only when the connection between multiserver 10
and internet is provided through a telephone connection or other serial connection.
Dial up Telephone Number  Telephone number of internet service provider
Dial up Authorized User Name  User name provided by internet access account
Dial up Authorized Password  Password for internet access account

PART TWO: CONFIGURATION

Multiserver 10 is configured by the administrator using configuration management interface 20. Figure 3 shows a status screen 100 of the configuration management interface 20. Status screen 100 comprises status section 102 and manufacturer information section 106. Status section 102 indicates the current status of the multiserver 10 and allows the administrator to monitor the configuration components of the multiserver 10. Each of these components and the corresponding status indicators will be described below. A plurality of configuration screen pushbuttons 104 allows access to other screens which allow the administrator to monitor and configure components of multiserver 10. Pushbuttons 104 are also displayed on other screens comprising part of the configuration management interface 20.

The configuration of multiserver 10 involves four general steps.

First, the administration of multiserver 10 must be configured using a set of administration subscreens. Second, the networks on which multiserver 10 may communicate must be defined. A multiserver may be equipped for communication on two networks: a LAN, which connects the multiserver 10 to local users and the Internet. Third, LAN services must be defined. This step includes configuring the users and groups that will have access to the multiserver 10, configuring the file server 22; configuring the print server 24 and configuring the fax server 34. Fourth, internet hosting services must be configured, if the administrator wishes to use these services.

During each of these steps, the administrator defines various characteristics of the computer services, based on the operation desired by the administrator. For example, the administrator may defined the characteristics of LAN firewall 62 with respect to the type of internet access available from various LAN workstations 42. These characteristics are used by the configuration management interface 20 to configure the underlying servers such that the servers provide computer services according to the desired characteristics.

During the configuration of multiserver 10, certain configuration changes cannot be made when a core configuration change is being processed. The following changes are defined as core changes:

1. Any of the following daemons are being reset:
   (i) BIND daemon named;
   (ii) Sendmail daemon sendmail;
   (iii) Apache daemon httpd; and
   (iv) Netatalk daemon papd.
2. The backup agent is running (described below).
3. The LAN firewall rules are being changed. (This is done by running the Internet Firewall Configuration Script and the LAN Firewall Configuration Script.)

To ensure that none of these core changes is taking place, the unix pidof command is used to check for the process id (pid) of the process which performs the core change. If no pid is found, this will indicate that the corresponding core change is not taking place. In the description below, a reference to ensuring that a core change is not taking place indicates that the pidof command is run for each such process. If none of the processes is found, then a core change is not taking place.

In the descriptions below of steps taken when an option is selected or a configuration change is made, a statement that “an error is returned” indicates that a message indicating that the option cannot be selected or the configuration change cannot be implemented is displayed and the remaining steps are not taken.

Further, one skilled in the art will recognize that some of the data files must be hashed using the unix makemap command and that the hashed output file of this command is actually used by the executable programs of the software packages described above. Although some references are made below to hashing data files, other data files referred to below may need to be hashed.

**Configuration of the Administration of Multiserver 10**

The administration of multiserver 10 is controlled through a set of administration subscreens, shown in Figures 4-8, which show, respectively, administration locks subscreen 500, administration miscellaneous subscreen 600, administration backups subscreen 650, administration remote access subscreen 700 and administration DNS subscreen 750.

Each of administration subscreens 500, 600, 650, 700 and 750 has a lock/unlock system control 502 and a plurality of administration subscreen pushbuttons 504. Lock/unlock system control 502 will either read “Unlock System” or “Lock System”, when configuration management interface 20 is, respectively, in a locked state or one of two unlocked states: a management unlocked state or an administration unlocked state.

Multiserver 10 is designed to be administered by two groups: managers and administrators. When configuration management interface 20 is in the management unlocked state, a manager may access any screen or subscreen of configuration management interface 20. When configuration management interface 20 is in the administration unlocked state, an administrator may access screens or subscreens of configuration management interface 20 which have been authorized for administration access by the manager. When configuration management interface 20 is in the locked state, any person may access screens or subscreens of configuration management interface 20 which have been designated by the manager and the administration.
When multiserver 10 is first turned on, the configuration management interface 20 is initially in the locked state. If the “Admin” pushbutton is selected from configuration screen pushbuttons 104, an administration password dialog box is displayed (not shown). Managers and administrators may access the administration subscreens by selecting an “Administrator” or “Manager” control in administration password dialog box and entering, respectively, a management or administration password. At this time, lock/unlock system control 502 will read “Unlock System”. If lock/unlock control 502 is selected, configuration management interface 20 will enter either the management unlocked state or the administration unlocked state, depending on whether the management or administration password was entered. When configuration management interface 20 is in either the management unlocked state or the administration unlocked state, lock/unlock system control 502 will read “Lock System”.

When configuration management interface 20 is in the management unlocked state, a manager may display administration locks subscreen 500 (Figure 4) by selecting the “Locks” button from administration subscreen pushbuttons 504.

Referring to Figure 3, administration locks subscreen 500 comprises lock/unlock system control 502, administration subscreen buttons 504, administration locks section 512 and management locks section 540. Management locks section 540 further comprises a set of checkbuttons which control which screens or subscreens of configuration management interface 20 can be accessed by the administrator when configuration management interface 20 is in the administration unlocked state or by anyone when configuration management interface 20 is in the locked state:

<table>
<thead>
<tr>
<th>Control</th>
<th>Controls administrator/locked state access to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users &amp; Groups control 542</td>
<td>users &amp; groups screen 150 (Figure 10)</td>
</tr>
<tr>
<td>Filesharing control 544</td>
<td>file server screen 180 (Figure 11)</td>
</tr>
<tr>
<td>Printers control 546</td>
<td>print server screen 210 (Figure 12)</td>
</tr>
<tr>
<td>Fax control 548</td>
<td>fax server screen 240 (Figure 13) and fax</td>
</tr>
<tr>
<td></td>
<td>routing control screen 270 (Figure 14)</td>
</tr>
<tr>
<td>Domain control 550</td>
<td>domain server screen 300 (Figure 15)</td>
</tr>
<tr>
<td>Web control 552</td>
<td>web server screen 370 (Figure 17)</td>
</tr>
<tr>
<td>FTP control 554</td>
<td>FTP server screen 340 (Figure 16)</td>
</tr>
<tr>
<td>Mail control 556</td>
<td>mail server screen 400 (Figure 18)</td>
</tr>
<tr>
<td>Firewall control 558</td>
<td>firewall screen 450 (Figure 19)</td>
</tr>
<tr>
<td>Network control 560</td>
<td>networks screen 120 (Figure 9)</td>
</tr>
<tr>
<td>Misc. control 562</td>
<td>administration miscellaneous subscreen 600</td>
</tr>
<tr>
<td></td>
<td>(Figure 5)</td>
</tr>
<tr>
<td>Backup control 564</td>
<td>administration backup subscreen 650 (Figure</td>
</tr>
<tr>
<td></td>
<td>6)</td>
</tr>
<tr>
<td>Locks control 566</td>
<td>administration locks subscreen 500 (Figure 4)</td>
</tr>
<tr>
<td>Remote control 568</td>
<td>administration remote subscreen 700 (Figure 7)</td>
</tr>
</tbody>
</table>
DNS control 570 administration DNS subscreen 750 (Figure 8)

If a particular checkbutton in management locks section 540 is turned off, the administrator will have access to the corresponding screen or subscreen of configuration management interface 20. If a particular checkbutton in management locks section 540 is turned on, the administrator will be restricted from accessing the corresponding screen or subscreen. The configuration of management lock section 540 is recorded in a data file /root/MSconfig/dat/lockConfig.dat

The manager may change the management password by selecting change management password control 572, which brings up a change management password dialog box (not shown). The management password is recorded in a data file /root/MSconfig/dat/mgmtpass.dat

After setting management locks section 540 and the management password as desired, the manager may select lock/unlock system control 502, putting configuration management interface 20 in the locked state.

When an administrator puts configuration management interface 20 into the administration unlocked state and accesses the administration locks subscreen 500, management locks section 540 will not be shown; otherwise administration locks subscreen 500 will appear the same.

Administration locks section 512 comprises a set of checkbuttons that control which screens of configuration management interface 20 can be accessed when configuration management interface 20 is in a locked state:

<table>
<thead>
<tr>
<th>Control</th>
<th>Controls locked state access to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users &amp; Groups control 514</td>
<td>users &amp; groups screen 150 (Figure 10)</td>
</tr>
<tr>
<td>Filesharing control 516</td>
<td>file server screen 180 (Figure 11)</td>
</tr>
<tr>
<td>Printers control 518</td>
<td>print server screen 210 (Figure 12)</td>
</tr>
<tr>
<td>Fax control 520</td>
<td>fax server screen 240 (Figure 13) and fax routing control screen 270 (Figure 14)</td>
</tr>
<tr>
<td>Domain control 522</td>
<td>domain server screen 300 (Figure 15)</td>
</tr>
<tr>
<td>Web control 524</td>
<td>web server screen 370 (Figure 17)</td>
</tr>
<tr>
<td>FTP control 526</td>
<td>FTP server screen 340 (Figure 16)</td>
</tr>
<tr>
<td>Mail control 528</td>
<td>mail server screen 400 (Figure 18)</td>
</tr>
<tr>
<td>Firewall control 530</td>
<td>firewall screen 450 (Figure 19)</td>
</tr>
<tr>
<td>Network control 532</td>
<td>networks screen 120 (Figure 9)</td>
</tr>
</tbody>
</table>

The configuration of administration locks section 512 is also recorded in data file /root/MSconfig/dat/lockConfig.dat.

If a particular checkbutton in administration locks section 512 is turned off and the corresponding checkbutton in management locks section 540 is turned off, the corresponding screen will be available to any person when configuration management interface 20 is in a locked state. All other screens will not be available when the configuration management interface 20 is in a locked state.
The administrator may change the administration password by selecting change
administration password control 506, which brings up a change administration password
dialog box (not shown). (The manager may also change the administration password
when configuration management interface 20 is in management unlocked state.)

The administration password is recorded in data file
/root/MSconfig/dat/adminpass.dat.

After setting administration locks section 512 and the administration password as
desired, the administrator may select lock/unlock system control 502, putting
configuration management interface 20 in the locked state. Status screen 100 (Figure 3)
will then be displayed.

It is expected that in typical usage, multiserver 10 will be administered by an
administrator rather than by a manager. The manager will initially configure multiserver
10 as desired, select the screens and subscreens to which the administrator will have access
and then permit the administrator to modify the configuration of multiserver 10 on a
routine basis.

In the remainder of this disclosure, the various steps required to access various
configuration screens of configuration management interface 20 are described without
reference to the configuration of management locks section 540. It is assumed that the
administrator is permitted to access all screens of configuration management interface
20.

If the administrator selects the “Misc.” button from administration subscreen
pushbuttons 504, administration miscellaneous screen 600 (Figure 5) is displayed.
Administration miscellaneous screen 600 comprises mount/unmount CD-ROM control
602, reboot multiserver control 604, set data and time control 606, terminal control 608,
change administrator control 610, administrator name field 612, whois control 614,
domain name field 616, whois results area 618.

Mount/unmount CD-ROM control 602 will initially read “Mount CD-ROM”. If
the administrator selects mount/unmount CD-ROM control 602 and a CD-ROM has been
placed in a CD-ROM drive connected to multiserver 10, then the CD-ROM is mounted by
taking the following steps:

1. An attempt is made to mount the CD-ROM using the well known ISO 9660 CD-
   ROM standard, which is compatible with the unix and Windows platforms.
2. If step 1 fails, an attempt is made to mount the CD-ROM as a Macintosh HFS CD-
   ROM. If this succeeds, the Macintosh file information is provided to Netatalk.
3. If step 1 or step 2 succeeds, mount/unmount CD-ROM control 602 changes to
   read “Unmount CD-ROM” and the status of the CD-ROM is changed to
   “Mounted” in data file /root/MSconfig/dat/screens.dat.

This method of mounting a CD-ROM provides several advantages. First, the CD-ROM is
made available to all LAN workstations 42, including LAN workstations 42 which are
incompatible with the format of the CD-ROM. All types of workstations will be able to
access the CD-ROM as another file share volume connected to multiserver 10. Therefore, a Macintosh format CD-ROM may be read by a Windows workstation, and may be used to the extent that the contents of the CD-ROM are compatible with Windows workstation.

Second, more than one LAN user is able to simultaneously access the CD-ROM. A well-known aspect of unix based file systems is that a file is not locked simply because one user is accessing the file. It is inherent in unix that a copy of a file is served to a requesting workstation. Since the CD-ROM cannot be written to, there is no need to lock the original file to prevent other LAN users from accessing it simultaneously. Since all LAN workstations are accessing the CD-ROM through multiserver 10, a unix computer, more than one LAN workstation may access the same file on the CD-ROM simultaneously.

If mount/unmount CD-ROM control 602 is subsequently selected, the CD-ROM is unmounted, the status of the CD-ROM is changed to “Unmounted” in data file /root/MSconfig/dat/screens.dat and mount/unmount CD-ROM control 602 is changed to read “Mount CD-ROM”.

If the administrator selects reboot multiserver control 604, the multiserver 10 is rebooted by invoking the unix shutdown command, if no core change is taking place.

If set date and time control 606 is selected, a time utilities dialog box is displayed (not shown). Time utilities dialog box allows the administrator to modify the system date and time of multiserver 10. In addition, the time utilities dialog box allows the administrator to specify up to two time servers, which are used in conjunction with the well known network time protocol (ntp) utility to update the system clock on a periodic basis with data from the time servers, which are connected to multiserver 10 through the internet.

If terminal control 608 is selected, an xterminal is opened. To close the xterminal, the administrator may use the unix exit command. The administrator may use the xterminal to execute unix commands on multiserver 10.

The name of the current administrator is displayed in administrator name field 612. The administrator may be changed by selecting change administrator control 610, which brings up a dialog box (not shown) allowing the administrator to enter the name of the new administrator. The following steps are taken to change the administrator:

1. The name of the new administrator is checked to ensure that it is either the name of a current LAN user or e-mail enabled group. If it is not, an error is returned.

2. The name of the new administrator is stored in data file /root/MSconfig/dat/screens.dat.

3. Multiserver 10 is configured to forward any messages which would normally be sent to the administrator by modifying the standard unix /root/.forward file.

Whois control 614 is used to invoke the standard whois command. The administrator must first enter the domain name on which to perform the whois operation in domain name field 616. The results of the whois operation is displayed in whois results area 618.
If the administrator selects the “Backup” button from administration subscreen pushbuttons 504, administration backup subscreen 650 is displayed (Figure 6). Administration backup subscreen 650 comprises change backup settings control 652, backup configuration area 654, backup now control 656, and restore now control 658. Backup configuration area 654 displays the current backup configuration, indicating whether the file system of multiserver 10 will be backed up on each day of the week and the time at which the backup will take place on each day of the week. Backup configuration area 654 also indicates whether (1) user home directories, (2) web_server file share volume or (3) file server volumes or (4) the system files will be backed up.

The administrator may modify the backup configuration by selecting change backup settings control 652, which brings up a dialog box (not shown) allowing the administrator to modify all of the fields shown in backup configuration area 654. The backup configuration is recorded by taking the following steps:

1. Data file /root/MSconfig/dat/screens.dat is modified to reflect the backup configuration.
2. System file /etc/crontab is modified to run a backup agent (described below) on the selected days at the selected times.

In the preferred embodiment, the backup agent is a script which uses the unix tar command to backup the specified file share volumes.

The administrator may run the backup agent immediately by selecting backup now control 658.

The administrator may restore file share volumes previously backed up from a backup device such as a tape drive, if no core change is taking place. One skilled in the art will recognize that this process of restoring previously backed up files is not restricted to files which have been backed up using the backup agent. Any file backed up using the unix command tar may be restored using backup now control 658.

If the administrator selects the “Remote” button from administration subscreen pushbuttons 504, the administration remote login subscreen 700 (Figure 7) is displayed. Administration remote login subscreen 700 comprises an FTP accessibility section 702 and remote login section 710.

FTP accessibility section 702 comprises a set of three radio button controls: LAN control 704, specific control 706 and internet control 708. FTP accessibility section 702 is used to regulate FTP access to the file system of multiserver 10. Three types of users may get FTP access to the file system of multiserver 10. LAN users may get FTP access to their home directories. Virtual domain administrators may get FTP access to the directory (within the web_server file share volume) in which the public and private web sites of their respective domains are stored. FTP surfers may get access to the public anonymous FTP site of the primary domain of multiserver 10. The public anonymous FTP site of the primary domain is stored in the pftp file share volume. The actual classes of users who may access multiserver 10 by FTP is controlled on the FTP server screen 340 (described below). The locations from which these users may access multiserver 10
by FTP is controlled by the administrator’s choice of LAN control 704, specific control 706 and internet control 708:

<table>
<thead>
<tr>
<th>Selected control</th>
<th>FTP accessibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN control 704</td>
<td>FTP access is offered only to LAN workstations 42</td>
</tr>
<tr>
<td>specific control 706</td>
<td>FTP access is offered only to specified IP addresses</td>
</tr>
<tr>
<td>internet control 708</td>
<td>FTP access is offered to any IP address</td>
</tr>
</tbody>
</table>

If specific control 706 is selected, a dialog box (not shown) is opened to allow the administrator to enter IP addresses to which FTP access will be offered. In all cases, the following steps are taken when the FTP accessibility is changed:

1. The FTP accessibility selected is recorded in the FTP Accessibility field in /root/MSconfig/dat/screens.dat.
2. If “specific” FTP accessibility is selected, the specific IP addresses entered by the administrator are stored in the data file /root/MSconfig/dat/specFTP.dat.
3. The /etc/hosts.allow data file, which is part of the TCP Wrappers package is modified to correspond to the FTP accessibility configuration.

Remote login section 710 comprises no external login control 712, LAN control 714, specific control 716 and internet control 718. Remote login section 710 is used to control the accessibility of multiserver 10 by telnet. In the preferred embodiment of multiser\n
The administrator may configure the location from which a permitted LAN user may access multiser
ter 10 by telnet by selecting the appropriate control:

<table>
<thead>
<tr>
<th>Selected control</th>
<th>Telnet accessibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>no external login control 712</td>
<td>telnet access is not permitted from any IP address</td>
</tr>
<tr>
<td>LAN control 714</td>
<td>telnet access is permitted only from an IP address within the LAN</td>
</tr>
<tr>
<td>specific control 716</td>
<td>telnet access is permitted from specified IP addresses only</td>
</tr>
<tr>
<td>internet control 718</td>
<td>telnet access is permitted from any IP address</td>
</tr>
</tbody>
</table>

If specific control 716 is selected, a dialog box (not shown) is opened to allow the administrator to enter one or more specific IP addresses from which LAN users will be able to access multiser
ter 10 by telnet. In the preferred embodiment of multiser
ter 10, a LAN user who accesses multiser
ter 10 by telnet is initially connected to his or her home directory. The LAN user may have access to the remainder of the file system of multiser
ter 10, depending on the LAN user’s permissions and group membership. The following steps are taken when telnet accessibility is changed:

1. The selected telnet accessibility is recorded in /root/MSconfig/dat/screens.dat in the Remote Login field.
2. If specific telnet accessibility is selected, the specified IP addresses are recorded in data file /root/MSconfig/dat/specRemote.dat.

3. The /etc/hosts.allow data file, which is part of the TCP Wrappers package is modified to correspond to the telnet accessibility configuration.

If the administrator selects the "DNS" button from administration subscreen pushbuttons 504, administration DNS subscreen 750 (Figure 8) is displayed. Administration DNS subscreen 750 comprises DNS map section 752 and change host control 754.

The administrator may add additional hosts to any of the domains.

Each of the domains (primary domain, virtual domain, sub-domains) and hosted services (public web site, private web site, FTP server, mail server and fax server and any other configured hosts) may be configured to resolve to the computer on which multiserver 10 is installed or to another computer specified by its IP address.

DNS map section 752 shows the name of every domain, the services associated with each of them and the IP address of the computer from which the service is hosted. The only requirement in the DNS map is that the primary domain name (ntk.com in the example above) must always be hosted by the primary domain name server, indicated by PRIMARY in the DNS map.

The administrator may change the IP address from which a sub-domain, virtual domain or service is hosted by highlighting the domain or service name and then selecting change host control 754, which brings up a change host address dialog box (not shown). Change host address dialog box allows the administrator to select either the local IP address or another IP address to be the host of the selected service.

When the IP address from which a sub-domain, virtual domain or service is changed, the following steps are taken:

1. The data file /root/MSconfig/dat/dnsmain.dat is updated.
2. The configuration files for the BIND server are updated accordingly.
3. The named daemon, which is part of the BIND server is reset.

Configuring the Network

If the administrator selects the "Network" pushbutton from the configuration screen pushbuttons 104, the network screen 120 (Figure 9) is displayed. The Network screen 120 comprises an internet connection information section 122, a change internet connection control 124, a LAN connection information section 126, a change LAN connection control 128, an internet service provider (ISP) information section 130 and a change ISP authentication control 132.

The LAN connection information section 126 shows: the LAN Network IP address, which comprises an IP Number, a Subnet, a Network and a Broadcast; the type of connection used for the LAN; the name of the network interface on the multiserver 10 hardware at which the LAN is connected; and the connection policy for the LAN. If the administrator selects change LAN connection control 128, a change LAN connection
dialog box (not shown) is displayed, allowing the administrator to change the LAN Network IP address, the connection type and the network interface name. One skilled in the art will know how to select an appropriate LAN Network address for the LAN and how to select and identify the type of the LAN network connection. The LAN connection policy will always be permanent, indicating that multiserver 10 is always connected to the LAN.

Once the administrator has selected a LAN connection configuration, the configuration of the File Server, Print Server and the LAN Firewall is updated by taking the following steps:

1. Ensure that no core change is taking place. If a core change is taking place, an error is returned.
2. The Internal IP, Internal Subnet IP, Internal Network IP, Internal Broadcast IP, internal connection type and internal location fields in /root/MS config/dat/screens.dat are updated.
3. The network interface definition file for the selected network interface (for example, /etc/sysconfig/network-scripts/ifcfg-eth0, in the case of an ethernet connection on network interface eth0) is updated to reflect the selected LAN network IP address and is configured to take effect when the multiserver 10 is rebooted.
4. Sendmail configuration file /etc/mail/ip_allow is updated to permit LAN workstations 42 to relay e-mail through mail server 32, depending on the outgoing mail relay option selected on mail server screen 400 (using control 406, 408, 410 and 412).
5. TCP Wrappers configuration file /etc/hosts.allows is updated to reflect the selected LAN network IP address.
6. PAM configuration file /etc/security/access.conf is updated to reflect the selected LAN network IP address, based on the telnet accessibility selected on Administration remote subscreen 700.
7. Unix configuration file /etc/hosts is updated to reflect the new internal IP number.
8. Apache configuration file /etc/httpd/conf/httpd.conf is updated to reflect the new LAN network IP address.
9. Samba configuration file /etc/smb.conf is updated to reflect the selected LAN network IP address.
10. The BIND daemon named is reset.
11. The sendmail daemon sendmail is reset.
12. The apache daemon httpd is reset.

The internet connection information section 122 shows: whether the internet network IP address is fixed or dynamically assigned; if the internet network address is fixed, the IP Number, Subnet, Network and Broadcast comprising the internet network address; the connection type between the multiserver 10 and the internet; the physical interface on the multiserver 10 of the internet connection; the connection policy for the
internet connection; the timeout period if a dial-on-demand internet connection is used; and the gateway number, which will normally be supplied by the an internet service provider.

If the administrator selects the change internet connection control 124, a change internet connection dialog box (not shown) is displayed, allowing the administrator to enter new values for each of the values shown on the internet connection information section 122. One skilled in the art will be capable of correctly configuring the internet connection to provide the required services.

If multiserver 10 is connected to the internet by means of a dial-on-demand modem connection, when a LAN workstation 42 requests an internet-based service, an internet connection will be established and the requested service will be routed to the LAN workstation 42. When the connection has been idle for the specified time period, the connection will be disconnected.

Once the administrator has selected an internet connection configuration, the configuration of the Domain Name Server, Web Server, Mail Server, FTP Server and the Internet Firewall is updated by taking the following steps:

1. Ensure that no core change is taking place. If a core change is taking place, an error is returned.
2. The internet LAN network IP type, external IP, external subnet IP, external network IP, external broadcast IP, external connection type, external connection location, external connection policy, dial-on-demand disconnection and external gateway IP fields in /root/MSconfig/dat/screens.dat are updated.
3. The network interface definition file for the selected physical interface (for example, /etc/sysconfig/network-scripts/ifcfg-eth1, in the case of an ethernet connection on network interface eth1) is updated to reflect the selected internet network IP address and is configured to take effect when the multiserver 10 is rebooted.
4. Diald configuration file /etc/diald.conf is updated if the external connection location is a com port to reflect the external connection type. (Diald is a standard unix modem dialing utility which will be familiar to a person skilled in the art.)
5. The TCP Wrappers configuration file /etc/hosts.allow is updated to reflect the selected external IP number.
6. Unix configuration file /etc/hosts is updated to reflect the new external IP number.
7. Unix configuration file /etc/sysconfig/network is updated to reflect the new gateway number.
8. BIND configuration file /etc/named.conf is updated to reflect the new external IP number.
9. All BIND domain master files (for example, /var/named/named.DOMAINNAME) are updated to reflect the new external IP number.
10. All BIND reverse resolution files /var/named/named.rev are updated to reflect the new external IP number.

11. Diald configuration file /usr/lib/diald/standard.filter is updated to reflect the new external IP number and gateway number.

12. Diald configuration file /etc/phone.filter is updated to reflect the new timeout period.

13. Internet firewall configuration file /root/MSconfig/bin/fwINIT is updated to reflect the new external IP number.

14. The BIND daemon named is reset.

15. The sendmail daemon sendmail is reset.

16. The apache daemon httpd is reset.

When the external connection type is a serial modem, multiserver 10 will normally be connected to a remote internet service provider. Such a connection is made over a telephone line and normally requires password authentication. Password authentication may be automated, if the ISP supports Password Authentication Protocol (PAP) authentication, by entering the following information: the ISP's telephone number, an ISP user name designated by the ISP and an ISP password. The administrator may initially enter this information or subsequently modify it by selecting change ISP authentication control 132, which brings up a dialog box (not shown), allowing the administrator to enter the three pieces of data. This data is displayed in ISP information section 130. When the ISP information is changed, the following steps are taken:

1. /root/MSconfig/bin/connect is updated to reflect the ISP phone number.

2. PPP client configuration file /etc/ppp/pap-secrets/ is updated to reflect the ISP user name and ISP password. (PPP is a standard unix utility which authenticates communications between the ISP and multiserver 10.)

In the preferred embodiment of multiserver 10 certain features of the LAN and internet connection configurations are given default values.

With respect to the LAN connection, the default internal IP number is 192.168.1.1. This number is selected because it is not accessible from the internet. In the preferred embodiment, the LAN is connected using an ethernet network. The Connection type is set at "ethernet" and the connection location is set as eth0, the physical interface address of one of the ethernet cards installed in the computer on which multiserver 10 is run. In the preferred embodiment, a permanent LAN connection policy has been selected, so that the LAN is available to users at all times.

With respect to the internet connection, in the preferred embodiment domain name server 38 of multiserver 10 hosts all domains that have been added to multiserver 10. One skilled in the art will be aware that internet domain name hosting is only possible if the IP address of the physical computer on which the domain name server 38 is running is fixed. The IP Number and Subnet components of the internet network address must generally be assigned by an internet service provider. In the preferred
embodiment, an ISDN-2 connection type is used. The ISDN-2 connection is connected to multiserver 10 at an ethernet card, identified as eth1. The administrator may select other connection types, including serial modem, DSL modem, cable modem, T1 and T3. Multiserver 10 is used for hosting internet domains. Accordingly, a permanent connection policy has been selected.

Configuring LAN Services

Configuring Users and Groups

If the administrator selects the “User & Groups” button from the configuration screen pushbuttons 104, the Users and Groups screen 150 will be shown (Figure 10). Users and Groups screen 150 comprises LAN user information section 152, controls 154, 156 and 158 for respectively adding, editing or deleting a user, e-mail alias information section 160, controls 164, 166 and 168 for respectively adding, editing and deleting e-mail aliases, group information section 162 and controls 170, 172 for respectively adding and deleting groups.

Groups are used as a means to coordinate sets of LAN users that have similar requirements with respect to services provided by multiserver 10. For example, a group titled “accounting” may be created and each LAN user who is a member of the accounting department may be added to this group. As will be described below, each of these LAN users will then have access to e-mail intended for the accounting group, files stored for use by the accounting group, etc. The use of groups simplifies the use of multiserver 10 services by users and those attempting to communicate with LAN users.

Group information area 162 lists the groups which have been defined, indicating the name of the group and whether the group is permitted to receive group e-mail. If group e-mail is enabled all members of the group will receive a copy of e-mail addressed to the group. When the internet domain name hosting services have been configured (described below), the multiserver 10 may be configured to receive e-mail for LAN users at the primary domain. In this case, if a group e-mail has been enabled for the accounting group, each member of that group will receive a copy of e-mail sent to the virtual LAN user “accounting” at the primary domain (i.e. the e-mail address accounting@ntk.com).

Groups are added by selecting control 170, causing an add group dialog box (not shown) to be displayed. Using add group dialog box, the administrator can enter the name of a new group and define whether the group will be permitted to receive group e-mail. The following steps are taken to add a group:

1. Data file /root/MSconfig/dat/groups.dat is checked to ensure that the group name does not already exist. If it does, an error is returned.
2. If group e-mail is selected, then:
   (a) data file /root/MSconfig/dat/usersList.dat is checked to ensure that the group name does not already exist as a LAN user. If it does, an error is returned.
the group name is added as a restricted user account in the virtual mail group using the unix useradd command. This command will fail if this user name already exists in the unix user registry, in which case an error is returned;

c) data file /root/MSconfig/dat/grpMail/GROUPNAME.dat is created;

d) data file /home/virtualmailaccounts/GROUPNAME/.forward is created to contain the names of group members.

e) Sendmail is updated to direct mail addressed to GROUPNAME@PRIMARYDOMAIN to the restricted user added in step 2(b).

3. The new group name is added to data file /root/MSconfig/dat/groups.dat.

4. The group is added to unix group registry using the unix groupadd command.

Groups may be deleted by highlighting the target group in the group information area 162 and selecting control 172. The steps set out above are reversed to delete a group.

As described in Part One of this disclosure, certain groups are required for the various services offered by multiserver 10 to operate.

LAN user information section 152 lists the users which have been added to the system and groups of which each user is a member. Every LAN user is a member of the users group. The administrator may add a user by selecting control 154, bringing up an add user dialog box (not shown). The add user dialog box allows the administrator to define the new user’s name, password, the groups to which the user belongs and an e-mail forwarding option. Multiserver 10 provides the following e-mail forwarding options: a user’s e-mail may not be forwarded at all, or it may be forwarded to another internet e-mail address, to a fax machine (the administrator must provide a telephone number in this case), or the user’s e-mail may be processed by a custom procmail script. When any user is added to multiserver 10, the user is automatically given an e-mail address at the primary domain of multiserver 10. A new user is added to multiserver 10 by taking the following steps:

1. Data file /root/MSconfig/dat/groups.dat is checked to ensure that all of the groups entered by the administrator exist. If they do not, an error is returned. If the administrator has not selected the “users” group, it is added to the list of groups prior to this check.

2. Data file /root/MSconfig/dat/usersList.dat is checked to ensure that the user does not already exist. If it does, an error is returned.

3. Data file /root/MSconfig/aliasmail.primary is checked to ensure that the user name does not exist as an alias. If it does, an error is returned.

4. The user is added to the unix user registry using the unix useradd command with the following configuration:

(a) the directory /home/<user name> is created for use as the user’s home directory;

(b) the group “users” is the new user’s primary (or default) group;
(c) other groups entered by the administrator are added as supplementary
groups; and

(d) if the user is a member of the "admin" group, the user's shell is set to
/bin/bash, otherwise it is set to /bin/false.

5. The user's password is updated in the configuration file /etc/passwd using an
autpasswd script (described below).

6. The user's username and password are added to the Samba user registry.

7. The LAN user name is added to data file /root/MSconfig/data/userslist.dat.

8. If the user belongs to the "faxblast" group, the user's username and password
are added to a Fax CGI password file (described below).

9. Sendmail configuration file /etc/mail/virtusertable is updated by adding an e-mail
account ALIAS@PRIMARYDOMAIN linked to the LAN user name.
Configuration file /etc/mail/virtusertable is then hashed.

10. The user's e-mail forwarding is configured as follows:

(a) if the administrator has selected no forwarding option, nothing is done;

(b) if the administrator has selected forwarding to one or more e-mail
addresses, to a fax machine, or a custom e-mail forwarding option, the
files /home/USERNAME/.forward and /home/USERNAME/.procmailrc are
created or modified as required and the ownership of the .forward and
 procmailrc files is set to the new user.

11. For each e-mail enabled group to which the user belongs, the user is added to the
file
/home/virtualmail accounts/GROUPNAME/.procmailrc

12. If all LAN users have guest access to the authorized web server on the primary
domain (configured on the web server screen 370, which is described below), the
username and password of each LAN user is added to the Apache guest registry
for the primary domain.

The autopasswd script is written using the Expect programming language. The
autpasswd script communicates with the unix passwd command. The unix passwd
command is interactive and expects multiple user inputs, defining a user name and
password. The autopasswd script intercepts prompts from passwd and supplies the
appropriate response, making passwd non-interactive.

Sendmail uses a .forward file in the home directory of a user to process e-mail
sent to that user. If this .forward file is configured to run Procmail, then the e-mail is
processed by the Procmail package according to a configuration file .procmailrc, also
stored in home directory of the user.

In the preferred embodiment, e-mail received by a user may be forwarded to a
fax machine utilizing Procmail. To do this, the .procmailrc file is configured to keep a
copy of e-mail message in the incoming mail spool of the user and to use the Hylafax
faxmail program to also send the e-mail message to a specified fax telephone number.
A LAN user’s configuration may be modified by selecting control 156, which brings up a modify LAN user dialog box (not shown). Modify LAN user dialog box allows the administrator to change the LAN user’s settings. The data files created or modified when the LAN user was added are modified to reflect the new configuration.

A LAN user may be removed from the system by selecting control 158. The data files created or modified when a LAN user is added are deleted or the modifications are reversed.

The e-mail alias information section 160 lists e-mail aliases which have been created and the user that owns each alias. An e-mail alias acts like an e-mail address but is actually only an alias for an actual user of multiserver 10. For example, if an alias “finance” owned by user “andrew” has been set up on multiserver 10 which has a primary domain ntk.com, then when an e-mail message is sent to finance@ntk.com, the e-mail will be routed to andrew@ntk.com.

The administrator may add an alias by selecting control 164, bringing up an add alias dialog box (not shown), which allows the administrator to enter the alias and its owner. The alias is then added by taking the following steps:

1. Data file /root/MSconfig/aliasmail.primary is checked to ensure that the alias does not exist. If it does, an error is returned.
2. Data file /root/MSconfig/usersList.dat is checked to ensure that there is no user identical to the alias. If there is such a user, an error is returned.
3. The existence of a data file named /root/MSconfig/dat/grpMail/ALIAS.dat is checked (where ALIAS is the alias being added). If such a data file exists, then there is already an e-mail enabled group named ALIAS and an error is returned.
4. The alias is added to data file /root/MSconfig/data/aliasmail.primary.
5. Sendmail is updated by adding an e-mail account for the alias with the address ALIAS@PRIMARYDOMAIN.
6. Sendmail configuration file /etc/mail/virtusertable is updated by adding an e-mail account ALIAS@PRIMARYDOMAIN linked to the owner. Configuration file /etc/mail/virtusertable is then hashed.

Aliases are deleted by selecting control 168. The data files created or modified when an alias is added are deleted or the modifications are reversed.

**Configuring the File Server**

If the administrator selects the “File Server” button from the configuration screen pushbuttons 104, file server screen 180 will be displayed (Figure 11). File server screen 180 comprises, file server on control 182, file server off control 184, private user space control 186, file share volume information section 188 and controls 190,192 and 194 for respectively, adding, editing and deleting file share volumes.

File share volume information section 188 provides a list of all file share volumes which have been allocated on File Server 22, the name of the primary user group which
has access to each respective share, the type of access permitted by the primary group and the type of access permitted for users who are not members of the primary group.

If the administrator selects control 182, file sharing services of File Server 22 are turned on by taking the following steps:

1. Samba, Netatalk and NFS are started.
2. Samba, Netatalk and NFS initialization scripts are added to the startup sequence. This ensures that file sharing services remain on if the system is restarted.

If the administrator selects control 184, the File Server's 22 file sharing services are turned off by the following steps:

1. Samba, Netatalk and NFS are stopped.
2. Samba, Netatalk and NFS initialization scripts are removed from the startup sequence. This ensures that file sharing services remain off if the system is restarted.

If the administrator selects private user space 186, which operates as a toggle switch, each LAN user of the multiserver is either allowed or denied access to the LAN user's home directory on the multiserver file system. The administrator is permitted to access all home directories, regardless of whether the spaces are accessible to the individual LAN users. LAN users are allowed access to their home directories by modifying Samba configuration file /etc/smb.conf, Netatalk configuration file /usr/local/atalk/etc/AppleVolumes.default and NFS configuration file /etc/exports.

The same configuration files are modified to deny LAN users access to their home directories.

If the administrator selects control 190, an "Add File share volume Path" dialog box (not shown) will be displayed and will request the following information: (i) the path for the new file share volume; (ii) the group which will have primary access to the new file share volume; (iii) the type of access permitted for the primary group; and (iv) the type of access permitted for users who are not members of the primary group. A new file share volume is added to the file server 22 by taking the following steps:

1. Data file /root/MSconfig/dat/fShareList.dat is checked to ensure that the new file share volume does not exist. If it does, an error is returned.
2. The new file share volume is added to data file /root/MSconfig/dat/fSharelist.dat.
3. The directory /usr/filesharing/FILESHAREVOLUME/ is created.
4. The file share volume is added to Samba configuration file /etc/smb.conf, Netatalk configuration file /usr/local/atalk/etc/AppleVolumes.default and NFS configuration file /etc/exports.
5. NFS is instructed to re-read its configuration file /etc/exports by executing the command /usr/sbin/exportfs.

To modify or remove a file share volume, the administrator must highlight the relevant file share volume in the file share volume information section 188 and then select control 192 to edit the configuration of the file share volume or control 194 to
delete the file share volume. The operations required to edit or delete a file share volume will be apparent from the above description of adding a file share volume.

Configuring the Print Server

If the administrator selects the “Print Server” button from configuration screen pushbuttons 104, the print server screen 210 (Figure 12) will be displayed. Print server screen 210 comprises configuration screen pushbuttons 104, printer information section 212, printer add control 214, printer delete control 216, printer queue section 218, top of queue control 220 and remove print job control 222.

Printer information section 212 displays the name and type of each printer available to users for printing.

In the preferred embodiment, Macintosh LAN workstations 42 use a standard print dialog which is supplied with the MacOS operating system for all printing tasks. This dialog does not provide the user with the option of selecting all of the functions which might be available on a specific printer. For example, certain printers allow a document to be printed at one of three resolutions. The MacOS print dialog provides no way of selecting one of the three resolutions and all jobs originating from Macintosh workstations would normally be printed at the default resolution of the printer. To overcome this deficiency, when a single physical printer is added to the Print Server 24, one or more virtual printers, depending on the characteristics of the printer, may be added to Print Server 24. Each virtual printer will correspond to one specific set of options which may be selected for the physical printer. In the example here, three separate printer entries would appear in the printer list (on both Macintosh and Windows workstations). The three entries may be printerX_highres, printerX_medres and printerX_lowres.

Although Windows based workstations are generally capable of selecting the various features offered by different printers by means of specific print dialogs for different printers, this capability has been disabled in multiserver 10 and a standard print dialog has been substituted. Windows users are still able to select any combination of features by selecting the appropriate entry from the printer list. This has been done for consistency between MAC and Windows workstations but is not necessary.

The administrator adds printers to the Print Server by selecting printer add control 214, which brings up the add printer dialog box (not shown). The administrator then enters the name of the printer (chosen by the administrator), selects the type of printer from a list of printers for which a printer definition file has been pre-installed on multiserver 10, identifies the port (on multiserver 10 or one of the LAN workstations 42) the printer is connected to and whether the printer is a network printer. Once the administrator has identified the characteristics of the printer, it is added to print server 24 by taking the following steps:

1. Ensure that no core change is taking place. If a core change is taking place, an error is returned.
2. The physical printer information is added to data file /
   root/MSconfig/dat/printersList.dat.
3. A print spool is created for the printer in a directory named
   /var/spool/lpd/PRINTERNAME, where PRINTERNAME is the name of the
   physical printer. This is a consolidated spool for all of the virtual
   printers corresponding to the physical printer.
4. If the printer is a network printer, it is added to Netatalk configuration file
   /var/spool/lpd/PRINTERNAME/paprc
5. Virtual printers are added to unix configuration file /etc/printcap and Netatalk
   data file /usr/local/atalk/etc/papd.conf for each combination of features available
   on the selected physical printer. The number of virtual printers added for a
   specific physical printer will be defined in the printer definition file supplied with
   multiserver 10. The printer definition file is identified in /etc/printcap as an input
   filter used to pre-process queued files prior to being printed. Each virtual printer
   will be published to LAN workstations 42.
6. For each virtual printer, an input filter /etc/scripts/VIRTUALPRINTER is created.
   This file is used for pre-processing the postscript stream, as described below. The
   file is given permissions to make it executable by any LAN user.
7. Unix printer daemon lpd is reset. All instances of netatalk printer daemon papd
   are killed and new instance of papd is started.
   An entry may be removed from the list of printers in the printer information
   section 212 by selecting the entry and selecting printer delete control 216. The steps
   listed above will be reversed to remove the printer.
   Printer queue section 218 displays a list of print jobs currently being printed or
   queued for printing at any of the physical printers listed in printer information section
   212. To display the queue for a specific physical printer, the administrator highlights the
   printer in printer information section 212. The administrator may review the list of
   queued print jobs and may highlight any entry in the list. Selecting the top of queue
   control 220 moves the highlight to the first entry in the list. Selecting the remove print
   job control 222 removes the highlighted entry from the list, causing that print job to
   either not be printed, or if it has already been started, to be terminated without being
   completed. The queue management operations required to implement this functionality
   will be well known to a person skilled in the art.
   To ensure that any document may be printed at any printer which has been
   added to Print Server 24, Print Server 24 has been configured such that all printers,
   regardless of each printer's built-in capabilities, appears to each LAN workstation 42 as a
   postscript-2 compatible printer. This is accomplished by using a postscript-2 compatible
   printer driver for all printing operations at LAN workstations. In the preferred
   embodiment, Macintosh workstations always use Macintosh Laserwriter print dialog and
   Windows workstations always use a stock postscript-2 compatible printer driver regardless
   of the printer they choose for printing. The output of these printer drivers is a postscript
file which represents the printed document. This postscript file is queued to be printed at
the specified printer. When the document reaches the top of the print queue for the
printer, it is processed using the printer definition file for that printer.

Printer definition files can be divided into two groups. Printer definition files for
postscript compatible printers simply do nothing. No input filtering is done, and the
queued postscript print file is routed to the port at which the printer is connected by the
unix lpd daemon.

Printer definition files for non-postscript printers pre-process queued postscript
print files by taking the following steps to print a file:

1. If the postscript print file was created from a Macintosh workstation and if the
document is to be printed in landscape format, then a postscript command
(rotate) is added to the postscript stream to rotate the page in a standard fashion.
This step is required to standardize the commands used by Macintosh and
Windows print drivers when specifying landscape orientation.

2. The postscript stream produced in step (1) is routed into Ghostscript with the
appropriate Ghostscript printer driver for the selected printer.

Configuring the Fax Server

The fax server 34 of multiserver 10 provides both incoming and outgoing fax
services for users of the multiserver 10. Users must be members of the faxblast group in
order to send a fax.

If the administrator selects the “Fax Server” button from configuration screen
pushbuttons 104, a fax server screen 240 (Figure 13) is displayed. Fax server screen 240
comprises fax server on control 242, fax server off control 244, modem information
section 246, display modems and outgoing faxes control 248, display incoming fax
routing control 250, add modem control 252, edit modem control 254, delete modem
control 256, outgoing fax queue section 258, delete fax job control 260 and delete all
fax jobs control 262.

If the administrator selects fax server on control 242, the fax server 34 is enabled
by taking the following steps:

1. The Hylafax central queueing agent faxq is started.
2. The Hylafax central queueing agent faxq is added to the startup sequence to
ensure that fax server 34 continues to run when multiserver 10 is restarted.

If the administrator selects fax server off control 244, the fax server is disabled by
taking the following steps:

1. The Hylafax central queueing agent faxq is stopped.
2. The Hylafax central queueing agent faxq is removed from the startup sequence
to ensure that fax server 34 does not run when multiserver 10 is restarted.

Modem information section 246 shows the status of modems connected to the
multiserver 10 for faxing purposes. The station ID, telephone number, the physical port
on which the modem is connected and the current status of the modem. The status will
indicate whether the modem is operational and whether it is presently sending a fax, receiving a fax or idle. Each modem connected to the multiserver must be connected to a separate telephone line.

The administrator adds modems to the fax server 34 by selecting add modem control 252, which brings up an add modem dialog box (not shown). The administrator enters the station ID of the modem, the telephone number of the phone line to which the modem is connected, the physical port to which the modem is connected and identifies whether the specific modem will be capable of receiving faxes as well as sending them. Once the administrator has entered this information, the modem is added to the fax server 34 by taking the following steps:

1. Ensure that no core change is taking place. If a core change is taking place, an error is returned.

2. A Hylafax configuration file is created for the new modem.

3. The modem is assigned a reference code. In the preferred embodiment, a sequential two character reference code is used starting with FA, FB, FC, .... A record is added for the new modem in data file /var/spool/fax/modems.dat

4. The modem data is added to data file /root/MSconfig/data/modems.dat.

5. A new modem entry is added to unix startup configuration file /etc/inittab.

6. The Hylafax central queueing agent faxq is reset (if it is running).

Edit modem control 254 and delete modem control 256 respectively allow the administrator to edit the configuration of a modem or to remove it from the fax server altogether. These commands respectively edit the data or files created above, or remove them.

Outgoing fax queue section 258 displays a list of all faxes which are queued to be sent, showing the name of the sender (Owner ID), the destination of the fax, the number of pages which have been sent and the number of attempts that have been made to send the fax. There is only one queue for all modems. Faxes are added to this queue by a fax scanner described in Part Three of this disclosure. Hylafax is configured to operate on a fax rollover basis. If more than one modem is connected to fax server 34, and more than one fax request is queued in the outgoing fax queue, fax server 34 will use the next available idle modem for sending the next queued fax, if any modem is idle, until all fax jobs have been completed.

If the administrator highlights a specific fax job in the outgoing fax queue section and selects delete fax job control 260, the fax job will be removed from the outgoing fax queue using the Hylafax faxrm command. If the administrator selects delete all fax jobs control 262, all fax jobs will be removed from the outgoing fax queue by deleting and recreating the following Hylafax queues: doneq, docq, sendq and recvq. The recreated queues will be empty, effectively deleting any outstanding fax jobs.

If the administrator selects incoming fax routing control 250, a fax routing control screen 270 (Figure 14) is displayed. Fax routing control screen 270 comprises fax server on control 242, fax server off control 244, display modems and outgoing
faxes control 248, display incoming fax routing control 250, incoming fax routing section 272, add auto-delivery control 278, edit auto-delivery control 280, delete auto delivery control 282, undeliverable fax routing section 284, change undeliverable fax delivery control 286, undeliverable fax addressee field 287 and infax file share volume control 288.

When a fax is received, the station ID of the sending fax machine is normally communicated to the receiving fax machine prior to the actual communication of the data representing the faxed pages. It is desirable when a fax intended for a specific person is received to automatically route the fax to that person. To facilitate convenient delivery of these faxes to the specific person for whom they are intended, the administrator may create an auto-delivery rule, which correlates an incoming fax station ID with the e-mail address of the person for whom the fax is intended.

Incoming fax routing section 272 displays auto-delivery rules which have previously been configured. The incoming fax station ID and correlated e-mail accounts are listed.

The administrator may add an auto-delivery rule by selecting add auto-delivery control 278, which brings up an add auto-delivery rule dialog box (not shown). Add auto-delivery rule dialog box also allows the administrator to configure all faxes delivered according to the auto-delivery rule to be stored in the infax file share volume.

Once the administrator enters the station ID and e-mail address, the auto-delivery rule is added to fax server 34 by taking the following steps:

1. The auto-delivery rule is added to data file /root/MSconfig/dat/inFaxIDs.dat.
2. The auto-delivery rule is added to the Hylafax program file /var/spool/fax/etc/delivery, which is used by the faxrecd program.

Edit auto-delivery control 280 and delete auto-delivery control 282 allow the administrator to edit and delete auto-delivery rules. This is done by editing or removing the data added to the two files listed above.

Undeliverable fax routing section 284 displays an e-mail address or addresses to which all faxes are sent if they are not otherwise delivered according to an auto-delivery rule. The administrator may change these e-mail addresses by selecting change undeliverable fax delivery control 286, which brings up a set undeliverable fax address dialog box (not shown), which allows the administrator to set one or more e-mail addresses for undeliverable mail. When the administrator has done so, the following step is taken:

1. The e-mail addresses are added to data file /root/MSconfig/dat/inFaxRcvrs.dat.
2. The e-mail addresses are added to the Hylafax program file /var/spool/fax/etc/delivery, which is used by the faxrecd program.

The e-mail address(es) set by the administrator are displayed in undeliverable e-mail addressee field 287.
The administrator may configure fax server 34 to put a copy of all faxes which are not delivered in accordance with an auto-delivery rule in the infax file share volume by selecting infax file share volume control 288.

When second fax routing control screen 270 is displayed, the administrator may return to fax server screen 240 by selecting display modems and outgoing faxes control 248.

Configuring Internet Hosting Services

The internet hosting services of multiserver 10 allow the administrator to operate a web site using the web server 26, an FTP site using the FTP server 28, a telnet site using telnet server 30 and internet mail services using mail server 32. Mail server 32 also provides local mail services to LAN users.

Configuring the Domain Name Server

If the administrator selects the "Domain Server" button from configuration screen pushbuttons 104, domain server screen 300 is displayed (Figure 15). Domain server screen 300 comprises primary domain information section 302, change primary domain control 304, virtual domain information section 306, add virtual domain control 308, edit virtual domain control 310 and delete virtual domain control 312.

When the administrator enters the configuration data for the primary domain, two web sites are actually created in the web_server file share volume (/home/httpd). The first is a public web site, which allows the administrator to provide information to present and prospective clients, etc. The second is a private web site which is only accessible to guests given access by the administrator. Each of these web sites is stored in a directory within the web_server file share volume (/home/httpd).

In addition to the primary domain, the web server 34 can host a multiplicity of virtual domains. Each of these virtual domains also receives a public and a private web site, which are also stored in the web_server file share volume.

Primary domain information section 302 shows the domain name of the primary domain to be hosted by web server 34, the server name of the public and private web sites on the primary domain, the name assigned to the multiserver computer (the name by which the multiserver computer is identified by LAN workstations), the server names of the FTP and mail servers on the primary domain and the names of primary and secondary name servers for the primary domain. Primary domain information section 302 also shows the IP address of the secondary name server. This field will show "N/A" unless the secondary name server is located on a computer other than multiserver 10. In that case, this field will show the IP address or URL of that computer.

A default server name of "mspro" and a default primary domain, called "localdomain", with a private web server "auth", a public server "www", FTP server name "FTP", mail server name "mail" are defined when the software for multiserver 10 is first installed on the multiserver computer.
The administrator may change the primary domain configuration 36 by selecting
change primary domain control 304, which brings up a change primary domain dialog
box (not shown), allowing the administrator to enter new values for each element of the
primary domain configuration shown in primary domain information section 302. When
the administrator has entered the configuration of the primary domain, domain name
server 38 is configured by taking the following steps:

1. Ensure that a core change is not taking place. If a core change is taking place, an
   error is returned.

2. Data file /root/MSconfig/dat/domainList.dat is checked to ensure that the specified
   primary domain name is not already used as a sub-domain or virtual domain
   name. If it is an error is returned.

3. Data file /root/MSconfig/dat/domainList.dat is checked to ensure that there are no
   sub-domains defined on the primary domain. If there are any such sub-domains,
   an error is returned.

4. BIND master domain files for the primary domain are moved to a backup
directory.

5. The primary domain server section of data file /root/MSconfig/dat/screens.dat is
   updated. If no secondary name server is specified for the primary domain, then
   the primary name server is used for the unspecified field(s).

6. TCP Wrappers data file /etc/hosts is updated to reflect the primary domain name
   and name of the multiserver computer.

7. Unix configuration file /etc/sysconfig/network is updated to reflect the primary
   domain name and the name of the multiserver computer.

8. BIND configuration files /etc/named.conf, /var/named/named.PRIMARYDOMAIN
   and /var/named/named.rev are updated to reflect the new primary domain
   configuration.

9. Data file /root/MSconfig/data/dnsmap.dat is updated to reflect the new primary
   domain name.

10. Apache configuration /etc/httpd/conf/httpd.conf is updated to reflect the new
    primary domain configuration.

11. Samba configuration file /etc/smb.conf is updated to reflect the new primary
    domain configuration.

12. Sendmail configuration file /etc/mail/sendmail.cf is updated to reflect the new
    primary domain configuration.

13. BIND daemon named is reset.

14. Sendmail daemon sendmail is reset.

15. Apache daemon httpd is reset.

16. Sendmail configuration file /etc/mail/virtusertable is updated to map e-mail
    addresses for LAN users, primary domain aliases and primary domain groups to
    the proper LAN users. Configuration file /etc/mail/virtusertable is then hashed.
17. The configuration file (/etc/webalizer.conf) for Webalizer (described below) is created.

Virtual domain information section 306 lists the virtual domains which have been added to domain name server 38. The entry for each virtual domain indicates the name of the public web server and the private web server for that domain. It also lists a reference for the virtual domain, which is explained below. All virtual domains share their domain name services with the primary domain.

The administrator may add a virtual domain by selecting add virtual domain control 308, which brings up an add virtual domain dialog box (not shown). The add virtual domain dialog box allows the administrator to enter the virtual domain name and names for the public and private web servers on the virtual domain. The virtual domain is then added as follows:

1. Ensure that no core change is taking place. If a core change is taking place, an error is returned.

2. Data file /root/MSconfig/data/mailist.dat is checked to ensure that the virtual domain name is not in the blocked e-mail list. If it is, an error is returned.

3. The existence of a file named /root/MSconfig/vDomains/VIRTUALDOMAINNAME.guests is checked. If this file exists, then the virtual domain already exists and an error is returned.

4. Data file /root/MSconfig/dat/vDomRefCounter is used to determine the virtual domain reference. (The existing reference in /root/MSconfig/bin/refCounter is incremented and the result is used as the reference for the new virtual domain.)

5. Data files /root/MSconfig/dat/domainLists.dat and /home/httpd/legend.txt are updated by adding a record for the new virtual domain.

6. Data /root/MSconfig/vDomains/DOMAINNAME.guests is created.

7. Directories with the paths /home/httpd/VIRTUALDOMAINREFERENCE/public and /home/httpd/VIRTUALDOMAINREFERENCE/private are created in the web_server file share volume to contain, respectively, the public and private web sites of the virtual domain. The ownership of these directories is set to user nobody. The group of the directories is set to the web group. The permissions of these directories are changed to allow user nobody and the web group to read, write and execute the contents of the directories. Others are permitted to read and execute the contents of the directories.

8. Default public and private web sites are created for the virtual domain.

9. Data file /root/MSconfig/dat/aliasmail.VIRTUALDOMAINNAME is created to contain the e-mail accounts and aliases for the virtual domain.

10. Data file /home/httpd/users.VIRTUALDOMAINNAME is created to contain the names and encrypted passwords of guests of the private web site of the virtual domain.

11. BIND configuration file /etc/named.conf is updated.

12. BIND configuration file /var/named/named.VIRTUALDOMAIN is created.
13. Data file /root/MSconfig/dnsmap.dat is updated with entries for the virtual
domain, the public and private web sites and the mail server of the virtual domain.
14. Apache configuration file /home/httpd.conf is created.
15. The virtual domain and its mail server are added to Sendmail configuration file
/etc/mail/sendmail.cf.
5
LAN users of the multiserver 10 who are members of the "web" group have
access to the web_server public and private folders, allowing them to add and remove
files from the public and private web servers of all virtual domains.

As described above, the directories containing the private and public web sites are
owned by a user named nobody. Standard unix systems, including the
operating system of multiserver 10 are configured with an unprivileged user named
nobody when the unix operating system is installed. This unprivileged user may only
access portions of the file system of the multiserver computer which are owned by user
nobody. This user is used in the preferred embodiment to permit web surfers to access
web sites on multiserver 10 while reducing the possibility of a malicious web surfer
damaging multiserver 10.

During operation of multiserver 10, a single parent instance of the Apache httpd
daemon is run. This instance awaits requests from web surfers and guests for access to
web sites stored on the multiserver computer. When a request is received, the parent httpd
daemon spawns a child instance of httpd. This child runs as the user nobody, allowing
the spawned httpd instance to access the requested web site without allowing any access to
the rest of the file system of multiserver computer. If for any reason, the httpd instance
crashes and returns to a command line prompt, the web surfer or guest using the crashed
httpd instance will be able to execute only those commands allowed to user nobody. As
a result, the web surfer or guest will not be able to access any part of the file system other
than web site he was previously accessing.

The administrator may edit or delete a virtual domain by selecting edit virtual
domain control 310 or delete virtual domain control 312.

Configuring the FTP Server
If the administrator selects the "FTP Server" button from configuration screen
pushbuttons 104, FTP server screen 340 (Figure 16) is displayed. FTP server screen 340
allows the administrator to control access to the public anonymous FTP server on the
primary domain (which is stored in the pftp file share volume). FTP server screen
comprises FTP server on control 342, FTP server off control 344, public access control
section 346 and private access control section 356.

As described above in relation to domain server screen 300, the locations from
which the LAN user, FTP surfers and virtual domain administrators may access the file
system of multiserver 10 are controlled using FTP accessibility section 707 of remote
login subscreen 700 (Figure 7). The name of the FTP server of the primary domain is
configured using change primary domain control 304 (Figure 15).
Public access control section 346 further comprises no access control 348, read only access control 350, read & write access control 352 and write only access control 354. Private access control area 356 further comprises no access control 358 and read & write access control 360.

If the administrator selects FTP server on control 342, the FTP server is turned on by taking the following steps:

1. The FTP server record is updated in data file /root/MSconfig/dat/screens.dat.
2. Unix configuration file /etc/inetd.conf is updated to indicate that WU-FTPD FTP daemon ftpd is to be run.
3. Unix daemon inetd is reset, causing the daemon to read its revised configuration file and start WU-FTPD FTP daemon ftpd.

The FTP server on the primary domain is turned off by selecting FTP server off control 344. The following steps are taken:

1. The FTP server record is updated in data file /root/MSconfig/dat/screens.dat.
2. Unix configuration file /etc/inetd.conf is updated to indicate that WU-FTPD FTP daemon ftpd is not to be run.
3. Unix daemon inetd is reset, causing the daemon to read its revised configuration file and stop WU-FTPD FTP daemon ftpd.

The FTP site of the primary domain is stored in the pftp file share volume. In the preferred embodiment, the pftp file share volume has the path /home/FTP/pub/. This file share volume is created when multiserver 10 is initially configured and has no owner and its access permissions are set to disable any user from accessing.

Public access control section 346 allows the administrator to control access to the FTP site of primary domain by FTP surfers. When this is done, the access permissions of the pftp file share volume are changed to reflect the new configuration.

The administrator may select four levels of access:

<table>
<thead>
<tr>
<th>Control</th>
<th>Access level granted to FTP surfers</th>
</tr>
</thead>
<tbody>
<tr>
<td>no access control 348</td>
<td>no access</td>
</tr>
<tr>
<td>read only access control 350</td>
<td>read only</td>
</tr>
<tr>
<td>read &amp; write access control 352</td>
<td>read &amp; write</td>
</tr>
<tr>
<td>write only access control 354</td>
<td>write only</td>
</tr>
</tbody>
</table>

When the administrator selects a public access level, the following steps are taken to affect the selected configuration:

1. The FTP Public Section Setting record in /root/MSconfig/dat/screens.dat is updated.
2. The unix access permission of the pftp file share volume is set as follows:

<table>
<thead>
<tr>
<th>Access level selected</th>
<th>Access permission of pftp file share volume</th>
</tr>
</thead>
<tbody>
<tr>
<td>no access</td>
<td>user, group and other permission are set to none</td>
</tr>
<tr>
<td>read only</td>
<td>user, group and other permissions are set to read and execute (rx)</td>
</tr>
</tbody>
</table>
read & write user, group and other permissions are set to read, write and execute (rwx)
write only user, group and other permissions are set to write and execute (wx)

3. If the selected access level is "no access", then WU-FTPD configuration file /etc/ftpaccess is modified to refuse any FTP connection for FTP surfer. Otherwise, /etc/ftpaccess is modified to allow an FTP connection for an FTP surfer.

Private access control area 356 allows the administrator to control authorized access by authorized FTP users (LAN users and virtual domain administrators) to the file system of the multiserver computer. Each of these users has a specified portion of the file system multiserver 10 which they may access by FTP. In the case of LAN users, this specified area is the LAN user's home directory. In the case of virtual domain administrators, this specified area is the directory within the web-server file share volume in which the public and private web sites of the virtual domain are stored. Authorized access is access which requires the user to provide a password in order to access a designated part of the file system of the multiserver computer. Authorized access may be granted on two levels: "no access" prevents these users from accessing their specified portions of the file system; and "read & write" access allows authorized users to read, download from and write to the specified portions of the FTP server.

The administrator may configure multiserver 10 for no authorized FTP access by selecting no access control 358. The following steps are taken to configure no authorized FTP access:

1. The FTP Authorized Section setting in data file /root/MSconfig/dat/screens.dat is updated.

2. WU-FTPD configuration file /etc/ftpaccess is configured to deny all access to authorized FTP users.

The administrator may configure multiserver 10 for read & write access by selecting read & write access control 360. The following steps are taken to configure authorized FTP access:

1. The FTP Authorized Section setting in data file /root/MSconfig/dat/screens.dat is updated.

2. WU-FTPD configuration file /etc/ftpaccess is configured to permit authorized FTP users read and write access to their respective specified parts of the file systems of the multiserver computer.

Configuring the Web Server

If the administrator selects the "Web Server" button from configuration screen pushbuttons 104, the web server screen 370 (Figure 17) is displayed. Web server screen 370 allows the administrator to control the operation of the web server 26. Web server screen 370 comprises web server on control 372, web server off control 374, primary
domain private server access control 376, domain list section 378, guest information section 380, add guest control 382 and delete guest control 384.

The administrator may enable the operation of web server 26 by selecting web server on control 372. The following steps are taken to turn the web server on:

1. Apache daemon httpd is started.
2. Apache daemon httpd is added to the startup sequence to ensure that web server 26 continues to run when multiserver 10 is reset.

The administrator may disable the operation of web server 26 by selecting web server off control 374. This is accomplished by reversing the steps described above.

As described above, the primary domain and each virtual domain configured using domain name server 38 has two web sites, a public web site accessible to web surfers and a private web site accessible only to guests of the domain.

A list of all the domains configured using domain name server 38 is displayed in domain list section 378. The primary domain is listed first, followed by the sub-domains and virtual domains. When the administrator highlights a domain name in domain list section 378, a list of guests for that domain is displayed in guest information section 380. In Figure 18, guests of the domain ms.ntk.com are shown in guest information section 380.

The administrator may add a guest to a domain when that domain is highlighted in domain list section 378 by selecting add guest control 382, which brings up an add guest dialog box (not shown). The add guest dialog box allows the administrator to enter the name and password of the new guest. If the guest is being added to the primary domain, the following steps are taken:

1. If LAN users have been given guest access to the private web site of the primary domain (described below), data file /root/MSconfig/data/usersList.dat is checked to ensure that the guest name is not identical to a LAN user. If it is, an error is returned.
2. A new record is created for the guest in data file /root/MSconfig/vDomains/primary.domain.
3. The guest is added to the Apache guest registry for the private web site of the primary domain using an htautopasswd script.

The htautopasswd script is written using the Expect program. The htautopasswd script communicates with the Apache hpasswd command. The Apache hpasswd command is interactive and expects multiple user inputs, defining a guest name and password. The htautopasswd script intercepts prompts from hpasswd and supplies the appropriate response, making hpasswd non-interactive.

If the guest is being added to a sub-domain or virtual domain, the following steps are taken:

1. A new record is created for the guest in data file /root/MSconfig/vDomains/VIRTUALDOMAIN.guests, where VIRTUALDOMAIN represents the name of a virtual or sub-domain.
2. The guest is added to the Apache guest registry for the private web site of the virtual domain using an hhtautopasswd script. The hhtautopasswd script is identical to the hhtautopasswdp script described above, except that it is used to add guests to the sub-domains and virtual domains rather than the primary domain.

The administrator may remove a guest from a domain by selecting delete guest control 384. The guest is then removed from the appropriate data file mentioned above and from the Apache guest registry for the appropriate domain.

The administrator may allow LAN users to have guest access to the private web server of the primary domain by selecting primary domain private server access control 376, which acts as a toggle control. If primary domain private server access control 376 is selected to allow LAN users to access the private web site of the primary domain, the following steps are taken:

1. The /root/MSconfig/vDomains/primary.guests is checked to ensure that no LAN user and no guest of the primary domain have the same name. If any of them do, an error indicating the common name is returned.

2. Each LAN user is added to the Apache guest registry for the private web site of the primary domain using the hhtautopasswd script described above.

If primary domain private server access control 376 is selected again, the above steps are reversed, disallowing LAN users from accessing the private web site of the primary domain.

As noted above, web server 26 is implemented using the Apache package. The Apache web server generates standard NCSA format logs which record hits on web sites as they occur. In the preferred embodiment, a log file is created for both web sites on all domains hosted by multiserver 10.

Webalizer is a software package available under the GNU license. It is used in the preferred embodiment of multiserver 10 to convert the raw Apache log files into useable graphic management reports in html format. Webalizer is run every hour using the unix cron utility. The reports for both the public and private web sites of each domain are then stored in the private web site of the domain, where they are accessible to guests of the private web site of the domain.

Configuring the Mail Server

If the administrator selects the “mail server” button from configuration screen pushbuttons 104, mail server screen 400 (Figure 18) is displayed. Mail server screen 400 allows the administrator to control the use of internet e-mail by users of the primary and virtual domains. Mail server screen 400 also allows the administrator to create and edit e-mail accounts and aliases on virtual domains. E-mail accounts and aliases on the primary domain are added using the Users and Groups screen 150 (Figure 10).

Mail server screen 400 comprises authenticated IP address relay control 402, relay no outgoing mail control 406, relay LAN outgoing mail control 408, relay specific
outgoing mail control 410, relay internet outgoing mail control 412, virtual domain list
section 414, add virtual domain administrator control 416, edit virtual domain
administrator control 418, delete virtual domain administrator control 420, virtual
domain e-mail account section 422, add virtual domain e-mail account control 424, add
virtual domain e-mail alias control 426, edit e-mail alias/account control 428, delete e-
mail alias/account control 430, blocked mail list section 432, add blocked mail address
control 434 and delete blocked mail address control 436.

In order for a user of multiserver 10 to send outgoing e-mail through the
multiserver computer, mail server 32 must be configured to relay mail originating from
the IP address of the workstation or other computer being used by the user.

The administrator may select one of four mail relay settings: None, LAN, Specific
or Internet. When the None relay setting is chosen, by selecting relay no outgoing mail
control 406, no LAN user or virtual domain e-mail account user may send internet e-
mail. The None relay setting is configured by taking the following steps:

1. Ensure that no core change is taking place. If a core change is taking place, an
   error is returned.
2. The Outgoing Mail Relay record in data file /root/MSconfig/dat/screens.dat is
   updated.
3. Sendmail configuration file /etc/mail/ip_allow is configured to not allow e-mail to
   be relayed from any IP address.

When the LAN relay setting is chosen, by selecting relay LAN outgoing mail
control 408, mail server 32 will relay mail which originates from inside the LAN firewall
(i.e. from a LAN workstation 42, including mail sent by a LAN user (who must be in the
admin group) connected via modem to the multiserver computer). The LAN relay
setting is configured by taking the following steps:

1. Ensure that no core change is taking place. If a core change is taking place, an
   error is returned.
2. The Outgoing Mail Relay record in data file /root/MSconfig/dat/screens.dat is
   updated.
3. Sendmail configuration file /etc/mail/ip_allow is configured to allow e-mail to be
   relayed from the IP address of the LAN workstations 42 (this is a range of IP
   addresses which is determined by the first three parts of the IP address of the
   LAN recorded in the Internal IP record in data file
   /root/MSconfig/dat/screens.dat).

When the relay specific outgoing mail option is selected, mail server 32 will relay
mail which originates from any one of a specified group of IP numbers or subnets.
When the administrator chooses this option, by selecting relay specific outgoing mail
control 410, a define mail relay IP address dialog box is displayed (not shown) allowing
the administrator to enter one or more IP numbers or subnet from which internet e-mail
may originate. If the administrator would like e-mail originating from a LAN
workstation 42 to be relayed, the IP address range of the LAN must be specifically
entered using this dialog box. When the administrator has entered all of the desired subnet IP addresses, the relay specific outgoing mail option is configured by taking the following steps:

1. Ensure that no core change is taking place. If a core change is taking place, an error is returned.

2. The Outgoing Mail Relay record in data file /root/MSconfig/dat/screens.dat is updated.

3. Sendmail configuration file /etc/mail/ip_allow is configured to allow e-mail to be relayed only from IP addresses selected by the administrator.

When the relay internet outgoing mail option is chosen, by selecting relay internet outgoing mail control 412, the mail server 32 will relay internet e-mail which originates from any IP address. This option is configured by taking the following steps:

1. Ensure that no core change is taking place. If a core change is taking place, an error is returned.

2. The Outgoing Mail Relay record in data file /root/MSconfig/dat/screens.dat is updated.

3. Sendmail configuration file /etc/mail/ip_allow is configured to allow e-mail to be relayed only from any internet IP address.

It is desirable to permit LAN users and virtual domain e-mail account users to use the incoming and outgoing mail services of their respective domains from remote locations. For example, it is desirable to allow a LAN user to access his e-mail account from a remote internet location while he is away from his office. The LAN user will be able to access his incoming mail from the remote location by configuring the mail browser at the remote location such that the designated incoming mail server is the name of the primary domain (or a sub-domain or virtual domain in the case of a virtual domain e-mail account user), regardless of how mail server 32 is configured. However, the LAN user will only be able to send e-mail from the outgoing mail server of the primary domain if relay internet outgoing mail control 412 is selected. This solution allows any internet user to relay e-mail using mail server 32 without the knowledge or consent of the administrator. This allows unknown and unauthorized users to use relay mail using mail server 32.

Mail server 32 implements a more balanced solution to this problem. Every attempt to access Sendmail is recorded in Sendmail data file /var/mail/maillog. When a LAN user (or virtual domain e-mail account user) attempts to access the incoming mail server of his domain, he must enter his user name and password. If the user name and password are valid, Sendmail will record the internet IP address of the LAN workstation 42 or remote internet location from which the access is made, the user name, the protocol with which the access was made (for example, imap, pop2, pop3, etc.) and the date and time of the access. The IP address from which the access was made is defined as an authorized IP address, if the access was made in the preceding 15 minutes.
Authenticated IP address relay control 402 is a toggle control. If it is selected to be on, the unix cron utility is configured to run a script named /root/MSconfig/bin/passIP (the passIP script), every minute. The passIP script takes the following steps to allow e-mail originating from an authenticated IP address to be relayed through mail server 32:

1. If another instance of passIP is running, then passIP script exits.
2. For every entry in /var/mail/maillog which meets the following criteria, the IP address is deemed to be an authenticated IP address:
   (i) access was validated with a valid user name (of a LAN user or virtual domain e-mail account user) and the corresponding password, and thus Sendmail added the information described above to /var/mail/maillog
   (ii) access was validated within the preceding 15 minutes
3. The contents of Sendmail data file /etc/mail/popauth are deleted and replaced with a list of the authenticated IP addresses.
4. Sendmail data file /etc/mail/popauth is hashed.

Sendmail will relay mail from IP addresses which are listed in the hashed version of data file /etc/mail/popauth.

Virtual domain list section 414 shows a list of virtual domains hosted by multiserver 10. Each virtual domain may have a virtual domain administrator. In addition to receiving an e-mail account which is provided to other users of the virtual domain, the virtual domain administrator is permitted to use her or her account to connect to the domain via FTP and may upload web pages to the public and private web sites of his or her domain remotely.

The administrator may add a virtual domain administrator for a virtual domain by highlighting the virtual domain and selecting add virtual domain administrator control 416, which brings up an add virtual domain administrator dialog box (not shown). The add virtual domain administrator dialog box allows the administrator to configure the account name of the virtual domain administrator, the virtual domain administrator’s password, an e-mail forwarding option which can forward the virtual domain administrator’s e-mail to another e-mail account, to a fax machine, by a custom script or not at all. Once the administrator has entered this information, the virtual domain administrator is added by taking the following steps:

1. The existence of data file /root/MSconfig/dat/siteAdmin/VIRTUALDOMAIN. If this file exists, a virtual domain administrator already exists for the virtual domain and an error is returned.
2. Data file /root/MSconfig/dat/aliasmail.VIRTUALDOMAIN is checked to ensure that there is no e-mail account name identical to the virtual domain administrator’s name, in that specific virtual domain. If there is, an error is returned.
3. The virtual domain administrator’s name is added to the unix user registry with the primary (or default) group of web, a supplementary group of vadmin and with the home directory /home/httpd/DOMAINREFERENCE, where the
DOMAINREFERENCE is the domain reference assigned to the domain when it is created using domain server screen 300. If this fails, an error is returned. The directory /home/httpd/DOMAINREFERENCE is the directory in which the files for the public and private web sites of the virtual domain are stored.

4. The autopasswd script is used to add the virtual domain administrator’s password in the unix configuration file /etc/passwd.

5. WU-FTPD configuration file /etc/ftpaccess is updated to allow the virtual domain administrator to have FTP access to his home directory. This directory is configured to be the root directory for the virtual domain administrator, to ensure that the virtual domain administrator cannot access any other part of the multiserver computer’s file system.

6. Sendmail configuration file /etc/mail/virtusertable is updated by adding an e-mail account VIRTUALDOMAINADMINISTRATOR@VIRTUALDOMAIN linked to the virtual domain administrator’s name. Configuration file /etc/mail/virtusertable is then hashed.

7. Data file /root/MSconfig/dat/siteAdmin/VIRTUALDOMAIN is created and the virtual domain administrator’s name and password are added to it.

8. The virtual domain administrator’s e-mail forwarding is configured as follows:
   (a) if the administrator has selected no forwarding option, nothing is done;
   (b) if the administrator has selected forwarding to one or more e-mail addresses, to a fax machine, or a custom e-mail forwarding option, the files /home/httpd/DOMAINREFERENCE.forward and /home/httpd/DOMAINREFERENCE.procmailrc are created or modified as required and the ownership of the .forward and .procmailrc files is set to the virtual domain administrator.

A virtual domain administrator’s configuration may be modified or deleted by selecting edit virtual domain administrator control 418 or delete virtual domain administrator control 420, respectively. When a virtual domain administrator is deleted, the corresponding /root/MSconfig/dat/siteAdmin/VIRTUALDOMAIN file is deleted.

Virtual domain e-mail account section 422 lists e-mail accounts and aliases which have been created for the virtual domain which is highlighted by the administrator in virtual domain list section 414. If an administrator has been defined for the virtual domain, the virtual domain administrator’s account name is listed first in the list of e-mail accounts and aliases prefixed with an asterisk (*).

The administrator may add an e-mail account for the highlighted virtual domain by selecting add virtual domain e-mail account control 424, which brings up an add virtual domain e-mail account dialog box (not shown). The add virtual domain e-mail account dialog box allows the administrator to enter an account name, password and select an e-mail forwarding option. Once the administrator has entered this information, the new virtual domain e-mail account is added by taking the following steps:
1. Data file /root/MSconfig/dat/aliasmail.VIRTUALDOMAIN is checked to ensure that there is no existing e-mail account name or alias identical to the new e-mail account name, in the virtual domain. If there is, an error is returned.

2. The new e-mail account name is added to the unix user registry with the primary (or default) group of virtualmail, no supplementary group, with the home directory /home/virtualmailaccounts/ACCOUNTNAME, where the ACCOUNTNAME is the e-mail account name and with a shell of /bin/false. If this fails, an error is returned. Assigning the e-mail account a shell of /bin/false ensures that a malicious e-mail account user cannot execute any unix commands if his e-mail browser has an error which would otherwise return him to the command line.

3. The autopasswd script is used to add the e-mail account's password to the unix configuration file /etc/passwd.

4. Sendmail configuration file /etc/mail/virtusertable is updated by adding an e-mail account ACCOUNTNAME@VIRTUALDOMAIN linked to the e-mail account name. Configuration file /etc/mail/virtusertable is then hashed.

5. A record is added to data file /root/MSconfig/dat/aliasmail.VIRTUALDOMAIN for the new e-mail account.

6. The e-mail account's e-mail forwarding is configured as follows:
   (a) if the administrator has selected no forwarding option, nothing is done;
   (b) if the administrator has selected forwarding to one or more e-mail addresses, to a fax machine, or a custom e-mail forwarding option, the files /home/virtualmailaccounts/ACCOUNTNAME.forward and /home/virtualmailaccounts/ACCOUNTNAME.procmailrc are created or modified as required and the ownership of the .forward and .procmailrc files is set to the e-mail account.

An e-mail alias is an e-mail account which is linked to another email account. E-mail addressed to the e-mail alias is routed by the mail server 32 to the linked e-mail account. This allows one person to appear to have more than one e-mail address but to receive all of his e-mail in a single account. The administrator may add a virtual domain e-mail alias by selecting add virtual domain e-mail alias control 426, which brings up an add virtual domain e-mail alias dialog box (not shown). Add virtual domain e-mail alias dialog box allows the administrator to enter the alias name and the e-mail account to which the alias will be linked. Once the administrator enters this information, the virtual domain e-mail alias is added to the mail server 32 by taking the following steps:

1. Data file /root/MSconfig/dat/aliasmail.VIRTUALDOMAIN is checked to ensure that an identical alias or e-mail account name does not exist in the virtual domain. If such an alias or e-mail account name already exists, an error is returned.

2. Data files /root/MSconfig/data/aliasmail.VIRTUALDOMAIN and /root/MSconfig/dat/siteAdmin/VIRTUALDOMAIN are checked to ensure that the
specified owner is an existing e-mail account name in the virtual domain or the virtual domain administrator. If this fails, an error is returned.

3. The alias is added to data file /root/MSconfig/dat/aliasmail.VIRTUALDOMAIN.

4. Sendmail configuration file /etc/mail/virtusertable is updated by adding an e-mail account ALIAS@VIRTUALDOMAIN linked to the owner. Configuration file /etc/mail/virtusertable is then hashed.

Virtual domain e-mail accounts and aliases may be edited or deleted by highlighting the account or alias name and then selecting edit e-mail alias/account control 428 or delete e-mail alias/account control 430, respectively.

Mail server 32 permits the administrator to block internet e-mail from individual e-mail accounts or from entire internet domains. If internet e-mail is received from a blocked account or domain, a returned mail message is added to the received message and the message is sent back to the sending address. Blocked mail list section 432 lists e-mail addresses and internet domains which have been blocked. The administrator may add an e-mail address or internet domain to the list by selecting add blocked mail address control 434, which brings up add blocked address dialog box (not shown). Add blocked address dialog box allows the administrator to enter the e-mail address or internet domain from which mail is to be blocked and the message which is to be returned to the sending address. Once this information has been entered, the blocked address or domain is added to the mail server 32 by taking the following steps:

1. Data file /root/MSconfig/data/mailList.dat is checked to ensure that the blocked address or domain has not already been blocked. If it has, an error is returned.

2. Data file /root/MSconfig/dat/domainList.dat is checked to ensure that the blocked address or domain is not hosted by multiserver 10. If it is, an error is returned.

3. Data file /root/MSconfig/dat/screens.dat is checked to ensure that the blocked address or domain is not the primary domain or part of the primary domain. If it is, then an error is returned.

4. The blocked address or domain is added to data file /root/MSconfig/dat/mailList.dat

5. Sendmail data file /etc/mail/access is updated to block e-mail from the blocked address or domain.

6. Sendmail data file /etc/mail/is hashed.

A blocked e-mail address or internet domain may be removed by selecting delete blocked mail address control 436.

**Configuring the Firewall**

If the administrator selects the “Firewall” control from configuration screen pushbuttons 104, a firewall screen 450 is displayed (Figure 19). Firewall screen 450 is used to configure the LAN firewall 62 (Figure 2). Firewall screen 450 comprises LAN user access control 452, approved domain section 454, restricted domain section 460 and lan registry section 466.
LAN use access control 452 is a toggle control. When LAN access control 452 is toggled on, LAN users may access the internet from LAN workstations 42 added to the LAN registry (described below). When LAN access control 452 is toggled off, LAN users cannot access the internet from LAN workstations 42. When LAN access control 452 is toggled on, the following steps are taken:

1. Ensure that a core change is not taking place. If a core change is taking place, an error is returned.
2. The Internet firewall configuration script /root/MSconfig/bin/fwINIT is run.
3. The LAN firewall configuration script /root/MSconfig/bin/fwlan is run.

When LAN access control 452 is toggled off, the following steps are taken:

1. Ensure that a core change is not taking place. If a core change is taking place, an error is returned.
2. The Internet firewall configuration script /root/MSconfig/bin/fwINIT is run.

Approved domain section 454 comprises an approved domain list 455, an add approved domain control 456 and a delete approved domain control 458. Approved domain list 455 lists domains that a LAN user may access if the LAN workstation 42 he is using has been added to the LAN registry with an approved internet access policy. A domain may be added to the approved domain list 455 by selecting add approved domain control 456, which brings up an add approved domain dialog box (not shown).

Add approved domain dialog box allows the administrator to enter the name of a domain, which is then added to the approved policy by taking the following steps:

1. Ensure that no core change is taking place. If a core change is taking place, an error is returned.
2. Data file /root/MSconfig/dat/approved.dat is checked to ensure that the domain name is not already in the approved domain list. If it is, an error is returned.
3. Data file /root/MSconfig/dat/restricted.dat is checked to ensure that the domain is not in the restricted domain list used for the restricted internet access policy. If it is, an error is returned.
4. The domain name is added to /root/MSconfig/dat/approved.dat.
5. LAN firewall configuration script /root/MSconfig/bin/fwlan is modified to permit LAN workstations with an approved internet access policy to access the domain name.
6. The Internet firewall configuration script /root/MSconfig/bin/fwINIT is run.
7. If LAN access control 452 is toggled on, LAN firewall configuration script /root/MSconfig/bin/fwlan is run.

To remove a domain from the approved domain list 455, the administrator highlights the domain name in approved domain list 455 and selects the delete approved domain control. The domain is removed from data file /root/MSconfig/dat/approved.dat, LAN firewall configuration script /root/MSconfig/bin/fwlan is modified and the appropriate firewall configuration scripts are run.
Restricted domain section 460 comprises a restricted domain list 461, an add restricted domain control 462 and a delete restricted domain control 464. Restricted domain list 460 lists domains that a LAN user may not access if the LAN workstation 42 he is using has been added to the LAN registry with a restricted internet access policy. A domain may be added to the restricted domain list 461 by selecting add restricted domain control 462, which brings up an add restricted domain dialog box (not shown). Add restricted domain dialog box allows the administrator to enter the name of a domain, which is then added to the approved policy by taking the following steps:

1. Ensure that no core change is taking place. If a core change is taking place, an error is returned.
2. Data file /root/MSconfig/dat/approved.dat is checked to ensure that the domain name is not in the approved domain list. If it is, an error is returned.
3. Data file /root/MSconfig/dat/restricted.dat is checked to ensure that the domain is not already in the restricted domain list. If it is, an error is returned.
4. The domain name is added to /root/MSconfig/dat/restricted.dat.
5. LAN firewall configuration file /root/MSconfig/bin/fwlan is modified to block LAN workstations with a restricted internet access policy from accessing the domain name.
6. The Internet firewall configuration script /root/MSconfig/bin/fwINIT is run.
7. If LAN access control 452 is toggled on, LAN firewall configuration script /root/MSconfig/bin/fwlan is run.

A LAN workstation 42 must be added to a LAN registry before it can be used by a LAN user to access the internet. LAN registry section 466 comprises authorized workstation list 472, add workstation control 468 and delete workstation control 470. Authorized workstation list 472 lists the LAN workstations 42 which have been added to the LAN registry, the expiry time for the registration and the internet access policy for the LAN workstation 42. The LAN workstation 42 will be removed from the LAN registry on the date and time specified as the expiry time. If the registration is to be permanent, the expiry time is listed as NEVER. To add a LAN workstation 42 to the LAN registry, the administrator selects add workstation control 468, which brings up an add workstation dialog box (not shown). Add workstation dialog box allows the administrator to enter the IP address of the LAN workstation 42, the expiry time of the registration, and the internet access policy for the workstation. The LAN workstation 42 is then added to the LAN Registry by taking the following steps:

1. Ensure that no core change is taking place. If a core change is taking place, an error is returned.
2. The data file /root/MSconfig/dat/registry.dat is checked to ensure that the LAN workstation 42 is not already in the LAN registry. If it is, then an error is returned.
3. The IP address specified is checked to ensure it is within the range of IP addresses permitted for LAN workstations 42 by comparing it to the Internal IP and
Internal Subnet IP records in /root/MScconfig/dat/screens.dat. If the specified IP address is outside the permitted range, an error is returned.

4. A record is added to /root/MScconfig/dat/regstry.dat for the specified LAN workstation.

5. LAN firewall configuration file /root/MScconfig/bin/fwlan is modified to add the specified LAN workstation with the specified internet access policy.

6. The Internet firewall configuration script /root/MScconfig/bin/fwINIT is run.

7. If LAN access control 452 is toggled on, LAN firewall configuration script /root/MScconfig/bin/fwlan is run.

To remove a LAN workstation 42 from the LAN registry, the administrator highlights the LAN workstation’s entry in authorized workstation list 472 and selects delete workstation control 470. The LAN workstation 42 is removed from data file /root/MScconfig/dat/regstry.dat, lan firewall configuration script /root/MScconfig/bin/fwlan and the firewall configuration scripts are run.

15 **PART THREE: FAX SCANNER**

To send a fax using fax server 34, a LAN user must be a member of the faxblast group. The LAN user must take two steps to send a fax:

1. The files which comprise the body of the fax must be copied into the fax_blast file share volume. These files are referred to as the fax source files (FSF) and are the actual files which are faxed

2. A fax control file (FCF) or a fax web file (FWF) must be created in or copied into the fax_blast file share volume. FCF files must have the extension .fcf and a FWF must have the extension .fwf.

A FCF is created by the LAN user using any text editor. An FCF has the following format:

<table>
<thead>
<tr>
<th>Line</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>FSF</td>
<td>a space delimited list of fax source files. Each of these files must be in postscript or pdf format. The fax source files will be faxed sequentially in a single fax transmission.</td>
</tr>
<tr>
<td>2</td>
<td>From</td>
<td>a text string identifying the sender of the fax</td>
</tr>
<tr>
<td>3</td>
<td>Attempts</td>
<td>the maximum of attempts which will be made to send the fax</td>
</tr>
<tr>
<td>4</td>
<td>Resolution</td>
<td>m - indicates that the fax should be sent at 196 dots per inch (dpi) imaging</td>
</tr>
</tbody>
</table>
1 - indicates that the fax should be sent at 98 dpi imaging

5

5

coverpage

file name of an encapsulated postscript (EPS) format coverpage

6

subject

a text string which will be added to the coverpage if one is specified

7-n

comments

one or more lines of comments which will be added to the coverpage, if one is specified

15

n+1*

To

a text string identifying the addressee of the fax

n+2*

Fax number

the fax telephone number for the addressee

* Lines n+1 and n+2 may be repeated any number of times to send the same fax to additional addressees.

The primary domain fax service, which has the host name of fax.PRIMARYDOMAIN presents a web page form, which allows a LAN user to enter his LAN user name and password and all of the information required to create an FCF. When the LAN user submits the completed form, the form data is passed to fax.cgi.

Fax.cgi then validates the LAN user name and password using the Fax CGI password file. If a valid LAN user name and password were entered and if the LAN user is a member of the faxblast group, fax.cgi creates an FWF in the fax_blast file share volume.

An FWF is identical to an FCF, except that it has an extra line prepended to the FCF containing the LAN user name of the sender.

The unix cron utility is configured to run a transport agent named Fax Scanner every minute. The Fax Scanner uses FWF, FCF and FSF files and the Hylafax sendfax program to send a fax by taking the following steps:

1. All FWFs in the fax_blast file share volume are processed in the following manner:
   i. The timestamp of the FWF is checked to ensure it has not been modified in the previous 30 seconds. If it has, then the FWF is ignored.
   ii. The first line of the FWF is removed and the ownership of the FWF is set to the named LAN user. The resulting file is renamed to be a FCF.
2. All FCFs in the fax_blast file share volume are processed in the following manner:
   i. The timestamp of the FCF is checked to ensure it has not been modified in the previous 30 seconds. If it has, then the FCF is ignored.
   ii. Every FSF is checked to ensure that it exists in the fax_blast file share volume and has not been modified in the previous 30 seconds. If any of the FSFs are missing or is younger than 30 seconds old, the FCF is ignored.
   iii. If a coverpage is specified in the FCF and it exists in the fax_blast file share volume, Hylafax program faxcover is used to create a coverpage using the data in the FCF.
   iv. Hylafax program sendfax is used to queue the fax to Hylafax outbound server. The fax will consist of the coverpage if one was created and the FSFs.
   v. The FCF is deleted.

Although multiserver 10 has been described here in a relatively specific manner, one skilled in the art will recognize that multiserver 10 may be implemented on a computer running a different unix based platform or a non-unix based platform. Further, one skilled in the art will be capable of implementing the various components of multiserver 10 with different software packages than those described. These and other variations on the exemplary preferred embodiments will fall within the scope of the invention disclosed above and in the following claims.
We Claim:

1. A configuration management interface for configuring a plurality of computer services, said computer services installed on a computer system, said configuration management interface comprising:

   (a) configuration definition means for allowing characteristics of each of said computer services to be defined by an administrator; and

   (b) configuration implementation means for configuring the plurality of said computer services to correspond to said characteristics.

2. The configuration management interface of claim 1, wherein said configuration definition means includes a plurality of configuration definition screens for displaying the configuration of said plurality of computer services and for allowing said administrator to define said characteristics.

3. The configuration management interface of claim 2, wherein:

   i. said configuration definition screens allow a particular characteristic required to configure two or more of said computer services to be defined by a single input; and

   ii. said configuration implementation means configures said two or more of said computer services to correspond to said particular characteristic.

4. The configuration management interface of claim 1 further including locking means for ensuring that at least one of said characteristics may be defined only by said administrator.

5. The configuration management interface of claim 2 further including locking means for selectively restricting access to at least one of said configuration definition screens.

6. The configuration management interface of claim 2 wherein said plurality of computer services is provided by a plurality of servers, and wherein each of said servers may have one of a plurality of status conditions and wherein a visual indicator on said configuration definition screens indicates the respective status of each of said servers.

7. The configuration management interface of claim 2 wherein said plurality of computer services is provided by a plurality of servers, and wherein each of said servers
may have one of a plurality of status conditions and wherein sections of said configuration definition screens corresponding to each of said servers are colour coded to the indicate the respective status of each of said servers.

8. The configuration management interface of claim 7, wherein said configuration management interface further allows said administrator to control the operation of a firewall installed on said computer, and wherein the relationship between each of said servers and said firewall is indicated by displaying elements relating to each of said servers on said configuration definition screens in one or more selected colours.

9. A configuration management interface for configuring a plurality of computer services, said configuration management interface being embodied in a computer readable medium, and said configuration management interface comprising:

(a) configuration definition means for allowing characteristics of each of said computer services to be defined by an administrator; and

(b) configuration implementation means for configuring the plurality of said computer services to correspond to said characteristics.

10. A multiserver for providing a plurality of computer services to a plurality of users, said multiserver being capable of installation and execution on a computer system, said multiserver comprising:

i. a file server for providing file storage and retrieval services to at least some of said users;

ii. a print server for providing print services to at least some of said users;

iii. a mail server for providing e-mail services to at least some of said users; and

iv. a configuration management interface, said configuration management interface including configuration definition means for allowing an administrator to define:

(a) characteristics of said users;

(b) characteristics of said file storage and retrieval services, print services and e-mail services; and
(c) characteristics of the use of said file storage and retrieval services, print services and e-mail services by each of said users, and said configuration management interface including configuration implementation means for configuring said file server, said print server and said mail server to correspond to the characteristics defined by said administrator.

11. The multiserver of claim 10 wherein said configuration definition means includes a plurality of configuration definition screens for allowing said administrator to define said characteristics of said users, said file storage and retrieval services, said print services and said e-mail services.

12. The multiserver of claim 10 wherein said plurality of users includes one or more LAN users, and wherein said configuration implementation means automatically configures said file server to include a file share volume for each said LAN user and said mail server to include an e-mail account for each said LAN user.

13. The multiserver of claim 10 wherein said multiserver is capable of being coupled to one or more LAN workstations over a local area network and is capable of being coupled to one or more internet sites over an internet connection and wherein said multiserver further comprises a LAN firewall for controlling access from said LAN workstations to said internet sites and wherein:

(d) said configuration definition means allows said administrator to define one or more internet access policies, and to define an association between each of said LAN workstations and one of said internet access policies; and

(e) said configuration implementation means configures said LAN firewall to correspond to said internet access policies and said association between each of said LAN workstations and said internet access policies.

14. The multiserver of claim 10 further including a web server for hosting one or more internet domains and a domain name server for resolving internet IP addresses for each of said internet domains, and wherein:

(f) said configuration definition means allows said administrator to define said internet domains; and
(g) said configuration implementation means configures said web server to host said internet domains and to configure said domain name server to resolve internet IP address for said internet domains.

15. The multiserver of claim 10 further including a web server for hosting one or more internet domains wherein

(h) said configuration definition means allows said administrator to define said internet domains; and

(i) said configuration definition means configures said web server to host a public web site and a private web site for each said internet domain.

16. The multiserver of claim 14 further including an internet firewall for selectively permitting said users to access said web server and said domain server and for restricting said users from accessing said file server.

17. The multiserver of claim 12, wherein said multiserver is capable of being connected to one or more modems, said multiserver further including a fax server for receiving and sending fax transmissions, and wherein:

(j) said configuration definition means allow said administrator to define modem characteristics for each of said modems, said modem characteristics including an incoming station ID and a telephone number; and

(k) said configuration implementation means configures said fax server to control the operation of each of said modems in a manner corresponding to said modem characteristics.

18. The multiserver of claim 17 wherein:

(l) said configuration definition means further allows said administrator to identify one or more incoming station IDs, and to define a relationship between each of said incoming station IDs and one or more of said LAN users, and

(m) said configuration implementation means configures said fax server to communicate fax transmissions received from an identified incoming station ID to the one or more LAN users.
19. The multiserver of claim 18 wherein the fax server is configured to communicate fax transmissions received from an identified incoming station ID to the related one or more LAN users by communicating an image of said fax transmission to the e-mail accounts of said one or more LAN users.

20. The multiserver of claim 16 wherein a visual indicator is provided on at least some of said configuration definition screen for indicating a status condition of one or more selected servers, said one or more selected servers being selected from said file server, print server, mail server, web server or domain name server.

21. The multiserver of claim 16 wherein portions of said configuration definition screen corresponding to one or more selected servers, said one or more selected servers being selected from said file server, print server, mail server, web server or domain name server are displayed using one or more selected colours to indicate a status condition of said selected server.

22. The multiserver of claim 16 wherein said status condition indicates a relationship between said selected server and said internet firewall.

23. The multiserver of claim 16 wherein components of said configuration definition screen corresponding to said web server and said domain server are displayed in a first colour and components of said configuration definition screen corresponding to said file server are displayed in a second colour.

24. The multiserver of claim 10 wherein said characteristics of said users include the arrangement of said users into groups.

25. The multiserver of claim 10 wherein said characteristics of the use of said file storage and retrieval services by each of said users includes the accessibility of specific portions of said file server to each of said users.

26. The multiserver of claim 12 wherein said computer system is configured to operate using a first operating system; said computer system is capable of being coupled to a first LAN workstation; said first LAN workstation is configured to operate using a second operating system; said first operating system is distinct from said second operating system; and said file server includes a first file protocol conversion means for permitting said first LAN workstation to utilize said file storage and retrieval services, and wherein said configuration implementation means configures said first file protocol conversion means for use by each of said LAN users.
27. The multiserver of claim 26 wherein said first protocol conversion means consists of software programs and data files installed only on said computer system.

5
28. The multiserver of claim 26 wherein: said computer system is capable of being coupled to a second LAN workstation; said second LAN workstation is configured to operate using a third operating system; each of said first operating system, said second operating system and said third operating system is distinct from the other operating systems; said file server includes a second file protocol conversion means for permitting said second LAN workstation to access said file system; and said configuration implementation means includes means for configuring the use of said second file protocol conversion means by each of said LAN users.

10
29. The multiserver of claim 28 wherein each of said first protocol conversion means and second protocol conversion means consist of software programs and data files installed only on said computer system.

15
30. The multiserver of claim 10 wherein said computer is capable of being coupled to a printer, and wherein said printer has a first group of related modes and said configuration implementation means includes printer adding means for:

20
   (n) configuring said print server to control said printer; and

   (o) configuring said print server to include a plurality of virtual printers, each of said virtual printers corresponding to one mode selected from said first group of related modes.

25
31. The multiserver of claim 30 wherein said printer further has a second group of related modes and each of said virtual printers further corresponds to one mode selected from said second group of related modes.

30
32. The multiserver of claim 31 wherein each of said virtual printers corresponds to a unique combination of:

35
   (p) one mode selected from said first group of related modes; and

   (q) one mode selected from said second group of related modes.

33. A method of sending a fax transmission comprising the steps of:

40
   (a) providing a fax server capable of making a fax transmission;
(b) providing a fax control file including fields for identifying one or more fax source files to be faxed and identifying a destination telephone number to which the fax is to be sent;

(c) providing one or more documents corresponding to said fax source files;

(d) ensuring that said fax control file has not been modified for a first selected period of time;

(e) ensuring that each of said documents has not been modified for a second selected period of time;

(f) assembling a fax document consisting of said documents; and

(g) instructing said fax server to send said fax document to said destination telephone number.

34. The method of claim 33, wherein step (b) is performed by copying said fax control file into a selected file share volume of a computer and step (c) is performed by copying said documents in said selected file share volume.

35. The method of claim 33, wherein said fax control file includes a field for specifying two of more destination telephone numbers and wherein the following step is performed after step (g):

(h) repeating step (g) for each additional destination telephone number.

36. The method of claim 33 wherein step (b) comprises the following steps:

(b.1) providing a graphic interface for allowing a user to identify said fax source files and said destination telephone number; and

(b.2) creating said fax control file by completing said fields for identifying one or more fax source files to be faxed and identifying a destination telephone number to which the fax is to be sent.

37. The method of claim 36 wherein step (b) further comprises the following step:

(b.3) copying said fax control file into said selected file share volume.
38. A method of relaying a piece of electronic mail transmitted from a transmitting computer to a receiving computer through a host computer, said method comprising the steps of:

5  (a) recording a user name and password for a user;

(b) establishing a list of computers for which said host computer will relay electronic mail;

10 (c) waiting for said user to establish a communication link between said transmitting computer and said host computer and to enter said user name and said password;

(d) adding said transmitting computer to said list of computers;

15 (e) receiving said electronic mail from said transmitting computer; and

(f) relaying said electronic mail to said receiving computer.
FIG. 1
Remote login is a security risk. If enabled, any LAN user in the "admin" group can "telnet" into the MultiServer and perform any function from a remote location. While this can be useful, it is recommended that it be used sparingly as any user/password entered on a remote machine can be viewed/modified by a potential "hacker". If "No External Login" is selected, the only place the system can be viewed/modified is at the local keyboard — this is the recommended setting.
FIG. 8

 Administration

Lock System

Backups

Remote

DNS

Quit

Networks

Firewall

Mail Server

FTP Server

Print Server

Fax Server

File Server

Users & Groups

Domain Server

Misc.

Host Name

Address

750

752

704

502

504

754

ntk.com

ftp.ntk.com

mail.ntk.com

www.ntk.com

www.vip-ntk.com

www.fun.ntk.com

auth.ntk.com

auth.fun.ntk.com

auth.alpha.ntk.com

auth.vip-ntk.com

auth.file.ntk.com

PRIMARY

ntk.com

ntk.com

ntk.com

ntk.com

ntk.com

ntk.com

ntk.com

ntk.com

ntk.com

ntk.com

ntk.com

ntk.com

ntk.com

ntk.com

ntk.com

752

Change Host Address
### Users and Groups

<table>
<thead>
<tr>
<th>User Name</th>
<th>Groups Joined</th>
</tr>
</thead>
<tbody>
<tr>
<td>andrew</td>
<td>admin, faxblast, lads, multiserver, ntk, patents, support, users</td>
</tr>
<tr>
<td>anita</td>
<td>accounting, users</td>
</tr>
<tr>
<td>bob</td>
<td>faxblast, users</td>
</tr>
<tr>
<td>boop</td>
<td>ntk, patents, users</td>
</tr>
<tr>
<td>brian</td>
<td>admin, art, faxblast, lads, ntk, support, users, web</td>
</tr>
<tr>
<td>dave</td>
<td>faxblast, users</td>
</tr>
<tr>
<td>doug</td>
<td>users</td>
</tr>
</tbody>
</table>

### E-mail Aliases

<table>
<thead>
<tr>
<th>E-mail Aliases</th>
<th>Destination User</th>
<th>Group Name</th>
<th>Receive Mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>andrew</td>
<td>*admin</td>
<td></td>
</tr>
<tr>
<td>boni</td>
<td>brian</td>
<td>*faxblast</td>
<td></td>
</tr>
<tr>
<td>brianb</td>
<td>brian</td>
<td>*Infax</td>
<td>Enabled</td>
</tr>
<tr>
<td>devo</td>
<td>brian</td>
<td>*users</td>
<td></td>
</tr>
<tr>
<td>doctor</td>
<td>andrew</td>
<td>*vadmin</td>
<td></td>
</tr>
<tr>
<td>drock</td>
<td>doug</td>
<td>*web</td>
<td>Enabled</td>
</tr>
<tr>
<td>info</td>
<td>erin</td>
<td>accounting</td>
<td></td>
</tr>
</tbody>
</table>

**Add** | **Edit** | **Delete** | **Add** | **Delete**
### Fax Server Setup

**Modes and Outgoing Faxes**

**Modems and Outgoing Faxes**

<table>
<thead>
<tr>
<th>Station ID</th>
<th>Rel</th>
<th>A/C</th>
<th>Tel. No.</th>
<th>Port</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTK.COM</td>
<td>FA</td>
<td>905</td>
<td>602-5878</td>
<td>modem</td>
<td>Running and idle</td>
</tr>
</tbody>
</table>

**Add** | **Edit** | **Delete**

**OUTGOING QUEUE**

<table>
<thead>
<tr>
<th>Job Number</th>
<th>Owner ID</th>
<th>Destination</th>
<th>Pages Sent</th>
<th>Attempts</th>
</tr>
</thead>
</table>

**Delete** | **Delete All**

---

**FIG. 13**
### Virtual Domains

<table>
<thead>
<tr>
<th>Domain</th>
<th>Alias Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>poscen.com</td>
<td>jennifer</td>
</tr>
<tr>
<td>re.ntk.com</td>
<td>patrick</td>
</tr>
<tr>
<td>timsworld.ntk.com</td>
<td>jennifer</td>
</tr>
<tr>
<td>wellcarecanada.com</td>
<td>info</td>
</tr>
<tr>
<td>writingspace.ntk.com</td>
<td>sales</td>
</tr>
</tbody>
</table>

### Block Mail From

<table>
<thead>
<tr>
<th>Name/Domains</th>
<th>Message on Returned Mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>exit.de</td>
<td>Refused</td>
</tr>
<tr>
<td><a href="mailto:marketing@aol.com">marketing@aol.com</a></td>
<td>Get Lost</td>
</tr>
<tr>
<td>mnestt.com</td>
<td>Refused</td>
</tr>
</tbody>
</table>