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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 January 2003 (03.01.2003)

PCT

(10) International Publication Number
WO 03/001392 A1

(51) International Patent Classification⁷: G06F 15/00

(21) International Application Number: PCT/US02/20029

(22) International Filing Date: 21 June 2002 (21.06.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/300,191 21 June 2001 (21.06.2001) US

(71) Applicant *(for all designated States except US)*: **TURBOLINUX, INC.** [US/US]; 8000 Marina Boulevard, Suite 300, Brisbane, CA 94005 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BECKMAN, Peter, H.** [US/US]; 23 Taos Street, Los Alamos, NM 87544 (US). **HUDSON, Trammel** [US/US]; 5801 Nicholson Lane, Suite 1004, Bethesda, MD 20852 (US). **PAINTER, James, S.** [US/US]; 40 Ute Circle, Santa Fe, NM 87505 (US).

(74) Agent: **YIM, Peter, J.**; Morrison & Foerster LLP, 425 Market Street, San Francisco, CA 94105-2482 (US).

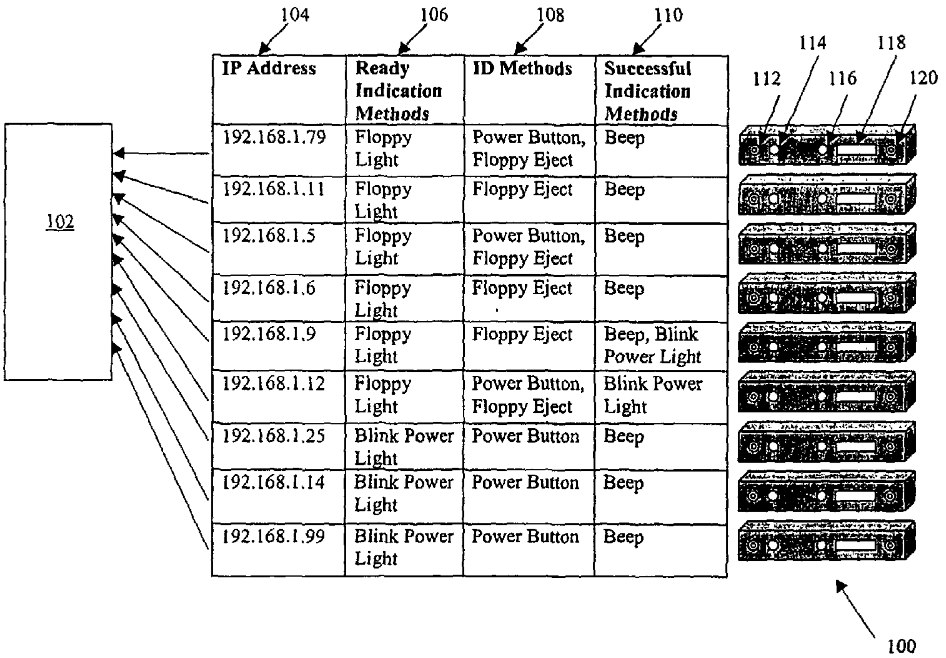
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT,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

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

Published:
— *with international search report*

[Continued on next page]

(54) Title: SEQUENTIAL IDENTIFICATION OF A GROUP OF COMPUTERS



IP Address	Ready Indication Methods	ID Methods	Successful Indication Methods
192.168.1.79	Floppy Light	Power Button, Floppy Eject	Beep
192.168.1.11	Floppy Light	Floppy Eject	Beep
192.168.1.5	Floppy Light	Power Button, Floppy Eject	Beep
192.168.1.6	Floppy Light	Floppy Eject	Beep
192.168.1.9	Floppy Light	Floppy Eject	Beep, Blink Power Light
192.168.1.12	Floppy Light	Power Button, Floppy Eject	Blink Power Light
192.168.1.25	Blink Power Light	Power Button	Beep
192.168.1.14	Blink Power Light	Power Button	Beep
192.168.1.99	Blink Power Light	Power Button	Beep

(57) **Abstract:** In identifying a computer among a group of computers (100) connected to a server, where each computer in the group is connected to a server and has a network identification (104), the computer to be identified is physically manipulated after being turned on. A signal is sent to the server that includes data which can be associated with a network identification for the computer and indicates that the computer has been physically manipulated. The server receives the signal. The network identification (104) associated with the sender of the received signal is associated with the physically manipulated computer.

WO 03/001392 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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

SEQUENTIAL IDENTIFICATION OF A GROUP OF COMPUTERS

CROSS-REFERENCE TO RELATED APPLICATIONS

The present application claims priority of an earlier filed provisional application U.S. Ser. No. 60/300,191, entitled SEQUENTIAL IDENTIFICATION OF A GROUP OF COMPUTERS, filed on June 21, 2001, the entire content of which is incorporated herein by reference.

BACKGROUND

1. Field of the Invention

The present application generally relates to identifying a computer in a group of computers. More particularly, the present application relates to identifying the network identification of the computer.

2. Related Art

A group of computers can be linked together on a computer network. In some applications, these computers can be arranged as a rack of computers. Each computer can function as a server, client, or both as a server and client.

The installation and maintenance of such a group of computers can involve correlating each computer with its network identification, such as an IP or MAC address. This network identification can be dynamically or statically assigned to each computer in the group. By identifying a computer's network identification, a server can communicate with a particular computer in the group of computers. Furthermore, a system operator can identify a computer within the group of computers that needs maintenance or attention.

Typically, a system operator identifies each computer in a group of computers by either writing down hardware identification numbers attached to each computer's physical hardware, or interacting with each computer using input devices such as a keyboard or a mouse. In particular, a system operator can sequentially attach a keyboard to each computer and use keyboard input to identify the computer. After identifying a computer in a group of computers, the system operator can optionally assign a new network identification, such as an IP or MAC address, to the computer.

However, these ways of identifying computers in a group of computers are time consuming and typically require error-free recordation of hardware identification numbers, such as a MAC address, and the subsequent error-free input of those hardware identification numbers into a system. Furthermore, when using input devices such as a keyboard to interact with each computer, a keyboard and monitor must be attached to each computer in the group of computers. This arrangement can be inconvenient, especially when a single keyboard and a single monitor must be manually connected to each of the computers in a group of computers as each computer is identified.

Another way of identifying computers in a group of computers involves using specialized hardware that is connected to the group of computers. This specialized hardware can match each computer's physical hardware to a network address. However, such specialized hardware can be costly to obtain and use.

Another way of identifying computers in a group of computers includes using individualized boot software. In particular, the individualized boot software can include media, such as a floppy disk or a CD-ROM, that includes a unique ID that can be used to identify and sequence the group of computers. However, both producing and using individualized boot software can be time consuming, particularly because the boot software media must be inserted into the correct computer within the group in order for the individualized boot software to identify the computer accurately. Furthermore, a failure of the boot software media requires rebuilding that specific boot software media for the individual computers that failed.

Yet another way of identifying computers in a group of computers includes sequentially booting the computers, and identifying each computer by determining the order in which the computers complete their boot-up sequence. However, this way of identifying a computer in a group of computers can be time consuming because it requires waiting for the computers to boot-up and obtain a network address. The time required for the computers to boot-up can depend on factors such as the details of the computer hardware, network load, and the like. Furthermore, if one or more of the computers fail during the boot-up sequence, the group of computers may provide no indication to the human operator that a computer in the group failed, thus producing an identification sequence that is missing one or more of the computers in the group. Accordingly, when the operator discovers the error, the sequence must be reconstructed.

SUMMARY

The present application relates to methods and apparatus for identifying a computer among a group of computers, where each computer in the group is connected to a server and has a network identification.

In one embodiment, a computer in the group is physically manipulated after being turned on. A signal is sent to the server that can be identified with the physically manipulated computer and indicates that the computer has been physically manipulated. The signal is received at the server. The network identification associated with the received signal is associated with the physically manipulated computer.

In another embodiment, the apparatus includes a system having a group of computers to be identified and a server. Each computer in the group of computers is configured to detect a physical manipulation to the computer and send a signal to the server indicating that the computer has been manipulated and can be identified with the computer. The server is configured to receive a signal from each computer in the group of computers and associate it with the manipulated computer.

DESCRIPTION OF DRAWING FIGURES

The present invention can be best understood by reference to the following description taken in conjunction with the accompanying drawing figures, in which like parts may be referred to by like numerals:

Fig. 1 is a schematic diagram depicting a server and a group of computers;

Fig. 2 is a flow chart depicting stages of an exemplary identification process;

Fig. 3 is a flow chart depicting stages of another exemplary identification process;

Fig. 4 is a flow chart depicting stages of yet another exemplary identification process;

Fig. 5 is a flow chart depicting an exemplary process that can be used to identify and sequence a computer in a group of computers; and

Fig. 6 is another schematic diagram depicting a server and a group of computers.

DETAILED DESCRIPTION

In order to provide a more thorough understanding of the present invention, the following description sets forth numerous specific details, such as specific configurations, parameters, examples, and the like. It should be recognized, however, that such description is not intended as a limitation on the scope of the present invention, but is intended to provide a better description of the exemplary embodiments.

With reference to Fig. 1, a group of computers 100 can be arranged in a stack, rack, or any other configuration, and connected to server 102. Each computer in the group of computers 100 can function as a server, client, or both as a server and client, depending on the application. Furthermore, server 100 can function as a server, client, or both as a server and client, depending on the application. Although Fig. 1 shows a group of computers 100 arranged in a rack configuration, it should be recognized that the group of computers 100 can be arranged in any configuration.

As shown in Fig. 1, each computer in a group of computers 100 can be identified by a server by associating a network address, such as an IP or MAC address 104, with the computer. In each of the embodiments described below, computers and servers can include software that allows the computers and servers to communicate with each other. In particular, this software can allow a computer to contact a server and register its network address, provide a list of ways that the computer can be identified, and the like. Furthermore, although the following embodiments describe identifying a single computer in a group of computers, each computer in the group of computers can be identified sequentially.

With reference to Fig. 2, an embodiment of a process that can be used to identify a computer in a group of computers 100 (Fig. 1) is shown. In step 200, an operator can physically manipulate the state of a computer that is already turned on in a manner that is detectable by the computer. Next, in step 202, the computer can detect the manipulation and send a message to server 102 (Fig. 1) indicating that the computer has been manipulated. The message can include information such as network identification of the computer, information about the manipulation, and the like. In step 204, server 102 (Fig. 1) can then identify the manipulated computer by associating which computer was physically manipulated with which computer sent the message. In particular, server 102 (Fig. 1) can associate a network identification, such as an IP or MAC address, and the like, to this computer.

With reference to Fig. 3, another embodiment of a process that can be used to identify a computer in a group of computers 100 (Fig. 1) is shown. In step 300, the computer can send heartbeat messages to server 102 (Fig. 1) on a periodic basis. The heartbeat messages can include information such as network identification, information about the computer, and the like. Next, in step 302, an operator can physically manipulate the state of the computer in a manner that is detectable by the computer. In step 304, the computer can detect the manipulation and consequently fail to send at least one heartbeat message to server 102 (Fig. 1). In step 306, server 102 (Fig. 1) can identify the manipulated computer by associating which computer was physically manipulated with which computer failed to send a heartbeat message. In particular, server 102 (Fig. 1) can associate a network identification, such as a network address, and the like, to this computer.

With reference to Fig. 4, another embodiment of a process that can be used to identify a computer in a group of computers 100 (Fig. 1) is shown. In step 400, an operator can physically manipulate the state of a computer that is already turned on in a manner that is detectable by the computer. Next, in step 402, software can automatically detect the manipulation and can identify the manipulated computer and associate it with a network identification, such as its IP or MAC address, and the like. The software can be installed on the server, or as a system installed on both the computer and server.

With reference to Fig. 5, an embodiment of a possible sequence that can be used to identify a computer in a group of computers is shown. In step 500, the computer can emit a signal indicating that the computer is ready to be identified. This signal can be detectable by an operator in some manner such as visibly, audibly, and the like. For instance, the signal can include activating a light, activating a light emitting diode (LED), manipulating the display on an integral LCD, manipulating the display on an integral display panel, ejecting or reinserting a CD-ROM, emitting an auditory sound, and the like. Activating a light or LED can include illuminating the light or LED, flashing the light or LED, and the like. It should be recognized, however, that step 500 may not be used in all applications, such as when a computer is always ready for identification.

In step 502 of the present embodiment, an operator can physically manipulate the state of the computer in a manner that is detectable by the computer. Next, in step 504, the computer can detect the manipulation and send a message to server 102 (Fig. 1) indicating that the computer has been manipulated. The message can include information such as network identification of the computer, information about the manipulation, and the like. Alternately, for a computer that sends heartbeat messages to server 102 (Fig. 1), the computer can fail to send at least one heartbeat message when the computer detects an manipulation in step 504.

In step 506 of the present embodiment, server 102 (Fig. 1) can then identify the manipulated computer by associating which computer was physically manipulated with which computer sent the message. In particular, server 102 (Fig. 1) can associate a network identification, such as an IP or MAC address, and the like, to this computer.

Next, in step 508, server 102 (Fig. 1) can send a message to the computer. The message can include information such as information that the computer has been properly identified and sequenced, and the like, and the message can include a command such as a command that the computer produce a signal indicating that the computer has been properly identified and sequenced.

In step 510, the computer being identified produces a signal. The signal produced by the computer can be detectable by an operator in some manner, such as visibly, audibly, and the like. For instance, the signal can include activating a light, activating a light emitting diode (LED), manipulateing the display on an integral LCD, manipulating the display on an integral display panel, ejecting or reinserting a CD-ROM, emitting an auditory sound, and the like. Activating a light or a to LED can include illuminating the light or LED, flashing the light or LED, and the like.

It should be recognized, however, that step 508 and/or step 510 may be omitted in some applications, such as when server 102 (Fig. 1) provides an indication that the computer has been properly identified. For instance, when a computer fails to send a heartbeat message, the server can emit a signal that can notify an operator that the computer has been properly identified and seqenced.

In step 512 of the present embodiment, identification and sequencing information gathered about the computers can be used to assign network identification, such as an IP address, and the like, to the computers in an ordered sequence. However, it should be recognized that step 512 may be omitted in some applications, such as when the computers have already been assigned proper network addresses.

With reference now to Fig. 6, a group of computers 100 connected to server 102 is shown. The following is an example of a process of identifying the computers in the group of computers 100. In particular, assume computers 600, 602, and 604 have already been identified. Specifically, assume computer 600 emitted a signal indicating that it was ready to be identified by activating its floppy light 106, 116. Then, an operator activated the power button 108, 112 on computer 600 in order to manipulate computer 600. After computer 600 was successfully identified, computer 600 emitted a sound 110, indicating that identification was successful.

Similarly, assume computers 602 and 604 have also been identified by server 102. In particular, assume computer 602 emitted a signal indicating that it was ready to be identified by activating its floppy light 106, 116. Then, an operator ejected a floppy disk 108, 118 from computer 602 in order to manipulate computer 602. After computer 602 was successfully identified, computer 602 emitted a sound 110, indicating that identification was successful.

Furthermore, assume computer 604 emitted a signal indicating that it was ready to be identified by activating its floppy light 106, 116. Then, an operator ejected a floppy disk 108, 118 from computer 604 in order to manipulate computer 604. After computer 604 was successfully identified, computer 604 emitted a sound 110, indicating that identification was successful.

In the present embodiment, assume computers 606, 608, 610, 612, 614, and 616 are waiting to be identified by server 102.

In each of the above-described embodiments, the state of a computer can be physically manipulated in various ways. In particular, the state of a computer can be manipulated by manipulating any device, switch, interface, signal, and the like, that is connected to or part of the computer, and that is detectable by server 102 either directly or through a message generated by software on the computer. For example, physically manipulating a computer can include inserting or ejecting a floppy disk (118, 120), CD-ROM disk, and the like, into or from the computer. Another way that a computer can be physically manipulated includes manipulating computer hardware, such as by moving a mouse, manipulating buttons or keys such as the power button (112), suspend button, reboot button, hotkey, keyboard key, and the like. In addition, a computer can be physically manipulated by attaching or removing a peripheral device, such as a keyboard, a mouse, dongle, serial device, parallel device, USB device, secondary network interface cable or card, and the like. Furthermore, a computer can be physically manipulated by attaching or removing a device, such as a keyboard, mouse, and the like, to or from any connector, such as a USB port, serial port, parallel port, Ethernet, other communications port, and the like. In addition, a computer can be physically manipulated by detaching a primary network cable, card, network interface device, and the like, where the detachment may be for a particular length of time, or may be detached until the entire set of computers has been identified and sequenced. Furthermore, a computer can be physically manipulated by a communication with an infrared port on the computer, or disconnecting the communications cable, card, network interface device, and the like, such as an Ethernet cable or card, while the server and computer or exchanging heartbeat messages. Moreover, a computer can be physically manipulated by inserting or ejecting a hot plug device, such as a hard drive, PCMCIA device, and the like.

Although the present invention has been described with respect to certain embodiments, examples, and applications, it will be apparent to those skilled in the art that various modifications and changes may be made without departing from the invention.

CLAIMS

We claim:

1. A method of identifying a computer among a group of computers connected to a server, wherein each computer in the group of computers has a network identification, the method comprising:

physically manipulating the computer to be identified,

wherein the computer is already turned on when the computer is physically manipulated;

sending a signal to the server that the computer has been physically manipulated,

wherein said signal includes network identification for the computer, or other data that can be used to obtain that network identification;

receiving said signal from the computer at the server; and

associating the network identification in said received signal with the physically manipulated computer.

2. The method of claim 1, wherein said network identification includes an IP address.

3. The method of claim 1, wherein said network identification includes an MAC address.

4. The method of claim 1, further comprising storing said association.

5. The method of claim 1, further comprising emitting a signal indicating that the network identification associated with said received signal has been properly associated with the physically manipulated computer.

6. The method of claim 5, wherein said emitted signal is visible to an operator.

7. The method of claim 5, wherein said emitted signal is audible to an operator.

8. The method of claim 1, further comprising emitting a signal indicating that the computer to be identified is ready to be physically manipulated.

9. The method of claim 8, wherein said emitted signal is visible to an operator.

10. The method of claim 8, wherein said emitted signal is audible to an operator.

11. The method of claim 1, wherein said physically manipulating includes inserting a disk into the computer to be identified.

12. The method of claim 1, wherein said physically manipulating includes removing a disk from the computer to be identified.

13. The method of claim 1, wherein said physically manipulating includes manipulating hardware of the computer to be identified.

14. The method of claim 1, wherein said physical manipulation includes attaching a peripheral device to the computer to be identified.

15. The method of claim 1, wherein said physical manipulation includes detaching a peripheral device from the computer to be identified.

16. The method of claim 1, wherein said physical manipulation includes communicating with an infra-red port on the computer to be identifed.

17. The method of claim 1,
wherein the group of computers is arranged in a rack, and
wherein each computer in the group of computers is sequentially identified.

18. A method of identifying a computer among a group of computers connected to a server, wherein each computer in the group of computers has a network identification, the method comprising:

detecting a physical manipulation to the computer to be identified,
wherein said manipulation changes the state of the computer,
wherein said manipulation occurs after the computer is turned on; and
sending a signal to the server that the computer has been manipulated,

wherein said signal can be associated with a network identification for the computer.

19. The method of claim 18, further comprising emitting a signal indicating that the computer is ready to be identified.

20. The method of claim 19, wherein said emitting includes activating a light.

21. The method of claim 19, wherein said emitting includes activating a light emitting diode.

22. The method of claim 19, wherein said emitting includes ejecting a CD-ROM.

23. The method of claim 19, wherein said emitting is visible to an operator.

24. The method of claim 19, wherein said emitting includes producing a sound.

25. The method of claim 19, wherein said emitting is audible to an operator.

26. The method of claim 18, further comprising:

receiving a signal from the server indicating that the network identification associated with said signal has been properly associated with the physically manipulated computer; and

emitting a signal in response to said receiving,

wherein said signal indicates that the computer has been properly associated by the server.

27. The method of claim 26, wherein said emitting includes activating a light.

28. The method of claim 26, wherein said emitting includes activating a light emitting diode.

29. The method of claim 26, wherein said emitting includes ejecting a CD-ROM.

30. The method of claim 26, wherein said emitting is visible to an operator.

31. The method of claim 26, wherein said emitting includes producing a sound.

32. The method of claim 26, wherein said emitting is audible to an operator.

33. The method of claim 18, wherein said signal sent to the server includes failing to send a heartbeat message.

34. The method of claim 18,
wherein the group of computers is arranged in a rack, and
wherein each computer in the group of computers is sequentially identified.

35. A method of identifying a computer among a group of computers connected to a server, wherein each computer in the group of computers has a network identification, the method comprising:
physically manipulating the computer to be identified,
wherein said manipulation changes the state of the computer,
wherein said manipulation occurs after the computer is turned on; and
receiving a signal from the computer indicating that the physically manipulated computer has been properly associated with a network identification.

36. The method of claim 35, wherein said physically manipulating includes inserting a disk into the client computer.

37. The method of claim 36, wherein said disk includes a floppy disk.

38. The method of claim 36, wherein said disk includes a CD-ROM.

39. The method of claim 35, wherein said physically manipulating includes removing a disk from the computer to be identified.

40. The method of claim 35, wherein said physically manipulating includes manipulating hardware of the computer to be identified.

41. The method of claim 40, wherein said manipulating hardware includes moving a mouse connected to the computer to be identified.

42. The method of claim 40, wherein said manipulating hardware includes manipulating a button on the computer to be identified.

43. The method of claim 42, wherein said manipulating a button includes manipulating a power button on the computer to be identified.

44. The method of claim 42, wherein said manipulating a button includes manipulating a suspend button on the computer to be identified.

45. The method of claim 42, wherein said manipulating a button includes manipulating a reboot button on the computer to be identified.

46. The method of claim 40, wherein said manipulating hardware includes manipulating a key.

47. The method of claim 46, wherein said key is a hotkey.

48. The method of claim 46, wherein said key is a keyboard key.

49. The method of claim 35, wherein said physically manipulating includes attaching a peripheral device to the computer to be identified.

50. The method of claim 35, wherein said physically manipulating includes detaching a peripheral device from the computer to be identified.

51. The method of claim 35, wherein said physically manipulating includes detaching a primary network cable connected to the computer to be identified.

52. The method of claim 35, wherein said physically manipulating includes detaching a card connected to the computer to be identified.

53. The method of claim 35, wherein said physically manipulating includes detaching a network interface device connected to the computer to be identified.

54. The method of claim 35, wherein said physically manipulating includes communicating with an infra-red port on the computer to be identified.

55. The method of claim 35, wherein said physically manipulating includes manipulating a hot plug device.

56. The method of claim 55, wherein said manipulating includes ejecting.

57. The method of claim 55, wherein said manipulating includes inserting.

58. The method of claim 55, wherein said hot plug device includes a hard drive.

59. The method of claim 55, wherein said hot plug device includes a PCMCIA device.

60. The method of claim 35,

wherein the group of computers is arranged in a rack, and

wherein each computer in the group of computers is sequentially identified.

61. A method of identifying a computer among a group of computers connected to a server, wherein each computer in the group of computers has a network identification, the method comprising:

receiving a signal from the computer to be identified,

wherein said signal indicates that the computer has been physically manipulated,

wherein said signal can be associated with a network identification for the computer;

associating the network identification associated with said received signal with the computer that has been physically manipulated.

62. The method of claim 61, wherein said network identification includes an IP address.

63. The method of claim 61, wherein said network identification includes a MAC address.

64. The method of claim 61, further comprising storing said association.

65. The method of claim 61, wherein said signal includes failing to send a heartbeat message.

66. The method of claim 61,
wherein the group of computers is arranged in a rack, and
wherein each computer in the group of computers is sequentially identified.

67. A system for identifying a computer among a group of computers connected to a server, wherein each computer in the group of computers has network identification, the system comprising:

a group of computers to be identified, each said computer configured to:

detect a physical manipulation to the computer,

send a signal to the server indicating that the computer has been manipulated,

wherein said signal includes data which can be associated with a network identification for the computer; and

a server configured to:

receive a signal from each computer in said group,

wherein said signal indicates that the computer sending the signal has been manipulated,

wherein said signal includes data which can be assocaited with a network identification for the manipulated computer,

associate the network identification associated with said sent and received signals with the manipulated computer.

68. The system of claim 67, wherein said server is further configured to store an association of the network identification associated with said sent and received signals with the manipulated computer.

69. The system of claim 67, wherein each computer in said group is further configured to emit a signal indicating that the computer is ready to be identified.

70. The system of claim 67, wherein each computer in said group is further configured to emit a signal indicating that the computer has been properly associated with a network identification.

71. The system of claim 67, wherein said server is further configured to send a signal to each computer in said group indicating that the computer has been properly associated with a network identification.

72. The system of claim 71, wherein said server is further configured to send a signal to each computer in said group requesting that the computer emit a signal indicating that the computer has been properly associated with a network identification.

73. The system of claim 67, wherein said server is further configured to:

sequentially receive a signal from each computer in the group,

associate the network identification in said received signal with an manipulated computer.

74. A system for identifying a computer in a group of computers, wherein each computer in the group of computers has a network identification, the system comprising:

a group of computers,

wherein each computer in said group is connected to a server,

wherein each computer is turned on; and

said server configured to:

detect each computer that has been physically manipulated, and associate a network identification with a physically manipulated computer.

75. The system of claim 74, wherein said server is configured to detect by receiving a network identification for the physically manipulated computer.

76. The system of claim 75, wherein said network identification includes an IP address.

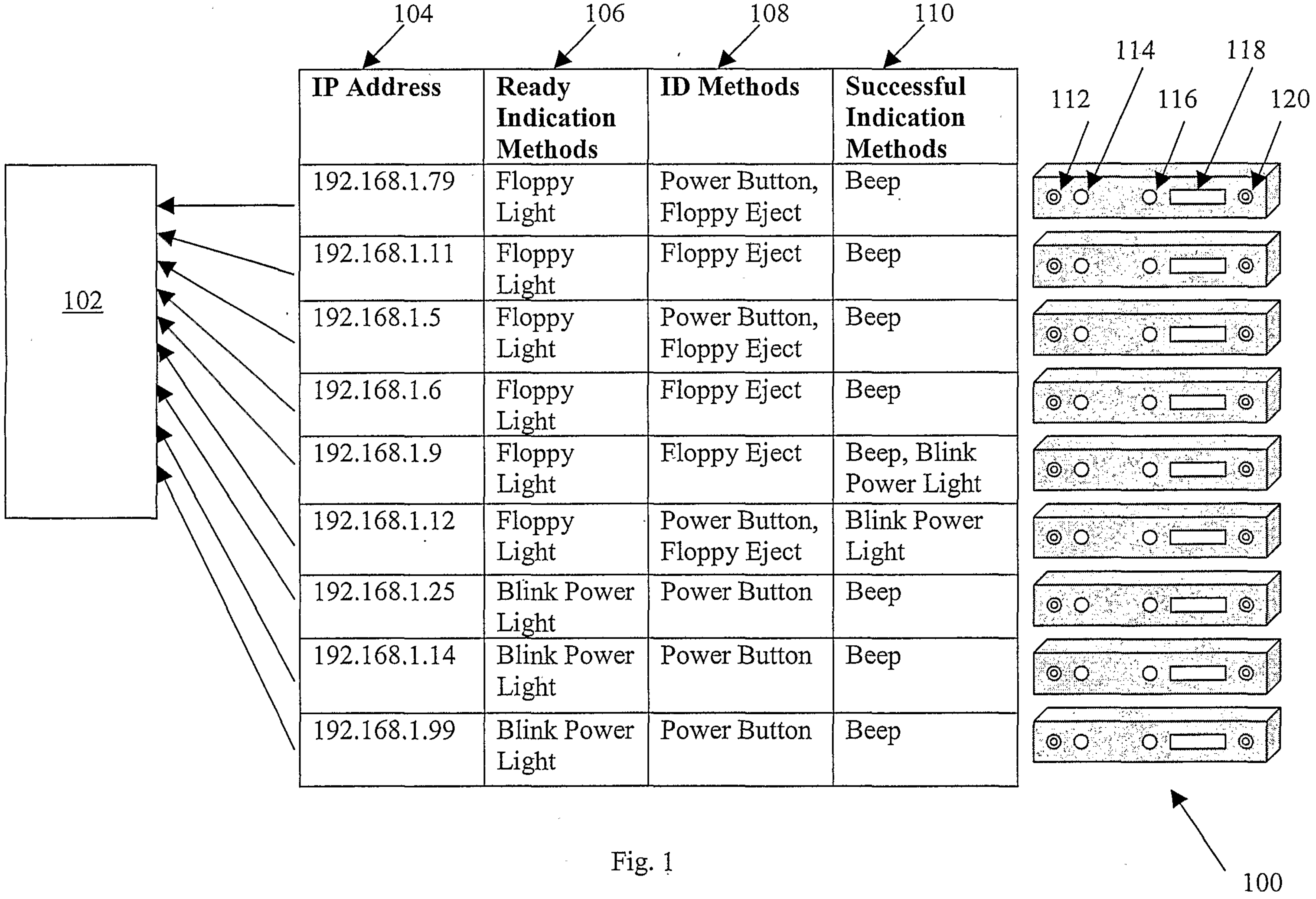
77. The system of claim 74, wherein said network identification includes an IP address.

78. The system of claim 74, wherein said network identification includes a MAC address.

79. The system of claim 74, wherein said server is further configured to :

sequentially detect each computer that has been physically manipulated, and

sequentically associate a network identification with a physically manipulated computer.



IP Address	Ready Indication Methods	ID Methods	Successful Indication Methods
192.168.1.79	Floppy Light	Power Button, Floppy Eject	Beep
192.168.1.11	Floppy Light	Floppy Eject	Beep
192.168.1.5	Floppy Light	Power Button, Floppy Eject	Beep
192.168.1.6	Floppy Light	Floppy Eject	Beep
192.168.1.9	Floppy Light	Floppy Eject	Beep, Blink Power Light
192.168.1.12	Floppy Light	Power Button, Floppy Eject	Blink Power Light
192.168.1.25	Blink Power Light	Power Button	Beep
192.168.1.14	Blink Power Light	Power Button	Beep
192.168.1.99	Blink Power Light	Power Button	Beep

Fig. 1

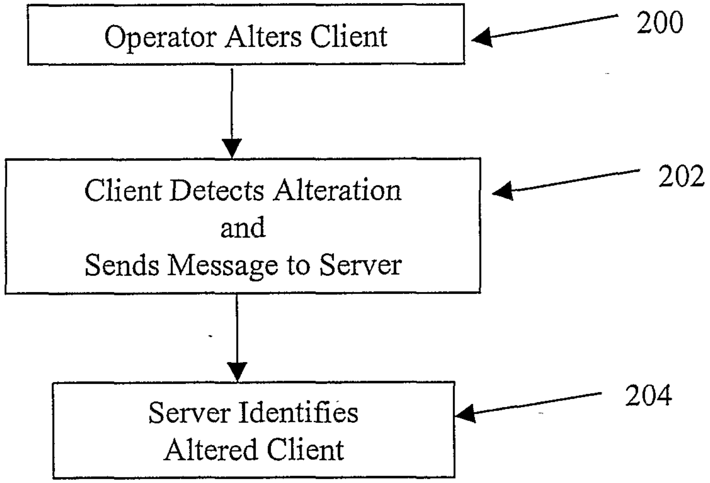

Operator Alters Client
200
Client Detects Alteration
and
Sends Message to Server
202
Server Identifies
Altered Client
204

Fig. 2

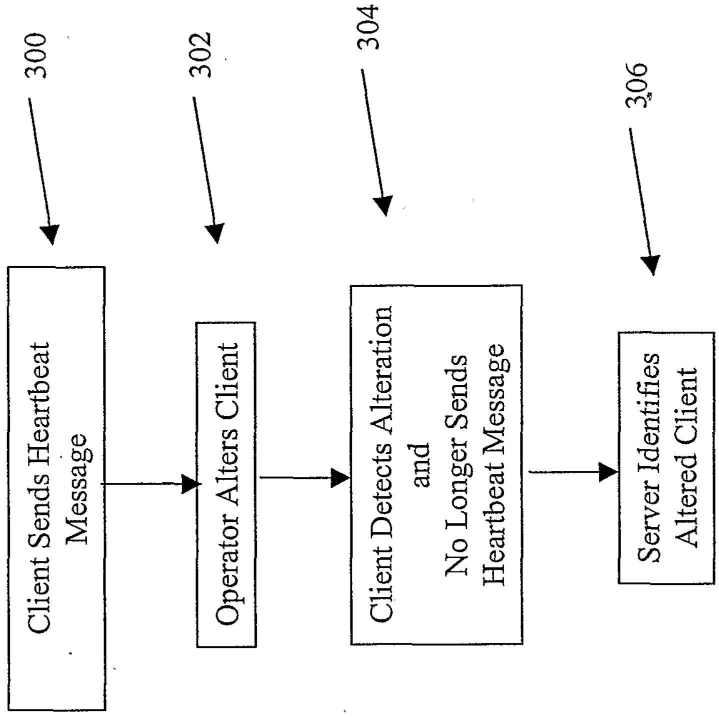

300
Client Sends Heartbeat Message
302
Operator Alters Client
304
Client Detects Alteration and No Longer Sends Heartbeat Message
306
Server Identifies Altered Client

Fig. 3

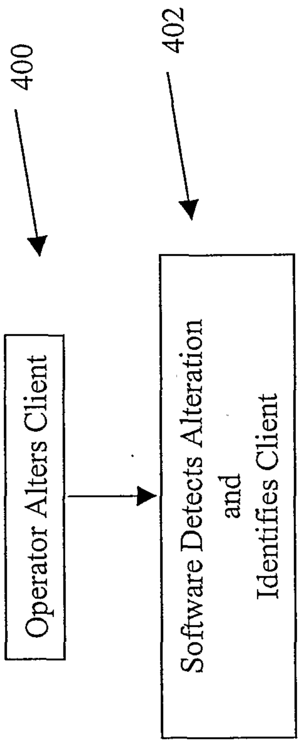

400
402
Operator Alters Client
Software Detects Alteration
and
Identifies Client

Fig. 4

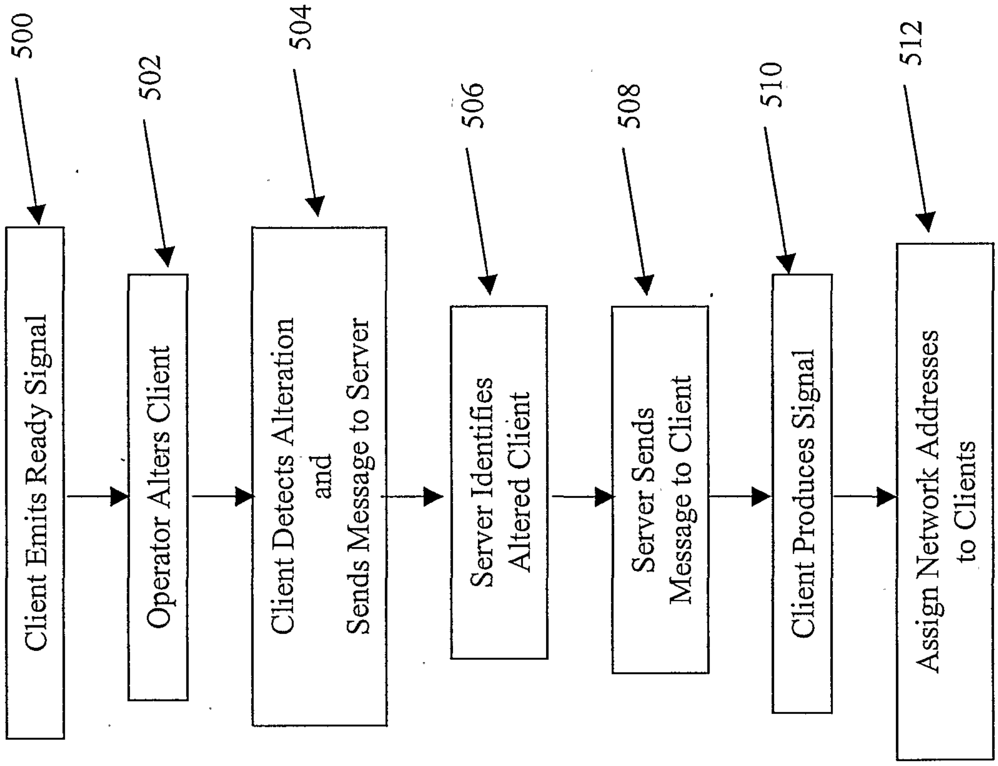
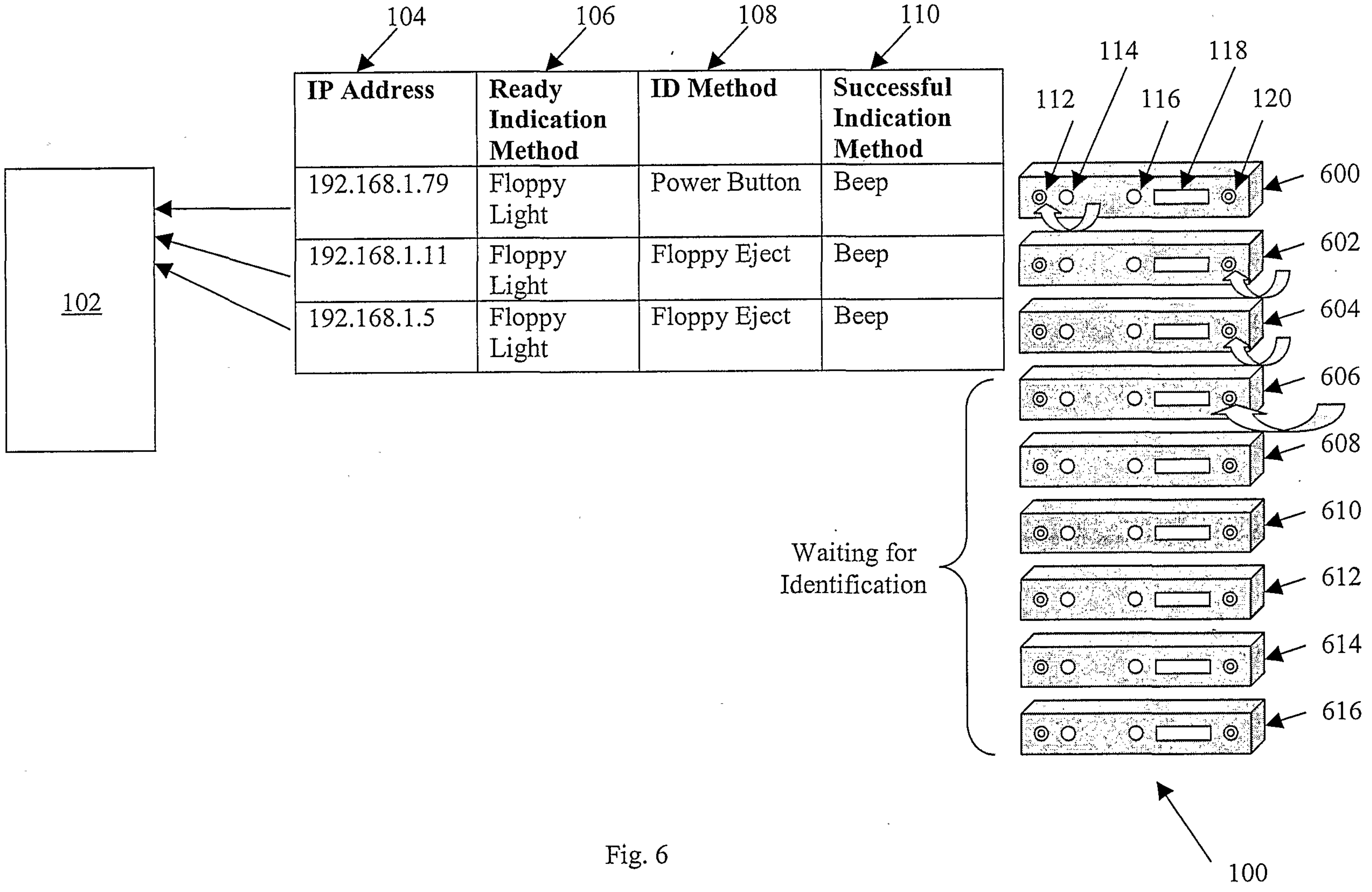

500
Client Emits Ready Signal
502
Operator Alters Client
504
Client Detects Alteration and Sends Message to Server
506
Server Identifies Altered Client
508
Server Sends Message to Client
510
Client Produces Signal
512
Assign Network Addresses to Clients

Fig. 5



IP Address	Ready Indication Method	ID Method	Successful Indication Method
192.168.1.79	Floppy Light	Power Button	Beep
192.168.1.11	Floppy Light	Floppy Eject	Beep
192.168.1.5	Floppy Light	Floppy Eject	Beep

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US02/20029

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 15/00
US CL : 709/220, 221, 222; 713/151, 153, 200
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 709/220, 221, 222; 713/151, 153, 200

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WEST - network identification; physically changing

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6,023,727 A (BARRETT et al) 08 February 2000 (08.02.2000), column 3, line 58 to column 29, line 67.	1-79
Y, P	US 6,286,039 B1 (VAN HORNE et al) 04 September 2001 (04.09.2001), column 10, line 39 to column 24, line 23.	1-79
Y	US 5,894,557 A (BADE et al) 13 April 1999 (13.04.1999), column 5, line 23 to column 15, line 46.	1-76

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

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

25 September 2002 (25.09.2002)

Date of mailing of the international search report

28 OCT 2002

Name and mailing address of the ISA/US

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

Facsimile No. (703)305-3230

Authorized officer

for
Matthew Smithers James R. Matthews

Telephone No. (703) 305-3900