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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 May 2001 (31.05.2001)

PCT

(10) International Publication Number
WO 01/38991 A1

(51) International Patent Classification[7]: G06F 13/00, 15/00

(21) International Application Number: PCT/IL00/00747

(22) International Filing Date:
15 November 2000 (15.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
133116 24 November 1999 (24.11.1999) IL

(71) Applicant *(for all designated States except US)*: **NET-SAFE COMMUNICATION LTD.** [IL/IL]; Goshen Street 57, 26313 Kiryat Motzkin (IL).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **RAZ, Alon** [IL/IL]; Gilboa Street 53, 32711 Haifa (IL).

(74) Agent: **MILLER - SIERADZKI, ADVOCATES & PATENT ATTORNEYS**; P.O. Box 6145, 31061 Haifa (IL).

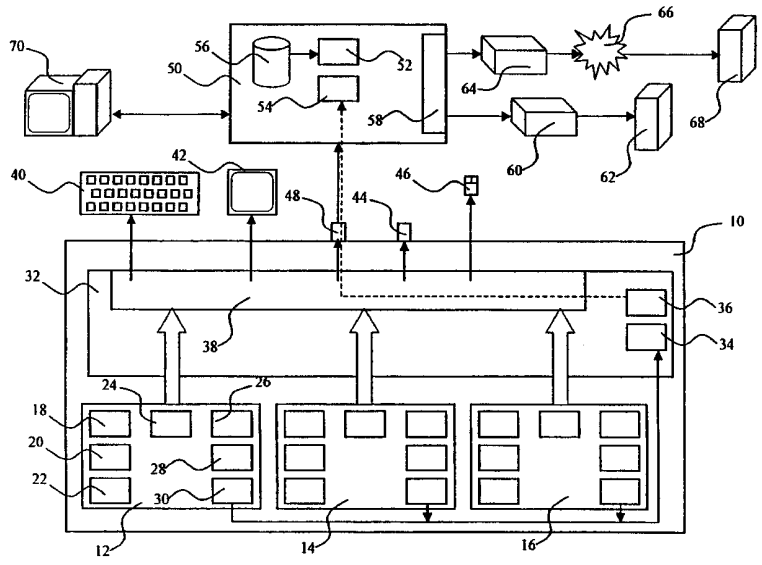
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE,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

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, 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, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

[Continued on next page]

(54) Title: METHODS AND APPARATUS FOR PROVIDING SECURE MULTIPLE-NETWORK ACCESS AT A SINGLE WORKSTATION



(57) Abstract: Apparatus and methods for providing secure multiple-network access at single workstation are disclosed. The apparatus includes a subcomputer assembly platform (10), a plurality of subcomputer assemblies includes a central processing unit (CPU) (18), and a network adapter (20), a network connection, a local control unit (32), for selectably connecting any one of the subcomputer assemblies to the network connction via its network adaptor (20) at any given time and a network control unit (32) for selectably connecting a first of the subcomputer assemblies to a first network and a second of the subcomputer assemblies to a second network, where each of the subcomputer assemblies operates in data isolation from every other of the subcomputer assemblies.

WO 01/38991 A1

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.

METHODS AND APPARATUS FOR PROVIDING SECURE MULTIPLE-NETWORK ACCESS AT A SINGLE WORKSTATION.

FIELD OF THE INVENTION

The present invention relates to network computing in general, and more particularly to methods and apparatus for providing secure multiple-network access at a single workstation.

BACKGROUND OF THE INVENTION

One of the main challenges today facing managers of private networks, such as Local Area Networks (LANs), is giving their authorized computer users access to both private networks and public networks, such as the Internet, while keeping confidential or restricted private network information from being copied to or otherwise accessed from the public network. Although technologies, such as firewalls, exist that prevent access to private networks from intruders, they are mainly intended to keep people out and do little to prevent private network users from transmitting confidential data. These technologies are also susceptible to break-ins by intruders who bypass hardware and software security measures that organizations use to protect their data. The problem has become so acute that many organizations, especially military and governmental organizations and companies who work with them, simply do not allow their users to access public networks from their facilities or provide workstations and servers for public network access that are completely separate from those of the private network, usually placed in separate rooms and with separate communication lines, and usually shared among several users. These separate private/public

network access facilities are bothersome to use, requiring users who need to work on both private and public networks to physically move between workstations in order to do so.

SUMMARY OF THE INVENTION

The present invention seeks to provide methods and apparatus for providing secure multiple-network access at a single workstation that overcome disadvantages of the prior art described hereinabove. A workstation is provided having multiple subcomputer assemblies, each subcomputer assembly having its own central processing unit (CPU), memory, hard disk or other non-volatile storage device, basic input/output system (BIOS), network adapter, and display adapter. The subcomputer assemblies share a single keyboard, monitor, mouse, I/O ports, and other peripheral devices, as well as the same network connection, via a local control unit (LCU) which determines which of the subcomputer assemblies control of the workstation and its peripherals at any given time. Each subcomputer assembly runs independently of the other, and no facility is provided for data transfer between subcomputer assemblies. Given physically separate and thus data-isolated subcomputer assemblies, one or more assemblies may be dedicated for public network access while one or more other assemblies may be dedicated for private network access. This total separation between public and private network access provided within the context of a single workstation ensures that private network data is not copied to a public network, that intruders cannot access the private network via the public network, and that a computer user need not physically move between multiple workstations.

It is noted throughout the specification and claims that the term "data isolation" and variants thereof as used herein refers to the inability of a first CPU to transmit data to a second CPU and/or to store data directly to memory or other storage associated with a second

CPU due to absence of a communication channel between the first CPU and the second CPU, its memory, or its storage.

There is thus provided in accordance with a preferred embodiment of the present invention apparatus for providing secure multiple-network access at single workstation, the apparatus including a subcomputer assembly platform, a plurality of subcomputer assemlies assembled with the subcomputer assembly platform, where each of the subcomputer assemlies Includes a central processing unit (CPU), and a network adapter, a network connection, a local control unit for selectably connecting any one of the subcomputer assemblies to the network connection via its network adapter at any given time and a network control unit for selectably connecting a first of the subcomputer assemblies to a first network and a second of the subcomputer assemblies to a second network, where each of the subcomputer assemblies operates in data isolation from every other of the subcomputer assemblies.

Further in accordance with a prreferred ambodiment of the present invention the subcomputer assemblies platform is operative to provide access to plurality of peripheral devices, and where any one of the subcomputer assemblies is operative to control any of the peripheral devices at any given time.

Still further in accordance with a preferred enbodiment of the present invention the network control unit is operative to selectably connect the first subcomputer assembly to the first network at a first time and the second subcomputer assembly to the second network at a second time.

Additionally in accordance with a preferred embodiment of the present invention the first network is a private network and where the second network is a public network.

Moreover in accordance with a preferred embodiment of the present invention the private network is a Local Area Network (LAN).

Further in accordance with a preferred embodiment of the present invention the public network is the Internet.

There is also provided in accordance with a preferred embodiment of the present invention apparatus for the providing secure multiple-network access at a single workstation, the apparatus including a motherboard including a central proccessing unit (CPU), a memory, a storage device having a first operating system, and a network adapter, a subcomputer assembly assembled with the motherboard, where the subcomputer assembly includes a memory including a second operating system, and a boot control program operative to selectably boot the workstation from either of the first operating system and the second operating system and disable the storage device when the workstation boots from the second operating system, a network connection, a local control unit for selectably connecting either of the motherboard and the subcomputer assembly to the network connection via the network adapter at any given time, and a network control unit for selectably connecting the motherboard to a first network and the subcomputer assembly to a second network, where the motherboard and the subcomputer assembly operate in data isolation from one another.

There is additionally provided in accordance with a preferred embodiment of the present invention in a system including a subcomputer assembly platform, a plurality of subcomputer assemblies assembled with the subcomputer assembly platform, where eacv of the subcomputer assemblies includes a central processing unit (CPU) and a network adapter, a network connection, and a plurality of networks, a method for providing secure multiple-network access, the method including the steps of operating each of the subcomputer assemblies in data isolation from every other of the subcomputer assemblies, selectably

connecting a first one of the subcomputer assemblies to the network connection via its network adapter, and selectably connecting the first subcomputer assembly to a first one of the plurality of networks.

Further in accordance with a preferred embodiment of the present invention the method further includes the steps of selectably disconnecting the first subcomputer assembly from the first network, selectably connecting a second one of the subcomputer assemblies to the network connection via its network adapter and selectably connecting the second subcomputer assembly to a second one of the plurality of networks.

Still further in accordance with a preferred embodiment of the present invention the subcomputer assembly platform is operative to provide access to a plurality of peripheral devices, and further including the step of providing the first subcomputer assembly with control of any of the peripheral devices.

Additionally in accordance with a preferred embodiment of the present invention the first one of the plurality of networks is a private network and where the second one of the plurality of networks is a public network.

Moreover in accordance with a preferred embodiment of the present invention the private network is a Local Area Network (LAN).

Further in accordance with a preferred embodiment of the present invention the public network is the Internet.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description taken in conjunction with the appended drawings in which:

Fig. 1 is a simplified illustration of a system for providing secure multiple-network access at a single workstation, constructed and operative in accordance with a preferred embodiment of the present invention;

Fig. 2 is a simplified flowchart illustration of a method of operation of the system of Fig. 1, operative in accordance with a preferred embodiment of the present invention;

Fig. 3 is a simplified illustration of a system for providing secure multiple-network access at a single workstation, constructed and operative in accordance with another preferred embodiment of the present invention; and

Fig. 4 is a simplified flowchart illustration of a method of operation of the system of Fig. 3, operative in accordance with a preferred embodiment of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Reference is now made to Fig. 1 which is a simplified illustration of a system for providing secure multiple-network access at a single workstation, constructed and operative in accordance with a preferred embodiment of the present invention. In Fig. 1 a workstation 10 acts as a subcomputer assembly platform having several subcomputer assemblies (SAs) 12, 14, and 16 assembled therewith. Although only one workstation 10 is shown, it is appreciated that the present invention may include multiple workstations configured as described hereinbelow. Each of the SAs 12, 14, and 16 typically includes a central processing unit (CPU) 18, a network adapter 20, a BIOS chipset 22, a display adapter 24, a memory 26, a storage device 28, and a control port 30. SAs 12, 14, and 16 are connected via control port 30 to a local control unit (LCU) 32 which preferably comprises a controller 34, a data modulation transmit/receive unit (DMU) 36, and an I/O switching unit 38 which connects any of the SAs 12, 14, and 16 to any peripheral devices that are connected to the subcomputer

assembly platform, such as a keyboard 40, a monitor 42, I/O ports 44, such as COM or LPT ports, a mouse 46, and a network connection 48. LCU 32 preferably selectably connects any one of subcomputer assemblies 12, 14, and 16 to network connection 48 via its network adapter 20 such that only one of subcomputer assemblies 12, 14, and 16 is connected to network connection 48 at any given time.

The term "network connection" as used herein refers to a single physical network path between an SA and a network, and not necessarily a single network connector or coupling. For example, although workstation 10 may be connected to a single RJ-45 jack housing 8-wire category 5 network cabling, only one SA may use all 8 wires at a given time, such as in 100BaseT full duplex networks. Alternatively, one SA may use 4 of the 8 wires at the same time that another SA uses the other 4 of the 8 wires, such as in 10BaseT half duplex networks.

A network control unit (NCU) 50 is preferably connected workstation 10 via network connection 48. NCU 50 preferably includes a control unit 52 for controlling NCU 50, a data modulation transmit/receive unit (DMU) 54, a user rights database 56, and a switching bank 58 which connects NCU 50 to any of several network hubs/switches 60 or routers 64, which in turn are connected to one or more network servers 62 and 68, either directly such as in a private network arrangement, as with hub 60 and server 62, or via a connection with a remote server such as in a public network arrangement, as with router 64 and server 68 connected via a network 66, such as the Internet. Communication between LCU 32 and NCU 50 is provided by DMUs 36 and 54 respectively via network connection 48 by modulating/demodulating data transmissions between them using known techniques. NCU 50 may itself be controlled by a computer 70. Multiple NCUs may also be used to control large numbers of workstations configured as described herein, and may be daisy-

chained and centrally controlled by computer 70 through access to any one of the NCUs.

Each of SAs 12, 14, and 16 preferably has its own operating system and network operation software and functions in data-isolation from any other SA. Each SA additionally includes SA control software that the SA executes and through which a user at workstation 10 may interact with the SA and "move between" SAs by requesting that one SA or another be given exclusive control over workstation 10's peripheral devices and be connected to a public or private network via network connection 48. In order to achieve true data-isolation, preferably only one SA in workstation 10 will be in control of workstation 10's peripheral devices and network connection 48 at any given time.

Reference is now made to Fig. 2 which is a simplified flowchart illustration of a method of operation of the system of Fig. 1, operative in accordance with a preferred embodiment of the present invention. In the method of Fig. 2 the SAs in a workstation operate independently and in data-isolation from other SAs, with one SA currently in control of the workstation's peripheral devices and the workstation's network connection (step 100). A user at the workstation instructs the control application running on the SA currently in control that he wishes to switch to another SA and connect to a network (step 110). The control application communicates this to the LCU which places the desired SA in control of the workstation (step 120). The LCU then informs the NCU which network the user's wishes to be connected to (step 130). The NCU then checks the user rights database to see in the requesting user and/or SA being selected is authorized to connect to the requested network (step 140). If so, the NCU switching bank opens a connection between the hub/switch and network server and the selected SA (step 150). If the requesting user and/or SA being selected is not authorized to connect to the requested network the connection request is refused (step 160).

Reference is now made to Fig. 3 which is a simplified illustration of a system for providing secure multiple-network access at a single workstation, constructed and operative in accordance with another preferred embodiment of the present invention. The system of Fig. 3 is similarly configured to that of Fig. 1 except as is noted hereinbelow. Workstation 10 is preferably configured with a motherboard 72 having a memory 74, a CPU 76, a network adapter 78, and a storage device 80 including an operating system. An SA 82 is also provided having a non-volatile memory 84 including its own operating system.

Reference is now made to Fig. 4 which is a simplified flowchart illustration of a method of operation of the system of Fig. 3, operative in accordance with a preferred embodiment of the present invention. In the method of Fig. 4 the workstation accesses SA 82 when booting and executes a control program stored on SA memory 84 (step 200). The control program asks the user whether he wishes to boot from the operating system on storage 80 or from the operating system on SA memory 84 (step 210). If the user chooses to boot from storage 80, the workstation boots normally and requests network access via the LCU and NCU as described hereinabove with reference to Fig. 2 (step 220). If the user chooses to boot from SA memory 84, the workstation boots from memory 84 and access to storage 80 is prevented, preferably through physical disconnection of storage 80 and/or power down of storage 80 (step 230). Operation thereafter of workstation 10 and SA 80 vis-a-vis the LCU and NCU are as described hereinabove with reference to Fig. 2, with the notable exception that both workstation 10 and SA 84 use the same network adapter for network access.

It is appreciated, with continuing reference to Figs. 3 and 4, that multiple SAs 82 may be assembled with workstation 10, with the boot control program asking the user which SA he wishes to boot from. Additionally or alternatively, one SA 82 may have multiple memories, each having its own operating system, in which case the user is asked which

memory he wishes to boot from. Additionally or alternatively, SA 82 may have one memory with multiple storage areas within the memory, with each storage area storing its own operating system, in which case the user is asked which memory storage area he wishes to boot from.

While the methods and apparatus disclosed herein may or may not have been described with reference to specific hardware or software, the methods and apparatus have been described in a manner sufficient to enable persons of ordinary skill in the art to readily adapt commercially available hardware and software as may be needed to reduce any of the embodiments of the present invention to practice without undue experimentation and using conventional techniques.

While the present invention has been described with reference to a few specific embodiments, the description is intended to be illustrative of the invention as a whole and is not to be construed as limiting the invention to the embodiments shown. It is appreciated that various modifications may occur to those skilled in the art that, while not specifically shown herein, are nevertheless within the true spirit and scope of the invention.

CLAIMS

What is claimed is:

1. Apparatus for providing secure multiple-network access at a single workstation, said apparatus comprising:

a subcomputer assembly platform;

a plurality of subcomputer assemblies assembled with said subcomputer assembly platform, wherein each of said subcomputer assemblies comprises:

a central processing unit (CPU); and

a network adapter;

a network connection;

a local control unit for selectably connecting any one of said subcomputer assemblies to said network connection via its network adapter at any given time; and

a network control unit for selectably connecting a first of said subcomputer assemblies to a first network and a second of said subcomputer assemblies to a second network,

wherein each of said subcomputer assemblies operates in data isolation from every other of said subcomputer assemblies.

2. Apparatus according to claim 1 wherein said subcomputer assembly platform is operative to provide access to a plurality of peripheral devices, and wherein any one of said subcomputer assemblies is operative to control any of said peripheral devices at any given time.

3. Apparatus according to claim 1 wherein said network control unit is operative to

selectably connect said first subcomputer assembly to said first network at a first time and said second subcomputer assembly to said second network at a second time

4. Apparatus according to claim 1 wherein said first network is a private network and wherein said second network is a public network.

5. Apparatus according to claim 4 wherein said private network is a Local Area Network (LAN).

6. Apparatus according to claim 4 wherein said public network is the Internet.

7. Apparatus for providing secure multiple-network access at a single workstation, said apparatus comprising:

a motherboard comprising:

a central processing unit (CPU);

a memory;

a storage device having a first operating system; and

a network adapter;

a subcomputer assembly assembled with said motherboard, wherein said subcomputer assembly comprises:

a memory comprising:

a second operating system; and

a boot control program operative to:

selectably boot said workstation from either of said first

operating system and said second operating system and

disable said storage device when said workstation boots from said second operating system;

a network connection;

a local control unit for selectably connecting either of said motherboard and said subcomputer assembly to said network connection via said network adapter at any given time; and

a network control unit for selectably connecting said motherboard to a first network and said subcomputer assembly to a second network,

wherein said motherboard and said subcomputer assembly operate in data isolation from one another.

8. In a system including a subcomputer assembly platform, a plurality of subcomputer assemblies assembled with said subcomputer assembly platform, wherein each of said subcomputer assemblies includes a central processing unit (CPU) and a network adapter, a network connection, and a plurality of networks, a method for providing secure multiple-network access, the method comprising the steps of:

operating each of said subcomputer assemblies in data isolation from every other of said subcomputer assemblies;

selectably connecting a first one of said subcomputer assemblies to said network connection via its network adapter; and

selectably connecting said first subcomputer assembly to a first one of said plurality of networks.

9. A method according to claim 8 and further comprising the steps of:

selectably disconnecting said first subcomputer assembly from said first network;

selectably connecting a second one of said subcomputer assemblies to said network connection via its network adapter; and

selectably connecting said second subcomputer assembly to a second one of said plurality of networks.

10. A method according to claim 8 wherein said subcomputer assembly platform is operative to provide access to a plurality of peripheral devices, and further comprising the step of providing said first subcomputer assembly with control of any of said peripheral devices.

11. A method according to claim 9 wherein said first one of said plurality of networks is a private network and wherein said second one of said plurality of networks is a public network.

12. A method according to claim 11 wherein said private network is a Local Area Network (LAN).

13. A method according to claim 11 wherein said public network is the Internet.

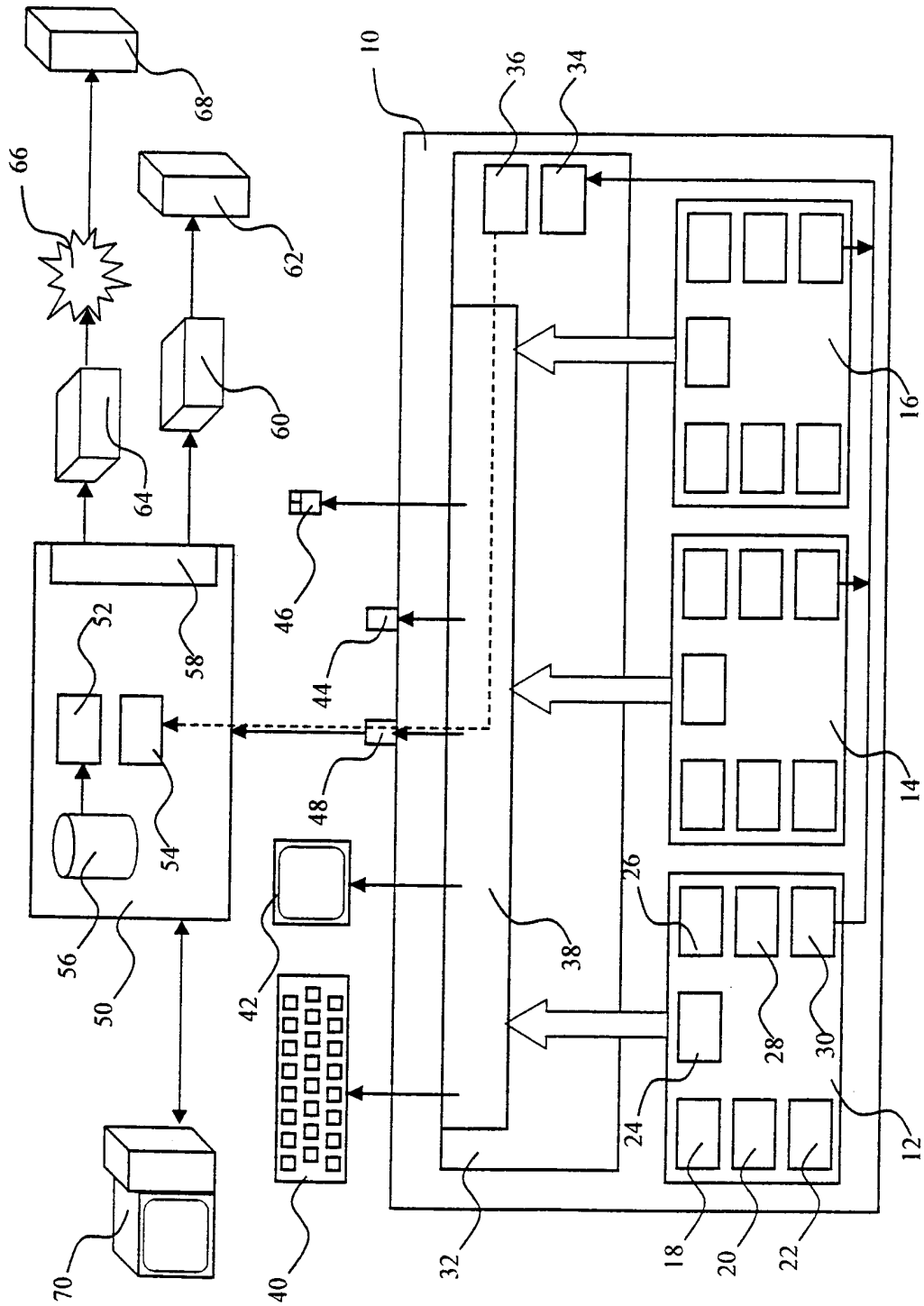

10
12
14
16
18
20
22
24
26
28
30
32
34
36
38
40
42
44
46
48
50
52
54
56
58
60
62
64
66
68
70

Fig. 1

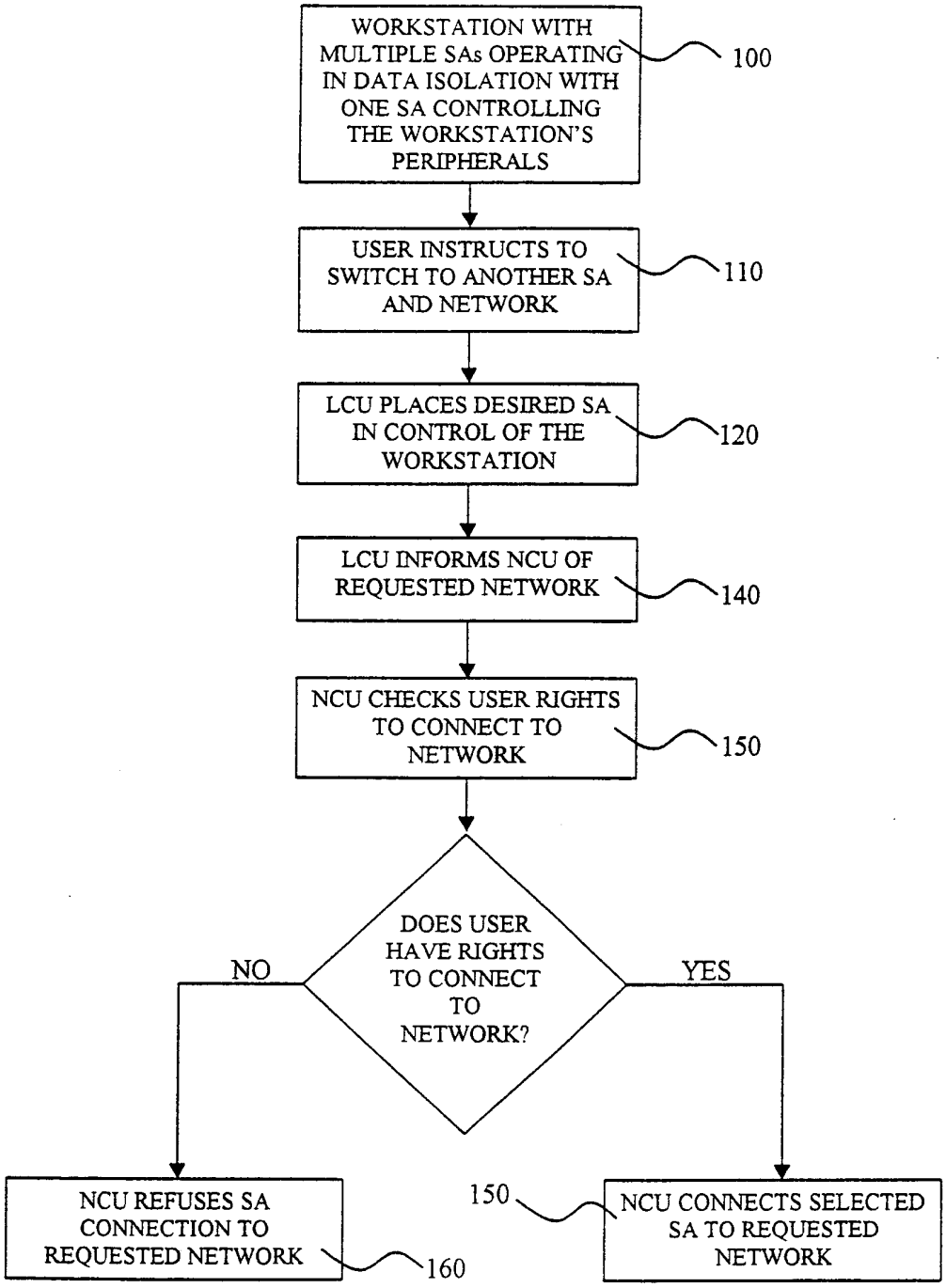

WORKSTATION WITH MULTIPLE SAs OPERATING IN DATA ISOLATION WITH ONE SA CONTROLLING THE WORKSTATION'S PERIPHERALS
100
USER INSTRUCTS TO SWITCH TO ANOTHER SA AND NETWORK
110
LCU PLACES DESIRED SA IN CONTROL OF THE WORKSTATION
120
LCU INFORMS NCU OF REQUESTED NETWORK
140
NCU CHECKS USER RIGHTS TO CONNECT TO NETWORK
150
DOES USER HAVE RIGHTS TO CONNECT TO NETWORK?
NO
YES
NCU REFUSES SA CONNECTION TO REQUESTED NETWORK
160
150
NCU CONNECTS SELECTED SA TO REQUESTED NETWORK

Fig. 2

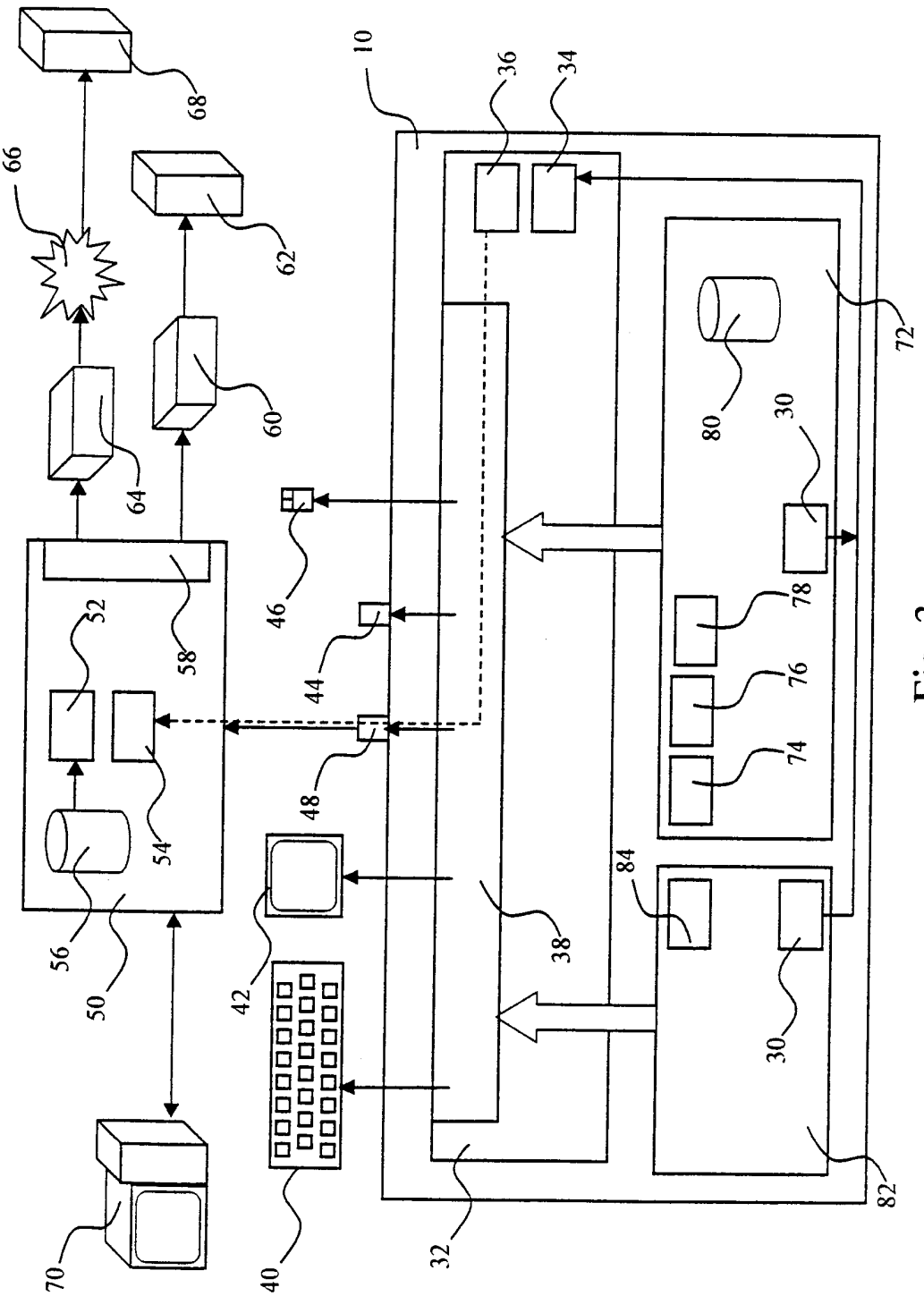

10
30
30
32
34
36
38
40
42
44
46
48
50
52
54
56
58
60
62
64
66
68
70
72
74
76
78
80
82
84

Fig. 3

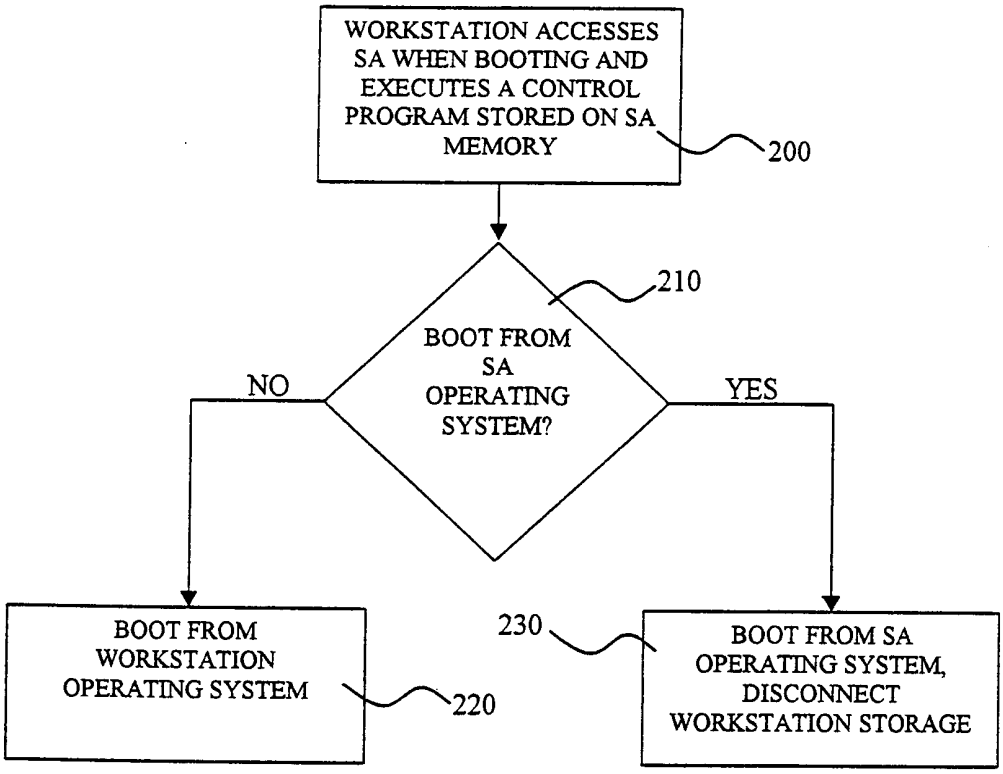

WORKSTATION ACCESSES SA WHEN BOOTING AND EXECUTES A CONTROL PROGRAM STORED ON SA MEMORY
200
BOOT FROM SA OPERATING SYSTEM?
210
NO
YES
BOOT FROM WORKSTATION OPERATING SYSTEM
220
230
BOOT FROM SA OPERATING SYSTEM, DISCONNECT WORKSTATION STORAGE

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL00/00747

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G0F6 13/00, 15/00
US CL : 709/200, 236

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. : 709/200, 236

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)

EAST, STN

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,764,918 A (POULTER) 09 June 1998, col.10, line 54-col.11, line 25.	1-13
Y	US 5,550,984 A (GELB) 27 August 1996, col. 4, line 56-col.7, line 39.	1-13

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

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

Date of the actual completion of the international search 22 MARCH 2001	Date of mailing of the international search report 27 APR 2001
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 FARZANEH FARAHI Telephone No. (703)308-6118

Form PCT/ISA/210 (second sheet) (July 1998)★