US 20110145451A1

(19) **United States**

(12) **Patent Application Publication**

Soffer et al.

(10) **Pub. No.: US 2011/0145451 A1**

(43) **Pub. Date: Jun. 16, 2011**

(54) **ISOLATED MULTI-NETWORK COMPUTER SYSTEM AND APPARATUS**

(75) Inventors: **Aviv Soffer**, Caesarea (IL); **Oleg Vaisband**, Kiryat Yam (IL)

(73) Assignee: **HIGH SEC LABS**, Tirat Carmel (IL)

(21) Appl. No.: **13/060,231**

(22) PCT Filed: **Aug. 19, 2009**

(86) PCT No.: **PCT/IL09/00815**

§ 371 (c)(1),
(2), (4) Date: **Feb. 22, 2011**

Related U.S. Application Data

(60) Provisional application No. 61/089,945, filed on Aug. 19, 2008.

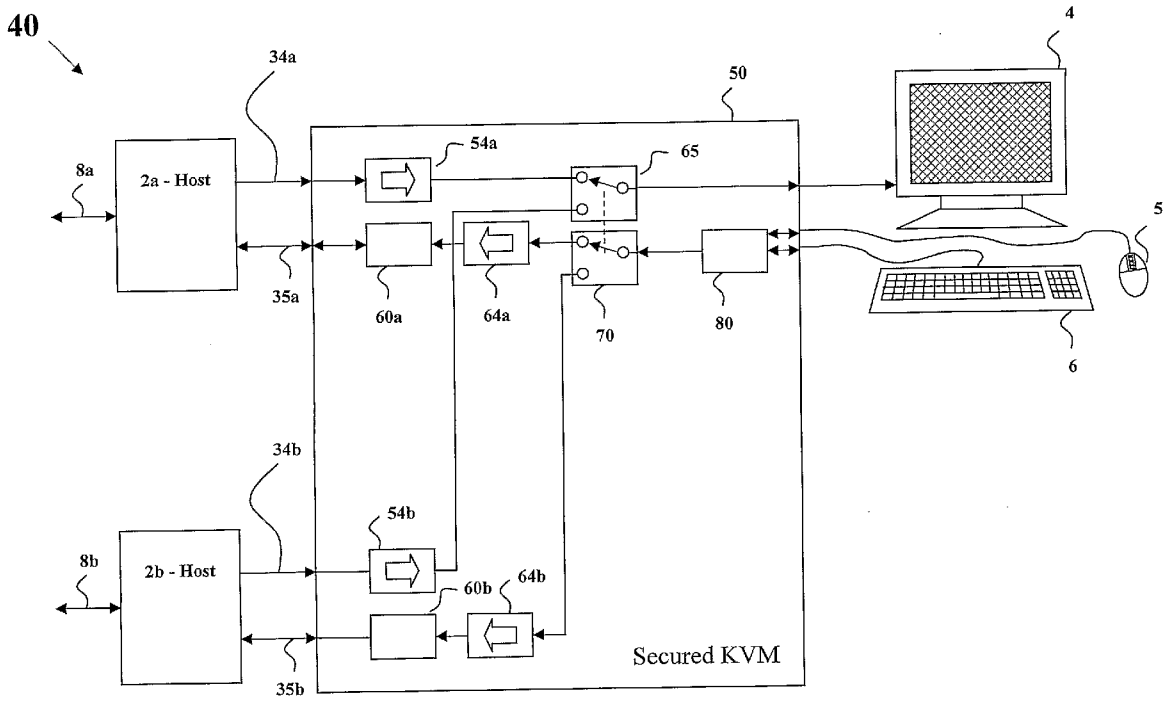
Publication Classification

(51) **Int. Cl.**
G06F 13/12 (2006.01)
G06F 21/04 (2006.01)

(52) **U.S. Cl.** **710/64**

(57) **ABSTRACT**

The present invention presents apparatuses and systems for operating multiple computers from a single console using a secured KVM device, while preventing information leakage between the computers. The system comprises several hosts connected through a secured KVM device to keyboard and mouse and one or more user displays. Secured KVM enables standard bi-directional communication between Secured KVM and user keyboard and mouse and between hosts peripheral ports and Secured KVM. Secured KVM physically enforces unidirectional data flow from attached keyboard and mouse to attached hosts peripheral ports to avoid potential leakages between hosts.



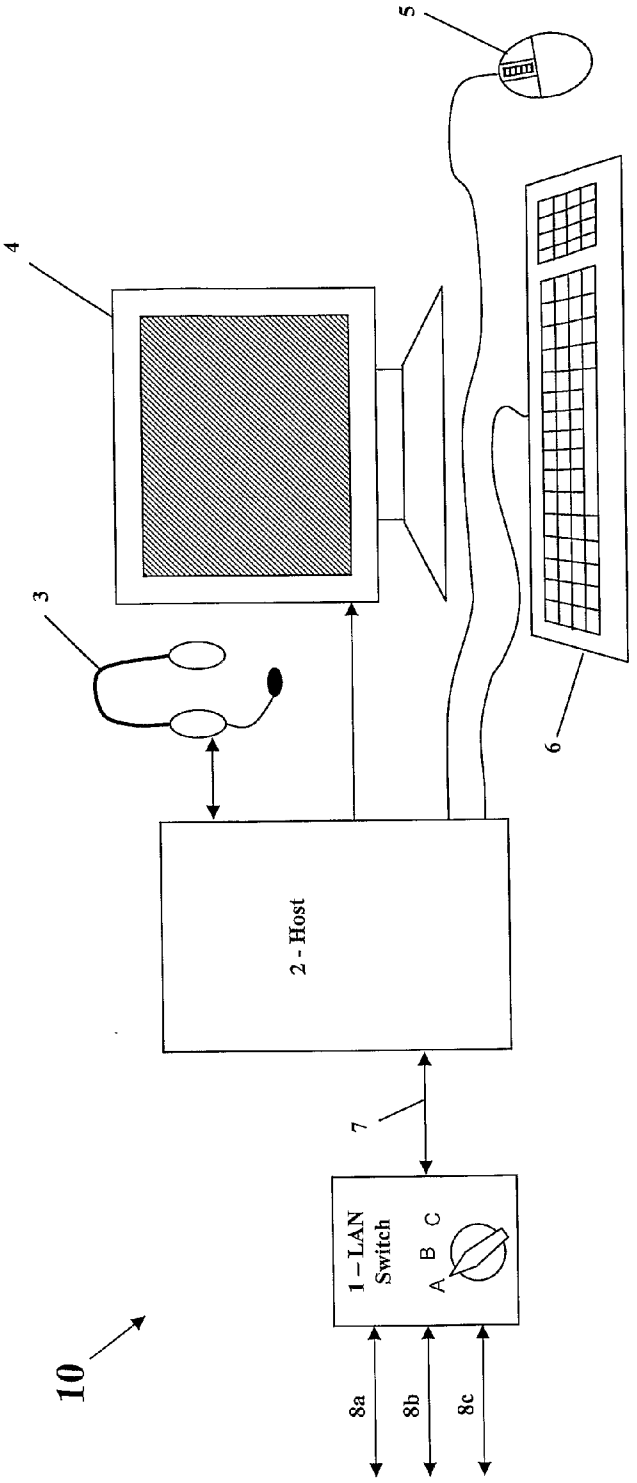


Figure 1 – Prior Art

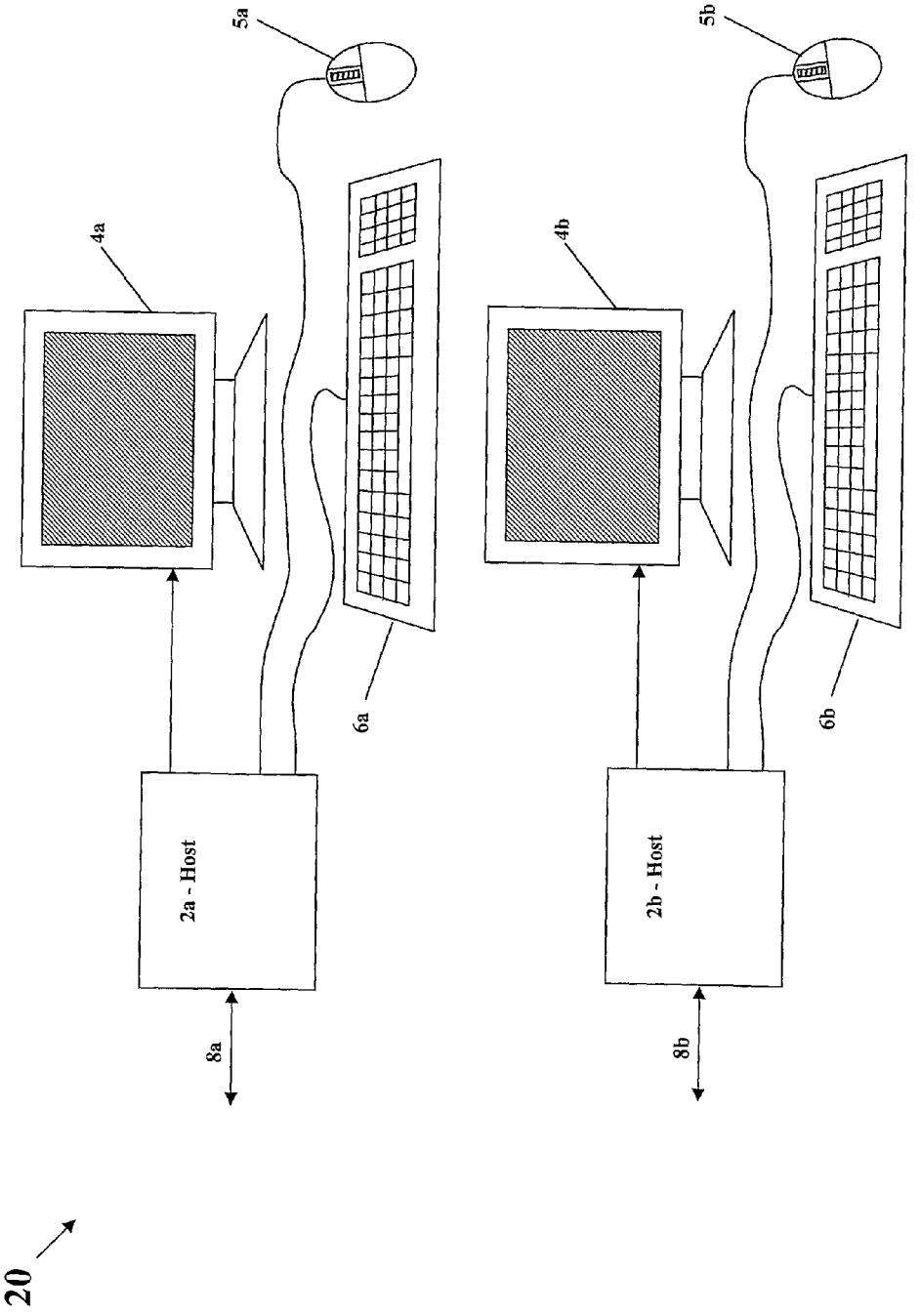


Figure 2 – Prior Art

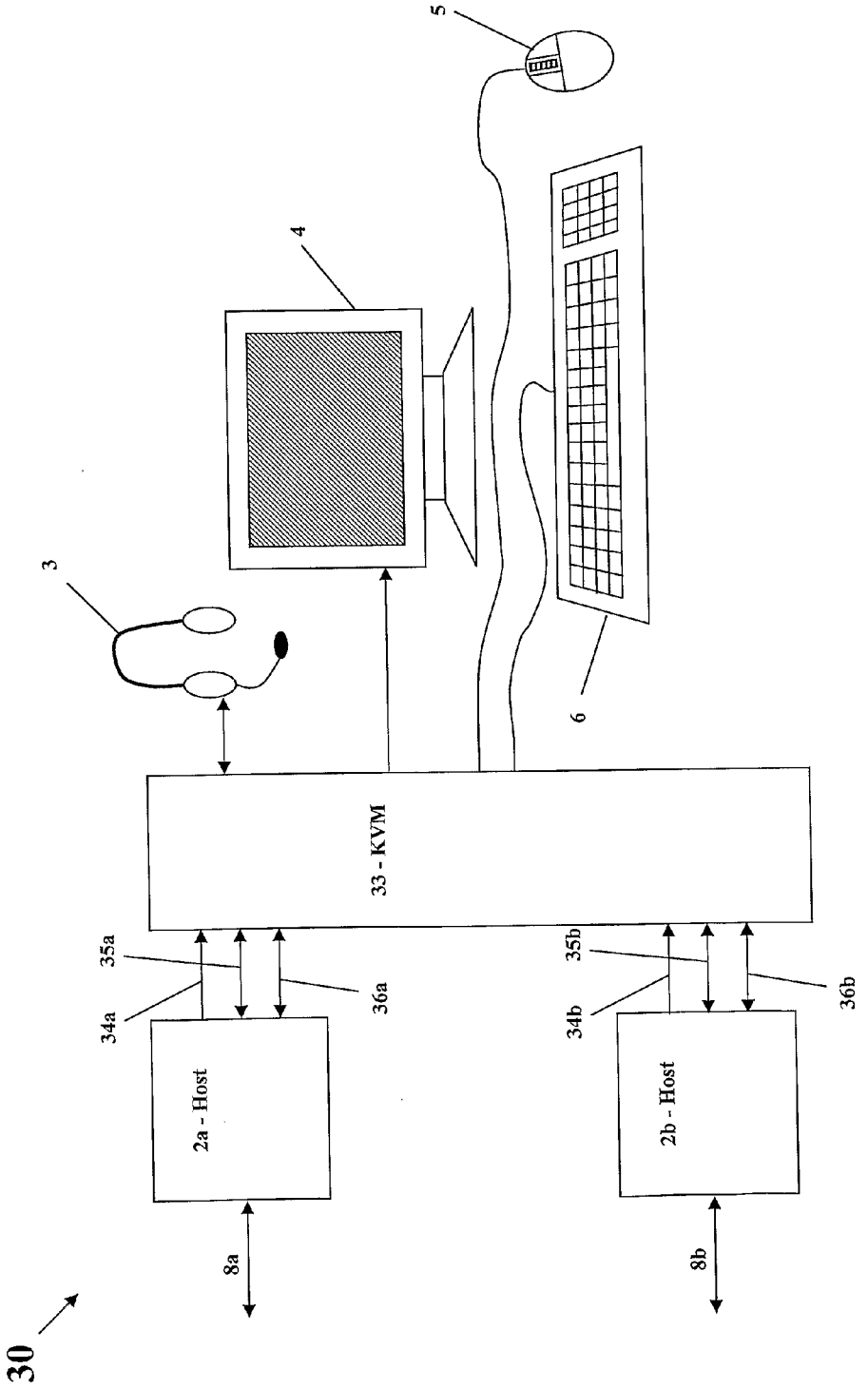


Figure 3 – Prior Art

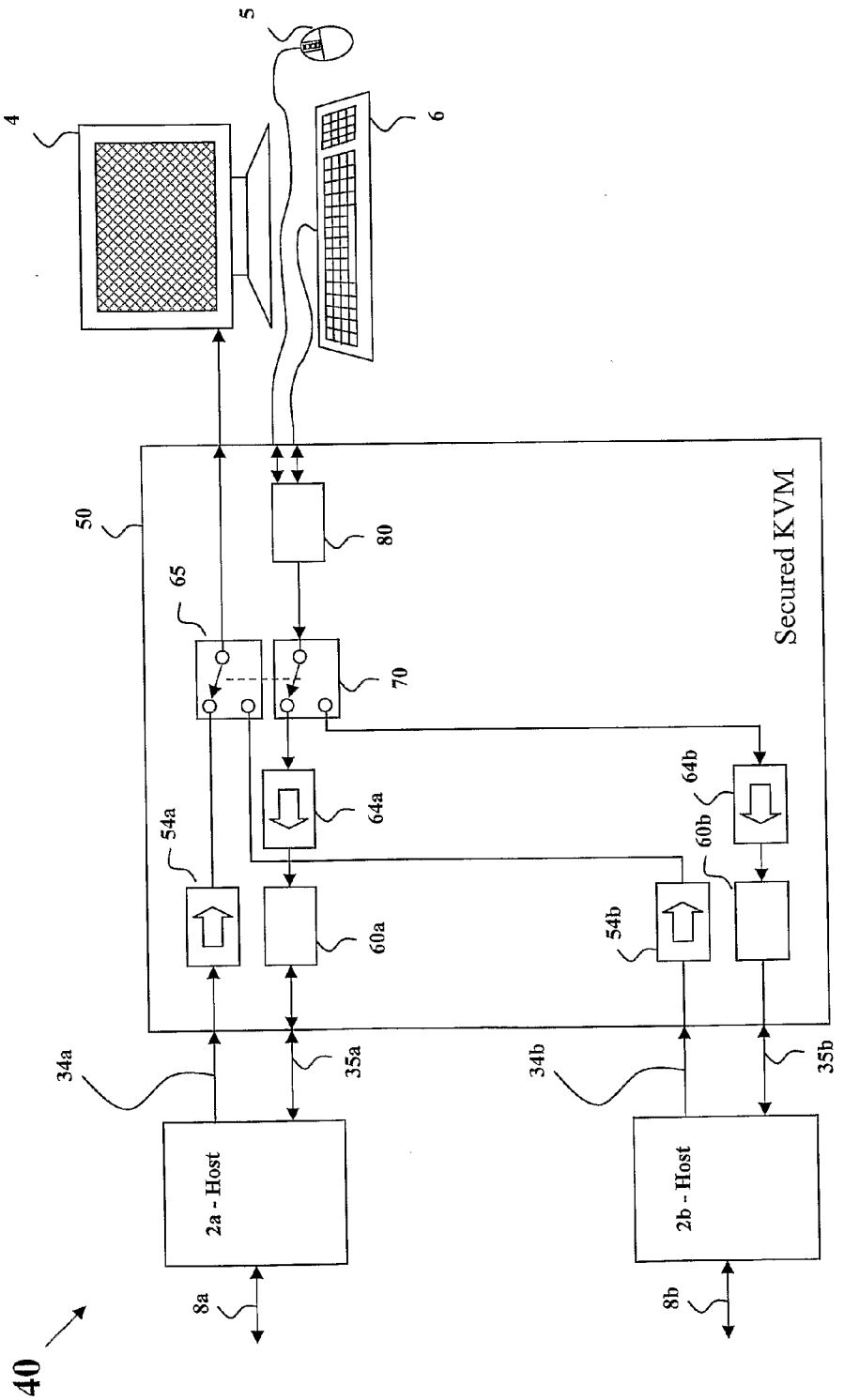

40
4
5
6
50
Secured KVM
80
65
70
64a
64b
54a
60b
60a
54b
34a
35a
34b
35b
2a - Host
2b - Host
8a
8b

Figure 4

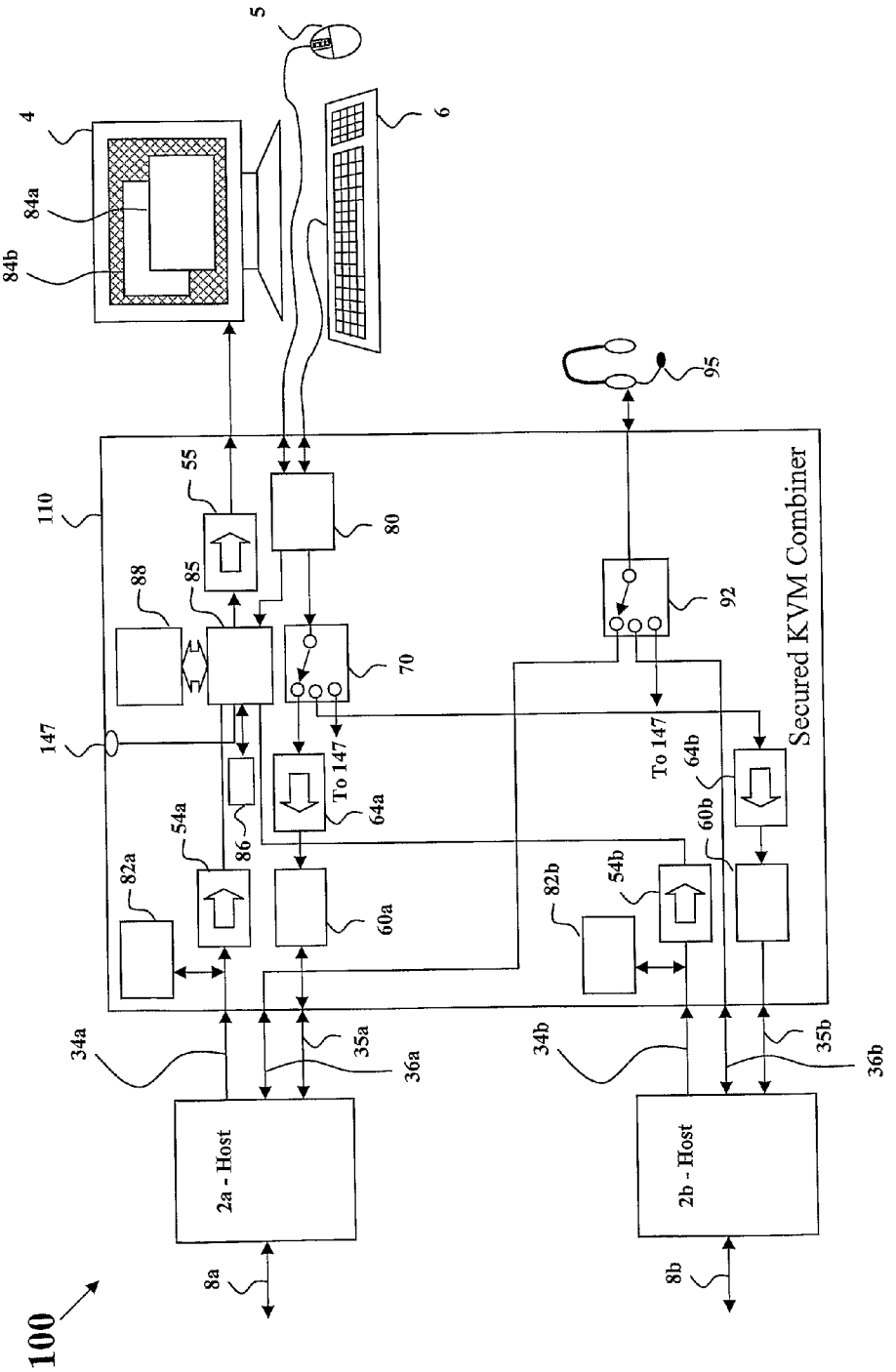

100
Secured KVM Combiner
2a - Host
2b - Host
To 147
To 147
4
5
6
84a
84b
95
110
55
80
88
85
92
70
147
64a
64b
54a
54b
86
82a
82b
60a
60b
34a
34b
35a
35b
36a
36b
8a
8b

Figure 5

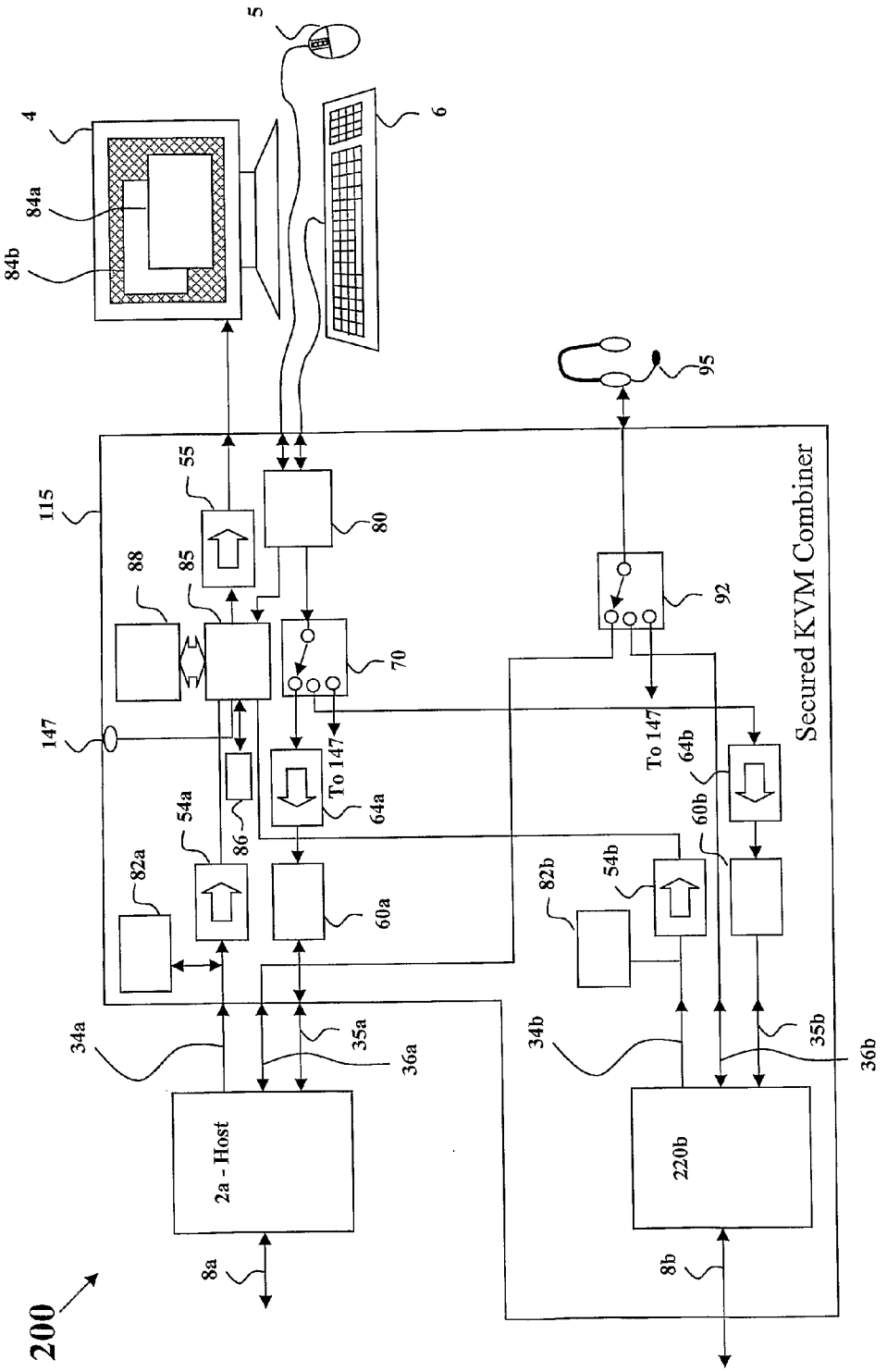

200
Secured KVM Combiner
2a - Host
220b
8a
8b
34a
35a
36a
34b
35b
36b
115
147
To 147
To 147
4
5
6
84a
84b
95
55
80
88
85
70
92
54a
86
82a
60a
64a
64b
60b
54b
82b

Figure 6a

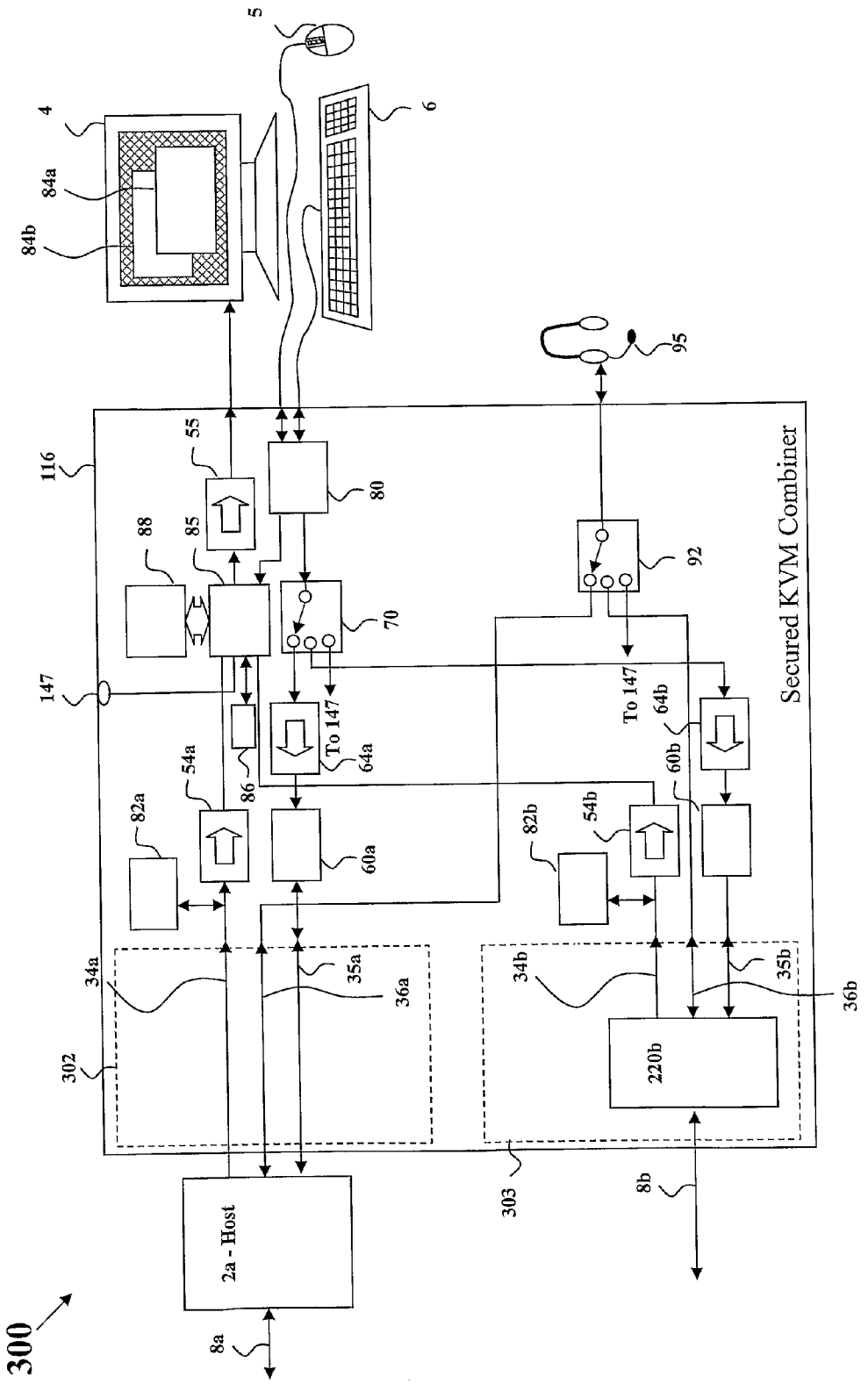

300
Secured KVM Combiner
2a - Host
8a
8b
303
302
116
147
4
5
6
84a
84b
95
55
80
88
85
92
70
To 147
64a
64b
60a
60b
54a
54b
82a
82b
86
34a
35a
36a
34b
35b
36b
220b

Figure 6b

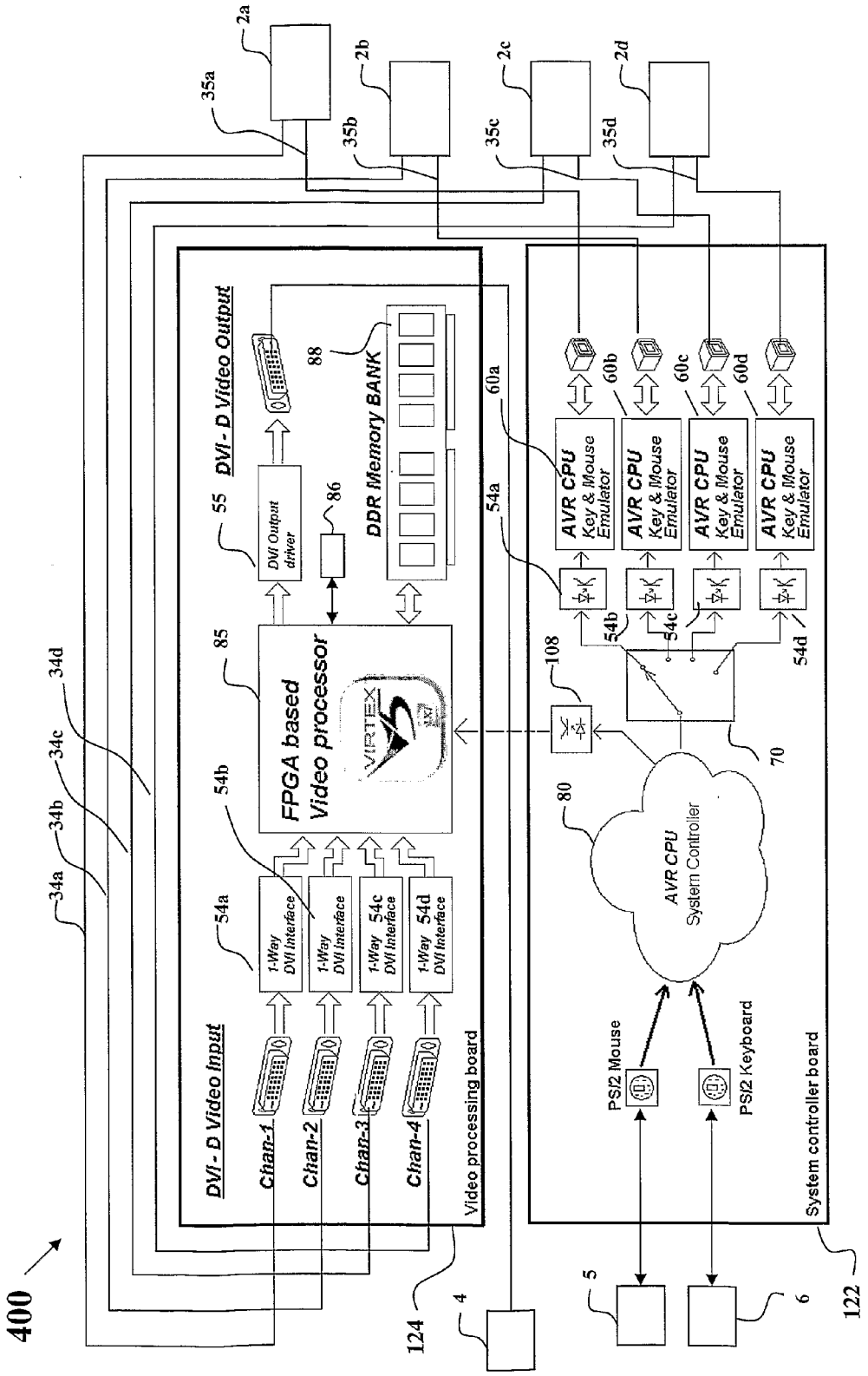

400
2a
2b
2c
2d
35a
35b
35c
35d
34a
34b
34c
34d
DVI - D Video Input
Chan-1
Chan-2
Chan-3
Chan-4
54a
1-Way DVI Interface
54b
54c
54d
FPGA based Video processor
VIRTEX
85
DVI - D Video Output
55
DVI Output driver
86
DDR Memory BANK
88
Video processing board
124
4
60a
60b
60c
60d
AVR CPU Key & Mouse Emulator
108
70
80
AVR CPU System Controller
PS/2 Mouse
PS/2 Keyboard
5
6
System controller board
122

Figure 7

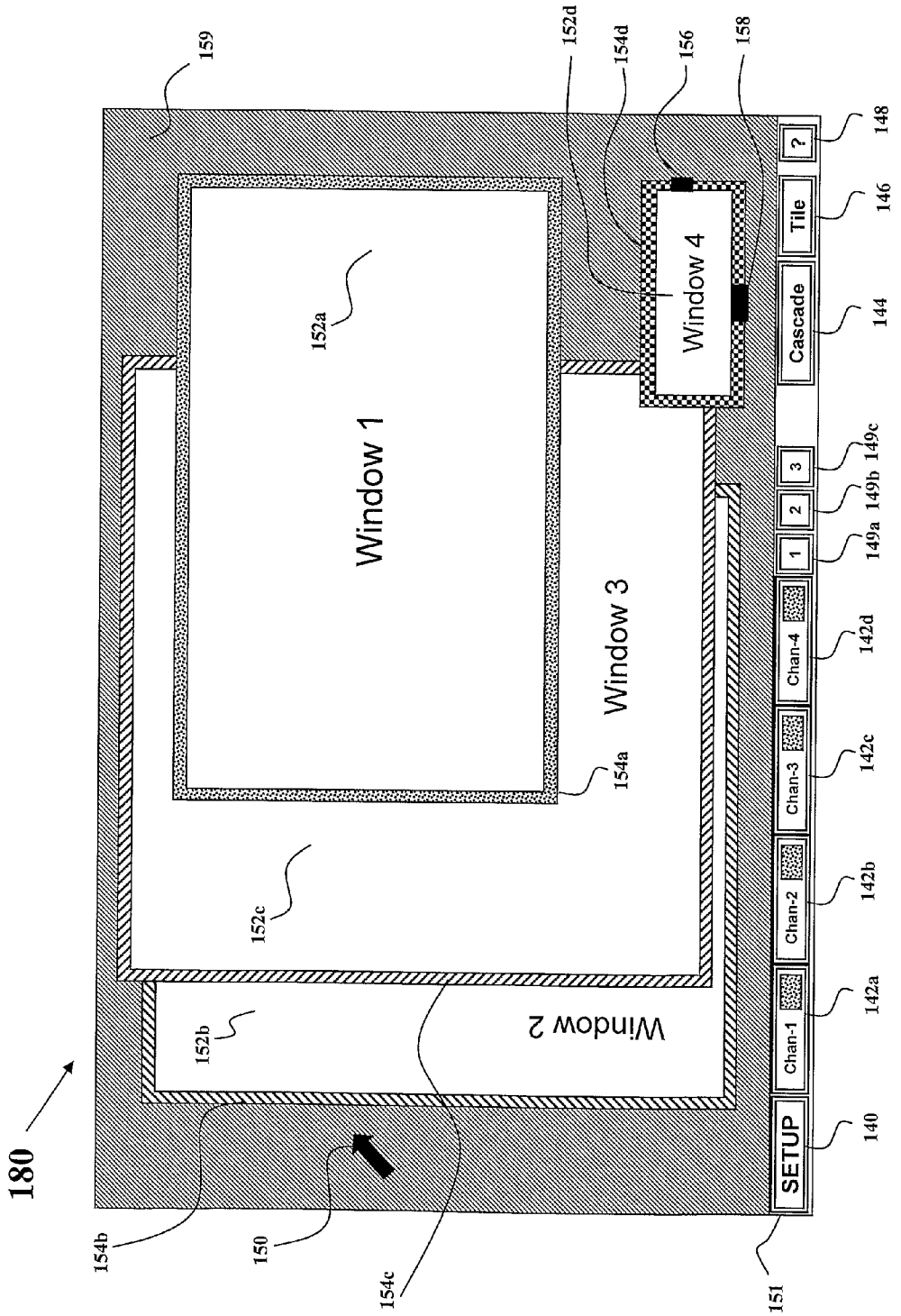

180
159
152d
154d
156
158
148
146
144
149c
149b
149a
142d
142c
142b
142a
140
151
154b
150
154c
152b
152c
154a
152a
Window 1
Window 3
Window 2
Window 4
SETUP
Chan-1
Chan-2
Chan-3
Chan-4
1
2
3
Cascade
Tile
?

Figure 8a

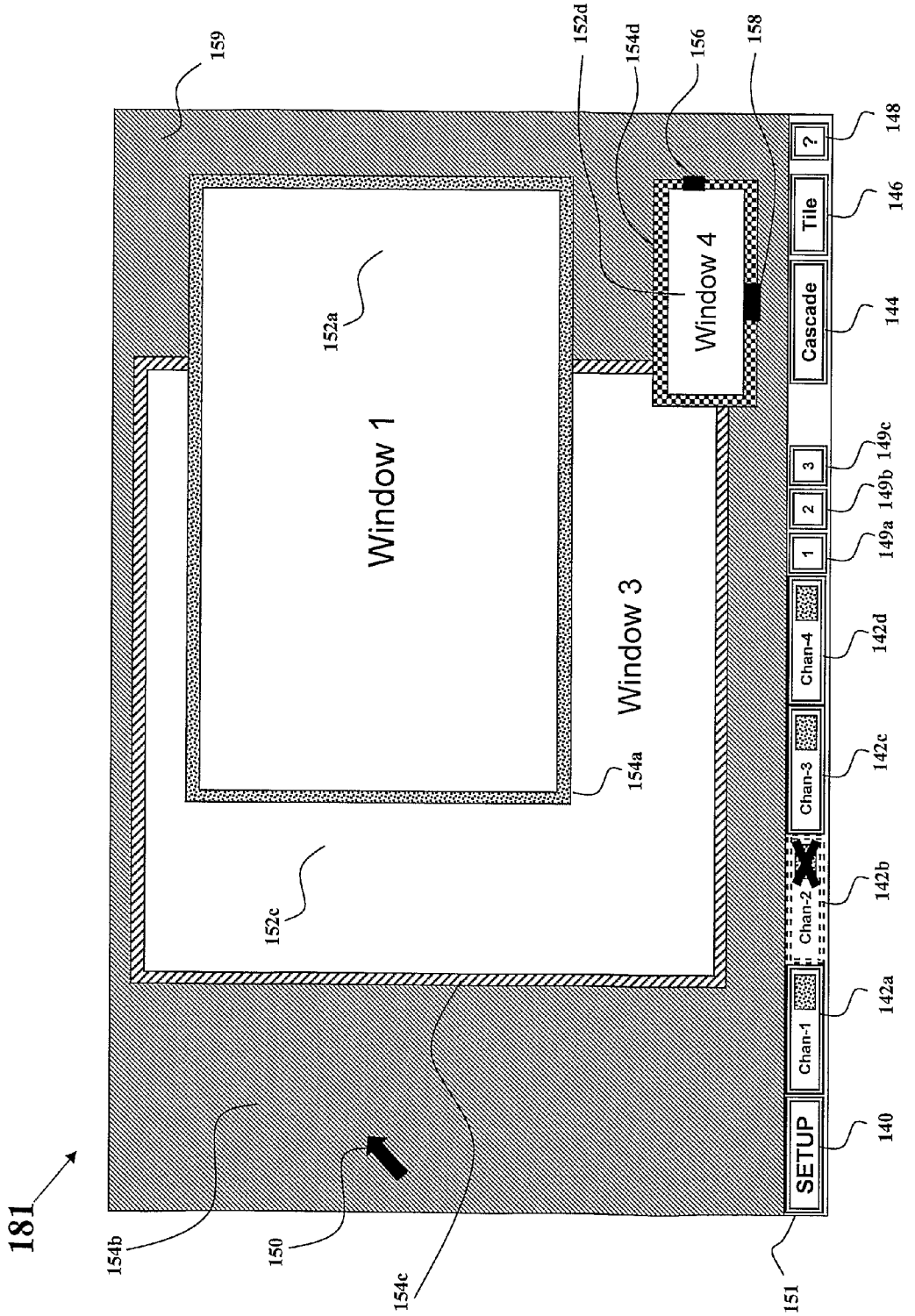

181
159
152d
154d
156
158
148
146
144
149c
149b
149a
142d
142c
142b
142a
140
151
154b
150
154c
152c
154a
152a
Window 1
Window 3
Window 4
SETUP
Chan-1
Chan-2
Chan-3
Chan-4
1
2
3
Cascade
Tile
?

Figure 8b

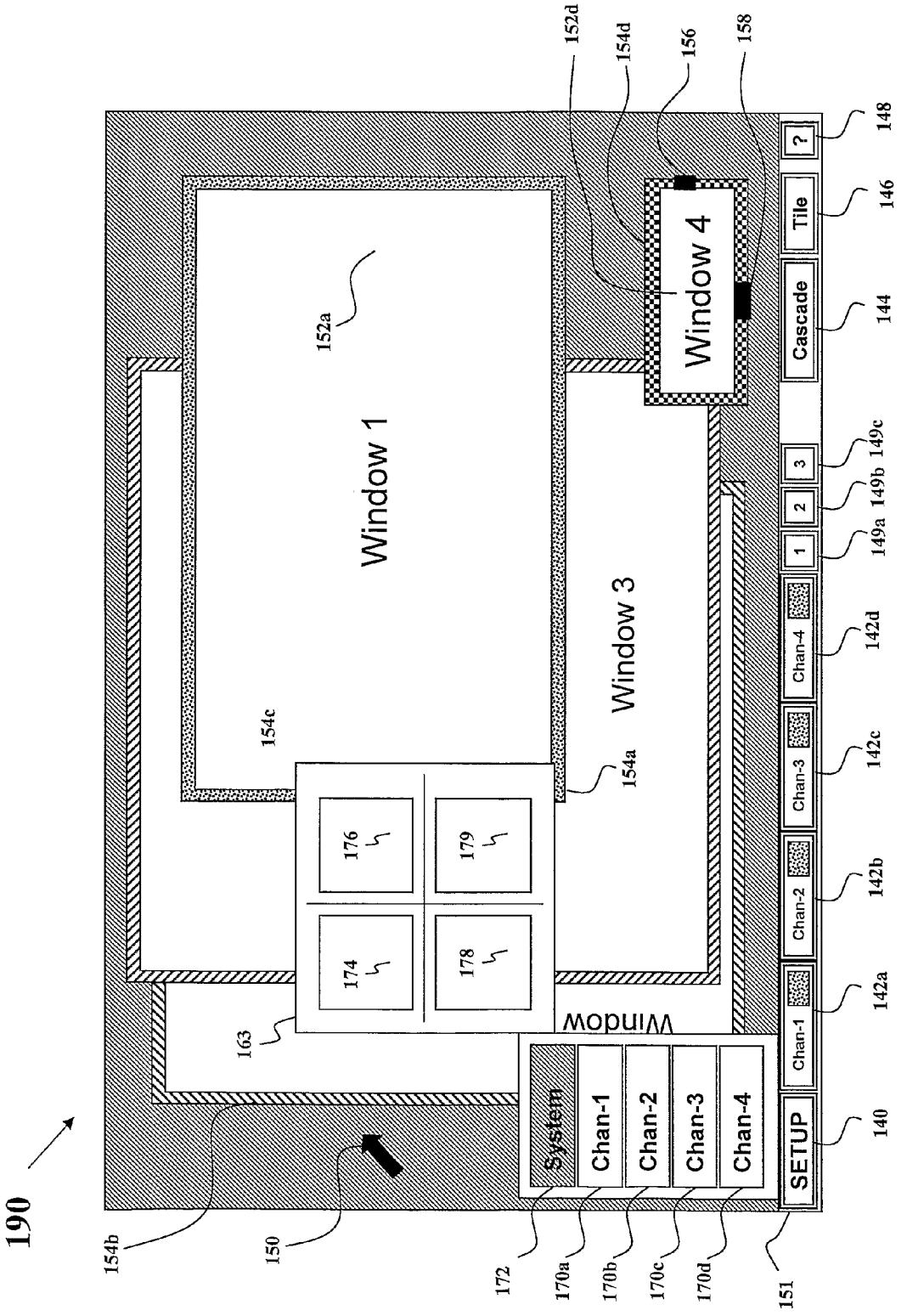

190
Window 1
Window 3
Window 4
Window
SETUP
Chan-1
Chan-2
Chan-3
Chan-4
System
Cascade
Tile
?
1
2
3
152a
152d
154d
156
158
154c
154a
154b
150
163
172
170a
170b
170c
170d
151
140
142a
142b
142c
142d
144
146
148
149a
149b
149c
174
176
178
179

Figure 9

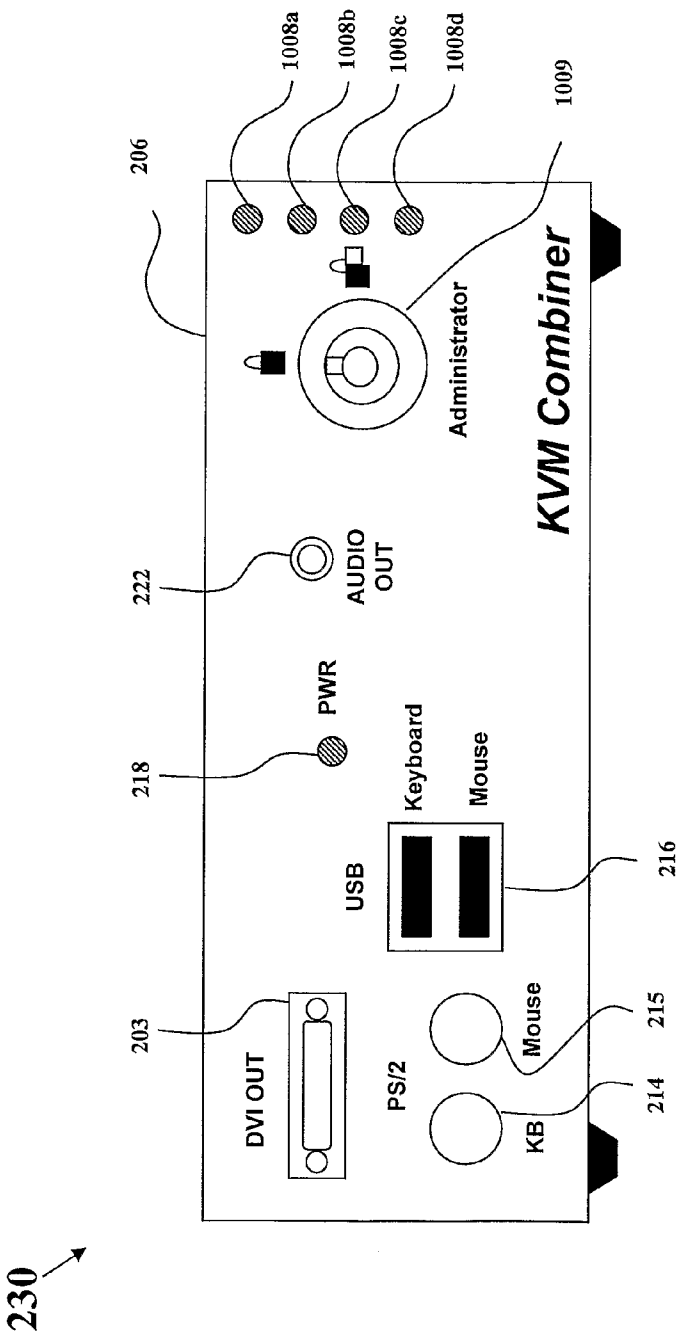

230
206
1008a
1008b
1008c
1008d
1009
Administrator
KVM Combiner
222
AUDIO OUT
218
PWR
Keyboard
Mouse
USB
216
203
DVI OUT
PS/2
Mouse
215
KB
214

Figure 10

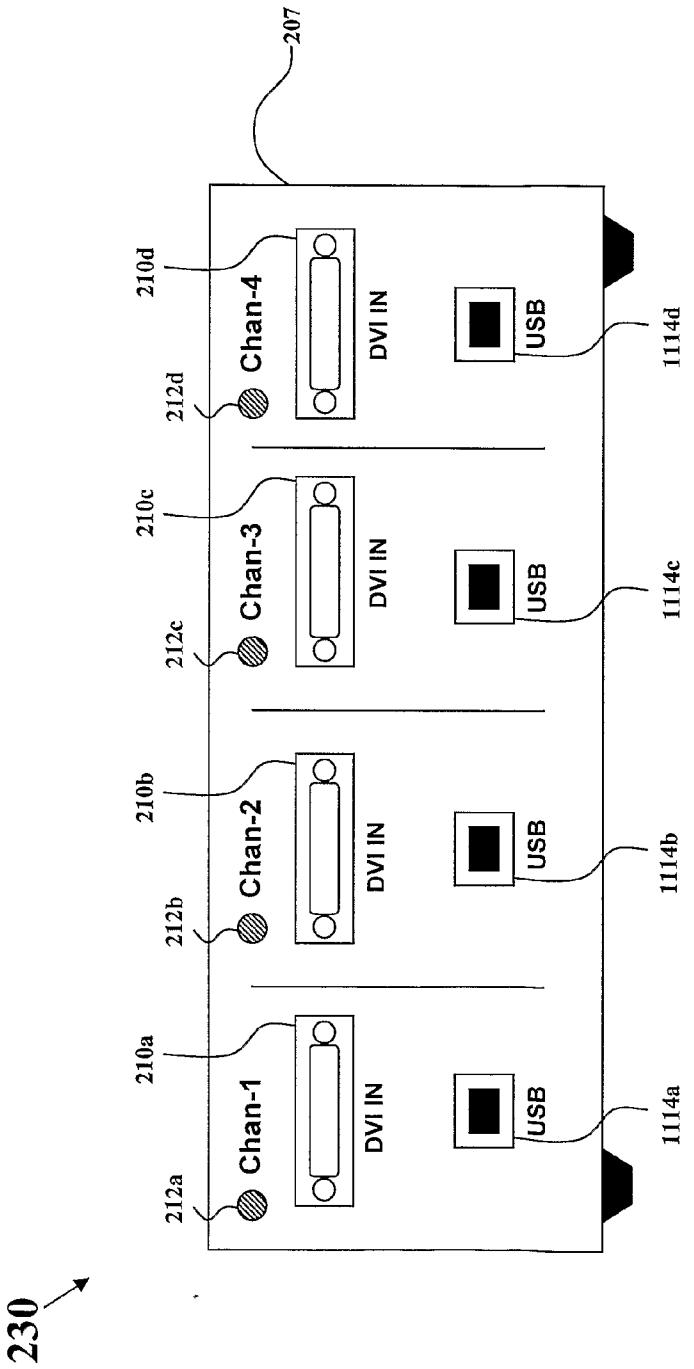

230
207
210a
210b
210c
210d
212a
212b
212c
212d
Chan-1
Chan-2
Chan-3
Chan-4
DVI IN
DVI IN
DVI IN
DVI IN
USB
USB
USB
USB
1114a
1114b
1114c
1114d

Figure 11

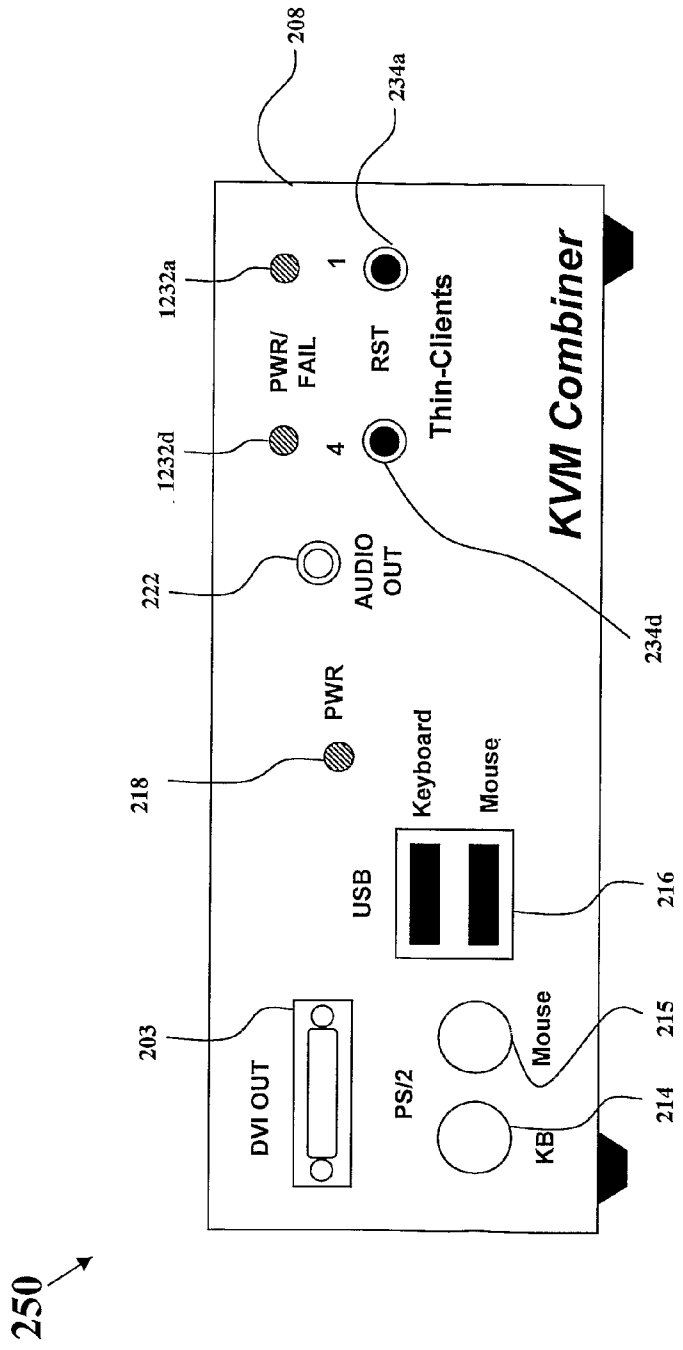

250
208
234a
1232a
PWR/
FAIL
1
RST
Thin-Clients
KVM Combiner
1232d
4
222
AUDIO
OUT
234d
PWR
218
Keyboard
Mouse
USB
216
203
DVI OUT
PS/2
Mouse
215
KB
214

Figure 12

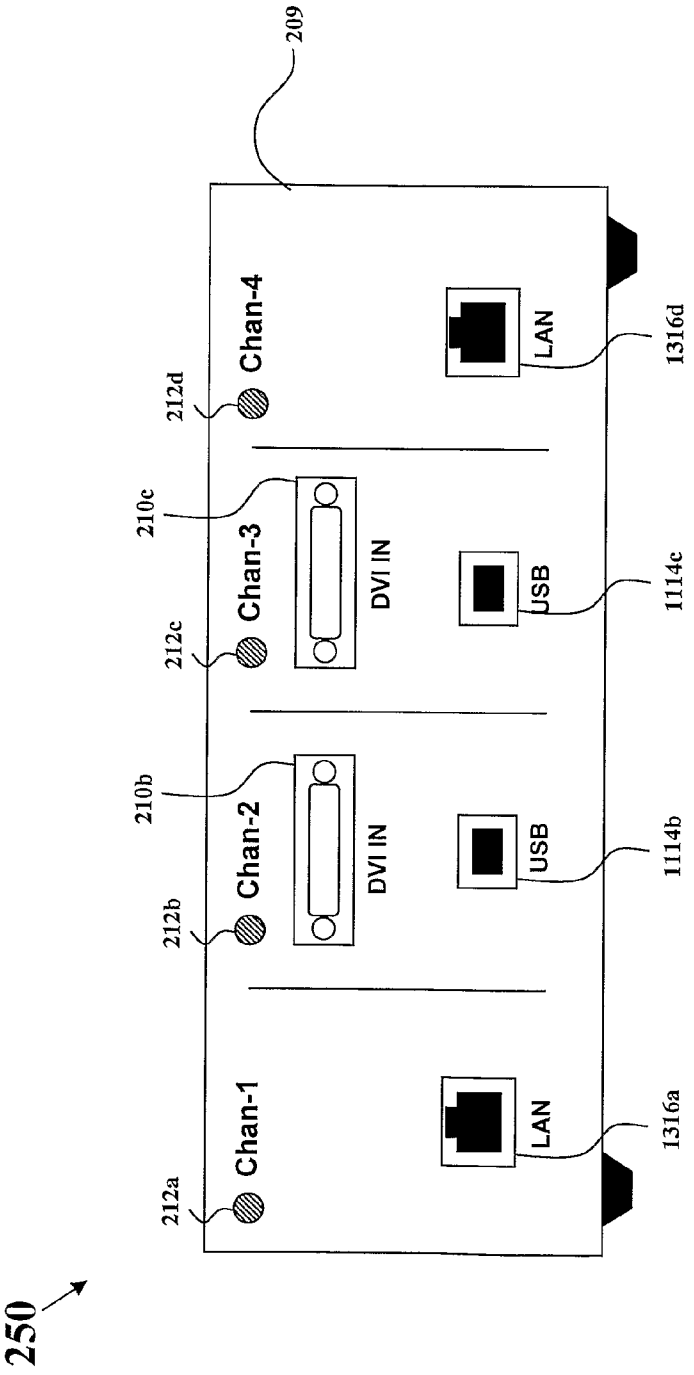

250
209
Chan-1
Chan-2
Chan-3
Chan-4
212a
212b
212c
212d
210b
210c
DVI IN
DVI IN
USB
USB
LAN
LAN
1114b
1114c
1316a
1316d

Figure 13

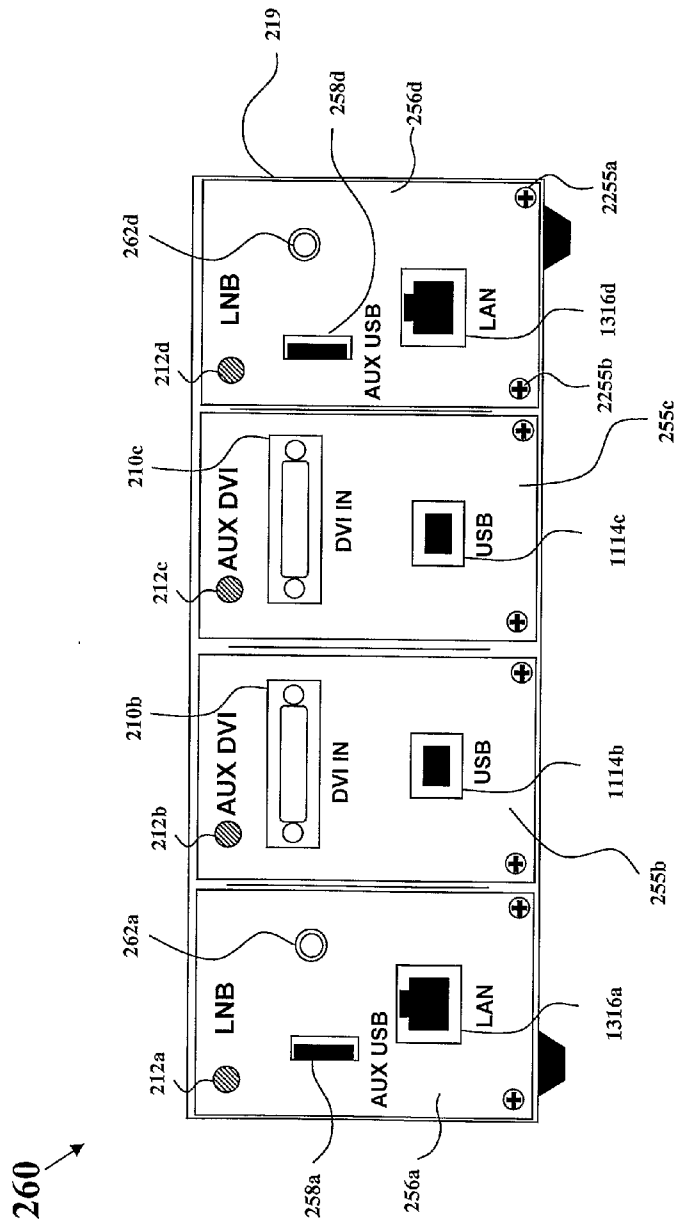

260
219
258d
256d
2255a
262d
LNB
AUX USB
LAN
1316d
212d
2255b
255c
210c
AUX DVI
DVI IN
USB
1114c
212c
210b
AUX DVI
DVI IN
USB
1114b
212b
255b
262a
LNB
AUX USB
LAN
1316a
212a
258a
256a

Figure 14

ISOLATED MULTI-NETWORK COMPUTER SYSTEM AND APPARATUS

FIELD OF THE INVENTION

[0001] The present invention, in some embodiments thereof, relates to apparatuses and systems for operating multiple computers from a single set of peripheral devices. More particularly, the invention presents a special secure KVM device for interacting with computers using a single console, while preventing data leakage between the connected computers and attached networks.

BACKGROUND OF THE INVENTION

[0002] Existing devices such as a Keyboard Video Moose (KVM) switch are used for interconnecting a single computer to multiple computers for control purposes. The switch enables sending commands and getting information from the controlled computers, thus a user of a KVM may have remote access to multiple computers from a single keyboard, a monitor, and a mouse. During access, keyboard characters or pointing data are sent to the remote computers and video signals are routed via the switch from the remote computers, processed, and displayed on the single video monitor. In general, the user navigates through an on-screen menu or display for easy of switching between the controlled computers.

[0003] Some KVM switches allow a user to view and access one of the controlled computers, while at the same time, the user can view video images from the others non-accessed computers on some parts of his video screen. This provides simultaneous information to the user and enables fast and simple on-screen navigation between the controlled computers.

[0004] Prior art for available products that allow a user to view video images from multiple sources simultaneously on a single screen, include the QuadView™ XL, and the device described in "Apparatus and system for managing multiple computers", to VanHarlingen, Brian, Leibow, Michael, Chen and Li-ter, US publication 11/105063 US; but these products do not protect the information passed through the combiner device and leakage between the controlled computers is made possible on the KVM switch even if the controlled computers are far apart.

[0005] Previous systems presenting a KVN include United States Patent Application Number 2006/0230110A1, titled "Apparatus and system for managing multiple computers" to Brian VanHarlingen, Michael Leibow, and Li-ter Chen. However, they describe a non-secured KVM wherein the managed computers are not isolated and no isolation means presented.

Other Referenced Patents and Applications

[0006] 1. United States Patent Application 20050044266—High isolation KVM switch
2. United States Patent Application 20040015980—Systems and methods for monitoring and controlling multiple computers
3. U.S. Pat. No. 7,240,111—Apparatus and system for managing multiple computers
4. U.S. Pat. No. 7,284,278—Secured KVM switch
5. U.S. Pat. No. 7,568,029—Apparatus and system for managing multiple computers
6. U.S. Pat. No. 7,113,978—Computer interconnection system

[0007] For many applications (such as transactions in banking markets) it is desirable to have a secured management device that, on one hand allows for simple interaction and control of multiple computers, yet, on the other hand, prevents information leakage between the controlled computers.

[0008] The present invention addresses this aspect of isolation in a combiner, thus providing higher level of security.

SUMMARY OF THE INVENTION

[0009] The present invention, in some embodiments thereof, relates to apparatuses and systems for managing multiple computers from a single location. More particularly, the invention presents a special secure KVM switch for managing computers from a single console, while preventing information leakage between the controlled computers.

[0010] According to an exemplary embodiment of the current invention, an Isolated multi-network computer system is provided, the system comprising:

[0011] Two or more Host Computers having video output port and peripheral port wherein each host computer connected to a different network having different or same security level; one or more User Display devices having video input port; a User Pointing device having peripheral port; a User Keyboard device having peripheral port; a Secured KVM device connected between Host Computer video output ports and User display device input port and between the User Pointing device peripheral port and Host Computers peripheral ports and between User Keyboard device peripheral port and Host Computers peripheral ports, wherein Secured KVM device enables standard bi-directional communications between Host Computer peripheral port and Secured KVM, between Secured KVM and User Pointing device, and between Secured KVM and User Keyboard device, and wherein Secured KVM device physically forces unidirectional data flow from User Pointing device and User Keyboard device to Host Computers peripheral ports and physically isolates Host Computers peripheral ports to prevent data leakage between Host Computers.

[0012] In some embodiments, in the Secured KVM device, each Host Computer peripheral port is connected to a separate circuitry emulating peripheral device to the Host Computer and connected to the physical unidirectional forcing circuitry.

[0013] In some embodiments, in the Secured KVM device, said physical unidirectional forcing circuitry is based on a unidirectional serial link.

[0014] In some embodiments, in the Secured KVM device, said physical unidirectional forcing circuitry is based on unidirectional optical isolator link.

[0015] In some embodiments, in the Secured KVM device, the physical unidirectional forcing circuitry is based on unidirectional electromagnetic isolator link.

[0016] In some embodiments, in the Secured KVM device, each said emulation circuitry is electrically isolated from the others and having different isolated ground planes.

[0017] In some embodiments, in the Secured KVM device, each said emulation circuitry is electromagnetically isolated from the others and from other Secured KVM circuitry.

[0018] In some embodiments, in the Secured KVM device, each said emulation circuitry is powered by an isolated power source internally generated or supplied by each connected Host Computer.

[0019] In some embodiments, in the Secured KVM device, said physical unidirectional forcing circuitry of each Host Computer are connected to a switching circuitry to automati-

cally or manually select active host to be operated by User Pointing device and User Keyboard device and wherein said switching circuitry is connected to a Peripheral Host Controller that is also connected to the user pointing device and user keyboard.

[0020] In some embodiments, in the Secured KVM device, said physical unidirectional forcing circuitry of each Host Computer are connected directly to a Peripheral Host Controller also connected to the user pointing device and user keyboard.

[0021] In some embodiments, in the Secured KVM device, the Peripheral Host Controller is a PS/2 keyboard controller connected to the User Keyboard device using PS/2 protocol and connected to the said switching circuitry or said physical unidirectional forcing circuitry using unidirectional standard or proprietary protocol.

[0022] In some embodiments, in the Secured KVM device, the Peripheral Host Controller is a PS/2 mouse controller connected to the User Pointing device using PS/2 protocol and connected to said switching circuitry using unidirectional standard or proprietary protocol.

[0023] In some embodiments, in the Secured KVM device, the Peripheral Host Controller is a USB controller connected to a USB User Keyboard device and USB User Pointing device using USB protocol and connected to the said switching circuitry or said physical unidirectional forcing circuitry using unidirectional standard proprietary protocol.

[0024] In some embodiments, in the Isolated multi-network computer system, said Host Computer video output ports are electrically, optically or wirelessly coupled to respective video input ports of said Secured KVM device.

[0025] In some embodiments, in the Secured KVM device, said video input ports are connected to video switching circuitry and to one or more video display output ports connected to one or more User Displays.

[0026] In some embodiments, in the Secured KVM device, said video input ports are analogically connected to analog video switching circuitry and to one or more analog video display output ports connected to one or more User Displays.

[0027] In some embodiments, in the Secured KVM device, the video input ports are digitally connected to a digital video receiver connected to a digital video multiplexer or processor circuitry and to one or more digital video display output ports connected to one or more User Displays.

[0028] In some embodiments, in the Secured KVM device, the video input ports are based on protocol selectable from: Digital Visual Interface (DVI) protocol, Display Port or High-Definition Multimedia Interface (HDMI) connected to a matching video receiver connected to a digital video multiplexer or processor circuitry and to one or more digital video display output ports connected to the User Display device.

[0029] In some embodiments, in the Secured KVM device, the video input ports are analog connected to a video Analog to Digital Converter (ADC) connected to digital multiplexer or processor circuitry and to one or more digital video display output port connected to the User Display device.

[0030] In some embodiments, in the Secured KVM device, the digital multiplexer/processor circuitry is capable of switching between host input video ports supplying to User Display device only one host video image based on user selection.

[0031] In some embodiments, in the Secured KVM device, the digital multiplexer/processor circuitry is further capable of simultaneously displaying more than one host input video windows on the User Display device.

[0032] In some embodiments, in the Secured KVM device, the digital multiplexer/processor circuitry is further capable of generating colored frames around host video windows to help users identifying window source.

[0033] In some embodiments, in the Secured KVM device, the digital multiplexer/processor circuitry is further comprising of a video frame buffer memory to enable simultaneous display of asynchronous video sources from Host Computers having different video resolution setting, different refresh rates and different video signal phases.

[0034] In some embodiments, in the Secured KVM device, the digital multiplexer/processor circuitry uses one of the host input video signals to synchronize video output signal.

[0035] In some embodiments, in the Secured KVM device the digital multiplexer/processor circuitry independently generating and sync required video output signals.

[0036] In some embodiments, in the Secured KVM device, the digital multiplexer/processor circuitry is substantially based on a Field Programmable Gate Array (FPGA).

[0037] In some embodiments, in the Secured KVM device, the digital multiplexer/processor circuitry is substantially based on Application Specific Integrated Circuit (ASIC).

[0038] In some embodiments, in the Secured KVM device, the digital multiplexer/processor circuitry is substantially based on programmable CPU.

[0039] In some embodiments, in the Secured KVM device, the digital multiplexer/processor circuitry and host controller are further connected to a cascading port to synchronize video display and peripherals activity between cascaded Secured KVM devices.

[0040] In some embodiments, in the Secured KVM device, the digital multiplexer/processor circuitry receives graphic commands from said peripheral host controller.

[0041] In some embodiments, in the Secured KVM device, the digital multiplexer/processor circuitry is having a non-volatile memory device to store multiplexer/processor programs, administrator and user settings and optional customized display background bitmaps.

[0042] In some embodiments, in the Secured KVM device, the user can select active Host Computer based on switch position.

[0043] In some embodiments, in the Secured KVM device, the user can select active Host Computer based on programmable User Keyboard key combination.

[0044] In some embodiments, in the Secured KVM device, the user can select active Host Computer based on programmable User mouse key triggering.

[0045] In some embodiments, in the Secured KVM device, the user can toggle between active Host Computers using User Pointing device wheel rotation.

[0046] In some embodiments, in the Secured KVM device, the active Host Computer is automatically selected based on system cursor location.

[0047] In some embodiments, in the Isolated multi-network computer system, the Host Computers further having an Audio output port connected to said Secured KVM device Audio Input port.

[0048] In some embodiments, in the Secured KVM device, the Audio Input ports are connected to an audio mixer or switch connected to an Audio output port. Audio output port may be connected to User Headphones or speakers.

[0049] In some embodiments, in the Secured KVM device, the audio mixer or switch is further connected to external cascading port to enable audio output device sharing between cascaded Secured KVMs.

[0050] In some embodiments, in the Secured KVM device, the Audio Input ports are electrically isolated to prevent electrical leakage between Host Computers.

[0051] In some embodiments, in the Isolated multi-network computer system, the Host Computers further having a Microphone input port connected to said Secured KVM device Microphone Output port.

[0052] In some embodiments, in the Secured KVM device, the Microphone Output ports are connected to an audio mixer or switch connected to a Microphone Input port. Microphone input port may be connected to User Headphones or microphone.

[0053] In some embodiments, in the Secured KVM device, the audio mixer or switch is further connected to external cascading port to enable audio input device sharing between cascaded Secured KVMs.

[0054] In some embodiments, in the Secured KVM device, the Microphone Output ports are electrically isolated to prevent electrical leakage between Host Computers.

[0055] In some embodiments, in the Secured KVM device, the Microphone and Audio output audio levels depending on active Host selected.

[0056] In some embodiments, in the Secured KVM device, the plurality of local device settings such as Host Computers display resolution, output display resolution, frame colours, frame thickness, cursor type, task-bar size and background bitmap can be accessed and modified by authorized user through a secured administrator mode.

[0057] In some embodiments, in the Secured KVM device, the plurality of local device settings such as Host Computers windows location and size can be modified and stored by authorized user through on-screen menus.

[0058] In some embodiments, in the Secured KVM device, the administrator mode can be accessed using programmable user name and password.

[0059] In some embodiments, in the Secured KVM device, the administrator mode can be accessed using electromechanical key switch.

[0060] In some embodiments, in the Secured KVM device, the administrator mode can be accessed using programmable portable storage device or card.

[0061] In some embodiments, in the Secured KVM device, the administrator mode can be accessed using console management port and remote computer.

[0062] In some embodiments, in the Secured KVM device, the local device settings can be further accessed and modified by authorized user using standard remote management protocol such as SNMP.

[0063] In some embodiments, in the Secured KVM device, the local device settings can be further loaded from or saved on a portable storage device such as flash disk or memory card.

[0064] In some embodiments, in the Secured KVM device, the device is further comprising of circuitry to signal Host Computer video controller Plug & Play Display Data Channel (DDC) compatibility information such as display resolution, display type and display refresh rate.

[0065] In some embodiments, in the Secured KVM device, the circuitry is device is further comprising of non-volatile memory such as ROM, programmable microcontroller or EEPROM containing standard display data to emulate a standard display.

[0066] In some embodiments, in the Secured KVM device, the device is further comprising of circuitry to automatically detect connected User Display parameters and configure device display output parameters accordingly.

[0067] In some embodiments, in the Secured KVM device, the device is further comprising of a cascading port to enable connection and synchronization of more than one Secured KVM devices and thus increasing the number of connected Host Computers.

[0068] In some embodiments, in the Isolated multi-network computer system, the one or more Host Computer can be substituted by a thin-client device.

[0069] In some embodiments, in the Isolated multi-network computer system, the one or more Host Computer can be substituted by an external video source interface to enable display of video source.

[0070] In some embodiments, in the Secured KVM device, the device is further comprising of one or more thin-client devices reducing the number of needed external Host Computers.

[0071] In some embodiments, in the Secured KVM device, the device is further comprising of one or more anti-tampering means such as PCB over-molding, micro-switch, light sensor, anti-tampering label, tampering memory, thermal sensor and case resistance sensor.

[0072] In some embodiments, in the Secured KVM device, the digital multiplexer/processor circuitry is further capable of reducing incoming video bandwidth by means selectable from the list of: colour-depth reduction, resolution reduction, refresh rate reduction, cropping, colour space conversion, and dropped frames.

[0073] In some embodiments, in the Secured KVM device, the digital multiplexer/processor circuitry is further capable of generating a task-bar to help user navigating between windows.

[0074] In some embodiments, in the Secured KVM device, the digital multiplexer/processor circuitry is further capable of minimizing Host Computer window into the task-bar and maximizing it to original size again.

[0075] In some embodiments, in the Secured KVM device, the user can use the task-bar to disable unused channels.

[0076] In some embodiments, in the Secured KVM device , the digital multiplexer/processor circuitry is further capable of enabling the user to scale a Host Computer window up and down and view window parts by using scroll-bars.

[0077] In some embodiments, in the Secured KVM device, the device is further comprising of a chassis with identical bays for each channels wherein bays enables field installation of plurality of compatible modules.

[0078] In some embodiments, in the Secured KVM device, the device is further comprising of a thin-client/computer module having matching connector to enable insertion into In some embodiments, in the chassis bays.

[0079] In some embodiments, in the Secured KVM device, the device is further comprising of an auxiliary host interface module having matching connector to enable insertion into the chassis bays and cable interfaces with connected host computer.

[0080] Unless otherwise defined, all technical and scientific terms used herein have the same meaning as commonly understood by one of ordinary skill in the art to which this

invention belongs. Although methods and materials similar or equivalent to those described herein can be used in the practice or testing of the present invention, suitable methods and materials are described below. In case of conflict, the patent specification, including definitions, will control. In addition, the materials, methods, and examples are illustrative only and not intended to be limiting.

BRIEF DESCRIPTION OF THE OF THE DRAWINGS

[0081] Some embodiments of the invention are herein described, by way of example only, with reference to the accompanying drawings. With specific reference now to the drawings in detail, it is stressed that the particulars shown are by way of example and for purposes of illustrative discussion of the preferred embodiments of the present invention only, and are presented in the cause of providing what is believed to be the most useful and readily understood description of the principles and conceptual aspects of the invention. In this regard, no attempt is made to show structural details of the invention in more detail than is necessary for a fundamental understanding of the invention, the description taken with the drawings making apparent to those skilled in the art how the several forms of the invention may be embodied in practice.

[0082] In the drawings:

[0083] FIG. **1** illustrates a high-level block-diagram of a prior art system that enables a computer user to access multiple isolated networks using a single host computer.

[0084] FIG. **2** illustrates a high-level block-diagram of yet another prior art system that enables a computer user to access multiple networks using multiple host computers.

[0085] FIG. **3** illustrates a high-level block-diagram of yet another prior art system that enables a computer user to access multiple networks using multiple host computers and legacy KVM (Keyboard Video Mouse) device.

[0086] FIG. **4** illustrates a high-level block-diagram of a preferred embodiment of the present invention that enables a computer user to safely access multiple isolated networks using multiple host computers and a secured KVM device.

[0087] FIG. **5** illustrates a high-level block-diagram of another preferred embodiment of the present invention having secured KVM combiner function.

[0088] FIG. **6***a* illustrates a typical implementation of a secured KVM combiner of another preferred embodiment of the present invention.

[0089] FIG. **6***b* illustrates yet another typical implementation of a Secured KVM

[0090] Combiner, similar to the Secured KVM Combiner of the previous figure but with removable modules according to an exemplary embodiment of the present invention.

[0091] FIG. **7** illustrates a typical implementation of a secured KVM combiner of yet another preferred embodiment of the present invention wherein implementation of the design is separated into two separate boards—video processing board and system controller board.

[0092] FIG. **8***a* illustrates a typical implementation of secured KVM combiner user display, in system mode, according to a preferred embodiment of the present invention.

[0093] FIG. **8***b* illustrates another typical implementation of secured KVM combiner user display, in system mode wherein one window was disabled according to another exemplary embodiment of the present invention.

[0094] FIG. **9** illustrates a typical implementation of secured KVM combiner user display, in administrator mode, of a preferred embodiment of the present invention.

[0095] FIG. **10** illustrates typical front panel features of a secured KVM combiner with four external host computer ports of a preferred embodiment of the present invention.

[0096] FIG. **11** illustrates typical rear panel features of a secured KVM combiner with four external host computer ports of a preferred embodiment of the present invention.

[0097] FIG. **12** illustrates typical front panel features of a secured KVM combiner with two external host computer ports and two internal thin-client modules according to yet another preferred embodiment of the present invention.

[0098] FIG. **13** illustrates typical rear panel features of a secured KVM combiner with two external host computer ports and two internal thin-client modules according to yet another preferred embodiment of the present invention.

[0099] FIG. **14** illustrates a typical rear panel features of a Modular Secured KVM

[0100] Combiner with two auxiliary host interface modules and two thin-client/computer modules according to yet another preferred embodiment of the present invention.

[0101] DETAILED DESCRIPTION OF THE DRAWINGS

[0102] Before explaining at least one embodiment of the invention in detail, it is to be understood that the invention is not necessarily limited in its application to the details set forth in the following description or exemplified by the examples. The invention is capable of other embodiments or of being practiced or carried out in various ways.

[0103] It will be appreciated that certain features of the invention, which are, for clarity, described in the context of separate embodiments, may also be provided in combination in a single embodiment. Conversely, various features of the invention, which are, for brevity, described in the context of a single embodiment, may also be provided separately or in any suitable sub-combination or as suitable in any other described embodiment of the invention. Certain features described in the context of various embodiments are not to be considered essential features of those embodiments, unless the embodiment is inoperative without those elements.

[0104] In discussion of the various figures described herein below, like numbers refer to like parts. The drawings are generally not to scale. For clarity, non-essential elements may have been omitted from some of the drawing.

[0105] FIG. **1** illustrates a high-level block-diagram of a prior art system **10** that enables a computer user to access multiple isolated networks using a single host computer. Host Computer **2** may be a PC, workstation, thin-client or portable computer connected to a single set of user mouse **5**, user keyboard **6**, user display **4** and user headset **3**. Host Computer **2** connected to three separate networks **8***a*, **8***b* and **8***c* via LAN (Local Area Network) cable **7** and LAN switch **1**. LAN switch **1** may be a simple mechanical switch controlled by the user to enable access to the three LAN ports **8***a*, **8***b*, and **8***c*. As the three networks may have different security levels it is typically desirable that LAN switch **1** will be designed in such way that it will reduce the risk electrical leakage between the three connected networks.

[0106] One major drawback of this method is that the connected of different security level networks to a single host **2** and its network adapter presenting the risk of leakage between the networks in the host. This can be done by hardware or by software means and although both networks are

not connected simultaneously to the host **2**, information leaks may happen after LAN switch **1** connecting the host **2** to a different network. Another drawback of this system is the need to reboot the host **2** after switching network. Even with this practice data may leak between networks through the single attached host **2**.

[0107] Another disadvantage of this prior-art system is that the user cannot work simultaneously at application from different networks. This switching between application and networks is though for users that needs to work on different networks on a daily basis.

[0108] FIG. **2** illustrates a high-level block-diagram of yet another prior art system **20** that enables a computer user to access multiple networks using multiple host computers. In this system the user uses two sets of computer hosts **2***a* and **2***b*, connected to two separate networks **8***a* and **8***b* accordingly. Computer hosts **2***a* and **2***b* also connected to two sets of desktop interaction devices—user keyboards **6***a* and **6***b*, user mice **5***a* and **5***b* and two user displays **4***a* and **4***b*.

[0109] While this system eliminates the risk of leakage between the two networks **8***a* and **8***b*, it has several disadvantages.

[0110] One disadvantage of this system is that the user needs to interact with two separate sets of keyboards mice and displays. This divided focus tends to confuse the user.

[0111] Another disadvantage is the desktop space needed and the added costs of the two separate sets.

[0112] FIG. **3** illustrates a high-level block-diagram of another prior art system **30** that enables a computer user to access multiple networks using multiple host computers and legacy KVM (Keyboard Video Mouse) device. In this system Host Computers **2***a* and **2***b* may be PC, workstation, thin-client or portable computer. Host computers **2***a* and **2***b* are connected to isolated networks **8***a* and **8***b* respectively.

[0113] Host computers **2***a* and **2***b* are connected to a KVM device **33** through a set of connection cables. Cables **34***a* and **34***b* delivers the video output of Host computers to the KVM. Cables **35***a* and **35***b* connects the peripheral interface of Host computers to the KVM. Peripheral interface may be PS/2 (IBM Personal System **2** standard), USB (Universal Serial Bus) or other peripheral protocol. Cables **36***a* and **36***b* connects the audio input/output of Host computers to the KVM. KVM device **33** switches the Host computer inputs/outputs to the connected set of Human Interface devices comprising of a display **4**, mouse **5**, keyboard **6** and headset or speakers **3**. Switch over from Host computer **2***a* to **2***b* and back is controlled by the user through special keyboard keys combination or by activation a switch located at the KVM **33**.

[0114] While this system has the advantage of reduced LAN leakage through the Host computers, it can still enable data leakage at the KVM **33** due to software or hardware vulnerabilities.

[0115] Another disadvantage of this system is that the user must switch completely from one environment to the other. Some legacy KVMs designed to provide electrical isolation between the host computers to reduce the risk of electrical and electromagnetic leakages between the isolated LANs.

[0116] FIG. **4** illustrates a high-level block-diagram of a preferred embodiment of the present invention **40** that enables a computer user to safely access multiple isolated networks using multiple host computers and a Secured KVM device. In this system Host Computers **2***a* and **2***b* may be PC, workstation, thin-client or portable computer. Host computers **2***a* and **2***b* are connected to isolated networks **8***a* and **8***b* respectively. It should be noted here that Secured KVM device may have many more ports to support additional Host Computers. To simplify the figures, only two channels are shown hereafter.

[0117] Host computers **2***a* and **2***b* are connected to a Secured KVM device **50** through a set of connection cables. Cables may be substituted by other connection means such as fiber-optical links or wireless connection. Cables **34***a* and **34***b* delivers the video output of Host computers to the Secured KVM device **50**. Cables **35***a* and **35***b* connects the peripheral interface of Host Computers **2***a* and **2***b* to the Secured KVM **50**. Peripheral interface may be PS/2 (IBM Personal System 2 standard), USB (Universal Serial Bus) or any other suitable peripheral protocol.

[0118] Secured KVM device **50** Host Computer **2***a* video inputs connected to an optional physical isolator **54***a*. Physical isolator may be opto-isolator, serial link, electromagnetic coupler, transformer or any other suitable circuitry. Similarly Host Computer **2***b* video input is connected to an optional physical isolator **54***b*. Isolation may be needed to avoid signal leakage between host computers due to common ground or power. If Host video input is analog additional buffer amplifier circuitry may be needed to properly interface with analog video source. If Host video input is digital (such as DVI) additional receiver circuitry may be needed to properly interface with digital video source.

[0119] Physical isolators **54***a* and **54***b* are connected to the video switch **65** to select active channel visible to the user through video output and User Display device **4**.

[0120] Physical isolators **54***a* and **54***b* may have built-in or separate Analog to Digital converter (ADC) to enable interfacing with analog video signals from Host Computers **2***a* and **2***b*.

[0121] Secured KVM device **50** Host Computer **2***a* peripheral port **35***a* is connected to peripheral emulator circuitry **60***a*. Secured KVM device **50** Host Computer **2***b* peripheral port **35***b* is connected to peripheral emulator circuitry **60***b*. Peripheral Emulators circuitry **60***a* and **60***b* emulating standard peripheral device such as USB or PS/2 keyboard or mouse. Peripheral Emulators circuitry **60***a* and **60***b* are connected to physical unidirectional enforcing circuitry **64***a* and **64***b* respectively. Physical unidirectional enforcing circuitry **64***a* and **64***b* are for example: opto-isolator, serial link, electromagnetic coupler, transformer or any other suitable circuitry assuring one directional flow of data. Physical unidirectional enforcing circuitry **64***a* and **64***b* are required in order to assure that in any case of software failure or intended sabotage in the Host Computers **2***a* and **2***b* or in the Secured KVM device **50**, peripheral interface cannot cause information leakage between host computers.

[0122] Physical unidirectional enforcing circuitry **64***a* and **64***b* are connected to peripheral switch **70** to select active peripheral channel connected to the user keyboard and mouse.

[0123] Host controller **80** connected to the peripheral switch **70** interfaces between the bidirectional data flow of the connected user peripherals (mouse **5** and keyboard **6**) and the physically forced unidirectional data flow to the said peripheral emulators **60***a* and **60***b*.

[0124] Since peripheral protocols are bi-directional in nature and the data path between the host controller **80** and the peripheral emulators **60***a* and **60***b* is forced to unidirectional flow, the host controller serves as an interface between the standard peripheral protocol (such as PS/2 or USB) and the

non-standard unidirectional internal protocol. This internal protocol may use one way serial, I2C or any other standard or non standard interface.

[0125] Video switch **65** and peripheral switch **70** can be manually operated by the user by means of mechanical switch. Video switch **65** and peripheral switch **70** can be alternatively controlled by host controller function **80** to switch sources based on preprogrammed keyboard keys combination or mouse control.

[0126] FIG. **5** illustrates a high-level block-diagram of a preferred embodiment of the present invention **100** similar to the previous FIG. **4** having Secured KVM Combiner function **110**. In this preferred embodiment of the present invention the video switch function **65** of the previous FIG. **4** replaced by video processing function **85**. This video processing function receives multiple digital video data from optional physical isolators **54***a* and **54***b* to generate windows **84***a* and **84***b* (respectively) on output video port. To enable asynchronous video input and to enable additional video function an optional volatile memory **88** serving as video frame buffer connected to the video processing function **85**. Volatile memory **88** may be DRAM, DDR or any suitable fast volatile memory type.

[0127] Video processing function **85** may optionally be comprised of discrete logic, CPU, FPGA or ASIC technology.

[0128] Video processing function **85** receives commands from host controller function **80** based on user mouse and keyboard input. The host controller function **80** calculates mouse location in system mode, keys status, windows sizes, priority and locations and all other machine states and send proper commands to the video processing function **85** directly or through optional unidirectional flow device. User specific settings and administrator settings are all stored in the host controller function **80** non-volatile memory.

[0129] Video processing function **85** can receive video data from hosts that are not at the same display setting (resolution, refresh rate, colors, and phase) and stores it temporarily on the volatile memory frame-buffer **88**. Video output is generated by reading the volatile memory frame-buffer **88** content at any needed rate. Output display resolution can be adapted to any desirable setting irrespective to video input settings. Video processor may have a non-volatile memory device **86** to store CPU, FPGA or ASIC program and optional customer specific graphics such as display background images. Video processing function **85** typically connected to the user display **4** through DVI or HDMI transmitter **55** acting as a unidirectional flow device. This DVI or HDMI transmitter converts the digital video stream to differential signals needed to drive standard displays.

[0130] Non-volatile memory **82***a* and **82***b* connected to the Host Computers **2***a* and **2***b* respectively. Non-volatile memory may contain display parameters readable to the host to emulate standard display DDC (Display Data Channel). Upon connection of Secured KVM Combiner to the Host Computers **2***a* and **2***b*, Host computers video circuitry interrogates the non-volatile memory functions **82***a* and **82***b* to receive Plug & Play parameters such as display name, supported display resolution, supported display refresh rate etc. Non-volatile memory functions **82***a* and **82***b* may be programmed by the user to provide adequate information to the Host Computers as needed.

[0131] As video input data may have higher combined bandwidth than memory and video processing bandwidth various methods may be used to reduce such bandwidth.

[0132] Cropping of input video data removes data of areas that are not visible on the user display at any particular moment

[0133] Frame dropping—reduces incoming video data by skipping some frame. This method may cause visible artifacts though.

[0134] Reduced color depth or color depth conversion reduces input data at the cost of reduced color representation.

[0135] Other methods may be used to avoid bandwidth limitations depending on required video input settings.

[0136] An optional audio switching or mixing may be added to the Secured KVM Combiner device **110** in order to enable user to operate audio peripherals such as microphone, headset **95** or speakers. Host Computers **2***a* and **2***b* having additional audio cables **36***a* and **36***b* connected to the Secured KVM Combiner apparatus. Cables may be audio out, audio in, microphone or any other digital or analog audio signal. Audio multiplexer/mixer **92** enables volume control of selected/unselected hosts based on programmed settings. For example selected host audio channel may have higher volume compared to other host audio signals. In some exemplary embodiments, audio signals comprises of speaker signals transmitted to the user speaker, but no microphone signals. By allowing only speaker signals, unidirectional signal flow is ensured.

[0137] Cascading port **147** connected to the video processor **85** and optionally connected to host controller **80**, enable parallel connection of more than one Secured KVM Combiner devices to increase the number of Host Computer ports. To support cascading of peripherals and audio, switches **70** and **92** may have an additional (third in the depicted exemplary embodiment) position to enable access of external cascaded Secured KVM Combiner to the attached set of headset **95**, keyboard **6** and mouse **5**. In order to coordinate cursor location and system states, host emulator function **80** may be also connected to the cascading port **147**.

[0138] FIG. **6***a* illustrates a typical implementation of a Secured KVM Combiner **115** similar to the Secured KVM Combiner **110** of the previous FIG. **5**. In this system **200**, second host **2***b* is replaced by an internal thin-client/computer module **220***b*. This thin-client module internally connected to other Secured KVM Combiner functions through peripheral interface **35***b*, video interface **34***b* and audio interface **36***b*. Thin-client/computer module connected to its local area network **8***b* through a LAN jack or fiber interface installed on the device panel. Other controls and indications may be installed to support the thin-client/computer module **220***b*, such as Power/Fail LED, Reset switch and direct USB port to support local peripherals such as printers and authentication devices.

[0139] FIG. **6***b* illustrates yet another typical implementation of a Secured KVM Combiner **116** similar to the Secured KVM Combiner **115** of the previous FIG. **6***a* but with removable modules. In this system **300**, the Secured KVM combiner **116** is designed as a modular chassis with several identical bays. Bays have electrical interfaces to enable insertion of required modules (**302** and **303** in this example). Module **302** is auxiliary interconnection module to interface external host **2***a*. This module passes through or converts the peripheral interface **35***b*, video interface **34***b* and audio interface **36***b* from attached host **2***a*. Second module **303** is a thin-client/computer module with internal thin-client/computer **220***b* attached to external LAN **8***b*. This modular arrangement enables easy adaptation to the user and the organization with selection of internal or external hosts all interchangeable in a

single chassis. Power to the module may be provided by KVM chassis **116** directly or through isolated supply or may be provided by external sources as required.

[0140] FIG. **7** illustrates an exemplary implementation of a Secured KVM Combiner **400**. In this implementation the design is separated into two separate boards—video processing board **124** and system controller board **122**. To enhance product security the only link between system controller board **122** and video processor board **124** is a physical unidirectional enforcing circuitry **108** that connects the host controller **80** and the video processor **88** to deliver video commands and settings such as windows location, size, menu items, frames etc. **1**-Way DVI interfaces **54***a*, **54***b*, **54***c* and **54***d* serves as a receiver (interface) between the differential DVI video in connected to the Host Computers video cards and a parallel (LCD bus) interface connected to the video processor **85**. Each DVI Receiver **54***a* to **54***d* also serves as a physical unidirectional enforcing circuitry. In case that electrical isolation between video inputs is needed, additional isolators are placed between the DVI receivers and the video processor (not shown here). DVI Receivers **54***a* to **54***d* may also powered independently by isolated power supplies to avoid common ground plane. DVI Receivers **54***a* to **54***d* may also have separate electromagnetic shielding to avoid radiation leakage between channels.

[0141] In this particular implementation **4** channels are shown, however larger or smaller number of channels may be used.

[0142] For simplicity, cascading options are not depicted in this figure

[0143] FIG. **8***a* illustrates an exemplary implementation of a Secured KVM Combiner user display **180** in system mode. In the display mode shown, the user may move between different windows and change window size by using a pointing device and special system cursor **150**. Task-bar **151** located at the bottom of the visible display presents push buttons for each of the 4 different sources. Channel **1** source is accessed by clicking on channel **1** key **142***a*. Channel **2** source is accessed by clicking on channel **2** key **142***b*, etc. Each channel key is preferably marked with the color selected for that source—for example channel **1** key is marked with colored box identical in color to the frame **154***a* generated by the video processor around window **152***a*. User may optionally cancel (disable) unused channel as will be explained in next FIG. **8***b*. Optionally, user may also use the wheel in wheel mouse device to toggle between the 4 channels and bring each window to the front. The optional setup key **140** in the task-bar **151** enable authorized administrator user to access setup screens. Access to the setup preferably requires authentication means such as front panel key-lock opening, user name and password, smart-card etc.

[0144] The background image **159** may be a programmed color or a custom bitmap stored at the Secured KVM Combiner in special non-volatile memory (see FIG. **5** item marked **86**).

[0145] Preferably, user can use system cursor **150** to drag windows, and change window size by dragging window corner or side frame.

[0146] The task-bar may optionally roll down or disappear to save desktop space if mode is changed from system to normal.

[0147] User preset keys marked as **149***a*, **149***b* and **149***c* enable user to program specific windows arrangement and store it in one of the keys (this is done foe example by clicking on the preset key and holding for few seconds). Once user settings were stored, clicking on the key will immediately reconfigure the display with the stored setting.

[0148] Optional cascade key **144** located in the task-bar **151** change display mode to multiple overlaid windows. The optional tile key **146** arranges all **4** channels side by side to show all channels simultaneously.

[0149] Optional help key **148** located in the task-bar **151** may provide help images and text to assist the user in initial operation an in training.

[0150] In this example channel **4** window **152***d* reduced to a size smaller than its native resolution. As a result a vertical scroll-bar **156** and horizontal scroll-bar **158** appeared on the window frame **154***d* to enable user control of visible area.

[0151] Change from system mode to normal mode and back is preferably done through mouse clicks or other pre-programmed triggers. Once in normal mode, the system cursor disappears and the active host window cursor will be coupled to the user mouse.

[0152] FIG. **8***b* illustrates the same display of FIG. **8** but with channel **2** disabled by the user. Windows **2** marked **152***b* of FIG. **8** is not shown anymore and channel **2** key in the task-bar **142***b* became gray and has a cross on it.

[0153] FIG. **9** illustrates an exemplary implementation of a Secured KVM Combiner user display **190** in administrator mode. This mode is accessible to authorized users through authentication means and by clicking on the SETUP key **140** located in the task-bar **151**.

[0154] Setup menu will appear on top of setup key **140** to enable user selection of system option **172** or each one of the individual channels **1** to **4** through keys **170***a* to a**70***d* respectively. If System key **172** is pressed another menu area **163** appears on top and present system level settings such as: frame width **176**, task-bar size **179**, system cursor symbol **174** and display output settings **178**. This area **163** also shows various hardware parameters and loaded firmware versions.

[0155] It should be noted that display output settings may be automatically detected through display DDC interrogation by the host controller **80**. This will override administrator selection at setup screen.

[0156] When selecting a specific channel key **170***a* to **170***d*, administrator may select channel color and channel input resolution.

[0157] Setup may be loaded and saved automatically by external means such as USB flash key or memory card to enable fast device setup.

[0158] FIG. **10** illustrates an exemplary front panel of a Secured KVM Combiner **230** with four external host computer ports of the present invention. This Secured KVM Combiner is similar to the Secured KVM Combiner shown in FIGS. **4**, **5** and **7** above with **4** channels in this specific embodiment of the present invention. It should be noted that more or less channels may be used.

[0159] Front panel **206** is preferably having the following features:

[0160] DVI OUT Connector **203** to connect a DVI user display. Fiber-optic display interface module may be fitted on the panel to support TEMPEST requirements or remote located display installations. Other display output interfaces, or multiple display output interfaces may optionally be used.

[0161] PS/2 keyboard connector **214** to enable connection of user PS/2 keyboard.

[0162] PS/2 mouse connector **215** to enable connection of user PS/2 mouse.

[0163] Dual USB connectors **216** to enable connection of USB user mouse and keyboard.

[0164] Optional Power LED **218** to indicate that the device is powered on.

[0165] Audio out jack **222** to enable connection of user headset or speakers.

[0166] Optional channel indicators, for example LEDs **1008***a* to **1008***d* may be used for indication the status of the corresponding channel.

[0167] Optional administrator lock, for example physical lock **1009** may be used for changing the operation of the apparatus from user mode to administration or set-up mode by authorized personnel. It should be noted that other security measures prevention unauthorized tempering with the system may be employed in hardware or software.

[0168] It should be noted that more USB connectors may be used for example for multiple pointing devices. It also noted that only one of PS/2 or USB ports may be used.

[0169] It should be noted that some other feature such as Audio input jacks, power input jack and power switch may be located on the front panel.

[0170] It should be noted that some of these features and/or other feature may be located at other enclosure sides not shown here. For example the audio input jacks and main power switch may be located on the left side.

[0171] FIG. **11** illustrates an exemplary rear panel of a Secured KVM Combiner **230** with four external host computer ports according to an exemplary embodiment of the present invention. This Secured KVM Combiner is similar to the Secured KVM shown in FIGS. **4**, **5** and **7** above with **4** channels in this specific embodiment of the present invention. Rear panel **207** is preferably having the following features:

[0172] USB Type-B connectors **1114***a* to **1114***d* to connect to the host computers **2***a* to **2***d* USB peripheral ports respectively.

[0173] DVI connectors **210***a* to **210***d* to connect to the host computers **2***a* to **2***d* video output ports respectively.

[0174] Optional channel selected LEDs **212***a* to **212***d* to indicate the active selected channel.

[0175] It should be noted that number of channels may be different.

[0176] It should be noted that other I/O interface standards may be used.

[0177] FIG. **12** illustrates an exemplary front panel of a Secured KVM Combiner **250** with two external host computer ports and two internal thin-client/computer modules of the present invention. This Secured KVM Combiner is similar to the KVM **115** shown in FIG. **6** above but with **4** channels. Front panel **208** is similar to panel **206** in FIG. **10** with the following differences:

[0178] Additional thin-client/computer Power LEDs **1232***a* and **1232***d* to indicate that the internal thin-client devices are powered on (green color) or failed in boot test (red color).

[0179] Additional thin-client/computer RESET switches **234***a* and **234***d* to allow the user to reset the internal thin-client devices.

[0180] FIG. **13** illustrates an exemplary rear panel of a Secured KVM Combiner **250** with two external host computer ports and two internal thin-client modules of the present invention. This Secured KVM Combiner is similar to the KVM **115** shown in FIG. **6** above but with 4 channels. Rear panel **209** is similar to panel **207** in FIG. **11** with the following differences:

[0181] USB Type-B connectors **1114***a* and **1114***d* replaced by LAN jack **1316***a* and **1316***d* respectively to enable LAN connection to internal thin-client modules. LAN connection may be changed to fiber-optic interface such as SFP type connector. LAN jacks **13116***a* and **1316***d* may have internal LEDs to indicate LAN Link and Activity status.

[0182] DVI connectors **210***a* and **210***d* were removed due to the internal thin-client modules at channels **1** and **4**.

[0183] FIG. **14** illustrates a typical rear panel features of a Modular Secured KVM

[0184] Combiner **260** with two auxiliary host interface modules **255***b* and **255***c* and two thin-client/computer modules **256***a* and **256***d*. This Secured KVM Combiner implementation of the present invention is similar to the KVM **116** shown in FIG. **6***b* above but with 4 channels. Rear panel shown is made of different modules inserted into KVM chassis **219**. Modules are inserted into the chassis **219** and secured by screws or Dzus fasteners **2255***a* and **2255***b*. Technician may remove these screws to exchange modules as needed while KVM is at the user desktop.

[0185] Modularity of the KVM Combiner offers several advantages compared to non-modular KVMs:

[0186] The number and type of modules used can be customized before or after deployment to any required configuration of internal or external hosts.

[0187] Cabling can be minimized when internal hosts are used

[0188] High security organizations may want to use security policies that dedicate hosts to specific networks after initial exposure to that network. With modular device it is possible to enforce such procedure and keep operational overhead to minimum.

[0189] Product maintenance and trouble shooting is simplified compared with integrated hosts.

[0190] Thin-client computer modules **256***a* and **256***d* panels are fitted with a LAN jacks **1316***a* and **1316***d* respectively to attach the LAN, optional auxiliary USB connectors **258***a* and **258***d* respectively to attach optional user authentication device or printer and push buttons **262***a* and **262***d* respectively to reset the thin-client/computer or to enable restore to factory defaults. Optional microphone jack and other features may be added to enable further user options. LAN jack **1316***a* or **1316***d* may be substituted by fiber LAN connection if needed. LEDs **212***a* and **212***d* may indicate module selection or status.

[0191] Auxiliary host interface modules **255***b* and **255***c* panels are fitted with DVI input connectors **210***b* to enable video input from connected host. USB jack **214***b* to enable peripheral interface connection to attached host. LED **212***b* and **212***c* may indicate module selection or status.

[0192] Although the invention has been described in conjunction with specific embodiments thereof, it is evident that many alternatives, modifications and variations will be apparent to those skilled in the art. Accordingly, it is intended to embrace all such alternatives, modifications and variations that fall within the spirit and broad scope of the appended claims. All publications, patents and patent applications mentioned in this specification are herein incorporated in their entirety by reference into the specification, to the same extent as if each individual publication, patent or patent application was specifically and individually indicated to be incorporated herein by reference. In addition, citation or identification of

any reference in this application shall not be construed as an admission that such reference is available as prior art to the present invention.

1-68. (canceled)

69. An Isolated KVM combiner for multi-network computer system comprising:

a keyboard input configured to connect to a keyboard;

a pointing device input configured to connect to a pointing device such as a mouse;

a host controller receiving signals from at least one of said keyboard and pointing device;

at least a first and a second peripheral interfaces, configured to connect to at least a first and second host computers respectively, wherein said at least two host computers are connected to at least two separate networks respectively;

a peripheral switch, selectively directing signals from said host controller to only to the selected one of said at least first and second peripheral interfaces at a time; and

at least a first and a second physical unidirectional enforcing circuitries connected between said peripheral switch and said at least a first and second peripheral interfaces respectively, enforcing data flow only from said peripheral switch to said peripheral interfaces.

70. The Isolated KVM combiner of claim **69** and further comprises at least a first and a second peripheral emulators connected between said at least a first and a second physical unidirectional enforcing circuitry and said and said at least a first and second peripheral interfaces respectively.

71. The Isolated KVM combiner of claim **69** wherein said host controller receives signals from both said keyboard and pointing device.

72. The Isolated KVM combiner of claim **69** wherein said host controller controls said peripheral switch in response to commands received from at least one of said keyboard and pointing device.

73. The Isolated KVM combiner of claim **69** and further comprises:

at least a first and a second video interfaces configured to connect to video outputs of said at least first and second host computers respectively; and

a video switch selectively directing to a display device video signals only from the selected one of said at least first and a second video interfaces at a time.

74. The Isolated KVM combiner of claim **73** and further comprises:

at least a first and a second physical unidirectional enforcing circuitries connected to said at least first and a second video interfaces respectively, enforcing data flow only from said at least a first and a second video interfaces to said video switch.

75. The Isolated KVM combiner of claim **69** and further comprises:

at least a first and a second video interfaces configured to connect to video outputs of said at least first and second host computers respectively;

at least a first and a second physical unidirectional enforcing circuitries connected to said at least first and a second video interfaces respectively, enforcing data flow only from said at least a first and a second video interfaces; and

a video processor, receiving unidirectional video data from said at least first and a second video interfaces and transmits combined video signal to a display device.

76. The Isolated KVM combiner of claim **75** and further comprises a volatile memory serving as video frame buffer connected to said video processor.

77. The Isolated KVM combiner of claim **75** wherein said video processor presents a combined video on said display device in response to commands received from said pointing device.

78. The Isolated KVM combiner of claim **75** and further comprises video transmitter acting as a unidirectional flow device enforcing flow of video signal to said display device.

79. The Isolated KVM combiner of claim **69** and further comprises:

at least a first and a second audio interfaces respectively connected to said at least first and second host computers; and

an audio multiplexer connected to a audio peripheral such as microphone, headset or a speaker and to said at least at least a first and a second audio interfaces.

80. The Isolated KVM combiner of claim **69** wherein at least one of said host computers is a computer module integrated within the Isolated KVM combiner.

81. The Isolated KVM combiner of claim **69** and further comprises at least one bay into which a host computer may be inserted.

82. The Isolated KVM combiner of claim **69** and further comprises an administrator lock enabling configuration of said Isolated KVM combiner.

83. The Isolated KVM combiner of claim **69** wherein said physical unidirectional forcing circuitry is a circuitry such as a serial link, optical isolator link, electromagnetic isolator link.

84. An Isolated multi-network computer system comprising:

at least a first and a second host computes connected to at least a first and a second networks respectively, each having a video output and a peripheral input ports;

a user display;

a user keyboard;

a user pointing device; and

an Isolated KVM combiner comprising:

a keyboard input connected to said user keyboard;

a pointing device input connected to said user pointing device;

a host controller receiving signals from at least one of said user keyboard and user pointing device;

at least a first and a second peripheral interfaces, connected to said at least a first and second host computers respectively;

a peripheral switch, selectively directing signals from said host controller only to the selected one of said at least first and second peripheral interfaces at a time; and

at least a first and a second physical unidirectional enforcing circuitries connected between said peripheral switch and said at least a first and second peripheral interfaces respectively, enforcing data flow only from said peripheral switch to said peripheral interfaces.

85. The Isolated multi-network computer system of claim **84** wherein said Isolated KVM combiner further comprises:

at least a first and a second video interfaces connected to said video outputs of said at least first and second host computers respectively;

a video switch selectively directing to said user display device video signals only from the selected one of said at least first and a second video interfaces at a time; and

at least a first and a second physical unidirectional enforcing circuitries connected to said at least first and a second video interfaces respectively, enforcing data flow only from said at least a first and a second video interfaces to said video switch.

86. The Isolated multi-network computer system of claim **85** wherein said host controller controls said video switch and said peripheral switch to select the same host computer in response to command received from at least one of said user keyboard and user pointing device.

87. The Isolated multi-network computer system of claim **84** wherein said Isolated KVM combiner further comprises:

at least a first and a second video interfaces connected to said video outputs of said at least first and second host computers respectively;

at least a first and a second physical unidirectional enforcing circuitries connected to said at least first and a second video interfaces respectively, enforcing data flow only from said at least a first and a second video interfaces; and

a video processor, receiving unidirectional video data from said at least first and a second video interfaces and transmits combined video signal to said user display device.

88. The Isolated multi-network computer of claim **87** wherein said video processor presents a combined video on said display device in response to commands received from said pointing device.

89. The Isolated multi-network computer of claim **87** and further comprises video transmitter acting as a unidirectional flow device enforcing flow of video signal to said display device.

90. The Isolated multi-network computer of claim **84** and further comprises:

at least a first and a second audio interfaces respectively connected to said at least first and second host computers; and

an audio multiplexer connected to a audio peripheral such as microphone, headset or a speaker and to said at least at least a first and a second audio interfaces.

91. The Isolated multi-network computer of claim **84** and further comprises at least one bay into which a host computer may be inserted.

92. A method for combining KVM function in an Isolated multi-network computer system comprising:

connecting peripheral ports of at least a first and a second host computers to at least a first and second peripheral emulator circuitries respectively;

receiving signals from a user keyboard and a user pointing device;

selecting one of said at least a first and second peripheral emulator circuitries to receive said signals from said user keyboard and a user pointing device; and

physically forcing unidirectional signal flow from said at least a first and second peripheral emulator circuitries to said peripheral port of at least a first and a second host computers.

93. The method for combining KVM function in an Isolated multi-network computer system of claim **92** and further comprising:

receiving video output signals from at least a first and a second host computer;

directing at least a portion of said received video signals to a user display; and

physically enforcing a unidirectional video signal flow from said at least a first and second host computers to said user display.

* * * * *