

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

LENOVO (UNITED STATES) INC.,
Petitioner,

v.

INTELLECTUAL VENTURES, II LLC,
Patent Owner.

IPR2024-00124
Patent 7,325,140 B2

Patent Owner Demonstratives

Overview of the Invention

SUMMARY OF THE INVENTION

The present invention addresses the foregoing problems, as well as other problems, by providing an exemplary embodiment of a Secure Management Access Control for Computer Chipset (SMACC) for inclusion in devices that are to be enabled for remote management. In this preferred exemplary embodiment, the SMACC functions are implemented on a separate processor with separate flash and memory; however, this is not intended to limit the implementation of these features to separate chipsets in a device. These features also can be combined with other hardware and software features such as being integrated with a modem or with the main processor of a device. Some of the features of the SMACC can also be implemented separately. Such implementations would still be within the spirit and scope of this invention.

An additional exemplary embodiment of the invention implements the SMACC processor and supporting chips on a card that can be inserted into the device to be managed. In this implementation, management of the device is controlled by the card and the administrator must connect to the card to manage the device. The administrator will be able to connect to the SMACC card through the Virtual Management Interface (VMI) or directly through a SMACC interface on the SMACC card.

A primary function of the SMACC is to provide for the separation of management data from user data both within the device being managed and while the management information is in transit. Within the device, the SMACC sets up a separate processor for receiving management information and interacting with the control functions of the device. Remote management functions will pass through the SMACC processor. The SMACC also provides for a separate interface for management functions that is network enabled to facilitate remote management. Various embodiments of the invention allow for different types of interfaces to be utilized for the network enabled management interfaces. Exemplary interfaces could include POTS connections to the PSTN, Packet Cellular connections to a cellular provider's infrastructure, an Ethernet interface to a broadband modem and the Internet, or a wireless connection. The types of interfaces are not limited to those in this list to be within the scope of this invention. A VMI is also established for logically separating management traffic from user data when the in-band path is to be used for management data. The VMI is the interface between the SMACC chipset and the user data interfaces. The VMI utilizes existing and developing technology such as VPN to build secure tunnels between the SMACC chipset and the management center while utilizing the user data interfaces of the managed device and the user network to provide the transport of the management data cost effectively. The VPN technology provides the logical separation, confidentiality, and integrity of the management traffic while it is in transit.

Representative Claim of the '140 Patent

1. A remote device management communication system for securely controlling access to management applications and communications to and from said management applications on network devices in a distributed computer network that includes one or more network services, one or more secure management access controllers, and one or more managed network devices, the remote device management system comprising:

at least one secure management access controller connected to one or more data bus of said managed network device for the communication of device management data;

an out-of-band access connection means for connecting said one or more network services or remote users with said secure management access controller for management of said network device; and

at least one virtual management interface connection means for connecting said one or more network services or remote users with said secure management access controller;

wherein said virtual management interface connection means provides logical separation of management data from user data and utilizes user interfaces of said managed network element for connecting said one or more network services or remote users with said secure management access controller.

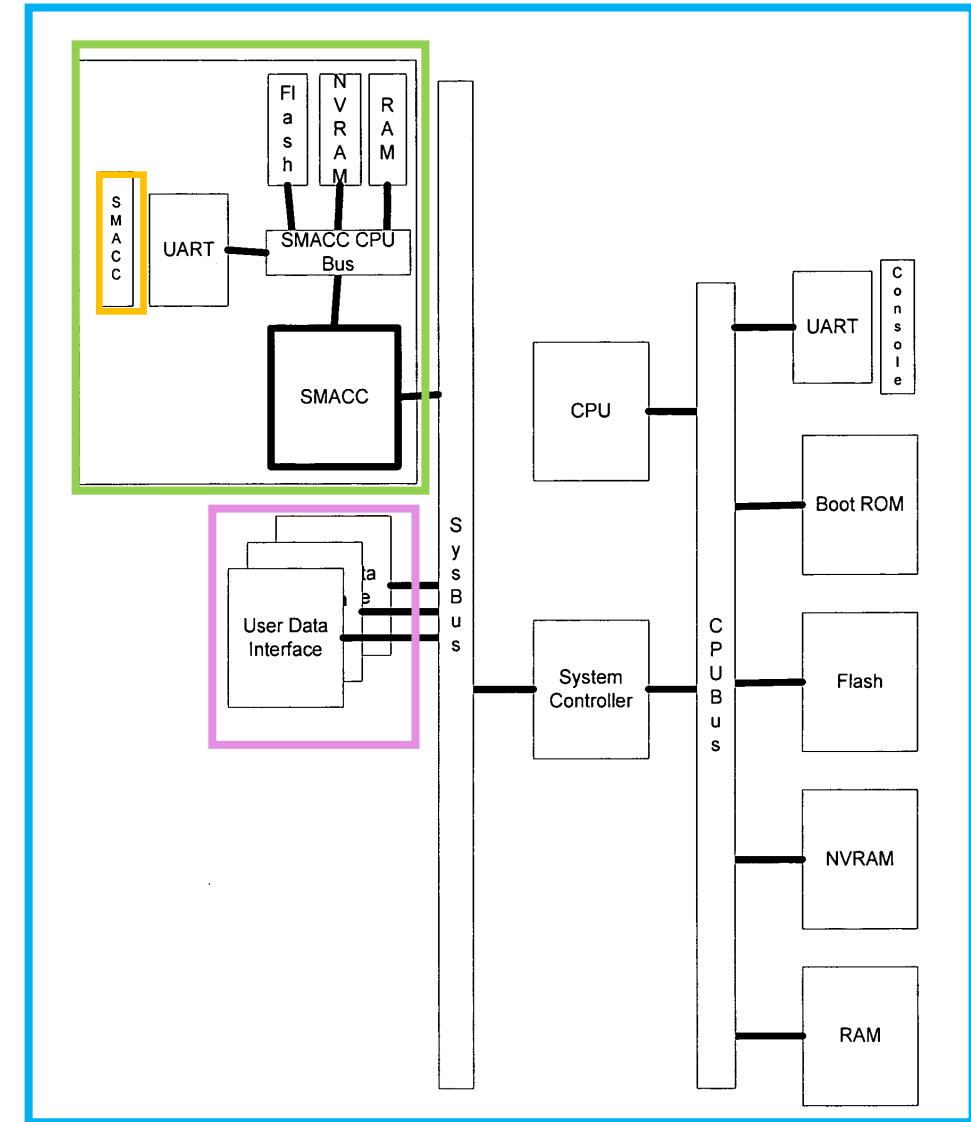


Fig. 19

The Virtual Management Interface (VMI)

to manage the device. The administrator will be able to connect to the SMACC card through the Virtual Management Interface (VMI) or directly through a SMACC interface on the SMACC card.

A primary function of the SMACC is to provide for the separation of management data from user data both within the device being managed and while the management information is in transit. Within the device, the SMACC sets up a separate processor for receiving management information and interacting with the control functions of the device. Remote management functions will pass through the SMACC processor. The SMACC also provides for a separate interface for management functions that is network enabled to facilitate remote management. Various embodiments of the invention allow for different types of interfaces to be utilized for the network enabled management interfaces. Exemplary interfaces could include POTS connections to the PSTN, Packet Cellular connections to a cellular provider's infrastructure, an Ethernet interface to a broadband modem and the Internet, or a wireless connection. The types of interfaces are not limited to those in this list to be within the scope of this invention. A VMI is also established for logically separating management traffic from user data when the in-band path is to be used for management data.

The VMI is the interface between the SMACC chipset and the user data interfaces. The VMI utilizes existing and developing technology such as VPN to build secure tunnels between the SMACC chipset and the management center while utilizing the user data interfaces of the managed device and the user network to provide the transport of the management data cost effectively. The VPN technology provides the logical separation, confidentiality, and integrity of the management traffic while it is in transit.

The VMI allows the SMACC processor to utilize data network ports to securely tunnel management traffic to the management center. The SMACC will run a suitable Virtual Private Network (VPN) protocol such as IPsec over the VMI. This allows the SMACC to take advantage of many services available at the management center such as network management applications, Network Time Protocol Servers, Log Server, Access Control Servers, and provide remote access to the managed device and more specifically the SMACC over the data network. Examples of protocols exemplary embodiments of the SMACC could utilize to allow an administrator access to the SMACC include but are not limited to HTTP, HTTPS, Telnet, or Secure Shell.

EX1002, 19:7-19

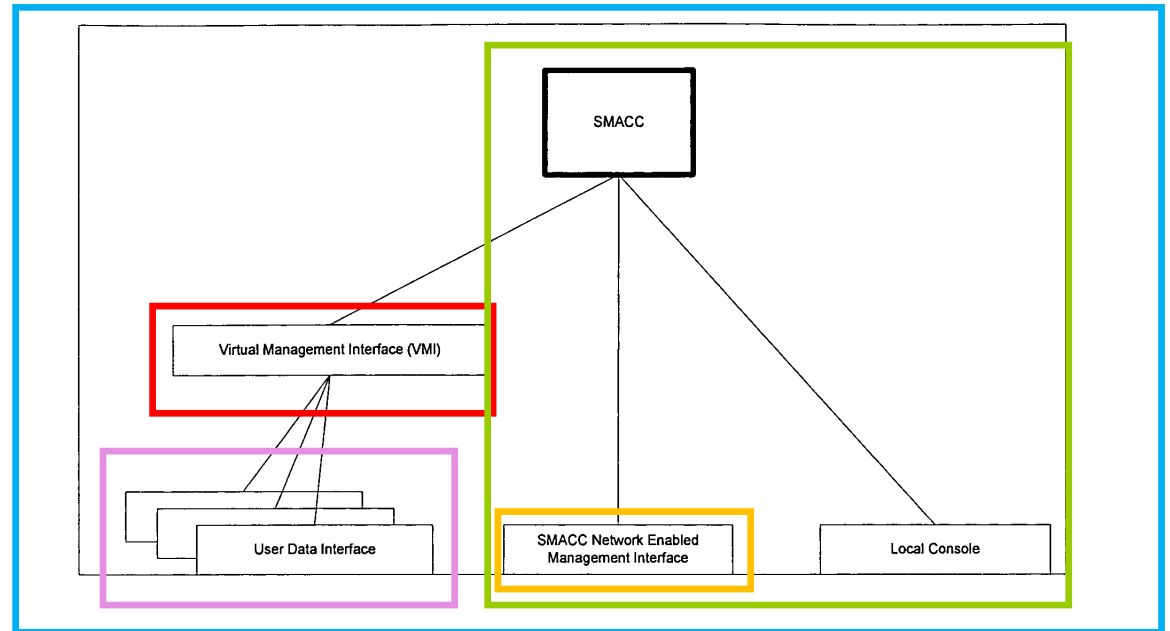


Fig. 3

EX1002, 6:1-33

"DEMONSTRATIVE EXHIBIT - NOT EVIDENCE"

EX1002, Fig. 3

Neufeld Neither Discloses Nor
Suggests a VPN/VMI That
Terminates Behind the NIC

The VMI Connection must be through the User Data interface

This assertion is unsupported. Neither Petitioner nor its expert (whose Declaration, at ¶ 115, merely repeats the conclusory language from the Petition) cites any portion of Neufeld disclosing that a VPN tunnel connects through or terminates at the managed server's user interfaces in the manner required by the '140 Patent.

Rather, Neufeld refers only to *general-purpose VPNs* used for *network access*, not internal communication paths within the managed device:

POR, 25

In sum, Claim 1 requires a VMI that terminates behind the user data interfaces, using them to connect remote users or services with the SMACC. Petitioner's focus on whether point-to-point VPNs were known misses this critical requirement, as even Petitioner's characterization of Dr. Noubir's testimony places the VPN endpoint at individual computers/networks—not behind the NIC. The '140 Patent makes clear, both in its claim language and drawings, that the VMI resides between the SMACC and user data interfaces, leveraging those interfaces to achieve the claimed logical separation of data. Neufeld, by contrast, only discloses VPNs for generic network access that terminate at the network side of the NIC, as depicted in its Figure 2. Petitioner has therefore failed to show how Neufeld could meet or render obvious this essential claim requirement, and Ground 1 cannot stand.

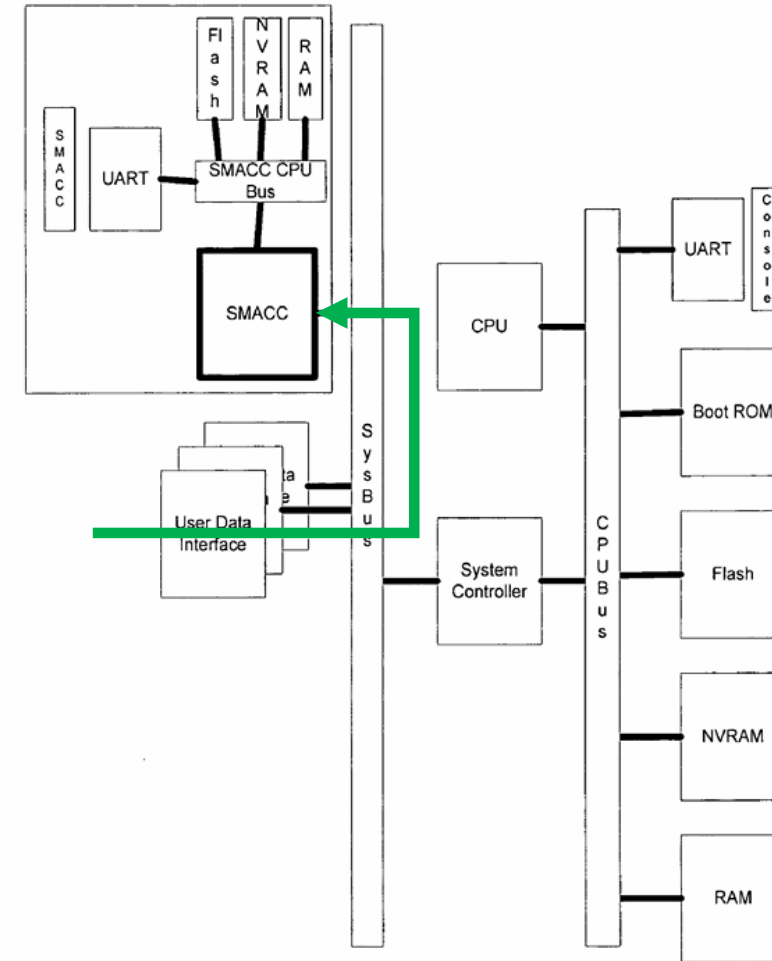


Fig. 19

Neufeld at most teaches a generic VPN

EX1005, ¶[0009]; EX1046, ¶109. Neufeld further discloses that in order for a network administrator to access the server from a remote terminal located outside of work, the administrator must typically use a VPN. EX1005, ¶[0022]; *see also id.*, ¶[0088, Table 4, User Id 7]; EX1046, ¶110. A POSITA would have understood such access involves communications with Neufeld's remote server management controller 116 given that it is a network administrator that is accessing the server. EX1046, ¶110.

Petition, 32-33

110. Neufeld further discloses that in order for a network administrator to access the server (which a POSITA would have understood involves communications with Neufeld's remote server management controller 116 given that it is a network administrator that is accessing the server) from a remote terminal located outside of work, the administrator must typically use a virtual private network. EX1005, ¶[0022]; *see also* ¶[0088, Table 4, User Id 7]. A POSITA would have understood such access involves communications with Neufeld's remote server management controller 116 given that it is a network administrator that is accessing the server. EX1046, ¶110.

EX1046, [0110]

Paragraph [0022] is in the background describing prior systems

METHOD AND APPARATUS FOR CONFIGURING SECURITY OPTIONS IN A COMPUTER SYSTEM

BACKGROUND OF THE INVENTION

[0001] 1. Field of the Invention

[0002] This invention relates generally to computer security systems and, more particularly, to a technique for providing user profiles.

[0003] 2. Background of the Related Art

[0004] This section is intended to introduce the reader to various aspects of art which may be related to various aspects of the present invention which are described and/or claimed below. This discussion is believed to be helpful in providing the reader with background information to facilitate a better understanding of the various aspects of the present invention. Accordingly, it should be understood that these statements are to be read in this light, and not as admissions of prior art.

[0005] Since the introduction of the first personal computer ("PC") over 20 years ago, technological advances to make PCs more useful have continued at an amazing rate. Microprocessors that control PCs have become faster and faster, with operational speeds eclipsing the gigahertz (one billion operations per second) and continuing well beyond.

[0006] Productivity has also increased tremendously because of the explosion in development of software applications. In the early days of the PC, people who could write their own programs were practically the only ones who could make productive use of their computers. Today, there are thousands and thousands of software applications ranging from games to word processors and from voice recognition to web browsers.

[0007] In addition to improvements in PC hardware and software generally, the technology for making computers more useful by allowing users to connect PCs together and share resources between them has also seen rapid growth in recent years. This technology is generally referred to as "networking." In a networked computing environment, PCs belonging to many users are connected together so that they may communicate with each other. In this way, users can share access to each other's files and other resources, such as printers. Networked computing also allows users to share internet connections, resulting in significant cost savings. Networked computing has revolutionized the way in which business is conducted across the world.

[0008] Not surprisingly, the evolution of networked computing has presented technologists with some challenging obstacles along the way. One obstacle is the sheer scope of modern computer networks. At one end of the spectrum, a small business or home network may include a few client computers connected to a common server, which may provide a shared printer and/or a shared internet connection. On the other end of the spectrum, a global company's network environment may require interconnection of hundreds or even thousands of computers across large buildings, a campus environment, or even between groups of computers in different cities and countries. Such a configuration would typically include a large number of servers, each connected to numerous client computers.

[0009] Further, the arrangements of servers and clients in a larger network environment could be connected in any of a large number of topologies that may include local area networks ("LANs"), wide area networks ("WANs"), and municipal area networks ("MANs"). Clients may also have the ability to access these networks via a virtual private network ("VPN") or via the Internet.

[0010] An important aspect of efficiently managing a large computer network is to maximize the amount of analysis and repair that can be performed remotely (for example, from a centralized administration site). Tools that facilitate remotely analyzing and servicing server problems help to control network management costs by reducing the number of network management personnel required to maintain a network in good working order. Remote server management also makes network management more efficient by reducing the delay and expense of analyzing and repairing network problems. Using remote management tools, a member of the network management team may identify problems and, in some cases, solve those problems without the delay and expense that accompanies an on-site service call to a distant location.

[0011] Remote management tools can communicate with a managed server using either (1) in-band communication or (2) out-of-band communication. In-band communication refers to communicating with the server over a standard network connection, such as the managed server's normal Ethernet connection. In-band communication with the server is, accordingly, only possible when the server is able to communicate over its normal network connection. Practically speaking, this limitation restricts in-band communication to times when the OS of the managed server is operational (online).

[0012] Out-of-band communication, which is not performed across the managed server's normal connection to the network, is a much more powerful tool for server management. In out-of-band communication, a "back door" communication channel is established by a remote server management tool (such as a remote console or terminal emulator) using some other interface with the server (such as (1) through the server's modem, (2) via a direct connection to a serial port, (3) through an infrared communication port, or (4) through an Ethernet interface or the Internet).

[0013] In a sense, out-of-band communication is like opening an unobtrusive window through which the inner workings of the operation of the managed server may be observed. After the out-of-band communication link with the server is established, the remote server management tool communicates with the server to obtain data that will be useful to analyze a problem or potential problem. After a problem has been analyzed, out-of-band communication may be possible to control the managed server to overcome the problem or potential problem.

[0014] In addition to the distinction between in-band and out-of-band communication with a managed server, another important distinction is whether the managed server is online or offline. The term "online" refers to a managed server in which the OS is up and running. The managed server is said to be "offline" if its OS is not up and running. Communications with a managed server may take place in one of these four states: (1) in-band online; (2) in-band offline; (3) out-of-band online; and (4) out-of-band offline.

[0015] An important goal in the development of remote server management tools is to increase the number of server problems that may be analyzed and repaired remotely (that is, without requiring direct, on-site intervention by a member of the network management team). To facilitate that goal, it is highly desirable to have a network management tool that is able to capture the maximum amount of information from a managed server in the maximum range of operational states of the server (for example, (1) in-band online; (2) in-band offline; (3) out-of-band online; and (4) out-of-band offline) and to allow control of the managed server based on that data.

[0016] Current remote management solutions combine the advantages of deep information gathering capability (software agent-based information gathering technology available when the OS of the managed server is online) with the ability to control the operation of the managed server independently via an out-of-band communication session using the dedicated server management computer system hosted in the managed server. Such remote management tools may also include the capability to capture video data and reset sequences from the managed server for remote display or replay at a later time. The capture of video data is facilitated by the close integration of a remote management tool with the managed server and the ability of the remote management tool to communicate with the managed server over existing communication links (such as an industry standard PCI bus). The ability of a remote management tool to capture video data from a managed server is a particularly powerful analysis tool because it lets a remote user have "virtual access" to the managed server, just as if the user was physically present and inspecting the managed server in person.

[0017] In a typical remote management system, a user (typically, a member of the network management team) can initiate an out-of-band session with the dedicated server management computer hosted in the managed server via a remote console application program being executed on a client computer. The management computer could be addressed by the user to control various aspects of the operation of the managed server via control circuitry connected to the embedded server management computer hosted by the managed server.

[0018] Regardless of whether the remote computer is communicating with the server to manage it or to carry out some other function, such as web serving, file sharing, device sharing, etc., security may be a very important issue. Indeed, computer security is becoming increasingly important in today's environment of heavily networked computer systems. As a result, security and integrity features are becoming desirable in the use of personal computers and servers. Providing security of a system involves protecting the system from a variety of possible attacks. Such security provisions may include protecting the system from accesses by hackers or other unauthorized entities. For example, for a specific business with proprietary internal systems and data, security systems may involve prevention of rogue or external devices from accessing the internal machines. Prevention of access by unauthorized external devices may be particularly problematic if the internal system is configured for remote access via a publicly accessible network, such as the Internet.

[0019] Remote access can be problematic, particularly when authentication and access control are required. Typically, remotely accessible devices, such as servers, have relied on locally defined lists of users and passwords to perform such authentication and access control. Unfortunately, network administrators must maintain these lists on multiple systems, and users often must keep track of separate accounts and passwords. Thus, this type of system is both time consuming and difficult to manage.

[0020] Certain techniques can significantly increase user convenience by replacing difficult-to-manage passwords with biometrics and/or smartcard technology. In regard to the latter, smartcards have long been proposed for holding digital certificates, private keys, and other means of proving one's identity. However, in the United States, they have not been widely deployed for various reasons. For example, companies have appeared reluctant to utilize smartcard technology due to the expense of retrofitting existing computers with smartcard readers. However, once implemented, smartcards require that users need only swipe the smartcard and type in a personal identification number to provide appropriate authentication.

[0021] Even with the use of passwords, personal identification numbers, and smartcards, a system is still only able to authenticate a computer and not a person because anyone who can guess or steal a user's password, personal identification number, and/or smartcard can digitally sign electronic documents and access data in that user's name. The formerly mentioned biometrics technology can be employed to solve some of these problems. In biometrics, a unique personal feature of each user, such as a retinal or fingerprint image or a voice pattern, is stored instead of a password. Access to computer resources are granted using a fingerprint or retinal identification scheme in much the same way as in a password scheme. However, instead of supplying a password, the user places an eye in front of a retinal scanner or a finger on a fingerprint reader that scans the person's feature and compares it with the previously stored data. Barring a malfunction or bodily mutilation, an authorized user always has a "key" or "password," and unauthorized users cannot easily come into possession of it. Thus, biometrics solves the problems of authorized users who may have forgotten their password, as well as unauthorized users that may have come into possession of the password. Unfortunately, like smartcard technology, companies have been reluctant to embrace biometrics due to the expense of retrofitting existing computers with biometric scanners.

[0022] Furthermore, regardless of the manner in which a particular user is identified, the privileges granted to an authenticated user are typically the same regardless of when, where, or how the user accesses the system. However, it is believed to be desirable to alter authentication services and possibly to restrict access rights and privileges in some instances to improve security. For example, if a network administrator logs onto the system from a physically secure location where the network administrator's identification can be determined for the network administrator even to access the facility, the amount of user authentication and the number of restrictions placed upon a user in such a location need not be as onerous as user authentication procedures and restrictions placed upon users attempting to access the server from locations outside of the physically secure facility. Similarly, if the network administrator is accessing the

server from a remote terminal that is affiliated with the business yet located outside of the secure facility, user authentication and restrictions may not need to be as onerous during working hours, when the user's identification can be somewhat assured and the user's actions somewhat monitored, as opposed to non-working hours, when a hacker or intruder could have more easily gained access to the remote terminal. Finally, this situation is potentially even more problematic if the system administrator attempts to access the server from a remote terminal located outside of work, such as at home or while traveling. In this situation, the system administrator must typically use the Internet or a virtual private network to access the system. However, because such an access is attempted from a location not directly affiliated with the business, there can be no assurances of the actual identity of the user absent rigorous authentication. Even with rigorous user authentication, greater restrictions may be placed on the same user when accessing the system remotely as opposed to accessing the system at work or directly from a secure facility. Furthermore, in the case of remote operation, even if the identity of the user can be determined with absolute certainty, some operations may be inherently more problematic because the user is not physically close to the work group using the server and may not know about a problem the user causes while remotely accessing the server.

[0023] The present invention may be directed to certain issues discussed above.

BRIEF DESCRIPTION OF THE DRAWINGS

[0024] The foregoing and other advantages of the invention will become apparent upon reading the following detailed description and upon reference to the drawings in which:

[0025] FIG. 1 is a connection diagram of a managed server and a remote management console according to one embodiment;

[0026] FIG. 2 is a block diagram of the managed server according to the embodiment of FIG. 1; and

[0027] FIG. 3 is a block diagram of the remote management controller of FIG. 2.

DESCRIPTION OF SPECIFIC EMBODIMENTS

[0028] The following patents or patent applications are hereby incorporated by reference:

[0029] U.S. Pat. No. 5,898,861, entitled "Transparent Keyboard Hot Plug" by Theodore F. Emerson, Geoff M. Krantz and Dayang Dai;

[0030] U.S. Pat. No. 5,790,895, entitled "Modem Sharing" by Theodore F. Emerson and Geoff M. Krantz;

[0031] U.S. patent application Ser. No. 08/733,254, entitled "Video Eavesdropping and Reverse Assembly to Transmit Video Action to a Remote Console" by Theodore F. Emerson, Peter J. Michaels and Geoff M. Krantz, filed Oct. 18, 1996; and

[0032] U.S. patent application Ser. No. 09/438,253, entitled "Operating System Independent Method and Apparatus for Graphical Remote Access" by Theodore F. Emerson and Wesley Ellinger, filed Nov. 12, 1999.

[0033] One or more specific embodiments of the present invention will be described below. In an effort to provide a concise description of these embodiments, not all features of an actual implementation are described in the specification. It should be appreciated that in the development of any such actual implementation, as in any engineering or design project, numerous implementation-specific decisions must be made to achieve the developers' specific goals, such as compliance with system-related and business-related constraints, which may vary from one implementation to another. Moreover, it should be appreciated that such a development effort might be complex and time consuming, but would nevertheless be a routine undertaking of design, fabrication, and manufacture for those of ordinary skill having the benefit of this disclosure. Indeed, an actual implementation of certain subject matter set forth herein may be found in Model DL360G2 available from Compaq Computer Corporation.

[0034] Referring first to FIG. 1, there is illustrated a managed server 2 connected to a remote console 5 by a network N. The managed server 2 includes a central processing unit ("CPU") 3 housing processing, memory, communications, interface, and other circuitry as described more fully below, and may be connected to a monitor 4. The remote console 5 also includes a CPU 6 and a monitor 8. The managed server 2 includes special circuitry and software for capturing, analyzing, compressing and transmitting video activity to the remote console 5 independent of an operating system ("OS"). The special circuitry and software operate without regard to the existence or type of OS present on the managed server 2. Therefore, the present technique may be useful for accessing, interacting, and/or monitoring the managed server 2 from the remote console 5 even before its OS has been loaded. More specifically, the video displayed on monitor 4 is capable of being viewed on a monitor 8 independent of the OS.

[0035] The network N can be virtually any sort of network capable of transmitting data between two devices. Without limitation, some examples of networks include: a local area network, a wide area network, a hardwired point-to-point connection, a point-to-point connection over a telecommunications line, a wireless connection, and an Internet connection.

[0036] Although the managed server 2 shown is of an International Business Machines (IBM) PC-compatible variety, the principles of the present technique are believed to be equally applicable to other computer platforms or architectures, such as those manufactured by Compaq, Apple, Sun, and Hewlett Packard. Additionally, the managed server 2 could be one architecture and the remote console 5 could be another. For example, the managed server 2 could be a x86 architecture computer running Microsoft Windows NT OS and the remote console 5 could be a Sun workstation running Solaris OS.

[0037] In the operation of the present technique, video data is captured, analyzed, compressed, and transmitted to the remote console 5 by circuitry and software in the managed server 2 without reliance or interference with the operating system. The remote console 5 includes software for receiving and interpreting the transmitted data to reproduce on its own monitor 8 the video data displayed on the

Neufeld's Paragraph [0022] the common usage of VPNs

•[0022] Furthermore, regardless of the manner in which a particular user is identified, the privileges granted to an authenticated user are typically the same regardless of when, where, or how the user accesses the system. However, it is believed to be desirable to alter authentication services and possibly to restrict access rights and privileges in some instances to improve security. For example, if a network administrator logs onto the system from a physically secure location where the network administrator's identification can be determined for the network administrator even to access the facility, the amount of user authentication and the number of restrictions placed upon a user in such a location need not be as onerous as user authentication procedures and restrictions placed upon users attempting to access the server from locations outside of the physically secure facility. Similarly, if the network administrator is accessing the server from a remote terminal that is affiliated with the business yet located outside of the secure facility, user authentication and restrictions may not need to be as onerous during working hours, when the user's identification can be somewhat assured and the user's actions somewhat monitored, as opposed to non-working hours, when a hacker or intruder could have more easily gained access to the remote terminal. Finally, this situation is potentially even more problematic if the system administrator attempts to access the server from a remote terminal located outside of work, such as at home or while traveling. In this situation, the system administrator must typically use the Internet or a virtual private network to access the system. However, because such an access is attempted from a location not directly affiliated with the business, there can be no assurances of the actual identity of the user absent rigorous authentication. Even with rigorous user authentication, greater restrictions may be placed on the same user when accessing the system remotely as opposed to accessing the system at work or directly from a secure facility. Furthermore, in the case of remote operation, even if the identity of the user can be determined with absolute certainty, some operations may be inherently more problematic because the user is not physically close to the work group using the server and may not know about a problem the user causes while remotely accessing the server.

Neufeld describes an out of band
system

Neufeld's Commands are received via Ethernet Interface 180

[0061] The embedded I/O controller 150 may also include an Ethernet interface 180, which is operatively coupled to the internal local bus 166. The Ethernet interface 180 provides the main external communication interface between the remote server management controller 116 and the outside world. In the exemplary embodiment shown in FIG. 3, the integrated portion of the Ethernet interface 180 includes a MAC (Media Access Controller), inbound and outbound FIFOs and a DMA engine to transfer packets automatically to and from memory. The Ethernet interface 180 utilizes a connection via interface 182 to an external PHY 183 and typical magnetics and connectors 185 to couple the PHY 183 to the wire that serves as the transmission media. For example, this connection is typically used to couple the remote management controller 116 to the management network M.

EX1005, [0069]

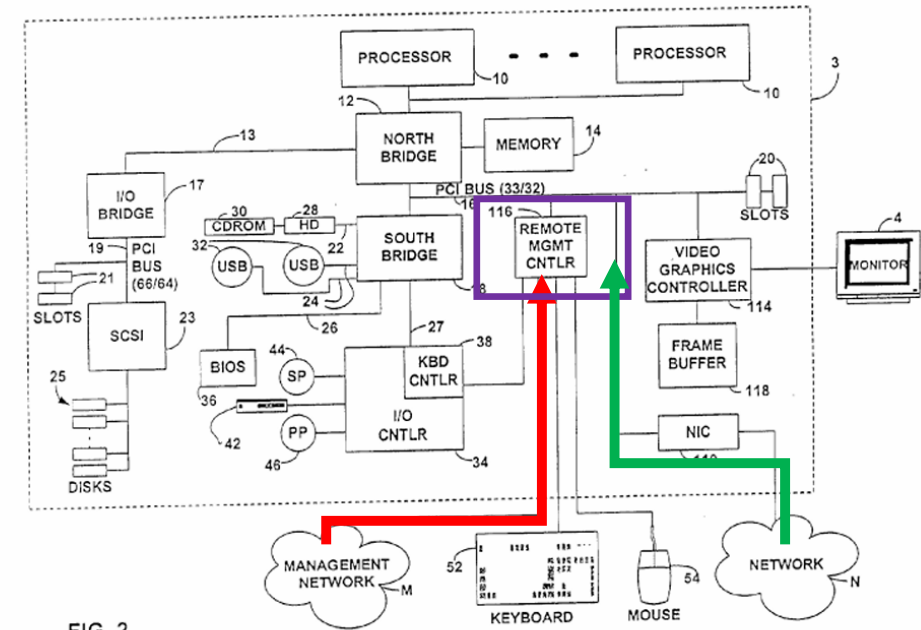


FIG. 2

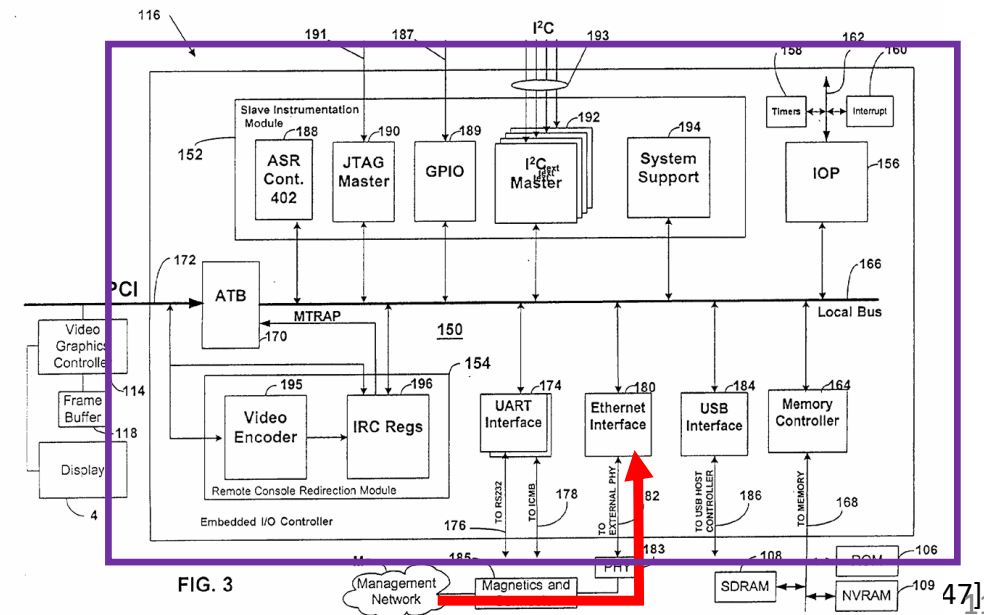


FIG. 3

"DEMONSTRATIVE EXHIBIT

Petitioner Offered No Evidence That Neufeld is in-band

Paragraph [0043] describes FIG. 2 (below) and states “[t]he remote management controller 116 connects to the keyboard controller 38, *the network N and/or a management network M*, a keyboard 52, and a mouse 54 to provide functionality for accessing, interacting, and monitoring the managed server 2 from the remote console 5” FIG. 2, nevertheless, *only shows* the network M passing through the RMC, with the Network N coupled to the NIC, which is coupled to the PCI Bus. From paragraph [0043] and FIG. 2, alone, Neufeld’s intention is un-clear. Paragraph [0043] states that the RMC connects to one, the other, or both, of Network N and/or M, but FIG. 2 only shows the RMC connected to the management network M, and not N.

Sur-Reply, 15-16

At best, paragraph [0043] is ambiguous when compared to the clear disclosure in the figures and the explicit description of the Ethernet interface 180 as the RMC’s “main external communication interface.” *Id.* at ¶ [0061]. Such ambiguity cannot substitute for actual disclosure of the claimed limitation. *See LG Elecs. Inc. v. Immervision, Inc.*, 39 F.4th 1364, 1372 (Fed. Cir. 2022) (“[W]here a prior art reference includes an obvious error of a typographical or similar nature that would be apparent to one of ordinary skill in the art who would mentally disregard the errant information as a misprint or mentally substitute it for the correct information, the errant information cannot be said to disclose subject matter.”).

Sur-Reply, 17

Patent Owner's Expert Confirms Neufeld is unclear and self contradictory

A. . . . Neufeld has inconsistencies. What will make sense is to go over the management network. There are mentions somewhere in Neufeld . . . , sometimes they refer to network N, but for mechanisms that don't make sense. So that is . . . what I explain in [my] declaration, and I tried to reconcile these things.

. . .

A. [T]o me, Neufeld, as the abstract says, it is a security system [that] includes different authentication levels and/or different privileges based on certain criteria.

So it is more about privileges . . . and higher level things and so on. The claims are all about that. It has description of various kind of things. A POSITA reading these things . . . will get confused because there are things that are inconsistent. The out-of-band . . . that's the one that will make sense. The other, the in-band, even if there are references to it . . . I explained a little bit how to try to make sense of that.

Q. Okay. Let's go to paragraph 46 of your declaration. . . .

You say the management network M . . . is in fact the only network coupled to Neufeld's remote server management controller 116, correct?

A. Yes.

Q. Now you're aware, and you discussed in your declaration . . . that paragraph 43 of Neufeld says something different. Paragraph 43 of Neufeld . . . says that the remote management controller 116 connects to a keyboard controller 38, the network N . . . and/or a management network M . . . and then some other devices, correct?

A. Yes.

Q. Okay. So your statement in paragraph 46 that the RMC 116 is only connected to network M is not correct in light of paragraph 43

because paragraph 43 says that the RMC is connected to the network N, correct?

A. No. What . . . I'm saying there . . . is . . . in Figure 3 of Neufeld the ethernet interface is coupled to the network [M]. The management network [M] is the only network coupled to Neufeld's remote server management.

And here by "coupled" I'm meaning that it has full control over it.

". . . At first glance, paragraph [0043]" . . . "may appear to suggest a contradiction by stating that the remote management controller 116 connects to . . . the network N and/or the management network M".

So basically . . . I'm explaining . . . that there is something inconsistent in some sense with how POSITA would have understood Neufeld. And . . . one of the last sentences [in my declaration] is that "POSITA would recognize that the reference to network N merely identifies that the remote management controller can passively monitor the data sent to or received from the managed device over the network; it must be connected to that path to snoop on the traffic, but that connection does not equate to active participation in the data transmission or use of the primary network interface for management communication".

Sur-Reply, 20-21

The burden is on Petitioner to demonstrate, by a preponderance of the evidence, that Neufeld teaches or suggests the claimed limitation. 35 U.S.C. § 316(e). **Where the prior art is contradictory or unclear, the Petitioner has not met its burden, and the Board must resolve that doubt against the challenger.** Neufeld repeatedly emphasizes OS-independent, out-of-band management via the Network M. Petitioner's theory depends on importing functionality Neufeld neither discloses nor suggests. That type of hindsight reconstruction cannot support a finding of obviousness.

Sur-Reply, 22

Logical Separation Requires Transmission over the same interface

The Petition fails to cite any passage in Neufeld for the “separation of management data from user data” claim element showing that management data is transmitted over the in-band network N. *See* Petition, 32:6-34:14. Moreover, the Petitioner fails to realize that *all management data in Neufeld is transmitted over the management network M*. *See id.* As made in clear in Neufeld: “[i]n-band communication with the server is . . . only possible when the server is able to communicate over its normal network connection.” Practically speaking, this limitation restricts in-band communication to times when the OS of the managed server is operational.” *See* Ex. 1005 at ¶ [0011]. Indeed, the management network M is the only network coupled to any of the communication interfaces of the remote management controller 116 in Neufeld – in both FIGs. 2 and 3, the Network N is coupled to the PCI bus, outside of the remote management controller 116.

POR, 28

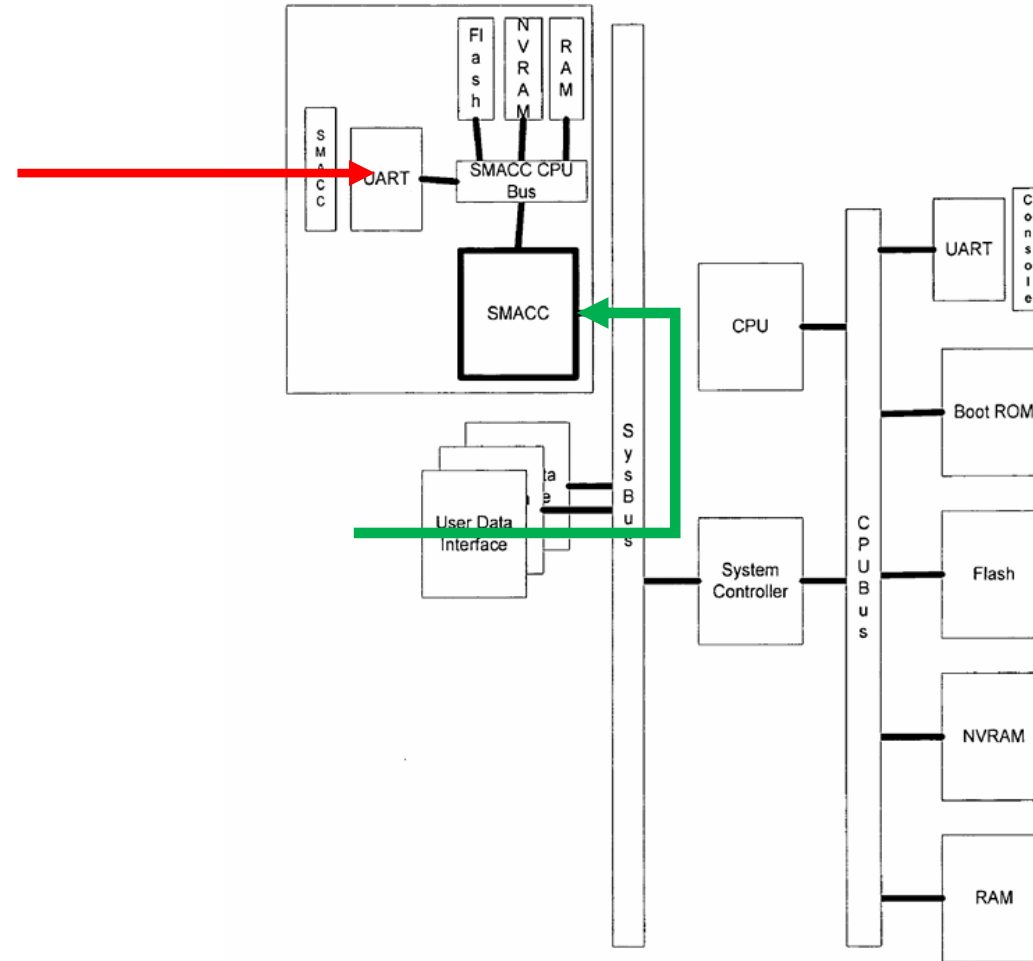
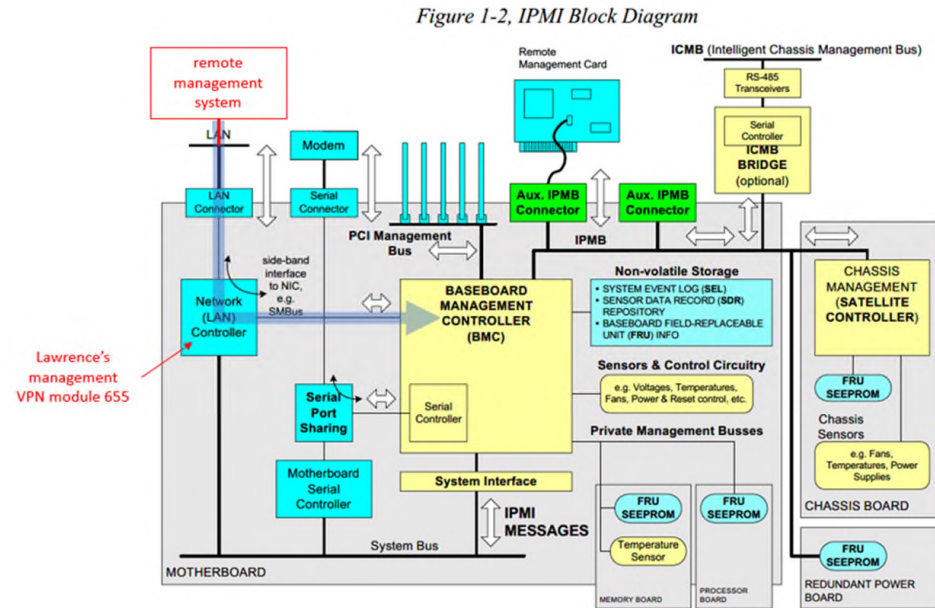


Fig. 19

A POSITA would not combine
IPMI and Lawrence

A POSITA would not utilize a VPN within a computer



This implementation of IPMI's side-band interface using Lawrence's VPN technology is the identical structure for this limitation disclosed in the 140 patent, namely a VPN. Both structures perform the identical claimed functions – connecting remote users (e.g., on IPMI's remote management system) with the BMC and providing logical separation of IPMI management data from user data utilizing the same LAN interface of the managed system and the network connected thereto. EX1046, ¶176.

Petition, 62

Institution Decision Confirm that a POSITA would not use a VPN on an internal connection

We view Petitioner's arguments as focusing on IPMI's side-band interface, and do not address having a VPN connect to the remote user. *See* Pet. 51–54, 64–65. Thus, at this stage, we agree with Patent Owner that Petitioner does not sufficiently show why one of ordinary skill in the art would have been motivated to use a VPN on an internal connection (side-band interface) within a server, absent such security on the external connection portion. *See* Prelim. Resp. 51–52. Similarly, we also find that Petitioner does not clearly explain how the corresponding structure (the VPN) “connect[s] said one or more . . . remote users with said secure management access controller.” *See* Pet. 65.

Institution Decision, 29

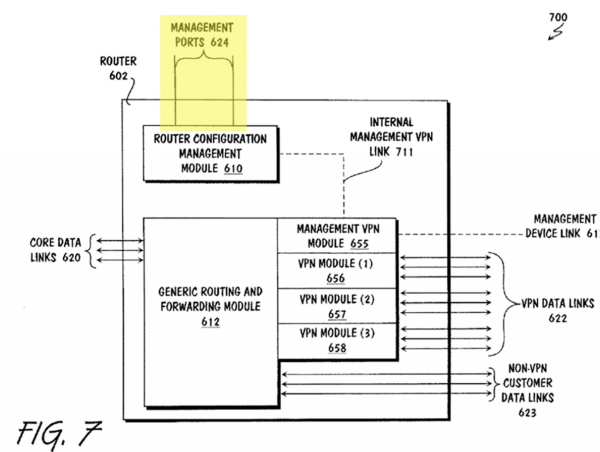
Accordingly, the basic functionality of LAN controllers is to route packets based on their addresses, and the LAN controller in IPMI does that without the addition of a VPN. In fact, if IPMI's LAN controller was combined with a VPN, as Petitioner suggests, and then encountered VPN packets, it would route them exactly the same as every other packet because, from the perspective of the LAN controller, the packets have the same destination address, and hence, are indistinguishable. There is simply nothing missing from IPMI that would have caused a POSITA to go looking for Lawrence. Therefore, as the Institution Decision acknowledges, “one of ordinary skill in the art would [not] have had a rational reason to combine IPMI and Lawrence's teachings as Petitioner does.” Institution Decision at 29.

POR, 42

Petitioner Offers a New Flawed Theory

The Petition notes that Lawrence discusses the advantages of in-band communication between management devices (e.g., remote management consoles) and managed devices, but specifically identifies the disadvantage such communications were performed in prior art systems over non-secure links and were thus susceptible to unauthorized management entry or interception of management commands. Petition, 53 (citing EX1043, 2:20-58). The Petition relies on Lawrence's Fig. 7 embodiment, which discusses secure in-band communication of management data and Lawrence's management VPN module 655. Petition at 53-54, citing Lawrence at 5:15-30 and 5:37-47. The passage of Lawrence at 5:15-30 specifically states that generic forwarding module 612 is coupled to the management VPN module 655. EX1043, 5:19-21. The disclosures that unsecured in-band communications were disadvantageous and that incoming management messages are routed to the management VPN module 655 indicate to a POSITA that the management traffic from a management device received over an external network at the generic routing and forwarding module 612 are protected by a VPN. traffic is protected by a VPN. Thus, while the focus of the Petition was directed toward the unique aspect of the Fig. 7 embodiment's use of an additional VPN to protect the internal link 711, Petitioner respectfully submits that a fair reading of the Petition and the passages of Lawrence cited therein establish that incoming remote management messages were also protected by a management VPN implemented by Lawrence's VPN module 655.

Reply, 21-22



Petition, 63

This serial interface/modem/PSTN structure disclosed by IPMI performs the identical function of connecting a remote user at the remote management system with the BMC for out-of-band communication of management data, and is the

This argument should be disregarded as an improper *new theory*. The Petition did not raise or rely on these passages of Lawrence, thus necessitating using them for the first time in its Reply. Petitioner's attempt to now rewrite its motivation-to-combine theory is barred by § 42.23(b) and controlling case law. Petitioner's theory also fails substantively as it amounts to an explanation of how Lawrence allegedly operates, not an explanation of why a POSITA would have been motivated to modify IPMI in view of Lawrence. See Reply at 20-21 (discussing Lawrence and not the alleged Lawrence/IPMI combination). Such discussion does not supply the missing rationale to bridge the two references. Accordingly, Petitioner's Reply both procedurally exceeds the scope of § 42.23(b) and substantively fails to cure the defect identified by the Board. The new argument should be disregarded, and even if considered, it cannot establish a motivation to combine IPMI and Lawrence.

Sur-Reply, 25

Conclusion

- Grounds I-IV Fail
 - Neufeld Neither Discloses Nor Suggests a VPN/VMI That Terminates Behind the NIC
 - Neufeld teaches an out of band system
 - Logical separation requires in band
- Grounds V-IX Fail
 - A POSITA would not combine IPMI and Lawrence
 - Petitioner's new theory does not correct this defect

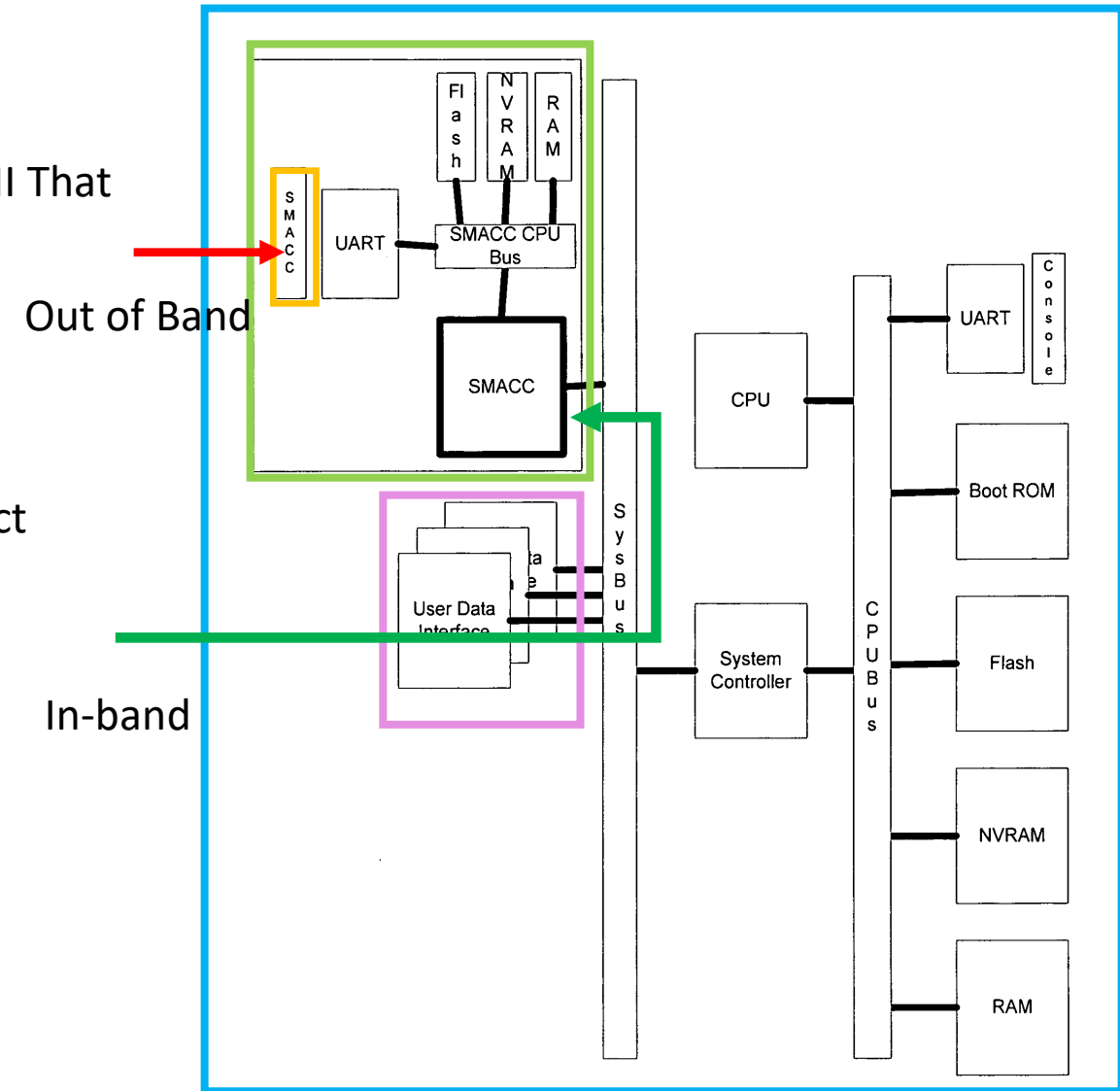


Fig. 19