

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

LENOVO (UNITED STATES) INC.,

Petitioner,

v.

INTELLECTUAL VETURES II, LLC,

Patent Owner

Case No. IPR2024-00109

U.S. Patent No. 8,474,016

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

PATENT OWNER’S EXHIBIT LIST	v
I. INTRODUCTION	1
II. SPECIFICATION OF '016 PATENT.....	4
A. Background.....	4
1. Maintenance and Trouble Shooting of Distributed Computer Networks ..	4
2. Tradeoffs Security of Network Elements and Servers in a Remote Management System.....	5
3. Problem Addressed By This Application.....	7
B. DETAILED DESCRIPTION	8
1. SMACC	8
2. Virtual Management Interface (VMI)	11
a) Connecting Remote Administrator with SMACC.....	11
b) Separating Management Data from User Data.....	12
c) In-Band Communication of Management Data (Using User Data Interfaces of Managed Device).....	12
3. Encrypted Management Requests	13
III. PRIOR ART RELIED ON IN THE PETITION.....	14
A. Neufeld	14
B. Frantz	18
C. PCI-to-PCI Bridge Architecture Specification (PCI Bridge Spec)	20
D. Intelligent Platform Management Interface Specification V1.5 (IPMI) ..	21
E. Huckins	24
F. Intelligent Platform Management Interface Specification v2.0 (IPMI v2.0)	25
IV. THE PETITION FAILS TO DEMONSTRATE A REASONABLE LIKELIHOOD OF SUCCESS ON THE MERITS	26

A.	Independent Claim 1 is Not Obvious Over Neufeld Pursuant To 35 U.S.C. § 103	26
1.	Neufeld Does Not Disclose “A Bus Controller Coupled To The Processor Via The First Bus” As Required By Claim 1	27
a)	Petitioner’s Expert Declaration Should Be Given Little, If Any, Weight	29
2.	Neufeld Fails to Disclose “Wherein The Bus Controller Is Also Coupled To A Second Bus Of The Network Device That Is Distinct From The First Bus” As Required By Claim 1	32
3.	Neufeld Fails to Disclose “The Bus Controller Is Configured To Receive The Encrypted Form Of The Management Requests From The Second Bus” As Required By Claim 1	33
4.	Neufeld Fails to Disclose “To Convey The Encrypted Form Of The Management Requests To The Processor Via The First Bus” As Required By Claim 1	35
5.	Neufeld Fails to Disclose “Wherein The Processor Is Configured To Decrypt The Encrypted Form Of The Management Requests” As Required By Claim 1	41
6.	Neufeld Fails to Disclose “The Bus Controller Is Configured To Receive The Encrypted Form Of The Management Requests From The Second Bus”, “And To Convey The Encrypted Form Of The Management Requests To The Processor Via The First Bus”, “Wherein The Processor Is Configured To Decrypt The Encrypted Form Of The Management Requests”, as required by claim 1 As Required By Claim 1	43
B.	Independent Claim 1 is Not Obvious Over Neufeld, Frantz, and PCI Bridge Spec Pursuant To 35 U.S.C. § 103	45
1.	The Combination Of Neufeld, Frantz, and PCI Bridge Spec Does Not Disclose “A Bus Controller Coupled To The Processor Via The First Bus” As Required By Claim 1	45
2.	The Combination Of Neufeld, Frantz, and PCI Bridge Spec Fails to Disclose “Wherein The Bus Controller Is Also Coupled To A Second Bus Of The Network Device That Is Distinct From The First Bus” As Required By Claim 1	49

3. The Combination Of Neufeld, Frantz and PCI Bridge Spec Fails to Disclose “The Bus Controller Is Configured To Receive The Encrypted Form Of The Management Requests From The Second Bus”, “And To Convey The Encrypted Form Of The Management Requests To The Processor Via The First Bus”, “Wherein The Processor Is Configured To Decrypt The Encrypted Form Of The Management Requests”, as required by claim 1 As Required By Claim 1	50
C. Independent Claim 1 is Not Obvious Over IPMI, Frantz, and Huckins Pursuant To 35 U.S.C. § 103	52
1. The Combination Of IPMI, Frantz, and Huckins Does Not Disclose “The Network Device Is Configured To Receive Data Requests And An Encrypted Form Of Management Requests Via The Network Interface” As Required By Claim 1	53
2. The Combination Of IPMI, Frantz, and Huckins Does Not Disclose “A Bus Controller Coupled To The Processor Via The First Bus” As Required By Claim 1	55
3. The Combination Of IPMI, Frantz, and Huckins Does Not Disclose “Wherein The Bus Controller Is Also Coupled To A Second Bus Of The Network Device That Is Distinct From The First Bus” As Required By Claim 1	60
4. The Combination Of IPMI, Frantz, and Huckins Does Not Disclose “The Bus Controller Is Configured To Receive The Encrypted Form Of The Management Requests From The Second Bus” As Required By Claim 1	60
5. The Combination Of IPMI, Frantz, and Huckins Does Not Disclose “And To Convey The Encrypted Form Of The Management Requests To The Processor Via The First Bus” As Required By Claim 1	61
6. The Combination Of IPMI, Frantz, and Huckins Does Not Disclose “The Bus Controller Is Configured To Receive The Encrypted Form Of The Management Requests From The Second Bus”, “And To Convey The Encrypted Form Of The Management Requests To The Processor Via The First Bus”, “Wherein The Processor Is Configured	

	To Decrypt The Encrypted Form Of The Management Requests”, as required by claim 1	61
D.	Independent Claim 1 is Not Obvious Over IPMI, IMPIV2.0, and Huckins Pursuant To 35 U.S.C. § 103.....	64
V.	PETITIONER HAS NOT MET ITS BURDEN OF PROVING UNPATENTABILITY OF THE CHALLENGED CLAIMS	65
VI.	CONCLUSION.....	68

PATENT OWNER'S EXHIBIT LIST

EX2001	Declaration of Dr. Steven Goldberg
EX2002	Resume of Dr. Steven Goldberg
EX2003	Information Security Management: Global Challenges in the New Millennium, Gurpreet Dhillon, Idea Group Publishing., 2001
EX2004	The Froehlich/Kent Encyclopedia of Telecommunications, Vol. 9, Editor in Chief: Fritz E. Froehlich, 1990
EX2005	Scott Mueller's UPGRADING AND REPAIRING PCs, Scott Mueller, Que Publishing, August 2003.

I. INTRODUCTION

Petitioner challenges claims 1-3, 6-9, 12, and 14-17 (hereinafter, “Challenged Claims”) of the US 8,474,016 (hereinafter “’016”) Patent on 15 grounds. The ‘016 Patent has 21 total claims, with claim 1 and 12 being independent.

In ground 1, Petitioner challenges independent claims 1 and 12, and certain dependent claims, as allegedly obvious over U.S. Patent Appl. Pub. No. 2003/0226015 to Neufeld et al. (hereinafter “Neufeld”).

In ground 2, Petitioner challenges independent claims 1 and 12, and certain dependent claims, as allegedly obvious over Neufeld, U.S. Patent No. 7,085,385 to Frantz et al. (hereinafter, “Frantz”), and PCI-to-PCI Bridge Architecture Specification Revision 1.1, December 18, 1998 (hereinafter, “PCI Bridge Spec”).

In ground 3, Petitioner challenges dependent claim 2 as allegedly obvious over Neufeld, Frantz, PCI Bridge Spec and U.S. Patent No. 6,219,708 to Martenson (hereinafter “Martenson”).

In ground 4, Petitioner challenges dependent claim 3 as allegedly obvious over Neufeld, Frantz, PCI Bridge Spec and U.S. Patent No. 5,654,137 to MacWilliams et al. (hereinafter “MacWilliams”).

In ground 5, Petitioner challenges dependent claims 7 and 16 as allegedly obvious over Neufeld, Frantz, PCI Bridge Spec, U.S. Patent No. 7,260,555 to

Rossman et al. (hereinafter “Rossman”) and RFC1492: An Access Control Protocol, Sometimes Called TACACS (hereinafter “RFC1492”).

In ground 6, Petitioner challenges dependent claim 8 as allegedly obvious over Neufeld, Frantz, PCI Bridge Spec and U.S. Patent Publication No. 2003/0097590 to Syvanne (hereinafter “Syvanne”).

In ground 7, Petitioner challenges dependent claim 14 as allegedly obvious over Neufeld, NTP AAPA, Frantz, PCI Bridge Spec and U.S. Patent No. 7,383,577 to Hrastar et al. (hereinafter “Hrastar”).

In ground 8, Petitioner challenges dependent claim 15 as allegedly obvious over Neufeld, Frantz, PCI Bridge Spec and RFC1157: A Simple Management Network Management Protocol (SNMP) (hereinafter RFC1157).

In ground 9, Petitioner challenges independent claims 1 and 12, and certain dependent claims, as allegedly obvious over Intelligent Platform Management Interface Specification V 1.5 (hereinafter, “IPMI”), Frantz, and U.S. Patent Appln. Pub. No. 2003/0097503 to Huckins (hereinafter, “Huckins”).

In ground 10, Petitioner challenges independent claims 1 and 12, and certain dependent claims, as allegedly obvious over IPMI, Intelligent Platform Management Interface Specification V 2.0 (hereinafter, “IPMI V2.0”), and Huckins.

In ground 11, Petitioner challenges dependent claim 6 as allegedly obvious over IPMI, Frantz or IPMIv2.0, Huckins, and VPN AAPA and/or Rossman.

In ground 12, Petitioner challenges dependent claims 7 and 16 as allegedly obvious over IPMI, Frantz or IPMIv2.0, Huckins, Rossman, and RFC1492 or RFC2865: Remote Authentication Dial In User Service (RADIUS) (hereinafter RFC2865).

In ground 13, Petitioner challenges dependent claim 8 as allegedly obvious over IPMI, Frantz or IPMIv2.0, Huckins, and Syvanne.

In ground 14, Petitioner challenges dependent claim 14 as allegedly obvious over IPMI, Frantz or IPMIv2.0, Huckins, and NTP AAPA and/or Hrastar.

In ground 15, Petitioner challenges dependent claim 15 as allegedly obvious over IPMI, Frantz or IPMIv2.0, Huckins, and RFC1157.

Dependent claims 4, 5, 10, 11, 13, and 18-21 are not challenged.

The Board should find that Petitioner has failed to demonstrate the unpatentability of the Challenged Claims. The cited references (Neufeld, Frantz, PCI Bridge Spec, Martenson, MacWilliams, Rossman, RFC1492, Syvanne, NTP AAPA, Hrastar, RFC1157, Huckins, IPMI, IPMIv2.0, VPN AAPA, Rossman, and RFC2865) lack at least one limitation of each of the Challenged Claims, and would not have been combined for the reasons alleged in the Petition by a person of ordinary skill in the art. Patent Owner's explanations herein are supported by the Declaration of Dr. Steven Goldberg, an expert in the field. EX2001.

II. SPECIFICATION OF '016 PATENT

The invention claimed in the '016 Patent addresses the technical problem of securely managing network devices remotely without compromising the security of the devices. The invention solves this problem by providing a computer network, which can be used to remotely manage a network device. More specifically, the Detailed Description of the '016 Patent describes “a Secure Management Access Control for Computer Chipset (SMACC) for inclusion in devices that are to be enabled for remote management.” EX1001, 5:50-52.

A. Background

1. Maintenance and Trouble Shooting of Distributed Computer Networks

Distributed computer networks are computer networks in which at least some, and usually most, of the network elements are not in the same geographic location. EX1001,1:31. For larger computer networks, including a large number of network elements distributed over a wide geographic area, network maintenance and/or everyday troubleshooting (collectively referred to hereafter as “network maintenance”) can become complex and difficult to implement in a secure manner. Technicians performing network maintenance, for example, need both regular and timely access to the network elements that can be geographically quite far away from the technician. EX1001,1:39-46. EX2001,¶ 31.

While arguably the most secure option for network maintenance is to require technicians to physically access any network element they work on, the distance between the technician and network elements also makes this the least practicable approach. EX1001,1:47-49. It would, for example, be prohibitively expensive to dispatch a technician to physically access every network element in a distributed system and would, in any event, take too much time to perform the required maintenance function. EX1001,1:49-51. At a minimum, computer networks implemented by businesses need to be operable at all times to enable employees, who generally work only during designated day time hours, to be able to perform work tasks in a timely manner. EX1001,1:39-46. Accordingly, businesses overwhelmingly use at least some form of remote management to maintain and troubleshoot network elements and servers. EX1001,1:51-53. EX2001,¶ 32.

2. Tradeoffs Security of Network Elements and Servers in a Remote Management System

Two general approaches to remote network management are in-band network access and out-of-band network access. In-band network access is generally a type of network access in which a remote administrator “communicates with the system using the same network as the network data for the managed system.” Out-of-band network access, on the other hand, is generally a type of network access in which a remote administrator “communicates with the system using a means other than the

network utilized by the user data of the managed system.” EX1001,1:55-60. EX2001,¶ 33.

Typically, when a network administrator accesses a network element using out-of-band communication, the administrator connects to a console or management port on the system. EX1001,1:60-63. This makes out-of-band communication a generally more secure option than in-band communication. For this reason, at least at the time the application for the ‘016 Patent was filed, out-of-band communication was considered the gold standard for remote network maintenance when it was not possible for network administrators to physically connect to all network elements to perform maintenance. EX1001,2:53-55. Relatedly, at least to some degree, in-band remote maintenance methods depend on the security of the network in which a network element being maintained resides to protect management traffic. While this is considered to potentially be a reasonable level of protection from external attacks, “it generally will not provide a sufficient level of protection from internal attacks (initiated from inside a network).” EX1001,2:19-22. Ex 2001,¶ 33.

Nevertheless, the use of out-of-band communication for network maintenance has certain drawbacks that need to be considered. Most significantly, using out-of-band communication for computer network maintenance requires “a dedicated network” to be built (“or at least dedicated network segments for remote network

administration of routers”), which can be prohibitively expensive EX1001,2:26-31. EX2001,¶ 34.

3. Problem Addressed By This Application

Because there are drawbacks to both in-band and out-of-band communication for network maintenance in distributed computer networks, distributed computer networks may use a combination of both in-band and out-of-band communication for network maintenance. However, in solutions where in-band communication is used, either as one option for network maintenance or as the only option, there is a problem with in-band communication that should be addressed, and that is addressed by the solutions described throughout the ‘016 Patent. That is: “[T]o control cost of most management solutions, user traffic, and management traffic are being comingled at multiple locations throughout the management path.”

The use of the user data network for the transport of management traffic is one place this comingling occurs. There is also a comingling of user and management data in the device itself. User traffic and device management traffic comes in over the same user interface, uses the same memory and buffers, and is processed by the same processor. The comingling of user traffic and management traffic can compromise the security of the device management. EX1001,3:19-29. EX2001,¶ 35.

The subject matter of the ‘016 Patent, therefore, sets out to provide a secure system that enables remote network maintenance using both in-band and out-of-band communication for network access. Moreover, the network described in the ‘016

Patent, and recited at least in independent claim 1, provides for secure management access control functions implemented on a separate processor, which may, as described in the specification of the '016 Patent, enable the network to ensure that management traffic is securely sent over the in-band path. EX1001,12:10-17. EX2001,¶ 36.

B. DETAILED DESCRIPTION

1. SMACC

FIG. 1 of the '016 Patent (reproduced below) illustrates a managed device, which is part of a distributed computer network (also referred to as a managed network). It should be noted that the invention of the '016 Patent is not limited to the layout shown in FIG. 1 and, for example, FIG. 14 also shows another possible layout. FIG. 1 is referred to here for purposes of explanation only. EX2001,¶ 37.

As can be seen in FIG. 1, the SMACC [red highlighting] is located within a managed device in a distributed computer network. The SMACC is communicatively coupled both to the CPU Bus and the System Bus [green highlighting] of the managed network device. As shown, the managed network device is configured for communication via various user data interfaces [blue highlighting] via the System Bus. EX1001,FIG. 1. EX2001,¶ 37.

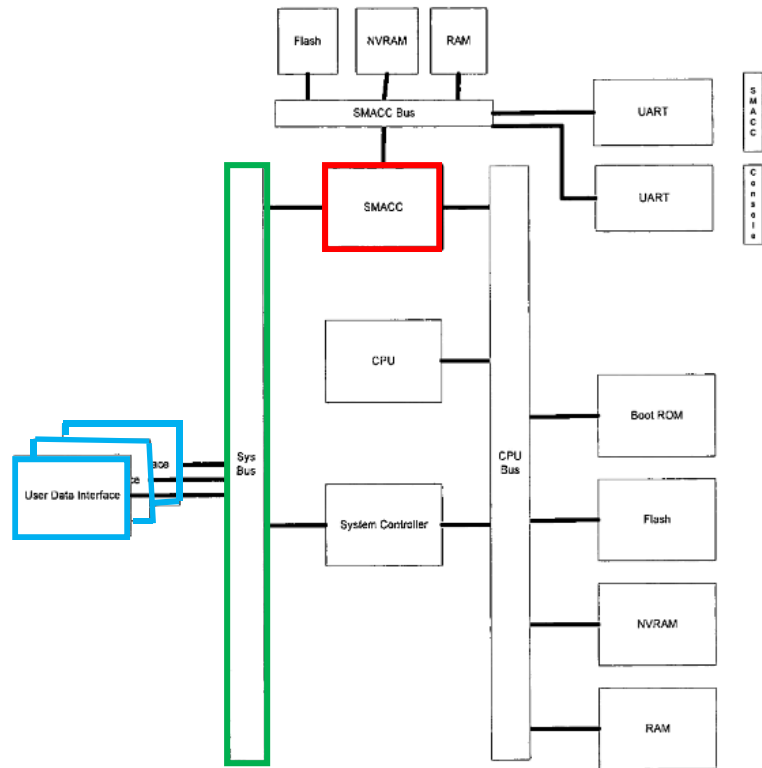


Fig. 1

EX2001, ¶ 37.

The managed device is configured with two types of interfaces for communicating management data for purposes of remote network maintenance, namely, a Virtual Management Interface (VMI) and a SMACC Network Enabled Management Interface. A network administrator may connect to the SMACC on a managed device either through the VMI or the SMACC Network Enabled Management Interface. EX1001,11:64-67; FIG. 3. FIG. 3 of the '016 Patent (reproduced below) illustrates these interfaces. EX2001, ¶ 38.

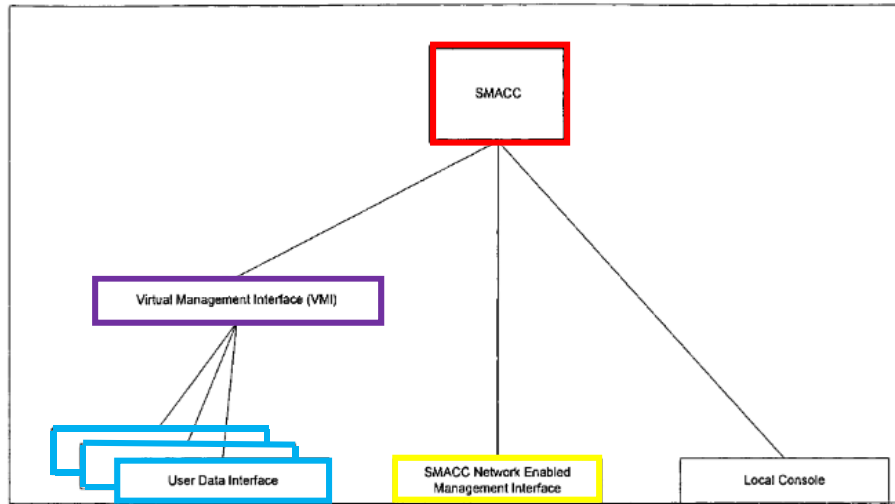


Fig. 3

EX2001, ¶ 39.

As shown in FIG. 3, the VMI [purple highlighting] is located between the SMACC [red highlighting] and the User Data Interfaces [blue highlighting]. The VMI “logically separates management traffic from user data traffic when a user interface on the managed device is going to be utilized for the network connection” (or, in other words, for in-band communication using a User Data Interface). EX1001,12:1-4. The SMACC Network Enabled Management Interface [yellow highlighting] “provides a physically separate interface for the management network connection rather than the user interfaces on the managed device” (or in other words, for out-of-band communication using a dedicated network for that purpose). EX1001, 2:5-6. EX2001, ¶ 39.

A bus controller or controller chip may be utilized for the SMACC processor to access the necessary bus as illustrated in FIGS. 28 and 29. EX1001,11:10-12. EX2001,¶ 40.

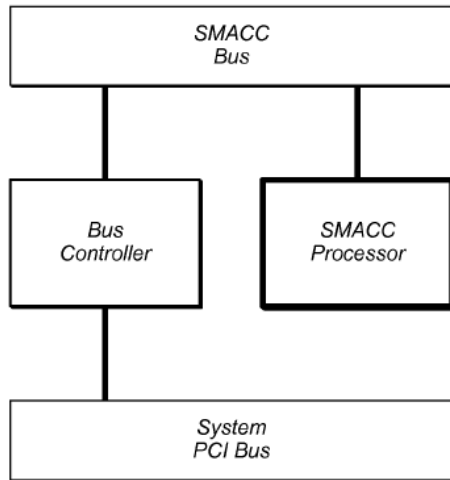


Fig. 28

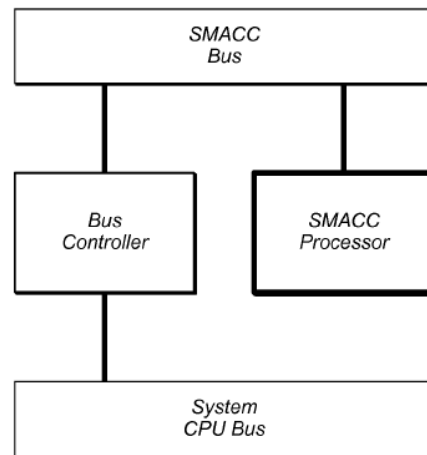


Fig. 29

2. Virtual Management Interface (VMI)

The VMI may be used for in-band communications between a device controlled by a network administrator and a managed device on which the VMI resides. The Detailed Description of the '016 Patent describes three primary functions of the VMI. EX2001,¶ 41.

a) Connecting Remote Administrator with SMACC

On the most basic level, the VMI connects remote administrators with the SMACC. “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.”

EX1001,6:7-11. EX2001,¶ 42.

b) Separating Management Data from User Data

“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.” EX1001, 6:21-24. “The [VMI] logically separates management traffic from user data when they are going to utilize the same interfaces on the managed device and the same physical network. In a preferred exemplary embodiment of the current invention, the VMI will utilize a Virtual Private Network (VPN) mechanism, such as IPSec to encrypt, protect and logically separate the management traffic before the traffic is passed to the user interface.” (emphasis added) EX1001,12:10-18. EX2001,¶ 42.

c) In-Band Communication of Management Data (Using User Data Interfaces of Managed Device)

In a distributed computer network, as described in the ‘016 Patent, the user data interfaces are used for in-band communication. As shown in FIG. 3 of the ‘016 Patent (reproduced above), the VMI is located between the SMACC and the User Data Interfaces of the managed device.

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.

EX1001,6:23-31.

The managed device is designed such that management traffic is not allowed to be sent directly to the user interfaces. All management traffic must go through one of the management interfaces (the VMI or the SMACC interface). The VMI allows any of the user interfaces to be utilized for management traffic while still protecting the management interface and traffic.

EX1001,12:17-24.

3. Encrypted Management Requests

The Virtual Management Interface (VMI) logically separates management traffic from user data when they are going to utilize the same interfaces on the managed device and the same physical network. EX1001, 12:10-13. In a preferred exemplary embodiment, the VMI will utilize a Virtual Private Network (VPN) mechanism such as IPSec to encrypt, protect and logically separate the management traffic before the traffic is passed to the user interfaces. EX1001, 12:14-17. Management traffic is not allowed to be sent directly to the user interfaces. All management traffic must go through one of the management interfaces (the VMI or the SMACC interface). The VMI allows any of the user interfaces to be utilized for management traffic while still protecting the management interface and traffic. EX1001,12:17-24. EX2001,¶ 42.

Management information may be sent over either the VMI or SMACC Interface and will be encrypted. EX1001,19:21-25. EX2001,¶ 42.

III. PRIOR ART RELIED ON IN THE PETITION

The Petition advances four grounds against independent Claim 1 of the ‘016 Patent. In Ground 1, the Petition offers only a single reference, Neufeld, in support of its assertion that Claim 1 of the ‘016 Patent is obvious under 35 U.S.C. § 103. In Ground 2, the Petition asserts that Claim 1 of the ‘016 Patent is obvious over Neufeld in combination with Frantz and PCI Bridge Spec. In Ground 9, the Petition asserts that Claim 1 of the ‘016 Patent is obvious over IPMI in combination with Frantz and Huckins. In Ground 10, the Petition asserts that Claim 1 of the ‘016 Patent is obvious over IPMI in combination with IPMIv2.0 and Huckins.

A. Neufeld

As its primary reference, the Petition relies on Neufeld. Neufeld describes a remote management system as shown in FIG. 1 (reproduced below). The remote management system includes a remote management PC 5 communicatively coupled to a managed server 2 via a network N and a management network M. The management network M may be used for out-of-band communications between the remote management PC5 and the managed server 2. The network N appears to be used for in-band communication of video activity between the managed server 2 and

the remote management PC 5, although use of the network N for in-band communication is not explicitly stated. EX1005,¶ [0034],[0035],[0037]. EX2001,¶ 45.

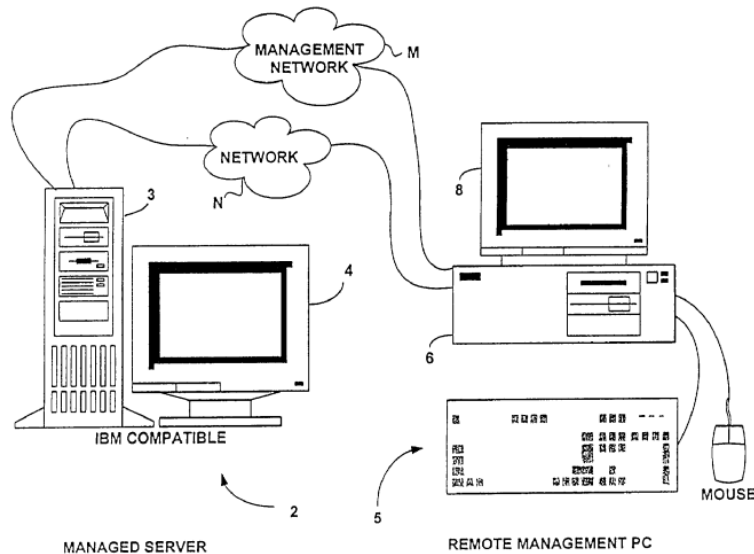


FIG. 1

The managed server 2, illustrated in FIG. 1, contains a remote management controller 116. FIG. 2 of Neufeld (reproduced below) shows the location of the remote management controller 116 within the CPU 3 of the managed server 2. FIG. 3 of Neufeld (also reproduced below) is a block diagram showing components of the remote management controller 116. The remote management controller 116, in Neufeld, resides in the managed server 2 and facilitates communication with the remote management PC 5 for purposes of both in-band and out-of-band communication. EX1005,¶ [0043], FIG.2, and FIG.3. EX2001,¶ 46.

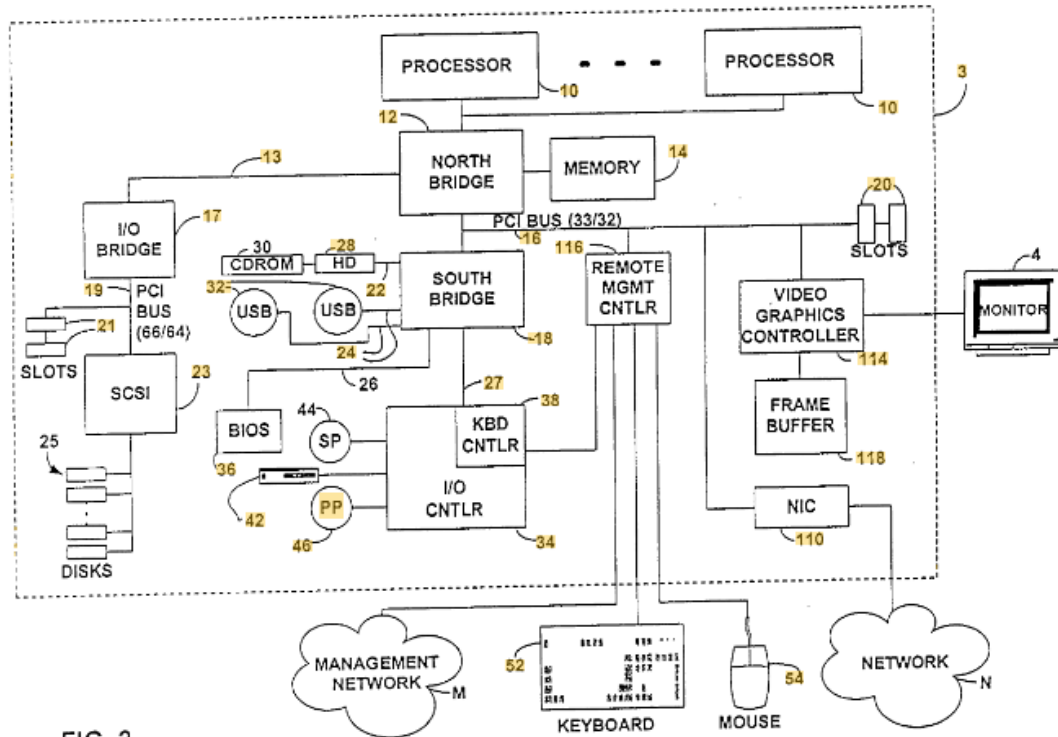


FIG. 2

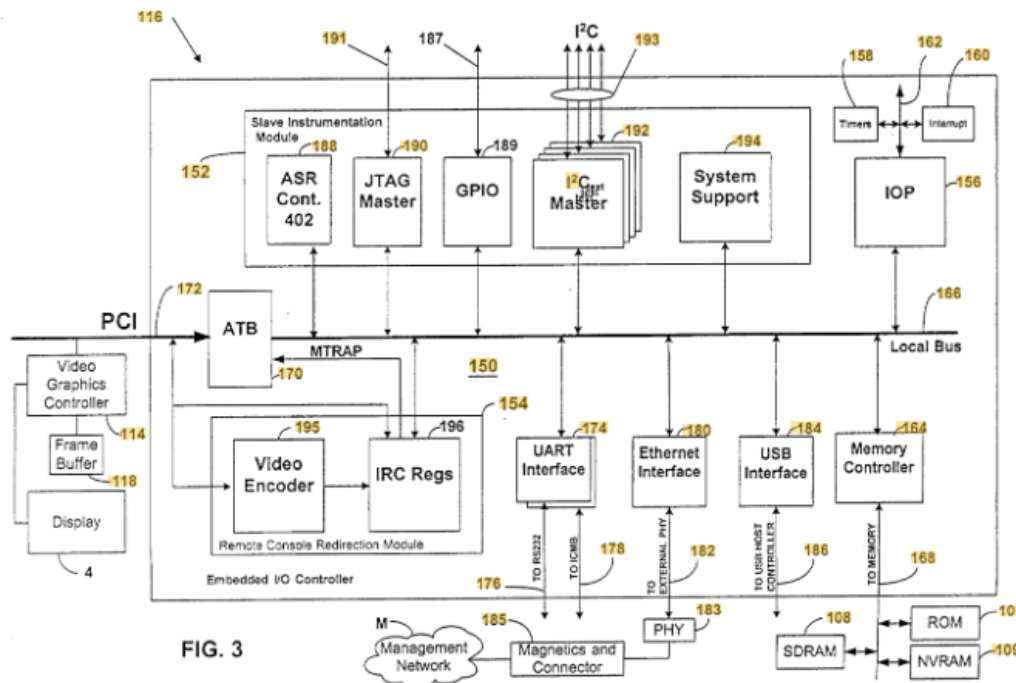


FIG. 3

In terms of in-band communication, the remote management controller 116 is “attached to the PCI bus 16.” EX1005, ¶ [0043]. “Further attached to the PCI bus 16

is a video graphics controller 114 and one or more communications devices, such as a network interface controller (“NIC”) 110.” EX1005,¶[0045]. “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”).” EX1005,¶[0034]. Such information may be transmitted over the network N to the remote management PC 5 via the network interface card (NIC) 110. Since this function of the remote management controller 116 is independent of the OS, this form of in-band communication can be performed whether the OS is operational or not, and can even be used for system setup before the OS is up and running. EX2001,¶46.

In the operation of the remote management controller 116, the I/O processor 156 (FIG. 3) may periodically read the video graphics data from the frame buffer 118 to determine whether the data has changed. If the data has changed, the I/O processor 156 will compress the video graphics data and transmit the data to the remote console 5 via one of the communications devices (i.e., modem or NIC 110). The remote console 5 will decompress and decode the data stream and display it at the remote console 5 for viewing by a user.

EX1005,¶[0048].

Another mode of in-band communication described in Neufeld is a so-called “lights out” mode. EX1005,¶[0076]. In this mode, users may be granted network privileges, and/or subject to certain authentication requirements and security settings, depending on the time of day the user attempts to access the network, the location

and IP address from which the user attempts to access the network, and/or the connection type the user attempts to use to access the network.

As shown in these examples, the more remote the connection, the more rigorous the authentication that may be required. Likewise, connections made during normal working hours may require less rigorous authentication than connections made during non-business hours. Also, similarly, the range of a particular user's privileges may be restricted depending upon the type and time of connection. In other words, a particular user or group of users may have a first feature set if accessing the managed server 2 from a relatively secure location during normal business hours, while the particular user or group of users may have other feature sets if accessing the managed server 2 from other locations and/or at other times.

EX1005, ¶[0084].

An address translation and bridging ("ATB") unit 170 is operatively coupled to the internal local bus 166 and to a PCI bus 172. EX1005, ¶[0057]. The ATB unit 170 allows the remote server management controller 116 to decode bus cycles on the PCI bus 172 and to communicate over the PCI bus 172 by initiating PCI bus cycles. . EX1005, ¶[0057]. EX2001, ¶ 47.

B. Frantz

Frantz discusses the goal of providing a remote network management tool that can establish a strongly encrypted communication path with a managed server across a publicly available communication path. EX1006,3:34-41. FIG.4 of Frantz

(reproduced below) shows a process for the establishment of a secure connection with a managed server across a publicly accessible data path such as the Internet. A remote console applet establishes a communication link that is not encrypted (“in the clear” link). EX1006,10:50-54;11:57-59. The remote console applet requests a browser to obtain a secret key from a remote web server EX1006,11:64-12:4. The web server provides the secret key to the browser via an encrypted communication link and the secret key is passed from the web server to the remote console sever EX1006,12:5-10. The browser passes the secret key to the remote control applet and the remote control applet and the remote console server used the shared secret key to begin encrypted communication EX1006,12:11-16. EX2001,¶ 48.

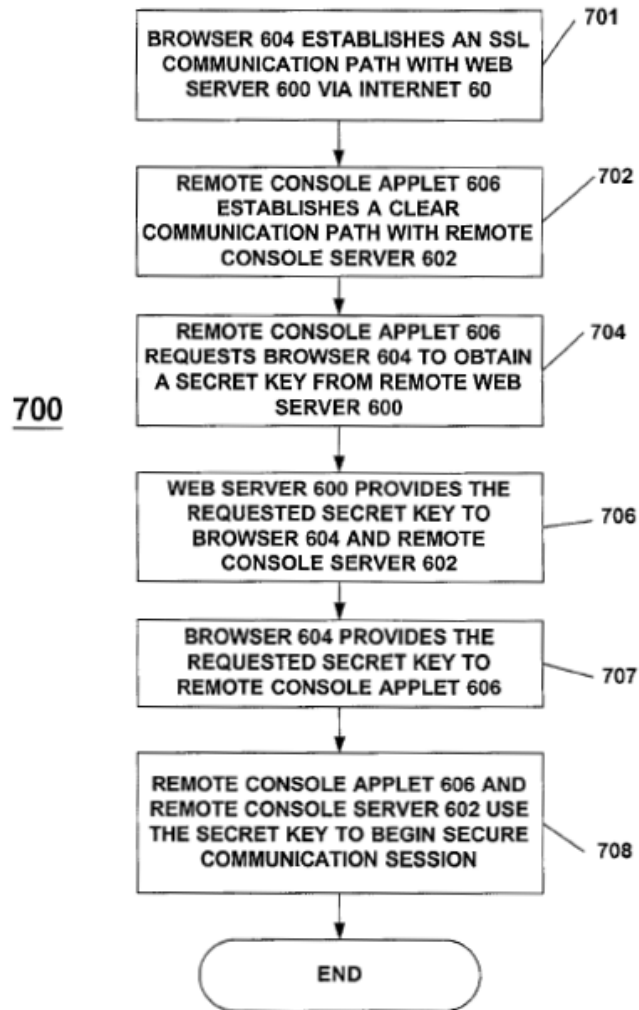


FIG. 4

C. PCI-to-PCI Bridge Architecture Specification (PCI Bridge Spec)

PCI Bridge Spec is a specification defining the behavior of a compliant PCI-to-PCI bridge. EX1008,9. A PCI-to-PCI bridge provides a connection path between two independent PCI buses. EX1008,11. The primary function of the bridge is to allow transactions to occur between a master on one PCI bus and a target on the other PCI bus. EX1008,11. A typical bridge application is shown in Figure 1-1

(reproduced below), a bridge is used to create a second PCI bus segment (labeled PCI Bus 1) to which additional PCI connectors are added. EX1008,12. EX2001¶49.

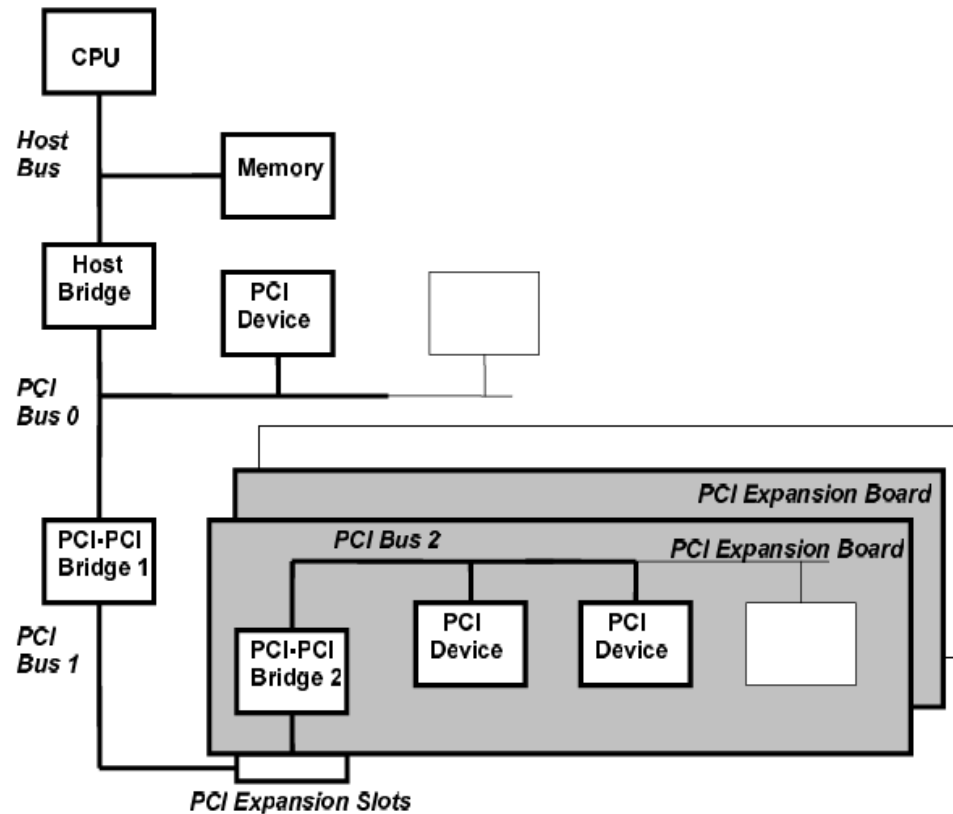


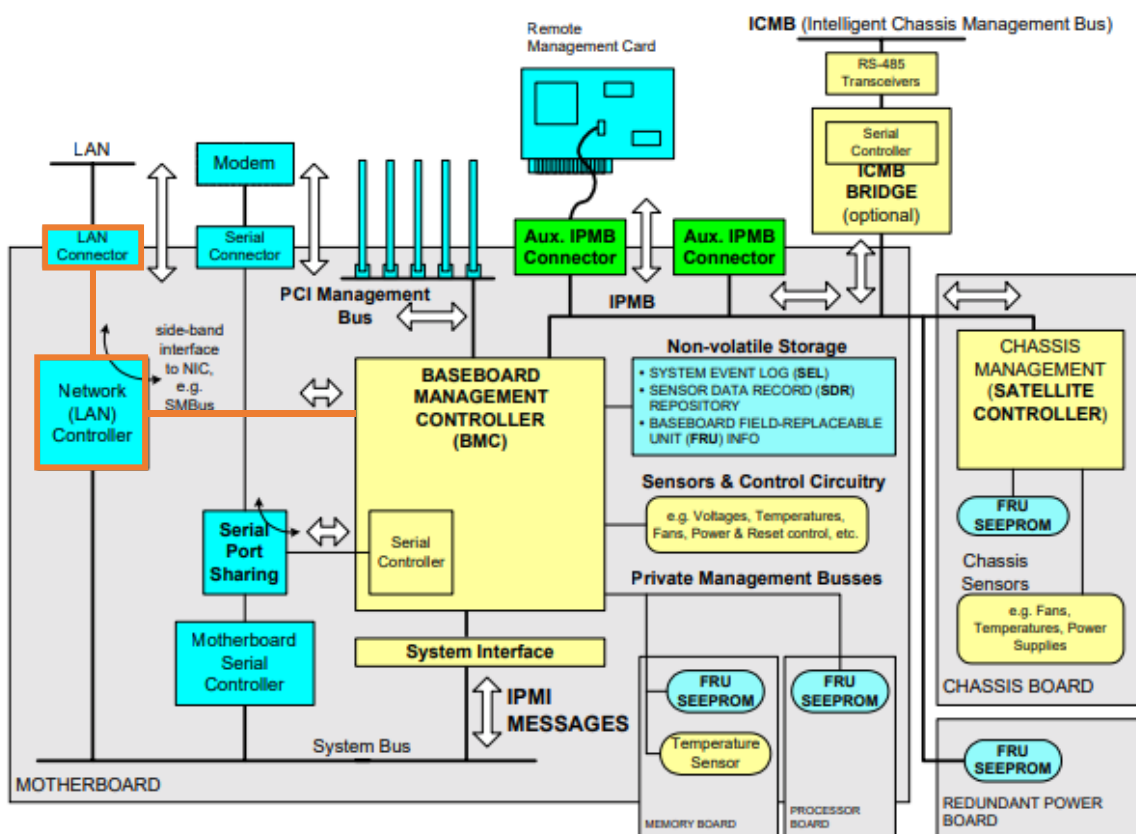
Figure 1-1: Typical Bridge Applications

D. Intelligent Platform Management Interface Specification V1.5 (IPMI)

IPMI is a standardized protocol, developed by Intel, and used to remotely manage and monitor servers, even when the main OS is down or the system is powered off. To accomplish this, IPMI primarily leverages out-of-band communication, providing several different dedicated management ports, including several auxiliary IPMB connectors for communications via remote management

cards, an Intelligent Chassis Management Bus (ICMB) bridge, and a serial connector. These management ports can be seen in FIG. 1-2 of IPMI (reproduced below). While IPMI is primarily designed for out-of-band management, there is a form of in-band communication available. EX2001,¶50.

Figure 1-2, IPMI Block Diagram



“At the heart of the IPMI architecture is a microcontroller called the *Baseboard Management Controller* or, BMC.”

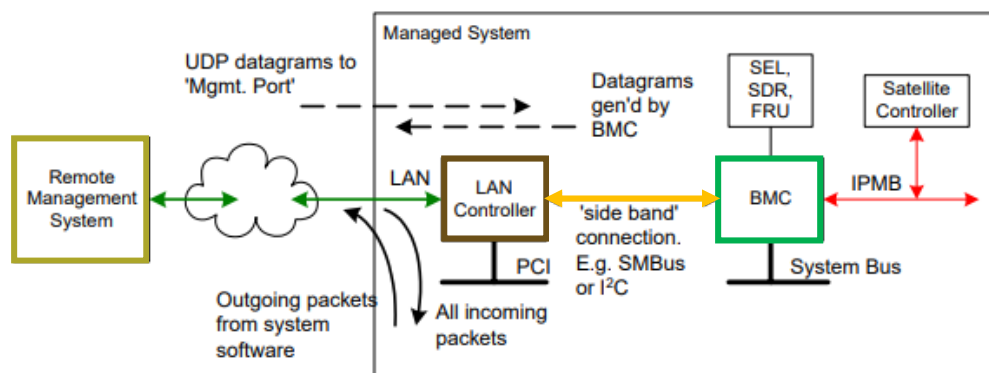
The BMC provides the intelligence behind Intelligent Platform Management. The BMC manages the interface between system management software and the platform management hardware,

provides autonomous monitoring, event logging, and recovery control, and serves as the gateway between system management software and the IPMB and the ICMB.

EX1020,9:1-6.

In terms of in-band-communication, as can be seen from FIG.1-2 of IPMI, the BMC shares a network interface with the managed system's network traffic. The communication path for such in-band-communication is highlighted in orange in FIG.1-2 above. FIG.12-1 of IPMI (reproduced below) is a block diagram of this interface (referred to in IPMI as the embedded LAN Controller Implementation).

Figure 12-1, Embedded LAN Controller Implementation

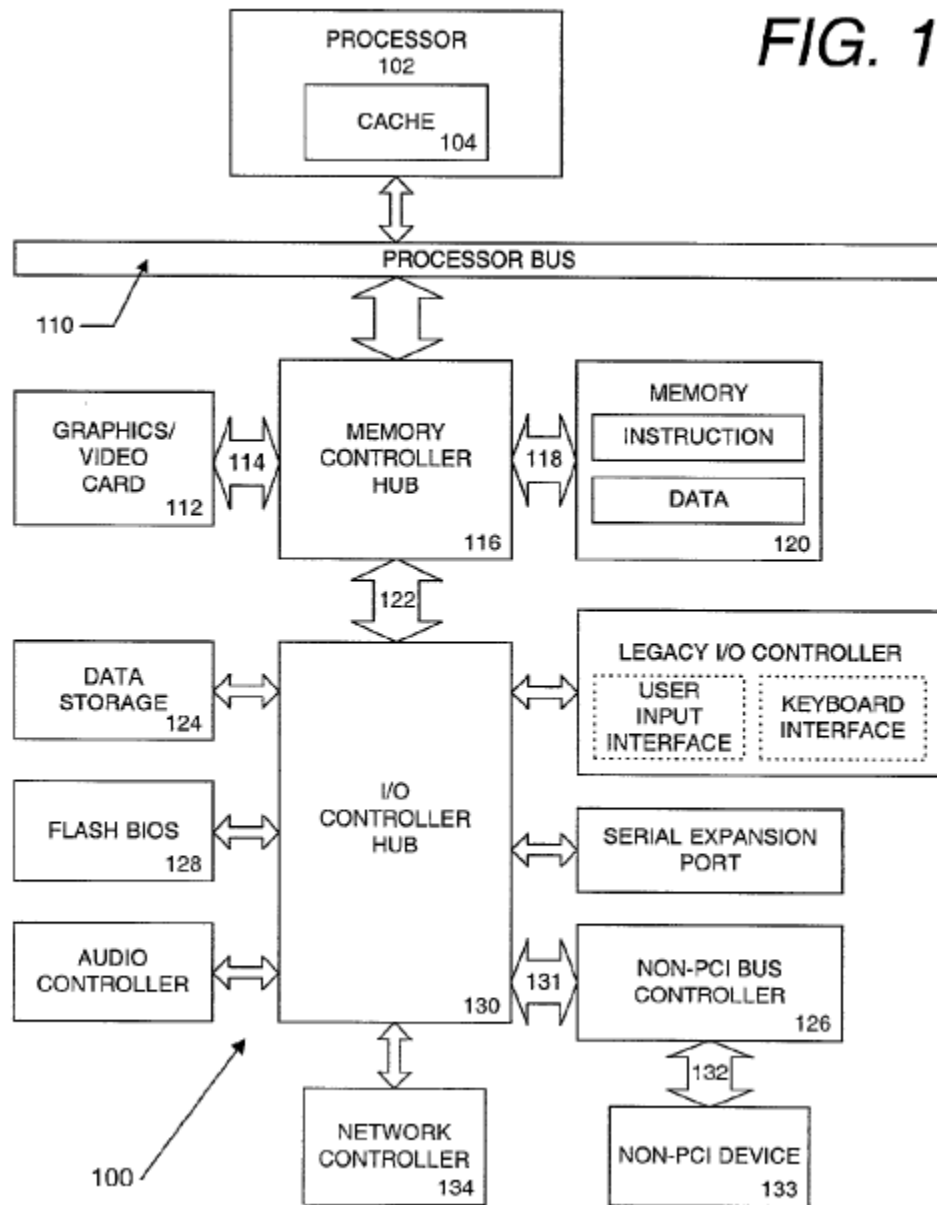


Using the embedded LAN Controller Implementation, IPMI messages may be transferred “between the BMC [green highlighting] and a remote management system (remote console) [gold highlighting] over an Ethernet LAN connection using UDP under Ipv4. The UDP datagrams are formatted to contain IPMI request and response messages....” EX1020,106:1-4. The LAN controller [brown highlighting] “has the ability to detect UDP datagrams sent to a ‘management port.’ Any

datagrams received on that port are forwarded on a ‘side-band’ interface [orange highlighting] that allows them to be delivered to, or received by, the BMC.” EX1020, 106:10-12. “The BMC can use this same interface to inject datagrams onto the LAN. These datagrams are interleaved with the network packets that are generated by system software.” EX1020,1060:4-15. EX2001,¶50.

E. Huckins

Huckins discloses that a non-PCI bus controller 126 is coupled on a PCI bus 131 to an I/O Controller hub (ICH) 130, as shown in Figure 1 (reproduced below). The non-PCI bus controller 126 is capable of receiving and transmitting signals to and from the system 100 on the PCI bus 131. The non-PCI bus controller 126 is also physically and electrically compatible to the PCI bus protocol in order to connect to the PCI bus 131. This non-PCI bus controller 126 can also be referred to as a bus bridge. Also coupled to the non-PCI bus controller 126 is a non-PCI device 133. This non-PCI device 133 is coupled on a bus 132 having a protocol different than the PCI protocol. Thus, the non-PCI device 133 can indirectly interact with the rest of the system 100 through the PCI bus 131, even though the non-PCI device is not designed to operate with the PCI protocol. The bus bridge 126 enables the computer system 100 to communicate with a non-PCI device 133 through a PCI bus 131 EX1007,¶[0026]. EX2001,¶51.



F. Intelligent Platform Management Interface Specification v2.0 (IPMI v2.0)

IPMI v2.0 is a standardized protocol, developed by Intel, that proposed additions to the IPMI specification. RMCP+ is the working name for enhanced protocol transferring IPMI messages and other types of payloads to an IPMI-based

BMC over IP. RMCP+ includes support for multiple payload types over an IPMI session, enhanced user authentication algorithms, encryption support, and better alignment with ASF 2.0. EX1023,7. EX2001,¶52.

IV. THE PETITION FAILS TO DEMONSTRATE A REASONABLE LIKELIHOOD OF SUCCESS ON THE MERITS

A. Independent Claim 1 is Not Obvious Over Neufeld Pursuant To 35 U.S.C. § 103

In Ground 1, the Petition relies on a single reference, Neufeld, in challenging independent Claim 1 as allegedly obvious under 35 U.S.C. § 103.

This allegation is deficient for a number of reasons. First, Neufeld does not disclose at least “a bus controller coupled to the processor via the first bus,” and “wherein the bus controller is also coupled to a second bus of the network device that is distinct from the first bus,” as recited in claim 1. Second, Neufeld does not disclose at least “wherein the bus controller is configured to receive the encrypted form of the management requests from the second bus,” and “and to convey the encrypted form of the management requests to the processor via the first bus,” as recited in claim 1. Third, Neufeld does not disclose at least “wherein the processor is configured to decrypt the encrypted form of the management requests,” as recited in claim 1.

Neufeld's ATB 170 is explicitly described as a bridge, facilitating communication between the PCI bus and the internal local bus, but it does not perform the distinct functions of a bus controller, which manages traffic flow and governs device access on a bus. The '016 Patent clearly differentiates between these roles, and the Petition offers no evidence to bridge this critical gap in functionality. Additionally, the speculative assertion that it would have been "customary" to modify the ATB 170 to include a bus controller lacks any supporting evidence or rationale, falling short of the requirements for demonstrating obviousness. Without a teaching, suggestion, or motivation to support such a modification, the Petitioner's claims are conclusory and insufficient to establish that Neufeld discloses or renders obvious the claimed invention for at least the following reasons.

1. Neufeld Does Not Disclose "A Bus Controller Coupled To The Processor Via The First Bus" As Required By Claim 1

The Petitioner's argument that Neufeld's ATB 170 functions as a "bus controller" misrepresents the distinction between a bridge and a bus controller, as understood by a person of ordinary skill in the art (POSITA). Neufeld describes the ATB 170 as facilitating communication between the PCI bus and an internal local bus by decoding and initiating PCI bus cycles, a functionality consistent with a bus bridge, which merely connects and enables communication between buses, rather than a bus controller, which governs traffic flow and manages device access. The '016 Patent explicitly identifies this distinction, highlighting the unique role of

a bus controller in managing access to the bus, a function the ATB 170 does not perform. Additionally, the Petitioner's assertion that it would have been obvious to modify Neufeld's ATB 170 to include a bus controller lacks evidentiary support. Under *Graham v. John Deere Co.*, a finding of obviousness requires concrete evidence of a teaching, suggestion, or motivation to modify the prior art, which the Petition fails to provide. Without substantiating evidence, the argument that incorporating a bus controller into the ATB 170 was inherent or customary in the field is conclusory and cannot support the claim that Neufeld discloses or renders obvious the claimed invention.

Neufeld discloses that an address translation and bridging ("ATB") unit 170 is coupled to an internal local bus and to a PCI bus. The ATB unit 170 "is constructed to allow the remote server management controller 116 to decode bus cycles on the PCI bus 172 and to communicate over the PCI bus 172 by initiating PCI bus cycles." EX1005, ¶[0057]. Petitioner incorrectly extrapolates that this implies that the ATB 170 performs the functions of a "bus controller." EX2001, ¶¶54-59.

The specification of the '016 Patent describes that "it may be necessary to utilize a controller chip to the SMACC processor to access the necessary bus as illustrated in FIGS. 28 and 29." EX1001,11:10-12. The controller chip (bus controller in claim 1) is used for accessing a bus and not simply a connector to

decode bus cycles on a PCI bus and to communicate over the PCI bus by initiating PCI bus cycles, as is the function of the ATB in Neufeld.

A bus controller, as understood by a POSITA, may be considered an arbiter, which manages or governs the flow of traffic on a bus, determining which device can access the bus and when it can access the bus. EX2001, ¶¶56-57; EX2005, Chapter 4, Page 342. On the other hand, a “bus bridge” is simply an extender and facilitates communication between multiple, potentially dissimilar buses and acts as a connector between two different types of buses, allowing data to be transferred between them. EX2001, ¶56. Simply decoding bus cycles on a PCI bus and communicating over the PCI bus by initiating PCI bus cycles, which is what the bridge (ATB) of Neufeld does, does not make it a bus controller or perform the functions of a bus controller (i.e. manage or govern the flow of data on a bus). EX2001, ¶58. Therefore, Neufeld fails to disclose a bus controller coupled to the processor via the first bus, as recited in claim 1.

a) Petitioner’s Expert Declaration Should Be Given Little, If Any, Weight

The courts and the PTAB alike have made clear that, when arguing that a feature naturally flows from the technology, some evidence, apart from conclusory statements, must be offered in support. *See Arendi S.A.R.L. v. Apple Inc.*, 832 F.3d 1355 (Fed. Cir. 2016). This is particularly true when conclusory statements in an

IPR petition are merely supported by the identical conclusory statements in Petitioner's expert declaration. In such circumstances, the expert's declaration should be given little, if any, weight. *See IPR2022-00624, Director Review Decision, Paper #12, February 10, 2023 (finding that "the Board was correct in giving little weight to Petitioner's expert because the expert declaration merely offered conclusory assertions without underlying factual support.")*. These cases collectively underscore that expert testimony in patent disputes must include independent, reasoned analysis and cannot merely reiterate the Petitioner's arguments or present conclusory opinions devoid of evidentiary support.

To substitute for a complete lack of disclosure, in Neufeld, of a bus controller, the Petition argues that "a POSITA would have found it obvious to include a bus controller in ATB 170. It was known in the art and customary for a bus bridge that links a primary bus to a secondary bus to include a bus controller to control the secondary bus." For this proposition, the Petition cites to the Declaration of Dr. Meldal at 96, which states the exact same thing. This is nothing other than a conclusory statement that does little, if anything, to explain why these concepts were so well-known at the time of invention, and yet Petitioner has not produced a single shred of evidence supporting it (and neither has their expert).

Table 1, below, provides a comparison of the arguments in the Petition, and the alleged supporting evidence in Dr. Meldal's declaration (any differences

between the two are highlighted in yellow). They are nearly identical, and both fail to provide anything other than conclusory statements. Accordingly, Dr. Meldal’s declaration should be given little weight.

TABLE 1

Petition	¶96 Expert Declaration
Should the Board determine that the ATB 170 does not includes a bus controller, a POSITA would have found it obvious to include a bus controller in ATB 170. It was known in the art and customary for a bus bridge that links a primary bus to a secondary bus to include a bus controller to control the secondary bus.	In the event that the Board determines that the ATB 170 does not includes a bus controller, a POSITA would have found it obvious to include a bus controller in ATB 170. It was known in the art and customary for a bus bridge that links a primary bus to a secondary bus to include a bus controller to control the secondary bus.

To be clear, all of Dr. Meldal’s testimony as to the obviousness of a bus controller are mere conclusory statements and do not even attempt to answer the lingering question as to why this functionality was obvious. In *Facebook v. Windy City Innovations, LLC*, the Court affirmed the Board’s holding that independent claim 1 was not unpatentable as obvious over the asserted prior art when “the Board considered Facebook’s expert’s testimony but determined that it did not add materially to Petitioner’s unpersuasive attorney argument” because it merely repeated Petitioner’s argument, nearly verbatim, without citation to the basis for his testimony.” 973 F.3d 1321, 1340-41 (Fed. Cir. 2020). In fact, the Federal Circuit expressly held that “conclusory expert testimony and attorney argument cannot

constitute substantial evidence.” *Acoustic Tech., Inc. v. Itron Networked Sols., Inc.*, 949 F.3d 1366, 1375 (Fed. Cir. 2020). Accordingly, Dr. Meldal’s testimony should be given little, if any, weight. And since Dr. Meldal’s testimony is the only evidence submitted for the alleged obviousness of a bus controller, this Petition should not be instituted.

2. Neufeld Fails to Disclose “Wherein The Bus Controller Is Also Coupled To A Second Bus Of The Network Device That Is Distinct From The First Bus” As Required By Claim 1

The Petition offers no evidence other than an assertion that Neufeld discloses or renders this limitation obvious since, in addition to being coupled to the local bus 166, ATB 170 is coupled to a second distinct bus, the PCI bus 172. However, Neufeld does not disclose a bus controller, as discussed above. As discussed above, the ATB of Neufeld is not a bus controller, and a POSITA would not understand that the ATB in Neufeld, to be a bus controller. EX2001, ¶¶ 4-59. Since Neufeld fails to disclose a bus controller, Neufeld fails to disclose that the bus controller is also coupled to a second bus of the network device that is distinct from the first bus.

As explained by the Federal Circuit, “[t]o satisfy its burden of proving obviousness, a petitioner cannot employ mere conclusory statements.” *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016). Instead, the Petitioner has the burden to submit facts to the record that show “[w]hether the prior

art discloses a claim limitation, whether a skilled artisan would have been motivated to modify or combine teachings in the prior art, and whether she would have had a reasonable expectation of success in doing so.” *Univ. of Strathclyde v. Clear-Vu Lighting LLC*, 17 F.4th 155, 160 (Fed. Cir. 2021). If the petition does not clearly demonstrate how the cited prior art meets each claim element, the Petitioner will fail to meet its burden.

Here, since Petitioner has adduced no evidence of other than conclusory statements in the Petition, Petitioner has failed to meet their burden of showing that Neufeld teaches a bus controller and that the bus controller is coupled to a second bus of the network device that is distinct from the first bus.

3. Neufeld Fails to Disclose “The Bus Controller Is Configured To Receive The Encrypted Form Of The Management Requests From The Second Bus” As Required By Claim 1

The Petitioner’s reliance on Neufeld to demonstrate the encryption of management requests and the configuration of a bus controller to handle such encrypted requests is misplaced. While Neufeld describes a management system involving a remote management controller and discusses general security features, it does not disclose or teach the encryption of management request messages. Neufeld’s references to encryption are limited to authentication processes, such as verifying user credentials and establishing secure access to resources, rather than

encrypting the content of management requests themselves. Furthermore, Neufeld does not disclose a bus controller, let alone one configured to receive encrypted management requests via a second bus. The absence of these critical elements in Neufeld renders the Petitioner's arguments insufficient to support the alleged obviousness of the claimed invention.

Neufeld discloses a management message sent over a management network M from a remote management PC 5 to a managed server 2. A 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. EX1005 ¶[0043]. However, Neufeld does not disclose, mention, or teach that a management request is encrypted. Neufeld notes that security may be an important regardless of whether the remote computer is communicating with the server to manage it or to carry out some other function. EX1005,20[0018]. Neufeld also notes that any type of remote access would typically utilize encryption techniques, while direct access may not. EX1005,¶[0085]. However, this does not teach encryption of a management request message. At most, Neufeld teaches security and encryption for accessing or authenticating a system remotely. EX2001,¶ 1.

For example, Neufeld discusses that the managed server 2 includes a security manager that includes a security sign-on system that may be stored and operated on

the remote management controller and includes authentication of services to provide each user with entry into an appropriate function or resource, and a service that may include an encryption and certification component which verifies the user to the directory service. Further, Neufeld discusses that the managed sever 2 generates a unique signature key and encryption key pairs...to establish authenticity. EX1005,¶[0076]. So, the security and encryption that Neufeld mentions is for authentication and not for encryption of a management request. EX2001,¶61.

In addition to not disclosing an encrypted form of a management request, since Neufeld does not disclose a bus controller, as discussed above, Neufeld certainly does not disclose a bus controller configured to receive the encrypted form of the management requests from the second bus.

4. Neufeld Fails to Disclose “To Convey The Encrypted Form Of The Management Requests To The Processor Via The First Bus” As Required By Claim 1

The Petitioner’s reliance on Neufeld to demonstrate the encryption of management requests and the configuration of a bus controller to handle such encrypted requests is misplaced. While Neufeld describes a management system involving a remote management controller and discusses general security features, it does not disclose or teach the encryption of management request messages. Neufeld’s references to encryption are limited to authentication processes, such as verifying user credentials and establishing secure access to resources, rather than

encrypting the content of management requests themselves. Furthermore, Neufeld does not disclose a bus controller, let alone one configured to convey the encrypted form of the management requests to the processor via the first bus.

The absence of these critical elements of a bus controller and an encrypted form of management requests in Neufeld renders the Petitioner's arguments insufficient to support the alleged obviousness of the claimed invention. EX2001, ¶59.

Petitioner states that a "POSITA, therefore would have understood and found it obvious that IOP 156 would be configured to receive the encrypted form of the management requests and to decrypt and act on them, because IOP 156 is a processor and therefore can be programmed to perform these functions, and because the other devices in the remote management controller 110 are directed toward specific functions that do not include decrypting or acting on remote management requests."

For this proposition, the Petition cites to the Declaration of Dr. Meldal at 101, which states the same thing. This is nothing other than a conclusory statement that does little, if anything, to explain why a POSITA would have understood and found it obvious at the time of invention, and yet Petitioner has not produced a single shred of evidence supporting it (and neither has their expert).

Table 2, below, provides a comparison of the arguments in the Petition, and the alleged supporting evidence in Dr. Meldal's declaration (any differences

between the two are highlighted in yellow). They are nearly identical, and both fail to provide anything other than conclusory statements. Accordingly, Dr. Meldal's declaration should be given little weight.

TABLE 2

Petition	¶101 Expert Declaration
Neufeld further discloses that IOP 156 provides general control and functions as the management processor for the remote management controller 156, and that the IOP 156 dictates the control and monitoring functions performed via the slave instrumentation module 152. EX 1005, ¶¶[0054], [0066]; <i>see also</i> [1.a] above. A POSITA therefore would have understood and found it obvious that IOP 156 would be configured to receive the encrypted form of the management requests and to decrypt and act on them, because IOP 156 is a processor and therefore can be programmed to perform these functions, and because the other devices in the remote management controller 110 are directed toward specific functions that do not include decrypting or acting on remote management requests.	Neufeld further discloses that IOP 156 provides general control and functions as the management processor for the remote management controller 156, and that the IOP 156 dictates the control and monitoring functions performed via the slave instrumentation module 152. EX 1005, ¶¶[0054], [0066]. A POSITA therefore would have understood and found it obvious that IOP 156 would be configured to receive the encrypted form of the management requests and to decrypt and act on them, because IOP 156 is a processor and therefore can be programmed to perform these functions, and because the other devices in the remote management controller 110 are directed toward specific functions that do not include decrypting or acting on remote management requests.

The testimony provided by Dr. Meldal regarding the alleged obviousness of a bus controller configured to...convey the encrypted form of management requests is purely conclusory and fails to address the critical question of why this functionality would have been obvious. In *Facebook, Inc. v. Windy City Innovations*,

LLC, the Federal Circuit affirmed the Board's determination that independent claim 1 was not unpatentable as obvious over the asserted prior art, emphasizing that the Board had properly discounted the Petitioner's expert testimony because it merely echoed attorney argument without providing substantive analysis or evidentiary support. 973 F.3d 1321, 1340–41 (Fed. Cir. 2020). Similarly, the Federal Circuit in *Acoustic Technology, Inc. v. Itron Networked Solutions, Inc.* reaffirmed that "conclusory expert testimony and attorney argument cannot constitute substantial evidence." 949 F.3d 1366, 1375 (Fed. Cir. 2020).

Dr. Meldal's testimony is no different—it offers no independent analysis, factual foundation, or evidentiary support and should therefore be afforded minimal, if any, weight. Notably, Dr. Meldal's testimony is the only evidence proffered to support the alleged inherency of a data bus controller configured to...convey the encrypted form of the management requests. Without substantive evidence to support this assertion, the Petition fails to meet the threshold for institution and should be denied.

The Petition further asserts that to the extent that Neufeld does not disclose the limitation of 'convey the encrypted form of the managements requests to the processor via the first bus', it would have been obvious to a POSITA to provide for in-band communication of management requests from the remote management PC 5 to the IOP 156 of the remote management controller 116 for the reasons above in

light of Neufeld's disclosure of the desirability of providing for in-band communication to control the managed server at EX105¶[0015] and the need to decrypt management requests in order to act on them.

For this proposition, the Petition cites to the Declaration of Dr. Meldal at 102, which states the same thing. This is nothing other than a conclusory statement that does little, if anything, to explain why a POSITA would have understood and found it obvious at the time of invention, and yet Petitioner has not produced a single shred of evidence supporting it (and neither has their expert).

Table 3, below, provides a comparison of the arguments in the Petition, and the alleged supporting evidence in Dr. Meldal's declaration (any differences between the two are highlighted in yellow). They are nearly identical, and both fail to provide anything other than conclusory statements. Accordingly, Dr. Meldal's declaration should be given little weight.

TABLE 3

Petition	¶102 Expert Declaration
To the extent that Neufeld does not disclose this limitation, it would have been obvious to a POSITA to provide for in-band communication of management requests from the remote management PC 5 to the IOP 156 of the remote management controller 116 for the reasons above and in light of Neufeld's disclosure of the desirability of providing for in-band communication	To the extent that Neufeld does not disclose this limitation, it would have been obvious to a POSITA to provide for in-band communication of management requests from the remote management PC 5 to the IOP 156 of the remote management controller 116 in light of Neufeld's disclosure of the desirability of providing for in-band communication to control the managed

to control the managed server at ¶[0015] and the need to decrypt management requests in order to act on them.	server at ¶[0015] and the need to decrypt management requests in order to act on them.
---	--

The testimony provided by Dr. Meldal regarding the alleged obviousness of a bus controller configured to...convey the encrypted form of management requests is purely conclusory and fails to address the critical question of why this functionality would have been obvious. In *Facebook, Inc. v. Windy City Innovations, LLC*, the Federal Circuit affirmed the Board's determination that independent claim 1 was not unpatentable as obvious over the asserted prior art, emphasizing that the Board had properly discounted the Petitioner's expert testimony because it merely echoed attorney argument without providing substantive analysis or evidentiary support. 973 F.3d 1321, 1340–41 (Fed. Cir. 2020). Similarly, the *Federal Circuit in Acoustic Technology, Inc. v. Itron Networked Solutions, Inc.* reaffirmed that "conclusory expert testimony and attorney argument cannot constitute substantial evidence." 949 F.3d 1366, 1375 (Fed. Cir. 2020).

Dr. Meldal's testimony is no different—it offers no independent analysis, factual foundation, or evidentiary support and should therefore be afforded minimal, if any, weight. Notably, Dr. Meldal's testimony is the only evidence proffered to support the alleged inherency of a data bus controller configured to...covey the encrypted for of the management requests. Without substantive evidence to support

this assertion, the Petition fails to meet the threshold for institution and should be denied.

Accordingly, Petitioner's arguments fail as to the obviousness of Neufeld.

5. Neufeld Fails to Disclose “Wherein The Processor Is Configured To Decrypt The Encrypted Form Of The Management Requests” As Required By Claim 1

The Petitioner's assertion that a POSITA would have found it obvious for Neufeld's IOP 156 to decrypt and act on encrypted management requests is based on conclusory statements that lack substantive analysis or evidentiary support. The Petition and the supporting declaration by Dr. Meldal merely restate the same argument—that IOP 156, as a processor, could be programmed to perform these functions—without providing any rationale as to why a POSITA would have been motivated to configure the IOP in this manner at the time of invention. This reliance on unsubstantiated conclusions, as highlighted in Table 2 and 3 above, mirrors the issues identified by the Federal Circuit in cases *like Facebook, Inc. v. Windy City Innovations, LLC* and *Acoustic Technology, Inc. v. Itron Networked Solutions, Inc.*, where conclusory expert testimony was deemed insufficient to constitute substantial evidence. As Dr. Meldal's testimony lacks independent analysis or a factual foundation, it fails to substantiate the Petitioner's claims, rendering the argument deficient and unpersuasive.

As discussed above, Neufeld does not disclose an encrypted form of management requests and, therefore, does not need to have a processor to decrypt an encrypted form of the management requests. There is no such disclosure of a processor configured to decrypt a message. Just because the IOP 156 is a processor does not inherently require that it has the capability (power, speed, architecture) to decrypt encrypted management requests. Encryption / Decryption have historically been a power hungry, high-bandwidth functions that were not supported by many general purpose processors or processors that did not envision the requirement. EX2001, ¶¶66.

In *Par Pharm., Inc. v. TWi Pharm., Inc.*, the Court explains “the use of inherency, a doctrine originally rooted in anticipation, must be carefully circumscribed in the context of obviousness,” and “[t]he mere fact that a certain thing may result from a given set of circumstances is not sufficient to establish inherency.” *Par Pharm., Inc. v. TWi Pharm., Inc.*, 773 F.3d 1186, 1194-95 (Fed. Cir. 2014) (internal markings and citations omitted). The Court has “emphasized that the limitation at issue necessarily must be present in order to be inherently disclosed by the reference.” (*Southwire Co. v. Cerro Wire LLC*, 870 F.3d 1306, 1310-11 (Fed. Cir. 2017)) (internal citation omitted). Accordingly, “[a] party must...meet a high standard in order to rely on inherency to establish the existence of a claim limitation

in the prior art in an obviousness analysis.” *Millennium Pharms., Inc. v. Sandoz, Inc.*, 862 F.3d 1356, 1367 (Fed. Cir. 2017).

Here, Petitioner has failed to meet this high standard and has instead only proffered a conclusory opinion from Dr. Meldal that suggests the possibility of the feature occurring under some circumstances.

6. Neufeld Fails to Disclose “The Bus Controller Is Configured To Receive The Encrypted Form Of The Management Requests From The Second Bus”, “And To Convey The Encrypted Form Of The Management Requests To The Processor Via The First Bus”, “Wherein The Processor Is Configured To Decrypt The Encrypted Form Of The Management Requests”, as required by claim 1 As Required By Claim 1

The Petitioner alleges that Neufeld teaches or at least suggests encryption of management requests because “Neufeld notes that security may be an important issue when remotely communicating management requests to the managed server” and “discloses [] that ‘any type of remote access would typically utilize encryption techniques.’” Pet. at 20. To the extent this allegation is true, Neufeld does not teach or suggest, however, that a “bus controller is configured to ... convey the encrypted form of the management requests to the processor.” In fact, Neufeld teaches the opposite. EX2001, ¶62.

In particular, Neufeld states: “[t]he managed server 2 advantageously includes a security manager that includes a security sign-on system that may be stored and operated on the remote management controller 116 to provide for “lights out”

management.” EX1005,[0075]-[0076], FIG.2. Neufeld’s FIG. 2 shows that any commands received from the management network “M” are received directly by the “remote management controller 116.” Id., FIG.2. Any commands received from the network “N” are received via the NIC 110, and are received by the “remote management controller 116” via the “PCI BUS 16.” Id. In order to provide “lights out” management, the “security sign-on system,” which is “stored and operated on the remote management controller 116,” would decrypt the encrypted messages. As such, the received encrypted commands need not be sent to IOP 156, i.e., the alleged “processor,” see Pet. at 16, because Neufeld’s “remote management controller 116” itself appears to be configured for decrypting any encrypted messages. Nowhere does Neufeld describe that the IOP 156 is capable of or is configured for performing any encryption / decryption related operations. Ex 2001,¶63. Thus, any encrypted commands that the PCI BUS 16 may receive via the NIC 110 would be sent directly to the “remote management controller 116.” As these commands need not be and are not sent to the IOP 156, they would not be forwarded to the ATB 170 (the alleged “bus controller”), and then to the “Local Bus 166” (the alleged “first bus”). Thus, Neufeld does not teach or suggest “a bus controller coupled to the processor via the first bus ... wherein the bus controller is configured to receive the encrypted form of the management requests from the second bus, and to convey the encrypted form of the management requests to the processor via the first bus,” as claim 1 recites.

Accordingly, Petitioner's arguments fail as to the obviousness of Neufeld.

Independent claim 12 recites similar, although not identical, elements as independent claim 1 and independent claim 12 is not obvious over Neufeld for at least the same reasons provided above. EX2001, ¶67.

B. Independent Claim 1 is Not Obvious Over Neufeld, Frantz, and PCI Bridge Spec Pursuant To 35 U.S.C. § 103

In Ground 2, the Petition relies on a combination of Neufeld, Frantz, and PCI Bridge Spec, in challenging independent Claim 1 as allegedly obvious under 35 U.S.C. § 103. This allegation is deficient since neither Neufeld, nor Frantz, nor PCI Bridge Spec discloses, either individually or in combination, a bus controller with respect to the claim features “a bus controller coupled to the processor via the first bus,” and “wherein the bus controller is also coupled to a second bus of the network device that is distinct from the first bus.”

1. The Combination Of Neufeld, Frantz, and PCI Bridge Spec Does Not Disclose “A Bus Controller Coupled To The Processor Via The First Bus” As Required By Claim 1

The Petitioner's assertion that the combination of Neufeld, Frantz, and PCI Bridge Spec renders the inclusion of a bus controller in Neufeld's ATB 170 obvious is fundamentally flawed. The Petition argues that a POSITA would have looked to PCI Bridge Spec for guidance in implementing Neufeld's ATB 170 as a bridge

between the system PCI bus 172 and a PCI-based local bus 166. However, this argument misinterprets the disclosures of PCI Bridge Spec and overlooks the critical distinctions between a bridge and a bus controller as required by the claims. Furthermore, the Petition fails to establish any motivation for a POSITA to combine these references and improperly attempts to piece together an obviousness theory by selectively using discrete elements of the prior art without considering the references as a whole. These deficiencies render the Petitioner's argument untenable for multiple reasons.

For example, in Ground 2, the Petition alleges that to the extent not disclosed or rendered obvious by Neufeld alone or in combination with Frantz, the combination of Neufeld, Frantz and PCI Bridge Spec would have rendered obvious to a POSITA including a bus controller in Neufeld's ATB 170. The Petition contends that a "POSITA would have recognized that the local bus 166 could have been implemented as a PCI bus because Neufeld states that the type of local bus 166 is a design choice that is not critical..." and that a POSITA would have looked to a reference such as PCI Bridge Spec for guidance as implementing Neufeld's ATB 170 as a bridge between the system PCI bus 172 and a PCI implementation of local bus 166. Petition, page 39. Petitioner's contention is wrong for at least the following reasons.

First, PCI Bridge Spec does not disclose a bus controller. PCI Bridge Spec is a specification defining the behavior of a compliant PCI-to-PCI bridge. A PCI-to-PCI bridge provides a connection path between two independent PCI buses. EX1008, 11. The primary function of the bridge is to allow transactions to occur between a master on one PCI bus and a target on the other PCI bus. EX1008, 11. A typical bridge application is shown in Figure 1-1 (reproduced below), a bridge is used to create a second PCI bus segment (labeled PCI Bus 1) to which additional PCI connectors are added.

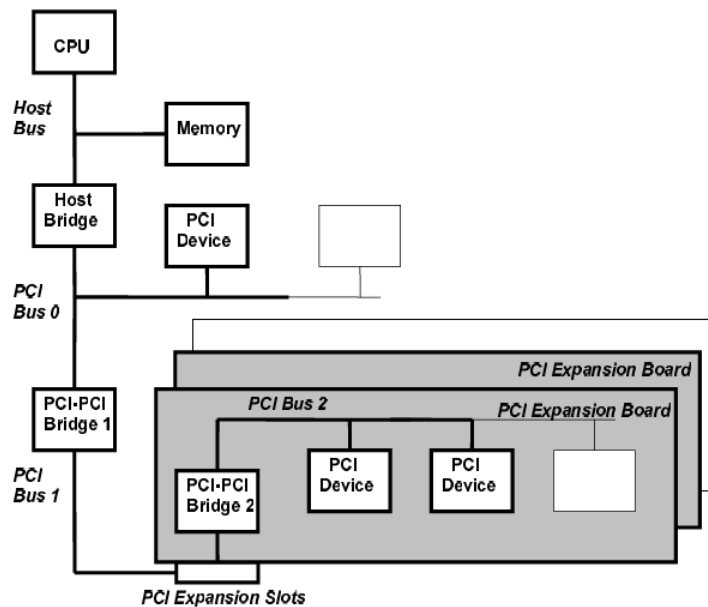


Figure 1-1: Typical Bridge Applications

At most, the PCI Bridge Spec shows implementation of a bridge or connection path, but does not disclose a bus controller as recited in claim 1. The specification of the '016 Patent describes that “it may be necessary to utilize a controller chip to the SMACC processor to access the necessary bus as illustrated in FIGS. 28 and 29.”

EX1001,11:10-12. The controller chip (bus controller in claim 1) is used for accessing a bus and not simply a connection path between two independent PC with a primary function to allow transactions to occur between a master on one PCI bus and a target on the other PCI bus buses. EX1001,11:10-12. A bus controller, as understood by a POSITA, manages or governs the flow of traffic on a bus, determining which device can access the bus and when it can access the bus. EX2001,¶¶56.

Second, there is no motivation to combine the Neufeld reference and the PCI Bridge Spec. The Neufeld reference states that the implementation details of the internal local bus 166 are a matter of design choice and are not believed to be a crucial aspect of the invention. EX1005,¶[0056]. Hence, there is no need for a POSITA to look elsewhere for guidance on implementing Neufeld's ATB 170 as a bridge to the local bus 166 and therefore no motivation to combine Neufeld and PCI Bridge Spec. EX2001,¶¶68-73.

Even if one were to combine Neufeld with PCI Bridge Spec, the combination would not disclose or teach a bus controller as recited in claim 1, since (1) the ATB of Neufeld is not a bus controller as discussed above and in relation to ground 1 and (2) PCI Bridge Spec does not disclose a bus controller as discussed above.

Further, the Federal Circuit "explains that § 103 does not permit [a Petitioner] to stitch together an obviousness finding from discrete portions of prior art

references without considering the references as a whole.” *In re Enhanced Sec. Research, LLC*, 739 F.3d 1347, 1355 (Fed. Cir. 2014). Accordingly, “[i]t is impermissible within the framework of section 103 to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art.” *In re Wesslau*, 353 F.2d 238 (CCPA 1965).

Here Petitioner has attempted to impermissibly stitch together Neufeld and PCI Bridge Spec because neither reference discloses a bus controller as recited in the claims and has not established a motivation to combine Neufeld and PCI Bridge Spec. Therefore, at least based on the above, the combination of Neufeld with PCI Bridge Spec does not disclose a bus controller.

2. The Combination Of Neufeld, Frantz, and PCI Bridge Spec Fails to Disclose “Wherein The Bus Controller Is Also Coupled To A Second Bus Of The Network Device That Is Distinct From The First Bus” As Required By Claim 1

Since the combination of Neufeld, Frantz, and PCI Bridge Spec fails to disclose a bus controller as discussed above, the combination of Neufeld, Frantz, and PCI Bridge Spec fails to disclose the bus controller is also coupled to a second bus of the network device that is distinct from the first bus. EX2001, ¶79.

Accordingly, Petitioner’s arguments fail as to the obviousness of the combination of Neufeld, Frantz, and PCI Bridge Spec.

Independent claim 12 recites similar, although not identical, elements as independent claim 1 and independent claim 12 is not obvious over Neufeld, Frantz, and PCI Bridge Spec for at least the same reasons provided above. EX2001,¶84.

3. The Combination Of Neufeld, Frantz and PCI Bridge Spec Fails to Disclose “The Bus Controller Is Configured To Receive The Encrypted Form Of The Management Requests From The Second Bus”, “And To Convey The Encrypted Form Of The Management Requests To The Processor Via The First Bus”, “Wherein The Processor Is Configured To Decrypt The Encrypted Form Of The Management Requests”, as required by claim 1 As Required By Claim 1

The Petitioner alleges that Neufeld teaches or at least suggests encryption of management requests because “Neufeld notes that security may be an important issue when remotely communicating management requests to the managed server” and “discloses [] that ‘any type of remote access would typically utilize encryption techniques.’” Pet. at 20. To the extent this allegation is true, Neufeld does not teach or suggest, however, that a “bus controller is configured to ... convey the encrypted form of the management requests to the processor.” In fact, Neufeld teaches the opposite. Ex 2001,¶81.

In particular, Neufeld states: “[t]he managed server 2 advantageously includes a security manager that includes a security sign-on system that may be stored and operated on the remote management controller 116 to provide for “lights out” management.” EX1005,[0075]-[0076], FIG.2. Neufeld’s FIG. 2 shows that any

commands received from the management network “M” are received directly by the “remote management controller 116.” Id., FIG.2. Any commands received from the network “N” are received via the NIC 110, and are received by the “remote management controller 116” via the “PCI BUS 16.” Id. In order to provide “lights out” management, the “security sign-on system,” which is “stored and operated on the remote management controller 116,” would decrypt the encrypted messages. As such, the received encrypted commands need not be sent to IOP 156, i.e., the alleged “processor,” see Pet. at 16, because Neufeld’s “remote management controller 116” itself appears to be configured for decrypting any encrypted messages. Nowhere does Neufeld describe that the IOP 156 is capable of or is configured for performing any encryption / decryption related operations. Ex 2001, ¶82.

Thus, any encrypted commands that the PCI BUS 16 may receive via the NIC 110 would be sent directly to the “remote management controller 116.” As these commands need not be and are not sent to the IOP 156, they would not be forwarded to the ATB 170 (the alleged “bus controller”), and then to the “Local Bus 166” (the alleged “first bus”). To the extent Frantz (EX1006) discloses encryption of management messages and/or PCI Bridge Spec (EX1008) discloses a bus controller, this combination does not cure the above-identified defect of Neufeld, that its IOP 156 is not configured for encryption / decryption and that the remote management controller 116 is. Therefore, any encrypted messages received at Neufeld’s NIC 110

would not be forwarded to the IPO 156 (the alleged “processor”) for decryption thereof. Thus, Neufeld, Frantz, and PCI Bridge Spec, individually or in combination, do not teach or suggest “a bus controller coupled to the processor via the first bus ... wherein the bus controller is configured to receive the encrypted form of the management requests from the second bus, and to convey the encrypted form of the management requests to the processor via the first bus,” as claim 1 recites.

Accordingly, Petitioner’s arguments fail as to the obviousness of the combination of Neufeld, Frantz, and PCI Bridge Spec.

Independent claim 12 recites similar, although not identical, elements as independent claim 1 and independent claim 12 is not obvious over Neufeld, Frantz, and PCI Bridge Spec for at least the same reasons provided above.

C. Independent Claim 1 is Not Obvious Over IPMI, Frantz, and Huckins Pursuant To 35 U.S.C. § 103

In Ground 9, the Petition relies on a combination of IPMI, Frantz, and Huckins, in challenging independent Claim 1 as allegedly obvious under 35 U.S.C. § 103.

This allegation is deficient for a number of reasons. First, the combination of IPMI, Frantz, and Huckins does not disclose the claim feature “the network device is configured to receive data requests and an encrypted form of management requests via the network interface.” Second, the combination of IPMI, Frantz, and Huckins does not disclose the claim features “a bus controller coupled to the processor via

the first bus,” and “wherein the bus controller is also coupled to a second bus of the network device that is distinct from the first bus.” Third, the combination of IPMI, Frantz, and Huckins does not disclose the claim features “wherein the bus controller is configured to receive the encrypted form of the management requests from the second bus,” and “and to convey the encrypted form of the management requests to the processor via the first bus.”

1. The Combination Of IPMI, Frantz, and Huckins Does Not Disclose “The Network Device Is Configured To Receive Data Requests And An Encrypted Form Of Management Requests Via The Network Interface” As Required By Claim 1

The Petitioner’s assertion that it would have been obvious to modify IPMI to encrypt in-band management messages relies on hindsight and fails to consider the explicit disclosures in IPMI. While IPMI discusses messaging between a BMC and a remote management system using the RMCP protocol, it explicitly states that common IPMI messaging protocols and authentication mechanisms do not utilize encrypted packets. The Petition attempts to reinterpret IPMI’s mention of a secure secondary RMCP port (port 298h) as suggesting the use of encryption, but this same section clearly specifies that encryption is not employed. The absence of any disclosure or indication in IPMI that encryption was considered necessary, coupled with the substantial costs in terms of bandwidth, power, and latency associated with encryption, undermines the argument that a POSITA would naturally look to Frantz

to add this feature. Without a clear motivation or rationale, the combination of IPMI, Frantz, and Huckins fails to teach or suggest encrypted management requests, as required by the claims.

The Petition admits that IPMI does not disclose encryption for in-band management messages received via a LAN at the BMC, but asserts that it would have been obvious to modify IPMI to encrypt these management messages as taught by Frantz to improve security for the IPMI system.

IPMI discloses that IPMI messages are sent between a BMC (baseboard management controller) and a remote management system (remote console) and these messages conform to a RMCP (Remote Management Control Protocol). IPMI states that common IPMI messaging protocols and authentication mechanisms in this specification do not use encrypted packets. EX1020, 128-130. The Petition asserts that IPMI discusses a secure secondary RMCP port (port 298h), which suggests to a POSITA sending encrypted IPMI management message packets. Petition, 59. However, this port 298h is the port in which IPMI discloses that common IPMI messaging protocols and authentication mechanisms in this specification do not use encrypted packets, as illustrated with the blue boxes in section 12.1.2 reproduced below. EX1020,130.

12.1.2 RMCP Port Numbers

RMCP uses two well-known ports under UDP. The following table describes these ports and summarizes their use.

Table 12-1, RMCP Port Numbers

Port #	Name	Description
623 (26Fh)	Aux Bus Shunt (Primary RMCP Port)	Hereon referred to as the Primary RMCP Port - This port and the required RMCP messages must be provided to be conformant with the RMCP specifications. There is a mandatory set of messages that are required to be supported on this port. These messages are always sent 'in the clear' so that system software can discover systems that have RMCP support.
664 (298h)	Secure Aux Bus (Secondary RMCP Port)	Hereon referred to as the Secondary RMCP Port or Secure Port. This port is only used when it is necessary to encrypt packets using an algorithm or specification that prevents also sending unencrypted packets from being transferred via the same port. Since discovery requires sending 'in the clear' RMCP Ping/Pong packets, the secondary port is used to transfer encrypted transfers while the primary port continues to support unencrypted packets. An implementation that utilizes this port must still support the Primary RMCP Port and the required messages on that port in order to be conformant with the RMCP specifications. Note that the common IPMI messaging protocols and authentication mechanisms in this specification do not use encrypted packets, therefore IPMI messaging does not need to use the secondary port.

Therefore, without hindsight, there is no reason that a POSITA would read IMPI and determine, as the Petition argues, that encryption would be helpful, necessary, or important. Encryption requires additional system bandwidth, often a significant amount, additional system power, and often significant transmission latency. Given that IMPI does not disclose encryption of management requests and specifically indicates not using encrypted packets, there is no reason that a POSITA would look to Frantz to add the feature. Ex 2001, ¶83. Therefore, the combination of IPMI, Frantz, and Huckins fails to teach an encrypted form of management requests.

2. The Combination Of IPMI, Frantz, and Huckins Does Not Disclose “A Bus Controller Coupled To The Processor Via The First Bus” As Required By Claim 1

The Petitioner's attempt to combine the teachings of IPMI and Huckins to address the claimed invention relies on speculative assertions that lack evidentiary support and fail to establish a clear motivation for a POSITA to make such a combination. At the core of the argument is the claim that a POSITA would have turned to Huckins to implement a side-band connection involving a LAN controller interfacing with a PCI bus. However, SMBus and I2C protocols, as disclosed in IPMI, were already well known and straightforward to implement, leaving no basis for seeking further guidance from other references. Additionally, the technical functionalities of the LAN controller described in IPMI and the bus controller described in Huckins serve distinct purposes, making the combination proposed by the Petitioner incongruous and dependent on hindsight reasoning.

IPMI discloses a LAN controller connected to a BMC (baseboard management controller) by a 'side band' connection (e.g. SMBus or I²C). The Petition argues that IPMI does not explain how to implement such a network controller with such a side-band interface and that a POSITA would look to prior art sources for guidance as to how to implement it.

SMBus or I2C were well known communication protocols to a POSITA, so a POSITA would not look elsewhere as to how to implement such a side-band interface to a LAN controller without hindsight. There is no motivation to look elsewhere and no motivation to combine IPMI and Huckins. EX2001, ¶88.

The LAN controller of IPMI is not related to the architecture disclosed in the ‘016 Patent with respect to the two distinct buses. A LAN controller manages access points for connectivity to external networks or systems, while a bus controller manages or governs the flow of messages within a network. A POSITA would not look at IPMI and then look to Huckins to add a bus controller without the benefit of hindsight. EX2001, ¶89.

The Petition asserts that a POSITA would have recognized that one way to implement a side-band connection using a Network (LAN) Controller that interfaces with a PCI bus is by (1) adding a bridge between the PCI bus to which the Network (LAN) Controller interfaces and the side-band bus, which IPMI identified in Figure 12-1 as an I²C bus or SMBus, and (2) configuring the Network (LAN) controller to direct packets addresses to the BMC bridge. Then a POSITA would, therefore look to known implementations of a bridge between a PCI bus and an I²C bus or an SMBus. For this proposition, the Petition cites to the Declaration of Dr. Meldal at 196, which states the same thing. This is nothing other than a conclusory statement that does little, if anything, to explain why a POSITA would have understood and found it obvious at the time of invention, and yet Petitioner has not produced a single shred of evidence supporting it (and neither has their expert).

Table 4, below, provides a comparison of the arguments in the Petition, and the alleged supporting evidence in Dr. Meldal’s declaration (any differences

between the two are highlighted in yellow). They are nearly identical, and both fail to provide anything other than conclusory statements. Accordingly, Dr. Meldal's declaration should be given little weight.

TABLE 4

Petition	¶196 Expert Declaration
A POSITA would have recognized that one way to implement a side-band connection using a Network (LAN) Controller that interfaces with a PCI bus is by (1) adding a bridge between the PCI bus to which the Network (LAN) Controller interfaces and the side-band bus, which IPMI identified in Figure 12-1 as an I ² C bus or SMBus, and (2) configuring the Network (LAN) controller to direct packets addresses to the BMC bridge. EX1003, ¶196. A POSITA would therefore look to known implementations of a bridge between a PCI bus and an I ² C bus or an SMBus. EX1003, ¶196.	A POSITA would have recognized that one way to implement a side-band connection using a Network (LAN) Controller that interfaces with a PCI bus is by (1) adding a bridge between the PCI bus to which the Network (LAN) Controller interfaces and the side-band bus, which IPMI identified in Figure 12-1 as an I ² C bus or SMBus, and (2) configuring the Network (LAN) controller to direct packets addresses to the BMC bridge. A POSITA would therefore look to known implementations of a bridge between a PCI bus and an I ² C bus or an SMBus.

The comparison in Table 4 underscores the redundancy and conclusory nature of the arguments presented in both the Petition and Dr. Meldal's declaration. While both assert that a POSITA would recognize the implementation of a side-band connection via a PCI-I2C bridge as described, neither provides substantive reasoning or evidence to support this conclusion. The statements merely restate the same hypothesis without elaborating on why a POSITA would be motivated to adopt such

a configuration based on the teachings of IPMI and Huckins. This lack of evidentiary depth highlights the speculative nature of the Petitioner's argument and undermines the credibility of Dr. Meldal's testimony.

Furthermore, the technical distinctions between the LAN controller disclosed in IPMI and the purported combination with Huckins emphasize why a POSITA would not be motivated to make such a combination without the benefit of hindsight. IPMI's LAN controller serves as a network element managing multiple devices and traffic flow on an external LAN, a functionality far removed from the basic bridging role described in Huckins. These differences demonstrate the lack of a clear nexus between the references, further illustrating that the proposed combination does not align with the requirements of claim 1.

The purported enhancement of adding a PCI-I²C Bus Controller Bridge along with an Ethernet Interface and Side-band Logic to implement the LAN controller based on the disclosure of Huckins would not be understood by a POSITA. EX2001, ¶90. The LAN controller, envisioned by IPMI, is intended to support both wireless and wired LAN's present on the network external to the managed server. The Petitioner's Ethernet Interface is a single network port while a LAN controller is a network element that manages multiple devices on an external LAN. This would include managing multiple access points and/or managing network traffic flow between multiple elements on a LAN. Huckins does not envision the control of

multiple devices on an external LAN. EX2001, ¶ 90. The LAN controller of IPMI is disclosed as an “interface” to the cloud for operation on an external LAN. A POSITA would understand a LAN controller could include features like network segmentation, traffic management, and device configuration, across a network. This is opposed to a bridge whose primary function is connecting two networks. EX2001, ¶91. Accordingly, a POSITA would not look at IPMI and then look to another source (e.g. Huckins) to add a bus controller without the benefit of hindsight. EX2001, ¶89. Therefore, the combination of IPMI, Frantz, and Huckins does not disclose a bus controller coupled to the processor via the first bus, as recited in claim 1.

3. The Combination Of IPMI, Frantz, and Huckins Does Not Disclose “Wherein The Bus Controller Is Also Coupled To A Second Bus Of The Network Device That Is Distinct From The First Bus” As Required By Claim 1

As discussed above, since the combination of IPMI, Frantz, and Huckins does not disclose a bus controller, the combination of IPMI, Frantz, and Huckins fails to disclose “wherein the bus controller is also coupled to a second bus of the network device that is distinct from the first bus.” EX2001, ¶ 98.

4. The Combination Of IPMI, Frantz, and Huckins Does Not Disclose “The Bus Controller Is Configured To Receive The Encrypted Form Of The Management Requests From The Second Bus” As Required By Claim 1

As discussed above, since the combination of IPMI, Frantz, and Huckins does not disclose an encrypted form of management requests and does not disclose a bus controller, the combination of IPMI, Frantz, and Huckins fails to disclose “the bus controller is configured to receive the encrypted form of the management requests from the second bus.” EX2001,¶99.

5. The Combination Of IPMI, Frantz, and Huckins Does Not Disclose “And To Convey The Encrypted Form Of The Management Requests To The Processor Via The First Bus” As Required By Claim 1

As discussed above, since the combination of IPMI, Frantz, and Huckins does not disclose an encrypted form of management request and does not disclose a bus controller, the combination of IPMI, Frantz, and Huckins fails to disclose the bus controller is configured to...convey the encrypted form of the management requests to the processor via the first bus. EX2001,¶106.

6. The Combination Of IPMI, Frantz, and Huckins Does Not Disclose “The Bus Controller Is Configured To Receive The Encrypted Form Of The Management Requests From The Second Bus”, “And To Convey The Encrypted Form Of The Management Requests To The Processor Via The First Bus”, “Wherein The Processor Is Configured To Decrypt The Encrypted Form Of The Management Requests”, as required by claim 1

The Petitioner alleges that “IPMI discusses a secure secondary RMCP port (port 298h), which suggests to a POSITA sending encrypted IPMI management message packets.” Pet. at 59. To the extent this is true, nowhere does the IPMI teach or suggest that the BMC (the alleged “processor”) is capable of or is configured to

perform encryption / decryption operations. In particular, IPMI provides Table 3-1 that “summarizes the major required and optional functions for an IPMI-conformant BMC.” EX1020 at 50-52 (emphasis added). Neither any required nor any optional functions listed in this table mentions any encryption / decryption related functions. EX2001, ¶¶ 93, 100.

It is noted that the above-referenced table describes the mandatory “IPM Device” function as: “[t]he BMC must implement the mandatory IPM Device commands. If an IPMB is provided, the mandatory commands must be accessible from the IPMB.” Id. at 50. IPMI also states that “[a]ll management controllers are required to implement the mandatory IPM Device commands.” Id. at 53. IPMI further discloses both the required and optional “commands that are common to all Intelligent Platform Management (IPM) devices that follow this specification’s message/command interface,” where the “IPMI Management Controllers shall recognize and respond to these commands.” Id. at 185. Table 17-1, which discloses these mandatory and optional commands, does not list any commands, including the optional ones, that may perform encryption / decryption operations. See id. at 185-218. EX2001, ¶¶ 94, 101.

Furthermore, in Table 18-1, IPMI discloses “the commands used to support the system messaging interface.” Id. at 219-249. Among these the “Get Session Challenge Command,” the “Activate Session Command,” and the “Get AuthCode

Command” appear to employ authentication via hashing. See *id.* at 232-236, 239-40. In particular, IPMI states that the “Get AuthCode” command “is used to send a block of data to the BMC, whereupon the BMC will return a hash of the data.” *Id.* at 239. IPMI further states: EX2001, ¶¶95, 102.

Remote console software could request that system software perform a particular operation. In response, local system software could deliver a challenge string to the remote console, which would be required to hash it with the desired password and return the AuthCode to the local system software. The local system software would then perform the requested operation only if it found that the AuthCode matched the one returned by the BMC. *Id.* EX2001, ¶¶96, 103.

Thus, in executing the above-noted commands the BMC may provide a hashed, i.e., encrypted value, that may be used by the system software for validation. Per its own mandatory and optional functions listed in Table 3-1, and the mandatory and optional IPM Device functions and related mandatory and optional commands listed in Tables 17-1 and 18-1, the BMC (the alleged “processor”) does not and is not configured to encrypt / decrypt any of the received commands. To the extent Frantz (EX1006) discloses encryption of management messages and/or Huckins (EX1007) discloses a bus controller, this combination does not cure the above-identified defect of IPMI, that its BMC is not configured for encryption / decryption of commands. Therefore, any encrypted messages received at IPMI’s LAN

Controller would not be forwarded to the BMC (the alleged “processor”) for decryption thereof. Ex 2001, ¶¶97, 104.

Therefore, IPMI, Frantz, and Huckins, individually or in combination, do not teach or suggest “a bus controller coupled to the processor via the first bus ... wherein the bus controller is configured to receive the encrypted form of the management requests from the second bus, and to convey the encrypted form of the management requests to the processor via the first bus,” as claim 1 recites. Ex 2001, ¶97, ¶ 105.

Accordingly, Petitioner’s arguments fail as to the obviousness of the combination of IPMI, Frantz, and Huckins.

Independent claim 12 recites similar, although not identical, elements as independent claim 1 and independent claim 12 is not obvious over IPMI, Frantz, and Huckins for at least the same reasons provided above. EX2001, ¶ 99.

D. Independent Claim 1 is Not Obvious Over IPMI, IMPIV2.0, and Huckins Pursuant To 35 U.S.C. § 103

In Ground 10, the Petition relies on a combination of IPMI, IMPI v2.0, and Huckins, in challenging independent Claim 1 as allegedly obvious under 35 U.S.C. § 103.

This allegation is deficient since the combination of IPMI, IMPI v2.0, and Huckins does not disclose at least the claim features “a bus controller coupled to the

processor via the first bus,” and “wherein the bus controller is also coupled to a second bus of the network device that is distinct from the first bus.”

The Petition indicates that the analysis for the above claim elements is the same as in Ground 9. IPMI v2.0 was cited in Ground 10 as an alternate to Frantz regarding encryption. IPMI v2.0 does not disclose a bus controller and does not cure the deficiency of IPMI and Huckins regarding a bus controller. EX2001, ¶114. Therefore, as discussed above in relation to Ground 9, the combination of IPMI, IMPI v2.0, and Huckins fails to disclose “a bus controller coupled to the processor via the first bus,” and “wherein the bus controller is also coupled to a second bus of the network device that is distinct from the first bus,” as recited in claim 1. EX2001, ¶¶110-114.

Accordingly, Petitioner’s arguments fail as to the obviousness of the combination of IPMI, IPMIV2.0, and Huckins.

Independent claim 12 recites similar, although not identical, elements as independent claim 1 and independent claim 12 is not obvious over IPMI, IPMIV2.0, and Huckins for at least the same reasons provided above. EX2001, ¶111.

V. PETITIONER HAS NOT MET ITS BURDEN OF PROVING UNPATENTABILITY OF THE CHALLENGED CLAIMS

In an inter partes review (IPR), the Petitioner bears the burden of proving unpatentability of the challenged claims by a preponderance of the evidence under 35 U.S.C. § 316(e). The Petitioner must provide sufficient evidence and reasoning to establish that the claims are anticipated under § 102 or rendered obvious under § 103, as interpreted in *Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966). This includes demonstrating the scope and content of the prior art, identifying differences between the prior art and the claimed invention, and showing that a person of ordinary skill in the art (POSITA) would have had a reason to combine or modify the prior art with a reasonable expectation of success. (*KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007)). Conclusory statements or assertions lacking evidentiary support are insufficient to meet this burden. (*In re Magnum Oil Tools Int'l, Ltd.*, 829 F.3d 1364, 1380-81 (Fed. Cir. 2016)).

The Petitioner's evidence must be clear and supported by expert testimony or other technical analysis, particularly for complex or technical issues. However, expert testimony must do more than mirror the arguments in the Petition; it must provide detailed, independent analysis and adequately explain how the cited prior art meets the claim limitations. (*Arendi S.A.R.L. v. Apple Inc.*, 832 F.3d 1355, 1366 (Fed. Cir. 2016)). The Federal Circuit has also held that if a petitioner fails to address certain claim limitations or provide adequate rationale for a combination, the Board

cannot fill in the gaps with its own reasoning. (*In re Magnum Oil Tools Int'l, Ltd.*, 829 F.3d at 1381).

In the present case, the Petitioner has failed to meet its burden on all Grounds. Petitioner provides a meagre few paragraphs of argumentation to explain why concepts that are at the heart of the invention in the '016 Patent, and completely missing from the cited art, would have been obvious to a POSITA. See *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999) (holding that inherency cannot be established by probabilities or possibilities, emphasizing that this principle is particularly critical when the missing limitation goes to the heart of the invention). Petitioner mis-construes the cited references, placing emphasis on features of these references that have little to do with the inventions described therein. And Petitioner provides as support for its assertions mere conclusions, with no evidentiary support other than the identical conclusory statements of their expert. Accordingly, for all the reasons provided herein, this Petition should not be instituted.

VI. CONCLUSION

For the above reasons, Patent Owner respectfully requests that the Board deny institution of the Petition.

Respectfully submitted,

Dated: November 21, 2024

By: /Brandon R. Theiss/
Brandon R. Theiss
Registration No. 70,507
Counsel for Patent Owner
Intellectual Ventures II LLC

CERTIFICATE OF COMPLIANCE WITH WORD COUNT

Pursuant to 37 C.F.R. § 42.24(d), I certify that this Patent Owner Preliminary Response complies with the type-volume limits of 37 C.F.R. § 42.24(b)(1) because it contains 13,964 words, excluding the parts of this Patent Owner's Preliminary Response that are exempted by 37 C.F.R. § 42.24(a), according to the word processing system used to prepare this Patent Owner's Preliminary Response.

Respectfully submitted,

Dated: November 21, 2024

By: /Brandon R. Theiss/
Brandon R. Theiss
Registration No. 70,507
Counsel for Patent Owner
Intellectual Ventures II LLC

CERTIFICATE OF SERVICE

The undersigned certifies that pursuant to 37 C.F.R. § 42.6(e), a copy of the foregoing **PATENT OWNER'S PRELIMINARY RESPONSE** was served via email (as consented to by counsel) on November 21, 2024 to lead and backup counsel of record for Petitioners as follows:

James Heintz
Jim.heintz@us.dlapiper.com

Gianni Minutoli
gianni.minutoli@us.dlapiper.com

DLA Piper LLP
One Fountain Square
11911 Freedom Drive
Suite 300
Reston, VA 20190-5602
Service email: DLA-LenovoIPR-IV@us.dlapiper.com

Dated: November 21, 2024

By: /Brandon R. Theiss/
Brandon R. Theiss
Registration No. 70,507
Counsel for Patent Owner
Intellectual Ventures II LLC