

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

LENOVO (UNITED STATES) INC.,  
Petitioner

v.

INTELLECTUAL VENTURES II, LLC,  
Patent Owner

---

IPR2024-00109  
U.S. Patent No. 8,474,016

**DECLARATION OF DR. STEVEN GOLDBERG  
IN SUPPORT OF PATENT OWNER RESPONSE**

## TABLE OF CONTENTS

|      |                                                                                                                                                            |    |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| I.   | INTRODUCTION .....                                                                                                                                         | 1  |
| II.  | Background and Qualifications .....                                                                                                                        | 2  |
| III. | MATERIALS USED .....                                                                                                                                       | 7  |
| IV.  | LEGAL FRAMEWORK .....                                                                                                                                      | 7  |
| A.   | Anticipation and Obviousness.....                                                                                                                          | 8  |
| B.   | Level of a Person of Ordinary Skill in the Art.....                                                                                                        | 10 |
| V.   | THE '016 PATENT AND THE CHALLENGED CLAIMS .....                                                                                                            | 12 |
| A.   | Overview of '016 Patent .....                                                                                                                              | 12 |
| B.   | Challenged Claims of the '016 Patent.....                                                                                                                  | 18 |
| C.   | Claim Construction.....                                                                                                                                    | 20 |
| VI.  | Overview of Prior Art.....                                                                                                                                 | 20 |
| A.   | Overview of Neufeld .....                                                                                                                                  | 20 |
| B.   | Overview of Frantz.....                                                                                                                                    | 22 |
| C.   | Overview of PCI Bridge Spec.....                                                                                                                           | 23 |
| D.   | Overview of IPMI .....                                                                                                                                     | 23 |
| E.   | Overview of Huckins.....                                                                                                                                   | 24 |
| F.   | Overview of IPMI v2.0 .....                                                                                                                                | 25 |
| VII. | OPINIONS REGARDING PETITION GROUND 1 .....                                                                                                                 | 25 |
| A.   | Neufeld Fails to Disclose Every Feature Recited in Challenged Claims 1-3, 6, 9, 12, and 17 as Required Under 35 U.S.C. 103 .....                           | 25 |
| 1.   | 1.e Neufeld Fails to Disclose “a bus controller coupled to the processor via the first bus”.....                                                           | 26 |
| 2.   | 1.f 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” ..... | 28 |
| 3.   | 1.g. Neufeld Fails to Disclose “the bus controller is configured to receive the encrypted form of the management requests from the second bus” .....       | 28 |

|                                                  |                                                                                                                                                                                                   |    |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 4.                                               | 1.h. Neufeld Fails to Disclose “to convey the encrypted form of the management requests to the processor via the first bus” ....                                                                  | 29 |
| 5.                                               | 1.i. Neufeld Fails to Disclose “wherein the processor is configured to decrypt the encrypted form of the management requests” .....                                                               | 30 |
| VIII. OPINIONS REGARDING PETITION GROUND 2 ..... |                                                                                                                                                                                                   | 31 |
| A.                                               | The Petition Fails to Prove That Claims 1-3, 6, 9, 12, and 17 are Obvious Over Neufeld In Combination With Frantz and PCI Bridge Spec .....                                                       | 31 |
| B.                                               | Claim 1 .....                                                                                                                                                                                     | 31 |
| 1.                                               | 1.e A combination of Neufeld, Frantz, and PCI Bridge Spec Fails to Disclose “a bus controller” .....                                                                                              | 35 |
| 2.                                               | 1.f A 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” ...    | 35 |
| 3.                                               | 1.g A 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” ..... | 36 |
| 4.                                               | 1.h A combination of Neufeld, Frantz, and PCI Bridge Spec Fails to Disclose “to convey the encrypted form of the management requests to the processor via the first bus” .....                    | 36 |
| C.                                               | Claim 12 .....                                                                                                                                                                                    | 37 |
| IX. OPINIONS REGARDING PETITION GROUND 9.....    |                                                                                                                                                                                                   | 38 |
| A.                                               | The Petition Fails to Prove That Claims 1-3, 9, 12, 15 and 17 is Obvious Over IPMI In Combination With Frantz and Huckins .....                                                                   | 38 |
| B.                                               | Claim 1 .....                                                                                                                                                                                     | 38 |
| 1.                                               | 1.b A combination of IPMI and Frantz fails to disclose “receive data requests and an encrypted form of management requests via the network interface” .....                                       | 38 |
| 2.                                               | 1.e A combination of IPMI and Huckins fails to disclose “a bus controller coupled to the processor via the first bus” .....                                                                       | 39 |

|     |                                                                                                                                                                                             |    |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 3.  | 1.f A combination of IPMI and Huckins fails to disclose “the bus controller is also coupled to the a second bus of the network device that is distinct from the first bus” .....            | 41 |
| 4.  | 1.g A 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” .....      | 41 |
| 5.  | 1.h A combination of IPMI, Frantz, and Huckins fails to disclose “convey the encrypted form of the management requests to the processor via the first bus” .....                            | 44 |
| C.  | Claim 12 .....                                                                                                                                                                              | 46 |
| X.  | OPINIONS REGARDING PETITION GROUND 10 .....                                                                                                                                                 | 47 |
| A.  | The Petition Fails to Prove That Claims 1-3, 9, 12, 15 and 17 is Obvious Over IPMI In Combination With IPMI V2.0 and Huckins..                                                              | 47 |
| 1.  | 1.e A combination of IPMI, IPMI V2.0, and Huckins fails to disclose “a bus controller coupled to the processor via the first bus” .....                                                     | 47 |
| 2.  | 1.f A combination of IPMI, IPMI V2.0, and Huckins fails to disclose “the bus controller is also coupled to the a second bus of the network device that is distinct from the first bus”..... | 49 |
| 3.  | 1.g A combination of IPMI, IPMI V2.0, and Huckins fails to disclose “the bus controller is configured to receive the encrypted form of the management requests from the second bus” .....   | 49 |
| 4.  | 1.h A combination of IPMI, IPMI V2.0, and Huckins fails to disclose “convey the encrypted form of the management requests to the processor via the first bus” .....                         | 50 |
| B.  | Claim 12 .....                                                                                                                                                                              | 50 |
| XI. | CONCLUSION.....                                                                                                                                                                             | 51 |

I, Steven Goldberg, hereby declare the following:

## **I. INTRODUCTION**

1. My name is Dr. Steven Goldberg. I have been retained by counsel for Patent Owner as a technical expert in the above-captioned *Inter Partes* Review (“IPR”) matter. Specifically, I have been asked to study and provide my opinions on the technology described and claimed by U.S. Patent Nos. 8,474,016 (the “’016 Patent”) and to provide my opinions as to the patentability of certain claims of the ‘016 Patent based on review of the prior art relied upon in the IPR. I understand that the patent application for the ‘016 Patent was filed on November 29, 2007 and ultimately claims priority to a U.S. patent application having a filing date of June 13, 2002. I understand the priority date for this patent is disputed. Petitioner contends that the filing date of the patent is October 21, 2003. However, the ‘016 Patent says: This application is a continuation of U.S. patent application Ser. No. 10/969,561, filed Oct. 20, 2004, which in turn is a continuation-in-part of U.S. patent application Ser. No. 10/461,827, filed Jun. 13, 2003. U.S. patent application Ser. No. 10/969,561 also claims the benefit of U.S. Provisional Application No. 60/512,777, filed Oct. 21, 2003. U.S. patent application Ser. No. 10/461,827 in turn claims the benefit of U.S. Provisional Application No. 60/388,287, filed Jun. 13, 2002, and U.S. Provisional Application No. 60/438,282, filed Jan. 6, 2003. The present invention is related to the invention described in co-owned U.S. Pat. No. 7,171,467, filed on Jun.

13, 2003 and issued on Jan. 30, 2007, which is incorporated herein by reference. The present invention is also related to the invention described in co-owned and co-pending U.S. patent application Ser. No. 11/611,210, filed on Dec. 15, 2006, which is incorporated herein by reference. I understand that the Challenged Claims are claims 1-21 from the '016 Patent. My opinions in this Declaration are limited to those Challenged Claims.

2. My compensation in this matter is not based on the substance of my opinions or the outcome of this matter. I have no financial interest in the Patent Owner. I am being compensated at an hourly rate of \$500 for my analysis and testimony in this case.

## **II. BACKGROUND AND QUALIFICATIONS**

3. I am currently a Partner at Finistere Ventures, an early-stage venture capital firm. Additionally, I am the sole proprietor of a consulting business, dba Air Access, where I provide engineering, technical and management services. In that role, I direct and advise a number of high-tech start-up companies and provide litigation technical consulting and support services. My current curriculum vitae (CV) is attached at Exhibit A and some highlights follow.

4. My forty-year career in the technology industry includes employment as an RF engineer, algorithm engineer, digital design engineer, engineering manager, business general manager, CEO, technology investor, and board member. The vast

majority of these positions were at companies involved in wireless communications, telematics, radar technology, communications technology, automotive, and/or embedded systems (those that include hardware, software, and algorithms).

5. I received a B.S.E.E. degree and M.S.E.E. degree from Washington University, St. Louis, Missouri in 1975 and 1980, respectively. I also received a Ph.D. in Electrical Engineering from the University of California, Santa Barbara in 1988.

6. My graduate education focused on digital and analog communications and related algorithms. My Ph.D. doctoral thesis focused on direct sequence spread spectrum communications and wireless technology, which includes technology related to the Global Positioning System (GPS), a technology based on direct sequence spread spectrum technology.

7. I was twice employed at Trimble Navigation, Sunnyvale, CA, a global leader in GPS technology. In my first position at Trimble, from 1991 to 1995, I was an Engineering Manager with the Vehicle Tracking Division of the company and a Senior Engineer in the Differential Corrections Group in the Survey Division. My group within the Vehicle Tracking Division—which was composed of hardware, software, and algorithm engineers—designed, developed, and manufactured tracking systems for cars, trucks, first responders, and public transportation systems. My second period of employment with Trimble Navigation was from September

2008 to September 2009. During this time, I was the Program Manager for the Trimble Military Division where I led approximately 20 hardware, software, algorithm, mechanical, and RF engineers in the design of the next generation M-Code GPS system for military aircraft.

8. My software and programming experience includes programming activity through undergraduate, graduate, Ph.D. programs in Fortran and Matlab (1971-1988). As a Systems Engineer at Applied Signal Technology (1988-1991), my job was to create algorithms to help the National Security Agency and the CIA to receive and decode wireless messages from entities of interest internationally (known as Signal Intelligence). I designed and tested my algorithms in MATLAB, a programming language used by systems engineers. From 1991-2009, I had hundreds of software engineers reporting to me in my roles as Engineering Manager, VP Engineering, and CEO, including over 250 software engineers as part of my role of VP of Engineering at Nokia. I regularly reviewed product software architectures and validated, at a system and algorithmic level, the functionality and the potential performance of a wide variety of products, from GPS receivers and wireless/microwave radios to Internet Security products.

9. Additionally, earlier in my career, I was an engineer with California Microwave, Inc., Emerson Electric Co., and an engineer at the Hewlett Packard

Company, where I regularly had responsibility for radar component design and/or radar system measurements.

10. Notably, I was also a founder and engineering leader at DataRunway, a startup company focused on the design, manufacture, and sale of a system that would provide high-speed data to aircraft in flight.

11. Throughout my career, I was very close to “product” and “product development.” As an engineer, engineering manager, VP of engineering, General Manager, CEO, and corporate board member, I have been directly involved in product definition, market validation, product development, testing, manufacturing, pricing, sales, and support. My product management experience includes the creation and oversight of Market Requirements Documents (MRD; created by Marketing Dept), Product Requirements Documents (PRD; created by Product Managers), and System Specification Documents (SSD; created by engineering departments). These documents are tied to a detailed process that guides and enables the creation of a product by assessing and responding to the market and customer needs.

12. Additionally, at Trimble Navigation, Cylink, Applied Signal Technology, Nokia, DataRunway, and Vidient, I was involved with the generation of intellectual property, specifically, patents, related to the products planned for current and future development in the fields of GPS, RF and microwave

communications, communications signal processing, receiver design, and RF and microwave components.

13. My professional experience also includes the comparative analysis of competing products and features in a given marketplace as a mechanism for product valuation and unit pricing. This analysis typically involves leveraging a multidisciplinary evaluation of the product that requires an understanding of the hardware, software, algorithmic, user interface, and aesthetic design, and a valuation of the intellectual property associated with these aspects of the product.

14. Additionally, I worked for 11 years at Venrock, a Venture Capital firm, as a Partner where I evaluated and provided technical diligence for a wide range of technology companies, including semiconductors, networking equipment and software, wireless technology, Internet security, electric vehicle manufacturers, electric utility grid generation and grid storage companies, electric vehicle charging companies and technology, and technology related to electric utility load balancing and supply.

15. My experience of nearly 40 years in academic, financial, and practical situations as well as my hands-on experience, has given me a detailed appreciation of the technology involved with the '016 Patent.

### III. MATERIALS USED

16. In writing this Declaration, I have considered the following: my own knowledge and experience, including my work experience in the above fields; my experience in teaching those subjects; and my experience in working with others involved in those fields. I have also reviewed the Petition and the following references as well as the background materials referenced below in my analyses:

- The Petition in the above-captioned IPR matter;
- U.S. Patent 8,474,016 (Ex. 1001)
- U.S Patent 8,474,016 File History (Ex. 1004)
- Neufeld, U.S. Patent Application, 2003/0226015A1 (Ex. 1005)
- Frantz, U.S. Patent No. 7,085,385 (Ex. 1006)
- Huckins, U.S. Patent Publication No. 2003 /0097503A1 (Ex. 1007)
- PCI Bridge Spec, “PCI-to-PCI Bridge Architecture Specification”, Rev 1.1 (Ex. 1008)
- IPMI, “IPMI – Intelligent Platform Management Interface Specification V1.5” (Rev 1.1 dated 2/20/2002) (Ex. 1020)
- IPMI v2.0, “IPMI – Intelligent Platform Management Interface Specification V2.0” (draft dated 9/15/2003) (Ex. 1023)
- Information Security Management: Global Challenges in the New Millennium, Gurpreet Dhillon, Idea Group Publishing., 2001 (Ex. 2003)
- The Froehlich/Kent Encyclopedia of Telecommunications, Vol. 9, Editor in Chief: Fritz E. Froehlich, 1990 (Ex. 2004)
- Scott Mueller’s UPGRADING AND REPAIRING PCs, Scott Mueller, Que Publishing, August 2003 (Ex. 2005)

### IV. LEGAL FRAMEWORK

17. I have been informed by counsel for Patent Owner that the following legal principles apply to an analysis of patentability based on 35 U.S.C. § 102 for

anticipation or lack of novelty, and 35 U.S.C. § 103 for obviousness. I have also been informed that, in an *Inter Partes* Review proceeding such as this proceeding, to render a patent claim unpatentable, Petitioner must show by a preponderance of the evidence that the claim would have been anticipated by a single reference or rendered obvious by one or more properly combined prior art patents or publications.

**A. Anticipation and Obviousness**

18. I understand that there are two ways in which prior art may render a patent claim unpatentable. First, the prior art can “anticipate” the Claim. I understand that a patent claim may be invalid as “anticipated” under 35 U.S.C. § 102 if each and every limitation of the claim as properly construed is found, either expressly or inherently, in a single prior art reference, such as a publication or Patent, that predates the claimed subject matter. Second, the prior art can render the claim “obvious” to a person of ordinary skill in the art (“POSITA”). I understand that for an invention claimed in a patent to be patentable, it must not be anticipated and must not be obvious based on what was known before the invention was made.

19. I understand that a feature may be expressly or inherently disclosed in a reference. I understand that in order to establish that a reference inherently teaches a feature, the mere fact that a certain thing may result from a given set of circumstances is not sufficient. Instead, to establish inherency, I understand that the missing descriptive matter is necessarily present in the thing described in the reference, and

that it would be so recognized by persons of ordinary skill. Put another way, inherency requires that one of ordinary skill in the art would recognize that a reference unavoidably teaches the property in question.

20. I understand that to find a Patent invalid for obviousness, the Petitioner must prove that the differences between the claimed invention and the prior art taken as a whole would have been obvious to one of ordinary skill at the time the invention was made.

21. I have been informed that to render a claim obvious, a combination of prior art references must disclose each claim element of that claim, and that obviousness is a question of law based on the underlying facts. I understand that the underlying factual inquiries are: (1) the scope and content of the prior art, (2) the differences between the prior art and the claims at issue, (3) the level of ordinary skill in the pertinent art, and (4) secondary considerations of non-obviousness.

22. I am also informed that the fact that all of the elements of a claimed invention can be found separately in more than one prior art reference is not sufficient to warrant a finding that a claimed invention is obvious. There must be a reason why it would have been obvious to modify or combine the prior art to arrive at the claimed invention. I understand that a helpful insight into this determination is whether there is a teaching, suggestion or motivation in the prior art that would lead one of ordinary skill in the art to combine the elements. When there is no

suggestion for the proposed combination, or when the prior art suggests something other than the combination, a finding of obviousness is generally not warranted.

23. I understand that the prior art must be considered in its entirety, including disclosures that teach away from the claimed invention. Furthermore, if a proposed modification to a prior art reference would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification.

24. I understand that the pertinent obviousness inquiry takes place at the time of the invention. Therefore, the use of hindsight in an obviousness analysis is impermissible.

25. I further understand that, in making a determination as to whether the claimed invention would have been obvious to a person of ordinary skill, the fact finder must consider certain objective factors, such as commercial success, long-felt, but unsolved need, unexpected results, copying, and praise by others in the field. The presence of such factors—known as “secondary considerations”—is evidence of non-obviousness. I also understand that a connection, or nexus, must exist between the secondary consideration and the claimed invention.

**B. Level of a Person of Ordinary Skill in the Art**

26. I was asked to provide my opinion as to the level of skill of a person of ordinary skill in the art (“POSITA”) of the ’016 Patent at the priority date of the

claimed invention, which counsel has told me to assume is June 13, 2003. In determining the characteristics of a hypothetical POSITA of the '016 Patent, I considered several factors, including the type of problems encountered in the art, the solutions to those problems, the rapidity with which innovations are made in the field, the sophistication of the technology, and the education level of active workers in the field.

27. In my opinion, a POSITA as of the effective filing date of the '016 Patent would be an engineer or team of engineers that have knowledge of computer networking, computer networking architecture, and computer security.

28. The POSITA would have had a Bachelor's Degree in electrical engineering, computer science, industrial engineering, or computer engineering or a related subject or similar discipline and/or one to two years of similar or like work experience in communications, embedded systems, computing devices, security, and/or distributed computing. Additional education could substitute for professional experience and vice versa. Such an individual POSITA or team of POSITAs would have been capable of understanding the '016 Patent and the prior art references discussed herein. I apply this level of ordinary skill throughout this declaration.

29. Based on my education, training, and professional experience in the field of the claimed invention, including teaching the requisite skills necessary for a POSITA during the relevant time period, I am familiar with the level and abilities of

a POSITA of computer networks at the time of the claimed invention. Additionally, I met at least these minimum qualifications to be a POSITA of computer networks as of the time of the claimed invention of the '016 Patent. Specifically, by June 13, 2003, I had already obtained a Ph.D. degree in Electrical Engineering and accumulated at least 20 years of experience in the design and/or testing of computer and/or communications technology.

## **V. THE '016 PATENT AND THE CHALLENGED CLAIMS**

### **A. Overview of '016 Patent**

30. The '016 Patent abstract states:

A computer network management apparatus and method for remotely managing a networked device. The apparatus and method includes a management processor which is in direct communication with the networked device. The apparatus and method provides access for remotely and securely managing a networked device. The apparatus and method further separates management communications from user communications to ensure the security of the management communications. The apparatus and method further includes network and power monitoring and notification systems. The apparatus and method further provides authentication and authorization capabilities for security purposes.

31. The Background of the Invention of the '016 Patent states “in distributed computer networks the vast majority of the networking elements are not in the same geographic location or easily accessible by the skilled technicians or network administrators typically responsible for normal maintenance of the elements.

32. This drove a strong requirement to provide for remote management of network elements and servers. However, the security of the network elements and servers is a concern when remote management is used. The remote management can come in the form of in-band management (where the management and control messages share the same communications path as the data) or out-of-band management (where a different communications path is used for management messages and control).

33. When network administrators use out-of-band communication to access a network element, they typically connect through a console or management port, making it a more secure option than in-band communication. At the time the '016 Patent application was filed, out-of-band communication was regarded as the gold standard for remote network maintenance when physical access to all network elements was not feasible. In contrast, in-band remote maintenance relies on the security of the network where the managed element resides to safeguard management traffic. While this approach may offer reasonable protection against

external threats, it is generally insufficient to defend against internal attacks originating within the network.

34. Despite its advantages, out-of-band communication for network maintenance has notable drawbacks. The most significant is the requirement for a dedicated network for using out-of-band communication for network maintenance. Establishing such infrastructure can be prohibitively expensive, making it a challenging solution for many organizations.

35. Due to the limitations of both in-band and out-of-band communication for network maintenance in distributed computer networks, many systems use a combination of the two approaches. However, in scenarios where in-band communication is employed—whether as an optional method or the sole method for network maintenance—a specific issue arises that must be addressed. The '016 Patent provides solutions to this problem. 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.

36. The '016 Patent addresses the need for a secure system enabling remote network maintenance through both in-band and out-of-band communication. Additionally, the network described in the patent, particularly as outlined in independent claim 1, incorporates secure management access control functions implemented on a separate processor. As detailed in the patent specification, this configuration ensures that management traffic can be securely transmitted over the in-band path.

37. FIG. 1 of the '016 Patent illustrates a managed device within a distributed computer network (also referred to as a managed network). It is important to note that the invention described in the '016 Patent is not limited to the configuration shown in FIG. 1; for example, FIG. 14 depicts an alternative layout. As shown in FIG. 1, the SMACC [red highlighting] is integrated into a managed device within the distributed computer network. The SMACC is communicatively coupled to both the CPU Bus and the System Bus [green highlighting] of the managed network device. The managed network device is configured for communication via various user data interfaces [blue highlighting] via the System Bus.

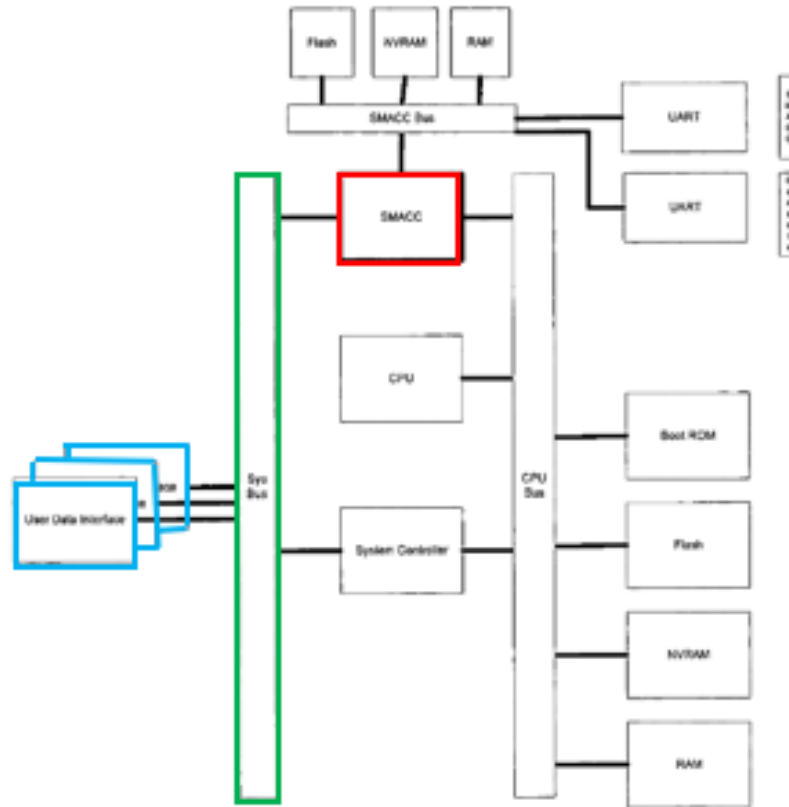


Fig. 1

38. The managed device is equipped with two types of interfaces for transmitting management data used in remote network maintenance: a Virtual Management Interface (VMI) and a SMACC Network Enabled Management Interface. A network administrator can connect to the SMACC on the managed device through either the VMI or the SMACC Network Enabled Management Interface. These interfaces are illustrated in FIG. 3 of the '016 Patent.

39. As shown in FIG. 3, the VMI [purple highlighting] is positioned 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 used for the network connection" (in other words, for in-band communication using a User Data Interface). The SMACC Network Enabled Management Interface provides "a physically separate interface for the management network connection, distinct from the user interfaces on the managed device" (or, in other words, for out-of-band communication over a dedicated management network).



Fig. 3

40. A bus controller or controller chip may be used to enable the SMACC processor to access the required bus, as shown in FIGS. 28 and 29.

41. 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. There is described three primary functions of the VMI: connecting a remote

administrator with the SMACC, separating management data from user data, and in-Band communication of management data.

42. The Virtual Management Interface (VMI) logically separates management traffic from user data when both are routed through the same interfaces on the managed device and the same physical network. In a preferred embodiment, the VMI uses a Virtual Private Network (VPN) mechanism, such as IPSec, to encrypt and protect the management traffic, ensuring it is logically separated before being passed to the user interfaces. Management traffic is not permitted to be sent directly to the user interfaces. It must pass through one of the dedicated management interfaces (either the VMI or the SMACC interface). The VMI enables any of the user interfaces to be used for management traffic while maintaining the security and integrity of the management interface and traffic. Management information can be transmitted over either the VMI or SMACC Interface, with encryption applied to protect the data.

## **B. Challenged Claims of the '016 Patent**

43. Petitioner challenges independent Claims 1 and 12 and dependent claims 2-11 and 13-21.

Independent Claim 1 recites:

An apparatus, comprising:

a processor configured to control one or more functions of a network device having a network interface, wherein the network device is configured to receive data requests and an encrypted form of management requests via the network interface, wherein the management requests are from a remote administrator;

a first bus; and

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

wherein the processor is configured to decrypt the encrypted form of the management requests, wherein the network device includes a processor configured to facilitate operation of the network device, and wherein the processor of the apparatus is distinct from the processor included in the network device.

Independent Claim 12 recites:

A method, comprising:

receiving, by a bus controller of a management device, an encrypted form of management requests via a first bus of a network device having a network interface, wherein the network device received the encrypted form of the management requests and data requests via the network interface, wherein the management requests are from a remote administrator;

conveying the encrypted form of management requests from the bus controller to a processor of management device via a second bus of the management device, wherein the network device includes a processor configured to facilitate operation of the network device, and wherein the processor of the management device is distinct from the processor included in the network device;

decrypting, by the processor, the encrypted form of the management requests;  
and

controlling, by the processor, one or more functions of the network device according to the management requests.

**C. Claim Construction**

44. I have been advised that, for the purpose of this IPR proceeding, the standard for construing the claim terms is the same standard as applied by federal district courts in patent litigation. I have been asked to assume that the words of the claims are generally given their ordinary and customary meaning as understood by a person of ordinary skill in the art at the time of the invention. I have further been advised that a person of ordinary skill in the art at the time of the invention should consider the ordinary meaning of the claim terms in the context of the entire Patent as a whole, including the specification. I also understand that dictionaries, encyclopedias, treatises, and textbooks available at the time the Patent may also be relied upon by a person of ordinary skill in the art when considering the meaning of patent claim terms.

**VI. Overview of Prior Art**

**A. Overview of Neufeld**

45. Neufeld describes a remote management system as shown in FIG. 1. 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.

46. The managed server 2, illustrated in FIG. 1, contains a remote management controller 116. FIG. 2 of Neufeld shows the location of the remote management controller 116 within the CPU 3 of the managed server 2. FIG. 3 of Neufeld 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. For in-band communication, the remote management controller 116 is "attached to the PCI bus 16." Also connected to the PCI bus 16 are a video graphics controller 114 and one or more communication devices, such as a network interface controller (NIC) 110. The managed server 2 is equipped with specialized circuitry and software capable of capturing, analyzing, compressing, and transmitting video activity to the remote console 5, independently of the operating system (OS). This video data can be transmitted over the network N to the remote management PC 5 via the NIC 110. Since the remote management controller 116 operates independently of the OS, this

in-band communication can occur whether the OS is operational or not, and it can also support system setup before the OS is active.

47. An address translation and bridging (“ATB”) unit 170 is operatively coupled to the internal local bus 166 and to a PCI bus 172. Ex. 1005, ¶ [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.

**B. Overview of Frantz**

48. Frantz discusses creating a remote network management tool capable of establishing a strongly encrypted communication path with a managed server over a publicly accessible network. Figure 4 of Frantz illustrates the process for setting up a secure connection with a managed server via the Internet. Initially, a remote console applet establishes an unencrypted communication link ("in the clear"). The applet then prompts the browser to request a secret key from a remote web server. The web server delivers the secret key to the browser over an encrypted link, which is subsequently shared with the remote console server. The browser transmits the secret key to the remote console applet, enabling the applet and the console server to initiate encrypted communication using the shared secret key.

**C. Overview of PCI Bridge Spec**

49. The PCI Bridge Specification outlines the behavior of a compliant PCI-to-PCI bridge. This bridge establishes a connection between two independent PCI buses. Its main function is to enable transactions between a master on one PCI bus and a target on the other. A typical application of the bridge, as depicted in Figure 1-1, involves creating a second PCI bus segment (labeled PCI Bus 1) to which additional PCI connectors are connected.

**D. Overview of IPMI**

50. IPMI (Intelligent Platform Management Interface) is a standardized protocol developed by Intel for remote server management and monitoring, even when the operating system is down or the system is powered off. It primarily utilizes out-of-band communication, offering multiple dedicated management ports, such as auxiliary IPMB connectors for remote management cards, an Intelligent Chassis Management Bus (ICMB) bridge, and a serial connector. These management ports are illustrated in FIG. 1-2 of the IPMI specification (reproduced below). While IPMI is primarily designed for out-of-band management, it also supports a form of in-band communication. The intelligence behind IPMI is provided by the Baseboard Management Controller (BMC), which manages the interface between system management software and platform management hardware. The BMC is responsible for autonomous monitoring, event logging, recovery control, and serves as the

gateway between the system management software and both the IPMB and ICMB.

In terms of in-band communication, as shown in Figure 1-2 of IPMI, the BMC shares a network interface with the managed system's network traffic. Using the embedded LAN Controller Implementation, IPMI messages are transmitted between the BMC and a remote management system (remote console) over an Ethernet LAN connection using UDP over IPv4. The UDP datagrams are formatted to carry IPMI request and response messages. The LAN controller detects UDP datagrams sent to a designated "management port," forwarding them to a "side-band" interface for delivery to or from the BMC. The BMC can also use this interface to inject datagrams onto the LAN, interleaving them with network packets generated by the system software.

#### **E. Overview of Huckins**

51. Huckins describes a system where a non-PCI bus controller 126 is connected to a PCI bus 131 and an I/O Controller Hub (ICH) 130, as shown in Figure 1. The non-PCI bus controller 126 is capable of both receiving and transmitting signals to and from the system 100 via the PCI bus 131. It is also physically and electrically compatible with the PCI bus protocol, allowing it to connect to the PCI bus 131. This non-PCI bus controller 126 can be referred to as a bus bridge. Additionally, a non-PCI device 133 is connected to the non-PCI bus controller 126 through a bus 132 that uses a protocol different from PCI. As a result, the non-PCI

device 133 can interact with the rest of the system 100 through the PCI bus 131, despite not being designed to operate with the PCI protocol. The bus bridge 126 enables communication between the computer system 100 and the non-PCI device 133 via the PCI bus 131.

**F. Overview of IPMI v2.0**

52. IPMI v2.0 is a standardized protocol developed by Intel that introduces enhancements to the original IPMI specification. RMCP+ (Remote Management Control Protocol Plus) is the name given to the improved protocol used for transferring IPMI messages and other payloads to an IPMI-based BMC over IP. RMCP+ includes support for multiple payload types within an IPMI session, enhanced user authentication algorithms, encryption capabilities, and better integration with ASF 2.0.

**VII. OPINIONS REGARDING PETITION GROUND 1**

**A. Neufeld Fails to Disclose Every Feature Recited in Challenged Claims 1-3, 6, 9, 12, and 17 as Required Under 35 U.S.C. 103**

53. Petitioner asserts in Ground 1 of the Petition that Neufeld renders obvious Challenged Claims 1-3, 6, 9, 12, and 17 of the '016 Patent under 35 U.S.C. § 103. Petitioner's arguments in Ground 1 do not establish a reasonable likelihood that any of the Challenged Claims are unpatentable because: (1) in Claims 1.e and

1.f the Petitioner improperly identifies the Neufeld ATB as the claimed “bus controller”, and (2) in Claims 1.h and 1.i, Petitioner improperly argues that Neufeld discloses an “encrypted form of the management requests” are conveyed to the first processor via the first bus and that the “processor is configured to decrypt the encrypted form of the management requests.”

**1. 1.e Neufeld Fails to Disclose “a bus controller coupled to the processor via the first bus”**

54. It is my opinion that Neufeld does not disclose “a bus controller” to render obvious Limitation 1.e under 35 U.S.C. § 103.

55. As Petitioner states, Neufeld discloses that the ATB 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.” Petitioner incorrectly extrapolates that this implies that the ATB 170 performs the functions of a “bus controller”. I disagree.

56. A POSITA would understand that a "bus controller" manages or governs the flow of traffic on a single bus, determining which device can access the bus and when it can access the bus. 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.

57. For example, a “PCI bus is an arbitrated bus: A central arbiter (part of the PCI bus controller in the motherboard chipset) governs all bus transfers, giving fair and controlled access to all the devices on the bus. Before a master can use the bus, it must first request control from the central arbiter, and then it is granted control for only a specified maximum number of cycles. This arbitration allows equal and fair access to all the bus master devices, prevents a single device from hogging the bus, and also prevents deadlocks because of simultaneous multiple device access”. (see Chapter 4, page 342, “*Scott Mueller’s UPGRADING AND REPAIRING PCs*”, Scott Mueller, August 2003).

58. 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).

59. A POSITA would not read the above disclosure in Neufeld and understand that that ATB 170 is a bus controller based on only the description in the specification.

**2. 1.f 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”**

60. Since Neufeld does not disclose a “bus controller” as discussed above regarding 1.e, Neufeld does not disclose a bus controller coupled to a second bus of the network device that is distinct from the first bus.

**3. 1.g. Neufeld Fails to Disclose “the bus controller is configured to receive the encrypted form of the management requests from the second bus”**

61. Petitioner states, without support, that “the ATB 170 receives the encrypted management requests from the remote management PC 5 through the NIC 110 via the PCI bus 172.” I disagree. Neufeld does not disclose “encrypted” management requests being received. Further, since Neufeld does not disclose a bus controller as discussed above regarding 1.e, Neufeld does not disclose the bus controller is configured to receive the encrypted form of the management requests from the second bus. Neufeld discusses security and encryption for *accessing or authenticating* a system remotely and does not teach an encrypted form of a management request.

**4. 1.h. Neufeld Fails to Disclose “to convey the encrypted form of the management requests to the processor via the first bus”**

62. Petitioner states that Neufeld teaches or at least suggests the encryption of management requests, citing statements in Neufeld that “security may be an important issue when remotely communicating management requests to the managed server” and that “any type of remote access would typically utilize encryption techniques.” Pet. at 20. Even if this assertion were accurate, Neufeld does not teach or suggest that a “bus controller is configured to ... convey the encrypted form of the management requests to the processor.” On the contrary, Neufeld teaches otherwise.

63. Specifically, Neufeld explains that “[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.” Ex. 1005, ¶¶ [0075]-[0076], FIG. 2. According to Neufeld’s FIG. 2, any commands received from the management network “M” are directed to the “remote management controller 116.” Id., FIG. 2. Similarly, commands received from the network “N” are routed through the NIC 110 and then delivered to the “remote management controller 116” via the PCI BUS 16. Id. For “lights out” management, the “security sign-on system,” which is “stored and operated on the remote management controller 116,” decrypts the

encrypted messages. As a result, the encrypted commands are not sent to the IOP 156 (the purported “processor,” see Pet. at 16) because the “remote management controller 116” itself is responsible for decrypting the messages. Neufeld does not indicate that the IOP 156 is configured to perform encryption or decryption operations.

64. Since Neufeld does not disclose a bus controller as discussed above regarding 1.e, Neufeld does not disclose the bus controller is configured to ... convey the encrypted form of the management requests to the processor via the first bus.

**5. 1.i. Neufeld Fails to Disclose “wherein the processor is configured to decrypt the encrypted form of the management requests”**

65. Petitioner states “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”. I disagree.

66. In my opinion, just because the IOP 156 is a processor does not imply 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.<sup>1</sup>

67. Independent claim 12 recites similar, although not identical elements, as independent claim 1, and Neufeld fails to teach at least independent claim elements 12.a, 12.d, and 12.g.

68. As a result, it is my opinion that Neufeld fails to inherently or expressly teach every element recited in the Challenged Claims as required for anticipation under 35 U.S.C. § 103.

## **VIII. OPINIONS REGARDING PETITION GROUND 2**

### **A. The Petition Fails to Prove That Claims 1-3, 6, 9, 12, and 17 are Obvious Over Neufeld In Combination With Frantz and PCI Bridge Spec**

69. The Petition fails to prove that Independent Claim 1 and Independent Claim 12 are Obvious over Neufeld In Combination With Frantz and PCI Bridge Spec for at least the following reasons.

### **B. Claim 1**

---

<sup>1</sup> Information Security Management: Global Challenges in the New Millennium, Gurpreet Dhillon, Idea Group Publishing., 2001, Page 133.

70. Neither Neufeld nor Frantz nor PCI Bridge Spec, either individually or in combination, discloses a bus controller as recited in claim 1.

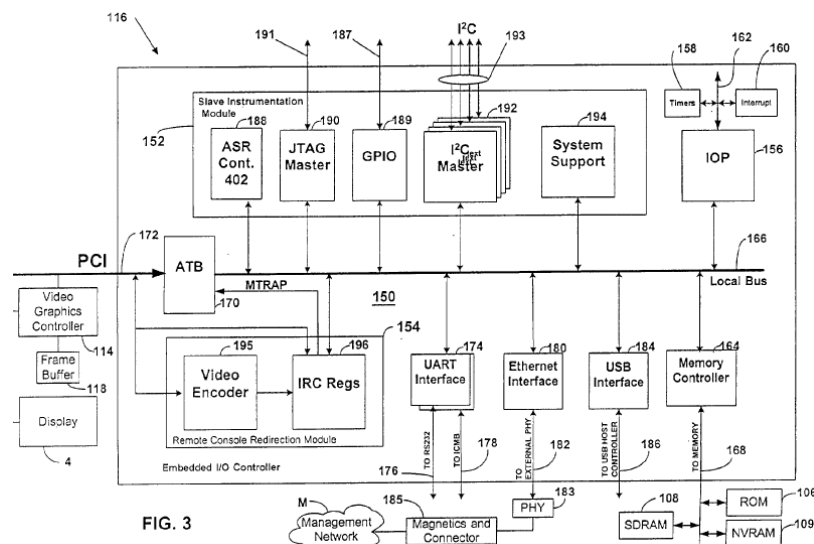
71. The Petitioner contends that a “POSITA would have recognized that the local bus 166 could have been implemented as a PCI bus because Neufeld states that the type of local bus 166 is a design choice that is not critical...” and that a POSITA would have looked to a reference such as PCI Bridge Spec 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.

72. I disagree. 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 (Ex. 1005 ¶[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.

73. Neufeld discloses that the ATB 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.” Hence, the bridge (ATB) of Neufeld is not a bus controller. A POSITA would understand a bus controller of managing or governing the flow of traffic on a single bus, determining

which device can access the bus and when it can access the bus. 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.

74. For example, a "PCI bus is an arbitrated bus: A central arbiter (part of the PCI bus controller in the motherboard chipset) governs all bus transfers, giving fair and controlled access to all the devices on the bus. Before a master can use the bus, it must first request control from the central arbiter, and then it is granted control for only a specified maximum number of cycles. This arbitration allows equal and fair access to all the bus master devices, prevents a single device from hogging the bus, and also prevents deadlocks because of simultaneous multiple device access". (see Chapter 4, page 342, "Scott Mueller's UPGRADING AND REPAIRING PCs", Scott Mueller, August 2003).



75. PCI Bridge Spec discloses a typical bridge application in Figure 1-1. A bridge has two PCI interfaces, the primary and secondary (Ex. 1008 page 12). Each interface is capable of both master and target operation (*Id.*). Two typical applications for a bridge are shown in Figure 1-1. The first application is the use of a bridge to create a second PCI bus segment to which additional PCI connector are added (*Id.*). The second application example is the use of a bridge to create a PCI bus segment on an expansion board that allows multiple PCI devices to reside on a single expansion board (*Id.*).

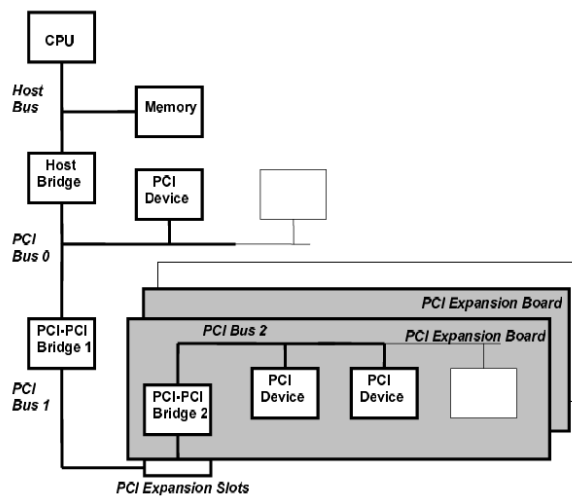


Figure 1-1: Typical Bridge Applications

76. A PCI-PCI Bridge as disclosed in PCI Bridge Spec is not a bus controller as recited in claim 1 and PCI Bridge Spec does not recite or disclose a “bus controller”. As discussed above, A POSITA would understand a bus controller of managing or governing the flow of traffic on a single bus, determining which

device can access the bus and when it can access the bus. 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.

**1. 1.e A combination of Neufeld, Frantz, and PCI Bridge Spec Fails to Disclose “a bus controller”**

77. The petition does not go into detail regarding claim element 1.e (bus controller) other than in VI. A. Introduction. As discussed above relating to VIII. A. 4 and 5, there is no motivation to combine Neufeld and PCI Bridge Spec and neither Neufeld, Frantz nor PCI Bridge Spec disclose, either individually or in combination, a bus controller coupled to the processor via the first bus.

78. As a result, it is my opinion that the combination of Neufeld, Frantz, and PCI Bridge Spec fails to inherently or expressly teach every element recited in the Challenged Claim 1 as required for anticipation under 35 U.S.C. § 103.

**2. 1.f A 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”**

79. Since neither Neufeld, Frantz nor PCI Bridge Spec discloses, either individually or on combination, a “bus controller” as discussed above regarding 1.e, the combination of Neufeld, Frantz nor PCI Bridge Spec does not disclose a bus

controller coupled to a second bus of the network device that is distinct from the first bus.

**3. 1.g A 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”**

80. Since neither Neufeld, Frantz nor PCI Bridge Spec discloses, either individually or on combination, a “bus controller” as discussed above regarding 1.e, the combination of Neufeld, Frantz nor PCI Bridge Spec does not disclose the bus controller is configured to receive the encrypted form of the management requests from the second bus.

**4. 1.h A combination of Neufeld, Frantz, and PCI Bridge Spec Fails to Disclose “to convey the encrypted form of the management requests to the processor via the first bus”**

81. Petitioner states that Neufeld teaches or at least suggests the encryption of management requests, citing statements in Neufeld that “security may be an important issue when remotely communicating management requests to the managed server” and that “any type of remote access would typically utilize encryption techniques.” Pet. at 20. Even if this assertion were accurate, Neufeld does not teach or suggest that a “bus controller is configured to ... convey the encrypted form of the management requests to the processor.” On the contrary, Neufeld teaches otherwise.

82. Specifically, Neufeld explains that “[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.” Ex. 1005, ¶¶ [0075]-[0076], FIG. 2. According to Neufeld’s FIG. 2, any commands received from the management network “M” are directed to the “remote management controller 116.” Id., FIG. 2. Similarly, commands received from the network “N” are routed through the NIC 110 and then delivered to the “remote management controller 116” via the PCI BUS 16. Id. For “lights out” management, the “security sign-on system,” which is “stored and operated on the remote management controller 116,” decrypts the encrypted messages. As a result, the encrypted commands are not sent to the IOP 156 (the purported “processor,” see Pet. at 16) because the “remote management controller 116” itself is responsible for decrypting the messages. Neufeld does not indicate that the IOP 156 is configured to perform encryption or decryption operations

83. Since neither Neufeld, Frantz nor PCI Bridge Spec discloses, either individually or on combination, a “bus controller” as discussed above regarding 1.e, the combination of Neufeld, Frantz nor PCI Bridge Spec does not disclose the bus controller is configured to ... convey the encrypted form of the management requests to the processor via the first bus.

### **C. Claim 12**

84. Claim 12 recites similar, although not identical, elements as claim 1, and it is my opinion that the combination of Neufeld, Frantz, and PCI Bridge Spec fails to inherently or expressly teach every element recited in Challenged Claim 12 as required for anticipation under 35 U.S.C. § 103, for at least the same reasons discussed above regarding claim 1.

## **IX. OPINIONS REGARDING PETITION GROUND 9**

### **A. The Petition Fails to Prove That Claims 1-3, 9, 12, 15 and 17 is Obvious Over IPMI In Combination With Frantz and Huckins**

85. The Petition fails to prove that Independent Claims 1 and 12 are Obvious over IPMI In Combination With Frantz and Huckins for at least the following reasons.

#### **B. Claim 1**

1. **1.b A combination of IPMI and Frantz fails to disclose “receive data requests and an encrypted form of management requests via the network interface”**

86. IPMI messages may be transmitted between the BMC and a remote management system (remote console) over an Ethernet LAN connection using UDP under IPv4 and the UDP datagrams are formatted to contain IPMI request and response messages. (Ex. 1023, 106). IPMI states that common IPMI messaging protocols do not use encrypted packets. (Ex. 1023, 108). Therefore, since IPMI does

not teach an encrypted form of management request, a POSITA would not look elsewhere and there is no motivation to combine IPMI and Frantz.

87. Petitioner agrees that the IMPI does not disclose encryption. Without hindsight, there is no reason that a POSITA would read IMPI and determine, as 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 is silent on the feature of encryption, there is no reason that a POSITA would look to Frantz to add the feature.<sup>2</sup>

**2. 1.e A combination of IPMI and Huckins fails to disclose “a bus controller coupled to the processor via the first bus”**

88. IPMI discloses a LAN controller connected to a BMC by a ‘side band’ connection (e.g. SMBus or I<sup>2</sup>C). (Ex. 1020, 106). The Petitioner 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. Additionally, SMBus or I<sup>2</sup>C were well known communication protocols to a POSITA, so a POSITA would not look elsewhere as to how to

---

<sup>2</sup> Information Security Management: Global Challenges in the New Millennium, Gurpreet Dhillon, Idea Group Publishing., 2001, Page 133.

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.

89. The LAN controller of IPMI is not related to the architecture taught in the '016 Patent with respect to the two distinct buses. A LAN controller manages connectivity to external networks, access points, 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.

90. Petitioner also discusses adding a PCI-I<sup>2</sup>C Bus Controller Bridge along with an Ethernet Interface and Side-band Logic to implement the LAN controller based on the disclosure of Huckins. I do not agree that this purported enhancement that would be understood by a POSITA. 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.

91. 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.<sup>3</sup>

**3. 1.f A combination of IPMI and Huckins fails to disclose “the bus controller is also coupled to the a second bus of the network device that is distinct from the first bus”**

92. Since IPMI in combination with Huckins does not disclose a bus controller, the combination of IPMI with Huckins does not disclose that the bus controller is also coupled to the a second bus.

**4. 1.g A 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”**

93. The Petitioner asserts that “IPMI discusses a secure secondary RMCP port (port 298h), which suggests to a POSITA sending encrypted IPMI management message packets.” Pet. at 59. Even if true, IPMI does not teach or suggest that the BMC (the alleged “processor”) is capable of or configured to perform encryption or decryption operations. Specifically, IPMI includes Table 3-1, which “summarizes the major required and optional functions for an IPMI-conformant BMC.” Ex. 1020 at 50-52. Notably, neither the required nor optional functions listed in Table 3-1 include any encryption or decryption capabilities.

---

<sup>3</sup> The Froehlich/Kent Encyclopedia of Telecommunications, Vol. 9, Editor in Chief: Fritz E. Froehlich, 1990

94. Table 3-1 describes the mandatory “IPM Device” function as requiring the BMC to “implement the mandatory IPM Device commands,” which, if an IPMB is present, “must be accessible from the IPMB.” Id. at 50. IPMI further specifies that “[a]ll management controllers are required to implement the mandatory IPM Device commands.” Id. at 53. Both the required and optional commands for Intelligent Platform Management (IPM) devices are detailed in Table 17-1, which discloses commands that all IPMI-conformant Management Controllers must recognize and respond to. Id. at 185-218. However, none of the commands listed—required or optional—pertain to encryption or decryption operations. See id.

95. Similarly, Table 18-1 outlines “the commands used to support the system messaging interface.” Id. at 219-249. Among these commands, the “Get Session Challenge Command,” the “Activate Session Command,” and the “Get AuthCode Command” involve authentication using hashing. For example, the “Get AuthCode” command is used to send data to the BMC, which then returns a hashed value. Id. at 239. IPMI explains this process as follows:

96. 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. While hashing is used for validation, it does not constitute encryption or decryption of commands.

97. Based on the mandatory and optional functions listed in Table 3-1, and the commands detailed in Tables 17-1 and 18-1, the BMC (the alleged “processor”) is neither designed nor configured to encrypt or decrypt received commands. Even if Frantz (Ex. 1006) discloses encryption of management messages and Huckins (Ex. 1007) describes a bus controller, this combination does not overcome the deficiency in IPMI—namely, that its BMC lacks encryption or decryption capabilities. Consequently, any encrypted messages received by IPMI’s LAN Controller would not be forwarded to the BMC (the alleged “processor”) for decryption.

98. Thus, IPMI, Frantz, and Huckins, individually or in combination, fail to 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 recited in claim 1.

99. Since IPMI in combination with Frantz does not disclose an encrypted form of management requests, as discussed above in relation to 1.b, a combination of IPMI, Frantz, and Huckins fails to disclose the bus controller is configured to receive the encrypted form of the management requests. Further, since IPMI in combination with Huckins does not disclose a bus controller as discussed above

regarding 1.e, the combination of IPMI with Huckins does not disclose that the bus controller is configured to receive the encrypted form of the management requests from the second bus.

**5. 1.h A combination of IPMI, Frantz, and Huckins fails to disclose “convey the encrypted form of the management requests to the processor via the first bus”**

100. The Petitioner asserts that “IPMI discusses a secure secondary RMCP port (port 298h), which suggests to a POSITA sending encrypted IPMI management message packets.” Pet. at 59. Even if true, IPMI does not teach or suggest that the BMC (the alleged “processor”) is capable of or configured to perform encryption or decryption operations. Specifically, IPMI includes Table 3-1, which “summarizes the major required and optional functions for an IPMI-conformant BMC.” Ex. 1020 at 50-52. Notably, neither the required nor optional functions listed in Table 3-1 include any encryption or decryption capabilities.

101. Table 3-1 describes the mandatory “IPM Device” function as requiring the BMC to “implement the mandatory IPM Device commands,” which, if an IPMB is present, “must be accessible from the IPMB.” Id. at 50. IPMI further specifies that “[a]ll management controllers are required to implement the mandatory IPM Device commands.” Id. at 53. Both the required and optional commands for Intelligent Platform Management (IPM) devices are detailed in Table 17-1, which discloses commands that all IPMI-conformant Management Controllers must recognize and

respond to. Id. at 185-218. However, none of the commands listed—required or optional—pertain to encryption or decryption operations. See id.

102. Similarly, Table 18-1 outlines “the commands used to support the system messaging interface.” Id. at 219-249. Among these commands, the “Get Session Challenge Command,” the “Activate Session Command,” and the “Get AuthCode Command” involve authentication using hashing. For example, the “Get AuthCode” command is used to send data to the BMC, which then returns a hashed value. Id. at 239. IPMI explains this process as follows:

103. 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. While hashing is used for validation, it does not constitute encryption or decryption of commands.

104. Based on the mandatory and optional functions listed in Table 3-1, and the commands detailed in Tables 17-1 and 18-1, the BMC (the alleged “processor”) is neither designed nor configured to encrypt or decrypt received commands. Even if Frantz (Ex. 1006) discloses encryption of management messages and Huckins (Ex. 1007) describes a bus controller, this combination does not overcome the deficiency

in IPMI—namely, that its BMC lacks encryption or decryption capabilities. Consequently, any encrypted messages received by IPMI’s LAN Controller would not be forwarded to the BMC (the alleged “processor”) for decryption.

105. Thus, IPMI, Frantz, and Huckins, individually or in combination, fail to 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 recited in claim 1.

106. Since IPMI in combination with Frantz does not disclose an encrypted form of management requests, as discussed above in relation to 1.b, a combination of IPMI, Frantz, and Huckins fails to disclose to convey the encrypted form of the management requests to the processor via the first bus. Further, since IPMI in combination with Huckins does not disclose a bus controller as discussed above regarding 1.e, the combination of IPMI with Frantz, and Huckins does not disclose that the bus controller is configured to ... convey the encrypted form of the management requests to the processor via the first bus.

107. As a result, it is my opinion that the combination of IPMI, Frantz, and Huckins fails to inherently or expressly teach every element recited in the Challenged Claim 1 as required for anticipation under 35 U.S.C. § 103.

### **C. Claim 12**

108. Claim 12 recites similar, although not identical, elements as claim 1, and it is my opinion that the combination of IPMI, Frantz, and Huckins fails to inherently or expressly teach every element recited in Challenged Claim 12 as required for anticipation under 35 U.S.C. § 103, for at least the same reasons discussed above regarding claim 1.

## **X. OPINIONS REGARDING PETITION GROUND 10**

### **A. The Petition Fails to Prove That Claims 1-3, 9, 12, 15 and 17 is Obvious Over IPMI In Combination With IPMI V2.0 and Huckins**

109. The Petition fails to prove that Independent Claims 1 are 12 are Obvious over IPMI In Combination With IPMI V2.0 and Huckins for at least the following reasons.

#### **1. 1.e A combination of IPMI, IPMI V2.0, and Huckins fails to disclose “a bus controller coupled to the processor via the first bus”**

110. IPMI discloses a LAN controller connected to a BMC by a ‘side band’ connection (e.g. SMBus or I<sup>2</sup>C). (Ex. 1020, 106). The Petitioner 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. Additionally, SMBus or I<sup>2</sup>C 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.

111. The LAN controller of IPMI is not related to the architecture taught in the '016 Patent with respect to the two distinct buses. A LAN controller manages connectivity to external networks, access points, 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.

112. Petitioner also discusses adding a PCI-I<sup>2</sup>C Bus Controller Bridge along with an Ethernet Interface and Side-band Logic to implement the LAN controller based on the disclosure of Huckins. I do not agree that this purported enhancement that would be understood by a POSITA. 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.

113. 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.<sup>4</sup>

114. IPMIV2.0 does not cure the deficiencies of IPMI and Huckins.

**2. 1.f A combination of IPMI, IPMI V2.0, and Huckins fails to disclose “the bus controller is also coupled to the a second bus of the network device that is distinct from the first bus”**

115. Since the combination of IPMI, IPMI V2.0, and Huckins does not discloses a bus controller, the combination does not disclose the bus controller is also coupled to the a second bus of the network device that is distinct from the first bus.

**3. 1.g A combination of IPMI, IPMI V2.0, and Huckins fails to disclose “the bus controller is configured to receive the encrypted form of the management requests from the second bus”**

116. Since the combination of IPMI, IPMI V2.0, and Huckins does not discloses a bus controller, the combination does not disclose the bus controller is

---

<sup>4</sup> The Froehlich/Kent Encyclopedia of Telecommunications, Vol. 9, Editor in Chief: Fritz E. Froehlich, 1990

configured to receive the encrypted form of the management requests from the second bus.

**4. 1.h A combination of IPMI, IPMI V2.0, and Huckins fails to disclose “convey the encrypted form of the management requests to the processor via the first bus”**

117. Since the combination of IPMI, IPMI V2.0, and Huckins does not disclose a bus controller, the combination does not disclose the bus controller is configured to ... convey the encrypted form of the management requests to the processor via the first bus.

**B. Claim 12**

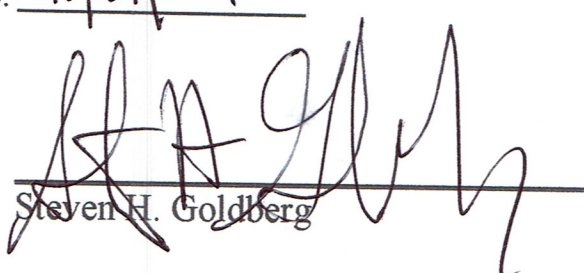
118. Claim 12 recites similar, although not identical, elements as claim 1, and it is my opinion that the combination of IPMI, IMPI V2.0, and Huckins fails to inherently or expressly teach every element recited in Challenged Claim 12 as required for anticipation under 35 U.S.C. § 103, for at least the same reasons discussed above regarding claim 1.

**XI. CONCLUSION**

119. For the reasons set forth in this Declaration, I believe claims 1-3, 6, 7, 12, and 17 of the '016 Patent are patentable over the prior art cited in the Petition.

120. I declare that all statements made herein of my knowledge are true, and that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Date: 11/21/24

By: 

Steven H. Goldberg