

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

LENOVO (UNITED STATES) INC.,
Petitioner

v.

INTELLECTUAL VENTURES II, LLC,
Patent Owner

IPR2024-00124
U.S. Patent No. 7,325,140 B2

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

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	Background and Qualifications	2
III.	MATERIALS USED	6
IV.	LEGAL FRAMEWORK	7
A.	Anticipation and Obviousness.....	7
B.	Level of a Person of Ordinary Skill in the Art	10
V.	THE '140 PATENT AND THE CHALLENGED CLAIMS	12
A.	Overview of '140 Patent	12
VI.	PRIOR ART RELIED ON IN THE PETITION	19
A.	Neufeld	19
B.	Intelligent Platform Management Interface Specification V1.5 (IPMI)	22
C.	Lawrence	25
a.	Challenged Claims of the '140 Patent	26
D.	Claim Construction.....	26
VII.	OPINIONS REGARDING PETITION GROUND 1	27
A.	Neufeld Fails to Teach Every Feature Recited in Challenged Claims 1-4, 6, 7, 10-14, and 16 as Required Under 35 U.S.C. §103	27
1.	1.c Neufeld Fails to Disclose “at least one virtual management interface connection means for connecting said one or more network services or remote users with said secure management access controller.”	28
VIII.	RESPONSE TO PETITION GROUND 5	32
IX.	RESPONSE TO PETITION GROUNDS 2-4, and 6-9	35
X.	CONCLUSION	36

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. 8,474,140 (the “’104 Patent”) and to provide my opinions as to the patentability of certain claims of the ‘140 Patent based on review of the prior art relied upon in the IPR. I understand that the patent application for the ‘140 Patent was filed on October 20, 2004 and ultimately claims priority to a U.S. patent application having a filing date of October 21, 2003. 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 ‘140 Patent says:

The present application is a continuation in part based on U.S. patent application Ser. No. 10/461,827, filed Jun. 13, 2003. The present application claims priority from U.S. Provisional Application Ser. No. 60/512,777, filed Oct. 21, 2003. The present invention is related to the invention described in co-owned, co-pending patent application Ser. No. 10/461,820 filed on Jun. 13, 2003, incorporated herein by reference.

My opinions are the same regardless of whether the provisional priority date is used (or the earlier date). I understand that the Challenged Claims are claims 1-4, 6, 7,

10-14, and 16 from the '140 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 '140 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 exhibits filed with the Petition including 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 7,325,140 (Ex 1004);
- U.S. Patent 7,325,140 File History
- Neufeld, U.S. Patent Application, 2003/0226015 A1
- Ex 2003 - Virtual private networks, Dennis Fowler, Morgan Kaufmann Publishers, Inc., 1999
- Ex 2004 –Virtual Private Networks, Charlie Scott, Paul Wolfe, Mike Erwin, O'Reilly, 1999, Page 8
- Ex 2005 - Networking Explained, Second Edition, Michael Gallo and William Hancock, Digital Press, 2002, Page 188.

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 '140 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 '140 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 '140 Patent. Specifically, by October 21, 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 '140 PATENT AND THE CHALLENGED CLAIMS

A. Overview of '140 Patent

30. The '140 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 '140 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. More specifically, distributed computer networks are networks in which at least some, and often most, network elements are located in different geographic locations. Ex. 1002, 1:27-31. In larger computer networks with a substantial number of network elements spread across a wide geographic area, maintaining the network and addressing routine troubleshooting tasks can become increasingly complex and challenging to perform securely. For instance, technicians responsible for network maintenance require regular and timely access to network elements that may be situated at significant distances from their physical location. Ex. 1002, 1:31-38.

33. While requiring technicians to physically access each network element offers the highest level of security, this approach is impractical in distributed networks due to the geographic separation between technicians and network elements. Ex. 1002, 1:39-41. The cost of dispatching technicians to physically access every network element in such systems would be prohibitively expensive and inefficient, resulting in significant delays in performing necessary maintenance tasks. Ex. 1002, 1:41-43. At a minimum, businesses implementing computer networks require those networks to be operational at all times, particularly during business hours, to enable employees to perform tasks efficiently and without disruption. Ex. 1002, 1:31-38. Consequently, businesses predominantly rely on some form of remote management.

34. 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).

35. In typical scenarios, when a network administrator accesses a network element using out-of-band communication, the administrator establishes a connection through a console or management port on the system. Ex. 1002, 1:52-55. Out-of-band communication is generally regarded as a more secure option compared to in-band communication. For this reason, as of the filing date of the application for the '140 Patent, out-of-band communication was widely considered the gold standard for remote network maintenance in situations where network administrators could not physically access all network elements to perform maintenance. Ex. 1002, 2:45-48.

36. By contrast, in-band remote maintenance methods rely, at least to some extent, on the security of the network within which the network element resides to safeguard management traffic. While this level of protection may provide reasonable

defenses against external attacks, it is generally insufficient to ensure an adequate level of security. Ex. 1002, 2:45-48.

37. The use of out-of-band communication for network maintenance, while offering enhanced security, presents certain drawbacks that must be considered. Most notably, implementing out-of-band communication for computer network maintenance necessitates the establishment of a dedicated network—or, at a minimum, dedicated network segments specifically allocated for remote network administration of routers. This requirement can result in significant costs, potentially rendering such an approach prohibitively expensive. Ex. 1002, 2:18-24.

38. The subject matter of the '140 Patent seeks to provide a secure system facilitating remote network maintenance by utilizing both in-band and out-of-band communication for network access. Ex. 1002, 6:5-13. Additionally, the network described in the '140 Patent, as recited at least in independent claim 1, implements a mechanism to separate management data from user data prior to transmitting management data over user interfaces via in-band communication. According to the specification of the '140 Patent, this separation enables the network to securely transmit management traffic over the in-band communication path. Ex. 1002, 12:6-13.

39. As illustrated in FIG. 1 of the '140 Patent (see reproduction below), the SMACC is positioned within a managed device in a distributed computer network.

The SMACC is communicatively connected to both the CPU Bus and the System Bus of the managed network device. The managed network device is further configured to facilitate communication through various user data interfaces via the System Bus, as depicted. Ex. 1002, FIG. 1.

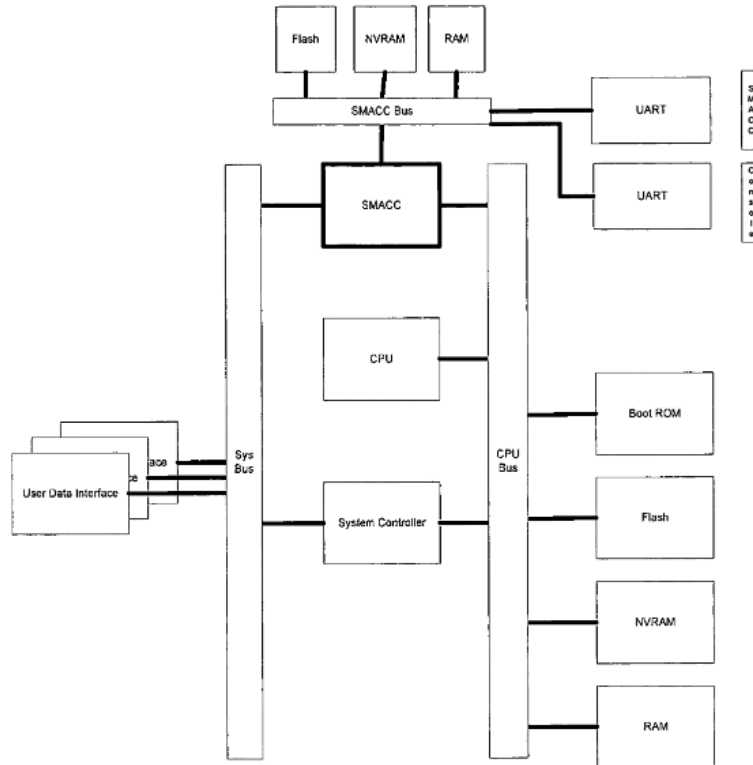


Fig. 1

40. The managed device is equipped with two distinct types of interfaces for transmitting management data to facilitate remote network maintenance: a VMI and a SMACC Network Enabled Management Interface. Ex. 1002, 11:60-63; FIG. 3. FIG. 3 of the '140 Patent illustrates these interfaces.

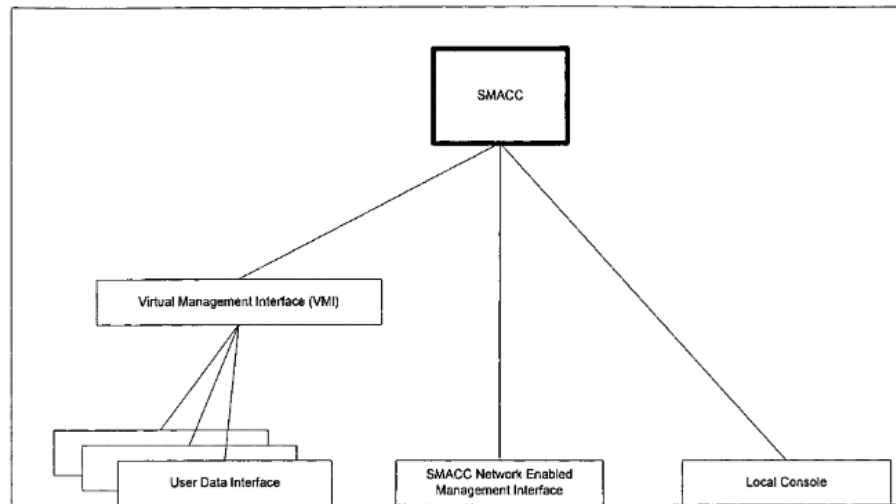


Fig. 3

41. As depicted in FIG. 3 of the '140 Patent, the VMI is positioned between the SMACC and the User Data Interfaces. The VMI is configured to "logically separate management traffic from user data traffic when a user interface on the managed device is going to be utilized for the network connection," effectively supporting in-band communication through a User Data Interface. Ex. 1002, 11:64-67. In contrast, the SMACC Network Enabled Management Interface provides "a physically separate interface for the management network connection rather than the user interfaces on the managed device," thereby enabling out-of-band communication via a dedicated network for management purposes. Ex. 1002, 12:1-4.

42. The VMI serves as an interface between the user data interfaces of a managed device and the SMACC. Ex. 1002, 6:25-26. When a user connects to the managed device to perform network maintenance, the VMI executes various

functions designed to enhance the security of management data when it is commingled with user data. The user data interfaces utilized for this connection are the same interfaces employed by users for performing non-maintenance functions within the managed network. See Ex. 1002, 6:26-31. Thus, these interfaces are used when a user connects to the managed device via in-band communication with the network. The Detailed Description of the '140 Patent outlines three primary functions of the VMI. Ex. 1002, 6:8-12, 12:6-33.

43. At a fundamental level, once a user accesses the managed network via in-band communication, the VMI facilitates the connection between the user and the SMACC. Within the managed device, the SMACC establishes a dedicated processor specifically configured to receive management information and interact with the device's control functions. All remote management functions are routed through this SMACC processor. Ex. 1002, 6:8-12.

44. The VMI is configured to logically separate management traffic from user data when the in-band communication path is utilized for transmitting management data. Ex. 1002, 6:22-24. Specifically, the VMI ensures the logical separation of management traffic from user data when both types of traffic share the same interfaces on the managed device and traverse the same physical network. In an exemplary embodiment of the invention, the VMI employs a Virtual Private Network (VPN) mechanism, such as IPSec, to encrypt, protect, and logically

separate the management traffic before it is transmitted through the user interface.

Ex. 1002, 12:6-13.

45. In the distributed computer network described in the '140 Patent, the user data interfaces facilitate in-band communication. As depicted in FIG. 3 of the '140 Patent (see above), the VMI is positioned between the SMACC and the user data interfaces of the managed device, serving as an intermediary.

46. The SMACC Network Enabled Management Interface facilitates out-of-band communication between a network administrator's device and a managed device hosting the VMI. According to the '140 Patent, "The SMACC Network Enabled Management Interface is dedicated for management traffic for management of the device." Ex. 1002, 12:24-25. As illustrated in FIG. 3, management data transmitted via the SMACC using out-of-band communication can pass directly through the SMACC without requiring logical separation from other types of data.

VI. PRIOR ART RELIED ON IN THE PETITION

A. Neufeld

47. As its primary reference, the Petition cites Neufeld, which discloses a remote management system depicted in FIG. 1 (reproduced below). The disclosed system comprises a remote management PC (5) in communication with a managed server (2) via two distinct networks: a management network (M) and a general-

purpose network (N). According to Neufeld, the management network (M) facilitates out-of-band communication between the remote management PC (5) and the managed server (2). The general-purpose network (N) is described as supporting in-band communication, such as video activity, between the managed server (2) and the remote management PC (5). However, the specific use of network (N) for in-band communication is not explicitly articulated in the reference. Ex. 1005, ¶¶ [0034], [0035], [0037].

48. As depicted in FIG. 1 of Neufeld, the managed server (2) includes a remote management controller (116). FIG. 2 of Neufeld (reproduced below) illustrates the placement of the remote management controller (116) within the CPU (3) of the managed server (2). Additionally, FIG. 3 of Neufeld (also reproduced below) provides a block diagram detailing the components of the remote management controller (116). According to Neufeld, the remote management controller (116) is integrated within the managed server (2) and is configured to facilitate communication with the remote management PC (5) for both in-band and out-of-band communication. Ex. 1005, ¶ [0043], FIG. 2, and FIG. 3.

49. As disclosed in FIG. 1 of Neufeld, the managed server (2) incorporates a remote management controller (116). FIG. 2 of Neufeld (reproduced below) further illustrates the positioning of the remote management controller (116) within the CPU (3) of the managed server (2). Moreover, FIG. 3 of Neufeld (also

reproduced below) presents a block diagram illustrating the components of the remote management controller (116). Neufeld describes the remote management controller (116) as being integrated within the managed server (2) to facilitate communication with the remote management PC (5), enabling both in-band and out-of-band communication. Ex. 1005, ¶ [0043], FIG. 2, and FIG. 3.

50. Tables 1, 2, and 3 collectively provide illustrative examples of various parameters related to network access, including IP Address/Connector types, times of access, authentication requirements, security settings, and access privileges that may be granted to or imposed upon an individual attempting to access a network. The examples of IP Address/Connector types include direct connection, in-house connection, remote direct, remote (Internet), and remote (VPN). Examples of access times include business hours (e.g., 8:00 AM to 5:00 PM) and after business hours (e.g., 5:00 PM to 8:00 AM). Authentication requirements include password-based authentication, smartcard, biometric authentication, or a combination of smartcard and biometric authentication. Security settings are exemplified as either encrypted or non-encrypted communication. Access privileges include full access, access to non-critical resources only, moderate access with non-critical resource limitations, or no access. Ex. 1005, Tables 1-3.

TABLE 2

<u>Network Administrator</u>					
User ID	IP Address/ Connector Type	Time of Day	Authentication	Security Settings	Privileges
1 Net-admin 1 (group:admin 1)	Direct	8 am–5 pm	Password	No encryption	Full
2 Net-admin 1 (group:admin 1)	In-house	8 am–5 pm	Smartcard	Encryption	Full
3 Net-admin 1 (group:admin 1)	Remote	8 am–5 pm	Biometric	Encryption	Moderate and non-critical only
4 Net-admin 1 (group:admin 1)	Direct	5 pm–8 am	Biometric	No encryption	Full
5 Net-admin 1 (group:admin 1)	In-house	5 pm–8 am	Biometric	Encryption	Moderate and non-critical only
6 Net-admin 1 (group:admin 1)	Remote	5 pm–8 am	Biometric	Encryption	Non-critical only

TABLE 3

<u>Administrative Assistant</u>					
User ID	IP Address/ Connector Type	Time of Day	Authentication	Security Settings	Privileges
1 Admin-asst 1 (group:admin 2)	Direct	8 am–5 pm	Password	No encryption	Full
2 Admin-asst 1 (group:admin 2)	In-house	8 am–5 pm	Smartcard	Encryption	Moderate and non-critical only
3 Admin-asst 1 (group:admin 2)	Remote	8 am–5 pm	Biometric	Encryption	Non-critical only
4 Admin-asst 1 (group:admin 2)	Direct	5 pm–8 am	Biometric	No encryption	Moderate and non-critical only
5 Admin-asst 1 (group:admin 2)	In-house	5 pm–8 am	Biometric	Encryption	Non-critical only
6 Admin-asst 1 (group:admin 2)	Remote	5 pm–8 am	Biometric	Encryption	Non-critical only

TABLE 4

<u>User</u>					
User ID	IP Address/ Connector Type	Time of Day	Authentication	Security Settings	Privileges
1 Joe-user (group:user 1)	Direct	8 am–5 pm	NA	NA	None
2 Joe-user (group:user 1)	In-house	8 am–5 pm	Password	Encryption	Non-critical
3 Joe-user (group:user 1)	Remote	8 am–5 pm	Smartcard/ Biometric	Encryption	Non-critical
4 Joe-user (group:user 1)	Direct	5 pm–8 am	NA	NA	None
5 Joe-user (group:user 1)	In-house	5 pm–8 am	Smartcard/ Biometric	Encryption	Non-critical
6 Joe-user (group:user 1)	Remote (Internet)	5 pm–8 am	NA	NA	None
7 Joe-user (group:user 1)	Remote (VPN)	5 pm–8 am	Smartcard/ Biometric	Encryption	Non-critical

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

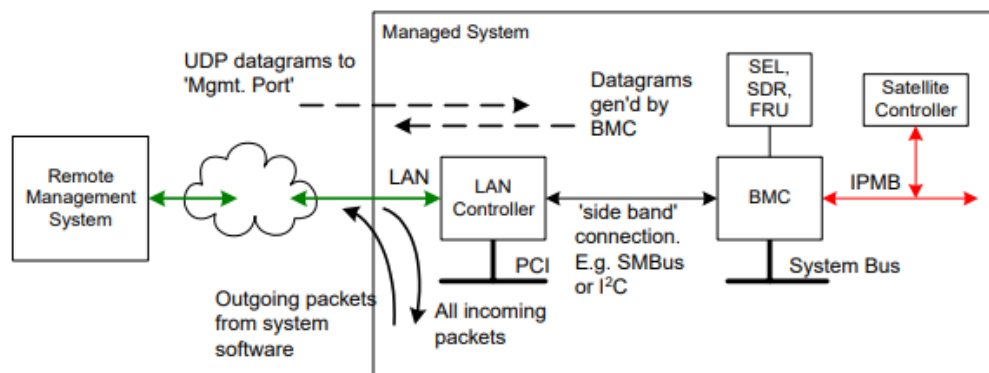
51. Intelligent Platform Management Interface (IPMI) is a standardized protocol originally developed by Intel, which enables remote management and monitoring of server systems. This capability extends even to scenarios where the primary operating system is non-operational or the system is powered off. IPMI achieves this functionality through the use of out-of-band communication mechanisms. Specifically, the protocol utilizes multiple dedicated management interfaces, including auxiliary Intelligent Platform Management Bus (IPMB) connectors for remote management card communication, an Intelligent Chassis Management Bus (ICMB) bridge, and a serial connector. These management interfaces are depicted in FIG. 1-2 of the IPMI documentation, as illustrated below. Although IPMI is primarily intended for out-of-band management, it also provides limited functionality for in-band communication.

52. The core component of the IPMI architecture is a microcontroller referred to as the Baseboard Management Controller (BMC). The BMC serves as the central processing unit for Intelligent Platform Management, providing the necessary functionality to bridge system management software with platform management hardware. Specifically, the BMC autonomously manages system monitoring, event logging, and recovery operations. It also acts as the gateway facilitating communication between the system management software and both the

Intelligent Platform Management Bus (IPMB) and the Intelligent Chassis Management Bus (ICMB). Ex. 1020, 9:1-6.

53. With respect to in-band communication, the BMC shares a network interface with the managed system's primary network traffic, as depicted in Figure 1-2 of the IPMI documentation. Additionally, Figure 12-1 of the IPMI documentation (reproduced below) provides a block diagram of this interface, which is referred to in IPMI as the "Embedded LAN Controller Implementation."

Figure 12-1, Embedded LAN Controller Implementation



54. The embedded LAN Controller Implementation facilitates the transfer of IPMI messages between the BMC and a remote management system, such as a remote console (indicated in gold), via an Ethernet LAN connection. These messages are transmitted using UDP under IPv4, with the UDP datagrams formatted to include IPMI request and response messages. Ex. 1020, 106:1-4.

55. The LAN controller is capable of detecting UDP datagrams directed to a designated "management port." Upon receipt, such datagrams are forwarded

through a "side-band" interface that enables delivery to or receipt by the BMC. Ex. 1020, 106:10-12. Furthermore, the BMC can utilize this same interface to inject datagrams onto the LAN. These datagrams are interleaved with network packets generated by the system software, enabling seamless communication between the BMC and the network. Ex. 1020, 106:14-15.

C. Lawrence

56. The disclosure of Lawrence is generally directed to routers configured for secure in-band management within packet data networks. Specifically, as illustrated in FIG. 7, Lawrence describes an in-band management configuration for a router (identified as router 602). The router 602 comprises two primary components (a) a generic routing and forwarding module (612), which is responsible for receiving data packets and performing fundamental routing and forwarding functions and (b) a router configuration management module (610), which processes management traffic to execute various management functions, such as adding or tearing down links, provisioning new customers, or configuring new router cards. Ex. 1043, 5:4-6, 15-16).

The router configuration includes an internal management VPN link that connects a management VPN module (655) to the router configuration management module. This connection allows management traffic to be internally routed from the management VPN module (655) to the router configuration management module via the internal management VPN link,

enabling secure and efficient in-band management operations. Ex. 1043, 5:42-47.

a. Challenged Claims of the '140 Patent

57. Petitioner challenges independent Claims 1 and dependent claims 2-4, 6, 7, 10-14, and 16.

Independent Claim 1 recites:

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

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

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

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

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

(Ex. 1004).

D. Claim Construction

58. 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.

VII. OPINIONS REGARDING PETITION GROUND 1

A. Neufeld Fails to Teach Every Feature Recited in Challenged Claims 1-4, 6, 7, 10-14, and 16 as Required Under 35 U.S.C. §103

59. Petitioner asserts in Ground 1 of the Petition that Neufeld renders obvious Challenged Claims 1-4, 6, 7, 10-14, and 16 of the '140 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) the Petitioner has failed to show that Neufeld discloses the "at least one virtual

management interface connection means for connecting said one or more network services or remote users with said secure management access controller.”

1. 1.c Neufeld Fails to Disclose “at least one virtual management interface connection means for connecting said one or more network services or remote users with said secure management access controller.”

60. It is first important to note that Neufeld, as cited from the abstract, is focused on a security system that “includes different authentication levels and/or different privileges based on certain criteria. For example, if a user's identity can be somewhat assured due to the directness of the connection, authentication may be less rigorous than in a situation where the connection is more remote, thus making the user's identity less assured. Also, a user's privileges may be restricted if the user accesses the system from a remote location or during non-business hours.”

61. Neufeld’s Claim 1 language supports this understanding.

A method of providing security in a computer system, the method comprising the acts of:

determining one of a plurality of different authentication levels for a user in response to at least one of connection type and time of connection; and

assigning one of a plurality of privilege sets to the user in response to at least one of connection type and time of connection.

62. Neufeld does focus on remote management, both in-band and out-of-band, but does so in the context of remote “authentication” that would provide

additional security related to the identification of system administrators and/or remote users. However, Neufeld does not disclose the concept of the separation of management data from user data.

63. Petitioner, when discussing the ‘140 Patent limitation 1.c, states that Neufeld discloses or renders obvious the limitation “at least one virtual management interface connection means for connecting said one or more network services or remote users with said secure management access controller.” I agree that Neufeld does disclose a VPN. However, Petitioner does not specifically discuss the ‘140 Patent limitation 1.d and how is discloses limitation 1.d as it relates to the simple disclosure of a VPN.

64. Limitation 1.d of the ‘140 Patent teaches “wherein said virtual management interface connection means provides *logical separation of management data from user data* and utilizes user interfaces of said managed network element for connecting said one or more network services or remote users with said secure management access controller.” (emphasis added). Petitioner argues that Neufeld’s disclosure of a VPN and/or the understanding of a POSITA discloses this limitation. I disagree.

65. The sections in the Neufeld specification where VPNs or virtual private networks are discussed are not at all in the context of separating management data from user data. Paragraph 9, in Neufeld, makes a general statement about client VPN

access. Paragraph 22 discusses using a virtual private network to access a system. Finally, in Paragraph 88 (related to Table 4), Neufeld discusses VPN's as an remote access method for a *user* (authorized or unauthorized).

66. In this same section of Neufeld, at Paragraph 91, Neufeld discloses “if a user is requesting virtual media storage.” In my opinion, this user request is related to user data and not management data tied to the function of a system administrator. It is further my opinion that Neufeld's sole reason for discussing VPN's is related to network access and the identification of the entity (system admin, admin assistant, or user) that is requesting the access. Neufeld does not envision, and certainly does not disclose, the use of a VPN to provide the “*logical separation of management data from user data.*”

67. Additionally, it is my opinion that a POSITA would not understand a VPN to inherently separate user data and management data. A VPN is “a logical local area network (LAN) that connects an organizations geographically dispersed sites in a way that makes them all appear to be part of one single network.”¹ Adding the concept of tunneling does not change my opinion with regard to Neufeld. Tunneling “simply allows you to encapsulate a packet within a packet to accommodate incompatible protocols”² VPN's use tunneling to provide an

¹ Virtual private networks, Dennis Fowler, Morgan Kaufmann Publishers, Inc., 1999

² Virtual Private Networks, Charlie Scott, Paul Wolfe, Mike Erwin, O'Reilly, 1999, Page 8

encrypted link that is safe and secure. Tunneling, combined with a VPN, also does not inherently separate user data and management data.

68. As a result, it is my opinion that Neufeld does not disclose limitation 1.d of the ‘140 Patent and therefore fails to inherently or expressly disclose or teach every element recited in the Challenged Claims as required for obviousness under 35 U.S.C. § 103.

69. Neufeld describes the use of a VPN in two distinct contexts:

1. **System Administrator Access:** Neufeld states that “[I]f the System administrator attempts to access the server from a remote terminal located outside of work, such as at home or while traveling ... the system administrator must typically use the Internet or a virtual private network to access the system.” (Ex. 1005, ¶ [0022]).
2. **User Access:** Table 4 depicts “Joe-user” accessing a managed server via a remote VPN. (Id., ¶¶ [0087]-[0088]).

70. In the first scenario, the VPN is established for the system administrator to access the system through their remote terminal. In the second scenario, the VPN is established for a user on their remote terminal.

71. The Petitioner argues that the VPN functionality could operate “via the in-band connection used for non-management user traffic (i.e., the NIC 110 and network N).” (Pet., p. 33). However, even if this were true, such a VPN would merely facilitate a connection between the system administrator or Joe-user and the NIC 110, not with the remote server management controller 116 (the purported

“secure management access controller”). Thus, even under the Petitioner’s assertion, Neufeld fails to disclose or suggest a VPN or a “virtual management interface connection means for connecting said one or more network services or remote users with said secure management access controller,” as required by claim 1.

72. Furthermore, Neufeld’s VPNs do not meet the claim requirement to “provide[] logical separation of management data from user data.” In both scenarios described by Neufeld, management and user data are intermingled, making logical separation unnecessary or inapplicable.

73. Thus, Neufeld fails to disclose or suggest all elements of claim 1.

VIII. RESPONSE TO PETITION GROUND 5

74. The Intelligent Platform Management Interface (IPMI) Version 1.5 prior art that Petitioner references is a set of industry specifications for managing and monitoring network hardware. It allows for network and system administrators to remotely control and monitor network hardware (e.g. servers) without being physically connected to them. The specifications are generally focused on out-of-band control to support situations where the network element under consideration is either in an “idle” and/or exhibiting a failure mode or not available through a standard in-band connection.

75. The IPMI Version 1.5 does not disclose encrypted communications channels nor does it disclose “how to implement the side-band interface for this in-band communication” (Petition page 52). Petitioner argues that a “POSITA would have recognized Lawrence’s Internal Management VPN Link as a desirable and convenient way to implement IPMI’ side-band interface.”. I disagree.

76. IPMI does not envision or disclose encrypted channels or VPN’s. Lawrence does not teach or disclose anything related to separation of management data and user data. Lawrence “discloses a method and system for providing in-band management.” (Petition Page 53). Petitioner argues that adding the Lawrence’s VPN would add a virtual management interface that would include “separation of management data and user data” to IMPI. There is nothing inherent in a VPN that separates management and user data. A VPN is simply an encrypted “tunnel” between two network devices that ensure that data is unreadable (i.e. encrypted) when viewed by unauthorized parties.

77. The LAN controller function in the IPMI prior art is a network element that manages data packet flow between devices. The LAN controller acts as a “traffic cop” in the sense that it inspects the address of each transmitted or received packet to appropriately determine its intended destination.³

³ Networking Explained, Second Edition, Michael Gallo and William Hancock, Digital Press, 2002, Page 188.

78. IPMI does not, and cannot, “provide[] logical separation of management data from user data,” as required by claim 1. The Petitioner asserts it would have been “obvious to include Lawrence’s VPN and tunneling technology in IPMI’s Network (LAN) Controller to implement IPMI’s side-band interface (corresponding to Lawrence’s Internal Management VPN link 711).” (Pet. at 64). However, this assertion is flawed. A person of ordinary skill in the art (POSITA) would not implement a VPN link over an already existing dedicated internal connection, such as IPMI’s “side band connection.” Lawrence supports this view. Specifically, Lawrence discloses two distinct types of embodiments:

1. ... **First Type:** Embodiments with “internal management connections” (311, 411) between the “routing and forwarding module” (312, 412) and “router configuration management module” (310, 410). In these embodiments, no VPN link is used over the internal management connections. (Ex. 1043, 2:24-27, 2:32-35, 2:44-47, Figs. 3, 4).
2. **Second Type:** Embodiments with a VPN link (711), but no “internal management connection.” (Id., 5:37-47, Fig. 7).

79. Given the “side band connection” between IPMI’s “LAN Controller” and the “BMC” (alleged “secure management access controller”), a POSITA would not implement a VPN link over this connection. Doing so would provide no additional security benefit and would result in unnecessary redundancy. Consequently, IPMI, whether considered individually or in combination with Lawrence, fails to disclose or suggest a VPN or a “virtual management interface

connection means for connecting said one or more network services or remote users with said secure management access controller,” as claim 1 requires.

80. Furthermore, even if Lawrence’s VPN modules (e.g., management VPN module 655) were considered as “provid[ing] logical separation of management data from user data,” these VPN modules cannot be incorporated into IPMI’s LAN Controller, contrary to the Petitioner’s assertion (Pet. at 64). Such a modification would compromise the functionality of IPMI’s LAN Controller. Specifically, the LAN Controller is designed to allow “incoming ‘platform management’ datagrams [to] be delivered to system software in parallel with being delivered to the BMC.” (Ex. 1020 at 128). A POSITA would recognize that such a combination would render the LAN Controller unworkable and would avoid making this modification.

81. Accordingly, IPMI, alone or in combination with Lawrence, fails to disclose or suggest a “virtual management interface connection means for connecting said one or more network services or remote users with said secure management access controller” and “provid[ing] logical separation of management data from user data,” as required by claim 1.

82. Without the benefit of hindsight, a POSITA would not look to Lawrence to enhance or improve IPMI.

IX. RESPONSE TO PETITION GROUNDS 2-4, and 6-9

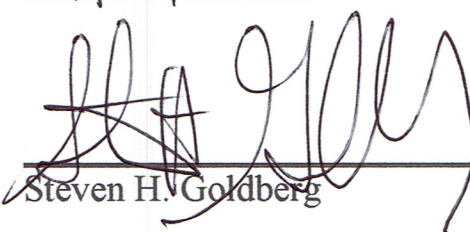
83. Ground 2-4 and 6-9 address claims dependent from Claim 1. It is my opinion that because Grounds based on either Neufeld/POSITA, or IMPI/Lawrence do not teach or disclose limitation 1.d of the '140 Patent, that the Petitioner's arguments as to the obviousness of the combinations of these other Grounds are not supported.

X. CONCLUSION

84. For the reasons set forth in this Declaration, I believe claims 1-4, 6, 7, 10-14, and 16 of the '140 Patent are patentable over the prior art cited in the Petition.

85. 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