

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

LENOVO (UNITED STATES) INC.,

Petitioner,

v.

INTELLECTUAL VETURES II, LLC,

Patent Owner

Case No. IPR2024-00124

U.S. Patent No. 7,325,140

PATENT OWNER'S PRELIMINARY RESPONSE

Table of Contents

PATENT OWNER’S EXHIBIT LIST	v
I. INTRODUCTION	1
II. SPECIFICATION OF '140 PATENT.....	2
A. Background.....	3
1. Maintenance and Trouble Shooting of Distributed Computer Networks 3	
2. Tradeoffs Between In-Band and Out-of-Band Approaches to Network Maintenance of Distributed Computer Networks	4
3. Problem Addressed By The ‘140 Patent	6
B. DETAILED DESCRIPTION	7
1. SMACC	7
2. Virtual Management Interface (VMI)	9
a) Connecting Remote Administrator with SMACC.....	10
b) Separating Management Data from User Data.....	10
c) In-Band Communication of Management Data (Using User Data Interfaces of Managed Device).....	11
3. SMACC Network Enabled Management Interface.....	11
III. PRIOR ART RELIED ON IN THE PETITION.....	12
A. Neufeld	13
B. Intelligent Platform Management Interface Specification V1.5 (IPMI)..	19
C. Lawrence.....	22
IV. THE PETITION FAILS TO DEMONSTRATE A REASONABLE LIKELIHOOD OF SUCCESS ON THE MERITS	23
A. Ground 1 – Claims 1-4, 6, 7, 10, 11, 13 and 16 Are Not Obvious Over Neufeld Pursuant To 35 U.S.C. § 103	23
1. Neufeld Does Not Disclose “At Least One Virtual Interface Connection Means [That] Provides Logical Separation Of Management Data From User Data,” As Required By Claim 1	24

2. The VPN Mentioned in Neufeld Does Not Obviously, or Inherently, Perform Separation of Management Data From User Data	29
a) Petitioner Has Not Established that It Would Have Been Obvious to Modify Neufeld to Arrive at the Claimed Invention	31
b) Separation Management Data from User Data is Not a Natural Result of the Technology (a VPN).....	33
c) Petitioner’s Conclusory Arguments, Backed Only by the Identical Conclusory Arguments of Petitioner’s Expert, Dr. Meldal, Should be Given Little, If Any, Weight.....	36
3. Neufeld’s VPN Implementations Fail to Disclose a “Virtual Management Interface Connection Means” or Logical Separation of Management and User Data.	40
4. Petitioner Has Failed To Meet Their Burden Of Showing The Challenged Claims Are Unpatentable Under Ground 1	41
B. Ground 2 – Dependent Claims 11 and 12 are Not Obvious over Neufeld and Syvanne	42
C. Ground 3 - Dependent Claim 14 is Not Obvious Over Neufeld and Fowler Pursuant To 35 U.S.C. § 103	42
D. Ground 4 - Dependent Claim 13 is Not Obvious Over Neufeld and Fowler Pursuant To 35 U.S.C. § 103	43
E. Ground 5 - Claims 1-3, 6, 7, 10 And 11 Are Not Obvious Over IPMI and Lawrence Pursuant To 35 U.S.C. § 103.....	43
1. The Claim Feature “At Least One Virtual Interface Connection Means [That] Provides Logical Separation Of Management Data From User Data” Would Not Be Obvious From IPMI And Lawrence	44
a) IPMI’s LAN Controller Does Not Separate Data, But Rather Detects Packets Addressed to the BMC	45
b) The VPN Of Lawrence Does Not Separate Management Data From User Data.....	46
c) Petitioner Has Not Established that It Would Have Been Obvious to Modify IPMI, With the Teachings of Lawrence, to Arrive at the Claimed Invention	48

d) A POSITA Would Not Be Motivated to Utilize A VPN On An Internal Connection Within a Server.	51
e) Petitioner Has Failed To Meet Their Burden Of Showing The Challenged Claims Are Unpatentable Under Ground 1	53
F. Ground 6 - Dependent Claim 4 is Not Obvious Over IPMI, Lawrence and Leedy Pursuant To 35 U.S.C. § 103	53
G. Ground 7 - Dependent Claims 11 And 12 Are Not Obvious Over IPMI, Lawrence And Syvanne Pursuant To 35 U.S.C. § 103.....	53
H. Ground 8 - Dependent Claims 13 and 14 Are Not Obvious Over IPMI, Lawrence and Fowler Pursuant To 35 U.S.C. § 103	54
I. Dependent Claim 16 is Not Obvious Over IPMI, Lawrence and RFC1492 Pursuant To 35 U.S.C. § 103.....	54
V. PETITIONER HAS NOT MET ITS BURDEN OF PROVING UNPATENTABILITY OF THE CHALLENGED CLAIMS	55
VI. CONCLUSION.....	56

PATENT OWNER'S EXHIBIT LIST

Ex. 2001	Declaration of Dr. Steven Goldberg
Ex. 2002	Resume of Dr. Steven Goldberg
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.

I. INTRODUCTION

Petitioner challenges claims 1-4, 6, 7, 10-14, and 16 (“Challenged Claims”) of the US 7,325,140 (“ ‘140 Patent”) on nine grounds. The ‘140 Patent has 16 total claims, with only claim 1 being independent. In ground 1, Petitioner challenges independent claim 1, and certain dependent claims, as allegedly obvious over US Patent Appln. Pub. No. 2003/0226015 to Neufeld et al. (hereinafter “Neufeld”). In ground 5, Petitioner challenges independent claim 1, and certain dependent claims, as allegedly obvious over Intelligent Platform Management Interface Specification V 1.5 (hereinafter, “IPMI”) and US Patent No. 7,269,639 to Lawrence (hereinafter “Lawrence”). The remainder of the grounds address dependent claims only. Dependent claims 5, 8, 9, and 15 are not challenged.

In Ground 1, Petitioner asserts that claim 1 is obvious over Neufeld, a single reference, and asserts that the differences between Claim 1 and Neufeld are mere “implementation details” that were allegedly very well-known at the time the application for the ‘140 Patent was filed. Pet, page 32-33. And yet, conspicuously missing from the Petition is any evidence of this. Petitioner cites the declaration of Dr. Meldal (Ex.1003) as “evidence.” Yet, Dr. Meldal’s declaration merely makes conclusory statements that this concept was well-known, and those conclusory statements are substantively identical to the conclusory statements made in the

Petition itself. These alleged “implementation details” are actually at the heart of ‘140 Patent, which is largely about separating management data from user data when an in-band connection is used, and Petitioner has not found any documents whatsoever that disclose, or even suggest, at least this feature of independent claim 1.

In Ground 5, Petitioner alleges that Claim 1 is obvious over IPMI, a technical specification, in view of Lawrence, an issued US Patent. In its argument, the Petition alleges that a LAN controller, which is used in the technical specification to control access to a side-band connection/system bus, is actually separating management data from user data and that a POSITA would have looked to Lawrence for implementation details. Pet., page 55. This is a complete mischaracterization of the reference. (see Ex. 2001, ¶¶76-77). The only place separation of management data from user data is mentioned in any art mentioned in the Petition is in the specification of the ‘140 Patent itself.

Petitioner’s entire argument is smoke and mirrors on all nine grounds. But the magician is hiding in plain sight.

II. SPECIFICATION OF '140 PATENT

The invention claimed in the ‘140 Patent addresses the technical problem of securely managing network devices remotely without compromising the security of the devices. The invention solves this problem by providing a controller (referred to

in the specification as a Secure Management Access Control for Computer Chipset (SMACC) that provides additional security for a user connected to the managed device using the in-band network. Ex. 1002, Abstract: 1-9. While the SMACC can also facilitate out-of-band communication, at the heart of the ‘140 Patent is a Virtual Management Interface (VMI), which separates management data from user data when the user is connected to the managed device using the in-band network. Ex. Ex. 1002, Abstract: 6:5-8, 22-24. The SMACC can pass user data through without any separation of the data. Ex. 1002, 7:58-63. These concepts are described in more detail below.

A. Background

1. Maintenance and Trouble Shooting of Distributed Computer Networks

Distributed computer networks are computer networks in which at least some, and usually most, of the network elements are not in the same geographic location. Ex. 1002, 1:27-31. For larger computer networks that include a large number of network elements distributed over a wide geographic area, network maintenance and/or everyday troubleshooting (collectively referred to hereafter as “network maintenance”) can become complex and difficult to implement in a secure manner. Technicians performing network maintenance, for example, need both regular and timely access to the network elements that can be geographically quite far away from the technician. Ex. 1002, 1:31-38; Ex. 2001, par. 32.

While arguably the most secure option for network maintenance is to require technicians to physically access any network element they work on, the distance between the technician and network elements also makes this the least practicable approach. Ex. 1002, 1:39-41. It would, for example, be prohibitively expensive to dispatch a technician to physically access every network element in a distributed system and would, in any event, take too much time to perform the required maintenance function. Ex. 1002, 1:41-43. At a minimum, computer networks implemented by businesses need to be operable at all times to enable employees, who generally work only during designated daytime hours, to be able to perform work tasks in a timely manner. Ex. 1002, 1:31-38. Accordingly, businesses overwhelmingly use at least some form of remote management to maintain and troubleshoot network elements and servers. Ex. 1002, 1:43-45; Ex. 2001, par. 33.

2. Tradeoffs Between In-Band and Out-of-Band Approaches to Network Maintenance of Distributed Computer Networks

Two general approaches to remote network management are in-band network access and out-of-band network access. Ex. 1002, 1:45-52. In-band network access is, generally speaking, a type of network access in which a remote administrator “communicates with the system using the same network as the network data for the managed system.” Out-of-band network access, on the other hand, is, generally speaking, a type of network access in which a remote administrator “communicates

with the system using a means other than the network utilized by the user data of the managed system.” Ex. 1002, 1:47-52.

Typically, when a network administrator accesses a network element using out-of-band communication, the administrator connects to a console or management port on the system. Ex. 1002, 1:52-55. This makes out-of-band communication a generally more secure option than in-band communication. For this reason, at least at the time the application for the ‘140 Patent was filed, out-of-band communication was considered the gold standard for remote network maintenance when it was not possible for network administrators to physically connect to all network elements to perform maintenance. Ex. 1002, 2:45-48. Relatedly, at least to some degree, in-band remote maintenance methods depend on the security of the network in which a network element being maintained resides to protect management traffic. While this is considered to potentially be a reasonable level of protection from external attacks, “it generally will not provide a sufficient level of protection from internal attacks (initiated from inside a network).” Ex. 1002, 2:12-14; Ex. 2001, pars. 34-36.

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

administration of routers”), which can be prohibitively expensive. Ex. 1002, 2:18-24; Ex. 2001, par. 37.

3. Problem Addressed By The ‘140 Patent

Because there are drawbacks to both in-band and out-of-band communication for network maintenance in distributed computer networks, distributed computer networks may use a combination of both in-band and out-of-band communication for network maintenance. However, in solutions where in-band communication is used, either as one option for network maintenance or as the only option, there is a problem with in-band communication that should be addressed, and that is addressed by the solutions described throughout the ‘140 Patent. That is: “[T]o control cost of most management solutions, user traffic, and management traffic are being comingled at multiple locations throughout the management path.” Ex. 1002, 3:11-

23

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. *Id.*

The subject matter of the ‘140 Patent, therefore, sets out to provide a secure system that enables remote network maintenance using both in-band and out-of-band communication for network access. Ex. 1002, 6:5-13. Moreover, the network

described in the ‘140 Patent, and recited at least in independent claim 1, separates management data from user data, before transmitting any management data over the user interfaces via in-band communication, which may, as described in the specification of the ‘140 Patent, enable the network to ensure that management traffic is securely sent over the in-band path. Ex. 1002, 12:6-13; Ex. 2001, par. 38.

B. DETAILED DESCRIPTION

The Detailed Description of the ‘140 Patent specification describes a computer network, which can be used to remotely manage a network element. More specifically, the Detailed Description of the ‘140 Patent describes “a Secure Management Access Control for Computer Chipset (SMACC) for inclusion in devices that are to be enabled for remote management.” Ex. 1002, 5:50-52.

1. SMACC

FIG. 1 of the ‘140 Patent (reproduced below) illustrates a managed device, which is part of a distributed computer network (also referred to as a managed network). It should be noted that the invention of the ‘140 Patent is not limited to the layout shown in FIG. 1 and, for example, FIG. 14 also shows another possible layout. FIG. 1 is referred to here for purposes of explanation only.

As can be seen in FIG. 1, the SMACC [red highlighting] is located within a managed device in a distributed computer network. The SMACC is communicatively coupled both to the CPU Bus and the System Bus [green

highlighting] of the managed network device. The managed network device is configured for communication via various user data interfaces [blue highlighting] via the System Bus, as shown. Ex. 1002, FIG. 1; Ex 2001, par. 39.

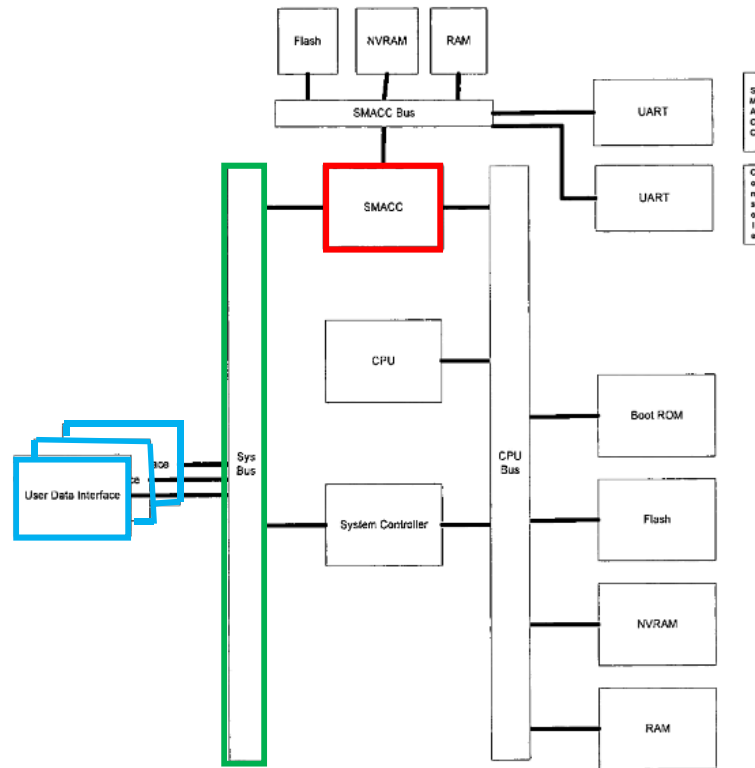


Fig. 1

The managed device is configured with two types of interfaces for communicating management data for purposes of remote network maintenance, namely, a VMI and a SMACC Network Enabled Management Interface. Ex. 1002, 11:60-63; FIG. 3. FIG. 3 of the '140 Patent (reproduced below) illustrates these interfaces; Ex. 2001, par. 40.

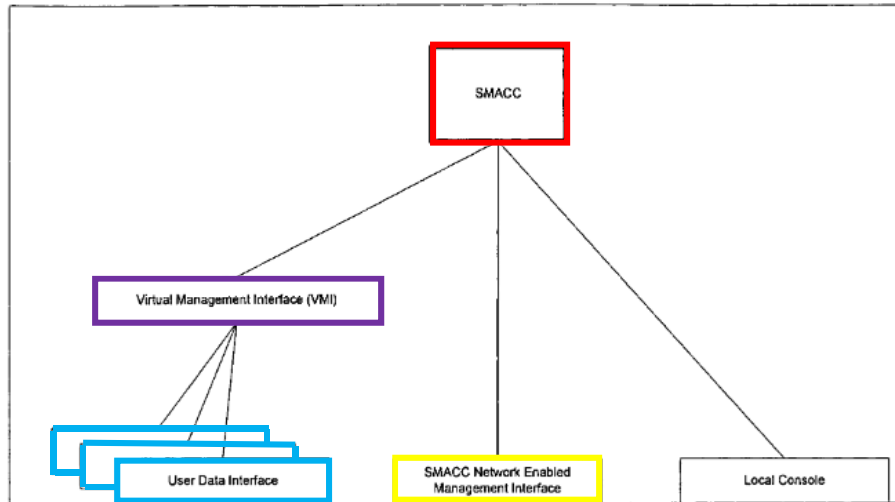


Fig. 3

As shown in FIG. 3, the VMI [purple highlighting] is located between the SMACC [red highlighting] and the User Data Interfaces [blue highlighting]. The VMI “logically separates management traffic from user data traffic when a user interface on the managed device is going to be utilized for the network connection,” (or, in other words, for in-band communication using a User Data Interface). Ex. 1002, 11:64-67. The SMACC Network Enabled Management Interface [yellow highlighting] “provides a physically separate interface for the management network connection rather than the user interfaces on the managed device,” (or, in other words, for out-of-band communication using a dedicated network for that purpose). Ex. 1002, 12:1-4; Ex. 2001, par. 41.

2. Virtual Management Interface (VMI)

The VMI is an interface between the user data interfaces of a managed device and the SMACC. Ex. 1002, 6:25-26. As such, if a user connects to the managed

device to perform network maintenance, the VMI performs a number of functions to better secure the management data when it is commingled with other user data. Such user data interfaces are the same user data interfaces the user uses to connect to the managed network to perform functions other than other network maintenance functions. Ex. 1002, 6:26-31. In other words, the user data interfaces are used when the user connects to a managed device using an in-band communication with the network. The Detailed Description of the '140 Patent describes three primary functions of the VMI. Ex. 1002, 6:8-12, 12:6-33.

a) Connecting Remote Administrator with SMACC

On the most basic level, once a user is logged in to the managed network using in-band communication, the VMI connects the user with the SMACC. “Within the device, the SMACC sets up a separate processor for receiving management information and interacting with the control functions of the device. Remote management functions will pass through the SMACC processor.” Ex. 1002, 6:8-12.

b) Separating Management Data from User Data

“A VMI is also established for logically separating management traffic from user data when the in-band path is to be used for management data.” Ex. 1002, 6:22-24. “The [VMI] logically separates management traffic from user data when they are going to utilize the same interfaces on the managed device and the same physical network. In an exemplary embodiment of the current invention, the VMI will utilize

a Virtual Private Network (VPN) mechanism, such as IPSec to encrypt, protect and logically separate the management traffic before the traffic is passed to the user interface.” Ex. 1002, 12:6-13.

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

In a distributed computer network, as described in the ‘140 Patent, the user data interfaces are used for in-band communication. As shown in FIG. 3 of the ‘140 Patent (reproduced above), the VMI is located between the SMACC and the User Data Interfaces of the managed device. Ex. 2001, par. 45.

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

Ex. 1002, 12:25-33.

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

Ex. 1002, 12:13-21.

3. SMACC Network Enabled Management Interface

The SMACC Network Enabled Management Interface may be used for out-of-band communication between a device controlled by a network administrator and a managed device on which the VMI resides. “The SMACC Network Enabled Management Interface is dedicated for management traffic for management of the device.” Ex. 1002, 12:24-25. Accordingly, as shown in FIG. 3, for example, any management data communicated via the SMACC via out-of-band communication can pass directly through the SMACC, without any logical separation of the data. Ex. 2001, par. 46.

The SMACC interface is a network enabled interface and therefore is able to support the full range of protocols that are typically utilized for management of a device such as SNMP, Trivial File Transfer Protocol (TFTP), File Transfer Protocol (FTP), DNS, SysLog, Telnet, Secure Shell (SSH), or HTTP. The SMACC interface will also control access to the management functions of the device and protect the management traffic in transit through the utilization of VPN technology such as IPsec. The SMACC interface can be utilized to connect to a central location that provides for these network services as well as for remote administrator access.

Ex. 1002, 12:26-36.

III. PRIOR ART RELIED ON IN THE PETITION

The Petition advances two grounds against independent Claim 1 of the ‘410 Patent. In Count 1, the Petition offers only a single reference, Neufeld, in support of its assertion that Claim 1 of the ‘140 Patent is obvious under 35 U.S.C. § 103. In Count 5, the Petition asserts that Claim 1 of the ‘140 Patent is obvious over IPMI in combination with Lawrence.

A. Neufeld

As its primary reference, the Petition relies on Neufeld. Neufeld describes a remote management system as shown in FIG. 1 (reproduced below). The remote management system includes a remote management PC 5 communicatively coupled to a managed server 2 via a network N and a management network M. The management network M may be used for out-of-band communications between the remote management PC 5 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. Ex. 1005, ¶ [0034], [0035], [0037]. Ex. 2001, ¶ 47.

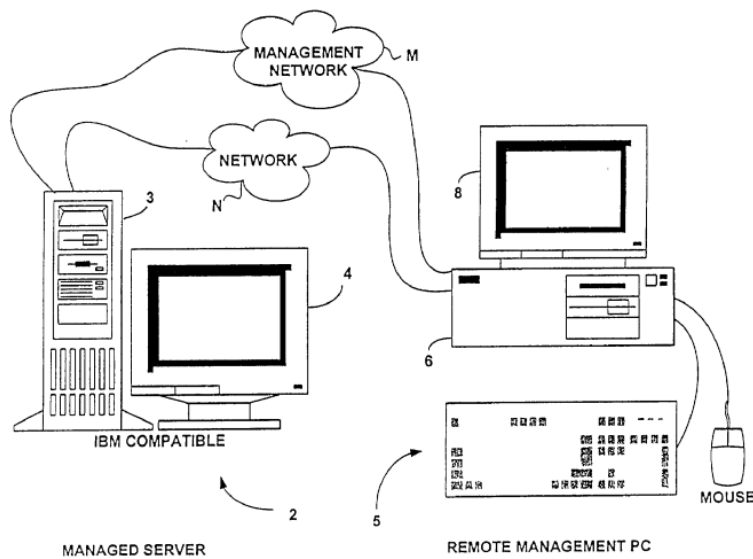


FIG. 1

The managed server 2, illustrated in FIG. 1, contains a remote management controller 116. FIG. 2 of Neufeld (reproduced below) shows the location of the remote management controller 116 within the CPU 3 of the managed server 2. FIG. 3 of Neufeld (also reproduced below) is a block diagram showing components of the remote management controller 116. The remote management controller 116, in Neufeld, resides in the managed server 2 and facilitates communication with the remote management PC 5 for purposes of both in-band and out-of-band communication. Ex. 1005, ¶ [0043], FIG. 2, and FIG. 3. Ex. 2001, ¶48.

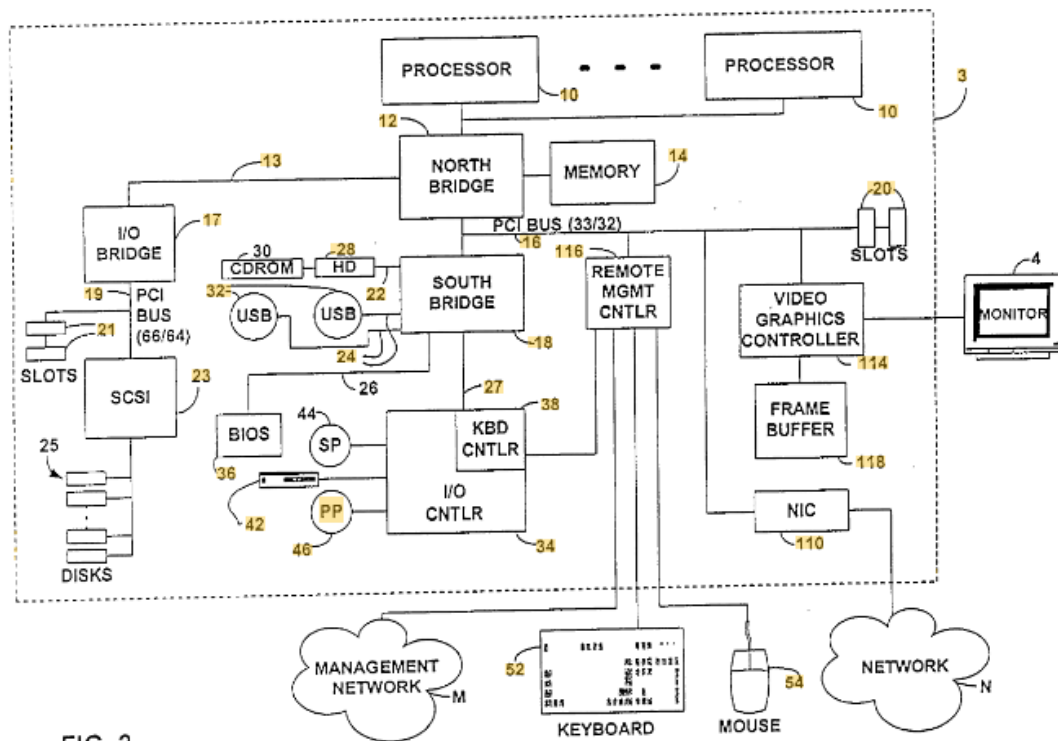


FIG. 2

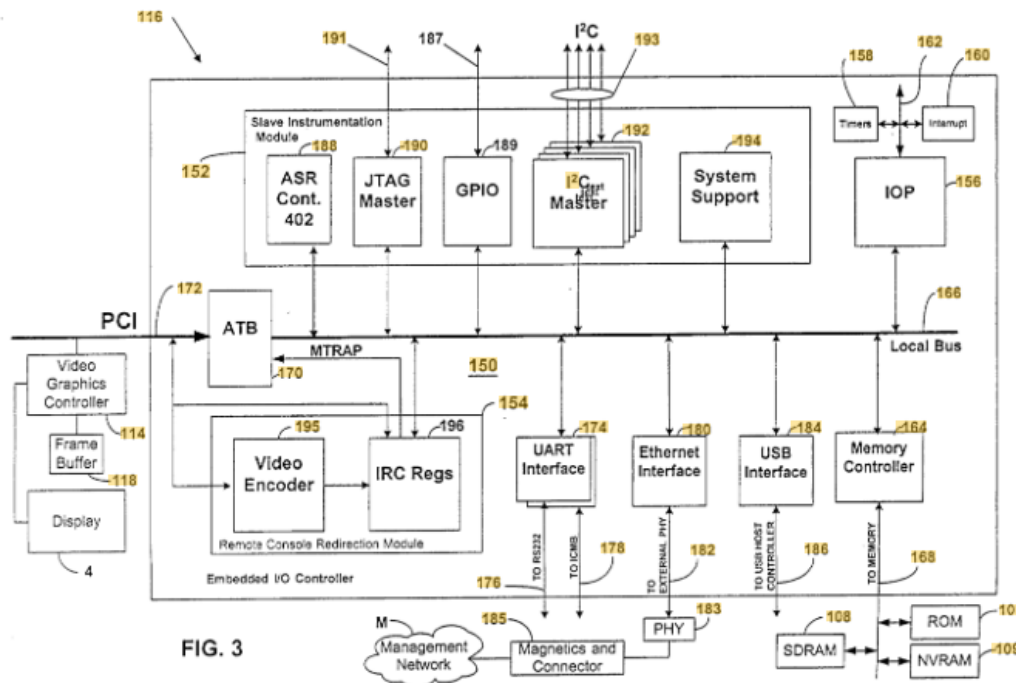


FIG. 3

In terms of in-band communication, the remote management controller 116 is attached to the PCI bus 16. Ex. 1005, ¶ [0043]. “Further attached to the PCI bus 16 is a video graphics controller 114 and one or more communications devices, such as a network interface controller (“NIC”) 110.” Ex. 1005, ¶ [0045]. “The managed server 2 includes special circuitry and software for capturing, analyzing, compressing and transmitting video activity to the remote console 5 independent of an operating system (“OS”).” Ex. 1005, ¶ [0034]. Such information may be transmitted over the network N to the remote management PC 5 via the network interface card (NIC) 110. Since this function of the remote management controller 116 is independent of the OS, this form of in-band communication can be performed

whether the OS is operational or not, and can even be used for system setup before the OS is up and running. Ex. 2001, ¶ 41.

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

Ex. 1005, ¶ [0048].

Another mode of in-band communication described in Neufeld is a so-called “lights out” mode. Ex. 1005, ¶ [0076]. In this mode, users may be granted network privileges, and/or subject to certain authentication requirements and security settings, depending on the time of day the user attempts to access the network, the location and IP address from which the user attempts to access the network, and/or the connection type the user attempts to use to access the network.

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

Ex. 1005, ¶ [0084].

Tables 1, 2, and 3 collectively provide examples of IP Address/Connector Types, times of day, authentication requirements, security settings, and privileges that can be granted to and/or imposed on a person attempting to access a network. Examples of IP Address/Connector types include direct connection, in-house connection, remote direct, remote (Internet), or remote (VPN). Examples of times of day include business hours (8 am to 5 pm) or after business hours (5 pm to 8 am). Examples of authentication requirements include password, smartcard, biometric, or smartcard/biometric. Examples of security settings include encryption or no encryption. Examples of privileges include full, non-critical only, non-critical, moderate and non-critical only, or none. Ex. 1005, Tables 1-3; Ex. 2001, ¶ 50.

TABLE 2

User ID	IP Address/ Connector Type	Network Administrator			
		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

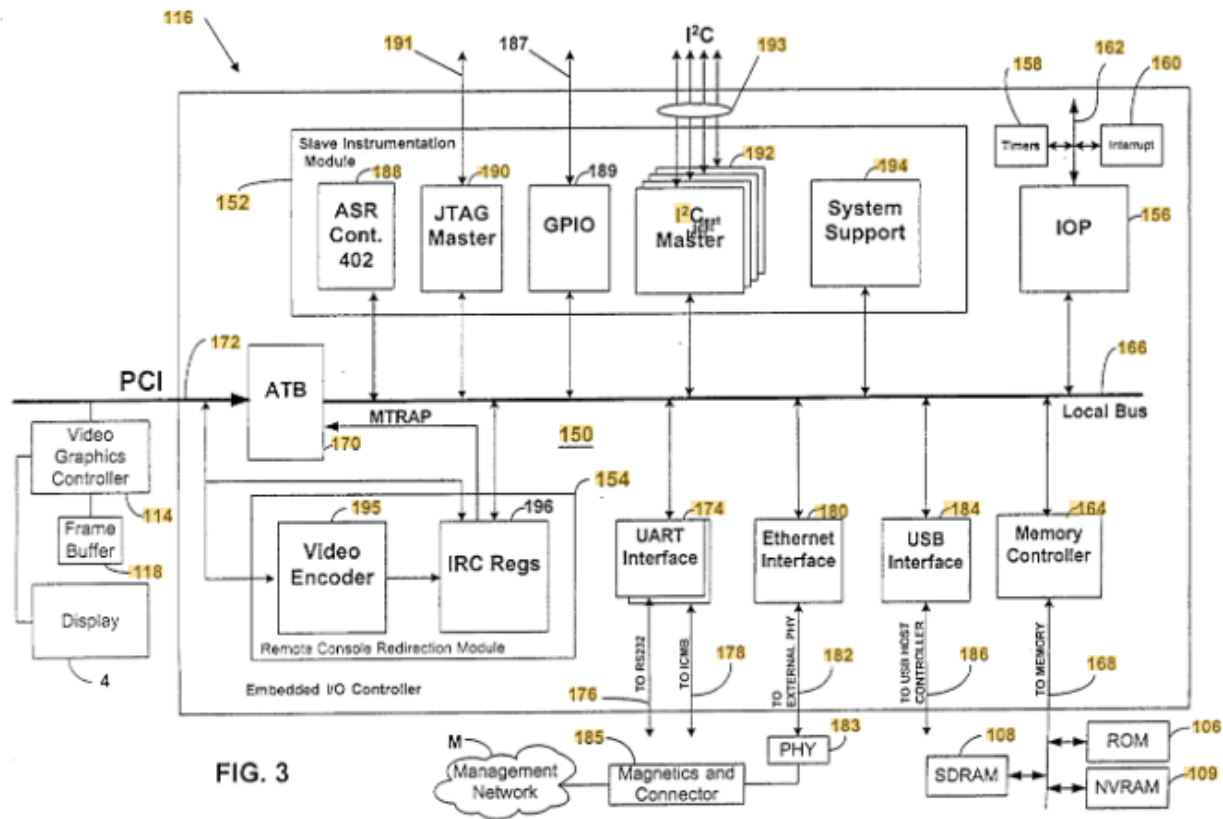
TABLE 4

User ID	IP Address/ Connector Type	Time of Day	<u>User</u>		
			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

In terms of out-of-band communication, the remote management controller 116 contains an embedded I/O controller 150. “The embedded I/O controller 150 provides a plurality of communication interfaces that can be employed to establish out-of-band communication sessions with the remote server management controller 116.” Ex. 1005, ¶ [0059]. The out-of-band communication interfaces of the embedded I/O controller 150 include UART interface module 174, Ethernet interface 180, and USB interface 184. Ex. 1005, ¶ [0059], [0061], [0063]. Relative, more specifically, to out-of-band communications of remote management functions, Neufeld states:

Those skilled in the art will appreciate that a user may connect remotely to the remote server management controller 116 via the Ethernet interface 180. Such a connection may be made, for example, using a remote console application running on a client computer anywhere on the network that includes managed server 2. The user may, thus, engage in out-of-band communication with the remote server management controller 116 for the purpose of diagnosing, correcting and/or preventing problems with the managed server 2.

Ex. 1005, ¶ [0062].

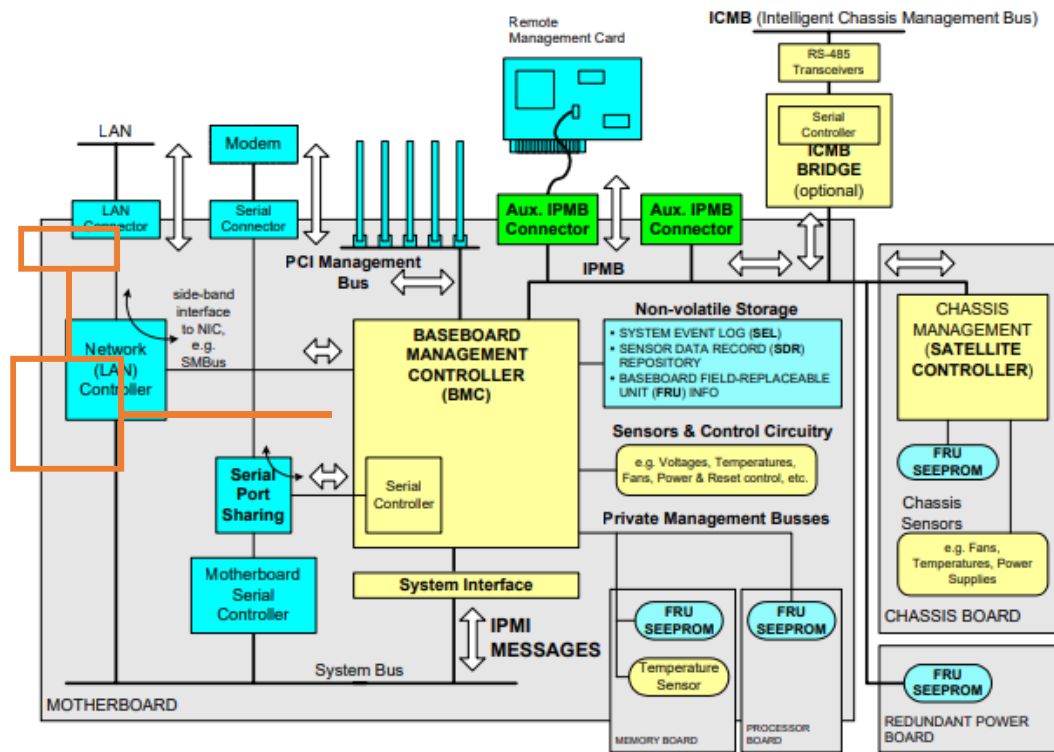


B. Intelligent Platform Management Interface Specification V1.5 (IPMI)

IPMI is a standardized protocol developed by Intel that is used to remotely manage and monitor servers, even when the main OS is down or the system is powered off. To accomplish this, IPMI primarily leverages out-of-band communication, providing several different dedicated management ports, including several auxiliary IPMB connectors for communications via remote management cards, an Intelligent Chassis Management Bus (ICMB) bridge, and a serial connector. These management ports can be seen in FIG. 1-2 of IPMI (reproduced below). While

IPMI is primarily designed for out-of-band management, there is a form of in-band communication available. Ex. 2001, 51.

Figure 1-2, IPMI Block Diagram



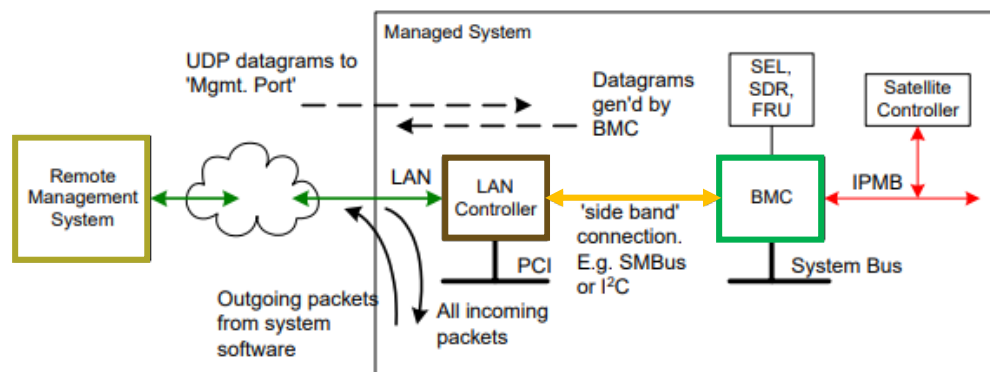
“At the heart of the IPMI architecture is a microcontroller called the *Baseboard Management Controller* or, BMC.”

The BMC provides the intelligence behind Intelligent Platform Management. The BMC manages the interface between system management software and the platform management hardware, provides autonomous monitoring, event logging, and recovery control, and serves as the gateway between system management software and the IPMB and the ICMB.

Ex. 1020, 9:1-6.

In terms of in-band-communication, as can be seen from Figure 1-2 of IPMI, the BMC shares a network interface with the managed system's network traffic. The communication path for such in-band-communication is highlighted in orange in FIG. 1-2 above. FIG. 12-1 of IPMI (reproduced below) is a block diagram of this interface (referred to in IPMI as the embedded LAN Controller Implementation). Ex. 2001, ¶ 53.

Figure 12-1, Embedded LAN Controller Implementation



Using the embedded LAN Controller Implementation, IPMI messages may be transferred “between the BMC [green highlighting] and a remote management system (remote console) [gold highlighting] over an Ethernet LAN connection using UDP under Ipv4. The UDP datagrams are formatted to contain IPMI request and response messages....” Ex. 1020, 106:1-4. The LAN controller [brown highlighting] “has the ability to detect UDP datagrams sent to a ‘management port.’ Any datagrams received on that port are forwarded on a ‘side-band’ interface [orange highlighting] that allows them to be delivered to, or received by, the BMC.” Ex.

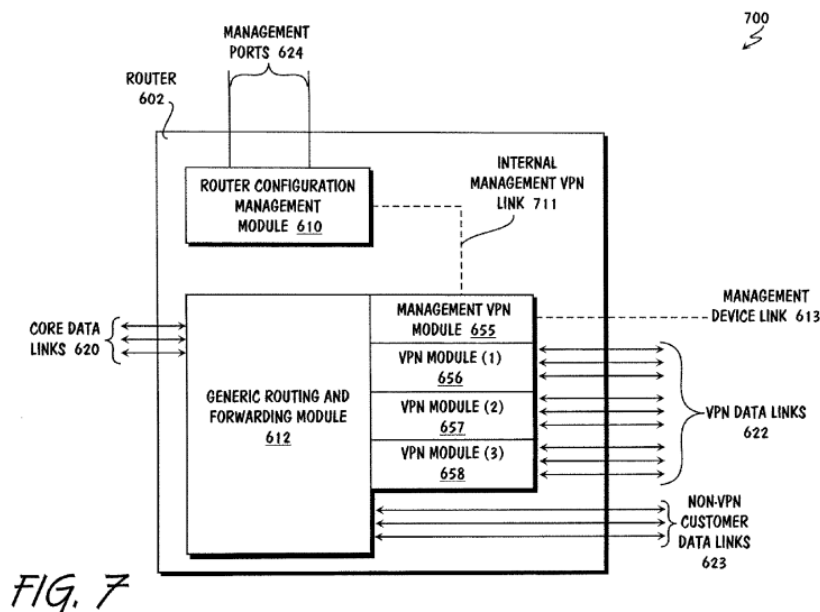
1020, 106:10-12. “The BMC can use this same interface to inject datagrams onto the LAN. These datagrams are interleaved with the network packets that are generated by system software.” Ex. 1020, 106:14-15; Ex. 2001, ¶ 54-55.

C. Lawrence

Lawrence is generally directed toward routers for secure in-band management for packet data networks. More specifically, FIG. 7 (reproduced below) shows an in-band management configuration for a router 602. The router 602 includes two main units: a generic routing and forwarding module 612, which “receives packets and performs basic routing and forwarding of data packets,” and a router configuration management module, 610, which receives “management traffic to perform functions, such as adding a link or customer, tearing down a link, or configuring a new card for a router.” Ex. 1043, 5:4-6, 15-16. An internal management VPN link 711 “connects management VPN module 655 to router configuration module 610,” such that “management traffic can be sent to router configuration management module 610 internally via management VPN module 655 and internal management VPN link 711.” Ex. 1043, 5:42-47; Ex. 2001, ¶ 57.

Each of the VPN modules 655 through 658 can perform VPN-related encapsulation, routing, and forwarding functions on packets through router 602. The encapsulation process entails adding extra headers to each data packet to identify VPN membership and access; furthermore, during the encapsulation process, the data packet may be encrypted using IP security (IPSec) process or another data encryption process. In this way, the packets are kept private and secure.

Ex. 1043, 5:22-30.



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

A. Ground 1 – Claims 1-4, 6, 7, 10, 11, 13 and 16 Are Not Obvious Over Neufeld Pursuant To 35 U.S.C. § 103

In Ground 1, the Petition relies on a single reference, Neufeld, in challenging Claims 1-4, 6, 7, 10, 11, 13 and 16 as allegedly obvious under 35 U.S.C. § 103. This allegation is deficient for a number of reasons. First, Neufeld does not disclose “at least one virtual interface connection means [that] provides logical separation of management data from user data.” Second, the VPN mentioned in Neufeld does not inherently perform “logical separation of management data from user data,” and such a feature would not have been obvious to a POSITA. Third, Petitioner provides the declaration of Dr. Meldal as “evidence” of the allegedly inherent features of a

VPN, but the supporting sections of Dr. Meldal’s declaration are identical to the text they are cited to support and, therefore, should be given no weight.

1. Neufeld Does Not Disclose “At Least One Virtual Interface Connection Means [That] Provides Logical Separation Of Management Data From User Data,” As Required By Claim 1

The Petition spuriously makes the argument that Neufeld discloses a VPN that performs this function of claim 1 and, therefore, concludes that Neufeld discloses this feature. This is a red herring. Neufeld is actually about user authentication to a network and not the separation of data. A VPN is only mentioned in the Neufeld specification in three places, and even in those sections, the VPN is merely used to connect to the network.

The Federal Circuit “explains that § 103 does not permit [a Petitioner] to stitch together an obviousness finding from discrete portions of prior art references without considering the references as a whole.” *In re Enhanced Sec. Research, LLC*, 739 F.3d 1347, 1355 (Fed. Cir. 2014). “It is impermissible within the framework of section 103 to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art.” *In re Wesslau*, 353 F.2d 238 (CCPA 1965).

In the Background paragraph [0009], Neufeld provides a general description of how clients and servers in larger networks can be connected. Neufeld states that there are “a large number of topologies that may be used for such purposes,” gives as examples Local Area Networks (LANs), Wide Area Networks (WANs) and Metro Area Networks (MANs), and notes that “[c]lients may also have the ability to access these networks via virtual private network (“VPN”) or via the Internet.” Ex. 1005, ¶ [0009] (emphasis added). The Background Section then turns to a discussion of network security, the particular threats to networks when users are permitted to access the network remotely, and problems with the way user authentication was conventionally performed. Paragraph [0022] specifically states that remote access “is potentially even more problematic if the system administrator attempts to access the server from a remote terminal outside of work, such as at home or while traveling” and notes that, in such situations, “the system administrator must typically use the Internet or a virtual private network to access the system.” Ex. 1005, ¶ [0022].

The only place in Neufeld’s Detailed Description that mentions VPNs at all is paragraph [0088]. In paragraph [0088], Neufeld explains an example of how the security manager, in a managed server, can operate to authenticate a user, with reference to TABLE 4 (reproduced below). More specifically, paragraph [0088] explains that “authentication services may become more rigorous and require the use of smartcard or biometrics if the confidence level in the actual identity of a user

attempting to access the network falls.” Additionally, paragraph [0088] mentions that users may attempt different types of remote connections, “such as via the Internet or via a virtual private network.” Ex. 1005, ¶ [0088].

TABLE 4

User ID	IP Address/ Connector Type	Time of Day	<u>User</u>		
			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

By way of example, TABLE 4 is one of four tables provided in Neufeld that contain user profiles that Neufeld’s system may use to authenticate a user attempting to login. TABLE 4, more specifically, provides an example profile for a non-administrator user, Joe-user. As shown in TABLE 4, Joe-user’s profile offers seven different possible combinations of User ID, IP Address/Connector Type, Time of Day, Authentication, Security Settings, and Privileges that may result in Joe-user being authenticated to the system (or not). TABLE 4 has been marked up for purposes of illustration.

Relevant to this discussion, the last two rows (in the red and blue boxes, respectively) indicate the circumstances under which Joe may be authenticated (or not authenticated). The data in the red box indicates that Joe will not be authenticated to the network if he tries to remotely login to the system after business hours using the Internet to access the system. However, he will be authenticated under the same circumstances if he tries to login using a VPN (blue box). This is because there is significantly more risk in allowing a non-administrator user to login remotely after business hours than there would be, for example, if he were an administrator and/or was trying to login during day time hours because attacks on networks are far more common when the user is not an administrator and when the connection takes place after business hours. Ex. 1005, ¶ [0084], [0088]. Neufeld recognizes that VPNs are a more secure way to access a network than the Internet, and therefore, Neufeld's system will only let Joe-users access the network using a VPN under these circumstances. Ex. 2001, ¶67.

While it is true that logging into a system using a VPN versus the Internet is generally more secure, there is nothing in Neufeld that states that Joe-user uses this VPN for anything other than logging into the network, and certainly does not disclose, or even suggest, that the VPN is also used as an interface between the remote management controller 116, which the Petition equates with the "at least one secure management access controller," of Claim 1, and the "user interfaces of said

managed network element,” over which the data is to be communicated. Further, strikingly missing from Neufeld is any mention whatsoever that the VPN, or any other feature in Neufeld, “provides logical separation of management data from user data.” That is because Neufeld did not even contemplate this functionality of a VPN as, in Neufeld, the VPN is only used as an option for connecting to a system. This is very different from the VMI of Claim 1. Ex. 2001, ¶65.

From the explicit disclosures in Neufeld, the only information discernable about the functionality of VPNs at all is the implication that they are more secure than “the Internet” as Neufeld’s system accounts for users logging in using different access technologies and places more restrictions on Internet use than on VPN use. This in no way discloses, or even implies, that the VPN mentioned in Neufeld has the necessary architecture for logically separating management data from user data.

The Petitioner’s argument that Neufeld discloses or suggests the functionality of claim 1 through its discussion of VPNs is unsupported and mischaracterizes the reference. Neufeld’s limited mentions of VPNs focus exclusively on their use as a secure option for user authentication and network access, without any disclosure or implication that VPNs in Neufeld provide logical separation of management data from user data or serve as an interface for communication between a remote management controller and managed network elements. The Federal Circuit has consistently rejected attempts to stitch together an obviousness argument by

selectively extracting portions of a reference without considering the reference as a whole, as explained in *In re Enhanced Sec. Research, LLC*. Here, the Petitioner improperly extrapolates functionality from Neufeld's general mention of VPNs, which are solely described as a means of logging into a system. Neufeld's disclosures do not contemplate, much less teach, the architecture required to achieve the logical separation of management and user data as recited in claim 1. As such, the Petitioner's arguments fail to meet the standard of obviousness and should be rejected.

2. The VPN Mentioned in Neufeld Does Not Obviously, or Inherently, Perform Separation of Management Data From User Data

Under 35 U.S.C. § 103, a claimed invention is unpatentable if the differences between the claimed subject matter and the prior art are such that the subject matter as a whole would have been obvious to a person of ordinary skill in the art at the time the invention was made. 35 U.S. Code § 103 (PRE-AIA). Obviousness is a question of law based on underlying factual findings, including: (1) the scope and content of the prior art, (2) the differences between the prior art and the claimed invention, (3) the level of ordinary skill in the art, and (4) any objective indicia of non-obviousness, such as commercial success or long-felt but unmet needs. *Graham v. John Deere Co.*, 383 U.S. 1, 1966.

A single prior art reference can render a claim obvious if it provides sufficient teaching, suggestion, or motivation (explicitly or inherently) to combine known elements or modify the reference to arrive at the claimed invention. A limitation not explicitly disclosed in the reference may still render the claim obvious if the missing feature is necessarily present or inherent in the reference. *In re Kubin*, 561 F.3d at 1357. However, inherency requires that the missing element be a natural result of the prior art teachings, not merely a possibility.

Regarding obviousness, or inherency, the Petition argues that “[a] POSITA would have found it obvious to utilize a point-to-point VPN with tunneling functionality on Neufeld’s managed server 2 via the in-band connection used for non-management user traffic (i.e., the NIC 110 and network N) in order to provide for a dedicated VPN for communications of management data.” Petition, page 33. The Petition goes on to state that “[a] POSITA would have had knowledge of point-to-point VPNs using tunneling at the time of invention, would have understood that tunneling employs encryption to secure the VPN communications, and would have found it obvious to configure Neufeld’s managed server to employ a point-to-point VPN because tunneling was a well-known, and indeed was the most common method, for implementing a point-to-point VPN.” *Id.* These arguments fail for at least the following reasons.

**a) Petitioner Has Not Established that It Would Have
Been Obvious to Modify Neufeld to Arrive at the Claimed
Invention**

For a single-reference obviousness rejection based on modification of the primary reference, a challenger must demonstrate: (1) a reason or motivation to modify the reference; (2) that the modification would yield predictable results; and (3) that a POSITA would have had a reasonable expectation of success. *KSR International Co. v. Teleflex Inc.*, 550 U.S. 398 (2007). If these elements are satisfied, and there is no teaching away or compelling objective evidence of non-obviousness, the claimed invention is likely unpatentable under 35 U.S.C. § 103. *Id.* Petitioner has not successfully established any of these requirements.

The Petition asserts that a POSITA would have been motivated to modify Neufeld for the following reasons: (1) “to provide for a dedicated VPN for communications of management data with the remote management PC 5,” and (2) “VPN tunneling was a well-known, and indeed was the most common method, for implementing a point-to-point VPN.” Petition, page 33. What Petitioner fails to explain, however, is why a POSITA would have been motivated to modify the reference. In this case, there is no reason aside from the specification of the ‘140 Patent itself, which is impermissible hindsight. (*KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 421 (2007); *In re Kotzab*, 217 F.3d 1365, 1369 (Fed. Cir. 2000) (holding hindsight is impermissible in an obviousness analysis, as the determination must be

based on the perspective of a person of ordinary skill in the art at the time of the invention, without using knowledge gleaned from the invention itself (*KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 421 (2007); *In re Kotzab*, 217 F.3d 1365, 1369 (Fed. Cir. 2000)). Further, as explained by the Federal Circuit, “[t]o satisfy its burden of proving obviousness, a petitioner cannot employ mere conclusory statements.” *In re Magnum Oil Tools Int'l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016). Instead, the Petitioner has the burden to submit facts to the record that show “[w]hether the prior art discloses a claim limitation, whether a skilled artisan would have been motivated to modify or combine teachings in the prior art, and whether she would have had a reasonable expectation of success in doing so.” *Univ. of Strathclyde v. Clear-Vu Lighting LLC*, 17 F.4th 155, 160 (Fed. Cir. 2021). If the petition does not clearly demonstrate how the cited prior art meets each claim element, the Petitioner will fail to meet its burden.

Petitioner’s argument, here, revolves around a complete mischaracterization of the importance of the VPN to Neufeld’s network. In terms of in-band communication, Neufeld is all about user authorization, the implementation of which takes into account the type of user access to the system (VPN or Internet). Ex. 2001, ¶¶66-67. However, in Neufeld, a VPN is only ever used to login to the system, and a user can be authenticated to the system (or not authenticated) “at the time the user

logs on to the system,” depending on the type of network access the user attempts (e.g., using a VPN versus the Internet). Ex. 1005, ¶ [0091].

There is no implication whatsoever that separation of management data from user data is at all important to the system, or is even a part of it at all. Additionally, the VPN mentioned in Neufeld is only an option, and, as a result, a POSITA would not have paid the VPN much attention, and would have had no reason to modify the VPN for this reason. The only place separation of user data from management data is mentioned is in the specification of the ‘140 Patent.

Regarding predictable results and reasonable expectation of success, the Petition is completely silent. In fact, the obviousness argument in the Petition is a mere single paragraph long, providing no detail whatsoever as to how or why a POSITA would have made this alleged modification to Neufeld.

Accordingly, the feature of “at least one virtual interface connection means [that] provides logical separation of management data from user data,” would not be obvious over Neufeld.

b) Separation Management Data from User Data is Not a Natural Result of the Technology (a VPN)

For an obviousness rejection based on a modification of a single reference, the challenger bears the burden of demonstrating a clear reason or motivation to modify the reference, a predictable outcome from the modification, and a reasonable expectation of success for a person of ordinary skill in the art (POSITA). The Petition,

however, fails to meet these requirements with respect to its proposed modification of Neufeld to include the claimed feature of “at least one virtual interface connection means [that] provides logical separation of management data from user data.” While the Petition asserts that a POSITA would have been motivated to modify Neufeld’s system to incorporate a dedicated VPN for management data, it does not provide any evidence or rationale supporting why such a modification would have been made at the time of the invention, aside from hindsight derived from the ’140 Patent itself. Moreover, the Petition mischaracterizes Neufeld’s VPN functionality, which is solely focused on user authentication during login and does not suggest or imply the logical separation of management and user data. The lack of any discussion in the Petition regarding predictable results or reasonable expectation of success further underscores its failure to satisfy the requirements for an obviousness analysis under *KSR International Co. v. Teleflex Inc.* and related precedents. Consequently, the Petitioner’s arguments fall short of establishing obviousness.

Petitioner alleges in its Petition that dedicated point-to-point VPNs *necessarily* provide logical separation of user data and management data. Petition, page 34. Strikingly, however, Petitioner provides no evidence in support of this assertion, concluding only that “a point-to-point VPN...performs the claimed function of the VPN,” and “VPN tunneling necessarily differentiates traffic for the

dedicated VPN from other traffic.” *Id.* However, separating management data from user data is not the natural result of a VPN.

A Virtual Private Network (VPN) is a service that encrypts your internet connection and routes it through a secure server, masking your IP address and protecting your online privacy. It allows you to safely access the Internet, especially on public networks, and can bypass geographic restrictions on content. Ex 2001, ¶¶67.

VPNs secure data by creating an encrypted “tunnel” between your device and the VPN server, ensuring that any data transmitted is scrambled and unreadable to unauthorized parties. This encryption uses complex algorithms, such as AES (Advanced Encryption Standard), to encode the data, which can only be decrypted with a corresponding key. Once encrypted, the data is transmitted through secure protocols, like OpenVPN or IKEv2/IPSec, preventing interception by hackers, ISPs, or other third parties. The VPN server then forwards your data to its destination, such as a website or online service, while masking your IP address to enhance privacy and security. This process safeguards your information, even on unsecured public networks. Ex 2001, ¶¶57.

There is nothing *inherent* in a VPN that separates different types of data from each other. In fact, to the contrary, without outfitting the VPN with a specific architecture to do so, a VPN will send all of the data, including both management and user data, over a secure tunnel. Ex 2001, ¶¶66.

c) Petitioner’s Conclusory Arguments, Backed Only by the Identical Conclusory Arguments of Petitioner’s Expert, Dr. Meldal, Should be Given Little, If Any, Weight

Further, The Courts and the PTAB alike have made clear that, when arguing a feature naturally flows from the technology, some evidence, apart from conclusory statements, must be offered in support. *See Arendi S.A.R.L. v. Apple Inc.*, 832 F.3d 1355 (Fed. Cir. 2016). This is particularly true when conclusory statements in an IPR petition are merely supported by the identical conclusory statements in Petitioner’s expert declaration. In such circumstances, the expert’s declaration should be given little, if any, weight. *See IPR2022-00624, Director Review Decision, Paper #12, February 10, 2023 (finding that “the Board was correct in giving little weight to Petitioner’s expert because the expert declaration merely offered conclusory assertions without underlying factual support.”)*. These cases collectively indicate that expert testimony in patent disputes must include independent, reasoned analysis and cannot merely reiterate the Petitioner’s arguments or present conclusory opinions devoid of evidentiary support. The Federal Circuit has “underscored that the expert’s conclusory statements and unspecific expert testimony d[o] not qualify as substantial evidence that could support the Board’s conclusions regarding obviousness.” *TQ Delta, LLC v. Cisco Sys.*, 942 F.3d 1352, 1360-61 (Fed. Cir. 2019).

To substitute for a complete lack of disclosure in Neufeld of a VMI that separates user data from management data, the Petition argues that a POSITA would have found this claim feature inherent, “because a POSITA would have found it obvious to utilize a point-to-point VPN with tunneling functionality on Neufeld’s managed server 2 via the in-band connection used for non-management traffic (i.e., the NIC 110 and network N) in order to provide for a dedicated VPN for communications of management data with the remote PC5).” Petition, page 33. Petitioner goes on to assert that “VPN tunneling was well-known, and indeed was the most common method, for implementing a point-to-point VPN.” *Id.* For this proposition, the Petition cites to the Declaration of Dr. Meldal at 111, which states the exact same thing. This is nothing other than a conclusory statement that does little, if anything, to explain why these concepts were so well-known at the time of invention, and yet Petitioner has not produced a single shred of evidence supporting it (and neither has their expert).

Table 1, below, provides a comparison of the arguments in the Petition, and the alleged supporting evidence in Dr. Meldal’s declaration (any differences between the two are highlighted in yellow). They are nearly identical, and both fail to provide anything other than conclusory statements. Of particular note is that Dr. Meldal’s declaration is completely devoid of any cross-citations in support of his position. Accordingly, Dr. Meldal’s declaration should be given little weight.

TABLE 1

Petition	¶111 Expert Declaration
<p>A POSITA would have had knowledge of point-to-point VPNs using tunneling at the time of invention, would have understood that tunneling employs encryption to secure the VPN communications, and would have found it obvious to configure Neufeld's managed server to employ a point-to-point VPN with tunneling for communication of management data because VPN tunneling was a well-known, and indeed was the most common method, for implementing a point-to-point VPN. EX1046 ¶111 (discussing the use of LTP/IPsec to create a secure L2TP protected by IPsec).</p>	<p>A POSITA would have had knowledge of point-to-point VPNs using tunneling at the time of invention, would have understood that tunneling employs encryption to secure the VPN communications, and would have found it obvious to configure Neufeld's managed server to employ a point-to-point VPN with tunneling for communication of management data because VPN tunneling was a well-known, and indeed was the most common method, for implementing a point-to-point VPN.</p>
<p>A point-to-point VPN with tunneling used for the communication of management data between the remote server management controller 116 and the remote management PC 5 via the network N also performs the claimed function performed by the VPN technology of the 140 patent, namely providing logical separation of user data and management data. EX1046, ¶113</p>	<p>¶113 A point-to-point VPN with tunneling used for the communication of management data between the remote server management controller 116 and the remote management PC 5 via the network N also performs the identical function performed by the VPN technology of the 140 patent, namely providing logical separation of user data and management data.</p>
<p>The use of a dedicated point-to-point VPN using tunneling technology provides for logical separation because the VPN tunneling necessarily differentiates traffic for the dedicated VPN from other user traffic. EX1046, ¶114</p>	<p>¶114 The use of a dedicated VPN necessarily provides for logical separation because the VPN tunneling necessarily differentiates traffic for the dedicated VPN from other traffic.</p>
<p>The VPN tunneling functionality dedicated to communications of</p>	<p>¶115 The VPN tunneling functionality dedicated to communications of</p>

management data from remote management PC 5 also performs the function of connecting a remote user on remote management PC 5 with Neufeld's remote server management controller 116 for communication of management data using the same user interface (Neufeld's NIC 110 connected to network N) over which non-management user data is communicated to the managed server 2. EX1046, ¶115	management data from remote management PC 5 also performs the function of connecting a remote user on remote management PC 5 with Neufeld's remote server management controller 116 for communication of management data using the same user interface (Neufeld's NIC 110 connected to network N) over which non-management user data is communicated to the managed server 2.
---	--

To be clear, *all* of Dr. Meldal's testimony as to the *inherency* of a VPN are mere conclusory statements and do not even attempt to answer the lingering question as to why this functionality was inherent. In *Facebook v. Windy City Innovations, LLC*, the Court affirmed the Board's holding that independent claim 1 was not unpatentable as obvious over the asserted prior art when "the Board considered Facebook's expert's testimony but determined that it did not add materially to Petitioner's unpersuasive attorney argument," because it merely repeated Petitioner's argument, nearly verbatim, without citation to the basis for his testimony." 973 F.3d 1321, 1340-41 (Fed. Cir. 2020). In fact, the Federal Circuit expressly held that "conclusory expert testimony and attorney argument cannot constitute substantial evidence." *Acoustic Tech., Inc. v. Itron Networked Sols., Inc.*, 949 F.3d 1366, 1375 (Fed. Cir. 2020). Accordingly, Dr. Meldal's testimony should be given little, if any, weight. And since Dr. Meldal's testimony is the only evidence

submitted for the alleged inherency of logical separation of data, this Petition should not be instituted.

3. Neufeld’s VPN Implementations Fail to Disclose a “Virtual Management Interface Connection Means” or Logical Separation of Management and User Data.

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

System Administrator Access: Neufeld explains 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]).

User Access: Table 4 illustrates “Joe-user” accessing a managed server through a remote VPN. (Id., ¶¶ [0087]-[0088]).

In the first scenario, the VPN facilitates access for the system administrator via their remote terminal. In the second scenario, the VPN enables access for a user via their remote terminal. Ex. 2001, ¶¶ 69-70.

The Petitioner contends 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 accepting this contention, such a VPN would merely establish a connection between the system administrator or Joe-user and the NIC 110—not with the remote server management controller 116, which the Petitioner identifies as the purported “secure management access controller.” Consequently, 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. Ex. 2001, ¶ 71.

Additionally, Neufeld’s VPN implementations do not satisfy the claim requirement of “provid[ing] logical separation of management data from user data.” In both scenarios described by Neufeld, management and user data are intermingled, rendering logical separation either unnecessary or inapplicable. Ex. 2001, ¶ 72.

23. Accordingly, Neufeld fails to disclose or suggest all the elements required by claim 1.

4. Petitioner Has Failed To Meet Their Burden Of Showing The Challenged Claims Are Unpatentable Under Ground 1

The critical flaws in Petitioner’s argument, as well as in the declaration of its expert, establish that Neufeld fails to teach or suggest, inherently, obviously, or otherwise, the separation of management data from user data required by the challenged claims. With regard to dependent claims 2-4, 6, 7, 10, 11, 13, and 16, Petitioner’s arguments fail for at least the same reasons as Claim 1.

For the IPR to be instituted, the Petitioner must “show[] that there is a reasonable likelihood that the Petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314. Moreover, “[u]nlike district court litigation—where parties have greater freedom to revise and develop their

arguments over time and in response to newly discovered material—the expedited nature of IPRs bring with it an obligation for petitioners to make their case in their petition to institute.” *Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1369 (Fed. Cir. 2016). Accordingly, in an IPR, the patent challenger has the burden of producing evidence in the Petition to support a conclusion of unpatentability.

Here, the Petitioner has clearly failed to meet its burden. Accordingly, the Petition has failed to meet its burden on Ground 1 for at least the reasons provided above.

B. Ground 2 – Dependent Claims 11 and 12 are Not Obvious over Neufeld and Syvanne

The Petition does not allege, nor does Syvanne teach, “at least one virtual management interface connection means [that] provides logical separation of management data from user data,” as recited in independent Claim 1. Accordingly, because Syvanne does not cure the shortcomings of Neufeld, the Petitioner has failed to meet its burden with regard to Ground 2 for at least the reasons discussed with regard to Ground 1 above.

C. Ground 3 - Dependent Claim 14 is Not Obvious Over Neufeld and Fowler Pursuant To 35 U.S.C. § 103

The Petition does not allege, nor does Fowler teach, “at least one virtual management interface connection means [that] provides logical separation of management data from user data,” as recited in independent Claim 1. Accordingly,

because Fowler does not cure the shortcomings of Neufeld, the Petitioner has failed to meet its burden with regard to Ground 3 for at least the reasons discussed with regard to Ground 1 above.

D. Ground 4 - Dependent Claim 13 is Not Obvious Over Neufeld and Fowler Pursuant To 35 U.S.C. § 103

The Petition does not allege, nor does Fowler teach, “at least one virtual management interface connection means [that] provides logical separation of management data from user data,” as recited in independent Claim 1. Accordingly, because Fowler does not cure the shortcomings of Neufeld, the Petitioner has failed to meet its burden with regard to Ground 4 for at least the reasons discussed with regard to Ground 1 above.

E. Ground 5 - Claims 1-3, 6, 7, 10 And 11 Are Not Obvious Over IPMI and Lawrence Pursuant To 35 U.S.C. § 103

In Ground 5, the Petition argues that Claim 1 is obvious over an alleged combination of IPMI and Lawrence. This allegation is deficient for a number of reasons. First, the claim feature “at least one virtual interface connection means [that] provides logical separation of management data from user data,” would not be obvious from IPMI and Lawrence. Second, the VPN of Lawrence does not perform “logical separation of management data from user data,” and such feature would not have been obvious to a POSITA.

1. The Claim Feature “At Least One Virtual Interface Connection Means [That] Provides Logical Separation Of Management Data From User Data” Would Not Be Obvious From IPMI And Lawrence

IPMI is a standardized interface used for remotely managing and monitoring computer hardware. The Petitioner’s argument largely centers around the BMC, which provides management functions. IPMI uses User Datagram Protocol (UDP) for sending IPMI packets. If IPMI is implemented in a system that makes use of out-of-band communication for network maintenance, a network LAN controller will detect UDP datagrams addressed to the BMC and send them to the BMC over a side band connection. Similarly, the BMC can inject UDP datagrams onto the side-band connection. Ex. 2001, ¶55.

Lawrence is directed toward a VPN. The VPN in Lawrence has the following functionality: performing “VPN-related encapsulation, routing, and forwarding functions on packets passing through router 602.” Ex. 1043, 5:23-24. Lawrence further mentions that “a VPN is a private data network that makes use of the currently implemented network by using a tunneling protocol for security purposes.” Ex. 1043, 2:35-37.

In its obviousness contention, the Petitioner argues as follows:

Since IMPI discloses in-band communication from the physical LAN connector to the LAN Controller, a POSITA would have found it obvious to incorporate Lawrence’s VPN module 655 into IPMI’s LAN Controller to separate the IPMI UDP datagrams from other user traffic and send the IPMI UDP

datagrams over the side-band interface to the BMC. In the IPMI-Lawrence combination, those packets are processed by Lawrence's dedicated management VPN module 655....

Petition, page 64 (citations removed).

a) IPMI's LAN Controller Does Not Separate Data, But Rather Detects Packets Addressed to the BMC

The Petition's main argument for Ground 5 is that IPMI discloses a LAN controller that "separate[s] the IPMI UDP datagrams from other user traffic and send[s] the UDP datagrams over the side-band interface to the BMC." Petition, page 64. "In the IPMI-Lawrence combination, those packets are processed by Lawrence's dedicated management VPN module 655." *Id.* This argument is based on a fundamental misunderstanding of how LAN controllers work.

LAN controllers function as intermediaries in network communication by managing data packet flow between devices and a computer's main processor. Acting as "traffic cops," LAN controllers inspect the address of each received packet to determine its intended destination. Using embedded logic, the LAN controller evaluates the packet's address against the network configuration and decides where to route it. This ensures that only relevant packets reach the appropriate bus or device, preventing unnecessary congestion and maintaining efficient data flow. Ex. 2001, ¶77.

Accordingly, the basic functionality of LAN controllers is to route packets based on their addresses, and the LAN controller in IPMI does that without the

addition of a VPN. In fact, if the LAN controller were to encounter VPN packets, it would route them exactly the same as every other packet because, from the perspective of the LAN controller, the packets are indistinguishable. There is simply nothing missing from IPMI that would have caused a POSITA to go looking for Lawrence. Ex. 2001, ¶76.

b) The VPN Of Lawrence Does Not Separate Management Data From User Data

Another major issue with the Petitioner's argument is that it assumes, once again, that VPNs with tunneling functionality necessarily separate management data from user data. As explained above with regard to Ground 1, this is not the case. Lawrence merely describes a VPN that performs tunneling, which has nothing to do with separating data.

A Virtual Private Network (VPN) is a service that encrypts your internet connection and routes it through a secure server, masking your IP address and protecting your online privacy. It allows you to safely access the Internet, especially on public networks, and can bypass geographic restrictions on content. Ex. 2001, ¶76.

VPNs secure data by creating an encrypted "tunnel" between your device and the VPN server, ensuring that any data transmitted is scrambled and unreadable to unauthorized parties. This encryption uses complex algorithms, such as AES (Advanced Encryption Standard), to encode the data, which can only be decrypted

with a corresponding key. Once encrypted, the data is transmitted through secure protocols, like OpenVPN or IKEv2/IPSec, preventing interception by hackers, ISPs, or other third parties. The VPN server then forwards your data to its destination, such as a website or online service, while masking your IP address to enhance privacy and security. This process safeguards your information, even on unsecured public networks. Ex. 2001, ¶57.

In *Par Pharm., Inc. v. TWi Pharm., Inc.*, the Court explains “the use of inherency, a doctrine originally rooted in anticipation, must be carefully circumscribed in the context of obviousness,” and “[t]he mere fact that a certain thing may result from a given set of circumstances is not sufficient to establish inherency.” *Par Pharm., Inc. v. TWi Pharm., Inc.*, 773 F.3d 1186, 1194-95 (Fed. Cir. 2014) (internal markings and citations omitted). The Court has “emphasized that the limitation at issue necessarily must be present in order to be inherently disclosed by the reference.” (*Southwire Co. v. Cerro Wire LLC*, 870 F.3d 1306, 1310-11 (Fed. Cir. 2017)) (internal citation omitted). Accordingly, “[a] party must...meet a high standard in order to rely on inherency to establish the existence of a claim limitation in the prior art in an obviousness analysis.” *Millennium Pharms., Inc. v. Sandoz, Inc.*, 862 F.3d 1356, 1367 (Fed. Cir. 2017).

There is nothing *inherent* in a VPN that separates different types of data from each other. In fact, to the contrary, without outfitting the VPN with a specific

architecture to do so, a VPN will send all of the data, including both management and user data, over a secure tunnel.

Therefore, Lawrence does not inherently teach “at least one virtual management interface connection means [that] provides logical separation of management data from user data,” as recited in independent Claim 1.

c) Petitioner Has Not Established that It Would Have Been Obvious to Modify IPMI, With the Teachings of Lawrence, to Arrive at the Claimed Invention

To establish obviousness under 35 U.S.C. § 103, a petitioner must demonstrate that the claimed invention would have been obvious to a person of ordinary skill in the art (POSITA) at the time of the invention. This requires showing a reason or motivation to combine or modify prior art references with a reasonable expectation of success, supported by evidence or reasoning. The analysis must be based on the scope and content of the prior art, differences between the prior art and the claimed invention, and the level of ordinary skill in the art. *Graham v. John Deere Co.*, 383 U.S. 1, 1966. As explained by the Federal Circuit, “[t]o satisfy its burden of proving obviousness, a petitioner cannot employ mere conclusory statements.” *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016). Further, “[a]n obviousness determination requires finding that a POSITA would have been motivated to combine or modify the teachings in the prior art and would have had a reasonable expectation of success in doing so.” *Endo Pharm., Inc.*

v. Actavis LLC, 922 F.3d 1365, 1373 (Fed. Cir. 2019) (emphasis added). Accordingly, “[w]hether there was a motivation to combine references, and a reasonable expectation of success in doing so to meet the limitations of the claimed invention are questions of fact” that must be established by a Petitioner for an IPR to be instituted. *Samsung Elecs. Co. v. Elm 3DS Innovations, LLC*, 925 F.3d 1373, 1380 (Fed. Cir. 2019)

With respect to a reason or motivation to modify the reference, the Petition gives the following reason:

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

However, this is not the case. As explained above, the VPN technology described in Lawrence does not separate management data from user data, and neither does the LAN controller in IPMI. This leaves the open question as to why a POSITA would have looked to Lawrence as a secondary reference. In this case, there is no reason aside from the specification of the ‘140 Patent itself, which is impermissible hindsight. Ex. 2001, ¶¶ 76 and 82.

As explained the Federal Circuit, “the inventor’s own path itself never leads to a conclusion of obviousness; that is hindsight. What matters is the path that the

person of ordinary skill in the art would have followed, as evidenced by the pertinent prior art.” *Otsuka Pharm. Co., v. Sandoz, Inc.*, 678 F.3d 1280, 1296 (Fed. Cir. 2012). Therefore, obviousness is not established under 35 U.S.C §103 when “[i]t is only with the benefit of hindsight that a person of skill in the art would have had a reasonable expectation of success in view of the asserted references.” *OSI Pharms., LLC v. Apotex Inc.*, 939 F.3d 1375, 1385 (Fed. Cir. 2019). Accordingly, a finding of obviousness under 35 U.S.C. § 103 cannot be based on hindsight; rather, it must be supported by a reasonable expectation of success from the perspective of a person of ordinary skill in the art, without relying on the inventor’s own path. Therefore, the obviousness allegation in this case fails to meet the required standard and should not be sustained.

Additionally, in *In re Ratti*, the Court held that a combination of references is improper if it renders the combined references inoperable for their intended purpose. 270 F.2d 810, 813, 47 C.C.P.A. 1059 (1959)). The Federal Circuit emphasized that a modification leading to an incompatible or inoperative result fails to support a finding of obviousness. In *In re Ratti*, the combination of prior art references would have required substantial alterations that changed the fundamental operation of the devices involved, thus making the combination non-functional. Similarly, the United States Patent and Trademark Office, Manual of Patent Examining Procedure

(MPEP)¹ explains that *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984) held that “[i]f a proposed modification 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.” (MPEP §2143.01). Accordingly, as explained in *In re Ratti* and *In re Gordon*, a proposed combination of references is improper under 35 U.S.C. §103 when the combination would render the references inoperable for their intended purpose.

The Petitioner’s proposed combination of IPMI and Lawrence would lead to a device that is not operable for its intended purpose. The LAN controller in IPMI works by reading the addresses of received packets and routing them to the appropriate entity (in this case, the BMC). Adding a VPN into the mix, allegedly to separate management data from user data, would completely change the operation of the LAN controller from routing data within a network to separating management data from user data. Therefore, Petitioner’s proposed combination would not result merely in an implementation of the LAN controller, but would only serve to change the functionality of IPMI’s LAN controller.

d) A POSITA Would Not Be Motivated to Utilize A VPN On An Internal Connection Within a Server.

¹ “The MPEP has no binding force ... but is entitled to notice so far as it is an official interpretation of statutes or regulations with which it is not in conflict.” *Litton Sys. v. Whirlpool Corp.*, 728 F.2d 1423, 1439 (Fed. Cir. 1984)

A person of ordinary skill in the art (POSITA) would not implement a VPN link over the “side band connection” between IPMI’s “LAN Controller” and the “BMC” (alleged “secure management access controller”). Such an implementation would offer no additional security benefit and would introduce unnecessary redundancy. Consequently, IPMI, whether considered alone or in combination with Lawrence, does not 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. Ex 2001, ¶¶ 78-79.

Even if Lawrence’s VPN modules (e.g., management VPN module 655) were interpreted as “provid[ing] logical separation of management data from user data,” these modules cannot be integrated into IPMI’s LAN Controller, contrary to the Petitioner’s argument (Pet. at 64). Such a modification would compromise the LAN Controller’s functionality, which is specifically 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 integrating Lawrence’s VPN modules into the LAN Controller would render it inoperable and would therefore avoid such a modification. Ex 2001, ¶ 80.

Accordingly, IPMI, whether analyzed individually 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 for “provid[ing] logical separation of management data from user data,” as required by claim 1. Ex, 2001, ¶ 81.

e) Petitioner Has Failed To Meet Their Burden Of Showing The Challenged Claims Are Unpatentable Under Ground 1

The critical flaws in Petitioner’s argument establish that the alleged combination of IPMI and Lawrence fails to teach or suggest the separation of management data from user data required by the challenged claims. Accordingly, for at least the reasons provided above, the Petition has failed to meet its burden regarding Ground 5.

F. Ground 6 - Dependent Claim 4 is Not Obvious Over IPMI, Lawrence and Leedy Pursuant To 35 U.S.C. § 103

The Petition does not allege, nor does Leedy teach, “at least one virtual management interface connection means [that] provides logical separation of management data from user data,” as recited in independent Claim 1. Accordingly, because Leedy does not cure the shortcomings of IPMI and Lawrence, the Petitioner has failed to meet its burden with regard to Ground 6 for at least the reasons discussed with regard to Ground 5 above.

G. Ground 7 - Dependent Claims 11 And 12 Are Not Obvious Over IPMI, Lawrence And Syvanne Pursuant To 35 U.S.C. § 103

The Petition does not allege, nor does Syvanne teach, “at least one virtual management interface connection means [that] provides logical separation of management data from user data,” as recited in independent Claim 1. Accordingly, because Syvanne does not cure the shortcomings of IPMI and Lawrence, the Petitioner has failed to meet its burden with regard to Ground 7 for at least the reasons discussed with regard to Ground 5 above.

H. Ground 8 - Dependent Claims 13 and 14 Are Not Obvious Over IPMI, Lawrence and Fowler Pursuant To 35 U.S.C. § 103

The Petition does not allege, nor does Fowler teach, “at least one virtual management interface connection means [that] provides logical separation of management data from user data,” as recited in independent Claim 1. Accordingly, because Fowler does not cure the shortcomings of IPMI and Lawrence, the Petitioner has failed to meet its burden with regard to Ground 8 for at least the reasons discussed with regard to Ground 5 above.

I. Dependent Claim 16 is Not Obvious Over IPMI, Lawrence and RFC1492 Pursuant To 35 U.S.C. § 103

The Petition does not allege, nor does RFC1491 teach, “at least one virtual management interface connection means [that] provides logical separation of management data from user data,” as recited in independent Claim 1. Accordingly, because RFC1491 does not cure the shortcomings of IPMI and Lawrence, the

Petitioner has failed to meet its burden with regard to Ground 9 for at least the reasons discussed with regard to Ground 5 above.

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

The Petition is required to include “[a] full statement of the reasons for relief requested, including a detailed explanation of the significance of the evidence including material facts,” 37 C.F.R. § 42.22(a)(2), which must include a statement of “[h]ow the challenged claim is to be construed” and “[h]ow the construed claim is unpatentable.” *Id.* § 42.104(b)(3)-(4). For the IPR to be instituted, the Petitioner must “show[] that there is a reasonable likelihood that the Petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314.

As stressed by the Federal Circuit:

It is of the utmost importance that petitioners in the IPR proceedings adhere to the requirement that the initial Petition identify with particularity the evidence that supports the grounds for the challenge to each claim. . . . [T]he expedited nature of IPRs bring with it an obligation for petitioners to make their case in their Petition to institute. *Wasica Finance GmbH v. Continental Automotive Systems, Inc.*, 853 F.3d 1272, 1286–87 (Fed. Cir. 2017).

Accordingly, in an IPR, the patent challenger has the burden of producing evidence in the Petition to support a conclusion of unpatentability.

In the present case, Petitioner mis-construes the cited references, placing emphasis on features of these references that have little to do with the inventions

described therein. For example, Petitioner hones in on the mere mention of a VPN in Neufeld that is just an option for connecting to a network, never even mentioning the authentication functions of Neufeld that are at the heart of their invention, and which provide the details necessary to understand that fact. For another example, Petitioner contorts the function of the LAN controller in IPMI, which merely routes packets based on addresses, creating the problem of separating management data from user data where no such problem existed. And all Petitioner provides as support for its wild assertions is mere conclusions, with no evidentiary support other than the identical conclusory statements of their expert. Accordingly, for all the reasons provided herein, this Petition should not be instituted.

VI. CONCLUSION

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

Respectfully submitted,

Dated: November 21, 2024

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

CERTIFICATE OF COMPLIANCE WITH WORD COUNT

Pursuant to 37 C.F.R. § 42.24(d), I certify that this Patent Owner Preliminary Response complies with the type-volume limits of 37 C.F.R. § 42.24(b)(1) because it contains 12,003 words, excluding the parts of this Patent Owner's Preliminary Response that are exempted by 37 C.F.R. § 42.24(a), according to the word processing system used to prepare this Patent Owner's Preliminary Response.

Respectfully submitted,

Dated: November 21, 2024

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

CERTIFICATE OF SERVICE

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

James Heintz
Jim.heintz@us.dlapiper.com

Gianni Minutoli
gianni.minutoli@us.dlapiper.com

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

Dated: November 21, 2024

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