

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. Pat. No. 7,325,140

PETITIONER'S REPLY TO PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. GROUNDS 1-4 DEMONSTRATE THE UNPATENTABILITY OF ALL CHALLENGED CLAIMS	2
A. PO Has Waived All Arguments for Grounds 1-4 Other Than Its Arguments on Limitation [1.c].....	2
B. PO’s Arguments on Neufeld Are Flawed	2
1. Neufeld Is Not Limited to Out-of-Band Communications	3
a. Neufeld Discloses or Renders Obvious In-Band Communication of Remote Management Messages	3
b. PO’s Argument that Neufeld Is Limited to Out-of-Band Communications Is Clearly Wrong.....	8
2. The Use of a Point-to-Point VPN Is Obvious Over Neufeld.....	14
C. The Petition’s Reasoning Is Sound Under Federal Circuit Precedent	18
III. GROUNDS 5-9 DEMONSTRATE THE UNPATENTABILITY OF ALL CHALLENGED CLAIMS	19
A. The Petition Establishes the Obviousness Using VPNs to Secure In-Band Communication Between Remote Users and a Secure Management Access Controllers.....	19
B. IPMI and Lawrence Render Obvious the Logical Separation of Management Data From User Data.....	22
IV. CONCLUSION.....	25

INDEX OF EXHIBITS

Exhibit No.	Description
1001	U.S. Patent No. 8,474,016
1002	U.S. Patent No. 7,325,140
1003	Declaration of Dr. Sigurd Meldal for IPR2024-00109
1004	File History for U.S. Pat. App. No. 10/969,561
1005	U.S. Pat. Pub. No. 2003/0226015 (“Neufeld”)
1006	U.S. Pat. No. 7,085,385 (“Frantz”)
1007	U.S. Patent Publication No. 2003/0097503 (“Huckins”)
1008	“PCI-to-PCI Bridge Architecture Specification”, Rev. 1.1 (“PCI Bridge Spec”)
1009	“Datasheet PCF8584 I2C-bus controller” (“PCF8584”)
1010	U.S. Pat. App. No. 09/438,253 downloaded from USPTO website (“Emerson”)
1011	U.S. Patent No. 6,219,708 (“Martenson”)
1012	U.S. Patent No. 5,651,137 (“MacWilliams”)
1013	“RFC1492: An Access Control Protocol, Sometimes called TACACS” (“RFC1492”)
1014	“RFC2865: Remote Authentication Dial In User Service (RADIUS)” (“RFC2865”)
1015	U.S. Patent No. 7,260,555 (“Rossman”)
1016	U.S. Patent Publication No. 2003/0097590 (“Syvanne”)
1017	U.S. Patent No. 7,383,577 (“Hrstar”)
1018	“RFC1157: A Simple Management Network Management Protocol (SNMP)” (“RFC1157”)
1019	Microsoft Computer Dictionary (5th ed. 2002)
1020	“IPMI – Intelligent Platform Management Interface Specification V1.5” (Rev. 1.1 dated 2/20/2002) (“IPMI”)
1021	“RFC3414: User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)” (“RFC3414”)
1022	“IP Filter Based Firewalls HOWTO” (“IPFILTER”)
1023	“IPMI – Intelligent Platform Management Interface Specification V2.0” (Draft dated 9/15/2003) (“IPMIv2.0”)
1024	Reserved
1025	U.S. Patent No. 7,055,148 (“Marsh”)
1026	Reserved
1027	U.S. Patent No. 6,286,074

Exhibit No.	Description
1028	U.S. Patent No. 6,973,517
1029	U.S. Patent No. 6,189,096
1030	U.S. Patent No. 7,469,298
1031	U.S. Patent No. 6,272,537
1032	IETF Bibtex listing for RFC 3414
1033	IETF Bibtex listing for RFC 1157
1034	IETF Bibtex listing for RFC 2865
1035	IETF Bibtex listing for RFC 1492
1036	U.S. Patent No. 7,496,950
1037	“DSP0114 Alert Standard Format (ASF) Specification (“DSP0114”)
1038	U.S. Patent No. 7,263,716
1039	Declaration of Nathaniel E. Frank-White
1040	WO 01/31849 A1 (“Fowler”)
1041	Reserved
1042	District Court Claim Construction Order dated 5/28/24
1043	U.S. Patent No. 7,269,639 (“Lawrence”)
1044	U.S. Patent No. 8,605,624 (“Desai”)
1045	WO 2004/015764 (“Leedy”)
1046	Declaration of Dr. Sigurd Meldal for IPR2024-00124
1047	U.S. Patent Application No. 10/461,827
1048	Deposition transcript of Prabhat Mishra, Ph.D. taken June 26, 2005
1049	Deposition transcript of Guevara Noubir, Ph.D. taken July 24, 2025
1050	Cisco Systems, “Internetworking Technologies Handbook,” Third Edition

I. INTRODUCTION

Patent Owner Response fails to identify a valid reason why the Board's preliminary finding that the Petition established the unpatentability of all Challenged Claims is incorrect. For Grounds 1-4 based on Neufeld, Patent Owner's ("PO") Response rests on two flawed arguments. First, PO alleges without support that Neufeld discloses only "general purpose VPNs used for network access," and such general purpose VPNs terminate outside the managed device. This first argument is flawed for two reasons. First, nothing in Neufeld supports PO's assertion that Neufeld is limited to general purpose VPNs that terminate outside the managed server. Second, the challenge to claim 1 based on Neufeld is an obviousness challenge based on the use of a point-to-point VPN tunneling technology in Neufeld's system, technology which even PO's expert admits was well-known. PO's argument therefore does not defeat the Petition's assertion of obviousness. PO's second argument that Neufeld is limited to out-of-band remote management communications is contradicted in multiple instances Neufeld. Once PO's flawed arguments are rejected, PO's arguments on Grounds 1-4 collapse, and the Board should find that all Challenged Claims are unpatentable for this reason alone. Grounds 5-9 based on IPMI provide an additional basis for finding all Challenged Claims unpatentable for the reasons discussed below.

II. GROUNDS 1-4 DEMONSTRATE THE UNPATENTABILITY OF ALL CHALLENGED CLAIMS

A. PO Has Waived All Arguments for Grounds 1-4 Other Than Its Arguments on Limitation [1.c]

Patent Owner's Response (the "POR") contests only one portion of one limitation of claim 1: a portion of limitation [1.c], "wherein said virtual management interface connection means provides logical separation of management data from user data and utilizes interfaces of said managed network element for connecting said one or more network services or remote users with said secure management access controller." Because the POR has not presented any other argument for Ground 1 (POR at 22-38, Section IV.A), and because PO relies only on its Ground 1 arguments for Grounds 2-4 (POR at 38-39, Sections IV.B-D), all other arguments for Grounds 1-4 should be deemed to have been waived. Paper 8 (Scheduling Order), at 9.

B. PO's Arguments on Neufeld Are Flawed

PO makes two related arguments regarding Neufeld's disclosure: PO argues that (1) Neufeld's system is limited to general purpose VPNs, and (2) Neufeld's system is limited to out-of-band communication of remote management messages. Both of these arguments are wrong. Because argument (1) appears to rely in part on argument (2), the latter is addressed first herein.

1. Neufeld Is Not Limited to Out-of-Band Communications

a. Neufeld Discloses or Renders Obvious In-Band Communication of Remote Management Messages

Neufeld discloses or at least renders obvious in-band communication of remote management messages between Neufeld's remote management PC 5 and managed server 3 over a network N, which is the same network over which Neufeld's user data travels.

Neufeld's "Background of the Invention" section distinguishes between in-band remote management communications, which take place over a server's "normal" network connection, and out-of-band remote management communications, which do not take place over a server's normal connection to the network. EX1005, ¶¶[0011]-[0012]. Neufeld then notes that remote management messages can occur while the managed server is on-line or off-line. EX1005, ¶[0014]. As a result, Neufeld defines four types of remote management communications: (1) in-band online; (2) in-band offline; (3) out-of-band online; and (4) out-of-band offline. After defining these four types of remote management communications, Neufeld discloses in the very next paragraph that it is "highly desirable" to have a network management tool that is capable of all four of these types of communication:

An **important goal** in the development of remote server management tools is to increase the number of server problems

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

EX1005, ¶[0015] (emphasis added). Neufeld further discloses that the then-current state of the art included servers that hosted dedicated remote management computer systems and highlights the “deep information gathering capability” available (only) when the OS of the managed server is online, and thus available through in-band communications:

Current remote management solutions combine the advantages of deep information gathering capability (software agent-based information gathering technology available when the OS of the managed server is online) with the ability to control operation of the managed sever independently via an out-of-band communication session using the **dedicated server management computer system hosted in the managed server.**

EX1005, ¶[0016] (emphasis added).

Consistent with the foregoing disclosures, Neufeld discloses a system with both in-band and out-of-band communications between a remote management PC

and a managed server that includes a dedicated server management computer system hosted in the managed server, referred to in Neufeld as a “remote management controller” (“RMC”). A block diagram of an exemplary remote server 3 including an RMC 116 is shown in Fig. 2 of Neufeld:

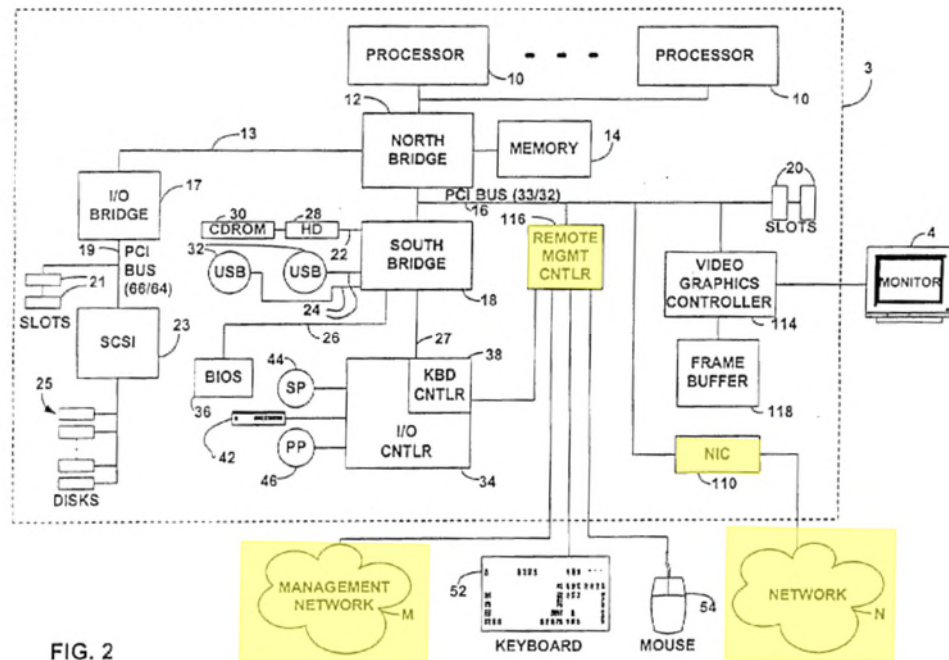


FIG. 2

The server 3 is connected to a remote management PC 5 via both a network N and management network M as shown in Fig. 1:

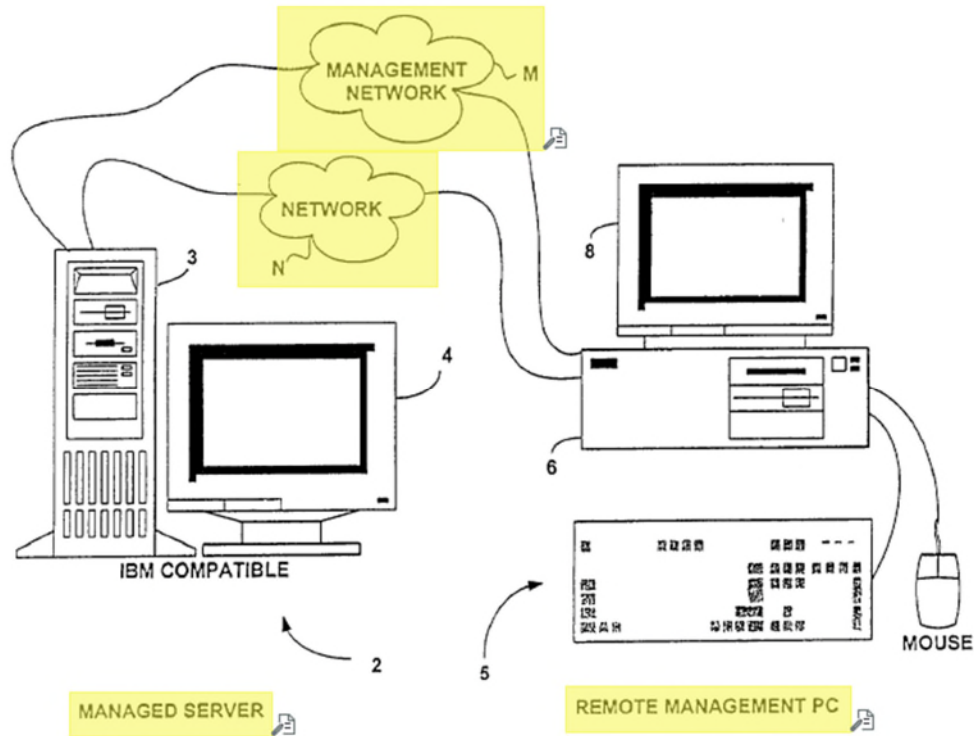


FIG. 1

Network N, which is connected to the server 3 via the NIC 110 as shown in Fig. 2, is the connection to the server 3 over which user data travels and can be an Internet connection, whereas network M is a separate remote management network, EX1005, ¶¶[0035], [0061]. Thus, communications between the remote management PC 5 and the managed server 3 via network N are in-band remote management communications, and communications between the remote management PC 5 and the managed server 3 via network M are out-of-band remote management communications as those terms are used in the '016 patent.

Consistent with Neufeld's above-discussed disclosures in ¶¶[0015]-[0016], and directly contrary to PO's assertion that Neufeld is limited to only out-of-band

remote management communications, Neufeld discloses that the RMC 116 can communicate with the remote management PC 5 via **both** network N and network M in order to remotely access, interact and monitor the managed server:

Further attached to the PCI bus 16 is a remote management controller 116. The remote management controller 116 connects to the keyboard controller 38, **the network N and/or a management network M**, a keyboard 52, and a mouse 54 *to provide functionality for accessing, interacting, and monitoring the managed Server 2 from the remote console 5* as will be more fully described below.

EX1001, ¶[0043] (emphasis added). Consistent with this statement, Neufeld further discloses that the “remote management controller 116 also includes circuitry to route keystrokes to the keyboard controller 38 from either the remote console 5 via the modem or NIC 110 which may be coupled to the network M.”

EX1001, ¶[0047]. While this passage mistakenly states that the NIC 110 is coupled to the network M, Fig. 2 shows the NIC 110 coupled to the network N and understanding this sentence as referring to network N is consistent with ¶¶[0015] and [0043].¹ This statement discloses remote management communications from

¹ Unlike IPR2024-00109, neither PO nor its expert Dr. Noubir assert here that this error sentence would not be understood by a POSITA as meaning that “remote management controller 116 also includes circuitry to route keystrokes to the keyboard controller 38 from either the remote console 5 via the modem or NIC 110

the remote console 5 to the RMC 116. The very next paragraph discloses that the RMC 116 transmits video to the remote management PC 5 via the NIC 110.

¶[0048]. NIC 110 is only connected to the Network N for in-band communication and has no connection to the management network M. EX1001, Fig. 2. Thus, Neufeld explicitly discloses remote management communications between the remote management PC 5 and the RMC 116 via the Network N and NIC 110. At a minimum, the aforementioned disclosures in Neufeld render these communications obvious.

b. PO's Argument that Neufeld Is Limited to Out-of-Band Communications Is Clearly Wrong

Contrary to Neufeld's express disclosures discussed above, PO and its expert assert that there are no in-band remote communications via network N and NIC 110 between the remote management PC 5 and the RMC 116 in Neufeld's system. POR, 27-28; EX2006, ¶[0045]-[0047] and ¶[0060]; EX1049 (Noubir Tr.), 55:17-56:10; 60:6-20. Each of PO's arguments in support of this flawed position fails for the following reasons.

which may be coupled to the network N.” To the extent that the Board considers such an argument in this IPR, Petitioner respectfully requests that the Board also consider Petitioner's arguments to the contrary in Petitioner's Reply in IPR2024-00109.

PO and its expert ignore Neufeld's teaching in ¶[0015] that in-band online remote management communication is "highly desirable" and instead focus on Neufeld's discussion of the capability of the RMC 116 to operate even before the OS is loaded using out-of-band communications. The plain truth is that in-band and out-of-band communications are not mutually exclusive options. A system that is capable of both in-band and out-of-band communications has all of the capabilities of an out-of-band only system, and neither PO nor its expert offer any explanation why a POSITA would not choose to implement a system with both forms of communication as taught by Neufeld. Indeed, when Dr. Noubir was asked at his deposition whether he would have wanted a managed server to have the capability to perform both in-band and out-of-band communications due to the possibility that the out-of-band network might become inoperative, he gave the only answer any reasonable person could: "of course." That he then dissembled about not seeing that disclosure in Neufeld and including in-band capability required tradeoffs did nothing to detract from this admission. EX1049, 71:8-72:10.

In discussing in-band remote management communications, Neufeld acknowledges that "[i]n-band communication with the server is, accordingly, only possible when the server is able to communicate over its normal network connection" and "[p]ractically speaking, this limitation restricts in-band communications to times when the OS of the managed server is operational

(online).” EX1005, ¶¶[0011]. While this statement is true, it is not a reason to exclude in-band communication of remote management messages. Neither this passage nor any other in Neufeld states that communication of remote management data between RMC 116 and the remote management PC only occurs when the OS is offline. In fact the opposite is true. *See* EX1005, ¶¶[0073]-[0074] (discussing use of IOP 156 in RMC 116 to create a virtual communications device to allow communications between remote management PC 5 and OS of the managed server). The POR refers to the passage at [0011] and argues that the management network M is the only network coupled to any of the communication interfaces of the RMC 116 (POR, 28) but ignores that Neufeld’s ¶[0043] states that the RMC 116 is coupled to NIC 110 which is connected to network N.

PO’s expert argues that “Neufeld is focused on solutions for remote server management when the managed server is powered down or while the OS is offline” and “since the proposed management solution in Neufeld operates before the OS is loaded, it cannot be using in-band communication, which is only usable when the OS of the managed server is operable.” EX2006, ¶[0059]. This argument ignores that while Neufeld may be “focused” on out-of-band communications, Neufeld’s “proposed management solution” operates *both* before the OS is loaded *and* after it is loaded, and thus nothing precludes the use of in-band remote

management communications at times the OS is loaded as discussed in Neufeld at ¶¶[0015], [0043], and [0073]-[0074].

PO's expert also attempts to explain away the disclosure in Neufeld's ¶[0043] that the RMC 116 is connected to the network N to provide functionality "for accessing, interacting and monitoring the managed server 2 from the remote console 5" as meaning only that the RMC is connected to the PCI bus to which the NIC 110 is connected to "passively monitor" data on network N but "that connection does not equate to active participation in the data transmission or use of the primary network interface for management communication." EX2006, ¶47. That opinion directly contradicts Neufeld's disclosure at ¶[0048] that the IOP 156 of the RMC 116 actively transmits video graphics data to the remote console 5 via the NIC 110 (which is only connected to network N), and Neufeld's disclosure in ¶[0047] of remote management communications via NIC 110 and network N from the remote console 5 to the RMC 116.

In support of his opinion in EX2006 ¶47 that remote management communications do not occur via network N, Dr. Noubir states without support that "Neufeld expressly states that the remote management controller communicates externally through a dedicated interface, such as Ethernet interface 180, and that the entire system is purposefully designed to operate independently of any software on the managed server." EX2006, ¶47. Neither is true. What

Neufeld says as acknowledged in EX2006, ¶46 is that the “Ethernet interface 180 provides **the main communication interface** between the remote server management controller 116 and the outside world.” EX2006, ¶46 (emphasis in original) (citing EX1005, ¶[0061]). That passage does *not* state that the RMC 116 **only** communicates through a dedicated interface or that the Ethernet interface 180 is the **only** interface to RMC 166. The passage states only that Ethernet interface is the **main** interface and therefore does not preclude the communications and connections discussed in Neufeld at ¶¶[0043], [0047], and [0048]. Dr. Noubir’s statement in EX2006 ¶47 that “the entire system is purposefully designed to operate independently of any software on the managed server” is unsubstantiated and appears nowhere in Neufeld. This statement also ignores the simple truth that Neufeld’s out-of-band communications provide the capability to operate independently of the operating system and that this capability is also present in a system that supports both out-of-band and in-band management communications as taught by Neufeld. The more accurate characterization is that Neufeld’s system is purposefully designed to have the capability to operate independently **in the absence of OS support**, providing a support system that functions both when the OS is running (employing in-band communication means and out-of-band communications as warranted) and when it is not (employing out-of-band

communications). EX1005, ¶¶[0043], [0047], [0048] (in-band) and [0034], [0043], [0052] (out of band).

At his deposition, Dr. Noubir repeatedly referred to “inconsistencies” in Neufeld. E.g., EX1049 at 51:18-23; 55:2-25; 56:16-17; 64:3-8; 65:15-25. These “inconsistencies” are imaginary and result from improperly extrapolating disclosures in Neufeld. One example of such an improper extrapolation is the assertion that the disclosure of the dedicated Ethernet interface 180 being the main interface by which the RMC 116 communicates with the outside world means that the RMC only communicates with the outside world via dedicated interfaces and/or only via the Ethernet Interface 180, as discussed above. Another example is extrapolating the disclosure of Neufeld’s capability of utilizing out-of-band communications that operate independently of the OS to mean that Neufeld’s system only utilizes out-of-band communications that operate independently of the operating system and/or when the OS is not operating. The assertion that Neufeld’s “entire system is purposefully designed to operate independently of any software on the managed server” discussed in the previous paragraph is still another example. The plain fact is that Neufeld consistently discloses that its system utilizes both in-band and out-of-band communications. Doing so is beneficial at least because it provides some remote management capability even if the management network cannot be used as discussed herein, and PO provides no

credible reason why this additional “highly desirable” capability would be excluded from Neufeld’s system. The only actual inconsistency here is Dr. Noubir’s assertion that Neufeld’s system does not utilize both forms of communication in the face of multiple express disclosures in Neufeld that it does.

For all of the reasons discussed above, Neufeld discloses or at least renders obvious the receipt of in-band remote management commands from the remote management PC 5 at the RMC 116 via the network N. PO’s and Dr. Noubir’s assertions are contrary to Neufeld and should be rejected.

2. The Use of a Point-to-Point VPN Is Obvious Over Neufeld

The Petition explains how and why a POSITA would have found it obvious in view of Neufeld’s disclosures of the use of VPNs for remote management communication to implement in Neufeld’s managed server a point-to-point VPN utilizing L2TP and IPSec technology to create a secure tunnel for remote management communications to/from Neufeld’s remote management PC 5 and RMC 116. Petition, 32-34, citing EX1046, ¶¶109-115. The POR does not dispute that L2TP and IPSec technology were well-known to a POSITA, and Dr. Noubir admitted that they were. EX1049, 48:2-19; EX2009, 23; *see also* EX1050 at 3-5 (2001 Handbook discussing VPN tunnel using L2TP and IPSec). The POR also does not assert that providing such a secure point-to-point tunnel using L2TP/IPSec VPN technology between the remote management PC 5 and the

managed server or the RMC 116 was not possible. To the contrary, Dr. Noubir admitted at his deposition that providing VPN tunnels with individual computers as endpoints was possible. EX1049, 48:25-50:8.

The use of such a point-to-point VPN for remote management traffic with that VPN traffic transiting Neufeld's NIC 110 as discussed in the Petition satisfies both the "logical separation of management data from user data" and "utilizes user interfaces of said managed network element" requirement of limitation [1.c]. The POR admits as much at 33: "such a VPN would theoretically separate management data (from the remote management PC 5) from all other network data passing through the network N." This admission is consistent with the '140 patent, which identifies the VPN as providing the claimed logical separation. EX1002, 7:1-3.

Instead of addressing the obviousness of a point-to-point VPN as alleged in the Petition, the POR latches onto three sentences in Neufeld to allege that Neufeld discloses only accessing networks using general purpose VPNs that terminate outside of a managed device. POR, 25. Even assuming that this assertion were true (it is not as discussed below), it ignores the fact that the Petition alleges that limitation [1.c] would have been obvious over Neufeld. Petition at 33 ("a POSITA would have found it obvious to use 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 with the remote PC 5.”)

Further, Neufeld does not state that the VPNs are “general purpose VPNs” or that they terminate outside the managed server 2 as alleged by the POR. The three bullet-pointed sentences on which the POR relies (POR, 25) do not support this assertion. The first sentence in Neufeld at ¶[0009] is in Neufeld’s Background section and simply discusses the wide variety of topologies and networks known in the art, including LANs, WANs and MANs, and then states that VPNs “may” be used to access those networks. PO reads far too much into this sentence. This sentence neither describes the VPN as “general purpose” nor states that the VPN terminates outside of a managed server. The statement that such VPNs “may” be used to access the networks is not indicative of where the endpoint of the VPN is located. A client at a remote management PC that uses a point-to-point VPN that traverses the Internet and terminates inside the managed server 2 is accessing the Internet. And even if PO’s extrapolations were correct, that this sentence uses “may” means it would not preclude point-to-point VPNs as discussed in the Petition. The other two bullet-pointed sentences are even less specific, and also neither state that any VPN is “general purpose” nor indicate where any VPN terminates. The sentence from ¶[0022], which refers to a VPN to “access the system” actually contradicts PO’s first point because the “system” in that sentence

is clearly the managed server rather than any network. The final bulleted sentence from ¶[0088] relied on in the POR at 25 similarly refers to “remote connections, such as via the Internet or via a virtual private network,” and the next sentence of ¶[0088] (which PO ignores) refers to “access to the managed sever 2” rather than to a network. PO’s assertion that these sentences in Neufeld somehow preclude or indicate something other than a point-to-point VPN as discussed in the Petition therefore fails.

PO next bootstraps its erroneous interpretation of Neufeld’s VPN disclosures by arguing that employing a point-to-point VPN as discussed in the Petition would require substantially redesigning the system to move the VPN endpoint inside Neufeld’s managed controller 116 and rearchitecting interfaces to match the claimed configuration. POR, 26. The notion that Neufeld discloses (let alone is limited to) a VPN endpoint outside the managed server 2 is false as discussed above, and the “rearchitecting interfaces” assertion, while not clear, appears to be based on PO’s mistaken belief that Neufeld does not disclose in-band communication of remote management messages, which is wrong as discussed above. The POR goes on to assert that the use of a point-to-point VPN as discussed in the Petition for limitation [1.c] is “economically and technically prohibitive, as recognized in the ’140 patent itself.” POR, 26 (citing ’140 patent, EX1002, at 9:26-36. That assertion fails because (1) nowhere in the cited passage of EX1002 is

there any discussion of any technical issue and Dr. Noubir has admitted that this solution was possible as discussed above, and (2) because the unsubstantiated assertion that it has been considered too expensive to implement does not make the solution unobvious. Moreover, self-serving statements in the '140 patent cannot be relied on to establish non-obviousness and PO offers no authority to the contrary. PO's characterization of the Petition's implementation of limitation [1.c] as contrary to Neufeld's teachings and requiring a "complete overhaul" are incorrect. The POR's citations to Federal Circuit case law at 26-27 are therefore inapposite because they are based on those incorrect beliefs, assertions, and characterizations.

C. The Petition's Reasoning Is Sound Under Federal Circuit Precedent

PO's arguments about flaws in the Petition's reasoning are based on its assertions that Neufeld only discloses or is limited to a "general purpose VPN" and Dr. Meldal does not disclose any explanation or analysis to explain how the "logical separation" and "interface utilization" features of limitation [1.c] are rendered obvious. However, as discussed above, Neufeld neither discloses nor is it limited to general purpose VPNs. Moreover, Dr. Meldal explained why a POSITA would have found it obvious to utilize a point-to-point VPN for remote management communications between the remote management PC 5 and RMC 116, and how the logical separation and interface utilization features of limitation [1.c] are present when such a point-to-point VPN is used for such communications.

EX1046, ¶¶108-115. Any opinion Dr. Noubir may have to the contrary is suspect because Dr. Noubir admitted in his deposition that he never even read Dr. Meldal's declaration. EX1049, 43:9-44:18. The other arguments in the POR at 35-38 simply rehash PO's arguments discussed above and fail for the same reasons.

Accordingly, PO has not provided any sound basis for the Board to reverse its preliminary conclusion as set forth in the Institution Decision (Paper 7, the "ID") that Grounds 1-4 of the Petition establish the obviousness of all Challenged Claims. The Board should issue a final written decision indicating the same.

III. GROUNDS 5-9 DEMONSTRATE THE UNPATENTABILITY OF ALL CHALLENGED CLAIMS

A. The Petition Establishes the Obviousness Using VPNs to Secure In-Band Communication Between Remote Users and a Secure Management Access Controllers

In its ID, the Board rejected PO's arguments that a VPN such as Lawrence's does not provide for logical separation of data, and that including a VPN would completely change the operation controller. ID, 28. The POR provides no sound basis for changing those findings.

The ID did find that the Petition failed to show a rational reason why a POSITA would have combined IPMI and Lawrence. This finding was because the ID viewed the Petition as focusing on IPMI's sideband interface and not addressing having a VPN connect to the remote user, and thus using a VPN to protect management data on Lawrence's sideband interface as asserted in the

Petition would not have been obvious when similar protection was not provided for management data on the external interface. ID at 29, citing Petition at 51-54 and 64-65.

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

module 655 as explained in the Petition at 53-54 is itself an indication to a POSITA that the data at the managed device's generic routing and forwarding module 612 is protected by a management VPN because for the very reason noted in the ID, that doing so would not make sense if the data arriving at the managed device on an external network were not similarly protected. This is entirely consistent with Lawrence's disclosure at 3:43-54 and 4:4-19 that this external traffic is protected by a VPN. Thus, while the focus of the Petition was directed toward the unique aspect of the Fig. 7 embodiment's use of an additional VPN to protect the internal link 711, Petitioner respectfully submits that a fair reading of the Petition and the passages of Lawrence cited therein establish that incoming remote management messages were also protected by a management VPN implemented by Lawrence's VPN module 655.

The ID also found that the Petition does not clearly explain how the VPN connects the claimed secure management access controller with remote users. ID, 29. The remote user is at one of Lawrence's management devices. Thus, the VPNs implemented at the management VPN module 655 that transfer incoming management messages from a management device received via the generic routing and forwarding module 612² (corresponding to IPMI's LAN Controller) over the

² Such management messages may reach the generic routing and forwarding module 612 via a VPN module 656-658 or a core data link 620. Alternatively, the

internal link 711 (corresponding to IPMI's sideband interface) to the router configuration management module 610 (corresponding to IPMI's BMC and the claimed secure management access controller) accomplishes that connection.

The Petition establishes that a POSITA would have found it obvious to combine IPMI and Lawrence including VPN technology as found in Lawrence's management VPN module 655 into IPMI's LAN Controller to protect remote management communications over the entire path from a user at a remote management console over a public network to IPMI's LAN Controller and from the LAN Controller over the sideband interface to the BMC. This combination satisfies all of the requirements of limitation [1.c], including the logical separation and utilizing user interfaces requirements, and the IPMI-Lawrence combination satisfies all other limitations of the Challenged Claims as explained in the Petition.

B. IPMI and Lawrence Render Obvious the Logical Separation of Management Data From User Data

PO's arguments that the logical separation of management data from user data requirement of limitation [1.c] is not obvious over the combination of IPMI and Lawrence are without merit.

management messages may be received via optional management device link 613. EX1043, Fig. 7 and 5:1-47.

PO first argues that IPMI's LAN controller already route packets based on address without Lawrence's VPN module 655 to protect management traffic sent to the BMC over the sideband interface. POR, 41-42. This argument ignores that the motivation for using Lawrence's VPN module to create an additional VPN between the LAN Controller and the BMC via the sideband interface is to protect that management traffic as discussed in the Petition at 55 (citing EX1046, ¶161). PO's argument also ignores the teaching in the '140 patent at 7:1-3 that the logical separation function results from the use of a VPN. *See also* ID at 28 (rejecting PO's argument that a VPN does not provide the claimed logical separation). This first PO argument therefore fails.

PO's second argument is that the Petition's obviousness combination is based on hindsight based on the statement in the Petition at 65:3-9 that Lawrence's VPN technology performs the claimed functions of connecting remote users to the BMC in the IPMI-Lawrence system. POR, 43-44. This discussion in the Petition is simply mapping the proposed IPMI-Lawrence combination to the claims. The motivation for the combination comes straight from Lawrence (i.e., protecting the management traffic on IPMI's sideband interface) as discussed in the Petition at 52-55 and in no way relies on hindsight. PO's second argument also fails.

PO's third argument, phrased in terms of inoperability for intended purpose and changed functionality, boils down to the argument that IPMI's LAN Controller would not be capable of implementing Lawrence's management VPN module 655. POR, 44-47. This argument was rejected in the ID at 28. This argument also ignores that IPMI's LAN Controller is not a conventional LAN Controller, but rather includes "special hardware that enables BMC traffic and system traffic to be interleaved," a disclosure ignored by PO and Dr. Noubir who was referring in his declaration to typical LAN Controllers. EX1012, 49; EX1049, 19:42-20:14 and 22:12-24. In any event, obviousness does not require a showing of bodily incorporation and thus PO's argument that a typical LAN controller cannot perform the functions of Lawrence's management VPN module 655 does not preclude a finding of obviousness. *Allied Erecting & Dismantling Co. v. Genesis Attachments, LLC*, 825 F.3d 1373, 1381 (Fed. Cir. 2016) (quoting *In re Keller*, 642 F.2d 413, 425 (C.C.P.A. 1981)). PO's third and final argument for Ground 5 again fails.

- The POR's arguments as to Grounds 6-9 all depend entirely on its arguments for Ground 1. Thus, the POR provides no meritorious argument that would preclude a finding that Grounds 5-9 establish the unpatentability of all Challenged Claims.

Although not mentioned in the POR, Petitioner notes that Dr. Noubir's declaration includes an argument that IPMI uses the terms "in-band" and "out-of-band" differently from the way they are used in the '140 patent, and that in-band communications between the BMC are not in IP (Internet Protocol) format and thus cannot be used with a VPN which only carries IP format packets. EX2006, ¶¶64-65. However, at his deposition, Dr. Noubir admitted that IPMI discloses that in-band (as that term is used in the '140 patent) remote management messages from an external administrator console are received at IPMI's LAN Controller in IP format and are transferred to the BMC over the sideband interface in IP format. EX1049, 12:23-14:5, 15:12-23. Dr. Noubir's argument at ¶¶64-65 is therefore not relevant to any issue in this IPR and should be disregarded as they were in the POR.

IV. CONCLUSION

All Challenged Claims of the '140 patent should be found unpatentable for the reasons discussed in the Petition and above.

Dated: August 6, 2025

Respectfully submitted,

/James M. Heintz 41,828/

James M. Heintz
Reg. No. 41,828
DLA Piper LLP
One Fountain Square
11911 Freedom Drive, Suite 300
Reston, VA 20190-5602
Phone: + 1 703 773 4000
Fax: + 1 703 773 5000
jim.heintz@us.dlapiper.com

*Attorney for Petitioner Lenovo (United States)
Inc.*

CERTIFICATION UNDER 37 CFR § 42.24(d)

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Reply to Patent Owner response totals 5309 as calculated by Microsoft Word, which is less than the 5600 allowed under 37 CFR § 42.24(c)(i).

Dated: August 6, 2025

Respectfully submitted,

/James M. Heintz 41,828/

James M. Heintz
Reg. No. 41,828
DLA Piper LLP
One Fountain Square
11911 Freedom Drive, Suite 300
Reston, VA 20190-5602
Phone: + 1 703 773 4000
Fax: + 1 703 773 5000
jim.heintz@us.dlapiper.com

*Attorney for Petitioner Lenovo (United States)
Inc.*

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 42.6(e) and 42.105(b), the undersigned hereby certifies that a copy of the foregoing Petitioner's Reply to Patent Owner's Response was served on Patent Owner by emailing a copy of same (by agreement) to the following attorneys of record for the Patent Owner:

Brandon R. Theiss
BTheiss@vklaw.com

Daniel H. Golub
DGolub@vklaw.com

Ryan W. O'Donnell
RODonnell@vklaw.com

Robert D. Leonard
RLeonard@vklaw.com

Russell J. Rigby
rrigby@intven.com

Dated: August 6, 2025

Respectfully Submitted,

/ James Heintz 41,828/

James M. Heintz

Reg. No. 41,828

Attorney for Petitioner Lenovo (United States) Inc.