

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
Patent 7,325,140 B2

Before HYUN J. JUNG, JOHN D. HAMANN, and STEPHENE. BELISLE,
Administrative Patent Judges.

HAMANN, *Administrative Patent Judge.*

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

In this *inter partes* review, Lenovo (United States) Inc. (“Petitioner”) challenges the patentability of claims 1–4, 6, 7, 10–14, and 16 (“the challenged claims”) of U.S. Patent No. 7,325,140 B2 (Ex. 1002, “the ’140 patent”), owned by Intellectual Ventures II LLC (“Patent Owner”). We have jurisdiction under 35 U.S.C. § 6. This Final Written Decision is entered pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73. For the reasons discussed herein, we determine that Petitioner shows by a preponderance of the evidence that the challenged claims are unpatentable.

A. Procedural History

Petitioner filed a Petition requesting *inter partes* review of the challenged claims. Paper 1 (“Pet.”). Patent Owner filed a Preliminary Response. Paper 6. We instituted *inter partes* review of the challenged claims on all grounds raised in the Petition. Paper 7 (“Dec. on Inst.”), 30.

Following institution, Patent Owner filed a Response to the Petition. Paper 9 (“PO Resp.”). Petitioner filed a Reply to Patent Owner’s Response. Paper 11 (“Pet. Reply”). Patent Owner filed a Sur-reply to Petitioner’s Reply. Paper 12 (“PO Sur-reply”). An oral hearing was held on November 19, 2025. A transcript of the hearing is in the record. Paper 20.

B. Real Parties-in-Interest

Petitioner identifies itself and Lenovo Group Ltd. as real parties-in-interest. Pet. 82. Patent Owner identifies itself as a real party-in-interest. Paper 4, 2.

C. Related Matters

The parties identify *Intellectual Ventures II LLC v. Lenovo Group Ltd.*, 6:23-cv-00307-ADA-DTG (W.D. Tex.) as a matter that may affect, or be affected by, a decision in this proceeding. Pet. 83; Paper 4, 2.

D. The Challenged Patent

The '140 patent “relates in general to . . . managing devices or systems in a communication network and more particularly to methods and apparatus for remote management of these devices or systems in a secure manner.” Ex. 1002, 1:19–23. The '140 patent explains that “[i]n distributed computer networks[,] the vast majority of the networking elements are not in the same geographic location or easily accessible by the skilled technicians or network administrators typically responsible for normal maintenance of the elements.” *Id.* at 1:27–31. Thus, “[i]n general, it is not practical to require physical access to the systems for general maintenance or troubleshooting and repair.” *Id.* at 1:39–41. “The costs would be prohibitive, both in time and person[ne]l, to require a skilled technician to be dispatched for every required activity on a system.” *Id.* at 1:41–43. “This has driven a strong requirement to provide for remote management of network elements and servers,” according to the '140 patent. *Id.* at 1:43–45. However, “the security of the network elements and servers is a concern when remote management is allowed.” *Id.* at 1:56–57.

“It is important . . . to realize that opening up a device to remote management allows a larger window for attackers to utilize in an attack,” and thus, “[t]he use and security of remote management must be carefully considered.” *Id.* at 1:64–67. The '140 patent explains that for known ways “to address most of the concerns” of remote management, “[i]t would take a number of different devices configured to work together,” which “would require a number of additional devices in an environment where rack space is very expensive.” *Id.* at 4:1–4.

In response, the '140 patent “provide[s] for the secure management of devices without requiring additional devices taking up additional rack space

by embedding the necessary hardware and software for secure management of the device in the device to be managed.” *Id.* at 4:7–11. More specifically, 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.” *Id.* at 5:48–52. Figure 1 of the ’140 patent is shown below.

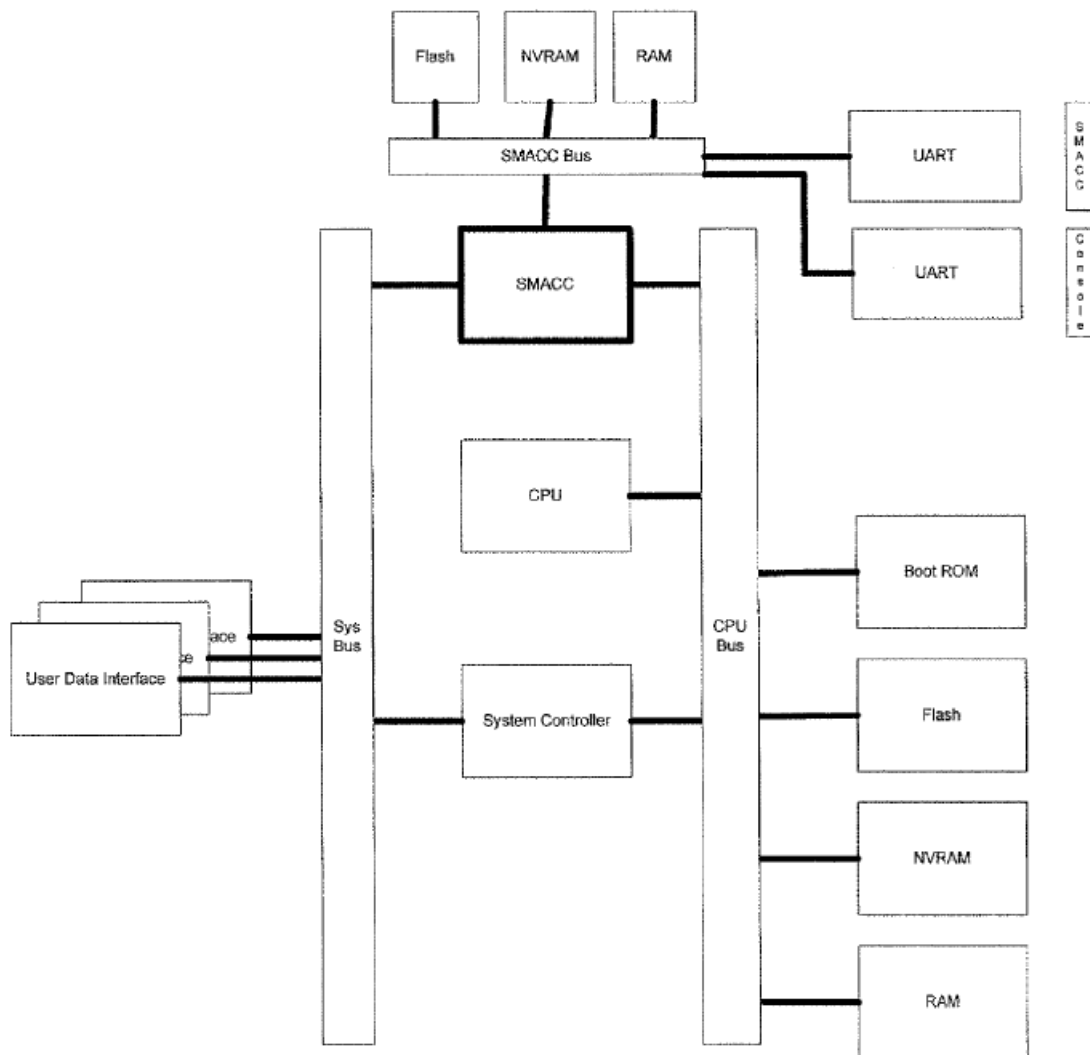


Fig. 1

Figure 1 “is a block diagram for an exemplary embodiment of the embedded SMACC” chipset and “illustrates the positioning of the SMACC chipset

within the managed device.” *Id.* at 9:41–43, 10:64–65. As illustrated, “the SMACC processor has its own flash, Non-Volatile Random Access Memory (NVRAM), and Random Access Memory (RAM) for operating.” *Id.* at 10:66–11:1, Fig. 1. The SMACC is coupled both to the Central Processing Unit (“CPU”) Bus and the System Bus of the managed device. *Id.* at Fig. 1. The System Bus also is coupled to User Data Interfaces for user data traffic. *Id.*

In addition, the ’140 patent discloses that “[r]emote management . . . can be provided in-band ([i.e.,]the remote administrator communicates with the system using the same network as the user data for the managed system).” *Id.* at 1:47–50. Moreover, the managed device can be configured with a Virtual Management Interface (“VMI”), which uses a Virtual Private Network (“VPN”) and “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.” *Id.* at 11:60–67, 12:6–9.

E. The Challenged Claims

Petitioner challenges claims 1–4, 6, 7, 10–14, and 16 in this proceeding. Claim 1 is the sole independent claim. Claim 1 is illustrative of the challenged claims and is reproduced below:

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

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

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

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

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

Ex. 1002, 22:32–57.

F. Instituted Grounds of Unpatentability

We instituted trial based on the following grounds of unpatentability, which are all the grounds of unpatentability raised in the Petition:

Claim(s) Challenged	35 U.S.C. § ¹	Reference(s)/Basis
1–4, 6, 7, 10, 11, 13, 16	103(a)	Neufeld ²
11, 12	103(a)	Neufeld, Syvanne ³
13, 14	103(a)	Neufeld, Fowler ⁴
1–3, 6, 7, 10, 11	103(a)	IPMI, ⁵ Lawrence ⁶
4	103(a)	IPMI, Lawrence, Leedy ⁷

¹ The Leahy-Smith America Invents Act (“AIA”) included revisions to 35 U.S.C. § 103 that became effective on March 16, 2013. Because the ’140 patent issued from an application having a filing date before March 16, 2013, we apply the pre-AIA version of the statutory basis for unpatentability.

² US 2003/0226015 A1, published Dec. 4, 2003 (Ex. 1005, “Neufeld”).

³ US 2003/0097590 A1, published May 22, 2003 (Ex. 1016, “Syvanne”).

⁴ WO 01/31849 A1, published May 3, 2001 (Ex. 1040, “Fowler”).

⁵ IPMI – Intelligent Platform Management Interface Specification V1.5 (Rev. 1.1 dated Feb. 20, 2002) (Ex. 1020, “IPMI”).

⁶ US 7,269,639, issued Sept. 11, 2007 (Ex. 1043, “Lawrence”).

⁷ WO 2004/015764 A2, published Feb. 19, 2004 (Ex. 1045, “Leedy”).

11, 12	103(a)	IPMI, Lawrence, Syvanne
13, 14	103(a)	IPMI, Lawrence, Fowler
16	103(a)	IPMI, Lawrence, RFC1492 ⁸

Pet. 1–2, 21–81. Petitioner submits as evidence the Declaration of Sigurd Meldal, Dr. Scient. (Ex. 1003), the Declaration of Sigurd Meldal, Dr. Scient. (Ex. 1046), and the Declaration of Nathaniel E. Frank-White (Ex. 1039). Patent Owner submits as evidence the Declaration of Dr. Steven Goldberg (Ex. 2001) and the Declaration of Dr. Guevara Noubir (Ex. 2006).

II. LEVEL OF ORDINARY SKILL IN THE ART

To determine whether an invention would have been obvious at the time it was made, we consider the level of ordinary skill in the pertinent art at the time of the invention. *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966). In assessing the level of ordinary skill in the art, various factors may be considered, including the “type of problems encountered in the art; prior art solutions to those problems; rapidity with which innovations are made; sophistication of the technology; and educational level of active workers in the field.” *In re GPAC, Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995) (citing *Custom Accessories, Inc. v. Jeffrey-Allan Indus., Inc.*, 807 F.2d 955, 962–63 (Fed. Cir. 1986)). “[O]ne or more factors may predominate.” *Id.*

In our Decision on Institution, we adopted the definition Petitioner proposes for one having ordinary skill in the art at the time of the invention of the ’140 patent. Dec. on Inst. 7–8. Namely, we found that one of ordinary skill in the art “would have had a Bachelors’ degree in electrical or computer engineering or a comparable field of study, plus approximately two to three years of professional experience in the field of computer and/or

⁸ RFC1492: An Access Control Protocol, Sometimes Called TACACS (July 1993) (Ex. 1013, “RFC1492”).

network design and security or other relevant industry experience,” and that “[a]dditional graduate education could substitute for professional experience, and significant experience in the field could substitute for formal education.” *Id.* (citing Pet. 7–8 (citing Ex. 1046 ¶ 54)). Patent Owner does not address Petitioner’s definition, nor provide its own. *See generally* PO Resp.

Because Petitioner’s definition of the level of skill in the art is consistent with the ’140 patent and the asserted prior art, we maintain it for purposes of this Final Written Decision. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001); *In re GPAC*, 57 F.3d at 1579; *In re Oelrich*, 579 F.2d 86, 91 (CCPA 1978).

III. CLAIM CONSTRUCTION

Because the Petition was filed after November 13, 2018, we apply the same claim construction standard that would be used in a civil action under 35 U.S.C. § 282(b), following the standard articulated in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). 37 C.F.R. § 42.100(b); 83 Fed. Reg. 51,340, 51,340–41, 51,343 (Oct. 11, 2018). In applying such standard, claim terms generally are given their ordinary and customary meaning, as would be understood by a person of ordinary skill in the art, at the time of the invention and in the context of the entire patent disclosure. *Phillips*, 415 F.3d at 1312–13. “In determining the meaning of the disputed claim limitation, we look principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence.” *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17).

Petitioner argues that the “said managed network element,” as recited in claim 1 means “said managed network device.” Pet. 9. Patent Owner does not dispute this construction. We adopt Petitioner’s proposed construction for this term as it appears to be consistent with the Specification’s use of “element” as referring to networked devices, and with the overall claim. *See generally* Ex. 1002.

In addition, Petitioner argues that certain terms are means-plus-function terms, and as such, Petitioner identifies the recited function and its corresponding structure in the Specification. Pet. 9–13. Petitioner states that the proposed functions and structures for these terms are what the district court adopted in the corresponding litigation. *Id.* at 10 (citing Ex. 1042, 2–6).

First, Petitioner argues that “an out of band access connection means” is a means-plus-function term with the recited function being “connecting said one or more network services or remote users with said secure management access controller for management of said network device.” *Id.* at 10. Petitioner argues that the function’s corresponding structure is “one or more of the following networks: a Public Switched Telephone Network (PSTN) (2:45–57, 3:2–4, 12:37–61), an Integrated Services Digital Network (ISDN) (2:45–57), a cellular network (6:14–21, 7:60–62, 12:37–61), an Ethernet network (12:37–61), a wireless network, and/or a Digital Subscriber Line (DSL) (12:37–61, 15:55–60), where the one or more networks use one or more of the following protocols: [Simple Network Management Protocol (“SNMP”)], TFTP, FTP, DNS, SysLog, Telnet, SSH, HTTP, HTTPS, point to point IP, and/or XML (8:30–38).” *Id.*

Second, Petitioner argues that “virtual management interface connection means” is a means-plus-function term with the following recited

functions: “‘connecting said one or more network services or remote users with said secure management access controller’; (ii) ‘provides logical separation of management data from user data,’ and (iii) ‘utilizes user interfaces of said managed network element for connecting said one or more network services or remote users with said secure management access controller.’” *Id.* at 10–11. Petitioner argues that the functions’ corresponding structure is a VPN. *Id.* at 11 (citing Ex. 1002, 6:22–44, 6:63–7:5, 12:5–21).

Third, Petitioner argues that “protection means” is a means-plus-function term having “protecting the management data” as its recited function. *Id.* Petitioner argues that the function’s corresponding structure is “a firewall (E[x.] 1002, 3:49–60), a virtual private network (VPN) (E[x.] 1002, 3:49–60), or a combination of a firewall, VPN, and authentication and authorization applications (E[x.] 1002, 6:22–7:6).” *Id.*

Fourth, Petitioner argues that “monitoring means for monitoring the status of at least one computer network component” is a means-plus-function term having “monitoring the status of at least one computer network component” as its recited function. *Id.* Petitioner argues that the function’s corresponding structure is “a processor performing an algorithm to monitor network components for loss of connectivity by testing the network connection (7:25–44, 17:50–18:4, 18:20–32, 21:13–65, F[igs.] 15–16), or an uninterruptable power supply (UPS) that monitors network components for loss of external power (11:25–46, 18:33–51, 20:36–47, F[igs.] 2 and 17).” *Id.* at 12.

Fifth, Petitioner argues that “a monitoring means for monitoring the status of the network power supply” is a means-plus-function term having “monitoring the status of the network power supply” as its recited function.

Id. Petitioner argues that the function’s corresponding structure is “an uninterruptable power supply (UPS) that monitors network components for loss of power (11:25–46, 18:33–51, 20:36–47, F[igs.] 2 and 17).” *Id.*

Sixth, Petitioner argues that “reporting means for reporting the status of the network power supply” is a means-plus-function term having “reporting the status of the network power supply” as its recited function.

Id. Petitioner argues that the function’s corresponding structure is “a processor performing the algorithm disclosed at 20:24–29 or the algorithm disclosed at 21:3–12.” *Id.* at 13.

Seventh, Petitioner argues that “means for monitoring connection attempts made through the management access controller” is a means-plus-function term having “monitoring connection attempts made through the management access controller” as its recited function. *Id.* Petitioner argues that the function’s corresponding structure is “an Access Control Server (ACS) using protocols to authenticate and authorize access (19:44–64), or a processor running one or more of RADIUS, TACACS+ and/or LDAP (6:22–57, 7:7–24, 15:26–39; *see also* 4:37–40, 8:13–19).” *Id.*

Patent Owner does not set forth any term for construction, nor address Petitioner’s construction arguments. *See generally* PO Resp.

We adopt Petitioner’s proposed constructions for these means-plus-function terms. Petitioner sufficiently identifies the recited functions and the specific portions of the specification corresponding to each recited function. *See* 37 C.F.R. § 42.104(b)(3).

Lastly, we determine that we do not need to construe any other terms to resolve the disputes between the parties. *See, e.g., Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803

(Fed. Cir. 1999)) (“[W]e need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy.’”).

IV. PRINCIPLES OF LAW

“In an [*inter partes* review], the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable.” *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (requiring *inter partes* review petitions to identify “with particularity . . . the evidence that supports the grounds for the challenge to each claim”)). This burden of persuasion never shifts to Patent Owner except in limited circumstances not present here. *See Dynamic Drinkware*, 800 F.3d at 1378 (discussing the burden of proof in *inter partes* review).

A claim is unpatentable under 35 U.S.C. § 103(a) 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 at the time of the invention to a person having ordinary skill in the art. *KSR Int’l Co. v. Teleflex, Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) objective evidence of non-obviousness, if present.⁹ *See Graham*, 383 U.S. at 17–18. When evaluating a claim for obviousness, we also must “determine whether there was an apparent reason to combine the known elements in the fashion

⁹ Patent Owner does not present arguments or evidence of such objective evidence of non-obviousness. *See generally* PO Resp.

claimed by the patent at issue.” *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

V. OBVIOUSNESS OVER NEUFELD

Petitioner argues that Neufeld renders claims 1–4, 6, 7, 10, 11, 13, and 16 obvious. Pet. 21–43. For the reasons that follow, we determine that Petitioner shows by a preponderance of the evidence that Neufeld renders these claims obvious.

A. *Summary of Neufeld*

Neufeld “relates generally to computer security systems and, more particularly, to a technique for providing user profiles.” Ex. 1005 ¶ 2. In particular, Neufeld teaches “[a] security system [which] includes different authentication levels and/or different privileges based on certain criteria.” *Id.* at code (57). “For example, if a user’s identity can be somewhat assured due to the directness of the connection, authentication may be less rigorous than in a situation where the connection is more remote, thus making the user’s identity less assured.” *Id.* Neufeld also teaches that “a user’s privileges may be restricted if the user accesses the system from a remote location or during non-business hours.” *Id.*

B. *Challenged Claim 1*

1. *Remote Device Management Communication System*

Claim 1’s preamble recites “[a] remote device management communication system for securely controlling access to management applications and communications to and from said management applications on network devices in a distributed computer network that includes one or more network services, one or more secure management access controllers, and one or more managed network devices.” Ex. 1002, 22:32–39. We agree

with Petitioner and find that Neufeld teaches claim 1's preamble. Pet. 21–25.

In particular, we agree with Petitioner that Neufeld's Figure 1, shown below, supports that Neufeld teaches this limitation.

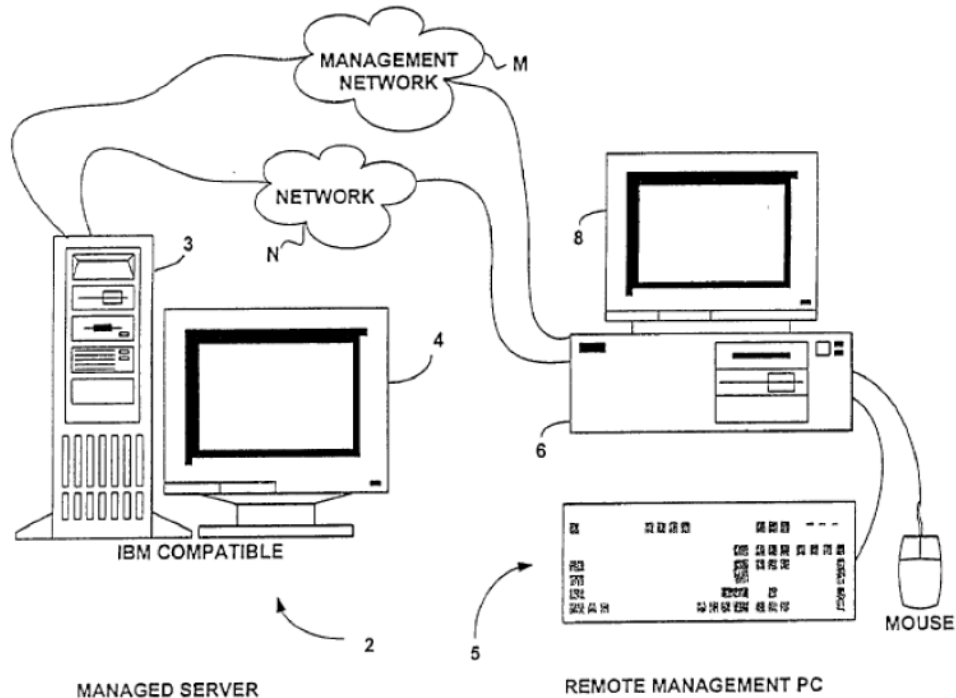


FIG. 1

Figure 1 “is a connection diagram of a managed server and a remote management console according to” Neufeld’s teachings. Ex. 1005 ¶ 25. We agree with Petitioner that Neufeld teaches a remote device management communication system that “includes one or more managed servers 2 [(i.e., the claimed ‘managed network devices’)] connected to a remote console 5 by a network N and a management network M.” Pet. 21 (citing Ex. 1005 ¶ 34, Fig. 1). Moreover, Neufeld teaches that “[t]he network N can be any sort of network capable of transmitting data between two devices.” Ex. 1005 ¶ 35. As illustrated, Neufeld’s managed server 2 includes a CPU 3. *Id.* ¶ 34, Fig. 1.

Neufeld's Figure 2, as annotated by Petitioner, is shown below.
Pet. 23.

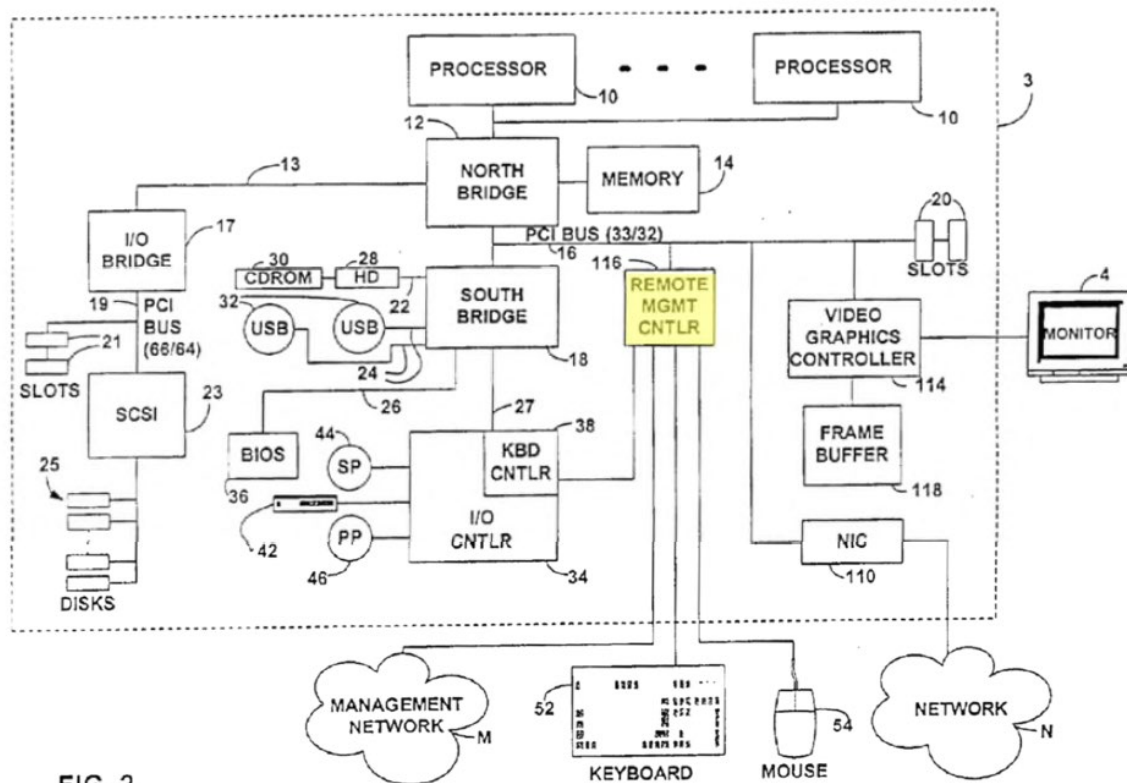


Figure 2 is a block diagram of a managed server for connection to a remote management console according to Neufeld's teachings. Ex. 1005 ¶¶ 25–26. Petitioner annotates this figure by coloring in yellow a remote manager controller 116. Pet. 17; Ex. 1005 ¶¶ 43, 45. We agree with Petitioner and find that CPU 3 houses the remote server management controller 116 (i.e., the claimed “secure management access controller”). Pet. 21–22. In addition, Neufeld teaches that the remote server management controller 116 can be implemented as a single application specific integrated circuit (“ASIC”). Ex. 1005 ¶¶ 50–51.

Neufeld's Figure 3, as annotated by Petitioner, is shown below.

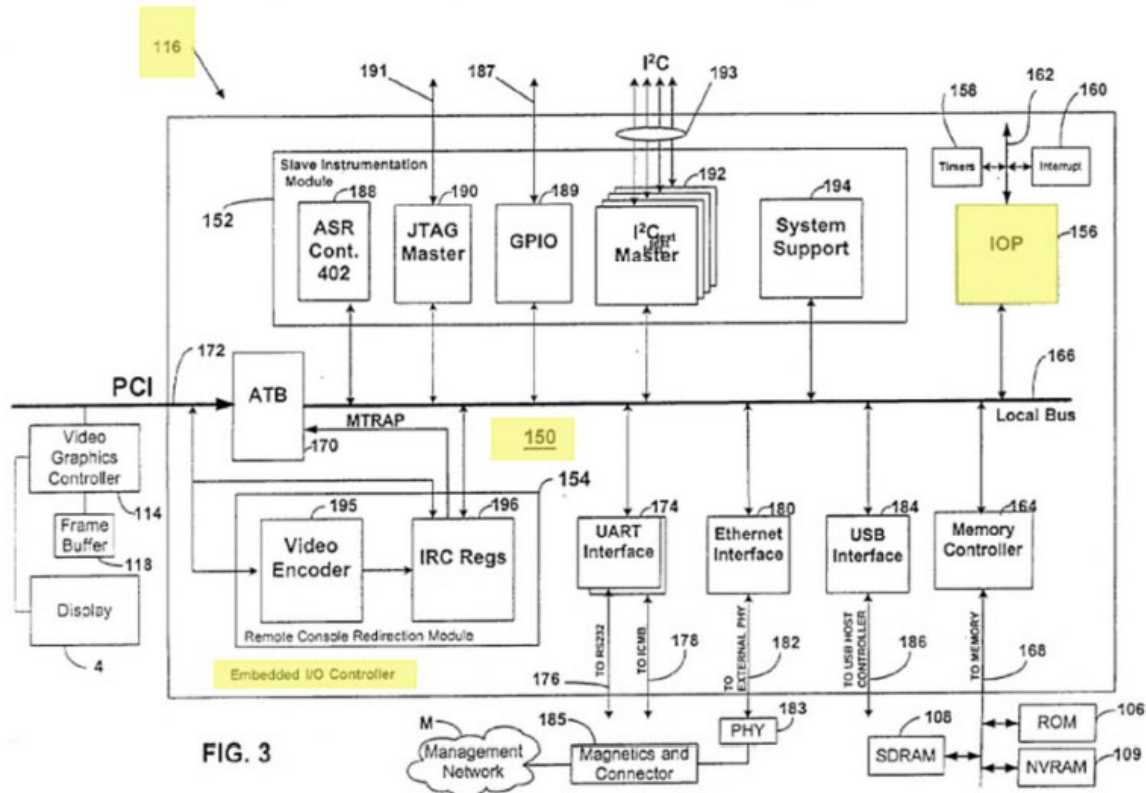


Figure 3 “is a block diagram of [a] remote management controller,” in accordance with Neufeld’s teachings. Ex. 1005 ¶ 27. Petitioner annotates this figure by coloring in yellow (i) the remote management controller’s reference numeral “116,” (ii) label “Embedded I/O Controller” and its reference numeral “150,” and (iii) an Input/Output processor (“IOP”) 156. Pet. 23.

As Petitioner argues, Neufeld’s embedded I/O controller 150 “includes an Input/Output processor (‘IOP’) 156,” which “is coupled to functional modules of the remote server management controller 116,” and “provides general control and functions as a management processor for the remote server management controller 116.” Ex. 1005 ¶¶ 34, 54, Figs. 2–3; Pet. 23. Neufeld teaches that the embedded I/O controller 150 also can be implemented as a single ASIC. Ex. 1005 ¶ 51.

In addition, we agree with Petitioner that Neufeld teaches “[t]he claimed ‘management applications’ [which] are access control and monitoring applications which are performed by the remote server management controller 116 to provide for ‘lights out’ management.” Pet. 23 (citing Ex. 1005 ¶ 76). We also agree that “[t]hese applications on the remote server management controller 116 implement critical functions (e.g., booting and powering down the managed server, modifying flash ROM/firmware), moderately critical functions (e.g., altering user profiles, performing or suppressing backups) and non-critical functions (e.g., file/device sharing, altering directories).” *Id.* at 23–24 (citing Ex. 1005 ¶ 80 & Table 1). Moreover, Neufeld teaches that “the IOP 156 dictates control and monitoring functions in managed server 2,” and “securely controls access to management applications by providing to the network device ‘functionality for accessing, interacting, and monitoring the managed server 2.’” Ex. 1005 ¶ 34.

In addition, we agree with Petitioner and find that “Neufeld’s remote device management communication system controls communications to and from management applications by establishing an ‘out-of-band communication session with the remote server management controller 116.’” Pet. 24 (quoting Ex. 1005 ¶ 59); Ex. 1005 ¶ 12 (“Out-of-band communication . . . is not performed across the managed server’s normal connection to the network,” but instead “a ‘back door’ communication channel is established by a remote server management tool . . . using some other interface with the server (such as . . . an Ethernet interface or the Internet).”).

We also agree with Petitioner that “[t]he claimed ‘distributed network’ includes the devices in networks N and M including the client

computers such as managed server(s) 2 and remote management PC(s) 5 as well as other client computers.” Pet. 25 (citing Ex. 1005 ¶¶ 8, 83). Neufeld further discloses that the network N can include the public Internet, which inherently includes large numbers of servers, client computers, and devices such as routers. Ex. 1005 ¶¶ 35, 88; Ex. 1046 ¶ 96.

In addition, we also agree with Petitioner that Neufeld teaches the claimed “network services,” which include sharing of files and printers, Emergency Management services, directory service, and authentication and encryption services. Pet. 25 (citing Ex. 1005 ¶¶ 7, 74, 76). And we agree with Petitioner and find that “Neufeld discloses that the network N can include the public Internet, which inherently includes network services such as Domain Name Service.” *Id.* (citing Ex. 1005 ¶¶ 35, 88; Ex. 1046 ¶ 97).

After reviewing Petitioner’s arguments and evidence, we find that Petitioner demonstrates by a preponderance of the evidence that Neufeld teaches claim 1’s preamble. In light of our finding, we need not, and thus do not, reach whether claim 1’s preamble is limiting.

2. Secure Management Access Controller

Claim 1 further recites “at least one secure management access controller connected to one or more data bus of said managed network device for the communication of device management data.” Ex. 1002, 22:40–43. We agree with Petitioner and find that Neufeld teaches this limitation. Pet. 25–28; Pet. Reply 3–14.

In particular, we agree with Petitioner that Neufeld’s remote management controller 116 teaches the claimed “secure management access controller,” and Neufeld’s managed server 2 teaches the claimed “managed network device.” Pet. 21–22, 25–26; *see supra* Section V.B.1 (finding that Neufeld teaches these elements). We also agree with Petitioner and find that

Neufeld teaches that the remote management controller 116 is connected to PCI bus 16/172 that is a data bus of the managed server 2 for in-band communication of device management data. Pet. 26–28; Ex. 1005 ¶¶ 15, 43, 45, 58 (the PCI bus 172 “is merely an extension of the PCI bus 16”), Figs. 2–3; Ex. 1046 ¶ 99. We discuss these findings in detail below.

Neufeld’s Figure 1 is shown below.

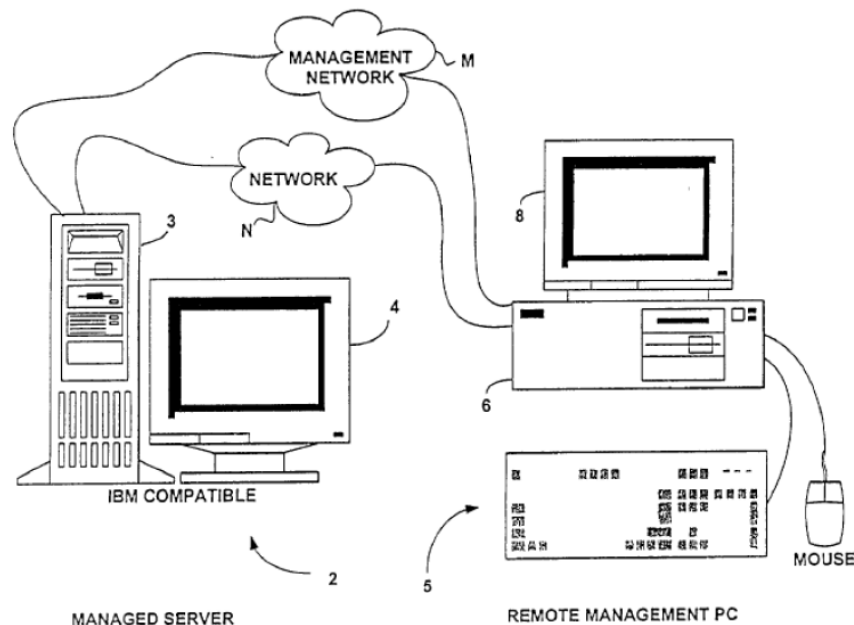


FIG. 1

Figure 1 “is a connection diagram of a managed server and a remote management console according to” Neufeld’s teachings. Ex. 1005 ¶ 25. As illustrated, Neufeld teaches that its CPU 3 of the managed server 2 (i.e., the managed network device) is connected to the remote management PC 5 via the network N. *Id.* at Fig. 1, ¶ 34.

In addition, Neufeld teaches that “[r]emote management tools can communicate with a managed server using either ([1]) in-band communication or (2) out-of-band communication,” where “[i]n-band communication refers to communicating with the server over a standard

network connection, such as the managed server's normal Ethernet connection.” *Id.* ¶ 11; Pet. Reply 3.

We also agree with Petitioner and find that Neufeld teaches “that it is ‘highly desirable’ to have a network management tool that is capable of all four of these types of communication.” Pet. Reply 3–4 (citing Ex. 1005 ¶ 15). More specifically, Neufeld’s paragraph 15 reads as follows:

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*;^[10] (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*.

Ex. 1005 ¶ 15 (emphases added). In other words, Neufeld teaches that it is highly desirable for remote server management tools to be able to control the managed server via an in-band online connection, as well as via other connections. *Id.*

In addition, as Petitioner argues, Neufeld teaches that “[t]he remote management controller 116 connects to . . . *the network N and/or a management network M* . . . to provide functionality for accessing, interacting, and monitoring the managed server 2 from the remote console 5.” Ex. 1005 ¶ 43 (emphasis added); Ex. 1003 ¶ 87; Pet. Reply 6–7. In other words, Neufeld teaches that the remote management PC 5 can

¹⁰ “The term ‘online’ refers to a managed server in which the [operating system (‘OS’)] is up and running,” and “[t]he managed server is said to be ‘offline’ if its OS is not up and running.” Ex. 1005 ¶ 14.

communicate with the remote management controller 116 via network N, as well as network M, to remotely access, interact, and monitor the managed server. Ex. 1005 ¶ 43.

Based on these above teachings¹¹ from Neufeld, we agree with Petitioner and find that Neufeld teaches that its remote management controller 116 is connected to the managed server 2's PCI bus 16/172 for in-band communication of management data over network N (via the NIC 110) from a remote management PC 5. See Ex. 1005 ¶¶ 11–12, 15, 34–35, 43, Figs. 1–2; Ex. 1046 ¶ 100.

We find unavailing Patent Owner's arguments¹² that Neufeld teaches “a system architecture where *management data is not communicated over network N at all.*” PO Resp. 27–28 (citing Ex. 2006 ¶¶ 47, 59). Similarly, Patent Owner argues that “Petitioner fails to realize that *all management data in Neufeld is transmitted over the management network M.*” *Id.* at 28. But as we find above, Neufeld teaches in-band communication (via network N) for management data, as well as out-of-band communication (via network M). See Ex. 1005 ¶¶ 11–12, 15, 34–35, 43, Figs. 1–2. And we do

¹¹ The parties also dispute whether paragraph 47 teaches using in-band communication. In particular, the parties agree that paragraph 47 has a typographical error, but dispute what correction one of ordinary skill in the art would have understood is needed. See, e.g., Pet. Reply 7–8 & n.1; PO Sur-reply 17–18. We do not reach this issue because we find that Neufeld's other teachings that we discuss establish by a preponderance of the evidence that Neufeld teaches in-band communication for remote management.

¹² Patent Owner's arguments regarding whether Neufeld teaches in-band communication of management data are made in the context of a later limitation (PO Resp. 27–35; PO Sur-reply 11–23), but we choose to address these arguments for this limitation, which is directed to such in-band communication.

not credit Dr. Noubir's cited testimony on this issue as it is contrary to these teachings of Neufeld.

We also find unavailing Patent Owner's arguments concerning Neufeld's teachings of using out-of-band communication to provide remote management for the managed server. *See, e.g.*, PO Resp. 30–32. There is no dispute that Neufeld teaches such out-of-band embodiments, but Petitioner also focuses on Neufeld's in-band teachings and how they relate to claim 1. Moreover, we agree with Petitioner that Neufeld teaches that in-band and out-of-band communication for remote management are not mutually exclusive, and having both is highly desirable. *E.g.*, Pet. Reply 9; Ex. 1005 ¶ 15.

We also find unavailing Patent Owner's arguments regarding what Neufeld purportedly “is primarily about” or “as a whole is directed toward” or its “overall intent” or “express purpose.” PO Sur-reply 13–15, 18. These arguments incorrectly do not consider all of what Neufeld teaches. *See EWP Corp. v. Reliance Universal Inc.*, 755 F.2d 898, 907 (Fed. Cir. 1985) (“A reference must be considered for everything it *teaches* by way of technology and is not limited to the particular *invention* it is describing and attempting to protect.”); *In re Applied Materials, Inc.*, 692 F.3d 1289, 1298 (Fed. Cir. 2012) (“A reference must be considered for everything that it teaches, not simply the described invention or a preferred embodiment.”). As we discuss above, Neufeld also teaches using in-band communication for remote management.

We also find unavailing Patent Owner's arguments that amount to arguing that Neufeld teaches away from using in-band communication for remote management. PO Resp. 28; PO Sur-reply 18. For example, Patent Owner's argument that Neufeld teaches that “[i]n-band communication with

the server is . . . only possible when the server is able to communicate over its normal network connection,” which “restricts in-band communication to times when the OS of the managed server is operational.” PO Resp. 28 (quoting Ex. 1005 ¶ 11). Similarly, Patent Owner argues that, as shown in Figures 2 and 3, only network M is directly coupled to remote management controller 116, which “enabl[es] remote and secure connection independent of the OS.” PO Sur-reply 18 (citing Ex. 1005, Figs. 2–3). We disagree with Patent Owner that Neufeld criticizes using in-band communication for remote management so as to discourage its use. Ex. 1005 ¶¶ 11–12; *In re Fulton*, 391 F.3d 1195, 1201 (Fed. Cir. 2004) (teaching away requires that a reference “criticize, discredit, or otherwise discourage” investigation into the claimed solution). At most, Neufeld teaches that out-of-band communication may be preferable, which is insufficient for teaching away. Ex. 1005 ¶ 12; *Galderma Labs., L.P. v. Tolmar, Inc.*, 737 F.3d 731, 738 (Fed. Cir. 2013) (“A reference does not teach away . . . if it merely expresses a general preference for an alternative invention but does not criticize, discredit, or otherwise discourage investigation into the invention claimed.”) (citation omitted); *Merck & Co. v. Biocraft Labs., Inc.*, 874 F.2d 804, 807 (Fed. Cir. 1989) (quoting *In re Lamberti*, 545 F.2d 747, 750 (CCPA 1976)) (“[I]n a section 103 inquiry, ‘the fact that a specific [embodiment] is taught to be preferred is not controlling, since all disclosures of the prior art, including unpreferred embodiments, must be considered.’”). In fact, as we discuss above, Neufeld teaches that it is highly desirable also to have in-band communication for remote management. Ex. 1005 ¶ 15.

We also find unavailing Patent Owner’s argument that Neufeld teaches that “[t]he Ethernet interface 180 provides the main external communication interface between the remote server management controller

116 and the outside world.” PO Resp. 30 (quoting Ex. 1005 ¶ 61). Neufeld explains that “this connection is typically used to couple the remote management controller 116 to the management network M” (i.e., an out-of-band connection). Ex. 1005 ¶ 61. And again, there is no dispute that Neufeld also teaches out-of-band embodiments. But, we agree with Petitioner that Patent Owner overreads this teaching to argue that Neufeld’s teachings are limited to out-of-band communication. Pet. Reply 11. This paragraph of Neufeld states that “Ethernet interface 180 provides the *main* external communication interface),” which at least suggests that it is not the only interface. Ex. 1005 ¶ 61 (emphasis added). And as we discuss above, Neufeld teaches that remote console 5 connects via network N to the managed server. *See, e.g.*, Ex. 1005 ¶ 43, Fig. 1.

We also find unavailing Patent Owner’s argument that paragraph 43 “is describing the hardware-level connections that enable the remote management controller 116 to perform passive out-of-band monitoring of the server—not active in-band communication.” PO Resp. 30. Rather, we agree with Petitioner that paragraph 43 is not so limited. Pet. Reply 7. It includes that “[t]he remote management controller 116 connects to . . . the network N . . . to provide functionality for accessing, interacting, and monitoring the managed server 2 from the remote console 5.” Ex. 1005 ¶ 43. Thus, Neufeld teaches that the remote console 5 (i) can connect to the remote management controller 116 via network N—(in-band communication)—and (ii) access and interact with the managed server 2—which provides management data. *Id.*

We also find unavailing Patent Owner’s argument that paragraph 43’s “reference to network N is simply identifying that the remote management controller is able to snoop on the data being sent/received by/to the managed

device via the network N.” PO Resp. 31. But Patent Owner does not identify any portion of Neufeld that teaches snooping data sent or received by the managed device via the network N. Patent Owner incorrectly conflates monitoring and snooping, despite the separate teachings of paragraphs 43 and 47. In particular, as we discuss above, paragraph 43 teaches that the remote console 5 can monitor the managed server 2, which thus requires a network connection. Ex. 1005 ¶ 43. On the other hand, Neufeld’s discussion of snooping relates to circuitry for snooping the PCI bus for transactions between processor 10 and the video graphics controller, all of which are within the network device, rather than snooping network traffic. Ex. 1005 ¶ 47.

In addition, we find inapposite Patent Owner’s argument that paragraph 43 “inform[s] a person of ordinary skill in the art that the remote management controller 116 is physically connected to system components, such as the PCI bus and keyboard controller, which allow it to snoop on system activity . . . without relying on or interfering with the host operating system.” PO Resp. 30–31. But this argument does not account for paragraph’s 43 teaching of networks M and N and that the monitoring is of the managed server from the remote console. *Id.* And snooping within a network device is inapposite to claim 1.

We also find unavailing Patent Owner’s argument that “[f]rom paragraph [43] and F[igure] 2, alone, Neufeld’s intention is un-clear,” in that paragraph 43 “states that the [remote management controller] connects to one, the other, or both, of [n]etwork N and/or M, but F[igure] 2 only shows the [remote management controller] connected to the management network M, and not N.” PO Sur-reply 16. We disagree that these Neufeld teachings are unclear or that Figure 2 does not show that the remote management

controller is connected to network N. Figure 2 shows that remote management controller 116 connects with network N via the PCI bus 16 and the NIC 110. *See* Ex. 1005, Fig. 2. In addition, Neufeld teaches that attached to the PCI bus 16 is remote management controller 116 and NIC 110. *Id.* ¶¶ 43, 45. Moreover, Figure 1 makes clear that remote console 5 is connected to the managed server 2 via network N. *Id.* at Fig. 1; *see also id.* ¶ 34 (“Referring first to F[igure] 1, there is illustrated a managed server 2 connected to a remote console 5 by a network N.”). Reading Neufeld as a whole, it is clear that paragraph 43 teaches that the remote console 5 (i) can connect to the remote management controller 116 via network N and (ii) monitor, access, and interact with the managed server 2. *Id.* ¶ 43.

We also find unavailing Patent Owner’s argument that Figures 2 and 3 do not show that network N is directly coupled to the remote management controller. PO Sur-reply 11. Patent Owner does not explain the basis for this argument. To the extent that it is based on the operating system or being online, we discuss above why such arguments are unavailing when we discuss teaching away. Similarly, we find unavailing Patent Owner’s argument that “F[igure] 3 also shows the [remote management controller] only coupled to the network M.” *Id.* at 18. This does not negate Neufeld’s teaching of using in-band communication for management data that we discuss above.

We also find unavailing Patent Owner’s arguments that Neufeld’s teachings as to in-band communication of management data are ambiguous or contradictory, or require inferences to be made. PO Sur-reply 11–12, 14. We disagree. As we discuss above, Neufeld teaches using in-band

communication for management data. *See* Ex. 1005 ¶¶ 11–12, 15, 34–35, 43, Figs. 1–2; Ex. 1046 ¶ 100.

We also find unavailing Patent Owner’s arguments based on Dr. Noubir’s testimony that Neufeld has ambiguities and inconsistencies. PO Sur-reply 19–22 (citing Ex. 1049,¹³ 56:16–59:17). This testimony is inconsistent with Neufeld’s teachings for in-band communication of management data that we discuss above. And we thus give the testimony little to no weight.

In sum, we find that Petitioner demonstrates by a preponderance of the evidence that Neufeld teaches this limitation.

3. *Out-of-band Access Connection Means*

Petitioner argues that Neufeld teaches “an out-of-band access connection means for connecting said one or more network services or remote users with said secure management access controller for management of said network device,” as recited in claim 1. Pet.28–32. As we conclude above, “an out of band access connection means” is a means-plus-function term (i) with the recited function being “connecting said one or more network services or remote users with said secure management access controller for management of said network device,” and (ii) the corresponding structures for performing this function including “an Ethernet network” that uses SNMP. *See supra* Section III.

Petitioner argues that “Neufeld’s remote server management controller 116, includes an Ethernet interface 180 connected to a Management [n]etwork M to provide the main external communication interface between the remote server management controller 116 and the

¹³ Transcript of the July 24, 2025 deposition of Guevara Noubir, Ph.D.

outside world.” Pet. 28–29 (citing Ex. 1005 ¶ 61, Fig. 3). According to Petitioner, “Neufeld’s Management [n]etwork M . . . connect[s] a remote user (e.g., a remote administrator) at remote management PC 5 via network M with the remote server management controller 116 to engage in out-of-band communication of management data with the remote server management controller 116.” *Id.* at 29 (citing Ex. 1005 ¶¶ 43, 62; Ex. 1046 ¶ 104).

In addition, Petitioner argues that it would have been obvious to one of ordinary skill in the art to use SNMP for the out-of-band connection on the Management network M accessed via the Ethernet interface 180 because, as admitted in the ’140 patent, this protocol is “typically utilized for management of a device.” *Id.* at 31 (quoting Ex. 1002, 12:23–29). Petitioner adds that “employ[ing] SNMP . . . as described in RFC1157 over the Ethernet connection to management network M as the SNMP protocol was very well-known in the art for remotely managing devices.” *Id.* at 31–32 (citing Ex. 1018,¹⁴ 2; Ex. 1046 ¶ 107).

After reviewing Petitioner’s arguments and evidence, we find that Petitioner demonstrates by a preponderance of the evidence that Neufeld teaches this limitation.

4. Virtual Management Interface Connection Means

Claim 1 further recites “at least one virtual management interface connection means for connecting said one or more network services or remote users with said secure management access controller, wherein said virtual management interface connection means provides logical separation

¹⁴ RFC1157: A Simple Management Network Management Protocol (SNMP) (May 1990).

of management data from user data and utilizes user interfaces of said managed network element for connecting said one or more network services or remote users with said secure management access controller.” Ex. 1002, 22:48–51. We agree with Petitioner and find that Neufeld teaches this limitation. Pet. 32–34; Pet. Reply 14–19.

As we conclude above, “virtual management interface connection means” is a means-plus-function term with the following recited functions: (i) “connecting said one or more network services or remote users with said secure management access controller”; (ii) “provides logical separation of management data from user data,” and (iii) “utilizes user interfaces of said managed network element for connecting said one or more network services or remote users with said secure management access controller.” *See supra* Section III. And the functions’ corresponding structure is a VPN. *Id.*

We agree with Petitioner and find Petitioner shows that Neufeld teaches employing a VPN. *See* Ex. 1005 ¶¶ 9, 22, 88 (Table 4). For example, Neufeld explains the following:

[T]he arrangements of servers and clients in a larger network environment could be connected in any of a large number of topologies that may include local area networks (“LANs”), wide area networks (“WANs”), and municipal area networks (“MANs”). Clients may also have the ability to access these networks via a virtual private network (“VPN”) or via the Internet.

Id. ¶ 9. Furthermore, Neufeld teaches that “if [a] system administrator attempts to access [a] 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.” *Id.* ¶ 22 (emphasis added).

We find persuasive Dr. Meldal’s testimony that one of ordinary skill in the art “would have understood such access involves communication with Neufeld’s remote server management controller 116 given that it is a network administrator that is accessing the server.” Ex. 1046 ¶ 110 (citing Ex. 1005 ¶¶ 22, 88 (Table 4, User Id 7)). This testimony is consistent with a network administrator being the one performing management via the remote management controller 116, and Neufeld’s teachings involving remote management and increasingly rigorous restrictions on users, especially remote users. Ex. 1005 ¶ 88 & Table 4; *see also id.* ¶ 35 (teaching point-to-point connections may be employed).

Thus, we find that Neufeld teaches that the VPN performs the function of connecting a remote user (i.e., network administrator) with the secure management access controller (i.e., the remote server management controller 116).

We also agree with Petitioner and find that one of ordinary skill in the art would have found it obvious to implement Neufeld’s VPN as a point-to-point VPN with tunneling functionality. Pet. 32–33 (citing Ex. 1046 ¶ 111). In particular, we find persuasive Dr. Meldal’s testimony that one of ordinary skill in the art would have found it obvious to implement Neufeld’s VPN as a point-to-point VPN with tunneling because such VPN technology was a well-known method for implementing a point-to-point VPN. Ex. 1046 ¶¶ 111–112; Ex. 1049, 48:2–19 (Dr. Noubir testifying that Layer Two Tunneling Protocol (L2TP) was “a well-known VPN technology at the time of the ’140 patent”); Ex. 1050,¹⁵ 3–5 (discussing L2TP implementation);

¹⁵ Excerpts of Cisco Systems, “Internetworking Technologies Handbook,” (3d ed.) (2001).

Ex. 2001 ¶ 67 (citing Ex. 2004,¹⁶ 8); Pet. Reply 14. We appropriately consider such evidence of the knowledge that one of ordinary skill in the art would have had as part of our obviousness analysis. *See Randall Mfg. v. Rea*, 733 F.3d 1355, 1362–63 (Fed. Cir. 2013); *see also Koninklijke Philips N.V. v. Google LLC*, 948 F.3d 1330, 1338 (Fed. Cir. 2020) (finding obviousness can rely on supported expert testimony); *KSR*, 550 U.S. at 417 (“When there is a design need or market pressure to solve a problem [(i.e., choosing a VPN)] and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp. If this leads to the anticipated success, it is likely the product not of innovation but of ordinary skill and common sense.”).

In addition, we agree with Petitioner and find that one of ordinary skill in the art would have found it obvious to implement Neufeld’s VPN using the in-band connection for normal user traffic (i.e., the NIC 110 and network N connection) to provide a dedicated VPN for communication of management data between the managed server 2 and the remote management PC 5. *See supra* Section V.B.2 (finding that Neufeld teaches that network N connects to the NIC 110, which connects to the PCI bus 16/172, which connects to the remote management controller 116 for accessing, interacting, and monitoring the managed server 2 from the remote console 5). Thus, we agree with Petitioner and find that Neufeld’s VPN performs the function of using managed server 2’s NIC 110 user interface for in-band communication of management data which connects the remote

¹⁶ Charlie Scott et al., *Virtual Private Networks*, (2d ed. 1999) (Ex. 2004).

user (i.e., network administrator) with the secure management access controller (i.e., the remote management controller 116).

In addition, we agree with Petitioner and find that Neufeld’s teaching of employing the VPN for the above discussed in-band communication of management data teaches that the VPN performs the function of providing logical separation of management data from user data. Pet. 34. More specifically, we agree with Petitioner and find that Neufeld’s VPN, like the VPN technology of the ’140 patent, provides for the claimed logical separation because the use of the VPN differentiates traffic of the dedicated VPN (i.e., management traffic) from other user traffic (i.e., “user data”). *Id.*; Ex. 1046 ¶¶ 113–114. This understanding is consistent with the Specification of the ’140 patent. *See, e.g.*, Ex. 1002, 6:31–33 (“The VPN technology provides the logical separation, confidentiality, and integrity of the management traffic while it is in transit.”), 7:1–3 (“The VPN tunnels provide for logical separation of the management traffic from any other traffic utilizing the network.”).

We find unavailing Patent Owner’s argument that “Neufeld refers only to *general-purpose VPNs* used for *network access*, not internal communication paths within the managed device.” PO Resp. 25 (citing Ex. 1005 ¶¶ 9, 22, 88); PO Sur-reply 4 (same). Patent Owner adds that one of ordinary skill in the art “would have understood that such *general-purpose VPNs* terminate outside the managed device—typically at a *VPN gateway or network router*—and do *not* utilize or connect through the user interfaces of the managed device itself.” PO Resp. 25 (citing Ex. 2006 ¶¶ 32–36, 57); PO Sur-reply 7–9. Rather, we agree with Petitioner that Neufeld does not refer to its VPNs as “general-purpose,” and that Neufeld’s paragraph 9 discusses various network topologies that a client may access

via a VPN, rather than fixing a VPN endpoint at an edge of the topology. Ex. 1005 ¶ 9; Pet. Reply 16. We also agree with Petitioner that Neufeld’s paragraph 22 refers to the managed server when teaching that for remote access “[t]he system administrator must typically use the Internet or a [VPN] to access the *system*.” Ex. 1005 ¶ 22 (emphasis added); Pet. Reply 16. This portion of the paragraph refers to the situation where “the system administrator attempts to access the *server*” remotely. Ex. 1005 ¶ 22 (emphasis added). Similarly, paragraph 88 teaches permitting certain users access to the managed server 2 via a VPN, which at least suggests that the server is an endpoint of the VPN. Ex. 1005 ¶ 88; Pet. Reply 16–17. Thus, we do not credit Dr. Noubir’s cited testimony on this issue as it is inconsistent with Neufeld’s teachings. *Compare* Ex. 1005 ¶¶ 9, 22, 88 (teaching or suggesting a managed server endpoint), *with* Ex. 2006 ¶¶ 32–36, 57 (testifying that a typical endpoint was a gateway or router). Moreover, for in-band communication, network N is connected to the remote management controller 116 via the NIC 110 and PCI bus 16, and thus when the managed server 2 is an endpoint, the remote management controller 116 is the first processing component encountered. *See, e.g.*, Ex. 1005 ¶¶ 43, 45, Figs. 2–3 (showing no other processor along the communication path from the NIC 110 to IOP 156).

We also find unavailing Patent Owner’s arguments that Petitioner fails to show that the VPN provides logical separation of management data from user data. PO Resp. 27–35. These arguments are premised on Neufeld not teaching in-band communication of management data, which is incorrect. *Id.*; *supra* Section V.B.2 (finding Neufeld teaches in-band communication of management data). As we discuss above, Neufeld’s VPN provides for the claimed logical separation because the use of the VPN

differentiates its traffic (i.e., management traffic) from other user traffic (i.e., “user data”), which is not sent over the VPN.

We also find unavailing Patent Owner’s argument that “to retrofit Neufeld’s architecture to comply with this claim feature[—that the [virtual management interface connection means] utilizes user interfaces of said managed network element—one of ordinary skill in the art] would need to substantially *redesign the system*, such as by moving the VPN endpoint inside Neufeld’s management controller 116 and rearchitecting its interfaces to match the claimed configuration.” PO Resp. 26. Patent Owner continues that “[t]his would not only be *contrary to the teachings of Neufeld*, but also *economically and technically prohibitive*,” and “amount[] to *hindsight reconstruction*.” But as we find above, Neufeld teaches that the VPN connects to the remote management controller via network N and the NIC 110, and doing so using a VPN tunnel would have been obvious. Thus, these arguments from Patent Owner have incorrect premises.

In sum, we find that Petitioner demonstrates by a preponderance of the evidence that Neufeld teaches this limitation.

5. Summary

In sum, we determine that Petitioner shows by a preponderance of evidence that claim 1 would have been obvious to one of ordinary skill in the art in view of Neufeld.

C. Challenged Claims 2–4, 6, 7, 10, 11, 13, and 16

Petitioner argues that Neufeld teaches claims 2–4, 6, 7, 10, 11, 13, and 16. Pet. 34–43. All of these claims depend, directly or indirectly, from independent claim 1. Patent Owner does not provide separate arguments directed to any of these claims, but rather relies on its arguments made for

independent claim 1. PO Resp. 21–38; *generally* PO Sur-reply. As we discuss above, we find these arguments unavailing. *See supra* Section V.B.

We have reviewed Petitioner’s showings for claims 2–4, 6, 7, 10, 11, 13, and 16. Based on the evidence and arguments of record, we find that Petitioner demonstrates by a preponderance of the evidence that the limitations of these claims are taught by Neufeld.

VI. REMAINING GROUNDS INVOLVING NEUFELD

Petitioner argues that the combination of (i) Neufeld and Syvanne renders claims 11 and 12 obvious and (ii) Neufeld and Fowler renders claims 13 and 14 obvious. Pet. 43–51. Patent Owner does not provide separate arguments directed to any of these claims for either of these grounds, but rather relies on its arguments made for independent claim 1 for the Neufeld ground. PO Resp. 38–39; *generally* PO Sur-reply. As we discuss above, we find these arguments unavailing. *See supra* Section V.B.

We have reviewed Petitioner’s showings for each of these challenged claims for each of these asserted grounds. Based on the evidence and arguments of record, we find that Petitioner demonstrates by a preponderance of the evidence that the limitations of these claims are taught by the asserted combinations, and that one of ordinary skill in the art would have been motivated to combine the references of the asserted combinations in the manner Petitioner does.

VII. ALLEGED OBVIOUSNESS OVER IPMI AND LAWRENCE

Petitioner argues that the combination of IPMI and Lawrence renders claims 1–3, 6, 7, 10, and 11 obvious. Pet. 54–76. The parties dispute, among other things, whether one of ordinary skill in the art would have been motivated to combine IPMI and Lawrence. We agree with Patent Owner as to this dispute, and thus, for the reasons that follow, we determine that

Petitioner does not show by a preponderance of the evidence that this combination renders these challenged claims obvious.

A. Summary of IPMI

IPMI “presents the base specifications for the *Intelligent Platform Management Interface* (IPMI) architecture.” Ex. 1020, 23. “The term ‘platform management’ is used to refer to the monitoring and control functions that are built in to the platform hardware and primarily used for the purpose of monitoring the health of the system hardware.” *Id.* “The IPMI specifications define standardized, abstracted interfaces to the platform management subsystem,” “includ[ing] the definition of interfaces for extending platform management between board within the main chassis, and between multiple chassis.” *Id.* In particular, IPMI “defines the overall architecture, common commands, event formats, data records, and capabilities used across IPMI-based systems and peripheral chassis.” *Id.* “This includes the specifications for IPMI management via LAN, serial/modem, PCI Management bus, and the local interface to the platform management.” *Id.*

B. Summary of Lawrence

Lawrence “relates generally to communication networks[, and m]ore particularly, . . . to a method and system to provide secure in-band management for a packet data network.” Ex. 1043, 1:7–10. More specifically, Lawrence teaches that a “network device is managed using the management traffic received over [a] VPN.” *Id.* at code (57). Lawrence teaches that “[a]n in-band management system is created by configuring a [VPN] for a network device and linking the VPN to a management device or a management function.” *Id.* “By using the VPN to carry management

Figure 12-1 is an implementation using an embedded LAN controller to deploy an IPMI LAN Interface using a shared LAN controller. Ex. 1020, 106. Petitioner argues that “IPMI does not detail or limit how to implement the side-band interface for . . . in-band communication, and therefore [one of ordinary skill in the art] would have looked to other sources for information as to how to implement IPMI’s side-band interface.” Pet. 52 (citing Ex. 1046 ¶ 156). And Petitioner argues that Lawrence teaches advantages of using internal secure links to communicate in-band management information. *Id.* at 53 (citing Ex. 1043, 2:20–58). Lawrence’s Figure 7 is shown below.

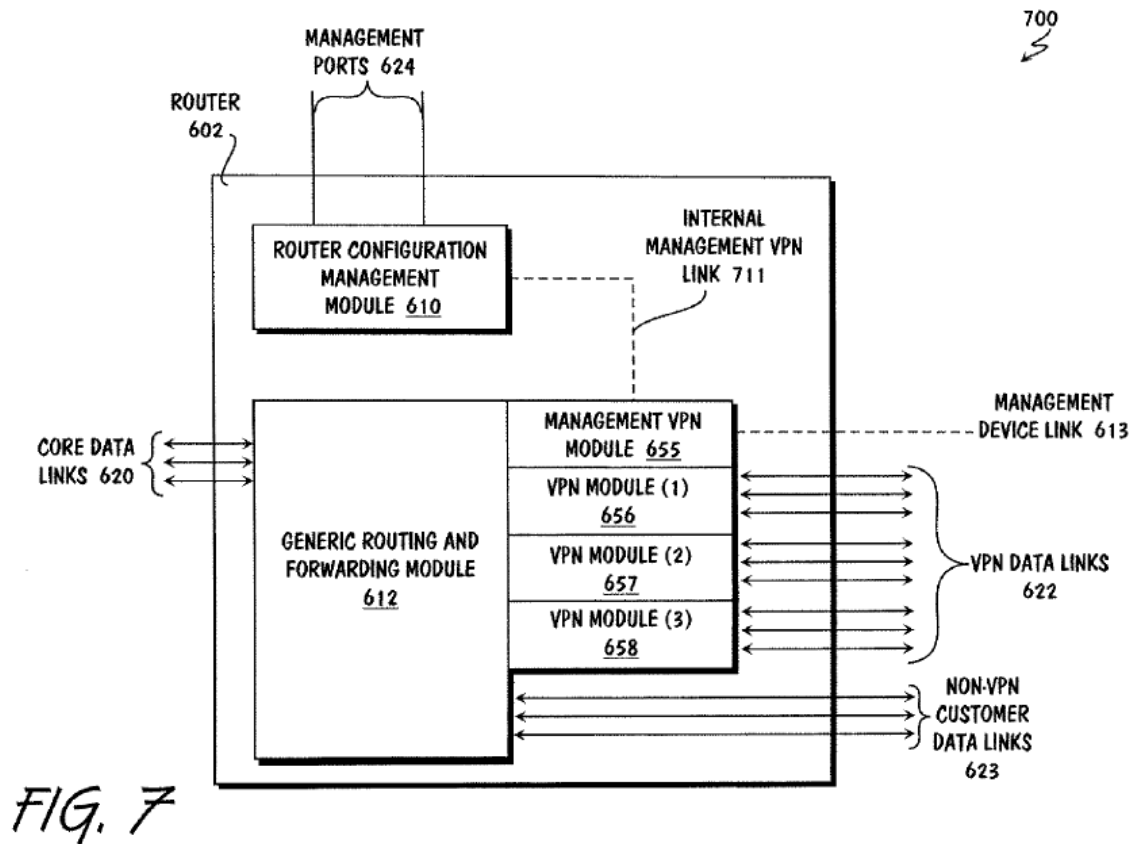


Figure 7 “illustrates an in-band management configuration for a router using a virtual private network to carry management traffic according to” Lawrence’s teachings. Ex. 1043, 3:33–35. Petitioner argues that one of

ordinary skill in the art “would have recognized Lawrence’s Internal Management VPN Link 711 in Figure 7 as a desirable and convenient way in which to implement IPMI’s side-band interface, and thus would have found it obvious to include Lawrence’s VPN tunneling technology in IPMI’s Network (LAN) controller in order to implement IPMI’s side-band interface (corresponding to Lawrence’s Internal Management VPN link 711).”

Pet. 54 (citing Ex. 1046 ¶ 160).

Petitioner argues that “Lawrence specifically discusses in-band management for a router but is not limited to routers and expressly states that the techniques disclosed therein may be used with other types of network devices.” Pet. 53 (citing Ex. 1043, 3:54–64; Ex. 1046 ¶ 157). This cited portion of Lawrence does not discuss in-band management. Ex. 1043, 3:54–64. We agree with Petitioner, however, that Lawrence teaches “advantages of in-band communication of management data but explains that prior art in-band systems were carried on non-secure data links and were therefore ‘susceptible to unauthorized management entry or interception of management commands.’” Pet. 53 (quoting Ex. 1043, 2:20–58). This cited portion of Lawrence discusses internal management connections, but its discussion of security issues relates to the core data links carrying management commands to the device externally, rather than the internal connections. Ex. 1043, 2:20–58.

In addition, Petitioner argues that Lawrence’s Figure 7 illustrates an embodiment “for secure in-band communication of management information, . . . in which management data is communicated to a router configuration management module 610 via a dedicated management VPN module 655 and an internal management VPN link 711.” Pet. 53–54 (citing Ex. 1043, 5:37–47, Fig. 7; Ex. 1046 ¶ 158). Lawrence explains that for this

Figure 7 embodiment that “an internal management VPN link 711 is used instead of an external management VPN links 624-1 to 624-2” to “connect[] management VPN module 655 to router configuration module 610.”

Ex. 1043, 5:40–44.

Petitioner argues that Lawrence teaches “that the dedicated management VPN module 655 performs VPN encapsulation, routing and forwarding functions and may include encryption using an IPSec or other process.” Pet. 54 (citing Ex. 1043, 5:15–30; Ex. 1046 ¶ 159); Pet. Reply 20–21. In relevant part, the cited portion of Lawrence teaches that management VPN module 655 “can perform VPN-related encapsulation, routing, and forwarding functions on packets passing through router 602.” Ex. 1043, 5:22–24. This teaching, however, is in the discussion of Figure 6, which uses external management VPN links 624-1 to 624-2, rather than an internal management VPN link 711. *Id.* To the extent that this teaching discloses using a VPN for the external management links 624-1 to 624-2, Petitioner does not show how one of ordinary skill in the art would have been motivated to apply it to an internal link. Nor does Petitioner establish that such an internal link would have similar security concerns as an external link. We thus agree with Patent Owner that Petitioner does not show that one of ordinary skill in the art would have been motivated to use a VPN on an internal connection (e.g., IPMI’s side-band interface) within a server. PO Sur-reply 24.

Accordingly, we find that Petitioner has not shown that one of ordinary skill in the art would have been motivated to modify IPMI with Lawrence’s teachings in the manner Petitioner proposes.

In addition, we find that Petitioner does not sufficiently address how the VPN “connect[s] said one or more . . . remote users with said secure

management access controller.” *See* Pet. 65–66. In particular, Petitioner identifies IPMI’s BMC as the claimed “secure management access controller.” Pet. 57–59. And Petitioner argues that one of ordinary skill in the art “would have found it obvious to include Lawrence’s VPN tunneling technology in IPMI’s Network (LAN) controller in order to implement IPMI’s side-band interface (corresponding to Lawrence’s Internal Management VPN link 711).” *Id.* at 54; *see also id.* at 64 (same). But, Petitioner does not identify any changes or additions to the BMC to accommodate being a VPN endpoint, or how and why they would be made. *See, e.g.,* Pet. 52–55, 64–65. Thus, we also find that Petitioner does not show that the combination teaches a VPN for connecting a remote user with the secure management access controller.

In sum, we find that Petitioner has not shown by a preponderance of the evidence that claim 1 is obvious.

D. Challenged Claims 2, 3, 6, 7, 10, and 11

Petitioner argues that the combination of IPMI and Lawrence renders claims 2, 3, 6, 7, 10, and 11 obvious. Pet. 66–72. These claims depend from independent claim 1. Above we find for this ground that Petitioner does not show that independent claim 1 would have been obvious. *See* Section VII.C. These dependent claims do not cure the deficiencies we find as to the independent claim 1, and thus, we find Petitioner does not show that these dependent claims would have been obvious over this combination.

Accordingly, we find that Petitioner does not show by a preponderance of the evidence that the combination of IPMI and Lawrence renders claims 2, 3, 6, 7, 10, and 11 obvious.

VIII. REMAINING GROUNDS INVOLVING IPMI AND LAWRENCE

Petitioner argues that the combination of (i) IPMI, Lawrence, and Leedy renders obvious claim 4, (ii) IPMI, Lawrence, and Syvanne renders obvious claims 11 and 12, (iii) IPMI, Lawrence, and Fowler renders obvious claims 13 and 14, and (iv) IPMI, Lawrence, and RFC1492 renders obvious claim 16. Pet. 73–81.

These claims and grounds all rely (directly or indirectly) on Petitioner’s showing for independent claim 1, which above we find deficient. *Id.*; *supra* Section VII.C. And these grounds do not cure the deficiencies. Accordingly, we find that Petitioner does not show by a preponderance of the evidence that the claims challenged for these asserted grounds would have been obvious.

IX. CONCLUSION¹⁷

Based on the full record, we determine that Petitioner shows by a preponderance of the evidence that the challenged claims would have been obvious.

Claim(s)	35 U.S.C. §	Reference(s) /Basis	Claim(s) Shown Unpatentable	Claims Not Shown Unpatentable
1–4, 6, 7, 10, 11, 13, 16	103(a)	Neufeld	1–4, 6, 7, 10, 11, 13, 16	

¹⁷ Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner’s attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. See 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. See 37 C.F.R. § 42.8(a)(3), (b)(2).

11, 12	103(a)	Neufeld, Syvanne	11, 12	
13, 14	103(a)	Neufeld, Fowler	13, 14	
1–3, 6, 7, 10, 11	103(a)	IPMI, Lawrence		1–3, 6, 7, 10, 11
4	103(a)	IPMI, Lawrence, Leedy		4
11, 12	103(a)	IPMI, Lawrence, Syvanne		11, 12
13, 14	103(a)	IPMI, Lawrence, Fowler		13, 14
16	103(a)	IPMI, Lawrence, RFC1492		16
Overall Outcome			1–4, 6, 7, 10– 14, 16	

X. ORDER

In consideration of the foregoing, it is hereby

ORDERED that, pursuant to 35 U.S.C. § 314(a), Petitioner has shown by a preponderance of the evidence that claims 1–4, 6, 7, 10–14, and 16 of the '140 patent are unpatentable; and

FURTHER ORDERED that parties to the proceeding seeking judicial review of this Final Written Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

IPR2024-00124
Patent 7,325,140 B2

For PETITIONER:

James M. Heintz
Gianni Minutoli
DLA PIPER LLP
jim.heintz@us.dlapiper.com
gianni.minutoli@us.dlapiper.com

For PATENT OWNER:

Brandon R. Theiss
Daniel H. Golub
Ryan W. O'Donnell
Robert D. Leonard
VOLPE KOENIG
btheiss@vklaw.com
dgolub@vklaw.com
rodonnell@vklaw.com
rleonard@vklaw.com

Russell J. Rigby
INTELLECTUAL VENTURES II LLC
rrigby@intven.com