

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

LENOVO (UNITED STATES) INC.,
Petitioner,

v.

INTELLECTUAL VENTURES, II LLC,
Patent Owner.

IPR2024-00109
Patent 8,474,016 B2

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

HAMANN, *Administrative Patent Judge.*

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

Lenovo (United States) Inc. (“Petitioner”) filed a petition for *inter partes* review of claims 1–3, 6–9, 12, and 14–17 (“the challenged claims”) of U.S. Patent No. 8,474,016 B2 (Ex. 1001, “the ’016 patent”). Paper 1 (“Pet.”). Intellectual Ventures II LLC (“Patent Owner”) filed a Preliminary Response. Paper 6 (“Prelim. Resp.”).

Institution of an *inter partes* review is authorized by statute when “the information presented in the petition . . . and any response . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a); *see* 37 C.F.R. § 42.108 (2024). Upon consideration of the papers, we conclude that the information presented shows that there is a reasonable likelihood that Petitioner would prevail in establishing the unpatentability of at least one challenged claim of the ’016 patent.

A. *Real Parties-in-Interest*

Petitioner identifies itself and Lenovo Group Ltd. as real parties-in-interest. Pet. 84. Patent Owner identifies itself as a real party-in-interest. Paper 4, 2.

B. *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. 85; Paper 4, 2.

C. *The Challenged Patent*

The ’016 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. 1001, 1:27–31. The ’016 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 1:35–39. Thus, “[i]n general, it is not practical to require physical access to the systems for general maintenance or troubleshooting and repair.” *Id.* at 1:47–49. “The costs would be prohibitive, both in time and person[ne], to require a skilled technician to be dispatched for every required activity on a system.” *Id.* at 1:49–51. “This has driven a strong requirement to provide for remote management of network elements and servers,” according to the ’016 patent. *Id.* at 1:51–53. However, “the security of the network elements and servers is a concern when remote management is allowed.” *Id.* at 1:64–65.

“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 2:4–8. The ’016 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 4:4–7.

In response, the ’016 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 4:10–14. More specifically, the ’016 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 5:50–52. Figure 1 of the ’016 patent is shown below.

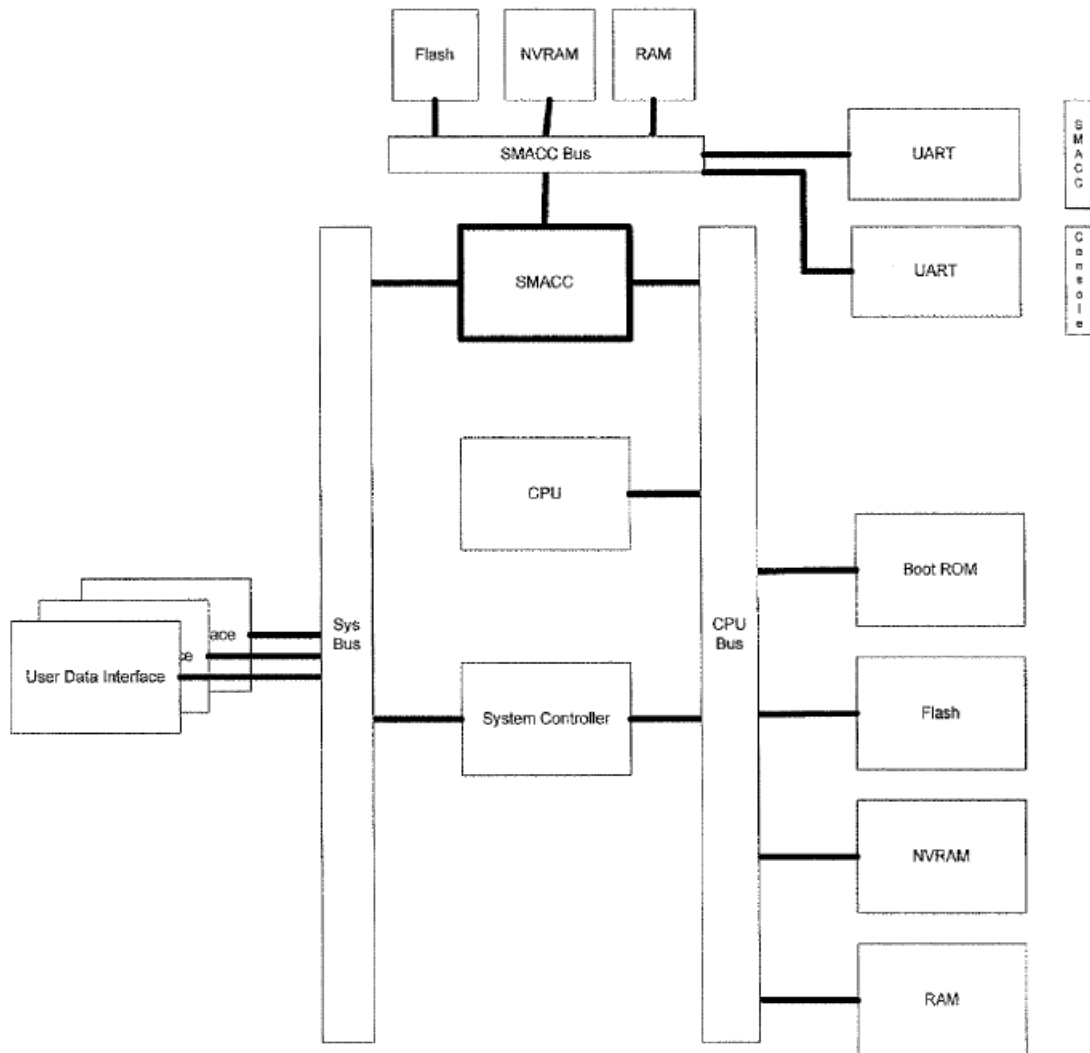


Fig. 1

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 9:39–41, 11:1–2. As illustrated, “the SMACC processor has its own flash, Non-Volatile Random Access Memory (NVRAM), and Random Access Memory (RAM) for operating.” *Id.* at 11:2–5, 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 ’016 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 1:55–58. 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 11:64–12:4, 12:10–17.

D. The Challenged Claims

Petitioner challenges claims 1–3, 6–9, 12, and 14–17 in this proceeding. Claims 1 and 12 are independent claims. Claim 1 is illustrative of the challenged claims and is reproduced below:

1. An apparatus, comprising:
 - a processor configured to control one or more functions of a network device having a network interface, wherein the network device is configured to receive data requests and an encrypted form of management requests via the network interface, wherein the management requests are from a remote administrator;
 - a first bus; and
 - a bus controller coupled to the processor via the first bus, wherein the bus controller is also coupled to a second bus of the network device that is distinct from the first bus, wherein the bus controller is configured to receive the encrypted form of the management requests from the second bus, and to convey the encrypted form of the management requests to the processor via the first bus;
 - wherein the processor is configured to decrypt the encrypted form of the management requests, wherein the network device includes a processor configured to facilitate operation of the network device, and wherein the processor of

the apparatus is distinct from the processor included in the network device.

Ex. 1001, 22:25–45.

E. Asserted Grounds of Unpatentability

Petitioner asserts that the challenged claims of the '016 patent are unpatentable based on the following grounds:

Claim(s) Challenged	35 U.S.C. §¹	Reference(s)/Basis
1–3, 6, 9, 12, 17	103(a)	Neufeld ²
1–3, 6, 9, 12, 17	103(a)	Neufeld, Frantz, ³ Peripheral Component Interconnect (“PCI”) Bridge Spec ⁴
2	103(a)	Neufeld, Frantz, PCI Bridge Spec, Martenson ⁵
3	103(a)	Neufeld, Frantz, PCI Bridge Spec, MacWilliams ⁶
7, 16	103(a)	Neufeld, Frantz, PCI Bridge Spec, Rossman, ⁷ RFC1492 ⁸
8	103(a)	Neufeld, Frantz, PCI Bridge Spec, Syvanne ⁹

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 '016 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 7,085,385 B2, issued Aug. 1, 2006 (Ex. 1006, “Frantz”).

⁴ “PCI-to-PCI Bridge Architecture Specification,” rev. 1.1 (Ex. 1008, “PCI Bridge Spec”).

⁵ US 6,219,708 B1, issued Apr. 17, 2001 (Ex. 1011, “Martenson”).

⁶ US 5,651,137, issued July 22, 1997 (Ex. 1012, “MacWilliams”).

⁷ US 7,260,555 B2, issued Aug. 21, 2007 (Ex. 1015, “Rossmann”).

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

⁹ US 2003/0097590 A1, published May 22, 2003 (Ex. 1016, “Syvanne”).

14	103(a)	Neufeld, Network Time Protocol (“NTP”) Applicant Admitted Prior Art (“AAPA”), ¹⁰ Frantz, PCI Bridge Spec, Hrastar ¹¹
15	103(a)	Neufeld, Frantz, PCI Bridge Spec, RFC1157 ¹²
1–3, 9, 12, 15, 17	103(a)	IPMI, ¹³ Frantz, Huckins ¹⁴
1–3, 9, 12, 15, 17	103(a)	IPMI, IPMIv2.0, ¹⁵ Huckins
6	103(a)	IPMI, Frantz, Huckins, Virtual Private Network (“VPN”) VPN AAPA ¹⁶
6	103(a)	IPMI, Frantz, Huckins, Rossman
6	103(a)	IPMI, Frantz, Huckins, VPN AAPA, Rossman
6	103(a)	IPMI, IPMIv2.0, Huckins, VPN AAPA
6	103(a)	IPMI, IPMIv2.0, Huckins, Rossman
6	103(a)	IPMI, IPMIv2.0, Huckins, VPN AAPA, Rossman
7, 16	103(a)	IPMI, Frantz, Huckins, Rossman, RFC1492
7, 16	103(a)	IPMI, Frantz, Huckins, Rossman, RFC2865 ¹⁷

¹⁰ Petitioner asserts that the ’016 patent contains NTP AAPA. Pet 52 (citing Ex. 1001, 3:30–36).

¹¹ US 7,383,577 B2, issued June 3, 2008 (Ex. 1017, “Hrastar”).

¹² RFC1157: A Simple Management Network Management Protocol (SNMP) (Ex. 1018, “RFC1157”).

¹³ IPMI – Intelligent Platform Management Interface Specification V1.5 (Rev. 1.1 dated Feb. 20, 2002) (Ex. 1020, “IPMI”).

¹⁴ US 2003/0097503 A1, published May 22, 2003 (Ex. 1007, “Huckins”).

¹⁵ IPMI – Intelligent Platform Management Interface Specification V2.0 (Sept. 15, 2003) (Ex. 1023, “IPMIv2.0”).

¹⁶ Petitioner asserts that the ’016 patent contains VPN AAPA. Pet 79 (citing Ex. 1001, 3:53–59).

¹⁷ RFC2865: Remote Authentication Dial In User Service (RADIUS) (Ex. 1014, “RFC2865”).

7, 16	103(a)	IPMI, IPMIv2.0, Huckins, Rossman, RFC1492
7, 16	103(a)	IPMI, IPMIv2.0, Huckins, Rossman, RFC2865
8	103(a)	IPMI, Frantz, Huckins, Syvanne
8	103(a)	IPMI, IPMIv2.0, Huckins, Syvanne
14	103(a)	IPMI, Frantz, Huckins, NTP AAPA
14	103(a)	IPMI, Frantz, Huckins, Hrastar
14	103(a)	IPMI, Frantz, Huckins, NTP AAPA, Hrastar
14	103(a)	IPMI, IPMIv2.0, Huckins, NTP AAPA
14	103(a)	IPMI, IPMIv2.0, Huckins, Hrastar
14	103(a)	IPMI, IPMIv2.0, Huckins, NTP AAPA, Hrastar
15	103(a)	IPMI, Frantz, Huckins, RFC1157
15	103(a)	IPMI, IPMIv2.0, Huckins, RFC1157

Pet. 1–2, 16–83. Petitioner submits in support of its arguments the Declaration of Sigurd Meldal, Dr. Scient. (Ex. 1003) and the Declaration of Nathaniel E. Frank-White (Ex. 1039). Patent Owner submits in support of its arguments the Declaration of Dr. Steven Goldberg (Ex. 2001).

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.*

Petitioner argues 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 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.” Pet. 6 (citing Ex. 1003 ¶ 56). Patent Owner does not address Petitioner’s definition, nor provide its own. *See generally* Prelim. Resp.

For purposes of this Decision, we adopt Petitioner’s definition of the level of skill for one of ordinary skill in the art. Pet. 6. We view this definition for the level of ordinary skill as consistent with the ’016 patent and the asserted prior art, and we apply it in our analysis below.

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 terms of the challenged claims should be given their plain and ordinary meaning. Pet. 6–7. In addition, Petitioner argues for claim 12’s “controlling, by the processor, one or more functions of the network device according to the management requests” limitation that the recited “processor” is “of [the] management device.” *Id.* at 7–8.

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

We determine that we need not expressly construe any claim terms for purposes of our Decision on Institution, and we afford the claim terms their plain and ordinary meaning. *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

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.¹⁸ *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 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. ALLEGED OBVIOUSNESS OVER NEUFELD

Petitioner argues that Neufeld renders claims 1–3, 6, 9, 12, and 17 obvious. Pet. 16–36. For the reasons that follow, we determine that Petitioner establishes a reasonable likelihood that it would prevail in showing that this combination renders at least one of 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.*

¹⁸ Patent Owner does not present arguments or evidence of such objective evidence of non-obviousness. *See generally* Prelim. Resp.

B. Challenged Claim 1

1. Apparatus

Petitioner argues that Neufeld teaches “[a]n apparatus,” as recited in the preamble of claim 1. Pet. 16. More specifically, Petitioner argues that Neufeld is titled “Method **and Apparatus** for Configuring Security Options in a Computer System,” and that “Neufeld’s remote management controller 116 . . . is the claimed ‘apparatus.’” *Id.* (quoting Ex. 1005, code (54); citing *id.* ¶ 43, Fig. 2) (first alteration in original).

After reviewing Petitioner’s arguments, which are not addressed by Patent Owner at this stage, we find 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. Processor To Control Functions of a Network Device

Petitioner argues that Neufeld teaches “a processor configured to control one or more functions of a network device having a network interface,” as recited in claim 1. Pet. 16–18. Petitioner annotates Neufeld’s Figure 2, as shown below, to support its arguments. *Id.* at 17.

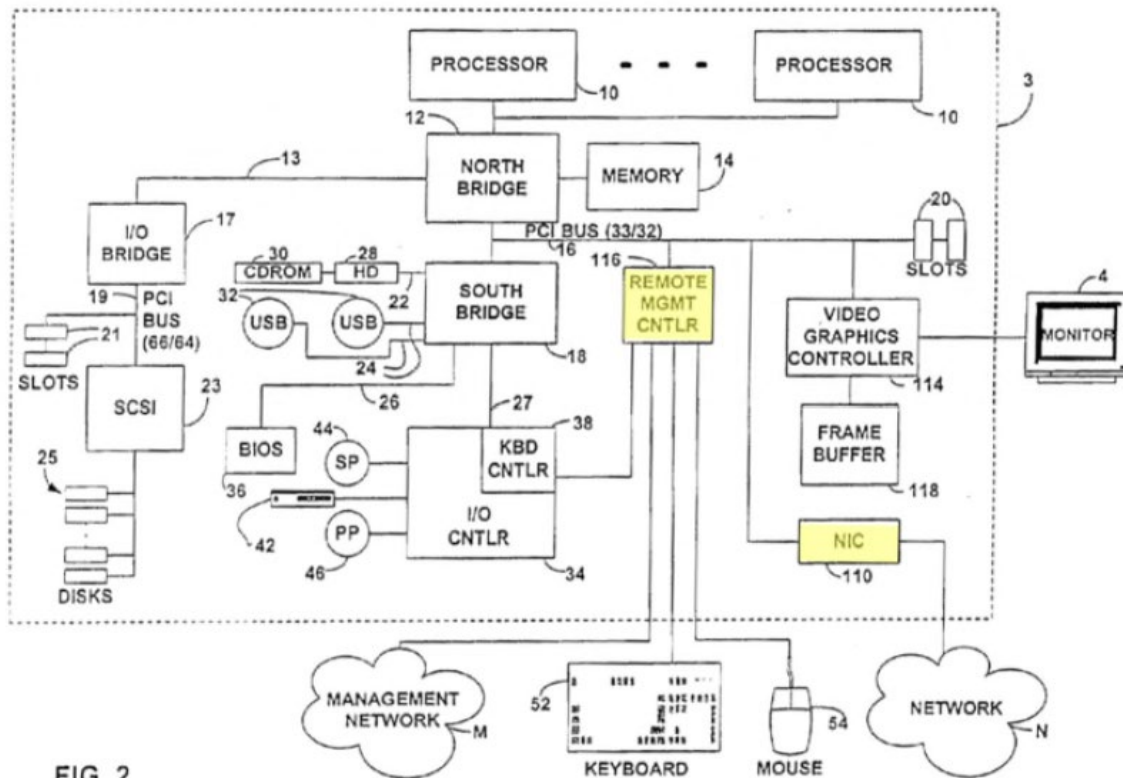


FIG. 2

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. As illustrated, the managed server “includes a [CPU] 3 housing processing, memory, communications, interface, and other circuitry . . . , and may be connected to a monitor 4.” *Id.* ¶ 34. Petitioner annotates this figure by coloring in yellow the remote manager controller 116 and the network interface controller (“NIC”) 110. Pet. 17; Ex. 1005 ¶¶ 43, 45. Petitioner argues that Neufeld’s managed server is the claimed “network device” and the NIC 110 is the claimed “network interface” that interfaces to the network N. Pet. 16–18 (citing Ex. 1005, Fig. 2, ¶ 45).

In addition, Petitioner argues that Neufeld teaches that the remote management controller 116 (i.e., the apparatus) “includes an Input/Output processor (‘IOP’) 156, which provides general control and functions as a management processor for the remote server management controller 116.”

Id. at 16–17 (quoting Ex. 1005 ¶ 54; citing *id.* at Fig. 3). In particular, Petitioner argues that the “IOP 156 controls functions of Neufeld’s managed server 2, such as rebooting, modifying BIOS and/or communicating with server operating system features such as the Emergency Management Services facility of Windows XP, via the slave instrumentation module 152.” *Id.* at 18 (citing Ex. 1005 ¶¶ 66–74). Petitioner argues that the IOP 156 is the claimed “processor.” *Id.* at 16.

After reviewing Petitioner’s arguments, which are not addressed by Patent Owner at this stage, we find that Neufeld teaches this limitation.

3. Network Device is Configured to Receive Requests

Claim 1 further recites “wherein the network device is configured to receive data requests and an encrypted form of management requests via the network interface.” Ex. 1001, 22:27–30. At this stage, we agree with Petitioner and find that Neufeld teaches this limitation. Pet. 18–21.

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

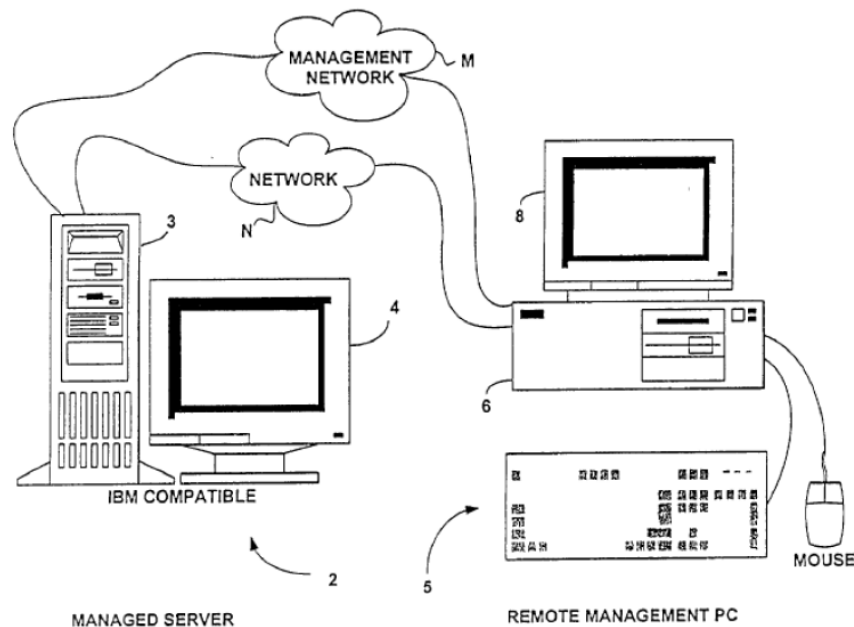


FIG. 1

Figure 1 “is a connection diagram of a managed server and a remote management console according to” Neufeld’s teachings. Ex. 1005 ¶ 25. As illustrated, Neufeld’s CPU 3 of the managed server 2 is connected to the remote management PC 5 via the network N. *Id.* at Fig. 1, ¶¶ 34, 43 (“The 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.”). Moreover, Neufeld teaches that “[r]emote management tools can communicate with a managed server using . . . in-band communication,” which is “communicating with the server over a standard network connection, such as the managed server’s normal Ethernet connection.” *Id.* ¶ 11. And at this stage, we find persuasive Dr. Meldal’s testimony that one of ordinary skill in the art “would have understood the ‘server’s normal Ethernet connection’ to be the Ethernet connection over which normal user (non-administrator) data requests are received,” as we find this testimony is consistent with Neufeld’s teachings. *Compare* Ex. 1003 ¶¶ 84–85, *with* Ex. 1005, Fig. 2 (showing that the managed server connects to the network N via the NIC 110) *and id.* ¶ 35 (“The network N can be virtually any sort of network capable of transmitting data between two devices” (e.g., a local area network (“LAN”, a wide area network, . . . and an Internet connection)).

In addition, we agree with Petitioner that Neufeld teaches the encryption of the remote management requests sent to the remote management controller 116 via network N. Pet. 20–21. In particular, Neufeld teaches that “any type of remote access would typically utilize encryption techniques, while direct access may not.” Ex. 1005 ¶ 85. Moreover, Neufeld provides a table showing that encryption is used when a network administrator connects via a remote in-house or outside terminal, in

contrast with using no encryption for a direct connection. *See id.* (Table 2). And at this stage, we find persuasive Dr. Meldal’s testimony that one of ordinary skill in the art would have understood that a network administrator would have been responsible for managing the server 2 and would have sent management requests, including when connecting remotely via the remote management controller 116. Ex. 1003 ¶¶ 88–90. This testimony is consistent with Neufeld’s teachings we discuss above.

At this stage, we find unavailing Patent Owner’s arguments that Neufeld does not “teach the encryption of management request messages.” Prelim. Resp. 33–35.¹⁹ In particular, we disagree with Patent Owner that “Neufeld’s references to encryption are limited to authentication processes, such as verifying user credentials and establishing secure access to resources, rather than encrypting the content of management requests themselves.” *Id.* at 33–34. Rather, Neufeld discusses authentication, encryption, and privileges as separate concepts. *See* Ex. 1005 ¶ 85. More specifically, Neufeld teaches using “a simple password for authentication if directly accessing the managed server 2,” but “requiring the use of a smartcard or biometrics for instance, if the network administrator attempts to log on” remotely. *Id.* Secondly, Neufeld teaches “any type of remote access would typically utilize encryption techniques, while direct access may not.” *Id.* And lastly, Neufeld turns to what privileges to allow depending on whether the connection is direct or remote. *Id.* The separateness of these concepts is reflected in Neufeld’s Table 2, which has a

¹⁹ Patent Owner’s arguments regarding whether Neufeld teaches the encryption of management request messages are made in the context of a later limitation (Prelim. Resp. 33–35), but we choose to address these arguments for this limitation, where encryption is first recited.

separate column for “Authentication,” “Security Settings” (encryption or not), and “Privileges.” *Id.* And we find that Patent Owner’s arguments relating to Neufeld’s teachings regarding ways to authenticate a user do not negate Neufeld’s teaching of using encryption for remote access communications. Prelim. Resp. 34–35 (citing Ex. 1005 ¶ 76); Ex. 1005 ¶ 85.

In sum, at this stage, we find that Neufeld teaches this limitation.

4. Management Requests From Remote Administrator

Petitioner argues that Neufeld teaches “wherein the management requests are from a remote administrator,” as recited in claim 1. Pet. 18–22. In particular, Petitioner argues that Neufeld’s CPU 3 of the managed server 2 is connected to the remote management PC 5 (i.e., a “remote administrator”) via the network N. *Id.* at 18–19 (citing Ex. 1005, ¶ 34, Fig. 1). More specifically, Petitioner argues that Neufeld teaches 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.” *Id.* at 20 (quoting Ex. 1005 ¶ 43).

After reviewing Petitioner’s arguments, which are not addressed by Patent Owner at this stage, we find that Neufeld teaches this limitation.

5. First Bus

Petitioner argues that Neufeld teaches “a first bus,” as recited in claim 1. Pet. 22. More specifically, Petitioner argues that Neufeld teaches an internal local bus 166 (i.e., the first bus) that is part of the remote management controller 116. *Id.* (citing Ex. 1005 ¶ 56); Ex. 1005 ¶ 56 (“The IOP 156 is operatively coupled to the other functional modules (and possibly many sub-modules) of the remote server management controller 116 via an internal local bus 166.”).

After reviewing Petitioner's arguments, which are not addressed by Patent Owner at this stage, we find that Neufeld teaches this limitation.

6. Bus Controller

Claim 1 further recites “a bus controller coupled to the processor via the first bus, wherein the bus controller is also coupled to a second bus of the network device that is distinct from the first bus, wherein the bus controller is configured to receive the encrypted form of the management requests from the second bus, and to convey the encrypted form of the management requests to the processor via the first bus.” Ex. 1001, 22:33–39. At this stage, we agree with Petitioner and find that Neufeld teaches this limitation. Pet. 22–28.

In particular, we agree with Petitioner and find that Neufeld's Figure 3, shown below as annotated by Petitioner, supports that Neufeld teaches this limitation.

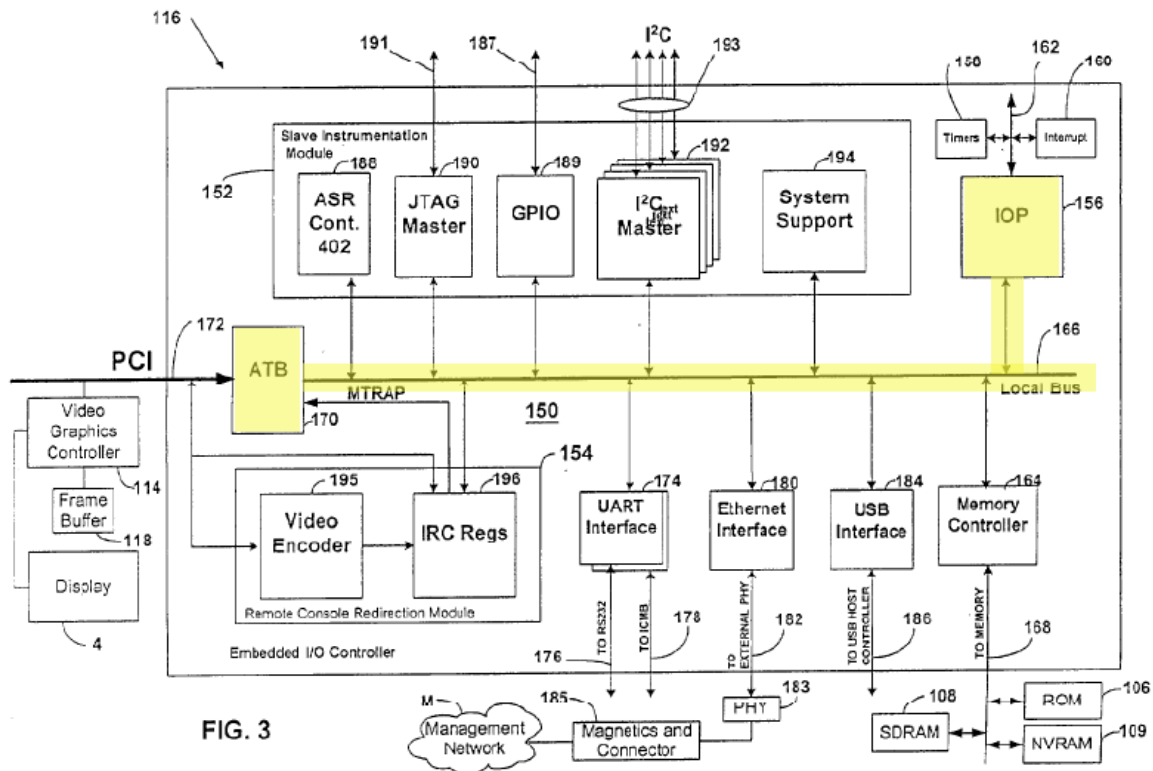


Figure 3 “is a block diagram of [a] remote management controller,” in accordance with Neufeld’s teachings. Ex. 1005 ¶ 27. Petitioner annotates this figure by coloring in yellow (i) the address translation and bridging (“ATB”) unit 170, (ii) the internal local bus 166, and (iii) the IOP 156. Pet. 23.

We agree with Petitioner and find that Neufeld’s ATB unit 170 teaches the claimed bus controller. First, we find that the ATB unit 170 is coupled to the IOP 156 (i.e., the processor) via the local bus 166 (i.e., the first bus). Ex. 1005 ¶¶ 56–57, Fig. 3. Second, we find that the ATB unit 170 is also coupled to a second bus (i.e., the PCI bus 172) of the network device (i.e., the managed server 2) that is distinct from the first bus (i.e., the local bus 166). *Id.* In particular, Neufeld teaches that the ATB “unit 170 is operatively coupled to the internal local bus 166 and to a PCI bus 172,” and that the “PCI bus 172 is integral within and operatively coupled with the managed server 2.” *Id.* ¶ 57.

Third, the ATB unit 170 is configured to receive the encrypted form of the management requests from the second bus (i.e., the PCI bus 172, which is “an extension of the PCI bus 16”), and to convey the encrypted form of the management requests to the processor (i.e., the IOP 156) via the first bus (i.e., the local bus 166). *Id.* ¶¶ 56–58, Fig. 3. In particular, Neufeld teaches that “[t]he PCI bus 172 . . . serves as the main communication interface between the managed server 2 and the remote server management controller 116.” *Id.* ¶ 57; *see also id.* Fig. 2 (showing that the Network N is connected to the NIC 110, which is connected to the remote management controller 116 via the PCI bus 16), ¶ 58 (the PCI bus 172 “is merely an extension of the PCI bus 16”). Moreover, Neufeld teaches that the internal local bus 166 exists to allow communication between and among logical

components of the remote server management controller 116, such as between the ATB unit 170 and the IOP 156. *Id.* ¶ 56.

In addition, Neufeld teaches that the PCI bus 172 “may be configured as a 32-bit, 33 MHz PCI master/slave interface.” *Id.* ¶ 57. Neufeld also teaches that “the ATB unit 170 is constructed to allow the remote server management controller 116 to decode bus cycles on the PCI bus 172 and to communicate over the PCI bus 172 by initiating PCI bus cycles.” *Id.* At this stage, we view these disclosures as sufficient for teaching that the ATB unit 170 is a bus controller. Neufeld explicitly teaches that it is the ATB unit 170 that “allow[s]” the remote server management controller 116 to decode PCI bus cycles (i.e., act as a “slave”) and to communicate over the PCI bus 172 by initiating PCI bus cycles (i.e., act as a “master”). *Id.*; *see also* Ex. 2001 ¶ 57 (describing an arbiter giving access to devices on a PCI bus).

Alternatively, at this stage, we agree with Petitioner and find that one of ordinary skill in the art would have found it obvious to include a bus controller in the ATB unit 170, which connects the PCI bus 172 to the internal local bus 166. Pet. 23–24, 39–41, 43–44. In particular, at this stage, we find persuasive Dr. Meldal’s testimony that “[i]t was known in the art and customary for a bus bridge that links a primary bus to a secondary bus to include a bus controller to control the secondary bus.” Ex. 1003 ¶¶ 96, 135–136. This testimony is supported by PCI Bridge Spec and Huckins’s teachings, which evidence what one of skill in the art would have known. *See* Ex. 1008, 11, 13, 109 (“Every bus segment in a PCI system requires an arbiter. Since a bridge creates a new bus segment, it is anticipated that an arbiter will be a common bridge feature.”), Fig. 1-1; Ex. 1007 ¶ 26, Fig. 1. 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). We also find that one of ordinary skill in the art would have had a reasonable expectation of success in including bus controller functionality in the ATB 170 because doing so was known. Ex. 1003 ¶ 136.

At this stage, we find unavailing Patent Owner’s argument that Neufeld teaches “functionality consistent with a bus bridge, which merely connects and enables communication between buses, rather than a bus controller, which governs traffic flow and manages device access.” Prelim. Resp. 27. In particular, “Petitioner incorrectly extrapolates that [Neufeld’s teachings] impl[y] that the ATB 170 performs the functions of a ‘bus controller,’” according to Patent Owner. *Id.* at 28 (citing Ex. 2001 ¶¶ 54–59). Patent Owner, however, does not address Neufeld’s teaching that it is the ATB unit 170 that “allow[s]” the remote server management controller 116 to communicate over the PCI bus 172, and instead mischaracterizes the ATB unit 170 as “simply a connector.” *Id.* at 28–29.

Moreover, Neufeld’s teachings for the ATB unit 170 meet the limitation’s requirements for a bus controller being configured to receive the encrypted management requests from the second bus, and to convey the encrypted management requests to the processor via the first bus, as we discuss above. *Compare* Ex. 1005 ¶ 57, Fig. 3, *with* Ex. 1001, 22:36–39. The parties should consider addressing further the construction of “bus controller” during trial, in accordance with our Rules.

We also find unavailing Patent Owner’s argument that “[a]ny commands received from the network ‘N’ are received via the NIC 110, and are received by the ‘remote management controller 116’ via the ‘PCI BUS 16,’” and that “the received encrypted commands need not be sent to IOP 156 . . . because Neufeld’s ‘remote management controller 116’ itself

appears to be configured for decrypting any encrypted messages.” Prelim. Resp. 44 (citing Ex. 1005 ¶¶ 75–76, Fig. 2). Rather, the remote management controller 116 as shown in Figure 2 is a block representing a single application specific integrated circuit (“ASIC”). Ex. 1005 ¶¶ 38, 43, 50, Fig. 2. The IOP 156 is part of (e.g., a component) of that remote management controller 116 ASIC. *Id.* ¶¶ 50, 53–57, Fig. 3. And Neufeld teaches that the IOP 156 “provides general control and functions as a management processor for the remote server management controller 116.” *Id.* ¶ 54. In other words, when Neufeld teaches that the remote management controller 116 performs a general function (e.g., decryption), Neufeld is teaching that the IOP 156 portion of the remote management controller 116 is doing it.

In sum, at this stage, we find that Neufeld teaches this limitation.

7. Processor Configured to Decrypt Management Requests

Claim 1 further recites “wherein the processor is configured to decrypt the encrypted form of the management requests.” Ex. 1001, 22:40–41. At this stage, we agree with Petitioner and find that Neufeld teaches this limitation. Pet. 27–28.

In particular, we agree with Petitioner and find that Neufeld teaches that the IOP 156 (i.e., the processor) “provides general control and functions as a management processor for the remote server management controller 116,” and dictates control and monitoring functions in the managed server 2. Ex. 1005 ¶¶ 54, 66. At this stage, we find persuasive Dr. Meldal’s testimony that one of ordinary skill in the art thus “would have understood and found it obvious that IOP 156 would be configured to receive the encrypted form of the management requests and to decrypt and act on them, because IOP 156 is a processor and therefore can be programmed to perform these functions.”

Ex. 1003 ¶ 101. This testimony is consistent with Neufeld’s teachings regarding the IOP 156. Ex. 1005 ¶¶ 54, 66. Moreover, Neufeld’s Figures 2 and 3 do not show another processor along the communications path from the NIC 110 to IOP 156. *See* Ex. 1005, Figs. 2–3. In addition, we also find persuasive Dr. Meldal’s testimony that one of ordinary skill in the art would have found obvious “the need to decrypt management requests in order to act on them.” Ex. 1003 ¶ 102.

At this stage, we find unavailing Patent Owner’s argument that this testimony from Dr. Meldal is conclusory. Prelim. Resp. 41. Rather, the testimony is consistent with Neufeld’s teachings, as we discuss above. *Compare* Ex. 1003 ¶¶ 101–102, *with* Ex. 1005 ¶¶ 54, 66, Figs. 2–3.

We also find unavailing Patent Owner’s argument that “[j]ust because the IOP 156 is a processor does not inherently require that it has the capability (power, speed, architecture) to decrypt encrypted management requests.” Prelim. Resp. 42 (citing Ex. 2001 ¶ 66). As we discuss above, Neufeld teaches that the IOP 156 functions as a management processor for the remote server management controller 116, and that “remote access would typically utilize encryption techniques,” which would include decryption. Ex. 1005 ¶¶ 54, 85; Ex. 1003 ¶¶ 101–102. Thus, we find that Neufeld teaches that the IOP 156 has the capability to decrypt encrypted management requests. *Id.* Moreover, we find Patent Owner’s argument concerning inherency is inapposite in light of these explicit teachings from Neufeld.

In sum, at this stage, we find that Neufeld teaches this limitation.

8. *Network Device Includes Processor*

Petitioner argues that Neufeld teaches “wherein the network device includes a processor configured to facilitate operation of the network

device,” as recited in claim 1. Pet. 28–29. More specifically, Petitioner argues that “Neufeld’s managed server 2 includes a CPU 3 with multiple processors 10 that facilitate operation of the managed server 2.” *Id.* (citing Ex. 1005 ¶ 38; annotating *id.* at Fig. 2 (processors 10)).

After reviewing Petitioner’s arguments, which are not addressed by Patent Owner at this stage, we find that Neufeld teaches this limitation.

9. Distinct Processors

Petitioner argues that Neufeld teaches “wherein the processor of the apparatus is distinct from the processor included in the network device,” as recited in claim 1. Pet. 30. More specifically, Petitioner argues that “[t]he IOP 156 in the remote management controller 116 is distinct from the processors 10 of the managed server CPU 3.” *Id.* (citing Ex. 1003 ¶ 105; Ex. 1005, Fig. 2).

After reviewing Petitioner’s arguments, which are not addressed by Patent Owner at this stage, we find that Neufeld teaches this limitation.

10. Summary

In summary, at this stage, we determine that Petitioner shows a reasonable likelihood that it would prevail in showing that claim 1 would have been obvious to one of ordinary skill in the art in view of Neufeld.

VI. ANALYSIS OF OTHER CLAIMS AND GROUNDS

Because Petitioner demonstrates a reasonable likelihood of success in proving that at least one claim of the ’016 patent is unpatentable, we institute on all grounds and all claims raised in the Petition. *See* 37 C.F.R.

§ 42.108(a). Therefore, at this stage, it is not necessary for us to provide an assessment of every challenge raised by Petitioner. Those challenges, in our view, are best left for trial after full development of the record.

However, in order to provide guidance to the parties, we address the remaining challenges that are disputed by Patent Owner. *See Consolidated Trial Practice Guide* (November 2019)²⁰ 6 (“If a trial is instituted, the Board generally will provide analysis of the strengths and weaknesses of all challenges in the petition in order to provide guidance to the parties for the upcoming trial.”). In particular, we address below Patent Owner’s arguments that the art cited for each of the remaining three grounds that challenge claim 1 does not render claim 1 obvious.

A. ALLEGED OBVIOUSNESS OVER NEUFELD, FRANTZ, AND PCI BRIDGE SPEC

Petitioner argues that the combination of Neufeld, Frantz, and PCI Bridge Spec renders claim 1 obvious. Pet. 36–45. The parties dispute whether (i) one of ordinary skill in the art would have been motivated to combine PCI Bridge Spec and Neufeld’s teachings so as to disclose the claimed “bus controller” and (ii) PCI Bridge Spec teaches a “bus controller.” We address these disputes below.

1. Summary of PCI Bridge Spec

PCI Bridge Spec is titled “PCI-to-PCI Bridge Architecture Specification.” Ex. 1008, 1. PCI Bridge Spec states that it “defines the behavior of a compliant PCI-to-PCI bridge,” and that such a “bridge that conforms to [its] specification and the *PCI Local Bus Specification* is a compliant implementation.” *Id.* at 9.

2. Combining Neufeld and PCI Bridge Spec

Petitioner argues that “Neufeld discloses that the ATB 170 bridges the PCI bus 172 to local bus 166, but does not disclose a bus protocol for the

²⁰ Available at <https://www.uspto.gov/TrialPracticeGuideConsolidated>.

local bus 166.” Pet. 39. In particular, Neufeld teaches that “[t]he implementation details of the internal local bus 166 are a matter of design choice and are not believed to be a crucial aspect of [its] present invention.” Ex. 1005 ¶ 56; Pet. 39. Thus, one of ordinary skill in the art “would have recognized that the local bus 166 could have been implemented as a PCI bus,” according to Petitioner. Pet. 39. Petitioner adds that one of ordinary skill in the art “would have understood that a PCI bus would have been acceptable for the relatively low (with respect to, *e.g.*, the front side bus for Neufeld’s CPU 3) bandwidth that would be necessary for Neufeld’s remote management controller 116 carrying encrypted management communications.” *Id.* (citing Ex. 1003 ¶ 134). Petitioner argues that accordingly, one of ordinary skill in the art “would have looked to a reference such as PCI Bridge Spec that discloses a PCI-to-PCI bridge for guidance on implementing Neufeld’s ATB 170 as a bridge between the system PCI bus 172 and a PCI implementation of local bus 166.” *Id.*

Patent Owner argues that “there is no motivation to combine the Neufeld reference and the PCI Bridge Spec.” Prelim. Resp. 48. In particular, Patent Owner argues that Neufeld “states that the implementation details of the internal local bus 166 are a matter of design choice and are not believed to be a crucial aspect of the invention,” and “[h]ence, there is no need for [one of ordinary skill in the art] to look elsewhere for guidance on implementing Neufeld’s ATB 170 as a bridge to the local bus 166 and therefore no motivation to combine Neufeld and PCI Bridge Spec.” *Id.* (citing Ex. 2001 ¶ 72).

At this stage, we find that Petitioner has provided sufficiently articulated reasoning with rational underpinning to support combining Neufeld and PCI Bridge Spec’s teachings in the manner Petitioner does. *See*

In re Kahn, 441 F.3d at 988. In particular, we agree with Petitioner and find that one of ordinary skill in the art “would have recognized that the local bus 166 could have been implemented as a PCI bus” in light of Neufeld’s teaching that “[t]he implementation details of the internal local bus 166 are a matter of design choice.” Ex. 1005 ¶ 56; Pet. 39. And we credit Dr. Meldal’s testimony that one of ordinary skill in the art “would have understood that a PCI bus would have been acceptable for the relatively (with respect to, *e.g.*, the front side bus for Neufeld’s CPU 3) low bandwidth that would be necessary for Neufeld’s remote management controller 116.” Ex. 1003 ¶ 134. The bus leading to the remote management controller 116 (the PCI bus 16/PCI bus 172) being a PCI bus supports the acceptability of using a PCI bus for the internal local bus 166. *Id.*; *see also KSR*, 550 U.S. at 417 (“When there is a design need or market pressure to solve a problem [(i.e., choosing a bus protocol)] and there are a finite number of identified, predictable solutions, [(i.e., a finite number of known protocols)] 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 that instance the fact that a combination was obvious to try might show that it was obvious under § 103.”).

At this stage, we find unavailing Patent Owner’s argument that “there is no need for [one of ordinary skill in the art] to look elsewhere for guidance on implementing Neufeld’s ATB 170 as a bridge to the local bus 166” because Neufeld teaches that the implementation details of the internal local bus 166 are a matter of design choice. Prelim. Resp. 48. Rather, as we discuss above, one of ordinary skill in the art would have found it obvious for the internal local bus 166 to constitute a PCI bus, and as such would have

been motivated to look to a known specification (PCI Bridge Spec) when having a bridge (the ATB unit 170) between two PCI buses.

Moreover, PCI Bridge Spec also evidences the knowledge of one of ordinary skill in the art that we appropriately consider as part of our obviousness analysis. *Randall Mfg.*, 733 F.3d at 1362–63. Thus, when one of ordinary skill in the art would have been motivated to employ a PCI bus for the internal local bus 166, the knowledge of also needing a controller should be considered. *See id.*; Ex. 1008, 109 (“Every bus segment in a PCI system requires an arbiter. Since a bridge creates a new bus segment, it is anticipated that an arbiter will be a common bridge feature.”); *cf. Koninklijke Philips N.V. v. Google LLC*, 948 F.3d 1330, 1338 (Fed. Cir. 2020) (finding obviousness can rely on supported expert testimony that an element “was not only in the prior art, but also within the general knowledge of a skilled artisan”).

3. *Bus Controller*

Petitioner argues that PCI Bridge Spec teaches a PCI-to-PCI bridge that includes a PCI bus controller for the secondary interface/local bus 166. Pet. 39–40 (citing Ex. 1008, 11 (defining primary and secondary interfaces), 13 (Fig. 1-1 illustrating bridge), 109 (disclosing bridge device providing arbiter for secondary bus). Petitioner argues that “[b]us arbitration is often performed by a bus controller.” *Id.* at 40 (citing Ex. 1003 ¶ 135).

Patent Owner argues that “PCI Bridge Spec does not disclose a bus controller,” but instead “is a specification defining the behavior of a compliant PCI-to-PCI bridge.” Prelim. Resp. 47. “At most, the PCI Bridge Spec shows implementation of a bridge or connection path, but does not disclose a bus controller as recited in claim 1,” according to Patent Owner. *Id.*

At this stage, we agree with Petitioner and find that PCI Bridge Spec teaches a bridge providing a bus controller. Pet. 39–40. In particular, PCI Bridge Spec teaches that “[e]very bus segment in a PCI system requires an arbiter,” and because “a bridge creates a new bus segment, it is anticipated that an arbiter will be a common bridge feature.” Ex. 1008, 9. PCI Bridge Spec further states that “[i]t is recommended that a bridge provide the arbiter for the secondary bus.” *Id.* Patent Owner does not address this portion of PCI Bridge Spec.

B. ALLEGED OBVIOUSNESS OVER IPMI, FRANTZ, AND HUCKINS

Petitioner argues that the combination of IPMI, Frantz, and Huckins renders claim 1 obvious. Pet. 54–67. The parties dispute whether one of ordinary skill in the art would have been motivated to combine the references to teach (i) encrypting management requests and (ii) a “bus controller.” In addition, the parties dispute whether the combination teaches a processor that decrypts management requests. We address these disputes below.

1. 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.” “This includes the specifications for IPMI management via LAN, serial/modem, PCI Management bus, and the local interface to the platform management.” *Id.*

2. *Summary of Frantz*

Frantz “relates generally to remote server management in networked computer systems and, more particularly, to providing secure communications paths for remote server management communications.” Ex. 1006, 1:9–12. Frantz explains that “[a]n important aspect of efficiently managing a large computer network is to maximize the amount of analysis and repair that can be performed remotely (for example, from a centralized administration site).” *Id.* at 2:19–22.

Frantz states that “[t]he growth of modern computer systems and the need to communicate remotely with servers on such a vast geographic scale has, unfortunately, resulted in some unintended negative consequences.” *Id.* at 2:34–37. In particular, “[l]arge, geographically diversified computer networks are susceptible to attacks by hackers who desire to gain access to information stored on those computer networks.” *Id.* at 2:37–40.

In response, Frantz states that “[t]o facilitate the goal of providing remote server management across publicly accessible data paths such as the Internet while at the same time inhibiting the ability of hackers to intercept such communications, a remote network management tool that is able to establish a strongly encrypted communication path with a managed server across the publicly available communication path is highly desirable.” *Id.* at 3:34–41. Frantz states that its embodiments relate to providing such secure communications in the context of remote server management, including by using encryption for communications. *Id.* at code (57).

3. *Summary of Huckins*

Huckins “relates generally to the field of microprocessors and computer systems,” and “[m]ore particularly, . . . relates to a method and apparatus for [PCI] compatible bus model for non-PCI compatible bus architectures.” Ex. 1007 ¶ 1. More specifically, Huckins teaches “a computer system . . . having the capability to communicate with a non-PCI bus architecture via a PCI compatible bus.” *Id.* ¶ 22. Huckins describes the following method: “identifying a hardware controller coupled to a PCI compatible bus, the hardware controller compatible to a PCI bus protocol and to a non-PCI bus protocol”; “[t]he hardware controller is initialized”; “[a] non-PCI compatible bus coupled to the hardware controller is searched for a non-PCI compatible device, the non-PCI compatible device compatible to the non-PCI bus protocol;” “[t]he non-PCI compatible device is configured;” and “[t]he non-PCI compatible device is recognized as a PCI compatible device coupled to said PCI compatible bus.” *Id.* at code (57).

4. *Combining to Teach Encrypting Management Requests*

The parties dispute whether one of ordinary skill in the art would have been motivated to combine IPMI and Frantz to teach encrypting management requests. Pet. 57–60; Prelim. Resp. 53–55. For the reasons below, at this stage, we find that Petitioner makes a sufficient showing to support making this combination.

In particular, we agree with Petitioner and find that IPMI teaches receiving in-band management requests from a remote management system via a LAN. Ex. 1020, 9 (Fig. 1-2), 106–07. In addition, we agree with Petitioner and find that Frantz teaches using encryption for in-band communication of remote management requests for a managed server for security. Ex. 1006, 3:19–41, 10:50–63. At this stage, we find persuasive

Dr. Meldal’s testimony that one of ordinary skill in the art “would have recognized that encrypting the payloads of [IPMI management message] packets would improve security, particularly in view of” Frantz’s teaching of the desirability to do so. Ex. 1003 ¶¶ 189 (citing Ex. 1006, 3:19–41, 10:50–63), 192. Thus, at this stage, we find that Petitioner has provided sufficiently articulated reasoning to support combining IPMI and Frantz’s teachings in the manner Petitioner does. *See In re Kahn*, 441 F.3d at 988.

At this stage, we find unavailing Patent Owner’s argument that “without hindsight, there is no reason that [one of ordinary skill in the art] would read IMPI and determine . . . that encryption would be helpful, necessary, or important.” Prelim. Resp. 55. This argument incorrectly focuses on IPMI’s teachings individually. *See In re Merck & Co.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986) (“Non-obviousness cannot be established by attacking references individually where the rejection is based upon the teachings of a combination of references”). The relevant inquiry is whether the claimed subject matter would have been obvious to those of ordinary skill in the art in light of the combined teachings of IPMI and Frantz. *See In re Keller*, 642 F.2d 413, 425 (CCPA 1981). And as we discuss above, Frantz teaches employing encryption for remote management of a device for security. Thus, the combined teachings render the claimed subject matter obvious.

We also find unavailing Patent Owner’s argument that “[g]iven that IMPI does not disclose encryption of management requests and specifically indicates not using encrypted packets, there is no reason that [one of ordinary skill in the art] would look to Frantz to add the feature.” Prelim. Resp. 55 (citing Ex 2001 ¶ 83). At this stage, we find that IPMI merely states that the packets are not encrypted, rather than criticizing, discrediting,

or otherwise discouraging encryption, and thus does not teach away from combining IMPI and Frantz in the manner Petitioner does. *See 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).

5. *Combining to Teach Bus Controller*

The parties dispute whether one of ordinary skill in the art would have been motivated to combine IPMI and Huckins to teach the claimed bus controller. Pet. 62–65; Prelim. Resp. 56–60. For the reasons below, at this stage, we find that Petitioner does not make a sufficient showing to support making this combination.

Petitioner argues that IPMI teaches a LAN Controller that connects to a PCI bus on the managed platform and that includes a side-band interface to an I²C bus or System Management Bus (“SMBus”) which connects to a Baseboard Management Controller (“BMC”) for conveying in-band IPMI management messages received from a remote management system to the BMC. Pet. 61–62 (citing Ex. 1020, 106 (Fig. 12-1)). We agree with Petitioner so far.

Petitioner next argues that IPMI “does not explain how to implement such a network controller with such a side-band interface,” and thus, one of ordinary skill in the art “would look to prior art sources for guidance as to how to implement such a side-band interface.” *Id.* at 62 (citing Ex. 1003 ¶ 196). In particular, Petitioner argues that one of ordinary skill in the art would “look to known implementations of a bridge between a PCI bus and an I²C bus or an SMBus.” *Id.* We also agree with these arguments.

Petitioner next argues that “Huckins discloses a ‘non-PCI bus controller 126’ that ‘can also be referred to as a bus bridge,’” and that “[t]his

bus controller-bridge can connect a non-PCI device 133 connected to a non-PCI bus 132 to a system 100 over a PCI bus 131.” *Id.* at 62–63 (citing Ex. 1007 ¶ 26, Fig. 1). Petitioner argues that Huckins teaches “that the non-PCI bus may be ‘one of many types of bus protocols available,’ and I²C was a well-known bus type available at the time of the [’]016 patent.” *Id.* at 63 (citing Ex. 1007 ¶ 40; Ex. 1003 ¶ 197).

Notably, Petitioner does not argue that Huckins teaches a known implementation of a bridge between a PCI bus and an I²C bus, which is what Petitioner argues that one of ordinary skill would look to, as we address above. *Id.* at 62 (citing Ex. 1003 ¶ 196). Nor does Petitioner cite any art that evidences that an I²C bus requires a controller. Nor does Petitioner explain why an I²C bus is appropriately “one of many types of bus protocols available” in Huckins, other than to say an I²C bus was well known.

Accordingly, at this stage, we agree with Patent Owner and find that Petitioner has not shown that one of ordinary skill in the art would “look at IPMI and then look to Huckins to add a bus controller without the benefit of hindsight.” Prelim. Resp. 57 (citing Ex. 2001 ¶ 89).

6. Processor to Decrypt the Encrypted Management Requests

The parties dispute whether the combination of IPMI and Frantz teaches that the processor is configured to decrypt the encrypted management requests. Pet. 57–60, 62–65, 67; Prelim. Resp. 61–64. For the reasons below, at this stage, we agree with Petitioner and find that the combination of IPMI and Frantz teaches a processor (i.e., BMC) configured to decrypt the encrypted management requests.

As we discuss above, we find that (i) IPMI teaches receiving in-band management requests from a remote management system via a LAN, and (ii) Frantz teaches using encryption for in-band communication of remote

management requests for a managed server for security. *See supra* Section VI.B.4. And at this stage, we find persuasive Dr. Meldal’s testimony that it would have been obvious to one of ordinary skill in the art “to configure the BMC to decrypt the[] encrypted messages because without decryption the BMC would not be able to act on them.” Ex. 1003 ¶ 205. Thus, we find that the combination of IPMI and Frantz teaches a processor (i.e., BMC) configured to decrypt the encrypted management requests.

At this stage, we find unavailing Patent Owner’s argument that IPMI does not “teach or suggest that the BMC (the alleged ‘processor’) is capable of or is configured to perform encryption / decryption operations.” Prelim. Resp. 61–62; *see also id.* at 62–64 (arguing that IPMI’s listed mandatory and optional functions and commands do not include decryption). We find that this argument is akin to arguing that the teachings cannot be physically combined, which is an improper focus for determining whether the claim would have been rendered obvious by the prior art as a whole. *See Allied Erecting & Dismantling Co. v. Genesis Attachments, LLC*, 825 F.3d 1373, 1381 (Fed. Cir. 2016) (quoting *In re Sneed*, 710 F.2d 1544, 1550 (Fed. Cir. 1983)); *see also id.* (quoting *In re Etter*, 756 F.2d 852, 859 (Fed. Cir. 1985) (en banc)) (“Etter’s assertions that Azure cannot be incorporated in Ambrosio are basically irrelevant, the criterion being not whether the references could be physically combined but whether the claimed inventions are rendered obvious by the teachings of the prior art as a whole.”). Rather, at this stage, we find that one of ordinary skill would have found it obvious to have the BMC processor perform decryption in light of the combined teachings of IPMI and Frantz, as we discuss above. *See also KSR*, 550 U.S. at 420–21 (one of ordinary skill in the art is “a person of ordinary creativity, not an automaton”).

C. ALLEGED OBVIOUSNESS OVER IPMI, IMPIV2.0, AND HUCKINS

Petitioner argues that the combination of IPMI, IPMIV2.0, and Huckins renders claims 1–3, 9, 12, 15, and 17 obvious. Pet. 76–79. At this stage, Patent Owner does not address separately Petitioner’s arguments and evidence as to how this combination teaches these claims. *See* Prelim. Resp. 64–65. Accordingly, the guidance we provide above also applies here.

VII. CONCLUSION

For the foregoing reasons, we determine that Petitioner has shown a reasonable likelihood that it would prevail in proving the unpatentability of at least one of the challenged claims of the ’016 patent. We thus institute an *inter partes* review of all of the challenged claims of the ’016 patent on all grounds asserted in the Petition.

Any findings or conclusions in this Decision are made only for the purposes of institution and are not dispositive of any issue. We have not made a final determination with respect to the patentability of any challenged claim. Our final determination will be based on the record as fully developed during trial, including any evidence or argument timely presented by the parties under our Rules.

VIII. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review of the ’016 patent is instituted on all of the challenged claims and all grounds asserted in the Petition; and

FURTHER ORDERED that pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial; the trial commences on the entry date of this Decision.

IPR2024-00109
Patent 8,474,016 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 Rigby
INTELLECTUAL VENTURES II LLC
rrigby@intven.com