

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.

Case No. IPR2024-00124

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

PATENT OWNER'S SUR-REPLY

TABLE OF CONTENTS

PATENT OWNER’S EXHIBIT LIST.....	iii
I. INTRODUCTION	1
II. PETITIONER’S REPLY DOES NOT CURE THE DEFICIENCIES OF ITS SOLE 103 REFERENCE, NEUFELD.....	1
A. Neufeld Neither Discloses Nor Suggests a VPN/VMI That Terminates Behind the NIC	3
1. Dr. Noubir’s Alleged Admission that a Point-to-Point VPN Would Have Been Known at the Time of Filing is Irrelevant to its Point of Terminus, Which is Never Addressed by Petitioner.....	3
2. Petitioner’s “Point-to-Point VPN” Thesis Ignores Where Termination Must Occur.....	6
3. Petitioner’s Obviousness Theory is Legally and Evidentiary Defective	9
B. Neufeld Does Not Clearly Disclose or Suggest an In-Band Network Over Which Management Data is Actively Communicated.....	11
1. Neufeld’s Overall System Architecture.....	12
2. Paragraph [0043] Does Not Support Petitioner’s Position.....	15
3. Paragraph [0047] Reinforces Passive Monitoring, Not In-Band Management, and Adds Further Confusion About Network N’s Function.....	17
4. Paragraph [0048] Describes Video Redirection, Not VPN-Based Logical Separation	18
5. Ambiguity and Contradiction Weighs Against Obviousness	19
6. Petitioner’s VPN-Based Obviousness Theory Fails Because it Depends on a Misreading of Neufeld and Lacks Any Evidentiary Support	22
III. PETITIONER’S REPLY IMPROPERLY RAISES A NEW ARGUMENT AND FAILS TO PROVIDE A MOTIVATION TO COMBINE IPMI AND LAWRENCE	24

IV. PETITIONER HAS FAILED TO DEMONSTRATE THE UNPATENTABILITY OF THE CHALLENGED CLAIMS.....	25
---	----

PATENT OWNER'S EXHIBIT LIST

Ex. 2001	Declaration of Dr. Steven Goldberg
Ex. 2002	Resume of Dr. Steven Goldberg
Ex. 2003	Virtual private networks, Dennis Fowler, Morgan Kaufmann Publishers, Inc., 1999
Ex. 2004	Virtual Private Networks, Charlie Scott, Paul Wolfe, Mike Erwin, O'Reilly, 1999, Page 8
Ex. 2005	Networking Explained, Second Edition, Michael Gallo and William Hancock, Digital Press, 2002, Page 188.
Ex. 2006	Declaration of Dr. Guevara Noubir
Ex. 2007	Resume of Dr. Guevara Noubir
Ex. 2008	Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, E. Lear, "Address Allocation for Private Internets", Internet Engineering Task Force (IETF), Network Working Group, February 1996.
Ex. 2009	Vijay Bollapragada, Mohamed Khalid, Scott Wainner, "IPSec VPN Design", Cisco Press, 2005.
Ex. 2010	Paul Barham, Boris Dragovic, Keir Fraser, Steven Hand, Tim Harris, Alex Ho, Rolf Neugebauer, Ian Pratt, and Andrew Warfield, "Xen
Ex. 2011	Mark Thorson, "System Management Mode Explained", Microprocessor Report 6 (1992): 14-16.
Ex. 2012	U.S. Patent No. 5,898,861 ("Transparent Keyboard Hot Plug").

I. INTRODUCTION

The Reply does not meet the Petition's burden. It still never identifies where Neufeld places a VPN/VMI endpoint inside the device that uses the device's user interfaces to connect to the SMACC and logically separates management from user data on those same interfaces (or anywhere else) or why this would be obvious. Nor does it supply a reasoned path to modify IPMI in view of Lawrence to achieve that same internal VMI. What remains are mischaracterizations, semantics, and new rationales beyond the Petition.

II. PETITIONER'S REPLY DOES NOT CURE THE DEFICIENCIES OF ITS SOLE 103 REFERENCE, NEUFELD

The contested issues for Ground 1 are about the claim language "at least one virtual management interface connection means": (1) "utiliz[ing] user interfaces of said managed network element for connecting..." and (2) "provid[ing] logical separation of management data from user data." To utilize user interfaces of the managed network element as claimed, Neufeld's VPN needs to terminate behind the NIC. POR at 23-24. Further, to provide logical separation of management data from user data, both types of data need to be co-mingled on the in-band path to begin with. *Id.* at 27-29.

Petitioner's Reply ("Reply") concedes by omission the fatal flaw in its case: Neufeld does not disclose, and a POSITA would not have understood it to suggest, a VPN that terminates behind the NIC. *See* Reply at 14-17; POR at 23-26. The claim

language is unequivocal—any VMI must utilize user interfaces of the managed device to connect with the secure management controller (SMACC). POR at 23-24. Petitioner never addresses this, because it cannot. *See* Reply at 14-17. Neufeld’s fleeting mentions of VPNs describe only their conventional use terminating at external gateways or routers, a point confirmed by both the specification and Dr. Noubir’s testimony. POR at 25-26; EX2006, ¶¶ 33-36, 56-58, Figs. 2-3. Petitioner’s reliance on semantics and distraction tactics does nothing to change this reality. Reply at 14-16. By ignoring the dispositive claim requirement and failing to explain how (or why) Neufeld could be reconfigured to provide it, Petitioner effectively admits that Ground 1 collapses under its own weight.

Petitioner’s attempt to recast Neufeld as teaching in-band management is equally untenable. Reply at 3-8. Neufeld never discloses management data traveling over Network N, and Petitioner’s reliance on a handful of ambiguous sentences cannot rewrite the reference. POR at 27-32; Reply at 7-8. The architecture is clear: Neufeld consistently routes management traffic through a dedicated out-of-band channel (Network M), with the RMC designed for hardware-level monitoring and redirection, not for in-band VPN tunneling. POR at 27-32. By insisting these stray passages somehow imply the opposite, Petitioner asks the Board to ignore the figures, the explicit description in the publication’s text, and its central purpose of secure out-of-band control. Reply at 7-8. At best, Neufeld is contradictory; at worst,

Petitioner imports the ‘140 Patent’s teachings into Neufeld through hindsight. Either way, Petitioner has not carried its burden, and its in-band theory collapses under the weight of the record.

A. Neufeld Neither Discloses Nor Suggests a VPN/VMI That Terminates Behind the NIC

There is no disclosure or suggestion in Neufeld of any VPN that terminates behind the NIC. POR at 23-26. Petitioner’s Reply was non-responsive to this argument, merely reiterating its viewpoint that a point-to-point VPN with tunneling would have been obvious from Neufeld, attempting to distract from this by hammering PO’s expert for the *unrelated* admission that a point-to-point VPN would have been known, and further distracting with an argument that Neufeld does not *limit* its disclosure to general purpose VPNs. Reply, 14-18.

1. Dr. Noubir’s Alleged Admission that a Point-to-Point VPN Would Have Been Known at the Time of Filing is Irrelevant to its Point of Terminus, Which is Never Addressed by Petitioner

The relevant language of claim 1 highlighted above means that any VMI read on claim 1 must terminate *behind the user data interfaces*, specifically using them to connect with the SMACC. POR, 23-24, EX2006, ¶¶ 55-56. This is regardless of whether that VMI is a general-purpose or a point-to-point VPN with tunneling, or what software it runs. *See* EX2006 at ¶ 33-36.

This is shown in FIG. 3 of the '140 Patent (below). As shown, the VMI (red) is between the SMACC (blue) and the user interfaces (green), allowing it to *utilize the user interfaces for connecting* network services or remote users with the SMACC. By contrast, Neufeld's VPN is used as a network connection to Network N, so it would be obvious only for the VPN to terminate within that network, which, as shown in FIG. 2 (below), terminates at the NIC, not behind it. See EX1005, ¶¶ [0009], [0022], [0088]; EX2006, ¶¶ 33-36, Figures 2, 3.

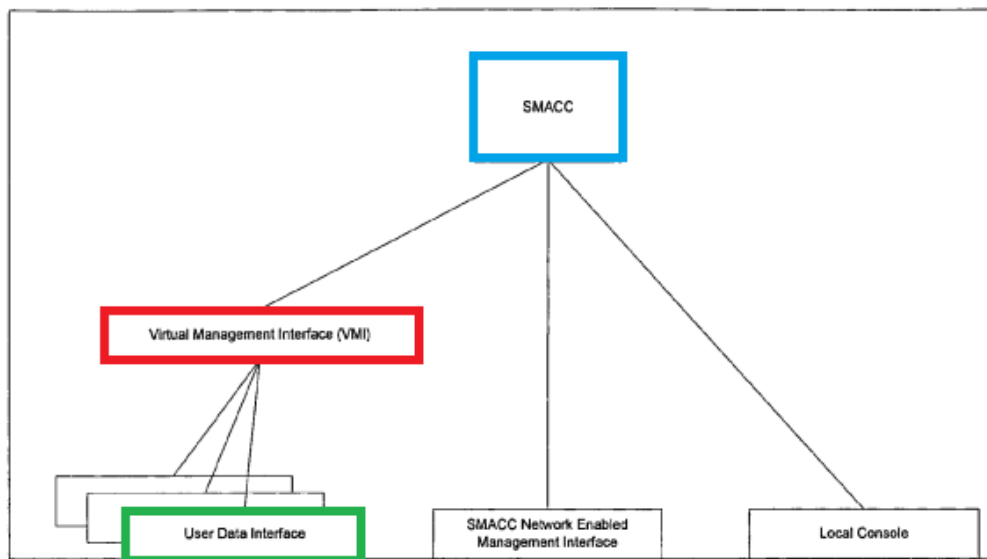
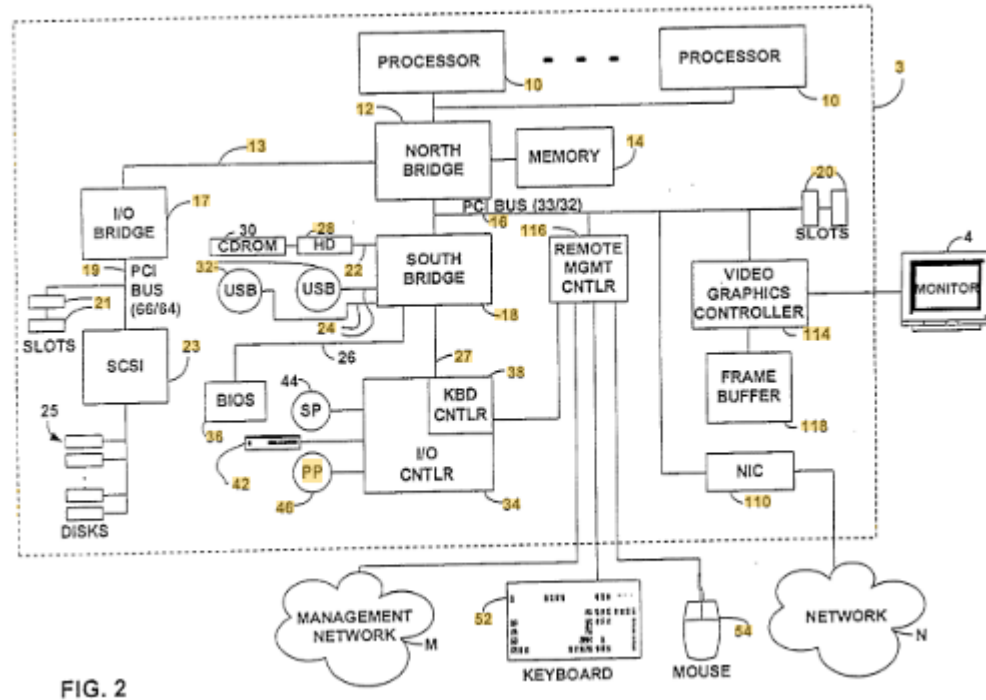


Fig. 3



Nevertheless, Petitioner focuses on the obviousness of *the possibility of* a point-to-point VPN, and never even addresses PO's position on its terminus. Reply at 14-17. This is underscored by Petitioner's accusation that "Dr. Noubir admitted at his deposition that providing VPN tunnels *with individual computers as endpoints* was possible." (Emphasis added). *Id.* at 15. Dr. Noubir is correct, that is possible; but if the termination point is at the individual computers, *rather than the RMC*, the VPN cannot be said to "utilize[] user interfaces of said managed network element for connecting..." as expressly required by Claim 1.

In sum, Claim 1 requires a VMI that terminates behind the user data interfaces, using them to connect remote users or services with the SMACC. Petitioner's focus on whether point-to-point VPNs were known misses this critical requirement, as

even Petitioner’s characterization of Dr. Noubir’s testimony places the VPN endpoint at individual computers/networks—not behind the NIC. The ‘140 Patent makes clear, both in its claim language and drawings, that the VMI resides between the SMACC and user data interfaces, leveraging those interfaces to achieve the claimed logical separation of data. Neufeld, by contrast, only discloses VPNs for generic network access that terminate at the network side of the NIC, as depicted in its Figure 2. Petitioner has therefore failed to show how Neufeld could meet or render obvious this essential claim requirement, and Ground 1 cannot stand.

2. Petitioner’s “Point-to-Point VPN” Thesis Ignores Where Termination Must Occur

Petitioner argues that “[i]nstead of addressing the obviousness of a point-to-point VPN as alleged in the Petition, the POR latches onto three sentences in Neufeld to allege that Neufeld only access[es] networks using general purpose VPNs that terminate outside of a managed device.” Reply at 15. This is a complete mischaracterization of PO’s argument. PO does not ignore obviousness, but rather makes the *different* point that Neufeld’s VPN would not obviously have terminated behind the NIC, given the express disclosures and drawings in Neufeld, and the testimony of PO’s expert. POR at 23-26; EX2006, ¶¶ 33-36, 44, 57, Figures 2-3.

Neufeld only mentions VPNs in four discrete sentences, and each is directed toward network access. *See* EX1005, ¶ [0009] (“Clients may also have the ability to *access these networks via a virtual private network*”), ¶ [0022] (“the system

administrator must typically *use . . . a virtual private network to access the system*”), ¶ [0088] (“a user . . . may *attempt different types of remote connections*, such as *via . . . a virtual private network*” and “users . . . *may be permitted access . . . via a virtual private network*”). These are not disclosures that the VPN is behind the NIC.

Looking, then, to what a POSITA would have understood, Dr. Noubir explained that a POSITA would have understood a VPN to terminate *outside the managed device—typically at a VPN gateway or network router*. EX2006, ¶¶ 33-36, 44, 57, Figures 2-3. Dr. Noubir also relied on documentation to support this. The relevant text from Dr. Noubir’s declaration states:

A Virtual Private Network (“VPN”) is a Private Network where some of the links are virtual, *meaning they connect two nodes by tunneling traffic over other networks such as the Internet*. . . . In the example shown in Figure 2, the two branches are “connected” to a VPN tunnel *that terminates at a router on each branch*. Ex. 2009, Page 6. A POSITA would understand that this is a typical layout for a general purpose VPN with two branches.

(Emphasis added).

FIG. 2 of EX2009 is reproduced below. Petitioner has not challenged its authority. Consistent with Dr. Noubir’s testimony, it shows *a VPN tunnel between two networks, each terminating at a router on one of them. These routers are external to any of the computers or other devices on the network*.

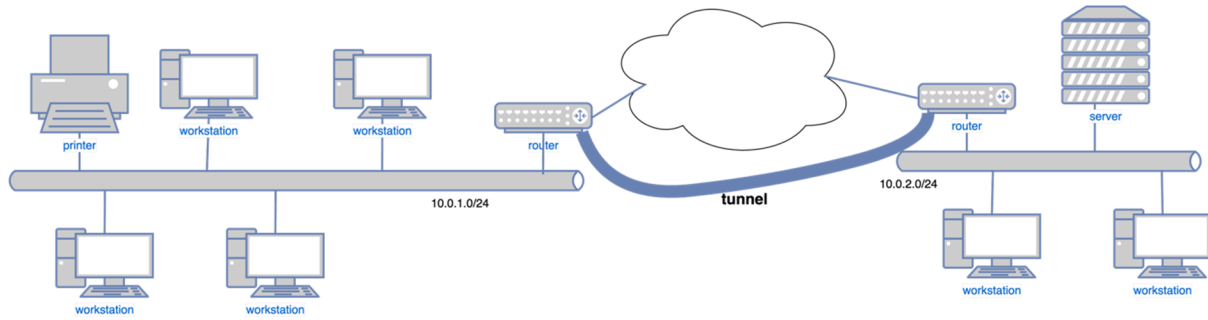


Figure 1. An example of virtual private network with two branches (each with private IP addresses) connected by a VPN tunnel.

Petitioner makes noise about Dr. Noubir’s use of the words “general purpose VPN” instead of “point-to-point VPN with tunneling.” Reply at 14-18. This is mere semantics. Dr. Noubir’s statement and citations make clear what he meant: a VPN that bridges two networks with a tunnel that terminates at points on those networks, such as the routers shown in Figure 2. This is in stark contrast to the VMI of Claim 1 and its supporting disclosures, such as FIG. 3, which shows a non-traditional use of the VMI, located between the SMACC and the user data interfaces, with its location being essential to separating management data from user data *before it is passed to those interfaces*. This is explicitly explained in the ‘140 Patent:

A VMI is also established for logically separating management traffic from user data when the in-band path is to be used for management data. *The VMI is the interface between the SMACC chipset and the user data interfaces.* The VMI utilizes existing and developing technology such as VPN *to build secure tunnels between the SMACC chipset and the management center while utilizing user data interfaces* of the managed device and the user network *to provide the transport* of the management data cost effectively. The VPN

technology provides the logical separation, confidentiality, and integrity of the management traffic while it is in transit.

EX1002, 6:22-33 (emphasis added).

Petitioner offers no evidence to contradict this. The only evidence presented in this proceeding from the standpoint of a POSITA indicates that a point-to-point VPN with tunneling, even if read into Neufeld, *would not have utilized user interfaces of the managed network element to make the connection to the network N*.

3. Petitioner’s Obviousness Theory is Legally and Evidentiary Defective

Federal Circuit precedent makes clear—§ 103 does not allow “stitching” together isolated fragments of prior art while ignoring their full context. *In re Enhanced Sec. Research, LLC*, 739 F.3d 1347, 1355 (Fed. Cir. 2014). Yet Petitioner does exactly that, lifting brief VPN references from Neufeld—limited to discussion of remote access and access control—not any disclosure of logical separation, internal VPN termination, or management channel routing. Petitioner then extrapolates an entire VMI from these few stray sentences, relying solely on conclusory assertions from Dr. Meldal without any contemporaneous evidence or reasoned analysis. Such ipse dixit opinions fall short of the evidentiary standard required under *Arendi S.A.R.L. v. Apple Inc.*, 832 F.3d 1355, 1362 (Fed. Cir. 2016) (rejecting reliance on “common sense” to supply non-trivial limitations), and *TQ*

Delta, LLC v. Cisco Sys., Inc., 942 F.3d 1352, 1360 (Fed. Cir. 2019) (requiring expert testimony to provide “reasoned analysis”). Because Petitioner’s case rests on selective citation and unsupported expert ipse dixit, it fails to establish prima facie obviousness of claim 1.

Throughout its Reply, Petitioner attempts to hide the ball. It mischaracterizes PO’s arguments and sidesteps the real issue: Neufeld’s passing references to VPNs disclose only their traditional use for network access, not the claimed architecture in which a point-to-point VPN tunnel terminates behind the NIC and is integrated with the SMACC as claimed. Petitioner attempts to make up for its lack of evidence by criticizing Dr. Noubir, going so far as casting doubt on his testimony because he “admitted at his deposition that he never read Dr. Meldal’s declaration.” Reply at 18-19. This actually highlights the evidentiary value of Dr. Noubir’s testimony versus Dr. Meldal’s—while Dr. Noubir’s declaration is highly supported by contemporaneous technical literature, Dr. Meldal’s merely parrots the Petition. There was no need for Dr. Noubir to read it because on all the relevant points, the Petition said the same thing. Dr. Noubir’s testimony, *and the scholarly articles he used to back up his opinions*, confirm that a POSITA would have understood VPNs to terminate at gateways or routers external to managed devices, not at an internal controller as claimed.

The '140 Patent expressly distinguishes itself by locating the VMI within the managed device and virtualizing the user data interfaces to achieve the claimed logical separation of data, and Petitioner offers no contrary evidence or explanation of how to reconfigure Neufeld to provide this capability. The Board should therefore reject Petitioner's attempt to rewrite Neufeld and find that Ground 1 fails for lack of any disclosure or motivation to arrive at the claimed configuration.

B. Neufeld Does Not Clearly Disclose or Suggest an In-Band Network Over Which Management Data is Actively Communicated

The Petition further argues that VPN tunneling would inherently or obviously separate management and user data. Petition at 34. Both parties agree that this function is never expressly stated in Neufeld. *See id*; POR at 28. The parties diverge on whether this functionality would have been inherent in Neufeld (or obvious therefrom).

Petitioner's reliance on paragraphs [0043], [0047], and [0048] of Neufeld to argue that management data is transmitted over the in-band Network N, such that a VPN would inherently or obviously separate management data from user data, is misplaced. See Reply at 7-8. A careful reading of Neufeld, including Figures 2 and 3, shows Network N is not directly coupled to the RMC. POR at 28-34. Instead, Neufeld consistently discloses that management data is transmitted through a dedicated out-of-band channel (Network M), such as via Ethernet interface 180. *Id*. Paragraphs [0043], [0047], and [0048], *when read in context*, describe the RMC's

hardware-level connections for passive snooping of server activity and redirection of keyboard/video traffic via the out-of-band network M—not active in-band management communication. At best, these passages are ambiguous, contradictory and do not support Petitioner’s theory. They in fact further support PO’s position. Petitioner attempts to re-characterize the express disclosures in Neufeld in terms of what a POSITA would have wanted—but that does not change the fact that the disclosed architecture is not capable of operating in the manner Petitioner suggests.

1. Neufeld’s Overall System Architecture

Petitioner contends that the claim language is obvious over Neufeld because it purportedly transmits management data over its in-band network path (Network N). While never directly stated, the Petition assumes that any VPN tunnel employed over Network N would inherently provide the claimed logical separation of management and user data. See Petition at 32–34.

This theory fails for one simple reason: **Neufeld never discloses transmitting management data over Network N.** Instead, Neufeld consistently teaches that management data is transmitted through a dedicated out-of-band channel via management network M, not through an in-band path, with a focus on independence from the system’s OS. For example, paragraph [0034] describes “special circuitry and software for capturing, analyzing, compressing and transmitting video activity to the remote console 5 independent of an operating system.” Paragraph [0037]

emphasizes this: “In the operation of the present technique, video data is captured, analyzed, compressed, and transmitted to the remote console 5 by circuitry and software in the managed server 2 without reliance or interference with the operating system.” This circuitry and software include, in relevant part, an RMC, which is directly coupled to the management network M for exactly this purpose. *See* EX1005, ¶ [0047]. Thus, the premise on which Petitioner’s argument rests is unsupported by the reference and inconsistent with its architecture.

Neufeld as a whole is directed toward minimizing security breaches that may occur when network administrators attempt remote access of other devices in a networked computing environment. EX1005, ¶¶ [0005]-[0010], [0015], [0016], [0018]-[0023]. Devices in such environments are networked via a user network, referred to as Network N. *Id.* at [0007]-[0009], [0034], [0035]. The system also includes a management network M—an out-of-band network used exclusively by network administrators. *Id.* at [0043], [0047], [0054], [0061] (referring to Network M as “maintenance” network M, explaining its direct connection with the RMC, describing the RMC’s operation with the IOP 156 for management processing, and explaining the RMC’s operation to route keystrokes via the network M).

The system, showing a remote management PC 5 and a managed server 2 are shown in FIG. 1 (below). Both are coupled to the Network N as they are both part of the same enterprise network. EX1005, ¶¶ [0007], [0034], [0035]. The Network M

is exclusively used for transmission of management data between the remote management PC and managed servers. EX1005, ¶¶ [0012], [0013].

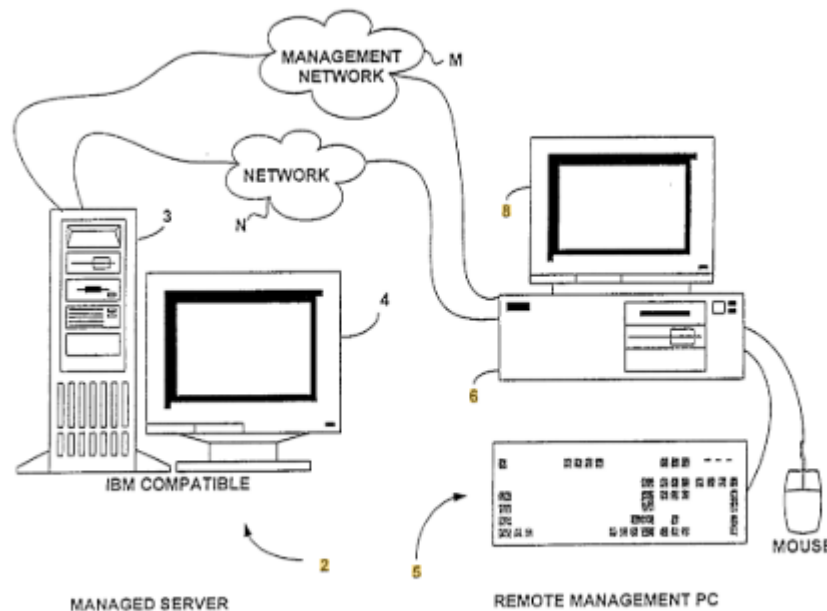


FIG. 1

While this system architecture is covered in the publication, Neufeld is primarily about enhancing security when management data is transmitted between the remote management PC and the managed server. EX1005, ¶¶ [0034], [0035], [0043], [0047], [0061], [0077]. The functioning of these networks, and what data is transmitted over them, is not clearly addressed in the publication. Both parties have instead largely referred to different text to *infer* the intent of Network N. Petitioner says the intent is a system that uses both in-band and out-of-band communication of management data. Reply at 3-5. PO argues the intent was to use only the more secure option, Network M, for exclusive out-of-band communication

of management data, consistent with the overall intent of the publication to increase security of management data and use a method that works independent of the OS. POR at 13, 30-32. What is clear, however, is that there is *no clear expression* in Neufeld that a POSITA could use to say *definitively* that management data is inherently or obviously transmitted over the Network N. Accordingly, Petitioner's argument that Neufeld inherently separates management data from user data over the in-band channel is fundamentally flawed: **there is no management data on the in-band channel to separate.**

2. Paragraph [0043] Does Not Support Petitioner's Position

Petitioner relies on paragraph [0043] to argue that the RMC is connected to “network N and/or management network M,” suggesting that management traffic may be routed over Network N. Reply at 7; EX1005, ¶ [0043]. This paragraph is at best inconsistent with FIG. 2. Further, read in context with the rest of the publication, this refers to the hardware-level coupling of the RMC to allow passive snooping, not active transmission of management data.

Paragraph [0043] describes FIG. 2 (below) and states “[t]he remote management controller 116 connects to the keyboard controller 38, *the network N and/or a management network M*, a keyboard 52, and a mouse 54 to provide functionality for accessing, interacting, and monitoring the managed server 2 from the remote console 5” FIG. 2, nevertheless, *only shows* the network M passing

through the RMC, with the Network N coupled to the NIC, which is coupled to the PCI Bus. From paragraph [0043] and FIG. 2, alone, Neufeld's intention is un-clear. Paragraph [0043] states that the RMC connects to one, the other, or both, of Network N and/or M, but FIG. 2 only shows the RMC connected to the management network M, and not N.

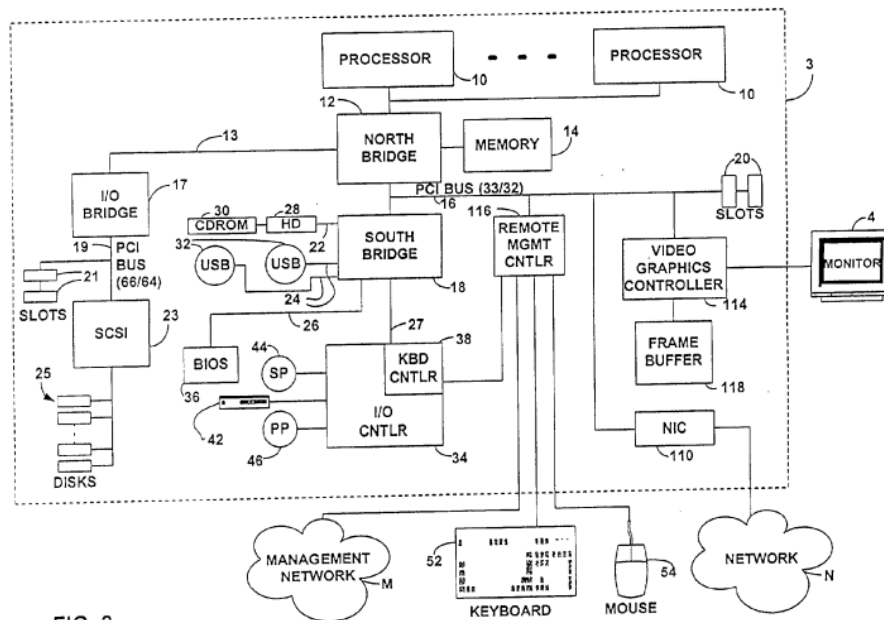


FIG. 2

Paragraph [0043] identifies the RMC's attachments to the PCI bus, and other system components, to support out-of-band monitoring. The purpose of these connections is enabling the RMC to capture video, keyboard, and bus activity without OS involvement. *Id.* at ¶¶ [0011], [0016], [0047], [0048]. **Figures 2 and 3 confirm Network N is not used for active management communication but is simply part of the system interconnect the RMC can observe.**

At best, paragraph [0043] is ambiguous when compared to the clear disclosure in the figures and the explicit description of the Ethernet interface 180 as the RMC's "main external communication interface." *Id.* at ¶ [0061]. Such ambiguity cannot substitute for actual disclosure of the claimed limitation. *See LG Elecs. Inc. v. Immervision, Inc.*, 39 F.4th 1364, 1372 (Fed. Cir. 2022) ("[W]here a prior art reference includes an obvious error of a typographical or similar nature that would be apparent to one of ordinary skill in the art who would mentally disregard the errant information as a misprint or mentally substitute it for the correct information, the errant information cannot be said to disclose subject matter.").

3. Paragraph [0047] Reinforces Passive Monitoring, Not In-Band Management, and Adds Further Confusion About Network N's Function

Paragraph [0047] states "[t]he remote management controller 116 also includes circuitry to route keystrokes to the keyboard controller 38 . . . ***via the modem or NIC 110 which may be coupled to the Network M.***" Petitioner relies exclusively on this sentence for active communication of management data ("keystrokes") via the Network N; however, the express language of that paragraph indicates that such communication is over the Network M, not the Network N. Reply at 7.

Petitioner, **for the first time in its Reply**, refers to this as a "mistake," suggesting the appropriate correction is a substitution of "Network N" for "Network

M,” which they say is consistent with FIG. 2. *Id.* However, for this to be correct, the Network N would have to be directly coupled to the RMC 116, as that is what paragraph [0047] expressly states. Since that is not shown in any of the drawings (FIG. 3 also shows the RMC only coupled to the network M), the obvious correction, if any, is to remove “or NIC” from the sentence. The resulting statement is entirely consistent with FIGs. 2 and 3, which show only Network M directly coupled to the RMC, and would fulfill the express purpose of the patent—enabling remote and secure connection independent of the OS. POR at 28, 30-32.

At face value, paragraph [0047] describes routing keystrokes as part of the RMC’s remote console redirection—a classic out-of-band function—over the management network M. Keystroke redirection is implemented at the hardware/firmware level to provide OS-independent remote access. See EX2006, ¶ 47. This is reinforced by the incorporation by reference of Patent No. 5,898,861, which emphasizes the snooping function and identifies this as console re-direction that is OS-independent. EX2012, 10:13-41. Nothing here suggests management commands travel over the in-band path as Petitioner asserts.

4. Paragraph [0048] Describes Video Redirection, Not VPN-Based Logical Separation

Paragraph [0048] describes the RMC’s ability to capture video data from the frame buffer, compress it, and transmit it “via one of the communications devices”

(modem or NIC 110). EX1005, ¶ [0048]. This pertains to remote console video redirection—another hallmark of out-of-band management.

Importantly, paragraph [0048] does not mention VPN tunneling, logical separation, *or transmission of management commands over the in-band network*. Instead, it describes the RMC sending *compressed video data* to a remote console for monitoring server activity. *The use of NIC 110 in this context does not transform the in-band path into a management channel*; it shows the RMC can redirect video output using available communication hardware.

The RMC is a control unit that resides on the managed server. EX1005, Figure 2. Video data is sent in one direction, from the managed server to the remote management PC. Accordingly, this is not transmission of management data, but rather user data sent over the connection that would normally be used for this purpose. Accordingly, at best, the redirection of video data is transmission of user data over the Network N.

Thus, paragraph [0048] further supports PO's position that Neufeld's architecture is designed for out-of-band management, not in-band VPN tunneling of management data.

5. Ambiguity and Contradiction Weighs Against Obviousness

As established, Neufeld's disclosures are ambiguous, and ambiguity cannot serve as a substitute for disclosure. In his deposition, Dr. Noubir highlighted such

inconsistencies and how they impact a POSITA's interpretation of Neufeld's architecture. One example is:

A. . . . Neufeld has inconsistencies. What will make sense is to go over the management network. There are mentions somewhere in Neufeld . . . , sometimes they refer to network N, but for mechanisms that don't make sense. So that is . . . what I explain in [my] declaration, and I tried to reconcile these things.

. . .

A. [T]o me, Neufeld, as the abstract says, it is a security system [that] includes different authentication levels and/or different privileges based on certain criteria.

So it is more about privileges . . . and higher level things and so on. The claims are all about that. It has description of various kind of things. A POSITA reading these things . . . will get confused because there are things that are inconsistent. The out-of-band . . . that's the one that will make sense. The other, the in-band, even if there are references to it . . . I explained a little bit how to try to make sense of that.

Q. Okay. Let's go to paragraph 46 of your declaration. . . .

You say the management network M . . . is in fact the only network coupled to Neufeld's remote server management controller 116, correct?

A. Yes.

Q. Now you're aware, and you discussed in your declaration . . . that paragraph 43 of Neufeld says something different. Paragraph 43 of Neufeld . . . says that the remote management controller 116 connects to a keyboard controller 38, the network N . . . and/or a management network M . . . and then some other devices, correct?

A. Yes.

Q. Okay. So your statement in paragraph 46 that the RMC 116 is only connected to network M is not correct in light of paragraph 43

because paragraph 43 says that the RMC is connected to the network N, correct?

A. No. What . . . I'm saying there . . . is . . . in Figure 3 of Neufeld the ethernet interface is coupled to the network [M]. The management network [M] is the only network coupled to Neufeld's remote server management.

And here by "coupled" I'm meaning that it has full control over it.

". . . At first glance, paragraph [0043]" . . . "may appear to suggest a contradiction by stating that the remote management controller 116 connects to . . . the network N and/or the management network M".

So basically . . . I'm explaining . . . that there is something inconsistent in some sense with how POSITA would have understood Neufeld. And . . . one of the last sentences [in my declaration] is that "POSITA would recognize that the reference to network N merely identifies that the remote management controller can passively monitor the data sent to or received from the managed device over the network; it must be connected to that path to snoop on the traffic, but that connection does not equate to active participation in the data transmission or use of the primary network interface for management communication".

EX1049, 56-59.

Petitioner dismisses these inconsistencies as "imaginary" and an improper extrapolation of Neufeld's disclosures and criticizes Dr. Noubir for saying that such inconsistencies, when read along with the remainder of the disclosure, make it difficult for a POSITA to conclude that the Network N is used for transmission of management data. *See* Reply at 11, 14. Yet Petitioner also admits to the very inconsistencies that Dr. Noubir highlighted in his testimony. Reply at 7. The only expert who testified in this IPR on the subject was Dr. Noubir, and his opinion was

that such inconsistencies should be resolved against the Petitioner's interpretation on page 7 of the Reply.

The burden is on Petitioner to demonstrate, by a preponderance of the evidence, that Neufeld teaches or suggests the claimed limitation. 35 U.S.C. § 316(e). Where the prior art is contradictory or unclear, the Petitioner has not met its burden, and the Board must resolve that doubt against the challenger. Neufeld repeatedly emphasizes OS-independent, out-of-band management via the Network M. Petitioner's theory depends on importing functionality Neufeld neither discloses nor suggests. That type of hindsight reconstruction cannot support a finding of obviousness.

6. Petitioner's VPN-Based Obviousness Theory Fails Because it Depends on a Misreading of Neufeld and Lacks Any Evidentiary Support

Petitioner's obviousness theory fails because it mis-reads Neufeld. Neufeld does not disclose management data traversing Network N, much less the use of VPN tunneling to separate traffic on that network. Instead, Neufeld describes the RMC's hardware attachments that enable OS-independent, out-of-band monitoring and redirection through dedicated management channels. Neufeld is ambiguous, and ambiguity cannot meet Petitioner's burden under § 316(e). Petitioner had every opportunity to provide the declaration of a POSITA to support their interpretation of

such inconsistencies, or to opine on their position that Neufeld is internally consistent, but did not.

Petitioner suggests the ambiguities should be resolved by a POSITA's desires and even highlights that Dr. Noubir was asked at his deposition whether he would have wanted a managed server to have this capability in case the out-of-band network becomes inoperative and "gave the only answer any reasonable person could: 'of course'." Reply at 9. Petitioner criticizes Dr. Noubir for suggesting that, regardless of what he would have wanted, it is not disclosed anywhere in the publication. *Id.* ("[H]e then dissembled about not seeing that disclosure in Neufeld . . ."). There was no dissembling...that disclosure simply isn't there, and a POSITA would **not** have read Neufeld's architecture as even supporting that functionality. As Dr. Noubir stated in his deposition:

A. So to be able to have Neufeld transmit data over the network and interface the NIC 110 . . first, the operating system has to be running and you need to have some software that works with the RMC to . . . whatever data needs to go over the network N and then re-inject it through . . . the software layers, the driver and so on, running on the device management to go over network N interface. That is . . . how I feel . . . what would need to do this.

Q. Is any of that software that would be needed to run described in Neufeld?

A. No

For these reasons, Neufeld does not teach or suggest the "virtual management interface connection means" of Claim 1, and the Petition must be denied.

III. PETITIONER'S REPLY IMPROPERLY RAISES A NEW ARGUMENT AND FAILS TO PROVIDE A MOTIVATION TO COMBINE IPMI AND LAWRENCE

Under the Board's rules, a Reply is strictly limited to responding to arguments raised in the POR. 37 C.F.R. § 42.23(b) (2024) "Petitioner may not submit new evidence or argument in reply that it could have presented earlier . . . to make out a prima facie case of unpatentability." *Office Patent Trial Practice Guide, August 2018 Update*, at 14. "To the extent that a reply . . . 'responds' to the institution decision . . . , 'respond,' . . . does not mean embark in a new direction with a new approach While replies . . . can help crystalize issues for decision, a reply . . . that raises a new issue . . . may not be considered." *Id.* at 14-15. "Examples of new issues [include] *a newly raised rationale to combine the prior art references that was not expressed in the petition.*" *Id.*

The ID found that "Petitioner does not sufficiently show why [a POSITA] would have been motivated to use a VPN on an internal connection (side-band interface) within a server . . ." ID at 29. Petitioner's Reply does not rebut PO's showing *that the Petition does not sufficiently show why a POSITA would have been motivated to use a VPN on the side-band interface within a server.* Reply at 19-22. Instead, Petitioner advances a ***new theory***: that a "fair reading" of the petition demonstrates that incoming management traffic received over Lawrence's generic routing and forwarding module 612 is already protected by Lawrence's VPN module

655, and thus a skilled artisan would have understood both external and internal management traffic as VPN-protected. *Id.* This is a ***new rationale*** constructed from different portions of Lawrence than those relied upon in the Petition, and is presented for the first time in the Reply.

This argument should be disregarded as an improper ***new theory***. The Petition did not raise or rely on these passages of Lawrence, thus necessitating using them for the first time in its Reply. Petitioner's attempt to now rewrite its motivation-to-combine theory is barred by § 42.23(b) and controlling case law. Petitioner's theory also fails substantively as it amounts to an explanation of how Lawrence allegedly operates, not an explanation of why a POSITA would have been motivated to modify IPMI in view of Lawrence. *See* Reply at 20-21 (discussing Lawrence and not the alleged Lawrence/IPMI combination). Such discussion does not supply the missing rationale to bridge the two references. Accordingly, Petitioner's Reply both procedurally exceeds the scope of § 42.23(b) and substantively fails to cure the defect identified by the Board. The new argument should be disregarded, and even if considered, it cannot establish a motivation to combine IPMI and Lawrence.

IV. PETITIONER HAS FAILED TO DEMONSTRATE THE UNPATENTABILITY OF THE CHALLENGED CLAIMS

Because Petitioner never shows where Neufeld or IPMI and Lawrence provide an internal VMI that uses the device's user interfaces to connect to the

SMACC and logically separates management/user data on those same interfaces, the

Petition fails to meet its burden and the challenged claims should be confirmed.

Respectfully submitted,

Dated: September 17, 2025

By: /Brandon R. Theiss/
Brandon R. Theiss (Reg. No. 70,507)
Volpe Koenig
Counsel for Patent Owner

CERTIFICATE OF COMPLIANCE WITH WORD COUNT

Pursuant to 37 C.F.R. § 42.24(d), I certify that this Patent Owner's Sur-Reply complies with the type-volume limits of 37 C.F.R. § 42.24(b)(1) because it contains 5,589 words, excluding the parts of this Patent Owner's Sur-Reply that are exempted by 37 C.F.R. § 42.24(a), according to the word processing system used to prepare this Patent Owner's Sur-Reply.

Respectfully submitted,

Dated: September 17, 2025

By: /Brandon R. Theiss/
Brandon R. Theiss (Reg. No. 70,507)
Volpe Koenig
Counsel for Patent Owner

CERTIFICATE OF SERVICE

The undersigned certifies that pursuant to 37 C.F.R. § 42.6(e), a copy of the foregoing **PATENT OWNER'S SUR-REPLY** was served via email (as consented to by counsel) on September 17, 2025 to lead and backup counsel of record for Petitioners as follows:

James Heintz
Jim.heintz@us.dlapiper.com

Gianni Minutoli
gianni.minutoli@us.dlapiper.com

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

Dated: September 17, 2025

By: /Brandon R. Theiss/
Brandon R. Theiss (Reg. No. 70,507)
Volpe Koenig
Counsel for Patent Owner