

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. IPR2024-00109
U.S. Patent No. 8,474,016

Patent Owner Demonstratives

Representative Claim of the '016 Patent

1. An apparatus, comprising:

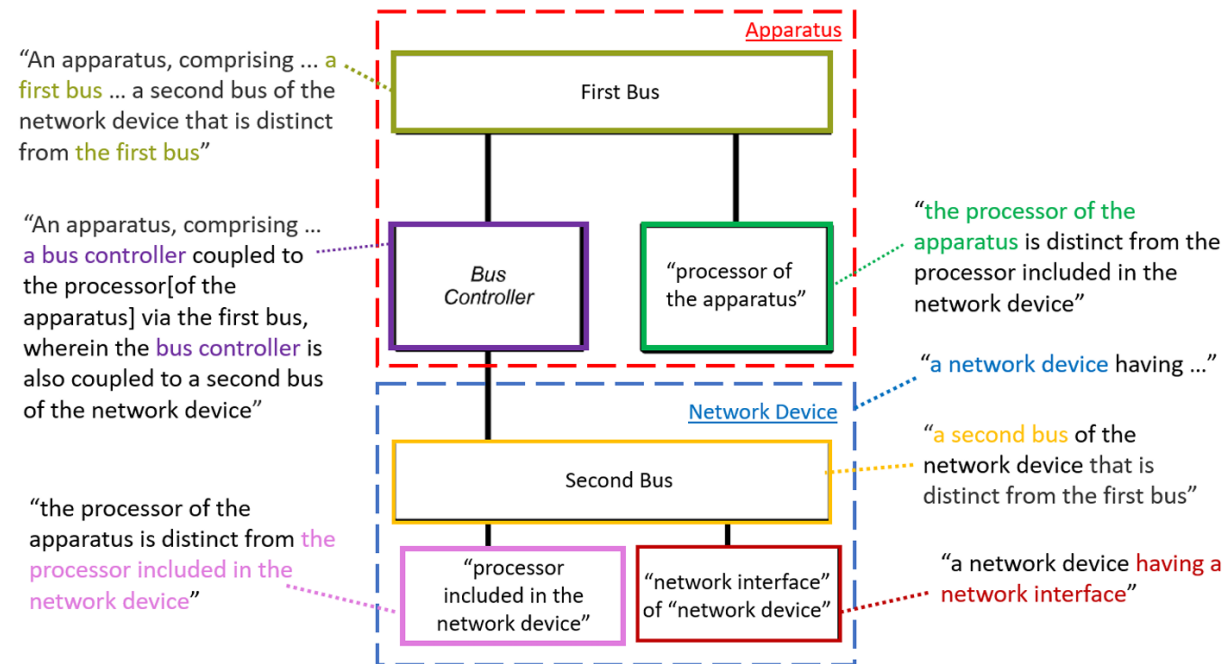
a processor configured to control one or more functions of a network device having a network interface, wherein the network device is configured to receive data requests and an encrypted form of management requests via the network interface, wherein the management requests are from a remote administrator;

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;

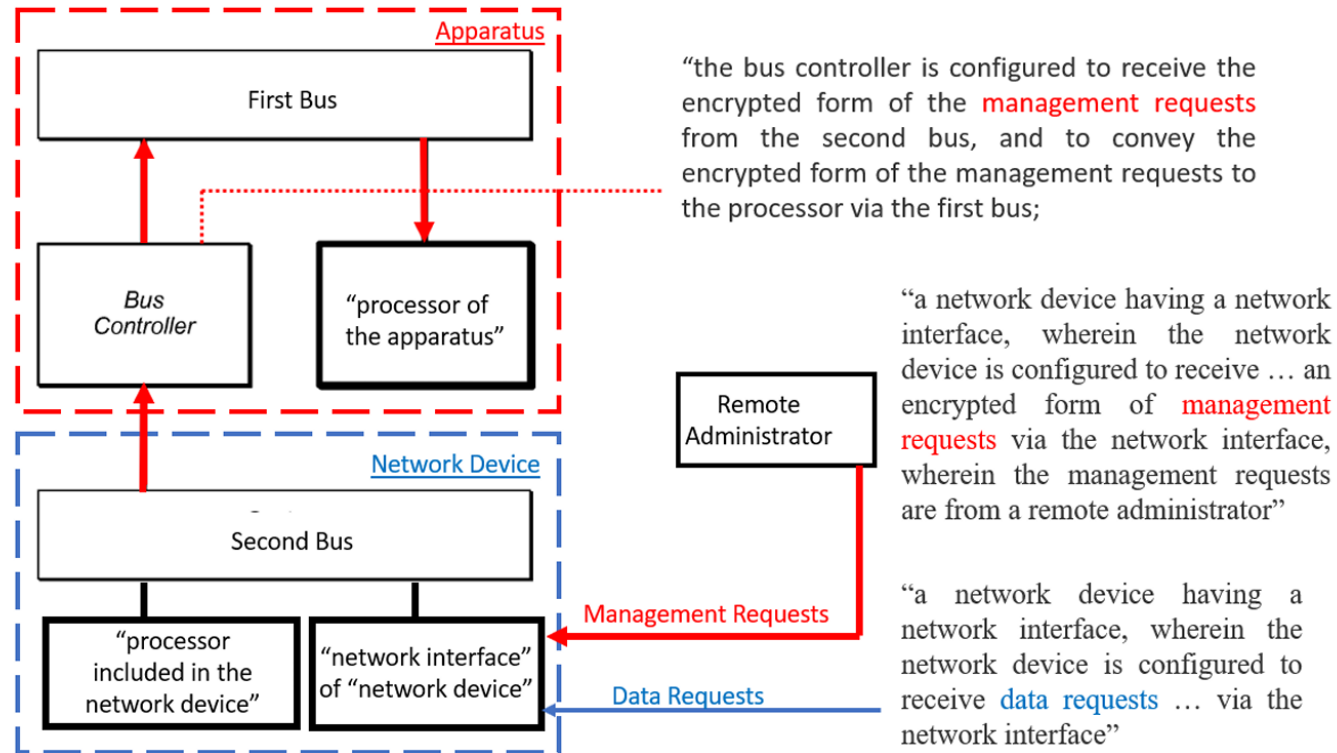
wherein the processor is configured to decrypt the encrypted form of the management requests, wherein the network device includes a processor configured to facilitate operation of the network device, and wherein the processor of the apparatus is distinct from the processor included in the network device.

Elements of the '016 Claims



POR, 21

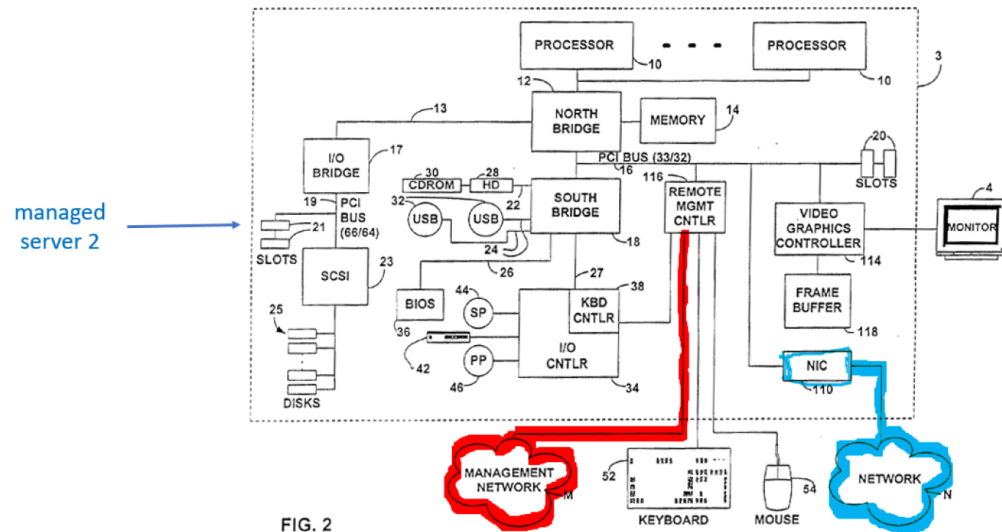
Actions of the '016 Claims



POR, 22

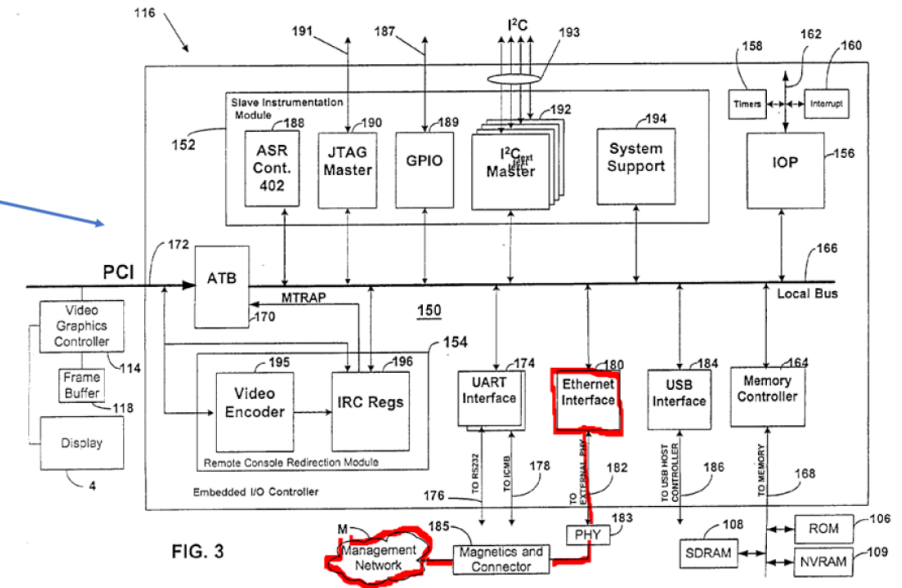
Neufeld Teaches “Out of Band” Communication

Neufeld's Management Requests are sent over the Management Network



POR, 27

Remote Management Controller (RMC) 116 within Managed Server 2



POR, 28

[0061] The embedded I/O controller 150 may also include an Ethernet interface 180, which is operatively coupled to the internal local bus 166. The Ethernet interface 180 provides the main external communication interface between the remote server management controller 116 and the outside world. In the exemplary embodiment shown in FIG. 3, the integrated portion of the Ethernet interface 180 includes a MAC (Media Access Controller), inbound and outbound FIFOs and a DMA engine to transfer packets automatically to and from memory. The Ethernet interface 180 utilizes a connection via interface 182 to an external PHY 183 and typical magnetics and connectors 185 to couple the PHY 183 to the wire that serves as the transmission media. For example, this connection is typically used to couple the remote management controller 116 to the management network M.

EX1005, [0061]

Petition “*Corrects*” a mistake in Neufeld

desirable” to provide in-band communications to capture the maximum amount of information from, and allow control of, the managed server). Neufeld also discloses that “[t]he remote management controller 116 **connects to ... the network N** and/or a management network M ... to provide functionality for accessing, interacting, and monitoring the managed server 2 **from the remote console 5** as will be more fully described below” and “[t]he remote management controller 116 also includes circuitry to route keystrokes to the keyboard controller 38 from either the local keyboard 52 or from the remote console 5 via the modem or NIC 110 which may be coupled to the network M [*sic*, N].” EX1005, ¶¶[0043], [0047]. See also EX1005, ¶[0045], Figs. 2-3 (showing connection between Network N and remote management controller 116); EX1003, ¶¶86-87.

Petition, 20

information from, and allow control of, the managed server). Neufeld also discloses that “[t]he remote management controller 116 **connects to ... the network N** and/or a management network M ... to provide functionality for accessing, interacting, and monitoring the managed server 2 **from the remote console 5** as will be more fully described below” and “[t]he remote management controller 116 also includes circuitry to route keystrokes to the keyboard controller 38 from either the local keyboard 52 or from the remote console 5 via the modem or NIC 110 which may be coupled to the network M [*sic*, N].” EX1005, ¶¶[0043], [0047]. See also EX1005, ¶[0045], Figs. 2-3 (showing connection between Network N and remote management controller 116); EX1003, ¶¶86-87.

Petition, 25

"DEMONSTRATIVE EXHIBIT - NOT EVIDENCE"

[0047] The remote management controller 116, as described in more detail below, includes circuitry for snooping the PCI bus for configuration transactions between the processor 10 and the video graphics controller 114 to determine configuration and mode information, such as whether the video graphics controller is in text or graphics mode. More specifically, the remote management controller 116 snoops indexed input/output (I/O) ports of the video graphics controller 114 to provide a set of shadow registers corresponding to mode information. These I/O ports are particularly helpful for legacy video graphics array (VGA) compatibility mode. In addition, the shadow registers of the remote management controller 116 provide a set of registers for the I/O processor 156 to access independently of the operating system running on processor 10, thereby preventing any conflicts that could arise if both processors were trying to access the indexed I/O ports simultaneously. The remote management controller 116 also snoops and stores configuration information sent by the processor 10 to the video graphics controller 114. This information is used to identify the location of the linear aperture as well as the location of other configurable resources in the video graphics controller 114, (e.g., location of SVGA register file). The remote management controller 116 also includes circuitry to route keystrokes to the keyboard controller 38 from either the local keyboard 52 or from the remote console 5 via the modem or NIC 110 which may be coupled to the network M.

This keyboard functionality is more fully explained in U.S. Pat. No. 5,898,861, entitled “Transparent Keyboard Hot Plug.”

EX1005, [0047]₇

Neufeld's Paragraph [0043] doesn't help either

[0043] Further attached to the PCI bus **16** is a remote management controller **116**. The remote management controller **116** connects to the keyboard controller **38**, the network **N** and/or a management network **M**, a keyboard **52**, and a mouse **54** to provide functionality for accessing, interacting, and monitoring the managed server **2** from the remote console **5** as will be more fully described below.

EX1005, [0043]

Accordingly, paragraph [0043] is simply describing that RMC 116 connects to the PCI bus in order to access, interact with and monitor the managed sever 2. As Patent Owner's expert explains, this underscores the remote management controller's (RMC's) ability to passively monitor, or "snoop," system activity by virtue of its direct connections to both the PCI bus and the keyboard controller. By being attached to the PCI bus, the RMC is positioned to observe bus-level transactions, including configuration and memory operations involving components like the video controller, allowing it to capture display data for redirection to a remote user. The RMC's connection to the keyboard controller further enables it to snoop keyboard input—monitoring scan codes transmitted from a physical keyboard to the system's 8042 controller—so that it can emulate or replicate those keystrokes remotely. These hardware-level connections enable the RMC to collect input/output state information non-intrusively, *without requiring cooperation from the host operating system*, and are foundational to its out-of-band management capabilities, such as remote console control and system diagnostics. EX2007, ¶125.

Several Ways to Correct the Mistake

Erroneous Sentence From Neufeld	Petitioner's Proposal For Correction	Patent Owner's Proposal For Correction
The remote management controller 116 also includes circuitry to route ... via the modem or <u>NIC 110</u> which may be coupled to the network <u>M</u> . EX1005, [0047] (emphasis and coloring added).	The remote management controller 116 also includes circuitry to route ... via the modem or <u>NIC 110</u> which may be coupled to the network <u>M</u> . Petition, 20 and 25 (emphasis and coloring added)	The remote management controller 116 also includes circuitry to route ... via the modem or ~~NIC 110~~ <u>Ethernet Interface 180</u> which may be coupled to the network <u>M</u> .

POR, 30

“where 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”

LG Elecs. Inc. v. Immervision, Inc., 39 F.4th 1364, 1372 (Fed. Cir. 2022)

In the POR, Patent Owner presented expert *testimony* that provided a *detailed rationale* explaining why a POSITA would *not* have corrected the “error” as suggested in the Petition, but instead would have changed “NIC 110” to “Ethernet Interface 180.” POR, 28-31, *citing* EX2007, ¶¶88-91. As part of this rationale, Patent Owner’s expert relied on (i) Neufeld’s *criticisms* of *in-band* systems where communication with the server is “only possible when the server is able to communicate over its normal network connection” which Neufeld contrasted with *out-of-band* communication that Neufeld characterized as “*a much more powerful tool* for server management,” and (ii) Neufeld’s *focus* as an *out-of-band* remote management solution. EX2007, ¶¶90-91, *citing*, EX1005, [0011]-[0014] (emphasis added); [0059] (discussing the establishment of “*out-of-band* communication sessions”); [0060] (discussing an *out-of-band* communication session with remote server management controller 116”); [0061] and [0062] (“The user may, thus, engage in *out-of-band* communication with the remote server management controller 116 ...”) During his deposition, Patent Owner’s expert did not waiver from

Sur-Reply, 3

Patent Owner's Expert Confirmed that Neufeld is out of band

Q. ... Given that you now understand that petitioner's position is that Neufeld's system includes both in-band and out-of-band communication of remote management messages, it is not true that, under petitioner's position, Neufeld is being transformed from an out-of-band system to an in-band system, correct?

MR. GOLUB: Objection, misstates his misstates the witness' declaration.

THE WITNESS: *I still stand by my statement.* Neufeld is out-of-band remote management system. That's what it teaches. And any construction trying to suggest it otherwise is flawed.

BY MR. HEINTZ:

Q. Your position is Neufeld teaches only out-of-band communication, right?

A. That is correct.

Q. And that also means that Neufeld's system as described in Neufeld is only capable of out-of-band communication of remote management messages, correct?

A. Anybody in 2003 with ordinary skill would make that interpretation.

* * *

Q. Let me rephrase the question. You're saying that it's your opinion that it's not possible for a remote management command to come to remote management controller 116 via network N and through NIC 110 of figure 2?

A. That is correct based on Neufeld.

Sur-Reply, 4

Q. Okay. It's not possible for Neufeld's system to send a remote management command through the network N, the NIC 110 over the PCI bus 16 to the remote management controller 116?

MR. GOLUB: Objection.

BY MR. HEINTZ:

Q. That's your opinion, correct?

MR. GOLUB: Objection, asked and answered.

Q. Correct, Dr. Mishra?

A. I already answered it.

Q. Did I state your opinion correctly?

A. It is not possible, based on Neufeld construction, remote management commands to come from network N to remote management controller 116.

Sur-Reply, 5

Petitioner Offers no evidence why their correction would be understood by a POSITA

[0015] An important goal in the development of remote server management tools is to increase the number of server problems that may be analyzed and repaired remotely (that is, without requiring direct, on-site intervention by a member of the network management team). To facilitate that goal, it is highly desirable to have a network management tool that is able to capture the maximum amount of information from a managed server in the maximum range of operational states of the server (for example, (1) in-band online; (2) in-band offline; (3) out-of-band online; and (4) out-of-band offline) and to allow control of the managed server based on that data.

EX1005, [0015]

Q. Well, sir, it does more than that, doesn't it? What it says is it's highly desirable to have a network management tool that is able to capture the maximum amount of information from a managed server in the maximum range of operational states, and then it lists all four. Isn't that a statement in Neufeld stating that the best system is the one that can do all four of those possibilities, yes or no?

A. No.

Q. Okay.

A. So I'll state the reason.

Q. All right.

A. The whole context of my declaration is to talk about Neufeld is all about out-of-band management. In that context, this paragraph has no meaning. This paragraph is simply saying the obvious. When you are doing the network management, you want to know what is happening to your server, whether it's doing in-band communication, out-of-band communication, whether they're offline or online. Irrespective of how you want to manage, you want to monitor these scenarios. You want to know these scenarios. This has nothing to do with my statement in the declaration.

Figure 1 of Neufeld does not show management requests over Network N

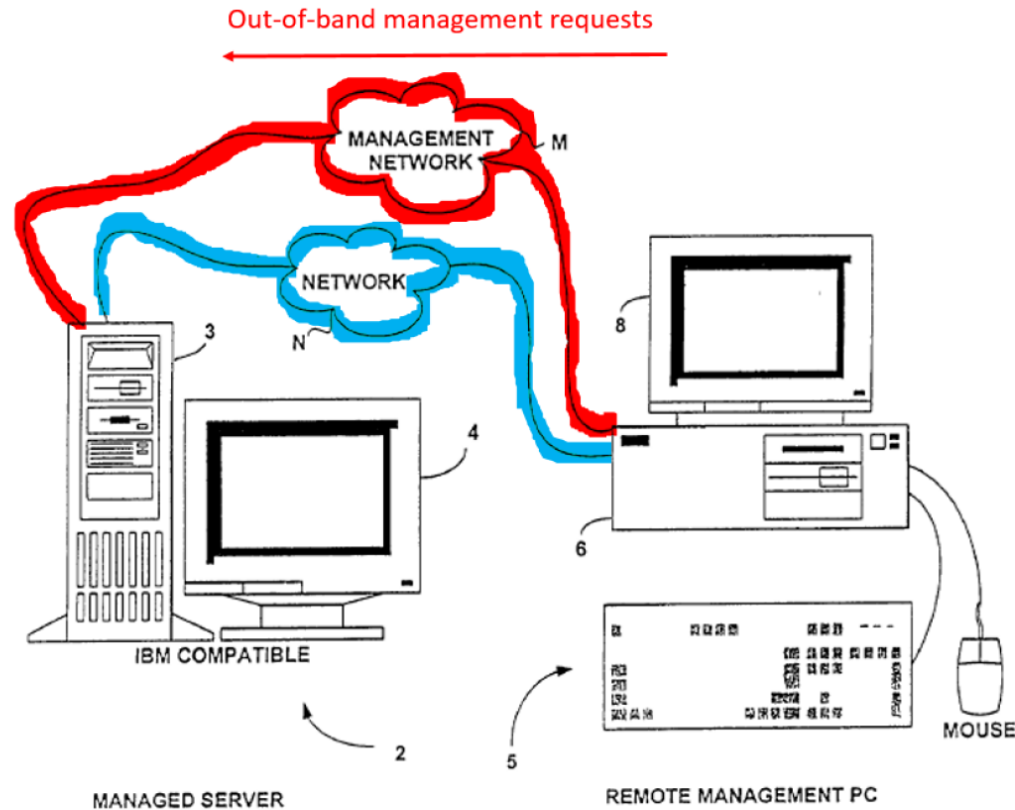


FIG. 1

POR, 25

Eight, the Reply (at 17) wrongly suggests that Patent Owner's expert could not identify "any reason why the remote management PC 5 was connected to the network N." Not so. In response to the question of why remote management PC is connected to the managed server 2 via network N, Patent Owner's expert testified that, in his view, it "would be that for *normal communication, network N can be used in-band* but for remote management, which is the core aspect of it, network M can be used." EX1043, 93:21-94:2 (emphasis added). Petitioner offers nothing to weigh against this expert testimony.

Sur-Reply, 10-11

Neufeld's Figures 2 and 3 show management requests over Network M

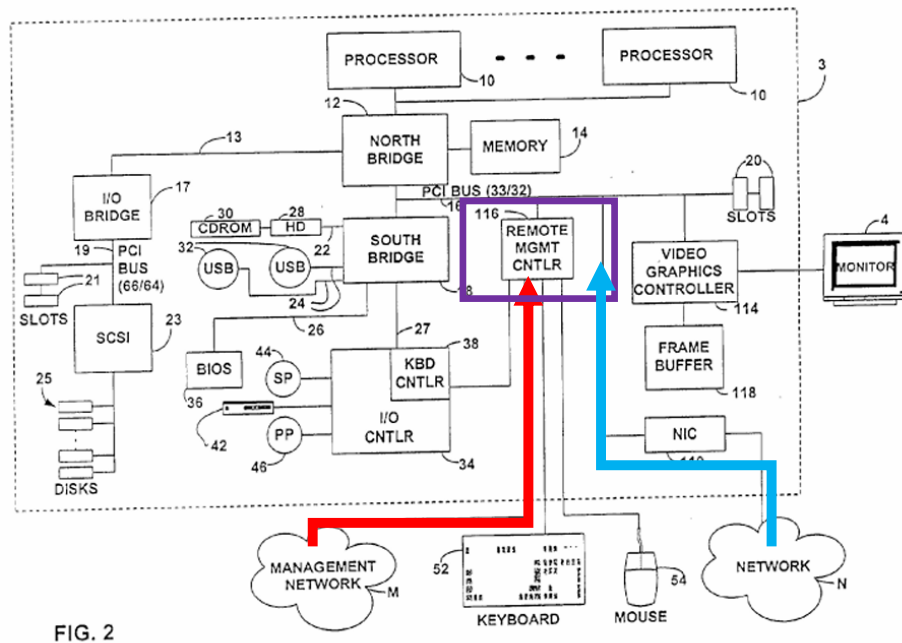


FIG. 2

EX1005, Fig. 2

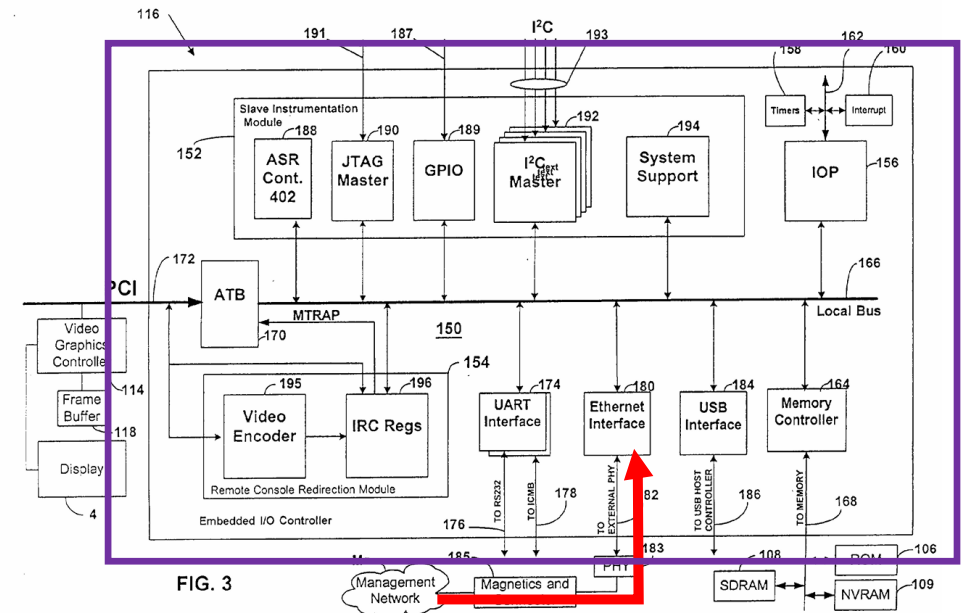


FIG. 3

EX1005, Fig. 3

Petitioner Cannot Identify a
“Second Bus” in Neufeld That Is
Distinct from the “First Bus.

Neufeld's Commands are received via local bus 166

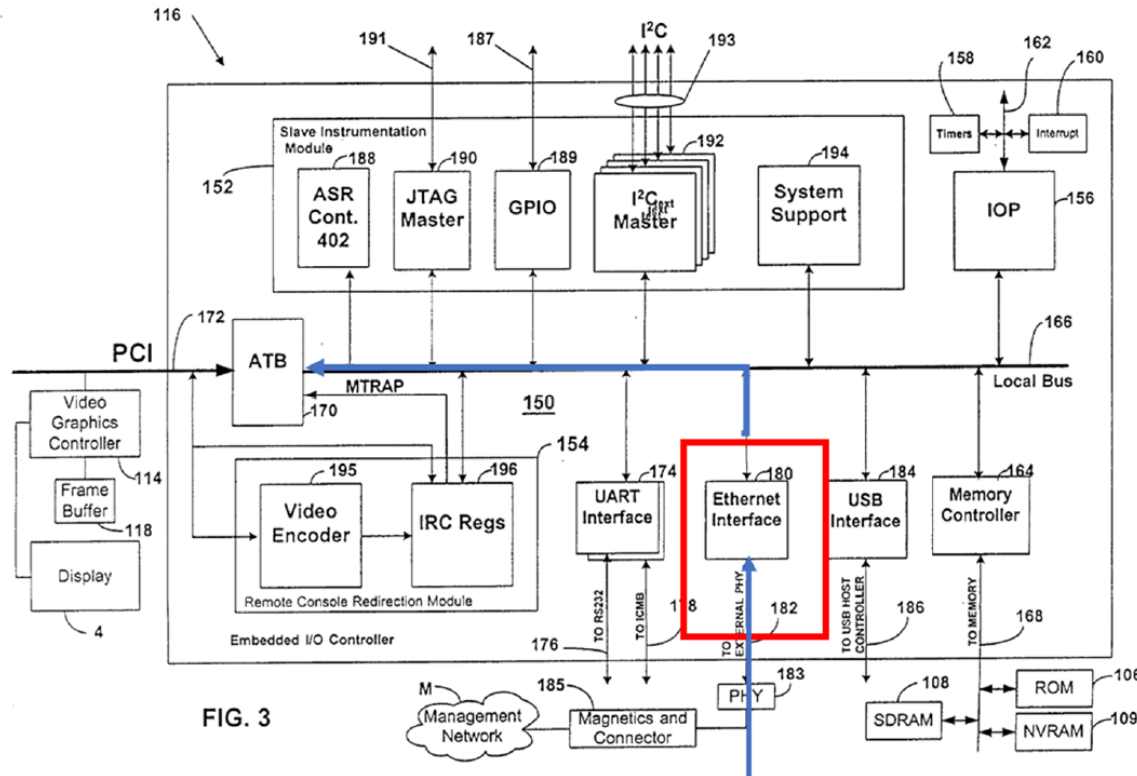


FIG. 3

POR,46

Accordingly, the ATB 170 receives the user commands via an internal bus 166 that allows for communication within the remote server management controller 116. However, the internal bus 166 cannot be the “second bus” recited in the claims because the claims expressly require “a second bus of the network device” that is distinct from the first bus.” In the case of Neufeld, the commands are not received from a second bus of the network device (i.e., managed server 2) and are instead received via a local bus 166 that is internal to RMC 116 and completely inaccessible to the managed server 2. EX2007, ¶116.

POR,46

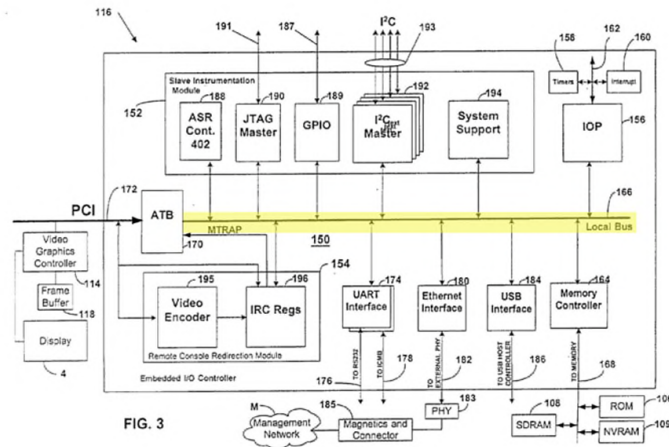
[0061] The embedded I/O controller 150 may also include an Ethernet interface 180, which is operatively coupled to the internal local bus 166. The Ethernet interface 180 provides the main external communication interface between the remote server management controller 116 and the outside world. In the exemplary embodiment shown in FIG. 3, the integrated portion of the Ethernet interface 180 includes a MAC (Media Access Controller), inbound and outbound FIFOs and a DMA engine to transfer packets automatically to and from memory. The Ethernet interface 180 utilizes a connection via interface 182 to an external PHY 183 and typical magnetics and connectors 185 to couple the PHY 183 to the wire that serves as the transmission media. For example, this connection is typically used to couple the remote management controller 116 to the management network M.

EX1005, [0061]

Accordingly, first bus and second bus are the same

[1.d] a first bus; and

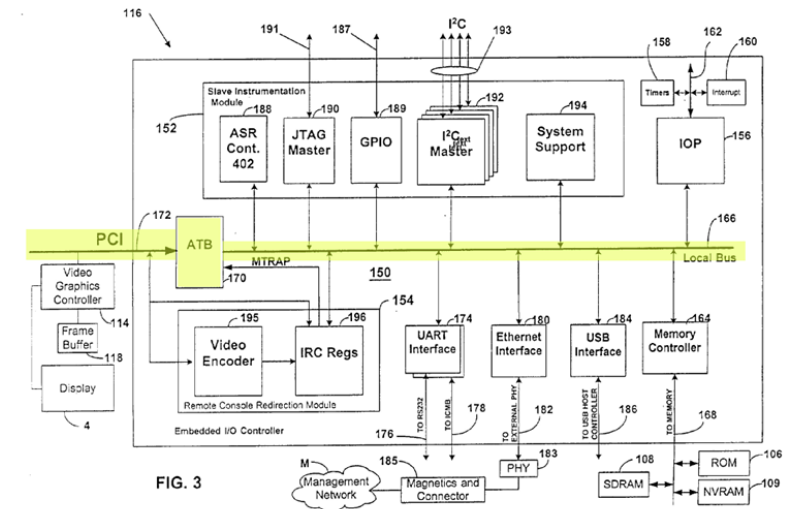
Neufeld discloses this limitation. Neufeld discloses an “internal local bus 166” that is part of the remote management controller 116. EX1005 ¶[0056], Fig. 3; EX1003, ¶93.



Petition, 22

[1.f] wherein the bus controller is also coupled to a second bus of the network device that is distinct from the first bus,

Neufeld discloses or renders obvious this limitation. In addition to being coupled to the local bus 166, ATB 170 is coupled to a second distinct bus, the PCI bus 172 as shown in Figure 3 below. EX1005, ¶[0057], Fig. 3; EX1003, ¶97.



Petition, 24

No Evidence that Commands are received via PCI Bus

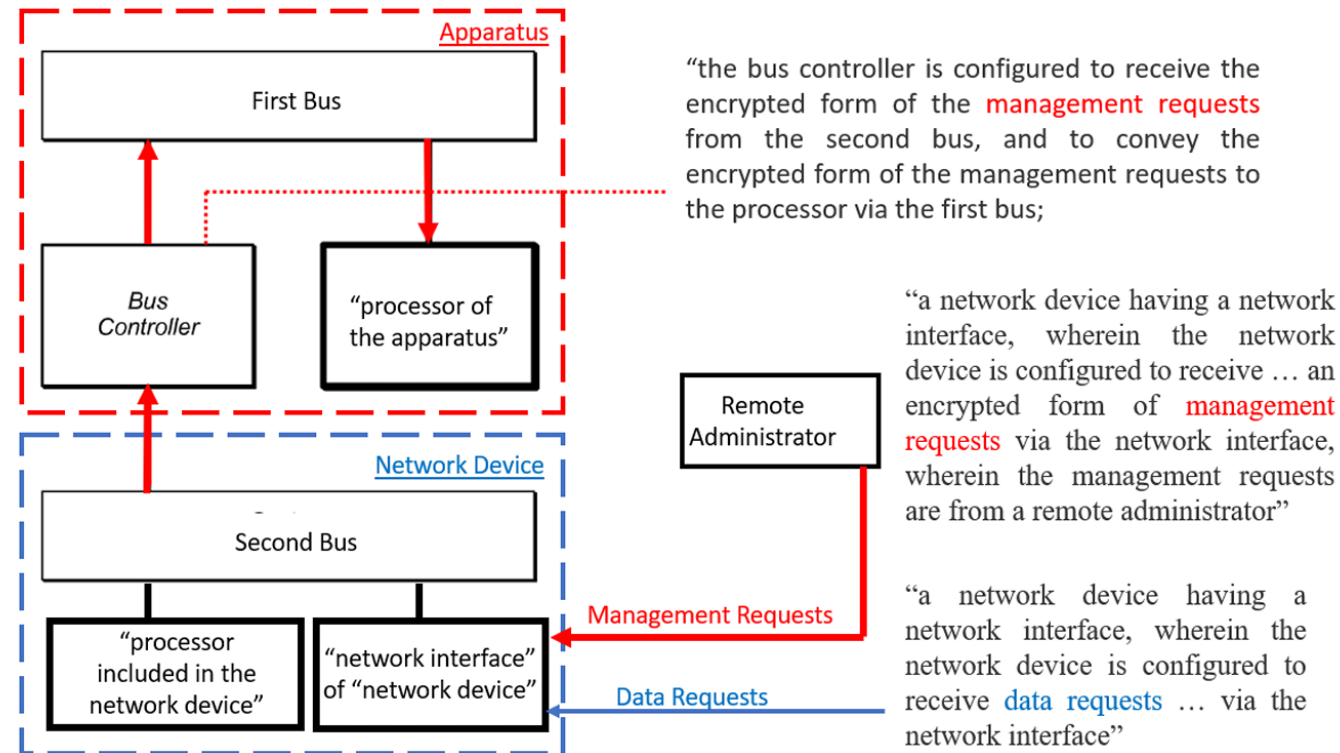
The Petition alleges that the PCI bus 172 is the second bus because “the ATB 170 receives the encrypted management requests from the remote management PC 5 through the NIC 110 via the PCI bus 172.” Petition, 25. Petitioner relies on its proposed edit to the erroneous sentence in paragraph [0047] of Neufeld for this proposition, which, as discussed above, is inconsistent with Neufeld as a whole. Moreover, Petitioner’s assertion that management commands are received by RMC 116 over PCI bus 172 reflects a fundamental misunderstanding of the architecture disclosed in Neufeld. A POSITA would have understood that the only reason Neufeld connects RMC 116 to PCI bus 172 is to allow RMC 116 to perform the passive snooping function described above. EX2007, ¶120; *see*, Section VII(A)(6). Rather than describing the receipt of management commands via the PCI bus 172, Neufeld repeatedly emphasizes the role of RMC 116 in passively “snooping” system activity—such as display configurations and keyboard input. *See*, Section VII(A)(6). Petitioner’s attempt to recast passive observation of activities as reception of commands from a remote administrator should be rejected. As discussed above, the

G. “Snooping” Is Not “receiving an encrypted form of management requests.”

The claims require that a bus controller receive the encrypted form of management requests from the second bus and then convey that same encrypted form to the management processor over a first bus. Neufeld’s “snoop” disclosures describe the RMC’s ability to observe PCI cycles and video-related transactions; that is passive observation/decoding, not being the addressed recipient of an incoming, encrypted management request from a remote administrator. EX1005, ¶[0057] (decode/initiate PCI cycles); ¶[0058] (video procurement). Nothing in those passages teaches that an encrypted management request resides on PCI, much less that the ATB receives that encrypted form from PCI and forwards it still encrypted to the IOP for later decryption. The only specific NIC-110 traffic Neufeld actually narrates is outbound video to the remote console, underscoring that Petitioner’s “snoop = receive” conflation is wrong. EX1005, ¶[0048].

Neufeld Fails to Render the Claims Obvious

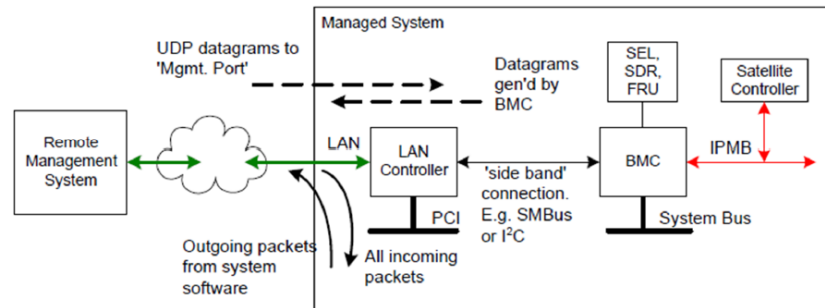
- Neufeld is an out of band system
- Management Commands are Received via ethernet 180 and the transmitted over local bus 166
- Snooping has nothing to do with receiving “encrypted form of management requests”



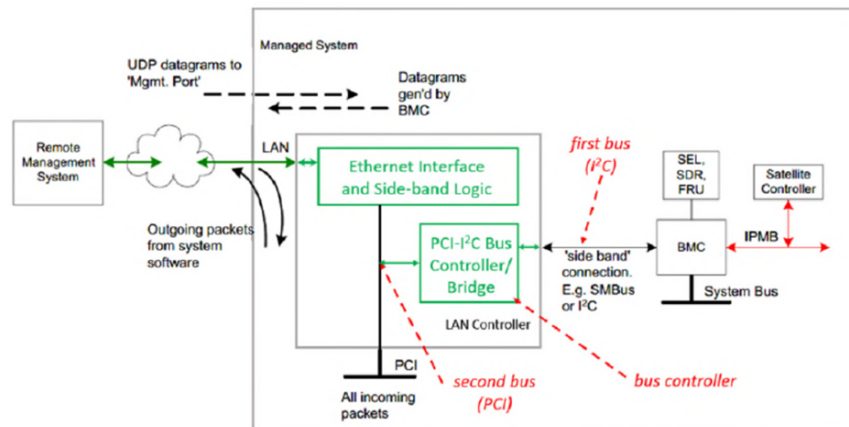
IPMI Does Not Support a PCI-to-I²C Detour

A POSITA would not graft Huckins into IPMI's LAN Controller

Figure 12-1, Embedded LAN Controller Implementation



The Petition (at 64) relies upon the Embedded LAN Controller Implementation and provides a version of Figure 12-1, including elements from Huckins annotated in green.



POR, 59

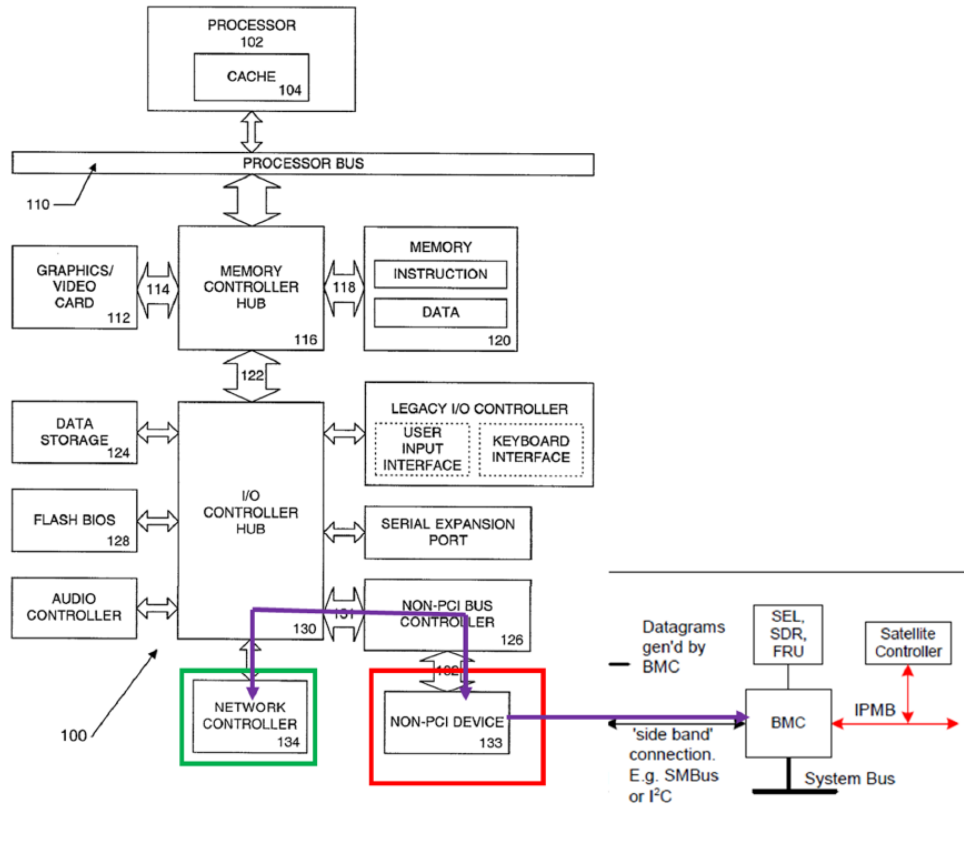
However, the Petition offers no explanation why a POSITA would be motivated to design a LAN controller that utilizes a PCI bus connection to communicate data within the LAN controller. As Dr. Mishra explains:

The PCI bus, or Peripheral Component Interconnect bus, is a parallel data bus standard used in computer systems to connect peripheral devices—such as network interface cards, sound cards, and storage controllers—to the central processing unit (CPU) and main memory. It provides a shared communication pathway where multiple devices can exchange data with the processor and memory using a common set of address, data, and control lines. EX2007, ¶143

Accordingly, in the PCI bus architecture, devices typically do not communicate directly with each other as suggested by the Petitioner. Instead, for components to exchange data with each other, the data needs to be coordinated by a centralized controller. *Id.*

POR, 60

Petitioner's Proposed combination would result in a rubegoldbergian design



POR, 62

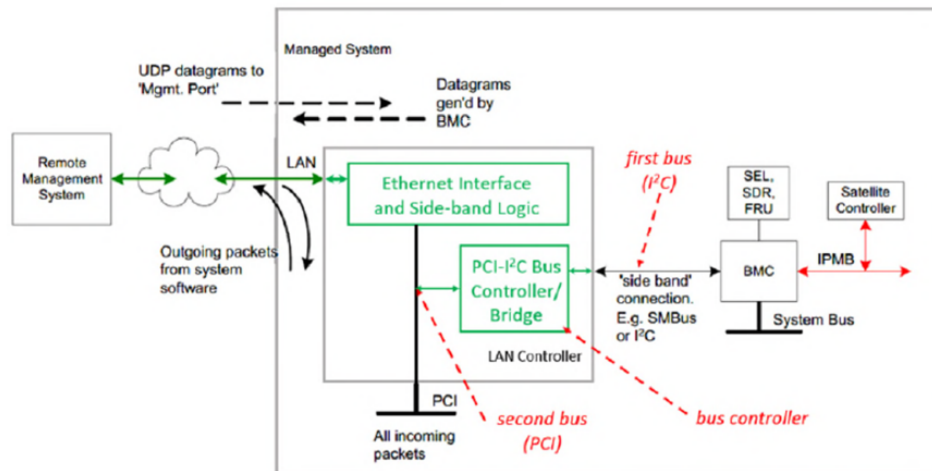
As illustrated above, in the Petition's proposed combination that requires the PCI architecture, the data would have to be received by the network controller, routed to the Non-PCI Device (I2C controller) over the PCI bus by the I/O Control Hub, and then onward to the BMC. This external coordination increases the LAN controller's complexity, decreases the LAN controller's throughput, decreases the PCI bus's bandwidth and increases power consumption. All of these are completely superfluous when communicating data within the same LAN controller. EX2007, ¶146.

POR, 63

The Encryption Location (Limitation [1.h]) Remains Unproven as Claimed

I2C is not inherently encrypted

Similarly, with regard to limitation 1.e of Ground 9, the Petition does not explain why communication along the “side-band” connection of IPMI is encrypted. In fact, the Petition’s discussion of limitation 1.e is completely silent with regard to the word “encrypt” or “encryption.” See, Petition, 62-65. At most, as illustrated below, the Petition alleges that the first bus is the I²C bus. EX2007, ¶158.



POR, 67

As Dr. Mishra explains:

I²C and SMBus are low-level, lightweight serial communication interfaces designed primarily for short-range, intra-board communication between chips—such as sensors, memory modules, and microcontrollers—on the same motherboard or hardware platform. Because of their simplicity and minimal overhead, these protocols do not include any built-in features for encryption, authentication, or integrity checking. They were developed under the assumption that the bus environment is physically secure and isolated from external threats. EX2007, ¶160.

POR, 68

As a result, Petitioner fails to establish that the combination of IPMI, Frantz, and Huckins renders limitation: “to convey the encrypted form of the management requests to the processor via the first bus” (1.h) obvious. Petitioner’s arguments focus on encrypting management requests transmitted over in-band network interfaces and do not address the internal communication path identified as the “first bus.” The Petition provides no explanation or evidence to support why encryption would be applied to the internal “side-band” connection within the embedded LAN controller, which is inherently out-of-band. Because the cited references do not teach or suggest encrypting management requests transmitted over the first bus, the Petition does not demonstrate that this limitation is rendered obvious. EX2007, ¶162.

POR, 69-70

IPMI et al Fails to Render the Claims Obvious

- A POSITA would not be motivated to combine IPMI and Huckins
- No evidence that data over the I2C bus is encrypted

