

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)

Inter Partes Review

Nos. IPR2024-00109, IPR2024-00124

U.S. Patents Nos. 8,474,016 and 7,325,140

Petitioners' Presentation

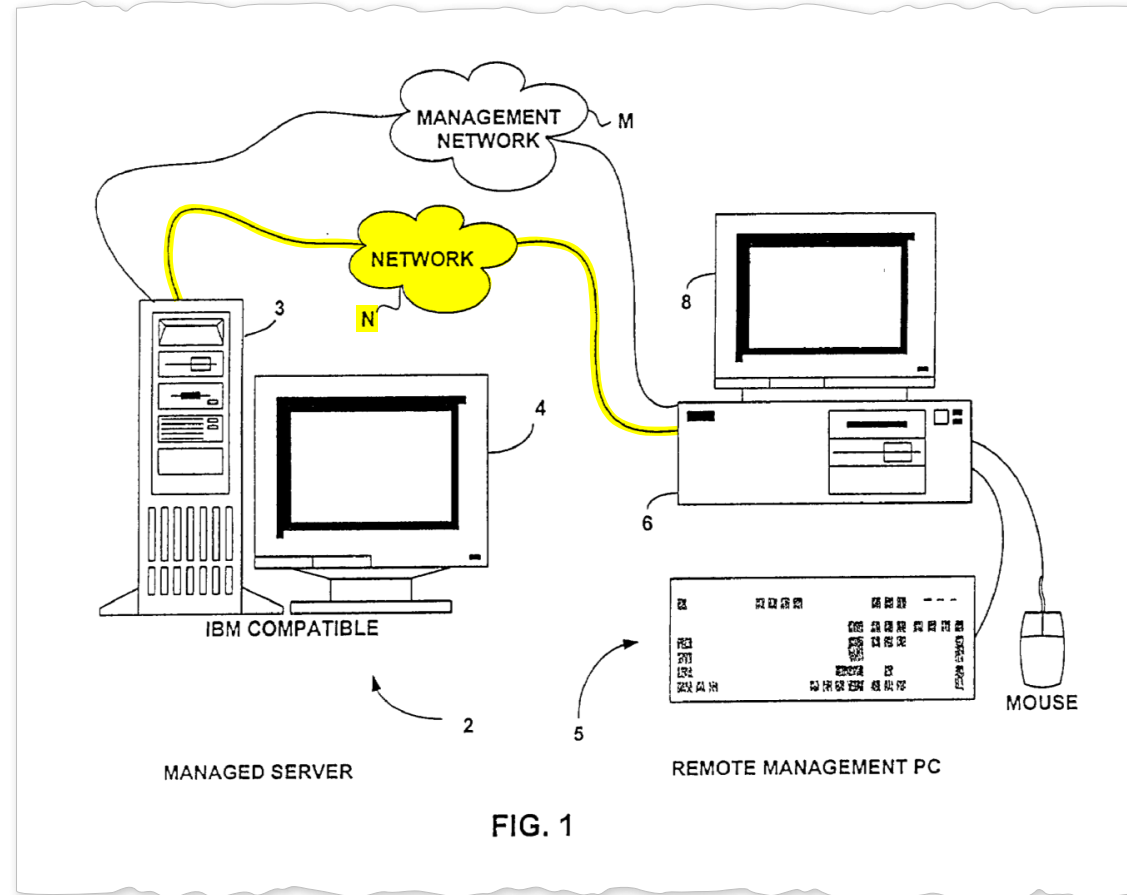
IPR2024-00109 and IPR2024-00124: Neufeld Discloses or Renders Obvious In-Band Remote Management Messages

PO's Arguments to the Contrary All Fail

- Including in-band and out-of-band communications as taught by Neufeld provides all of the benefits of out-of-band communications and additional benefits
 - PO cannot disprove this simple truth
-
- In-band and out-of-band remote management communications are not mutually exclusive alternatives

Neufeld Discloses or Renders Obvious In-Band Remote Management Messages

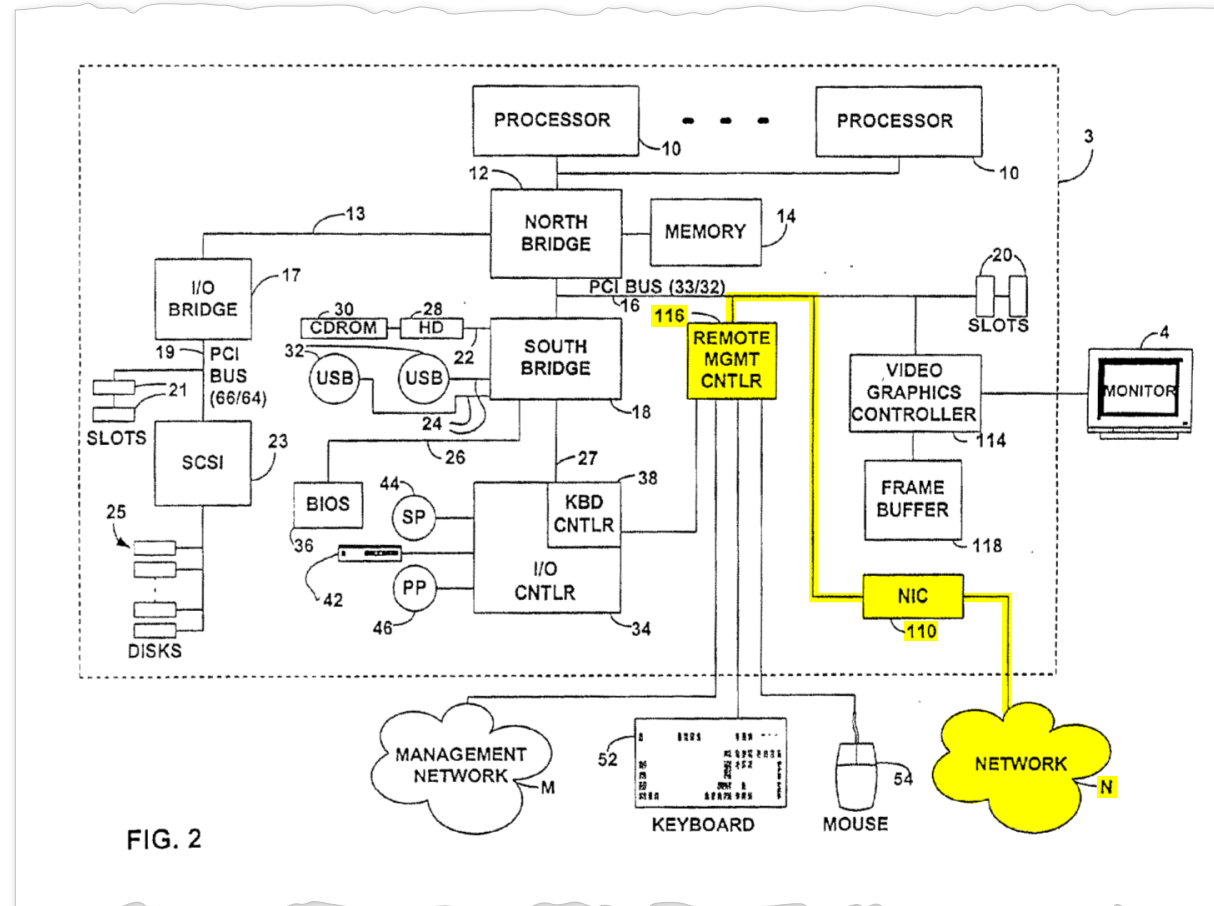
Neufeld



EX1005 at Fig. 1; 109 Petition at 9, 16

Neufeld Discloses or Renders Obvious In-Band Remote Management Messages

Neufeld



EX1005 at Fig. 2; 109 Petition at 10, 17

Neufeld Discloses or Renders Obvious In-Band Remote Management Messages

Neufeld

[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 at ¶43; EX1046 at ¶100; 109 Reply at 6; 109 Petition at 19-20; 124 Petition at 27, 29

Neufeld Discloses or Renders Obvious In-Band Remote Management Messages

Neufeld

[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 at ¶47; 109 Reply at 6

Neufeld Discloses or Renders Obvious In-Band Remote Management Messages

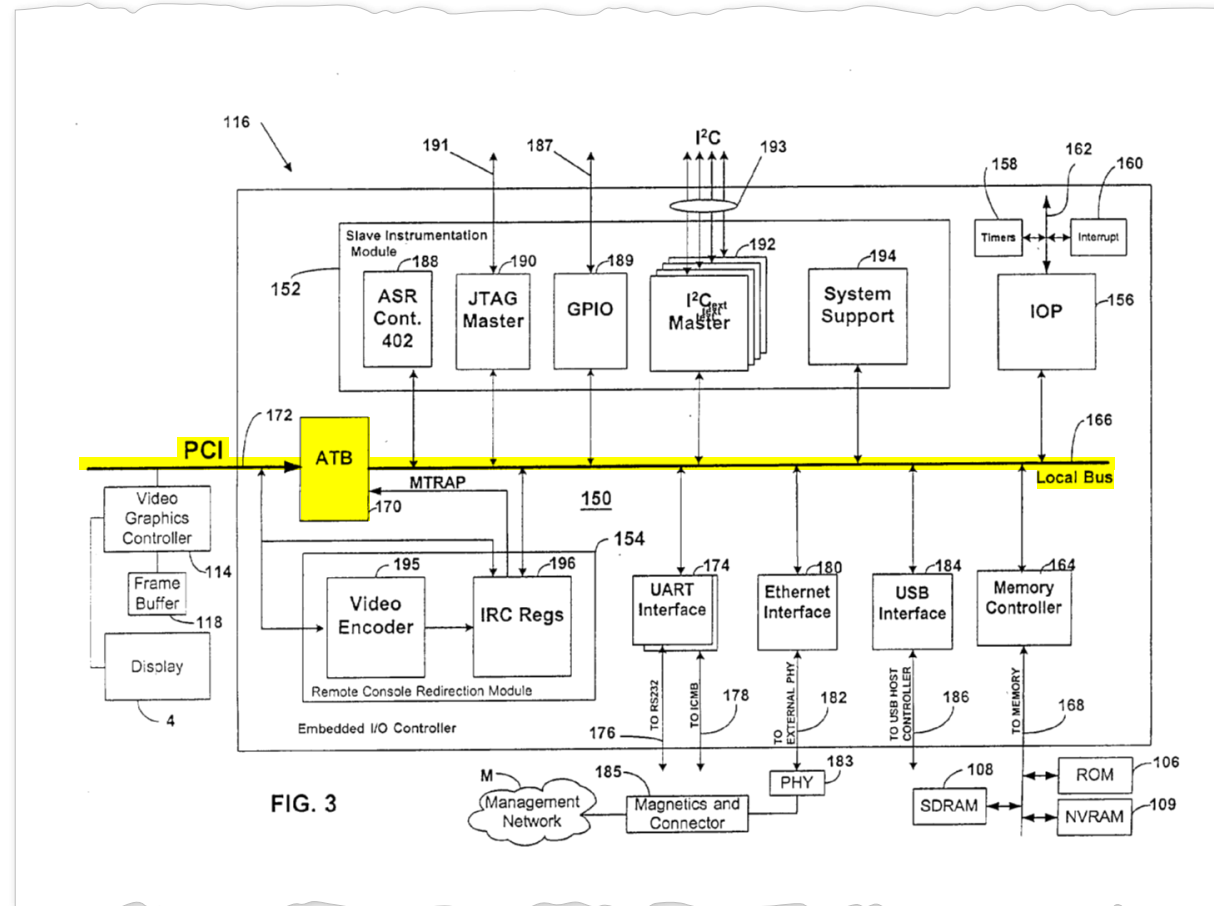
Neufeld

[0048] In the operation of the remote management controller 116, the I/O processor 156 (FIG. 3) may periodically read the video graphics data from the frame buffer 118 to determine whether the data has changed. If the data has changed, the I/O processor 156 will compress the video graphics data and transmit the data to the remote console 5 via one of the communications devices (i.e., modem or NIC 110). The remote console 5 will decompress and decode the data stream and display it at the remote console 5 for viewing by a user.

EX1005 at ¶48; 109 Reply at 6-7

Neufeld Discloses or Renders Obvious In-Band Remote Management Messages

Neufeld



EX1005 at Fig. 3; 109 Petition at 11

Neufeld Discloses or Renders Obvious In-Band Remote Management Messages

Neufeld

[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 at ¶15; 109 Reply at 3; 109 Petition at 20;
124 Petition at 27; EX1046 at ¶85

Neufeld Discloses or Renders Obvious In-Band Remote Management Messages

Meldal Declaration

86. Neufeld further discloses the desirability of providing in-band as well as out-of-band communications for monitoring and control of the managed server

2. EX1005, ¶[0015] (explaining that an “important goal” is to increase the number of server problems that can be analyzed and repaired remotely, and that it is “highly desirable” to provide in-band communications to capture the maximum amount of information from, and allow control of, the managed server).

EX1003 at ¶86; 109 Petition at 19-20

PO's Arguments to the Contrary All Fail

Noubir Declaration

47. At first glance, paragraph [0043] of Neufeld 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 . . . to provide functionality for accessing, interacting, and monitoring the managed server 2 from the remote console.” However, upon closer analysis, a POSITA would understand, particularly in light of FIGs. 2 and 3, that the remote management controller 116 is physically connected to internal system components, such as the PCI bus and keyboard controller, enabling it to snoop on system activity—such as capturing display output and keyboard inputs—without relying on or interfering with the server’s host operating system. This architecture underscores that the mention of network N or the management network M in paragraph [0043] does not imply that the remote management controller transmits management data through the NIC 110 or the server’s primary network path. To the contrary, Neufeld expressly states that the

remote management controller communicates externally through a dedicated interface, such as Ethernet interface 180, and that the entire system is purposefully designed to operate independently of any software on the managed server. Thus, a 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.

EX2006 at ¶47; 124 Reply at 11

PO's Arguments to the Contrary All Fail

Dr. Noubir Doubled Down During Deposition on His Incorrect Belief That Neufeld's RMC Could Not Communicate With the Remote Management PC

Meldal Deposition

Q. So there's no disclosure in Neufeld of RMC 116 transmitting data over network N in your opinion. Do I have that right?

A. **There is no place where it makes sense.** That's what I would say. Because I did the analysis. There might be some text where -- so Neufeld has various kind of thing that do not make sense to me. So if there's a reference, I'm happy -- just show me and I can look at it and explain why I am, you know, not considering that in my final, you know, declaration, in what I wrote in my declaration.

Q. Well, you're saying there's no disclosure that makes sense to you. Is there some disclosure of the RMC 116 transmitting data over the network N?

A. **I don't think so.**

EX1049 at 60:6-20; 124 Reply at 8

PO's Arguments to the Contrary All Fail

Neufeld

[0048] In the operation of the remote management controller 116, the I/O processor 156 (FIG. 3) may periodically read the video graphics data from the frame buffer 118 to determine whether the data has changed. If the data has changed, the I/O processor 156 will compress the video graphics data and transmit the data to the remote console 5 via one of the communications devices (i.e., modem or NIC 110). The remote console 5 will decompress and decode the data stream and display it at the remote console 5 for viewing by a user.

EX1005 at ¶48; 109 Reply at 6-7

PO's Arguments to the Contrary All Fail

Dr. Noubir Admitted at Deposition That Providing Ability to Have RMC Communicate Over Network N Would Be Desirable

Meldal Declaration

- Q. Let me ask you one last question. Two last questions. If you were an operator of a remote management console that was located far from where the server 2 was located, and your connection for the management network M, as in Mary, were somehow inoperative on your remote management PC5, would you want the ability for your remote management PC5 to be able to send management commands to the managed server via the network N in that situation?
- A. So the -- you know, your -- you're implying something obvious that of course people would want anything. Of course. But the -- but I think in engineering these systems my understanding is that there are trade-offs of what is feasible and what's -- how much additional, you know, components and software and hardware needs to be added for something to make sense.

PO's Arguments to the Contrary All Fail

The RMC and Remote Management PC Also Communicate When the OS is Online

Noubir Declaration

45. Neufeld also distinguishes between in-band and out-of-band communications. For example, Neufeld states in ¶ [0011]: “Remote management tools can communicate with a managed server using either (1) in-band communication or (2) out-of-band communication. In-band communication refers to communicating with the server over a standard network connection, such as the managed server’s normal Ethernet connection. In-band communication with the server is, accordingly, only possible when the server is able to communicate over its normal network connection. Practically speaking, **this limitation restricts in-band communication to times when the OS of the managed server is operational** (online).” Ex. 1005, ¶ [0011] (emphasis added). Neufeld, therefore, clearly states that in-band communication is limited to use when the OS of the managed server is running. It does not, however, discuss how in-band communication could work in Neufeld’s system as **Neufeld’s invention is limited to discussions of system operation when the OS is not running (offline).**

EX2006 at ¶45; 124 Reply at 8

PO's Arguments to the Contrary All Fail

The RMC and Remote Management PC Also Communicate When the OS is Online

Noubir Declaration

59. Further, the remote management approach described in Neufeld is not compatible with in-band communication (as defined in Neufeld). More specifically, Neufeld is focused on solutions for remote server management when the managed server is powered down (e.g., for a reboot), before the OS is up and running (e.g., for initial setup), or while the OS is offline. Ex. 1005, ¶ [0034]. However, Neufeld also acknowledges that in-band communication is not an option without the OS. Ex. 1005, ¶ [0011] (“Practically speaking, this limitation restricts in-band communication to times when the OS of the managed server is operational.”). Since the proposed solution in Neufeld operates before the OS is loaded, it cannot be using in-band communication, which is only usable when the OS of the managed server is operable.

EX2006 at ¶59; 124 Reply at 10

PO's Arguments to the Contrary All Fail

The RMC and Remote Management PC Also Communicate When the OS is Online

Neufeld

[0073] The VCD functionality may be used to present a virtual modem to the managed server, allowing it to be either exclusively owned or shared both by the OS and a remote console application. This technique is fully described in U.S. Pat. No. 5,790,895, which is incorporated by reference above.

[0074] In one exemplary embodiment of the remote server management controller of the present invention, the VCD presents a virtual 16550 UART to the internal architecture of managed server 2. The VCD logic enables the remote server management controller 116 to communicate with specific OS features, such as the Emergency Management Services (“EMS”) facility that is implemented in Windows XP.

EX1005 at ¶¶73-74; 124 Reply at 10

PO's Arguments to the Contrary All Fail

The RMC and Remote Management PC Also Communicate When the OS is Online

Neufeld

[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.

Noubir Declaration

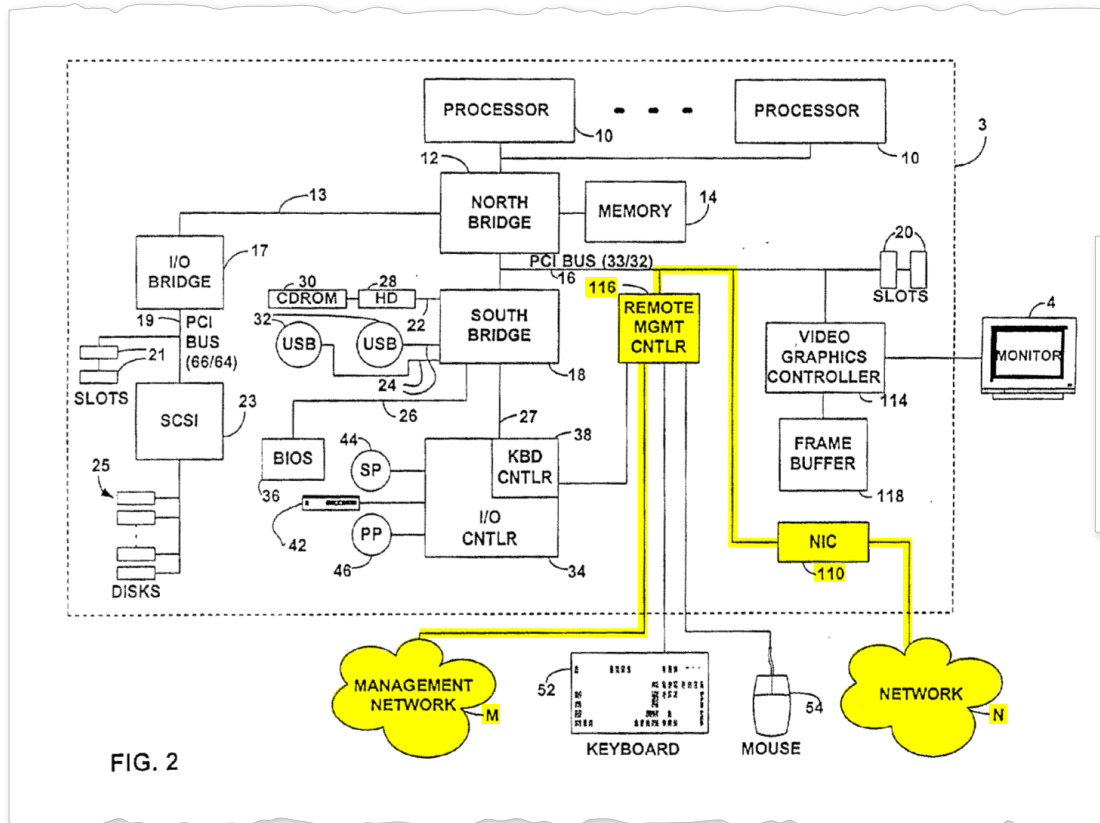
times when the OS of the managed server is operational.”). Since the proposed solution in Neufeld operates before the OS is loaded, it cannot be using in-band communication, which is only usable when the OS of the managed server is operable.

1005 at ¶43;
EX2006 at ¶59; 124 Reply at 10

PO's Arguments to the Contrary All Fail

There is a Clear Error in Paragraph 47

Neufeld

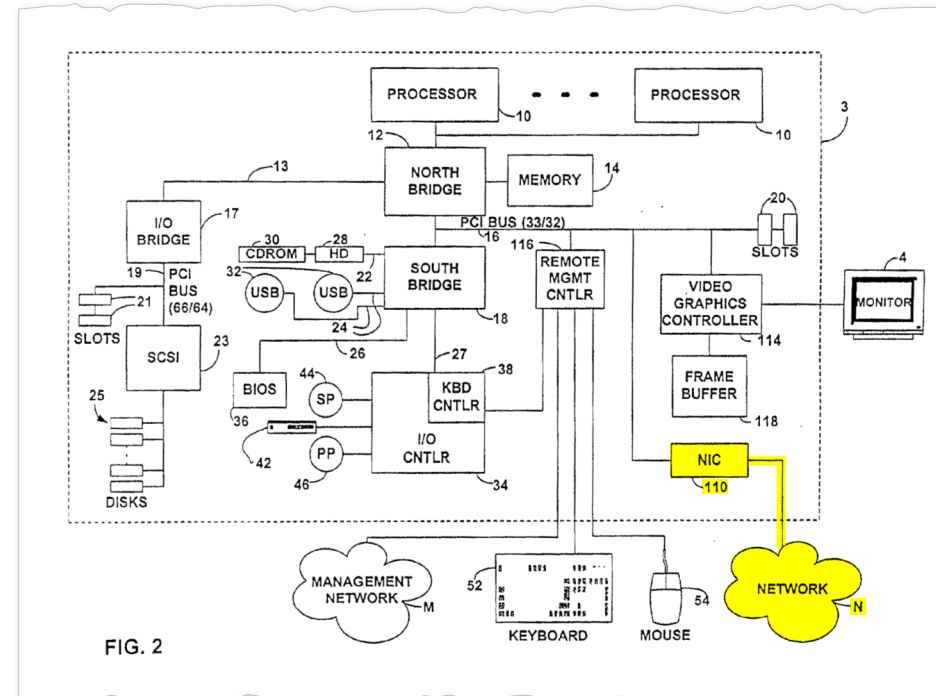


ics controller **114**, (e.g., location of SVGA register file). The remote management controller **116** also includes circuitry to route keystrokes to the keyboard controller **38** from either the local keyboard **52** or from the remote console **5** via the modem or **NIC 110** which may be coupled to the network **M**.

EX1005 at ¶47, Fig. 2; 109 Reply at 9-10

PO's Arguments to the Contrary All Fail

- Fig. 2 shows NIC 110 connected to Network N, not M



EX1003 at Fig. 2; 124 Reply at 7

- ¶[0048] discloses that the RMC transmits video data to the Remote Management PC 5 via the NIC 110 109 Reply at 10

PO's Arguments to the Contrary All Fail

- ¶[0047] discusses Fig. 2, but Ethernet interface 180 is not in Fig. 2
- ¶[0048] expressly refers to Fig. 3 when discussing components of Fig. 3 while ¶[0047] does not refer to Fig. 3

109 Reply at 11

Neufeld

[0048] In the operation of the remote management controller 116, the I/O processor 156 (FIG. 3) may periodically read the video graphics data from the frame buffer 118 to determine whether the data has changed. If the data has changed, the I/O processor 156 will compress the video graphics data and transmit the data to the remote console 5 via one of the communications devices (i.e., modem or NIC 110). The remote console 5 will decompress and decode the data stream and display it at the remote console 5 for viewing by a user.

EX1005 at ¶48

PO's Arguments to the Contrary All Fail

- Neufeld does not “disparage” in-band communications

Neufeld

[0011] Remote management tools can communicate with a managed server using either (1) in-band communication or (2) out-of-band communication. In-band communication refers to communicating with the server over a standard network connection, such as the managed server's normal Ethernet connection. In-band communication with the server is, accordingly, only possible when the server is able to communicate over its normal network connection. Practically speaking, this limitation restricts in-band communication to times when the OS of the managed server is operational (online).

[0012] Out-of-band communication, which is not performed across the managed server's normal connection to the network, is a much more powerful tool for server management. In out-of-band communication, a “back door” communication channel is established by a remote server management tool (such as a remote console or terminal emulator) using some other interface with the server (such as (1) through the server's modem, (2) via a direct connection to a serial port, (3) through an infrared communication port, or (4) through an Ethernet interface or the Internet).

EX1005 at ¶¶11-12; 109 Reply at 7-8

PO's Arguments to the Contrary All Fail

- Neufeld does not “disparage” in-band communications
 - Neufeld does not state that in-band remote management messages should be avoided
 - Neufeld does not state that in-band remote management messages are not useful
 - Neufeld does disclose in-band remote management messages in ¶¶[0043], [0047] and [0048]
 - Neufeld renders obvious a system with both in-band and out-of-band remote management communications

109 Reply at 8-9

PO's Arguments to the Contrary All Fail

- Dr. Mishra was not able to identify any disclosure in Neufeld of the Remote Management PC doing anything other than remote management communications with RMC 116

Mishra Deposition

Q. Does Neufeld disclose that remote management PC 5 performs any function other than remote management of the server 2?

A. Let me check.

Q. Okay.

A. Based on my quick review, it performs remote management of PC 2.

Q. And your quick review doesn't disclose any other function for remote management PC 5, correct?

A. Yes.

EX1043 at 81:15-94:21; 109 Reply at 17; 109 Sur-Reply at 11

Q. Okay. And the second question was what functions does Neufeld disclose is being performed by the remote management PC 5? Do you have an answer to that question?

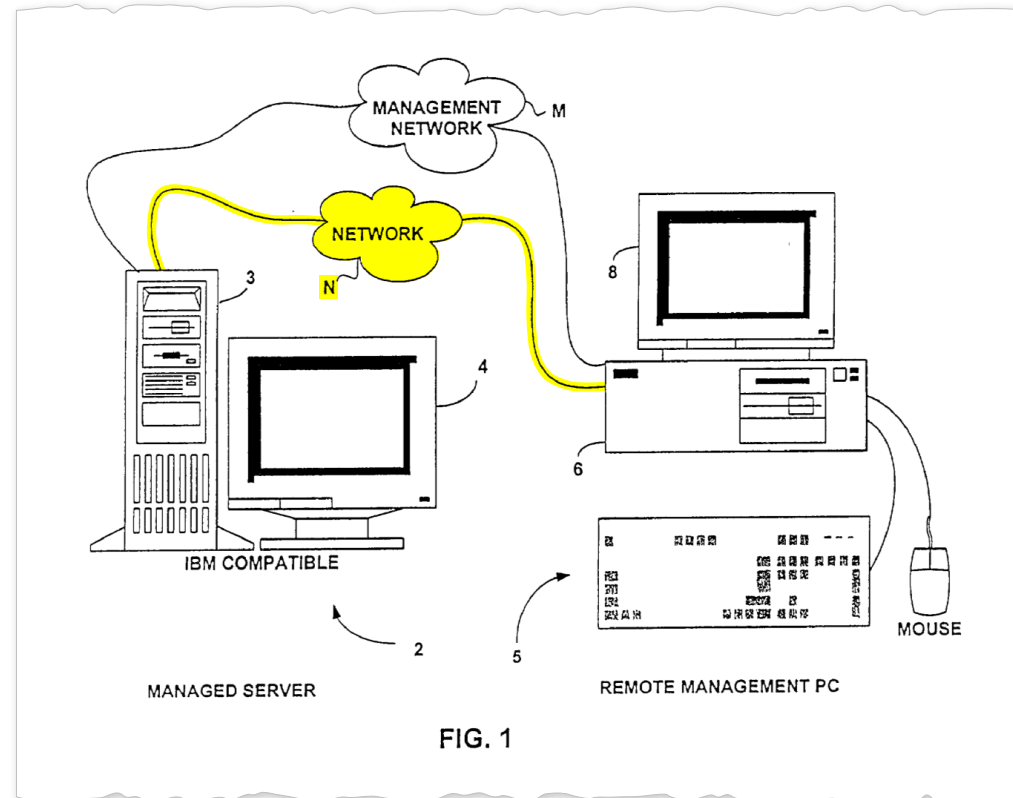
A. Let me repeat the question. Does Neufeld disclose any functions for remote management PC 5 other than performing management for the managed server 2 including RMC 16?

So this particular answer is no with the footnote that the majority of the Neufeld is about securing through remote management systems. In majority of it, it talks about different kind of scenarios where it may fail so that it can handle it. And specifically it's gone into details talking about authentication by different parties with different privilege level with different time of the day, et cetera, which I still believe is part of the remote management, what it's supposed to do. That's the whole thing about.

PO's Arguments to the Contrary All Fail

- There would be no reason for connecting the Remote Management PC to the managed server via Network N without in-band communication of management messages

Neufeld



EX1005 at Fig. 1; 109 Reply at 5

PO's Arguments to the Contrary All Fail

- PO's position is based on a false choice between in-band and out-of-band systems

Mishra Declaration

91. Petitioner provides no rationale why the subject sentence should be corrected in the manner suggested in the Petition. Given Neufeld's singular focus as an out-of-band remote management solution, a POSITA would have understood that remote management commands destined for the RMC 116 in Neufeld would have necessarily remained on Neufeld's Management Network M. Moving Neufeld's remote management commands to Network N as suggested by Petitioner would transform Neufeld from an out-of-band solution to an in-band solution, which makes no sense in the context of the reference as a whole which began by disparaging in-band systems in which communication with the server is "only possible when the server is able to communicate over its normal network connection" in favor of out-of-band communication which Neufeld characterized as "a much more powerful tool for server management." EX1005, [0011]-[0014] (emphasis added); *see also*, [0059]

EX2007 at ¶91; 109 POR at 23, 31

- All of PO's "inconsistencies" are the result of this false choice

PO's Arguments to the Contrary All Fail

- Contrary to PO's "transform" argument, the Petition and Dr. Meldal clearly alleges that Neufeld's system uses **both** in-band and out-of-band communications for management messages

Meldal Declaration

86. Neufeld further discloses the desirability of providing in-band as well

as out-of-band communications for monitoring and control of the managed server

2. EX1005, ¶[0015] (explaining that an "important goal" is to increase the number of server problems that can be analyzed and repaired remotely, and that it is "highly desirable" to provide in-band communications to capture the maximum amount of information from, and allow control of, the managed server).

EX1003 at ¶86; 109 Petition at 19-20; 109 Reply at 12; see also 124 Petition at 14; 124 Reply at 12

PO's Arguments to the Contrary All Fail

- Including in-band and out-of-band communications as taught by Neufeld provides all of the benefits of out-of-band communications and additional benefits
 - PO cannot disprove this simple truth
-
- In-band and out-of-band remote management communications are not mutually exclusive alternatives

IPR2024-00124: Neufeld Renders Obvious the Use of a Point-Point VPN

Neufeld Renders Obvious the Use of a Point-Point VPN

Meldal Declaration

110. Neufeld further discloses that in order for a network administrator to access the server (which a POSITA would have understood involves communications with Neufeld's remote server management controller 116 given that it is a network administrator that is accessing the server) from a remote terminal located outside of work, the administrator must typically use a virtual private network. EX1005, ¶[0022]; *see also* ¶[0088, Table 4, User Id 7]. A POSITA would have understood such access involves communications with Neufeld's remote server management controller 116 given that it is a network administrator that is accessing the server. EX1046, ¶110.

EX1046 at ¶110; 124 Petition at 32; 124 Reply at 14

Neufeld Renders Obvious the Use of a Point-Point VPN

Neufeld

terminal. Finally, this situation is potentially even more problematic if the system administrator attempts to access the server from a remote terminal located outside of work, such as at home or while traveling. In this situation, the system administrator must typically use the Internet or a virtual private network to access the system. However, because such an access is attempted from a location not directly affiliated with the business, there can be no assurances of the actual identity of the user absent rigorous authentication. Even with rigorous user authentication, greater restrictions may be placed on the same user when accessing the system remotely as opposed to accessing the system at work or directly from a secure facility. Furthermore, in the case of remote operation, even if the identity of the user can be determined with absolute certainty, some operations may be inherently more problematic because the user is not physically close to the work group using the server and may not know about a problem the user causes while remotely accessing the server.

EX1005 at ¶¶22; EX1046 at ¶¶110; 124 Petition at 32

Neufeld Renders Obvious the Use of a Point-Point VPN

Meldal Declaration

111. A POSITA would also have found obvious the requirement in limitation [1.c] for providing logical separation of management data from user data because a POSITA would have found it obvious to utilize a point-to-point VPN with tunneling functionality on Neufeld's managed server 2 via the in-band connection used for non-management user traffic (i.e., the NIC 110 and network N) in order to provide for a dedicated VPN for communications of management data with the remote management PC 5. A POSITA would have had knowledge of point-to-point VPNs using tunneling at the time of invention, would have understood that tunneling employs encryption to secure the VPN communications, and would have found it obvious to configure Neufeld's managed server to employ a point-to-point VPN with tunneling for communication of management data because VPN tunneling was a well-known, and indeed was the most common method, for implementing a point-to-point VPN.

EX1046 at ¶¶111; 124 Petition at 33;
124 Reply at 14

Neufeld Renders Obvious the Use of a Point-Point VPN

Meldal Declaration

112. Such VPN technology is the same as, or is at least equivalent, to the corresponding VPN structure for this limitation disclosed by the 140 patent. POSITA would have had knowledge of point-to-point VPN tunneling at the time of invention, and would have found it obvious to configure Neufeld's managed server to employ such tunneling to implement Neufeld's VPN for communication of management data because VPN tunneling was a well-known, and indeed was the most common method, for implementing a point-to-point VPN. Moreover, L2TP/IPsec (Layer Two Tunneling Protocol (L2TP) with Internet Protocol Security (IPSEC) is a tunneling protocol used to support VPNs or as part of the delivery of services by ISPs. It uses encryption ('hiding') only for its own control messages (using an optional pre-shared secret). L2TP does not provide any encryption or confidentiality of content by itself. Rather, it provides a tunnel for Layer 2 (which may be encrypted), and the tunnel itself may be passed over the Layer 3 encryption protocol IPsec.

EX1046 at ¶¶112; 124 Petition at 33;
124 Reply at 14

Neufeld Renders Obvious the Use of a Point-Point VPN

Internetworking Technologies Handbook

Layer 2 Tunneling Protocol

* * *

L2TP simulates a point-to-point connection by encapsulating PPP datagrams for transportation through routed networks or internetworks. Upon arrival at their intended destination, the encapsulation is removed, and the PPP datagrams are restored to their original format. Thus, a point-to-point communications session can be supported through disparate networks. This technique is known as *tunneling*.

Adding More Security

As useful as L2TP is, it is important to recognize that it is not a panacea. It enables flexibility in delivering remote access, but it does not afford a high degree of security for data in transit. This is due in large part to the relatively nonsecure nature of PPP. In fairness, PPP was designed explicitly for point-to-point communications, so securing the connection should not have been a high priority.

An additional cause for concern stems from the fact that L2TP's tunnels are not cryptographic. Their data payloads are transmitted in the clear, wrapped only by L2TP and PPP framing. However, additional security may be afforded by implementing the IPSec protocols in conjunction with L2TP. The IPSec protocols support strong authentication technologies as well as encryption.

EX1050 at 3-5; 124 Reply at 14

Neufeld Renders Obvious the Use of a Point-Point VPN

Meldal Declaration

113. A point-to-point VPN with tunneling used for the communication of management data between the remote server management controller 116 and the remote management PC 5 via the network N also performs the identical function performed by the VPN technology of the 140 patent, namely providing logical separation of user data and management data.

EX1046 at ¶113; 124 Petition at 34; 124 Reply at 14

Neufeld Renders Obvious the Use of a Point-Point VPN

Meldal Declaration

115. The VPN tunneling functionality dedicated to communications of management data from remote management PC 5 also performs the function of connecting a remote user on remote management PC 5 with Neufeld's remote server management controller 116 for communication of management data using the same user interface (Neufeld's NIC 110 connected to network N) over which non-management user data is communicated to the managed server 2.

B. Claim 2: The system of claim 1 wherein the at least one secure management access controller includes a flash chip, non-volatile random access memory and random access memory.

EX1046 at 115; 124 Petition at 34; 124 Reply at 14

Neufeld Renders Obvious the Use of a Point-Point VPN

- Dr. Noubir admitted that L2TP was a well-known VPN technology at the time of the '140 patent

Noubir Deposition

Q. Okay. Was L2TP a well-known VPN technology at the time of the '140 patent?

A. Yes, it was.

EX1049 at 48:7-9; 124 Reply at 14

Neufeld Renders Obvious the Use of a Point-Point VPN

- L2TP and IPSEC are discussed in the book relied on by Dr. Noubir

IPSec VPN Design

VPN Technologies

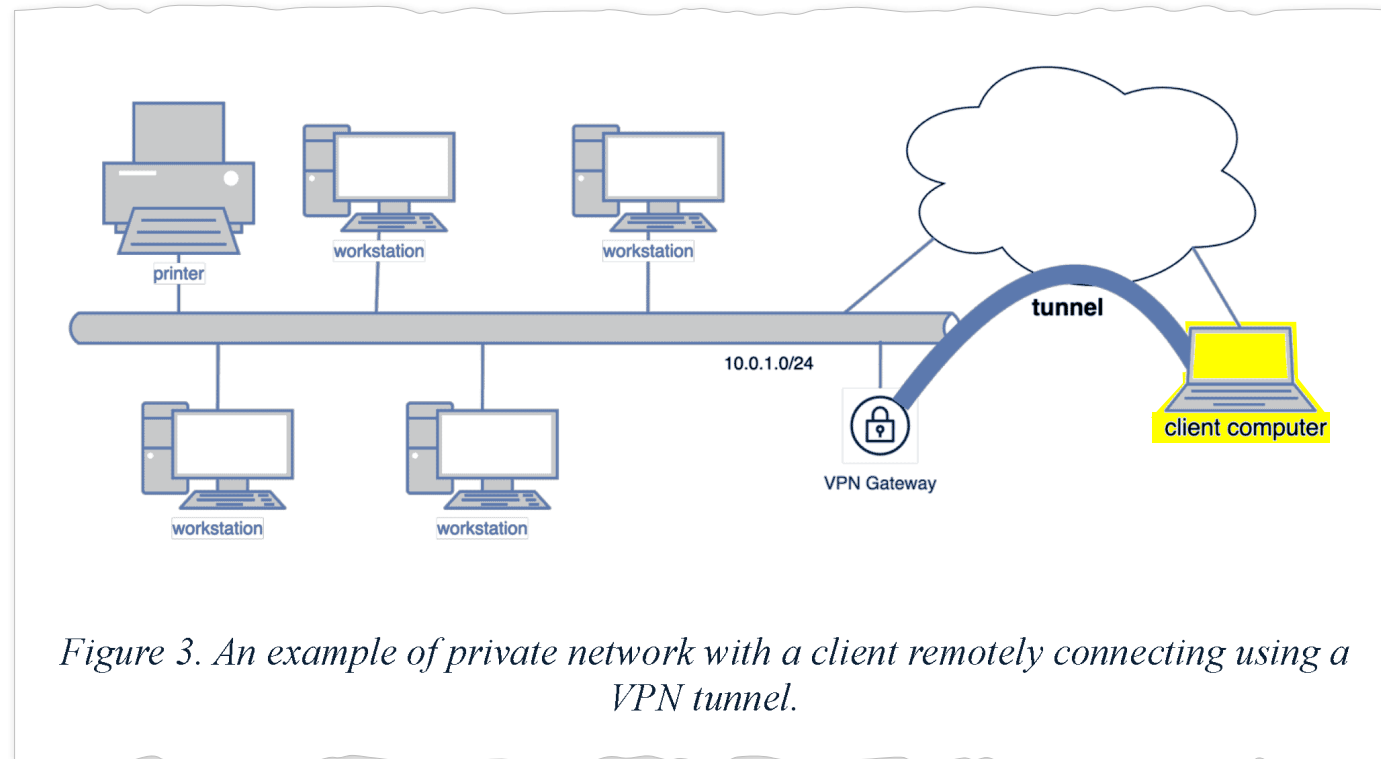
In the simplest sense, a VPN connects two endpoints over a public network to form a logical connection. The logical connections can be made at either Layer 2 or Layer 3 of the OSI model, and VPN technologies can be classified broadly on these logical connection models as Layer 2 VPNs or Layer 3 VPNs. Conceptually, establishing connectivity between sites over a Layer 2 or Layer 3 VPN is the same. The concept involves adding a “delivery header” in front of the payload to get it to the destination site. In the case of Layer 2 VPNs, the delivery header is at Layer 2, and in the case of Layer 3 VPNs, it is (obviously) at Layer 3. ATM and Frame Relay are examples of Layer 2 VPNs; GRE, L2TP, MPLS, and IPSec are examples of Layer 3 VPN technologies.

EX2009 at 23; 124 Reply at 14

Neufeld Renders Obvious the Use of a Point-Point VPN

- Dr. Noubir's own evidence proves that a VPN tunnel can terminate at a client computer rather than outside a client computer at a router

Noubir Declaration



EX2006 at 14; 124 Sur-Reply at 7

Neufeld Renders Obvious the Use of a Point-Point VPN

- Dr. Noubir admitted that it was possible to have a VPN tunnel terminating at two client computers at the time of the '140 patent

Noubir Deposition

Q. Was it possible to have a VPN tunnel between two client computers going through the internet at the time of the '140 patent?

A. Yes, it is possible.

Q. And a des -- the description of that that one might use would be a point-to-point VPN tunnel, correct?

A. So in the context of IPsec that -- that is called transport mode via -- and you can have that. This -- the -- so yes, you can definitely run VPN between two clients.

Q. And a way to describe that to a person who's skilled in the art would be a point-to-point VPN, correct?

A. So you could[] say that, yeah.

Neufeld Renders Obvious the Use of a Point-Point VPN

- Dr. Noubir admitted that it was possible to have a VPN tunnel terminating at two client computers at the time of the '140 patent

Noubir Deposition

Q. Such a point-to-point VPN tunnel could include encryption technology such as IPsec to encrypt the communications via the tunnel, correct?

A. Yes, you could have a VPN tunnel between two computers.

EX1049 at 50:4-8; 124 Reply at 15

Neufeld Renders Obvious the Use of a Point-Point VPN

- PO's Sur-Reply states that Neufeld's VPN disclosures are directed toward **network** access
- This is belied by the Neufeld disclosures on which it relies, which discuss accessing the server **system**

124 Sur-Reply

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.

124 Sur-Reply at 6-7

- The server **system** endpoint in a point-to-point tunneling VPN is necessarily “behind the NIC” 110

Neufeld Renders Obvious the Use of a Point-Point VPN

- PO's Sur-Reply states that Neufeld's VPN disclosures are directed toward **network** access
- This is belied by the Neufeld disclosures on which PO relies, which discuss accessing the server **system**

Neufeld

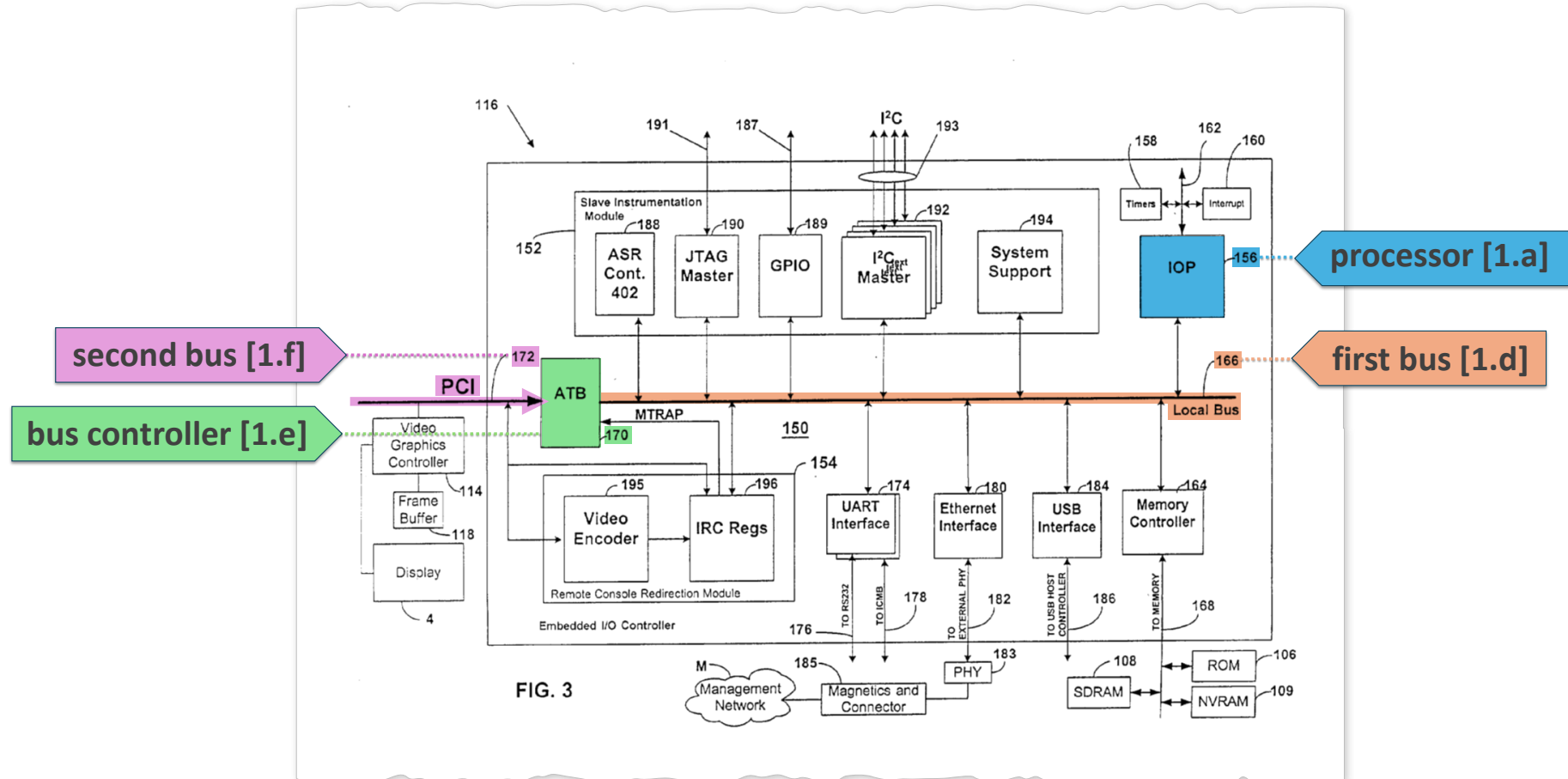
[0088] Of course, as the confidence level in the actual identity of the authorized user falls, such as in remote and/or off hour connections depicted in situations 3 and 5, the authentication services may become more rigorous and require the use of a smartcard or biometrics, for example. Once the user is properly authenticated, access to non-critical functions is granted. Finally, a user, such as the typical user depicted in Table 4, may attempt different types of remote connections, such as via the Internet or via a virtual private network. It may be determined that all users, or at least certain groups of users, should not be granted access to the managed server 2 via an Internet connection as set forth in situation 6. However, all users, or certain groups of users, may be permitted access during normal and/or off business hours via a virtual private network with proper authentication, as set forth in situation 7.

EX1005 at ¶88; 124 Reply at 17; 124 Sur-reply at 7

IPR2024-00109:
**Neufeld Renders Obvious Receipt of Encrypted
Management Messages Via Local Bus 166 at RMC 116**

Neufeld Renders Obvious Receipt of Encrypted Management Messages Via Local Bus 166 at RMC 116

Neufeld



EX1005 at Fig. 3; 109 Petition at 16-18, 22-25

Neufeld Renders Obvious Receipt of Encrypted Management Messages Via Local Bus 166 at RMC 116

Meldal Declaration

98. As discussed above, Neufeld discloses and/or renders obvious to a POSITA that the remote management controller 116 receives in-band communications including management requests from the remote management PC 5 via the NIC 110. *see also* limitation [1.b] and EX1005, ¶[0043] (“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”), ¶[0047] (“[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]”) and Figs. 2-3 (showing connection between Network N and remote management controller 116).

EX1003 at ¶98;
109 Petition at 24-25

Neufeld Renders Obvious Receipt of Encrypted Management Messages Via Local Bus 166 at RMC 116

Meldal Declaration

99. As shown in Fig. 2, the NIC 110 is connected to the PCI bus 16 in the server CPU 3. As discussed above for limitation [1.f], the PCI bus 172 of Fig. 3 is an extension of the PCI bus 16 of Fig. 2. Thus, the ATB 170 receives the encrypted management requests from the remote management PC 5 through the NIC 110 via the PCI bus 172.

EX1003 at ¶99; 109 Petition at 24-25

Neufeld Renders Obvious Receipt of Encrypted Management Messages Via Local Bus 166 at RMC 116

Meldal Declaration

100. Neufeld discloses and/or renders this limitation obvious to a POSITA.

See limitation [1.g] establishing that management requests are received by the

ATB 170. Neufeld further discloses that the ATB 170 is connected to IOP 156 via the first bus 166. *See* limitation [1.e]; *see also* EX1005, Fig. 3.

EX1003 at ¶100; 109 Petition at 26

Neufeld Renders Obvious Receipt of Encrypted Management Messages Via Local Bus 166 at RMC 116

Meldal Declaration

101. Neufeld further discloses that IOP 156 provides general control and functions as the management processor for the remote management controller 156, and that the IOP 156 dictates the control and monitoring functions performed via the slave instrumentation module 152. EX1005, ¶¶[0054], [0066]. A POSITA therefore 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, and because the other devices in the remote management controller 110 are directed toward specific functions that do not include decrypting or acting on remote management requests.

EX1003 at ¶101;
109 Petition at 27

Neufeld Renders Obvious Receipt of Encrypted Management Messages Via Local Bus 166 at RMC 116

Meldal Declaration

102. To the extent that Neufeld does not disclose this limitation, it would have been obvious to a POSITA to provide for in-band communication of management requests from the remote management PC 5 to the IOP 156 of the remote management controller 116 in light of Neufeld's disclosure of the desirability of providing for in-band communication to control the managed server at ¶[0015] and the need to decrypt management requests in order to act on them.

EX1003 at ¶102; 109 Petition at 27-28

Neufeld Renders Obvious Receipt of Encrypted Management Messages Via Local Bus 166 at RMC 116

- Dr. Mishra testified that IOP 156 cannot transmit data over NIC 110

Mishra Declaration

124. Paragraph [0043] of Neufeld is describing the hardware-level connections that enable the RMC 116 to perform passive out-of-band monitoring of the server—not active in-band communication. Paragraph [0043] would have informed a POSITA that the RMC 116 is physically connected to system components such as the PCI bus and keyboard controller, which allows it to snoop on system activity (e.g., intercepting display data or keyboard inputs) without relying on or interfering with the host operating system. The mention of network N or a management network M does not imply that the RMC uses NIC 110 to receive

management requests through the server's primary network path; to the contrary, the Neufeld makes clear that the RMC's external communications are handled through a dedicated interface (e.g., Ethernet interface 180), and that the entire system is designed to operate independently of any software on the managed server. Instead, the reference to network N is simply identifying that RMC 116 is able to snoop on the data being sent/received by the managed device via the network N. RMC 116 could not snoop on such traffic unless it was connected to Network N. Thus, Paragraph [0043] of Neufeld describes the hardware context for the RMC's out-of-band functionality—not a software-dependent in-band communication path.

EX2007 at ¶124; 109 Reply at 13

Neufeld Renders Obvious Receipt of Encrypted Management Messages Via Local Bus 166 at RMC 116

- Dr. Mishra's testimony that IOP 156 cannot transmit data over NIC 110 is directly contradicted by Neufeld at ¶48

Neufeld

[0048] In the operation of the remote management controller **116**, the I/O processor **156 (FIG. 3)** may periodically read the video graphics data from the frame buffer **118** to determine whether the data has changed. If the data has changed, the I/O processor **156** will compress the video graphics data and transmit the data to the remote console **5** via one of the communications devices (i.e., modem or NIC **110**). The remote console **5** will decompress and decode the data stream and display it at the remote console **5** for viewing by a user.

EX1005 at ¶48; 109 Reply at 14

Neufeld Renders Obvious Receipt of Encrypted Management Messages Via Local Bus 166 at RMC 116

- Dr. Mishra's testimony demonstrates two techniques for in-band communications by RMC 116 over the NIC 110 to Remote Management PC 5

Mishra Declaration

129. The RMC 116 requires the host server to run software in order to send data over NIC 110 because unlike Ethernet interface 180, the RMC 116 lacks direct, independent control of the NIC hardware. In typical server architectures, NIC 110 is initialized and managed by the host operating system, which configures the network interface, assigns IP addresses, and handles all protocol-level communication. If the RMC attempts to use this same NIC, it must either pass its management data through the host's networking stack or rely on a specialized sideband interface, such as NC-SI, that supports out-of-band communication. Without such hardware support, the RMC cannot independently transmit data over NIC 110, as it would lack access to essential network services like ARP resolution, routing, and protocol handling. In such cases, software on the host system is needed to coordinate or tunnel RMC communications through the NIC.

EX2007 at ¶129;
109 Reply at 15-16

Neufeld Renders Obvious Receipt of Encrypted Management Messages Via Local Bus 166 at RMC 116

- Dr. Mishra's objection is based on the false assertion that in-band and out-of-band communications are mutually exclusive

Mishra Declaration

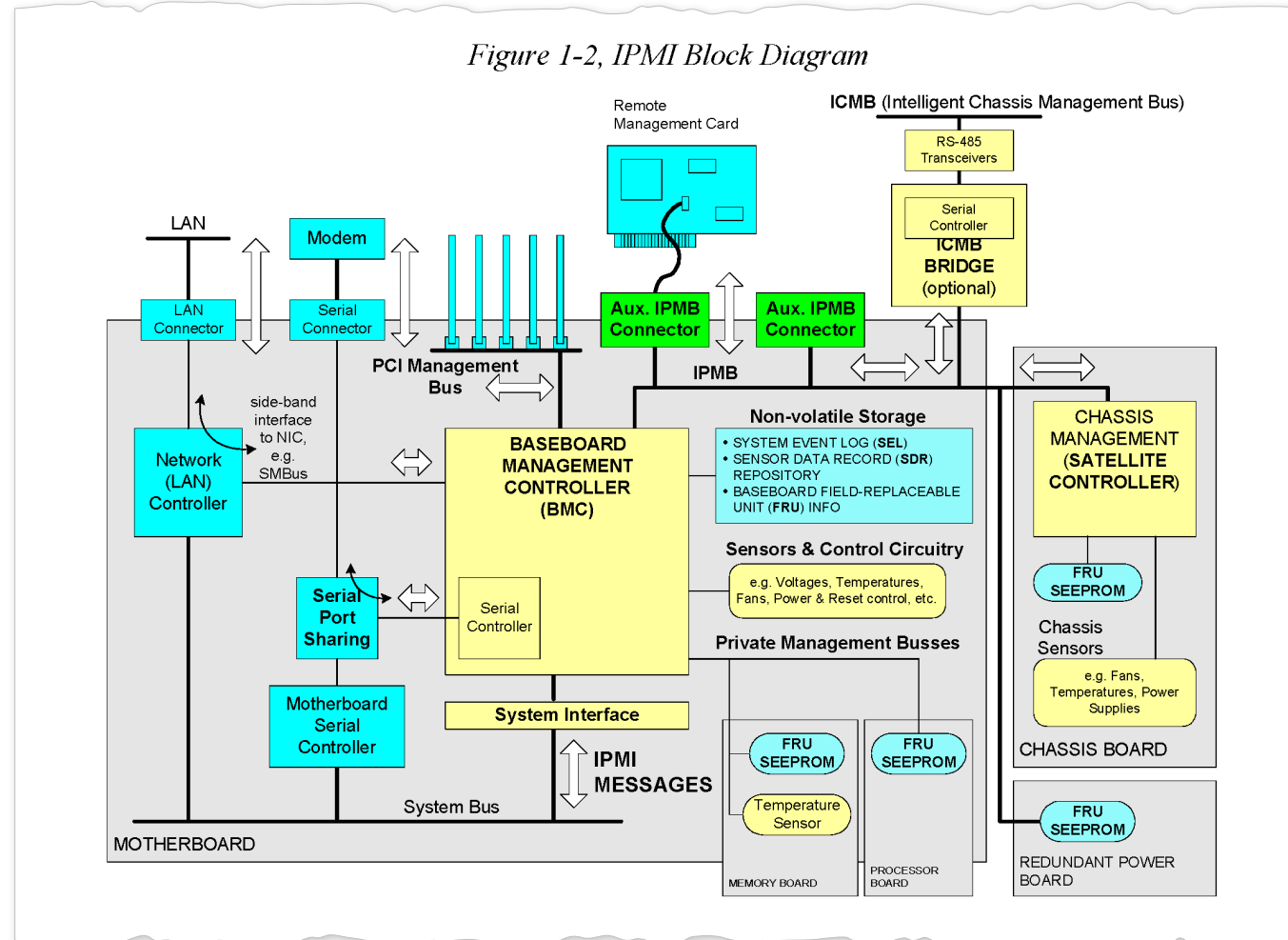
130. As a result, the RMC 116 would necessarily depend on host software to transmit data through NIC 110 to network N, rendering such communication in-band rather than out-of-band. This dependency is fundamentally at odds with the goal of Neufeld's out-of-band management, which is to maintain remote access even when the host operating system is down or unresponsive.

EX2007 at ¶130; 109 Reply at 15

**IPR2024-00109:
IPMI, Huckins and Frantz Render Obvious
Claims 1-3, 9, 12, 15 and 17**

IPR2024-00109: IPMI, Huckins and Frantz Render Obvious Claim 1

IPMI

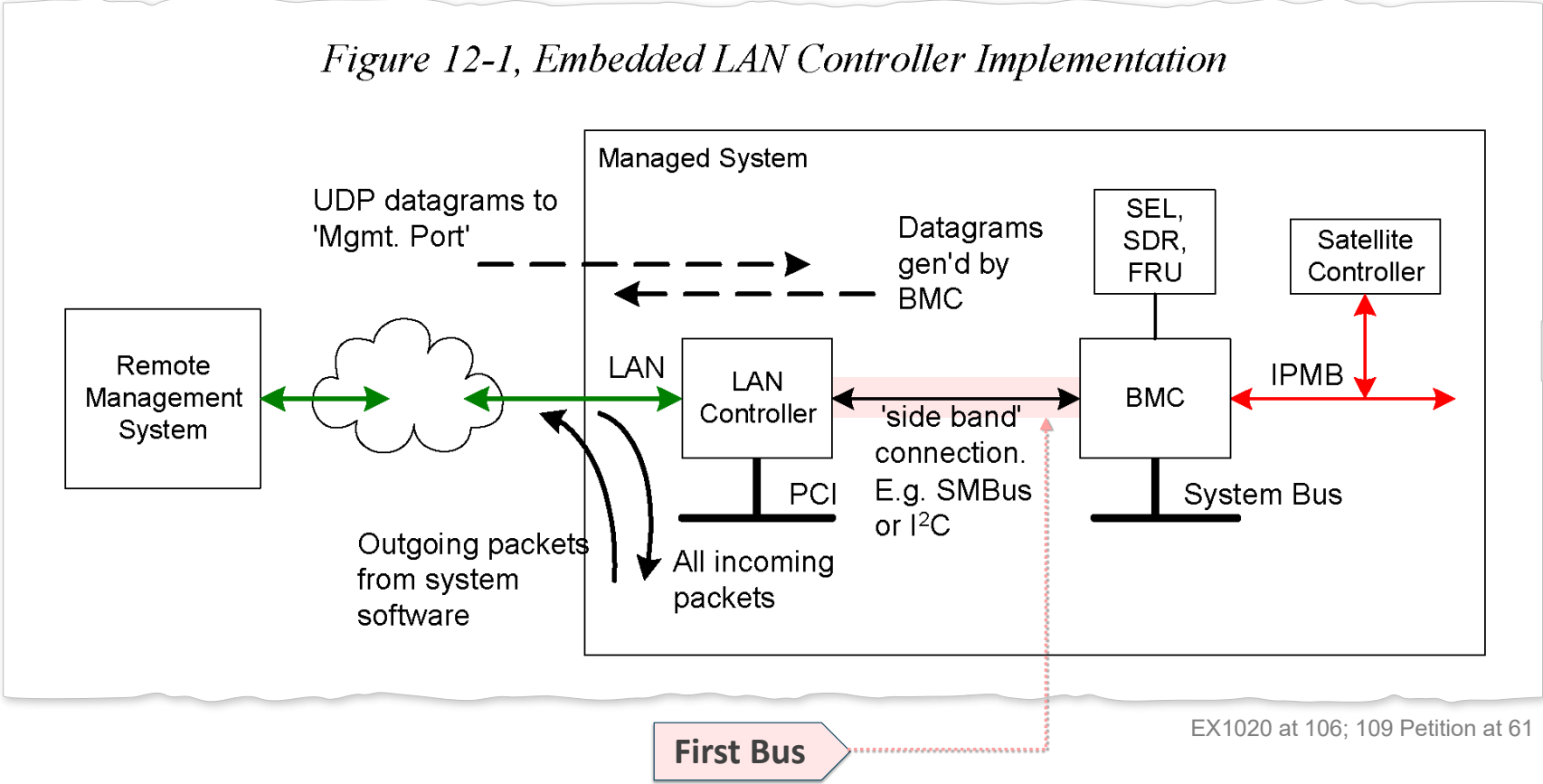


EX1020 at 9; 109 Petition at 56

IPR2024-00109: IPMI, Huckins and Frantz Render Obvious Claim 1

IPMI

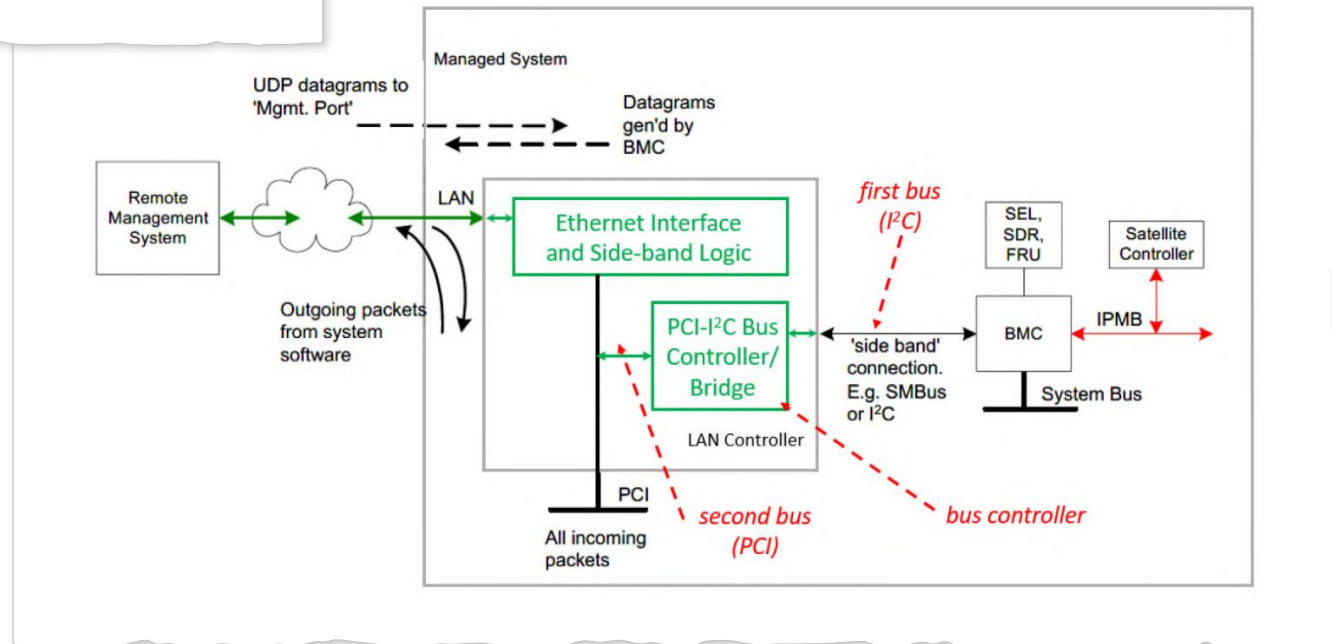
Figure 12-1, Embedded LAN Controller Implementation



IPR2024-00109: IPMI, Huckins and Frantz Render Obvious Claim 1

Meldal Declaration

198. A POSITA would have found it obvious to implement a network controller/side-band interface as described in IPMI by combining Ethernet LAN controller logic with a PCI-I²C bus controller and bridging device of the type described in Huckins as shown in the modified version of Fig. 12-1 below.



EX1003 at ¶198; 109 Petition at 64

IPR2024-00109: IPMI, Huckins and Frantz Render Obvious Claim 1

The only issue raised in the Institution Decision was whether IPMI and Huckins teach the claimed bus controller

109 Institution Decision

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.

109 Institution Decision at 33

IPR2024-00109: IPMI, Huckins and Frantz Render Obvious Claim 1

The only issue raised in the Institution Decision was whether IPMI and Huckins teach the claimed bus controller

109 Institution Decision

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.

109 Institution Decision at 33

IPR2024-00109: IPMI, Huckins and Frantz Render Obvious Claim 1

The only issue raised in the Institution Decision was whether IPMI and Huckins teach the claimed bus controller

109 Institution Decision

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).

IPR2024-00109: IPMI, Huckins and Frantz Render Obvious Claim 1

The only issue raised in the Institution Decision was whether IPMI and Huckins teach the claimed bus controller

109 Institution Decision

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.

109 Institution Decision at 34

IPR2024-00109: IPMI, Huckins and Frantz Render Obvious Claim 1

The only issue raised in the Institution Decision was whether
IPMI and Huckins teach the claimed bus controller

Huckins

[0040] FIG. 6A is a flow chart showing one embodiment of a method in accordance with the present invention to communicate with a non-PCI compatible device across a PCI bus. The method of this example describes what occurs during an access from the system to a non-PCI compatible device that is coupled to the system PCI bus through a bus bridge. For this embodiment, one end of the bus bridge connects to the system PCI bus and the other end of the bus bridge connects to a non-PCI compatible bus. The non-PCI compatible bus of this example is not specified, but the non-PCI compatible bus can be one of many types of bus protocols available, depending on the embodiment.

EX1007 at ¶40; EX1003 at ¶97;
109 Petition at 63

- PO does not assert that a POSITA did not know how to implement a PCI-I²C bridge
- PCF8584 (EX1009) is a “parallel-bus to I²C but protocol converter and interface”

IPR2024-00109: IPMI, Huckins and Frantz Render Obvious Claim 1

The only issue raised in the Institution Decision was whether IPMI and Huckins teach the claimed bus controller

109 Institution Decision

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.

109 Institution Decision at 34

IPR2024-00109: IPMI, Huckins and Frantz Render Obvious Claim 1

The only issue raised in the Institution Decision was whether IPMI and Huckins teach the claimed bus controller

I²C-bus Controller Data Sheet

Philips Semiconductors

Product specification

I²C-bus controller

PCF8584

1 FEATURES

- Parallel-bus to I²C-bus protocol converter and interface
- Compatible with most parallel-bus microcontrollers/microprocessors including 8049, 8051, 6800, 68000 and Z80
- Both master and slave functions
- Automatic detection and adaption to bus interface type
- Programmable interrupt vector
- Multi-master capability
- I²C-bus monitor mode
- Long-distance mode (4-wire)
- Operating supply voltage 4.5 to 5.5 V
- Operating temperature range: -40 to +85 °C.

2 GENERAL DESCRIPTION

The PCF8584 is an integrated circuit designed in CMOS technology which serves as an interface between most standard parallel-bus microcontrollers/microprocessors and the serial I²C-bus. The PCF8584 provides both master and slave functions.

Communication with the I²C-bus is carried out on a byte-wise basis using interrupt or polled handshake. It controls all the I²C-bus specific sequences, protocol, arbitration and timing. The PCF8584 allows parallel-bus systems to communicate bidirectionally with the I²C-bus.

EX1009 at 3; WX1003 at ¶136; 109 Reply at 21; 109 Petition at 40

IPR2024-00109: IPMI, Huckins and Frantz Render Obvious Claim 1

The only issue raised in the Institution Decision was whether IPMI and Huckins teach the claimed bus controller

Mishra Deposition

Q. And there's going to be a bus controller for every I²C bus, right? Not necessarily multiple but there will be at least one?

A. Yes.

EX1043 at 147:14-17

I²C-bus Controller Data Sheet

Philips Semiconductors

Product specification

I²C-bus controller

PCF8584

1 FEATURES

- Parallel-bus to I²C-bus protocol converter and interface
- Compatible with most parallel-bus microcontrollers/microprocessors including 8049, 8051, 6800, 68000 and Z80
- Both master and slave functions
- Automatic detection and adaption to bus interface type
- Programmable interrupt vector
- Multi-master capability
- I²C-bus monitor mode
- Long-distance mode (4-wire)
- Operating supply voltage 4.5 to 5.5 V
- Operating temperature range: -40 to +85 °C.

2 GENERAL DESCRIPTION

The PCF8584 is an integrated circuit designed in CMOS technology which serves as an interface between most standard parallel-bus microcontrollers/microprocessors and the serial I²C-bus. The PCF8584 provides both master and slave functions.

Communication with the I²C-bus is carried out on a byte-wise basis using interrupt or polled handshake. It controls all the I²C-bus specific sequences, protocol, arbitration and timing. The PCF8584 allows parallel-bus systems to communicate bidirectionally with the I²C-bus.

EX1009 at 3; 109 Reply at 21

IPR2024-00109: IPMI, Huckins and Frantz Render Obvious Claim 1

The only issue raised in the Institution Decision was whether IPMI and Huckins teach the claimed bus controller

109 Institution Decision

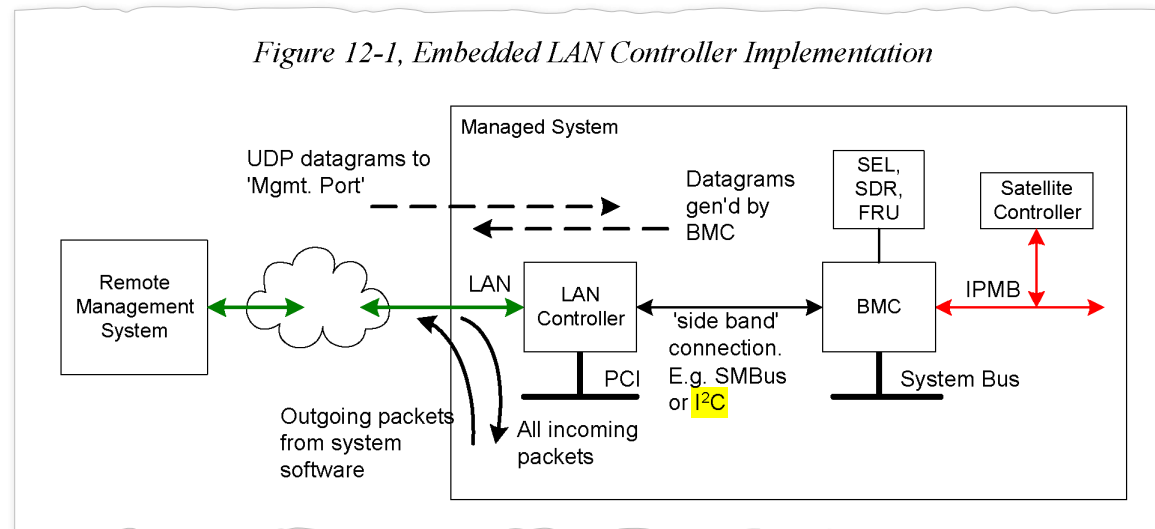
Notably, Petitioner does not argue that Huckins teaches a known implementation of a bridge between a PCI bus and an I²C bus, which is what Petitioner argues that one of ordinary skill would look to, as we address above. *Id.* at 62 (citing Ex. 1003 ¶ 196). Nor does Petitioner cite any art that evidences 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.

109 Institution Decision at 34

IPR2024-00109: IPMI, Huckins and Frantz Render Obvious Claim 1

The only issue raised in the Institution Decision was whether IPMI and Huckins teach the claimed bus controller

IPMI



EX1020 at ¶128; EX1003 at ¶¶196-197; 109 Petition at 62

Meldal Declaration

6. [1.e] a bus controller coupled to the processor via the first bus;

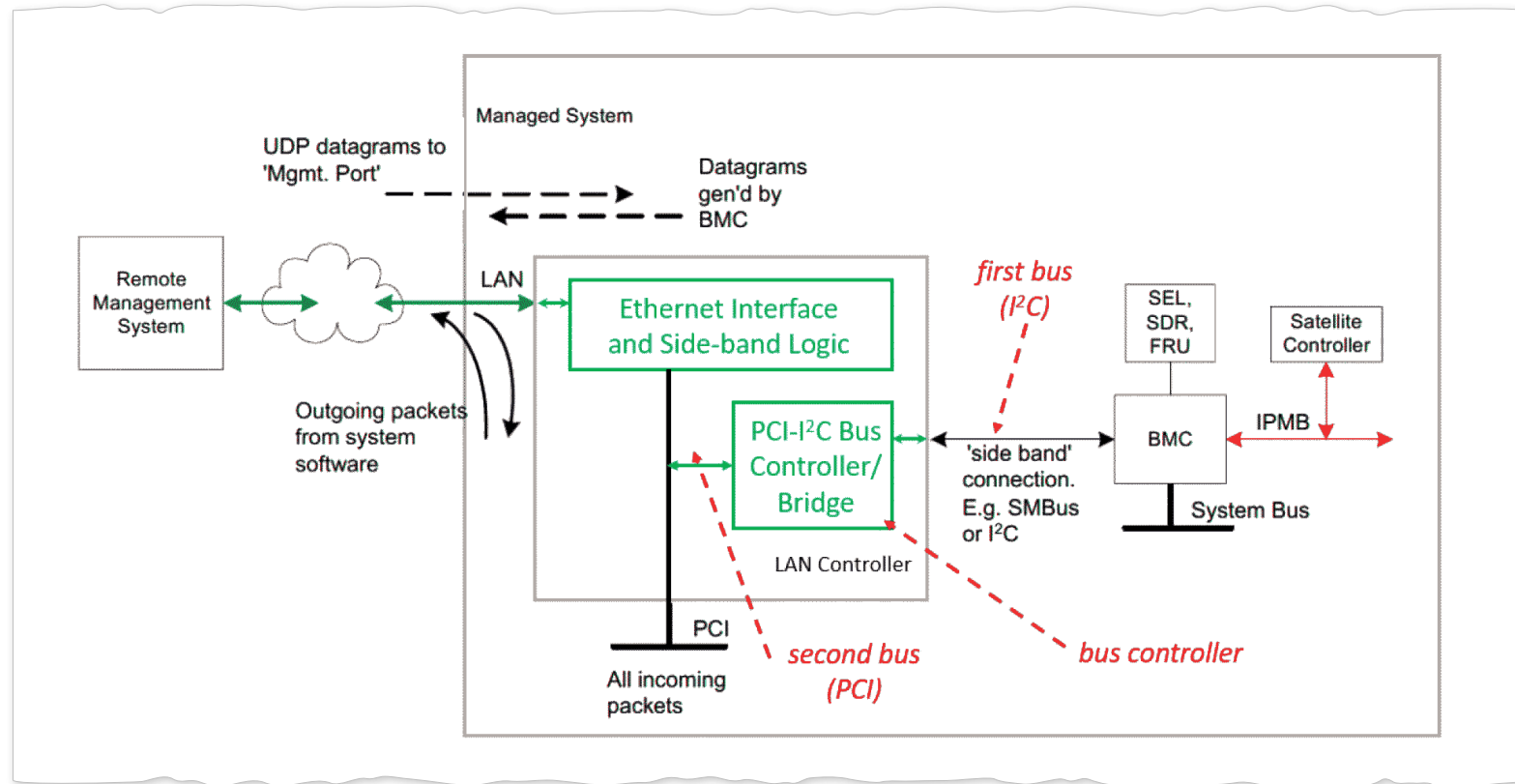
196. IPMI in combination with Huckins renders obvious this limitation.

As discussed above, IPMI discloses in Fig. 12-1 a “Network (LAN) Controller” that connects to a PCI bus on the managed platform and that includes a side-band interface to an I²C bus or SMBus on which in-band IPMI management messages received from a remote management system are sent to the BMC, but does not explain how to implement such a network controller with such a side-band interface. In IPMI Figure 12-1 above, the Network (LAN) Controller must interface to a PCI bus. A POSITA would have recognized that one way to implement a side-band connection using a Network (LAN) Controller that interfaces with a PCI bus is by (1) adding a bridge between the PCI bus to which the Network (LAN) Controller interfaces and the side-band bus, which IPMI identified in Fig. 12-1 as an I²C bus or an SMBus, and (2) configuring the Network (LAN) controller to direct packets addressed to the BMC to the bridge. A POSITA would therefore look to known implementations of a bridge between a PCI bus and an I²C bus or an SMBus.

IPR2024-00109: IPMI, Huckins and Frantz Render Obvious Claim 1

The Petition makes the “upstream showings” 109 Sur-Reply at 22

Meldal Declaration



EX1003 at ¶198; 109 Petition at 64

IPR2024-00109: IPMI, Huckins and Frantz Render Obvious Claim 1

The Petition makes the “upstream showings” 109 Sur-Reply at 22

109 Institution Decision

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.

109 Institution Decision at 31

IPR2024-00109: IPMI, Huckins and Frantz Render Obvious Claim 1

The Petition makes the “upstream showings” 109 Sur-Reply at 22

Meldal Declaration

199. In this modified version of Figure 12-1, the Network (LAN) Controller is implemented using known Ethernet Interface logic with additional Sideband logic that recognizes UDP datagram packets directed toward the management port which carry IPMI management messages. These packets can be differentiated from packets carrying normal user data based on IP addresses and/or or UDP port numbers. Those packets are transmitted over the PCI bus (the claimed second bus of limitation [1.f]) to a PCI-I²C bus controller-bridge of the type described in Huckins. EX1007, ¶[0026]. The packets are then transmitted from the PCI-I²C bus controller-bridge over the I²C/first bus to the BMC (the claimed processor). EX1007, ¶[0026]. The normal user data packets are transmitted from the Ethernet Logic to the system PCI bus for normal processing by the managed platform.

EX1003 at ¶199; 109 Petition at 64

IPR2024-00109: IPMI, Huckins and Frantz Render Obvious Claim 1

The Petition makes the “upstream showings” 109 Sur-Reply at 22

Meldal Declaration

200. This is a straightforward implementation of a Network (LAN) controller with side-band logic as described in IPMI that would have been obvious to, and well within the skill level of, a POSITA at the time of the 016 patent. A POSITA would have had a reasonable expectation of success in implementing the IPMI Network (LAN) Network (LAN) Controller in this manner.

EX1003 at ¶200; 109 Petition at 65

IPR2024-00109: IPMI, Huckins and Frantz Render Obvious Claim 1

Dr. Mishra admitted that it is possible to send encrypted communications over an I²C bus

Mishra Deposition

Q. So it's perfectly possible to send encrypted communications over an I²C bus, right?

A. When you encrypt a set of bits, it remain another set of bits, so the answer is yes.

EX1043 at 105:8-11; 109 Reply at 27

**IPR2024-00124:
Claims 1-3, 6-7 and 10-11
Are Obvious Over IPMI and Lawrence**

IPR2024-00124: Claims 1-3, 6-7 and 10-11 Are Obvious Over IPMI and Lawrence

124 Institution Decision

We view Petitioner’s arguments as focusing on IPMI’s side-band interface, and do not address having a VPN connect to the remote user. *See* Pet. 51–54, 64–65. Thus, at this stage, we agree with Patent Owner that Petitioner does not sufficiently show why one of ordinary skill in the art would have been motivated to use a VPN on an internal connection (side-band interface) within a server, absent such security on the external connection portion. *See* Prelim. Resp. 51–52. Similarly, we also find that Petitioner does not clearly explain how the corresponding structure (the VPN) “connect[s] said one or more . . . remote users with said secure management access controller.” *See* Pet. 65.

124 Institution Decision at 33

IPR2024-00124: Claims 1-3, 6-7 and 10-11 Are Obvious Over IPMI and Lawrence

Lawrence

A disadvantage of using the prior art an in-band management schemes is a **lack of security** for carrying management traffic. That is, the management traffic or commands are carried on **non-secure data links** (e.g., core data links **420**). Thus, prior art in-band management configuration schemes are susceptible to unauthorized management entry or interception of management commands.

EX1043 at 2:52-58; EX1046 at ¶158; 124 Petition at 53

IPR2024-00124: Claims 1-3, 6-7 and 10-11 Are Obvious Over IPMI and Lawrence

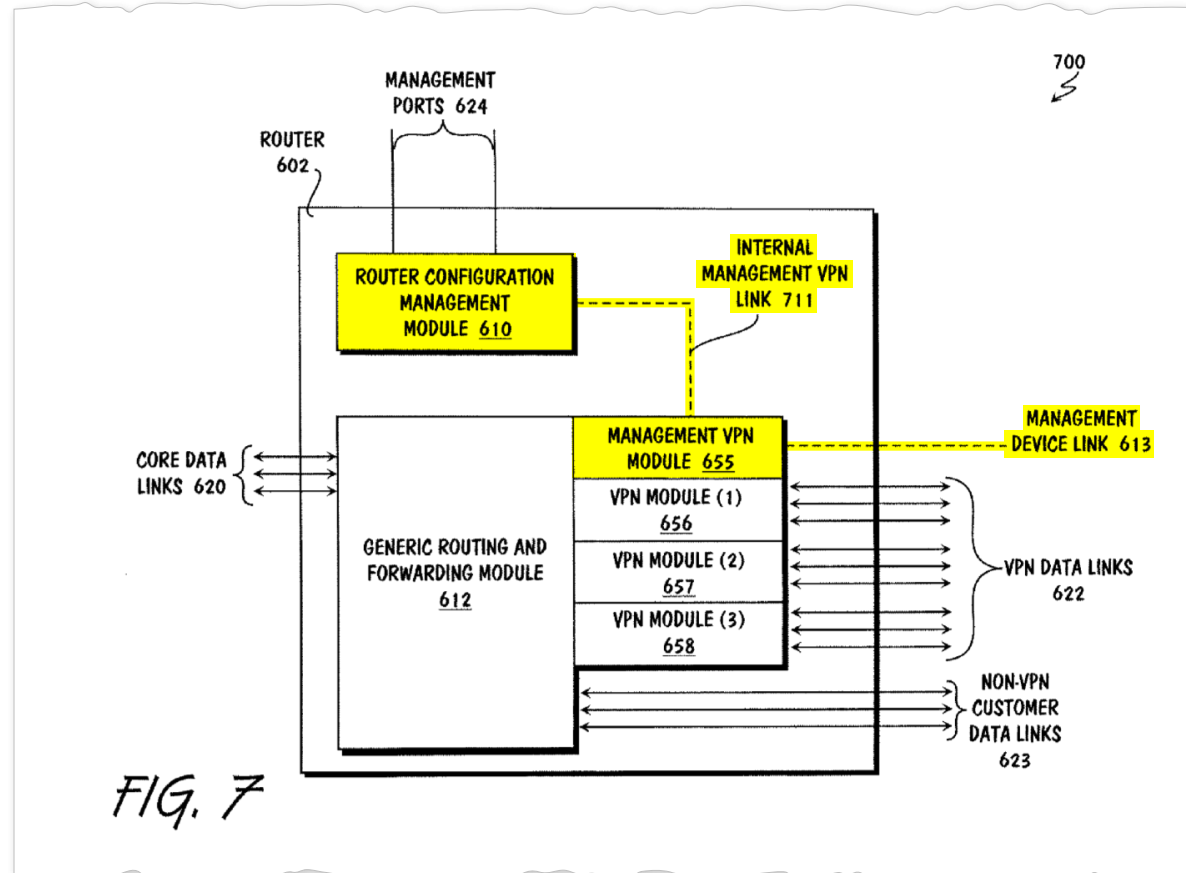
Meldal Declaration

158. Lawrence discusses the advantages of in-band communication of management data but explains that prior art in-band systems were carried on non-secure data links and were therefore “susceptible to unauthorized management entry or interception of management commands.” EX1043, 2:20-58. Lawrence discloses embodiments for secure in-band communication of management information, including the embodiment shown in Figure 7 below in which management data is communicated to a router configuration management module 610 via a dedicated management VPN module 655 and an internal management VPN link 711 (with highlighting):

EX1046 at ¶158; 124 Petition at 54

IPR2024-00124: Claims 1-3, 6-7 and 10-11 Are Obvious Over IPMI and Lawrence

Lawrence



EX1043 at Fig.7; EX1046 at ¶158; 124 Petition at 54

IPR2024-00124: Claims 1-3, 6-7 and 10-11 Are Obvious Over IPMI and Lawrence

Meldal Declaration

159. Lawrence further discloses that such dedicated management VPN modules 655 performs VPN encapsulation, routing and forwarding functions and may include encryption using an IPSec or other process. EX1043, 5:15-30. The disclosure of encapsulation indicates VPN tunneling.

EX1046 at ¶159; 124 Petition at 54

IPR2024-00124: Claims 1-3, 6-7 and 10-11 Are Obvious Over IPMI and Lawrence

Lawrence

The generic routing and forwarding module 612 performs basic routing and forwarding of data packets for router 602. That is, generic routing and forwarding module 612 can maintain routing tables, which are used to send packets to a destination using an optimal path. The generic routing and forwarding module 612 is coupled to management VPN module 655 and to VPN module 1 (656) through VPN module 3 (658). Each of the VPN modules 655 through 658 can perform VPN-related encapsulation, routing, and forwarding functions on packets passing through router 602.

The encapsulation process entails adding extra headers to the each data packet to identify VPN membership and access; furthermore, during the encapsulation process, the data packet may be encrypted using IP security (IPSec) process or another data encryption process. In this way, the packets are kept private and secure. Furthermore, some

EX1043 at 5:15-30; EX1046 at ¶159; 124 Petition at 54

A POSITA would have understood that incoming management packets received at Management VPN Module 655 are encrypted because otherwise protecting them using a VPN before forwarding them over an internal link to the management module 610 makes no sense as the Board itself recognized.

124 Reply at 20-21

IPR2024-00124: Claims 1-3, 6-7 and 10-11 Are Obvious Over IPMI and Lawrence

The arguments and evidence cited in the 124 Reply are entirely proper

- There is no new rationale to combine the prior art
 - Petition and Reply both rely on adding Lawrence’s VPN functionality to IPMI’s LAN Controller to securing management data as motivation for combination 124 Petition at 53-55; 124 Reply at 20-21
- Citing new arguments and evidence in Reply to support that motivation is entirely proper

Genzyme Therapeutic Prods. Ltd. P’ship v. Biomarin Pharm. Inc.



Holding “the introduction of new evidence in the course of the trial is to be expected in [IPR] trial proceedings” and permissible “as long as the opposing party is given notice of the evidence and an opportunity to respond to it.”

Genzyme Therapeutic Prods. Ltd. P’ship v. Biomarin Pharm. Inc., 825 F.3d 1360, 1366 (Fed. Cir. 2016)

Rembrandt Diagnostics, LP v. Alere, Inc.



Finding new argument in reply that cost and time savings provide motivation for combination was proper response to lack of motivation argument by patent owner

Rembrandt Diagnostics, LP v. Alere, Inc., 76 F.4th 1376, 1385 (Fed. Cir. 2023)