

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

MPH TECHNOLOGIES OY,
Patent Owner.

IPR2019-00819
Patent 7,620,810 B2

Before KEVIN C. TROCK, JOHN D. HAMANN, and
STACY B. MARGOLIES, *Administrative Patent Judges*.

HAMANN, *Administrative Patent Judge*.

JUDGMENT

Final Written Decision on Remand
Determining Challenged Claims 4–6 Not Shown Unpatentable
35 U.S.C. §§ 144, 318(a)

I. INTRODUCTION

This case returns on remand from the United States Court of Appeals for the Federal Circuit in *Apple Inc. v. MPH Techs. Oy*, Nos. 2021-1355, 2021-1356, 2022 WL 4103286 (Fed. Cir. Sept. 8, 2022).¹ In our prior Final Written Decision in this proceeding, we determined that by a preponderance of the evidence Apple Inc. (“Petitioner”) (i) did not prove that claims 1–6 of U.S. Patent No. 7,620,810 B2 (Ex. 1001, “the ’810 patent”) are unpatentable, and (ii) proved that claim 7 of the ’810 patent is unpatentable. Paper 37 (“FWD”), 54–55. On Petitioner’s appeal, the Federal Circuit held that we erred in our construction for “encrypted” messages, and as a result, vacated our judgment of no unpatentability for claims 1–6 and remanded to the Board for further proceedings. *Apple*, 2022 WL 4103286, at *6, 8.

After the Federal Circuit’s decision, and before the mandate issued, Patent Owner filed a statutory disclaimer under 37 C.F.R. § 1.321, which states that Patent Owner “hereby disclaims and dedicates to the public the entirety of claims 1–3 of the ’810 Patent.” Ex. 3003, 1; Paper 50. Accordingly, claims 1–3 are no longer part of this proceeding. And for the reasons that follow, we determine that Petitioner does not show by a preponderance of the evidence that claims 4–6 are unpatentable.

¹ The Federal Circuit issued a joint decision, addressing Petitioner’s appeal from this proceeding, as well as Petitioner’s appeal from *Apple Inc. v. MPH Techs. Oy*, IPR2019-00820 (“the -820 case”). *Apple*, 2022 WL 4103286, at *1. On remand, we issue separate decisions for these cases for purposes of clarity.

A. Procedural History

Petitioner filed a Petition requesting *inter partes* review of claims 1–7 of the ’810 patent. Paper 2 (“Pet.”). MPH Technologies Oy (“Patent Owner”) filed a Preliminary Response. Paper 8.

We instituted *inter partes* review of claims 1–7 of the ’810 patent on all of the grounds raised in the Petition. Paper 10 (“Dec. on Inst.”), 7, 40. As to the Decision on Institution in this proceeding, Patent Owner filed a Request for Rehearing, and requested review by the Precedential Opinion Panel (“POP”). Paper 13; Ex. 3001. Patent Owner’s request for POP review was denied (Paper 16), and we denied Patent Owner’s Request for Rehearing (Paper 24).

Thereafter, Patent Owner filed a Response to the Petition. Paper 23 (“PO Resp.”). Petitioner filed a Reply to Patent Owner’s Response. Paper 26 (“Pet. Reply”). Patent Owner filed a Sur-reply to Petitioner’s Reply. Paper 29 (“PO Sur-reply”). An oral hearing was held on June 25, 2020. A transcript of the oral hearing is included in the record. Paper 36 (“Tr.”).

After the remand, we authorized a simultaneous exchange of additional briefing for the parties to address the legal effect of the statutory disclaimer. Paper 52, 6. Pursuant to that authorization, Petitioner filed an Opening Brief Post-Remand (Paper 54, “Pet. Rem. Open.”), Patent Owner filed an Opening Brief (Paper 55, “PO Rem. Open.”), Petitioner filed a Response Brief Post-Remand (Paper 57, “Pet. Rem. Resp.”), and Patent Owner filed a Response Brief (Paper 56, “PO Rem. Resp.”).

B. Related Matters

The parties identify as related matters the following: (i) *MPH Techs. Oy v. Apple Inc.*, No. 5:18-cv-05935-PJH (N.D. Cal.); (ii) *Apple Inc. v. MPH*

Techs. Oy, IPR2019-00820 (PTAB) (involving related U.S. Patent No. 7,937,581 B2); (iii) *Apple Inc. v. MPH Techs. Oy*, Appeal No. 21-1355 (Fed. Cir.); (iv) *MPH Techs. Oy v. Apple Inc.*, Appeal No. 21-1390 (Fed. Cir.); (v) Ex Parte Reexamination No. 90/015,174, filed Dec. 14, 2022; and (vi) Ex Parte Reexamination No. 90/015,175, filed Dec. 14, 2022. Paper 49, 1–2; Paper 53, 1.

C. The Challenged Patent

The '810 patent relates to “secur[ing] mobile connections in telecommunication networks.” Ex. 1001, 1:13–14. In particular, the '810 patent describes reducing the handover latency and computational overhead for secure connections, such as those employing Internet Protocol (“IP”) Security (“IPSec”) with mobile terminals² (i.e., terminals that can move from one network to another). *Id.* at 1:13–15, 1:57–64, 4:10–31, 6:48–50, 7:28–42, 10:34–42.

IPSec comprises a set of rules defined by the Internet Engineering Task Force (“IETF”) to “provide[] the capability to secure communications between arbitrary hosts,” according to the '810 patent. *Id.* at 1:57–64, 2:3, 2:6–10. The '810 patent states that these rules describe, *inter alia*, providing “access control based on the distribution of cryptographic keys.” *Id.* at 2:11–20. The '810 patent also describes the concept of a Security Association (“SA”), which according to the '810 patent is “a one-way relationship between a sender and a receiver that offers [negotiated] security services to the traffic carried on it.” *Id.* at 2:21–24.

² The '810 patent discloses that “the term[s] mobility and mobile terminal do[] not only mean physical mobility, . . . [but also] mean[] moving from one network to another, which can be performed by a physically fixed terminal as well.” Ex. 1001, 4:27–31.

The '810 patent discloses that IPSec supports two modes of operation (i.e., transport mode and tunnel mode). *Id.* at 3:8–9. “Typically, transport mode is used for end-to-end communication between two hosts.” *Id.* at 3:10–13. “Tunnel mode . . . is generally used for sending messages through more than two components,” such as “when one or both ends of a SA is a security gateway, such as a firewall or a router that implements IPSec.” *Id.* at 3:16–21.

“IPSec is intended to work with static network topolog[ies],” according to the '810 patent. *Id.* at 4:10–11. For example, IPSec can secure communications between hosts across a local area network (“LAN”), as well as across a private or public wide area network (“WAN”). *Id.* at 1:57–59. Figure 1, shown below, “illustrates an example of a telecommunication network to be used in the invention” of the '810 patent. *Id.* at 8:40–41.

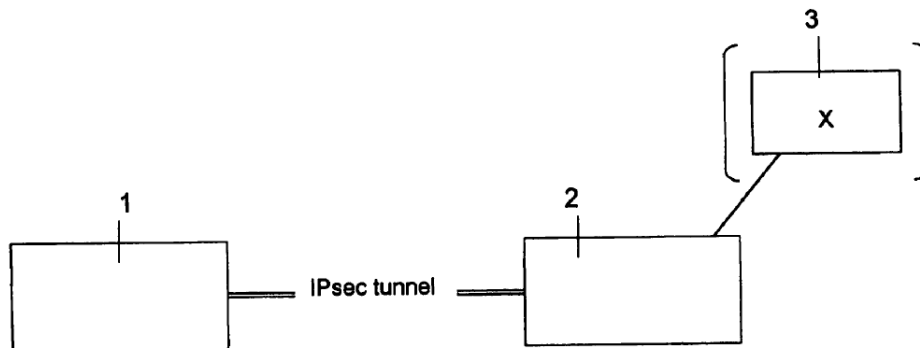


FIG. 1

Figure 1 depicts an example telecommunication network comprising “computer 1 . . . and computer 2[,] a destination computer, to which the secure messages are sent . . . by means of an IPSec tunnel established between computer 1 and computer 2.” *Id.* at 8:54–58. The '810 patent adds: “Computer 2 [can] be a security gateway for a third computer 3. Then, the

messages sent from computer 2 to computer 3 are sent in plaintext.” *Id.* at 8:53–60.

The ’810 patent discloses that in forming an IPSec tunnel under IPSec’s default automated key management protocol (i.e., the Internet Key Exchange (“IKE”) protocol), “the tunnel endpoints are fixed and remain constant.” *Id.* at 3:66–4:4, 4:12–17. The ’810 patent adds: “If IPSec is used with a mobile host the IKE key exchange will have to be redone from every new[ly] visited network. This is problematic, because IKE key exchanges involve computationally expensive” calculations and require exchanging numerous messages between the endpoints, leading to higher latency. *Id.* at 4:15–26.

To address these problems, the ’810 patent discloses avoiding a full re-negotiation between the tunnel endpoints, when computer 1 moves networks. *E.g., id.* at 9:33–44 (describing prior art requires a full re-negotiation), 9:63–66. More specifically, the ’810 patent discloses initially establishing an IPSec tunnel between computer 1 (address A) and computer 2 (address X) using IKE, as in the prior art. *Id.* at 9:48–62, Fig. 5 (illustrating steps 1a–9a for setting up the tunnel); *compare id.* at Fig. 5, *with id.* at Fig. 4 (showing the same nine steps as the prior art solution); *see also id.* at 9:12–39 (describing the prior art IKE establishment of the tunnel).

The ’810 patent discloses that, when computer 1 moves from address A to address B, computer 1 sends from its new address (address B) to computer 2 (address X) at the other end of the established IPSec tunnel, a request for computer 2 to register its new address. *Id.* at 9:63–10:2. According to the ’810 patent, this request can be “encrypt[ed] and/or

authentica[ed] . . . us[ing] the same IPSec SA [that is used] for protecting both data and registration traffic.” *Id.* at 10:4–8.

The ’810 patent thus discloses that the tunnel’s IPSec SA is carried over to the new connection point, and computer 1 can send IPSec-protected messages to computer 2 after sending the request, which “essentially makes the handover latency zero.” *Id.* at 10:11–19, 10:34–37. “[T]he exact method of signalling is not important[;] the essence is to carry over the IPSec SA to the new connection point.” *Id.* at 10:11–13.

D. The Challenged Claims

Petitioner challenged claims 1–7 of the ’810 patent in the Petition. Pet. 4. Of these, claims 1–6 are the subject of the remand. *Apple*, 2022 WL 4103286, at *8. In light of Patent Owner’s statutory disclaimer (Ex. 3003, 1), however, only claims 4–6 remain for our consideration. Each of claims 4–6 depend directly from claim 3, which is the focus of our analysis below. We thus reproduce claim 3 below, as well as claim 1 from which it depends for context.

1. A method for ensuring secure forwarding of a message in a telecommunication network, having at least one mobile terminal and another terminal and a security gateway therebetween, the method comprising:

a) establishing a secure connection between a first address of the mobile terminal and an address of the security gateway, the secure connection defined by at least the addresses of the mobile terminal and the security gateway,

b) the mobile terminal changing from the first address to a second address,

c) while at the second address, the mobile terminal sending a request message to the address of the security gateway to request the security gateway to change the secure connection to be defined between the second address and the address of the security gateway,

in response to the request message from the mobile terminal, the security gateway changing an address definition of the secure connection from the first address to the second address, the mobile terminal sending a secure message in the secure connection from the second address of the mobile terminal to the other terminal via the security gateway,

the secure connection being established by forming a Security Association (SA) using IPSec protocols, and the request message and/or a reply message being encrypted and/or authenticated by using the same SA already established.

Ex. 1001, 10:48–11:8.

3. The method of claim 1 wherein the method further comprises the security gateway sending back a reply message to the mobile terminal at the second address to confirm the address change.

Id. at 11:12–15.

E. Instituted Grounds of Unpatentability

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

	References	Basis ³	Challenged Claim(s)
1.	Ishiyama, ⁴ Murakawa ⁵	§ 103(a)	1, 4, 5, 7
2.	Ishiyama, Murakawa, Ahonen ⁶	§ 103(a)	2, 3
3.	Ishiyama, Murakawa, Forslöw ⁷	§ 103(a)	6

³ The Leahy-Smith America Invents Act (“AIA”) included revisions to 35 U.S.C. § 103 that became effective on March 16, 2013. Because the ’810 patent issued from an application filed before March 16, 2013, we apply the pre-AIA version of the statutory basis for unpatentability.

⁴ US Patent No. 6,904,466 B1 (issued June 7, 2005) (Ex. 1004).

⁵ US Patent No. 7,028,337 B2 (issued Apr. 11, 2006) (Ex. 1005).

⁶ US Patent No. 6,976,177 B2 (issued Dec. 13, 2005) (Ex. 1006).

⁷ US Patent No. 6,954,790 B2 (issued Oct. 11, 2005) (Ex. 1007).

Pet. 4, 12–69. Petitioner submits in support of its arguments the Declaration of David Goldschlag, Ph.D. (Ex. 1002) and an additional Declaration of David Goldschlag, Ph.D. (Ex. 1020). Patent Owner submits in support of its arguments the Declaration of Professor George N. Rouskas, Ph.D. (Ex. 2003).

F. Prior Final Written Decision

In our prior Final Written Decision, we disagreed with Petitioner that Ishiyama taught a “request message . . . being encrypted,” as recited in independent claim 1. FWD 16–23; Ex. 1001, 11:6. In particular, we found that, as Petitioner admitted, “in Ishiyama the request message’s outer packet’s source address is unencrypted,” and “Ishiyama only teaches that the encapsulated packet (payload) is encrypted.” FWD 20 (citing Ex. 1004, 7:56–60; Tr. 27:9–16). We also found that “the outer packet’s source address is a part of the request message in Ishiyama.” *Id.* (citing Ex. 1004, Fig. 4, 8:59–65). Thus, we found that these teachings were contrary to “the request message . . . being encrypted” because “the plain words of the claim state that the message is encrypted—not that a portion of the message is encrypted.” *Id.* In other words, we found that “claim 1 requires that the request message (not just a portion thereof) is encrypted, and Petitioner fail[ed] to show that Ishiyama’s request message (which includes the unencrypted outer packet’s source address) meets this requirement.” *Id.* at 21 (citations omitted).

Accordingly, we found that Petitioner did not demonstrate by a preponderance of the evidence that claim 1 would have been obvious in view of Ishiyama and Murakawa, which is the sole ground challenging claim 1. FWD 8, 23. Furthermore, we found that the Petition does not present any

information with respect to claims 2–6—which depend directly or indirectly from claim 1—that addresses this deficiency in Ishiyama. *Id.* at 23, 53–54. Thus, we found that Petitioner did not demonstrate by a preponderance of the evidence that claims 2–6 would have been obvious in view of the asserted unpatentability grounds. *Id.*

G. The Federal Circuit’s Decision

The Federal Circuit held that we construed an encrypted request message, and erred in doing so. *Apple*, 2022 WL 4103286, at *4–6. In particular, the Federal Circuit held that we “performed a claim construction” when we stated that “the *plain words of the claim* state that the message is encrypted—not that a portion of the message is encrypted,” and that “claim 1 requires that the request message (not just a portion thereof) is encrypted.” *Id.* at *4 (citing FWD 20–21). The Federal Circuit stated that “[i]n doing so, the Board ‘establish[ed] the scope and boundaries of the subject matter that is patented.’” *Id.* (citations omitted).

The Federal Circuit, *inter alia*, addressed the specification of the ’810 patent and stated that “the specification[] contemplate[s] that ‘encrypted’ messages can be sent using outer packets with certain unencrypted addressing information, contrary to the Board’s construction.” *Id.* at *6; *see also id.* at *5 (addressing the specification) (citations omitted). The Federal Circuit thus held “that the Board adopted an erroneous claim construction of ‘request message and/or a reply message being encrypted’ within claim 1 of the ’810 patent . . . that excludes ‘encrypted’ messages because those messages are sent using packets with certain unencrypted addressing information.” *Id.* at *6. The Federal Circuit stated that the ’810 patent “contemplate[s] that a message can still be considered ‘encrypted’ if its

packet has unencrypted ‘outer IP header’ information.” *Id.* The Federal Circuit vacated the portions of our prior Final Written Decision “that rel[ie]d on that erroneous claim construction and remand[ed] for further proceedings.” *Id.*

In addition, the Federal Circuit noted Patent Owner’s arguments that the Federal Circuit could have “nevertheless affirm[ed] the Board’s determination as to claims 4–6 of the ’810 patent because [Petitioner] relied on Ahonen to meet the intervening limitations in claim 3 and did not include Ahonen in its grounds challenging those claims.” *Id.* at *6 n.4 (citation omitted). The Federal Circuit responded to these arguments by stating the following:

The Board did not reach this issue because it found [Petitioner] did not demonstrate claim 1 to be unpatentable. [FWD 23, 54]. Because we vacate the portions of the Board’s decision[] based on its construction of an “encrypted” request or reply message in claim 1, the Board should decide whether to consider this issue on remand.

Id.

II. LEVEL OF ORDINARY SKILL IN THE ART

To determine whether an invention would have been obvious at the time it was made, we consider the level of ordinary skill in the pertinent art at the time of the invention. *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966). In assessing the level of ordinary skill in the art, various factors may be considered, including the “type of problems encountered in the art; prior art solutions to those problems; rapidity with which innovations are made; sophistication of the technology; and educational level of active workers in the field.” *In re GPAC, Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995)

(citing *Custom Accessories, Inc. v. Jeffrey-Allan Indus., Inc.*, 807 F.2d 955, 962 (Fed. Cir. 1986)). “[O]ne or more factors may predominate.” *Id.*

In our Decision on Institution, we adopted Petitioner’s proposed definition for one having ordinary skill in the art at the time of the invention of the ’810 patent as one who “would have had a B.S. degree in Computer Engineering, Electrical Engineering, or an equivalent field, as well as at least 3–5 years of academic or industry experience in the Internet security industry.” Pet. 12 (citing Ex. 1002 ¶¶ 20–21). We maintained this definition in our prior Final Written Decision. FWD 9. Patent Owner did not dispute our adoption of Petitioner’s definition, nor otherwise address the level of ordinary skill at the time of the invention of the ’810 patent. *See generally* PO Resp.

Petitioner’s definition of the level of skill in the art is consistent with the ’810 patent and the asserted prior art, and we maintain Petitioner’s definition for purposes of this Final Written Decision. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001); *GPAC*, 57 F.3d at 1579; *In re Oelrich*, 579 F.2d 86, 91 (CCPA 1978). We apply Petitioner’s definition in our analysis below.

III. CLAIM CONSTRUCTION

Because the Petition was filed after November 13, 2018, we construe the challenged claims by applying “the standard used in federal courts, in other words, the claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. [§] 282(b), which is articulated in *Phillips [v. AWH Corp.]*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc).” *See* Changes to the Claim Construction Standard for Interpreting Claims in Trial Proceedings Before the Patent Trial and Appeal Board, 83 Fed. Reg. 51,340,

51,340, 51,358, 51,343–44 (Oct. 11, 2018) (amending 37 C.F.R. § 42.100(b) effective November 13, 2018) (now codified at 37 C.F.R. § 42.100(b) (2019)). Under *Phillips*, the words of a claim are generally given their “ordinary and customary meaning,” which is the meaning they would have had to a person of ordinary skill in the art at the time of the invention, in light of the specification and prosecution history. *See Phillips*, 415 F.3d at 1312–13.

Petitioner does not submit any terms for construction. Pet. 12 (arguing that “[a]ll claim terms of the ’810 patent should receive their ordinary and customary meaning”). Patent Owner submits the term “security gateway” for construction, and argues that its meaning is in dispute. PO Resp. 11–24. Our below analysis of Petitioner’s unpatentability arguments for claims 4–6, however, does not implicate this claim term. *See supra* Section V.C. Thus, we do not provide an express construction for “security gateway.” *See, e.g., Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)) (“[W]e need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy.’”).

In addition, we note that the Federal Circuit corrected our construction of “the request message and/or a reply message being encrypted,” as recited in claim 1 of the ’810 patent. *Apple*, 2022 WL 4103286, at *4–6; *see supra* Section I.G. This limitation, however, is not implicated in our analysis of the parties’ arguments concerning unpatentability of claims 4–6—the claims on remand that remain after Patent Owner’s statutory disclaimer.

IV. PRINCIPLES OF LAW

A claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time of the invention to a person having ordinary skill in the art. *KSR Int’l Co. v. Teleflex, Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) objective evidence of non-obviousness, if present.⁸ See *Graham*, 383 U.S. at 17–18. When evaluating a claim for obviousness, we also must “determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

V. CHALLENGED CLAIMS 4–6

Petitioner argues that the combination of Ishiyama and Murakawa renders claims 4 and 5 obvious. Pet. 54–59; Pet. Reply 22–25. In addition, Petitioner argues that the combination of Ishiyama, Murakawa, and Forsl w renders claim 6 obvious. Pet. 66–69; Pet. Reply 22–25. Patent Owner disputes that these combinations render these claims obvious, respectively. PO Resp. 63–64, 73; PO Sur-reply 24–25.

For the reasons that we discuss below, we determine that Petitioner does not show by a preponderance of the evidence that claims 4–6 would have been obvious. We first provide a summary of Ishiyama and

⁸ Patent Owner does not present arguments or evidence of such objective evidence of non-obviousness in its Response. See generally PO Resp.

Murakawa, as their teachings are referenced in our analysis below, followed by our analysis.

A. Summary of Ishiyama

Ishiyama relates to improving a mobile computer's "capab[ility] of carrying out communications while moving among a plurality of inter-connected networks." Ex. 1004, 1:9–11. In furtherance of this mobility, Ishiyama discloses having the mobile computer notify its correspondent host (i.e., the host at the other end of a communication) of its new address when the mobile computer moves networks. *E.g., id.* at 3:43–67, 6:13–18, 15:37–16:10. The mobile computer makes this notification by changing the source address of an outer packet of an encapsulated packet to the mobile computer's new address before sending the packet to the correspondent host. *Id.* When the correspondent host receives the packet from the mobile computer, the correspondent host detects the address change and updates its stored information to reflect the new address for the mobile computer. *E.g., id.* at 3:9–14.

Figure 4, shown below, is a schematic diagram illustrating a mobile computer changing locations in an exemplary configuration of a mobile communication system, in accordance with an embodiment of Ishiyama's invention. *Id.* at 5:5–7, 5:11–13.

FIG. 4

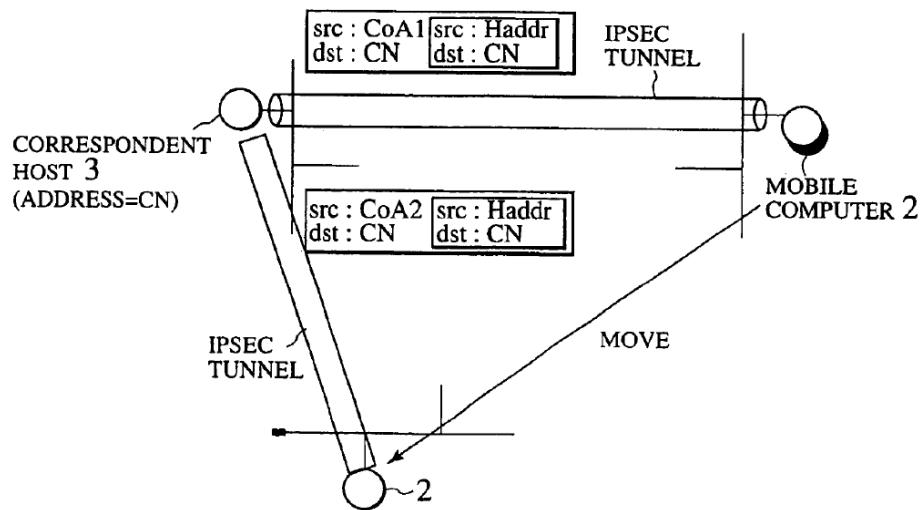


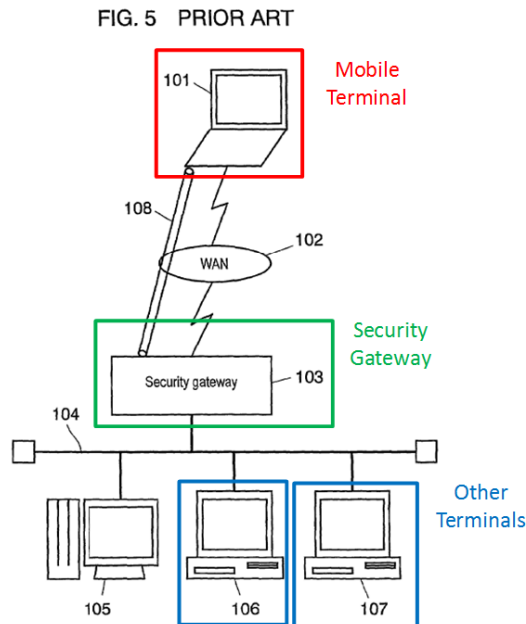
Figure 4 “shows an exemplary situation in which a packet is transferred from mobile computer 2 to . . . correspondent host 3 using [an] IPSEC tunnel.” *Id.* at 8:33–35. Initially, mobile computer 2 communicates with correspondent host 3 via an IPsec tunnel, with mobile computer 2’s address (CoA1) indicating its endpoint of the tunnel. *Id.* at 8:43–49. In other words, “mobile computer 2 transmits an encapsulated packet in which the outer packet has the source address=‘CoA1’ and the destination address=‘CN.’” *Id.* at 8:50–54. As shown, when mobile computer 2 moves, its address changes from CoA1 to CoA2. *Id.* at 8:55–58, Fig. 4 (showing that mobile computer 2 moves networks). To convey this change, mobile computer 2 changes the source address of the outer packet to CoA2 and transmits the packet to correspondent host 3 via the IPsec tunnel. *Id.* at 8:59–63, Fig. 4. Correspondent host 3 detects this change in mobile computer 2’s address, and replaces the CoA1 address with CoA2 in its database for the IPsec tunnel. *Id.* at 8:66–9:4; *see also id.* at Figs. 9B, 9D (showing the update of the address in correspondent host 3’s SA database),

12:51–59. Ishiyama discloses that the other SA information “remain[s] unchanged, so that there is no need to re-negotiate keys for IPS[ec] encryption and authentication.” *Id.* at 9:5–10.

B. Summary of Murakawa

Murakawa relates to allowing a PC outside a LAN to be virtually regarded as a PC on the LAN and communicate with a terminal on the LAN. Ex. 1005, 1:16–24, 3:62–65. Specifically, Murakawa discloses allowing an outside terminal to communicate (via a WAN, a security gateway, and a LAN) with a terminal on the LAN. *Id.* at 1:11–24, 3:61–4:16.

Petitioner’s annotated version of Murakawa’s Figure 5, which illustrates a “prior art typical network system,” *id.* at 4:32–33, is shown below.



Murakawa’s Figure 5 above shows a “prior art typical network system” and is further annotated by Petitioner to add labels for a mobile terminal, security gateway, and other terminals. Pet. 28. According to Murakawa, Figure 5 “is a block diagram of a typical network system

including a WAN.” Ex. 1005, 1:51–53. As shown in Figure 5, the network system includes “PC 101 [(labeled by Petitioner as ‘Mobile Terminal’)], which is located outside . . . LAN [104 and] establish[es] a dialup connection to the provider, WAN 102, and security gateway 103 [(labeled by Petitioner as ‘Security Gateway’)] that connects WAN 102 and LAN 104.” *Id.* at 1:54–58. In addition, “LAN 104[,] being subjected to security gateway 103[,] includes . . . client PCs 106, 107” (labeled by Petitioner as “Other Terminals”). *Id.* at 1:59–60. Also shown is virtual private network (“VPN”) 108, which is established between PC 101 and security gateway 103 to perform IPSec communication. *Id.* at 1:61–63. Murakawa discloses that this network system ensures safe communications between PC 101 and the terminals on LAN 104. *Id.* at 2:1–4.

C. Our Analysis

Claims 4–6 depend directly from claim 3. Ex. 1001, 11:16–24. Claim 3 recites “[t]he method of claim 1 wherein the method further comprises the security gateway sending back *a reply message* to the mobile terminal at the second address to confirm the address change.” Ex. 1001, 11:11–14 (emphasis added). The Petition does not address claim 3’s reply message in its showings for claims 4–6. *See* Pet. 54–59, 66–69. Nor does the Petition allege that (i) the combination of Ishiyama and Murakawa, or (ii) the combination of Ishiyama, Murakawa, and Forslöw, renders claim 3 unpatentable. *Id.* at 4. Instead, the Petition challenges claim 3 based on another ground (Ishiyama, Murakawa, and Ahonen), and relies on Ahonen to teach claim 3’s reply message. *Id.* at 59–66. The Petition does not contend, however, that claims 4–6 are obvious over any combination that includes Ahonen. *Id.* at 4.

We already addressed the above scenario in IPR2021-00820, where Petitioner relied on Ahonen to teach the same limitation as recited in claim 3, but failed to include Ahonen in another ground challenging dependent claims that incorporated this limitation. -820 case, Paper 37 (Final Written Decision) at 49–55. We determined that Petitioner did not meet its burden to show unpatentability for this scenario. *Id.* The Federal Circuit upheld this determination from the -820 case:

[W]e agree the Board properly declined to consider Ahonen in Grounds 1 and 3 of the [-820] IPR. Apple only raised Ahonen in Ground 2, which challenged claims 3 and 5 of the '581 patent. Even though claims 6–8 depend from claim 5, Apple did not include Ahonen in Grounds 1 and 3 challenging those claims, nor did it address or reference Ahonen in its substantive analysis. The Board did not err by declining to consider arguments that Apple did not make.

Apple, 2022 WL 4103286, at *7 (citations omitted); *see also id.* at *8 (“We *affirm* the Board’s patentability determination that Apple failed to meet its burden as to claims 6–8 of the '581 patent.”).

In addition, the Federal Circuit noted that we “should decide whether to consider this issue on remand” for claims 4–6 in this case. *Id.* at *6–8 & *6 n.4; *see also id.* *6 n.4 (noting that “[t]he Board did not reach this issue because it found [Petitioner] did not demonstrate claim 1 to be unpatentable”) (citation omitted).

We now consider this issue as it is dispositive of whether Petitioner shows that claims 4–6 of the '810 patent are unpatentable. The parties’ arguments here are substantively the same as in the -820 case for this scenario. *Compare* Pet. 54–59, 66–69; Pet. Reply 22–25; PO Resp. 63–64, 73; *and* PO Sur-reply 24–25, *with* -820 case, Paper 2, 50–54; Paper 23, 63–64; Paper 26, 22–26; *and* Paper 29, 25–26. And our reasoning that

Petitioner does not show by a preponderance of the evidence that claims 4–6 would have been obvious is the same reasoning that we provided in the -820 case for this scenario. *Compare infra*, with -820 case, Paper 37, 49–55. We address the parties’ arguments below, mirroring how we did so for the -820 case.

We agree with Patent Owner that “Petitioner’s assertion that claims 4–5 are unpatentable under [Ishiyama and Murakawa] . . . fails because it does not account for the limitations of intervening claim 3.” PO Resp. 64 (citing Pet. 54–59). We likewise agree with Patent Owner that Petitioner’s Ishiyama, Murakawa, and Forslöw asserted ground “fails to address that claim 6 also depends on claim 3.” *Id.* at 73 (citing Pet. 66–69). Moreover, we disagree with Petitioner that Patent Owner makes a “form-over-substance argument” and “improperly tak[es] too stringent of a reading of the Petition.” Pet. Reply 22–23.

The Petition guides the proceeding. *See Koninklijke Philips N.V. v. Google LLC*, 948 F.3d 1330, 1335–36 (Fed. Cir. 2020). The Federal Circuit explained that “Congress chose to structure a process in which it’s the petitioner . . . who gets to define the contours of the proceeding,” and that “the statute envisions that a petitioner will seek an *inter partes* review of a particular kind—one guided by a petition describing ‘each claim challenged’ and ‘the grounds on which the challenge to each claim is based.’” *Id.* at 1335 (quoting *SAS Inst. Inc. v. Iancu*, 138 S. Ct. 1348, 1355 (2018) (quoting 35 U.S.C. § 312(a)(3))) (emphasis added). “Although the Board is not limited by the exact language of the petition, . . . the Board does not ‘enjoy[] a license to depart from the petition and institute a *different* *inter partes* review of his own design.’” *Id.* at 1336 (quoting *SAS*, 138 S. Ct. at 1356)

(citing *Sirona Dental Sys. GmbH v. Institut Straumann AG*, 892 F.3d 1349, 1356 (Fed. Cir. 2018)).

Here, the Petition alleges that claims 4 and 5 are obvious in view of Ishiyama and Murakawa, and claim 6 is obvious in view of Ishiyama, Murakawa, and Forslöw. Pet. 4, 54–59, 66–69. In other words, these combinations are “the grounds on which the challenge to [these] . . . claim[s] is based.” *Koninklijke Philips*, 948 F.3d at 1335. In view of how the Petition is worded and the analysis provided for claims 4–6, we do not consider one of the challenged grounds to be whether claims 4 and 5 would have been obvious in view of Ishiyama, Murakawa, *and Ahonen*, and likewise Ishiyama, Murakawa, Forslöw, *and Ahonen* for claim 6.

We are not persuaded by Petitioner’s argument that “*inter partes* reviews are notice based proceedings,” and that Patent Owner “had notice of [Petitioner’s] arguments since the beginning of this proceeding.” Pet. Reply 25 (citing *Sirona Dental*, 892 F.3d at 1356; Pet. 54–59, 66–69). Nor are we persuaded by Petitioner’s argument that if Patent Owner “believe[s] there is a deficiency in the art relating to the limitations of claims 4–6 . . . , [Patent Owner] ha[d] sufficient opportunity to address any purported deficiencies in its sur-reply.” *Id.* (citing *Sirona Dental*, 892 F.3d at 1356). Again, it is the Petition that guides the proceeding. *See Koninklijke Philips*, 948 F.3d at 1335–36. Furthermore, any statements in the Decision on Institution regarding the sufficiency of Petitioner’s showings for claims 4–6 were preliminary. *See Trivascular, Inc. v. Samuels*, 812 F.3d 1056, 1068 (Fed. Cir. 2016) (“At th[e Institution] point, the Board is considering the matter preliminarily without the benefit of a full record. The Board is free to change its view of the merits after further development of the record”).

Upon a review of the full record, and in light of *Koninklijke Philips*, we find that Petitioner’s showings for claims 4–6 are insufficient for the reasons we provide herein.

We also are not persuaded by Petitioner’s argument that “Ahonen is not needed to show the unpatentability of the limitations recited in claims 4–6 because claims 4–6 do not further limit the elements recited in claim 3, and instead only limit elements that appear in claim 1.” Pet. Reply 23. Rather, “[c]laims in dependent form shall be construed to include all the limitations of the claim incorporated by reference into the dependent claim.” 37 C.F.R. § 1.75(c). In other words, claims 4–6 include claim 3’s requirements regarding the reply message. *Id.* The Petition fails to account for the claimed reply message in its analysis of claims 4–6, and thus, does not demonstrate their unpatentability. Pet. 54–59, 66–69.

We also are not persuaded that the Petition presents, “as an alternative theory, [that claims 4–6] are unpatentable over the combination of Ishiyama and Murakawa due to the well-known ‘ACK’ functionality used in the TCP/IP protocol taught by Ishiyama.” Pet. Reply 22 (citing Pet. 60; Ex. 1020 ¶¶ 63–65). Rather, the Petition provides that “in the TCP/IP protocol, destination computers receiving data packets are required to transmit positive acknowledgments (ACK) to source computers to provide a reliable and secure IP connection.” Pet. 60. More specifically, Petitioner argues that “[t]he TCP must recover from data that is damaged, lost, duplicated, or delivered out of order by the internet communication system[, and that t]his is achieved by assigning a sequence number to each octet transmitted, and requiring a positive acknowledgment (ACK) from the receiving TCP.” *Id.* at n.10 (quoting Ex. 1012, 4; citing Ex. 1002 ¶ 113).

This argument—which appears in a separate ground (Ishiyama, Murakawa, and Ahonen)—fails to show that Ishiyama teaches an ACK that is sent to a mobile terminal’s second address to confirm an address change, as required by claim 3. Nor does Petitioner tether this argument to any specific portions of Ishiyama or Murakawa. Pet. 60. To the contrary, Petitioner admits that “Ishiyama and Murakawa . . . do not explicitly describe this reply message.” *Id.* Petitioner further admits that “after an address update request message has been sent from a mobile terminal, Ishiyama and Murakawa do not describe how a mobile terminal would be informed that the address was successfully updated before initiating communications from the new address.” *Id.* at 60–61 (citing Ex. 1002 ¶ 116). Petitioner’s analysis of claim 3 under this ground addresses what Ahonen adds to the combination of Ishiyama and Murakawa. *Id.* at 61–66. Petitioner does not assert that claim 3 is obvious over Ishiyama, Murakawa, and the knowledge of ACK functionality in the TCP/IP protocol. *Id.* at 4 (summarizing ground as obviousness over Ishiyama, Murakawa, and Ahonen), 60–66 (analyzing ground as including Ahonen).

Nevertheless, even if we consider the Petition to include an assertion that claim 3 is unpatentable as obvious over Ishiyama and Murakawa (without adding Ahonen), we are not persuaded that Petitioner made such a showing. Specifically, we are not persuaded by Petitioner’s argument that in light of the TCP’s ACK that “the reply message as recited in claim[] . . . 3 was obvious as a concept in the prior art and would have been obvious in view of Ishiyama and Murakawa.” *Id.* at 60; *see also* Ex. 1002 ¶ 115. Although “[a] person of ordinary skill in the art is also a person of ordinary creativity, not an automaton,” *KSR*, 550 U.S. at 421, there may be limits in a

particular case as to how much gap-filling may be based on such creativity. *See Arendi S.A.R.L. v. Apple Inc.*, 832 F.3d 1355, 1361–63 (Fed. Cir. 2016); *DSS Tech. Mgmt., Inc. v. Apple Inc.*, 885 F.3d 1367, 1374–75 (Fed. Cir. 2018) (reliance on ordinary creativity to supply a missing limitation requires the same “searching” inquiry as reliance on common sense). We find that Petitioner does not provide persuasive evidence that one of ordinary skill in the art would have found it obvious to send a reply message to a mobile terminal’s second address to confirm an address change in view of TCP’s ACK.

We do not find persuasive Dr. Goldschlag’s declaration testimony that claim 3’s reply message “would be an obvious concept to confirm the successful updating of the address at the security gateway,” and that “in view of the well-known TCP/IP protocol, . . . [one of ordinary skill in the art] would have understood that a reply message would be an obvious implementation detail in view of Ishiyama and Murakawa.” Ex. 1002 ¶ 115. Dr. Goldschlag’s discussion of TCP using ACKs to address data that is damaged, lost, duplicated, or delivered out of order does not provide sufficient factual corroboration for these opinions concerning using ACKs in the context of address updating. Ex. 1002 ¶ 113 (citing Ex. 1012, 4); *see also In re Am. Acad. of Sci. Tech Ctr.*, 367 F.3d 1359, 1368 (Fed. Cir. 2004) (“[T]he Board is entitled to weigh the declarations and conclude that the lack of factual corroboration warrants discounting the opinions expressed in the declarations.”); 37 C.F.R. § 42.65(a). Dr. Goldschlag also opines that “a mobile terminal that moves to a new address would expect to receive an acknowledgment or confirmation message before transmitting packets from its new address,” and that “[a] mobile terminal would likely not blindly

transmit data packets from its new address without first receiving confirmation that the security gateway is ready to accept data packets from the new address.” Ex. 1002 ¶ 113. We likewise do not find this testimony persuasive, as it too lacks sufficient factual corroboration, and is contrary to the ’810 patent’s teaching that a reply message is “optional.” *See* Ex. 1001, 10:2–4, 10:9.

We also disagree with Petitioner that Patent Owner’s Response “explicitly recognized” Petitioner’s “alternative theory” that claim 3 was obvious “due to the well-known ‘ACK’ functionality used in the TCP/IP protocol taught by Ishiyama.” Pet. Reply 22. Rather, the alternative theory Patent Owner responds to is based on Ishiyama’s “message (7) from the correspondent host to the mobile terminal in Ishiyama’s Figure 7.” PO Resp. 72 (citing Pet. 64–66; Ex. 1004, Fig. 7). For this theory, Petitioner argues that in operation 7 “the destination of the message is ‘CoA2’ and confirms the updated address of the mobile computer.” Pet. 65 (citing Ex. 1004, 12:66–13:5). Petitioner argues that “[u]sing CoA2, the correspondent host 3 may originate communications sent to the mobile computer 2 at the updated Care-of address.” *Id.* (citing Ex. 1004, 13:6–9). We are not persuaded by Petitioner’s arguments. Rather, we agree with Patent Owner and find that “the message in step (7) is simply an encapsulated message using the new care-of address CoA2 in the outer packet[, and] . . . is not a [confirmatory] reply to a request for an address change from the mobile terminal.” PO Resp. 72; *see also* Ex. 1004, Fig. 7, 12:66–13:5. Moreover, Ishiyama does not teach that operation 7’s message is recognized as a confirmation of the address change. Ex. 1004, Fig. 7, 12:66–13:9. Instead, Ishiyama simply sends and receives messages at the

second address (e.g., correspondent host sends a secure message to the mobile computer). *Id.* at Fig. 7, 12:66–13:5; *see also id.* at 13:3–5 (“Consequently the session is guaranteed even when the mobile computer 2 moves (the operations (6) and (7) of FIG. 7).”).

Lastly, we find unpersuasive Petitioner’s argument from its post-remand briefing that “[the] disclaimer is a strong clue that a patent examiner and, by concession, the applicant, thought the claims in the continuation lacked a patentable distinction over the parent.” Pet. Rem. Open. 4 (citing *SimpleAir, Inc. v. Google LLC*, 884 F.3d 1160, 1168 (Fed. Cir. 2018)); Pet. Rem. Resp. 5–6 (same). In particular, we find this argument unpersuasive because *SimpleAir* addressed a terminal disclaimer, rather than a statutory disclaimer. 884 F.3d at 1167–68. Moreover, this argument is inapposite as to what Petitioner alleged in the Petition for these claims.

Accordingly, Petitioner has not demonstrated by a preponderance of the evidence that claims 4–6 would have been obvious.

VI. CONCLUSION

Based on the full record before us, we determine that Petitioner has not demonstrated by a preponderance of the evidence that claims 4–6 of the ’810 patent are unpatentable.

Claim(s)	35 U.S.C §	Reference(s)/Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
4, 5	103(a)	Ishiyama, Murakawa		4, 5
6	103(a)	Ishiyama, Murakawa, Forsl�w		6

Overall Outcome				4–6
----------------------------	--	--	--	-----

VII. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, pursuant to 35 U.S.C. § 314(a), Petitioner has not shown by a preponderance of the evidence that claims 4–6 of the '810 patent are unpatentable; and

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

IPR2019-00819
Patent 7,620,810 B2

PETITIONER:

David W. O'Brien
Andrew S. Ehmke
HAYNES AND BOONE, LLP
david.obrien.ipr@haynesboone.com
andy.ehmke.ipr@haynesboone.com

PATENT OWNER:

James T. Carmichael
Stephen Schreiner
CARMICHAEL IP LAW, PLLC
jim@carmichaelip.com
schreiner@carmichaelip.com

Christopher J. Lee
Richard B. Megley
Brian E. Haan
Ashley E. LaValley
LEE SHEIKH MEGLEY & HAAN LLC
clee@leesheikh.com
rmegley@leesheikh.com
bhaan@leesheikh.com
alavalley@leesheikh.com

Kenneth J. Weatherwax
Patrick Maloney
Jason C. Linger
LOWENSTEIN & WEATHERWAX LLP
weatherwax@lowensteinweatherwax.com
maloney@lowensteinweatherwax.com
linger@lowensteinweatherwax.com