

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

HEWLETT PACKARD ENTERPRISE COMPANY,
Petitioner,

v.

SOVEREIGN PEAK VENTURES, LLC,
Patent Owner.

U.S. Patent 8,270,384 B2
Issue Date: September 18, 2012

Title: WIRELESS POINT THAT PROVIDES FUNCTIONS FOR A WIRELESS
LOCAL AREA NETWORK TO BE SEPARATED BETWEEN THE WIRELESS
POINT AND ONE OR MORE CONTROL NODES, AND METHOD FOR
PROVIDING SERVICE IN A WIRELESS LOCAL AREA NETWORK HAVING
FUNCTIONS SEPARATED BETWEEN A WIRELESS POINT AND ONE OR
MORE CONTROL NODES

Inter Partes Review No.: IPR2023-01262

**PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT 8,270,384
UNDER 35 U.S.C. §§311-319 and 37 C.F.R. §§42.1-.80, 42.100-.107**

Mail Stop “PATENT BOARD”
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450

TABLE OF CONTENTS

	Page
I. Introduction.....	1
II. Grounds for Standing.....	2
III. Reasons for the Requested Relief.....	2
A. Summary of the '384 Patent.....	3
B. Prosecution History	6
C. Claim Construction	7
D. Priority of the Challenged Claims.....	8
E. Person of Ordinary Skill in the Art	8
F. State of the Art	9
1. 802.11	9
2. Centralized Management of WLANs	10
3. CAPWAP.....	11
4. LWAPP	13
IV. Identification of Challenges.....	13
A. Challenged Claims	13
B. Statutory Grounds for Challenges.....	13
C. Prior Art Basis	14
V. Identification of How the Challenged Claims are Unpatentable.....	15
A. Ground 1: Claims 1-6 are Anticipated by Calhoun.....	15
1. Calhoun (EX-1005).....	15
2. Detailed Application to the Challenged Claims	16

B.	Ground II: Claims 1-6 are Obvious over Calhoun/CAPWAP/LWAPP in view of a POSA's Skill and Knowledge.....	37
1.	CAPWAP	37
2.	LWAPP	38
3.	Motivation to Combine Calhoun with CAPWAP and LWAPP	38
4.	Detailed Application to the Challenged Claims	41
VI.	The Board Should Not Exercise its Discretion to Deny Institution	62
A.	The Board Should Not Deny Institution Under <i>Fintiv</i>	62
B.	This Petition Presents Arguments Not Before the Examiner.....	65
VII.	Mandatory Notices under 37 C.F.R. §42.8.....	67
A.	Real Parties-In-Interest Under 37 C.F.R. § 42.8(b)(1).....	67
B.	Related Matters Under 37 C.F.R. § 42.8(b)(2)	67
C.	Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)	68
D.	Service Information Under 37 C.F.R. § 42.8(b)(4).....	68
VIII.	Conclusion	69

TABLE OF AUTHORITIES

Federal Cases

<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005)	7
<i>Sovereign Peak Ventures, LLC v. Hewlett Packard Enterprise Co.</i> , 2:23-cv-00009 (E.D. Tex.)	67

Regulatory Cases

<i>Advanced Bionics, LLC v. MED-L Elektromedizinische Geräte GmbH</i> , IPR2019- 01469, Paper 6 (Feb. 13, 2020).....	65-66
<i>HP Inc. v. Slingshot Printing LLC</i> , IPR2020-01084, Paper 13 (Jan. 14, 2021)	64
<i>PEAG LLC v. Varta Microbattery GMBH</i> , IPR2020-01214, Paper 8 (Jan. 6, 2021)	63
<i>Puma N. Am., Inc. v. Nike, Inc.</i> , IPR2019-01058, Paper 10, 19 (Oct. 31, 2019).....	67
<i>Sand Revolution II LLC v. Continental Intermodal Group – Trucking LLC</i> , IPR2019-01393, Paper 24 (June 16, 2020).....	63-64
<i>Sotera Wireless, Inc. v. Masimo Corp.</i> , IPR2020-01019, Paper 12 (Dec. 1, 2020).....	63

Federal Statutes

35 U.S.C. §103	1, 14
35 U.S.C. §112, ¶6	<i>Passim</i>

Regulations

37 C.F.R. §42.8	67
37 C.F.R. §42.8(b)(1).....	67
37 C.F.R. §42.8(b)(2).....	67
37 C.F.R. §42.8(b)(3).....	68
37 C.F.R. §42.8(b)(4).....	68
37 C.F.R. §42.104(a).....	2
37 C.F.R. §42.106(a).....	2
37 C.F.R. §42.108	2

PETITIONER’S EXHIBIT LIST

<i>Exhibit #</i>	<i>Description</i>
1001	U.S. Patent 8,270,384 (“’384 Patent”)
1002	Prosecution History of the ’384 Patent
1003	U.S. Patent No. 8,045,531 (“’531 Patent”)
1004	Prosecution History of the ’531 Patent
1005	U.S. Patent No. 7,508,801 to Calhoun et al (“Calhoun”)
1006	Light Weight Access Point Protocol (LWAPP), P. Calhoun, et al., Internet Engineering Task Force (IETF) of the Internet Society, June 28, 2003 (“LWAPP”)
1007	P. Calhoun and J. Aaron, “LWAPP brings harmony to WLANs,” Network World, December 1, 2003, available at: https://www.networkworld.com/article/2328757/lwapp-brings-harmony-to-wlans.html (last accessed July 31, 2023)
1008	Control and Provisioning of Wireless Access Points (CAPWAP), Internet Engineering Task Force (IETF) of the Internet Society, October 2, 2003 (“CAPWAP”)
1009	IEEE 802.11-1999
1010	[Omitted]
1011	RFC 5412, <i>Lightweight Access Point Protocol</i> , P. Calhoun et al, (February 2010)
1012	Declaration of Dr. Kevin Negus
1013	Plaintiff’s Preliminary Infringement Contentions, <i>Sovereign Peak Ventures, LLC v. Hewlett Packard Enterprise Company</i> , Case No. 2:23-cv-00009 (E.D. Tex.), served on Feb. 28, 2023
1014	Amended Docket Control Order, <i>Sovereign Peak Ventures, LLC v. Hewlett Packard Enterprise Company</i> , Case No. 2:23-cv-00009 (E.D. Tex.), filed on April 13, 2023
1015	Expert Declaration of Dr. Sylvia Hall-Ellis with respect to <i>Inter Partes</i> Review
1016	Declaration of Alexa Morris

I. INTRODUCTION

Hewlett Packard Enterprise Company (“Petitioner”) hereby petitions for *Inter Partes* Review (“IPR”) of U.S. Patent No. 8,270,384 (“’384 Patent”) (EX-1001). Petitioner respectfully submits that Claims 1-6 (“Challenged Claims”) of the ’384 Patent are unpatentable under 35 U.S.C. §103 in view of the prior art discussed herein. The Challenged Claims are directed to apparatus and methods for separating between control nodes (“CNs”) and wireless access points (“WAPs”) the functions to be performed by a wireless local area network (“WLAN”). During prosecution, the applicant argued that the alleged novelty over the prior art identified by the examiner was the CNs sending information about their functions to the AP in the form of “discovery response messages including information of functions offered by the associated control node of said one or more control nodes.” This allegedly distinguishing feature, however, was well known in the prior art. In fact, one such prior art reference, U.S. Patent No. 7,508,801 (“Calhoun”) that was directed to lightweight APs to be used with CNs and a WLAN, anticipated this and every other limitation of the Challenged Claims. Likewise, the named inventors of Calhoun contributed to contemporaneous papers and standard setting submissions that added further detail to the elements of Calhoun and that render the Challenged Claims obvious. Accordingly, this Petition, which relies on Calhoun and the related non-patent literature, demonstrates by a preponderance of the evidence that there is a

reasonable likelihood that Petitioner will prevail with respect to at least one of these claims and it is respectfully requested that the Board institute an IPR, pursuant to 37 C.F.R. §42.108.

II. GROUNDS FOR STANDING

Petitioner certifies that the '384 Patent is available for IPR and Petitioner is not barred or estopped from requesting this review. 37 C.F.R. §42.104(a). This Petition has been filed less than one year after the date on which the Petitioner or a privy of the Petitioner was served with a Complaint alleging infringement of '384 Patent. This Petition is filed under 37 C.F.R. §42.106(a).

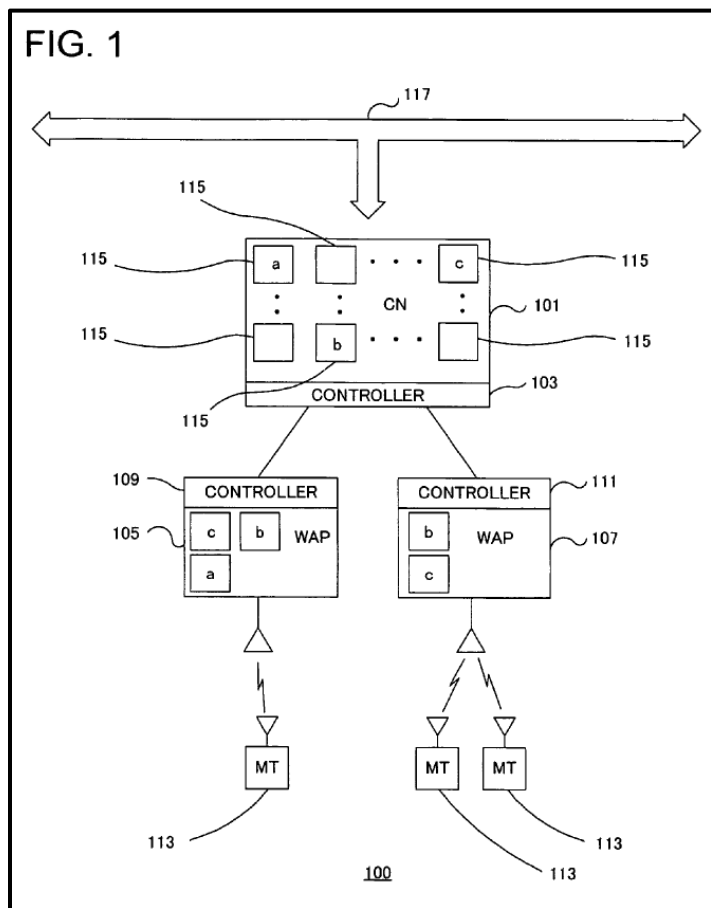
III. REASONS FOR THE REQUESTED RELIEF

As explained in this Petition and the Declaration of Petitioner's Expert, Dr. Kevin Negus (EX-1012), the apparatus and methods claimed in the '384 Patent were anticipated and obvious in view of the prior art to a person of ordinary skill in the art ("POSA") at the time of the invention.

A. Summary of the '384 Patent

The '384 Patent relates to the field of “split architecture” WLANs in which the various functions of the network are divided between one or more central CNs and several WAPs. EX-1001, 1:20-25, 1:38-41. In split architecture systems, certain “control aspects” of the WLAN are centralized in CNs while WAPs perform other aspects of the WLAN. The '384 Patent illustrates this split architecture in

Figure 1, which depicts a CN connected to two WAPs. The '384 Patent acknowledges that, as of its filing, “many WLAN equipment manufacturers” had introduced split architecture systems and that “[t]here are currently some efforts to provide standardized means” for managing them, such as by the Control and Provisioning of Wireless Access Points working



group operating under the umbrella of the Internet Engineering Task Force (“IETF”). EX-1001, 1:36-53.

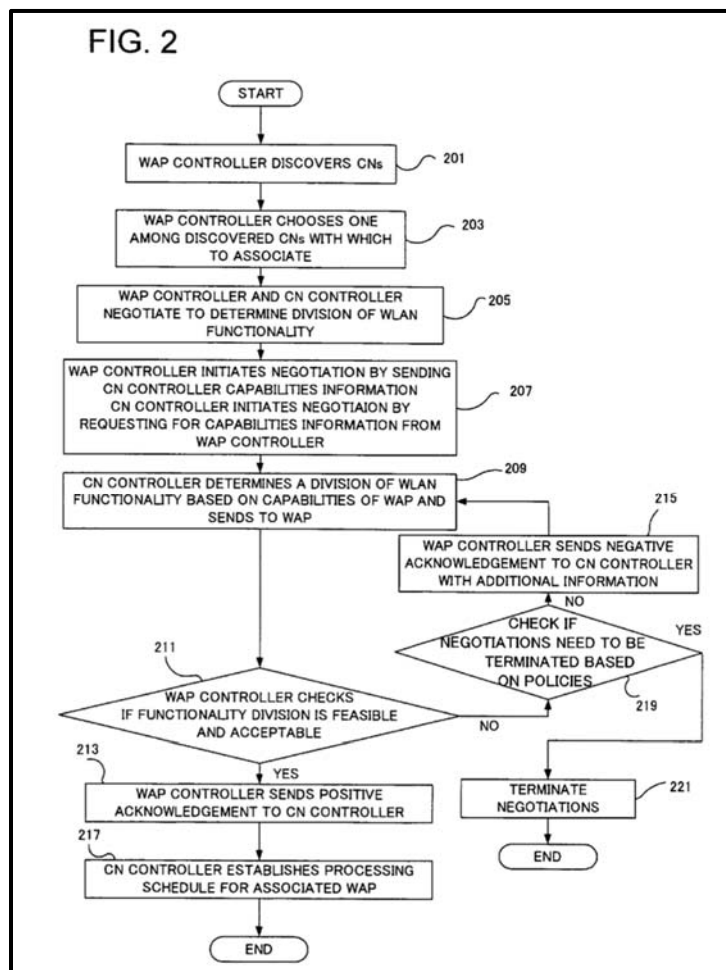
According to the '384 Patent, earlier efforts did “not consider the problems of accommodating WAPs with dissimilar functional capabilities within a single WLAN.” EX-1001, 1:50-53. The purported result is “WLAN entities from various vendors are incapable of interoperation in a single WLAN and are also incapable of operation in a dynamic topology WLAN.” EX-1001, 2:13-16. Accordingly, the '384 Patent purports to provide an apparatus/method “for negotiations between controlling nodes (CNs) and wireless access points (WAPs) of a WLAN based on policies that allow for accommodating static and dynamic differences among the WLAN entities” and to “provide a method and policy for negotiations between WLAN entities for the purpose of determining selected subsets of functional, load, or other components to be processed by each of said WLAN entities so as to accommodate variations in system design, processing load or network topology.” EX-1001, 3:30-41.

The '384 Patent explains its purported invention by reference to the traditional split architecture system displayed in Fig. 1 (shown above). The different “functional components” of each “WLAN entity” (*e.g.*, the CN and WAPs) are represented by “functional component codes” ('a,' 'b,' and 'c'). EX-1001, 7:21-35. These functional codes are “logical[] represent[at]ions[]” of “functional components” of the WLAN, and “may include encryption, decryption, medium access control protocol data unit (MAC PDU) processing, authentication, association, [...], etc.”

EX-1001, 7:26-31. Figure 1, depicting a WAP with a subset of the functional components of a second WAP, demonstrates that because the “WAPs may be from different manufacturers or of different implementations, they may incorporate among them varying degrees of WLAN functional components.” EX-1001, 7:53-65.

The '384 Patent purports to solve the problem of WAPs with different functional capabilities by offering methods for dividing functions between WAPs and CNs. EX-1001, 5:48-51, 9:16-24. The '384 Patent describes these negotiations with reference to Figure 2, which reflects three “phases” of interaction between the

WAPs and the CNs. First, in the “discovery” phase, a WAP discovers an available CN. EX-1001, 8:64-67. Second, in the “association phase” the WAP associates with a chosen CN in a process that “may include mutual authentication, exchanges of security information and the establishment of communication protocols for further exchanges.”



EX-1001, 9:14-16. Third, in the “negotiation phase” the CN obtains information about the “functional capabilities” of the associated WAP and “determines an initial division of WLAN functionality” between the CN and the WAP. EX-1001, 9:20-24. According to the ’384 Patent, the CN can obtain information about a WAP’s functional capabilities by the WAP sending a message containing capability information or by the CN “infer[ring]” the capabilities based on the WAP’s ability to process a data unit sent by the CN. EX-1001, 11:41-44.

B. Prosecution History

Application No. 13/235,912, which became the ’384 Patent, was filed on September 19, 2011, and claimed priority to Application No. 10/591,184 (now U.S. Patent No. 8,045,531, EX-1003). EX-1002, 7. The Examiner rejected the claims over Architecture for Control and Provisioning of Wireless Access Points (CAPWAP) (“O’Hara”), published February 8, 2004. EX-1002, pp. 243-247. The Applicant argued in response that O’Hara does not disclose that the discovered CNs called access routers or “ARs” send information about their functions to the AP during the AR discovery and thus does not disclose “discovery response messages including information of functions offered by the associated control node of said one or more control nodes.” EX-1002, pp.260-267. After an Examiner interview, the Applicant rewrote claim 1 to incorporate the additional limitation of dependent claim 2, “a negotiation unit configured to exchange information about the functions to be

separated between said selected one control node and said wireless point.” EX-1002, pp. 272-276, 281. The claims issued.

C. Claim Construction

For this IPR, Petitioner proposes that each claim term of the Challenged Claims be given “their ordinary and customary meaning” as understood by a POSA at the time of the claimed invention. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312, 1327 (Fed. Cir. 2005). Petitioner contends that no specific construction of any claim term is required because the prior art relied on in this Petition meets each of the claim terms under any reasonable construction. EX-1012 ¶103. However, if the Patent Owner (“PO”) argues and the Board determines that certain limitations should be construed as means-plus-function limitations subject to 35 U.S.C. §112, ¶6, Petitioner proposes that the Board adopt the below structures for these limitations:

<u>Limitation</u>	<u>Function</u>	<u>Structure</u>
“discovery unit configured to [send]”	“send a discovery request message to said one or more control nodes”	Step 201 in Figure 2 and the applicable text in 8:59-67 of the ’384 Patent
“a selecting unit configured to [select]”	“select one control node of said one or more control nodes based on one or more discovery response messages sent to said wireless point from said one or more control nodes in response to said discovery request message,”	Step 203 in Figure 2 and the applicable text in 9:1-11 of the ’384 Patent

<u>Limitation</u>	<u>Function</u>	<u>Structure</u>
“session establishing unit configured to [establish]”	“establish a secure session with said selected one control node”	Step 203 in Figure 2 and the applicable text in 9:11-16 of the '384 Patent
“negotiation unit configured to [exchange]”	“exchange information about the functions to be separated between said selected one control node and said wireless point”	Steps 205, 207, 209, 211, 213, 215, 219, and 221 in Figure 2 and the applicable text in 9:17-11:3 of the '384 Patent

For these terms, Petitioner has identified the closest disclosed structure in the '384 Patent that relates to the recited function, but by doing so, Petitioner does not intend to, and does not, waive any argument that the structure for performing the claimed function of each term is not sufficiently disclosed in the '384 Patent.

D. Priority of the Challenged Claims

The '384 Patent was filed September 19, 2011. EX-1001, (22). In related District Court litigation, PO has asserted that the '384 Patent is entitled to a priority date of at least as early as March 2, 2004. For purposes of this Petition, Petitioner relies on prior art as of the March 2, 2004, priority date alleged by the PO.

E. Person of Ordinary Skill in the Art

A POSA pertinent to the '384 Patent would have had at least a Bachelor's degree in Electrical Engineering or a related field and at least two years of professional experience in wireless communications. Ex-1012, ¶25. Alternatively, a POSA would have had a more advanced degree, such as a Master's degree in

Electrical Engineering or an equivalent field, combined with at least one year of work experience in wireless communication. *Id.*

A POSA would also have been familiar with wireless communications network and equipment, and would have had a working knowledge of the applicable standards-based protocols and architectures for common wireless networks at the time and an understanding of the components and subsystems within available wireless communication equipment. Ex-1012, ¶24. The level of skill in the art is further demonstrated by the references cited herein, including the asserted art and the background references discussed in §IV.F below. Regardless of tense used, Petitioner’s analysis is from the perspective of a POSA as of the time of the purported invention.

F. State of the Art

This section describes the state of the art, including general knowledge, skill, common sense, and creativity possessed by a POSA as of March, 2004. It explains the conventional purposes, methods, and components in the art, informing the motivations and reasonable expectations of success.

1. 802.11

The IEEE 802.11 WLAN standard (“802.11-1999”) was published in August, 1999. EX-1009, p.iii; EX-1008, p.7. 802.11-1999 describes “a medium access control and a physical layer specification for wireless connectivity for fixed,

portable, and moving stations within a local area.” EX-1009, §§1.1, 1.2. The main addressable unit in 802.11 is a “station” or “STA,” and 802.11 also describes the functionality of a specific device, called an “access point” or “AP.” EX-1009, §§5.2.1.1, 5.2.2; EX-1008, p.7. Each STA “associates” with only one AP at a time. EX-1009, §5.4.2.2. Multiple APs may be connected together to make an “extended service set” known as a WLAN. EX-1008, pp.7-8.

2. Centralized Management of WLANs

Traditional WLANs functioned on a “stand-alone basis” using “fat” APs, which contained “all wireless processing capabilities.” EX-1007. By 2003, “centralized security and management of [WLANs] was a rapidly growing trend.” EX-1007. One purported problem with the fat AP architecture was that it would not let “different vendors’ equipment interoperate.” *Id.* This led to the development of “lightweight” APs that used “a WLAN device such as a switch, appliance, or router . . . to create and enforce policies across many streamlined, or lightweight” APs. *Id.* An advantage of having lightweight APs paired with dedicated appliances (called “access controllers” or “AP controllers”) was that it simplified the hardware in light APs, and turned the APs into “essentially remote radio frequency interfaces that no longer house all the mandatory wireless remote processing capabilities and are controlled by the access controller.” *Id.*

The IETF proposed a new working group to create a new WLAN architecture, with this working group called “Control and Provisioning of Wireless Access Points” (“CAPWAP-WG”). *Id.*; EX-1008, p.1. In 2003, CAPWAP-WG was considering a draft standard called “Lightweight Access Point Protocol (LWAPP),” which was proposed to “provide consistent behavior across WLAN devices, ensure multi-vendor WLAN compatibility, protect WLAN hardware investments, [] create a foundation for delivering advanced WLAN functionality in enterprise environments[,] simplify WLAN deployment and management, and build large-scale wireless networks.” EX-1007.

3. CAPWAP

CAPWAP was created because there was “overwhelming support in the market for a new WLAN architecture.” EX-1008, p.9. CAPWAP’s architecture, “moves much of the functions that would reside in a traditional [AP] to a centralized access router (AR).” *Id.* CAPWAP’s architecture, also called “Split AP,” put “real-time components of the 802.11 protocol in the [AP], while access control components of the 802.11 protocol terminate in the [AR].” *Id.*, pp.9-10.

A benefit of CAPWAP’s architecture included “ease of use” because a WLAN was “centrally manag[ed]” as a system instead of a series of discrete components, making “management and control of the WLAN easier.” *Id.*, p.9. Terminating management messages in the AR also provided for enhanced mobility without

needed special client software. *Id.* Further, having a centralized AR manage RF links enabled “efficient load balancing” across multiple APs making the wireless network more efficient. *Id.*, pp.9-10. CAPWAP explicitly references using the “LWAPP protocol” with the CAPWAP architecture. *Id.*, p.10.

CAPWAP discloses four possible network topologies where APs and ARs are linked: (1) “ARCH0,” where a “classic AP” has “a self-contained controller” and communicates with other APs; (2) “ARCH1,” where APs “defer all WLAN functions other than real-time services” that creates a “vertical (real-time frontend AP and aggregated backend AC) functional distribution”; (3) “ARCH3,” where APs “shift some normally real-time functions as well to the backend,” with benefits such as extending “over-the-air[] protection”; and (4) “ARCH4,” where the AR becomes a “single ‘AP-switch’” and treats all connected APs as smart antennae. *Id.*, p.10. Figure 1 shows the “basic outline of communications architecture between AP & [AR].” *Id.*, p.12.

CAPWAP further explains that the services that “MUST” be in a lightweight AP are “those that are directly related to the real-time aspects of the 802.11 MAC and those related to the radio nature of an 802.11 AP.” Conversely, functions that may be moved to an AR are “those dealing with the management and control aspects of an 802.11 AP.” *Id.*, pp.14-15.

4. LWAPP

LWAPP is “a protocol allowing a router or switch to interoperably control and manage a collection of wireless [APs].” EX-1006, p.2. LWAPP’s “goal is to provide consistent behavior across WLAN devices, ensure multivendor WLAN interoperability, protect WLAN hardware investments, and create a foundation for delivering advanced WLAN functionality in enterprise environments.” EX-1007. Further, LWAPP governs how APs and ARs communicate with each other, and defines activities including “access point device discovery and authentication,” “access point information exchange, configuration[,] and software control,” and “communications control and management between access point and wireless system devices.” *Id.* LWAPP centralizes “traffic handling, authentication, encryption[,] and policy enforcement (quality of service and security) capabilities within the access controller, improving the effectiveness of WLAN management.” *Id.*

IV. IDENTIFICATION OF CHALLENGES

A. Challenged Claims

Claims 1-6 of the '384 Patent are challenged in this Petition.

B. Statutory Grounds for Challenges

The Challenges are set forth in detail below and summarized as follows:

Ground	Claim(s)	Basis	Reference
1	1-6	§102	Calhoun
2	1-6	§103	Calhoun/CAPWAP/LWAPP (referred to as “Calhoun/CAPWAP/LWAPP”) in view of a POSA’s knowledge

C. Prior Art Basis

U.S. Patent No. 7,508,801 (“Calhoun”) titled “Light-weight Access Point Protocol” was filed on March 21, 2003 and issued March 24, 2009. EX-1005, (10), (22), (45), (54), (75). Calhoun is prior art to the ’384 Patent under at least §102(e).

Light Weight Access Point Protocol (LWAPP) by P. Calhoun, B. O’Hara, S. Kelly, and R. Suri (“LWAPP”) was published as a draft by the Internet Engineering Task Force (IETF) of the Internet Society on June 28, 2003. Ex-1006, 1. LWAPP is publicly available at: <https://datatracker.ietf.org/doc/pdf/draft-calhoun-seamoby-lwapp-03>, and was publicly accessible to a member of the interested public as of at least July 3, 2003. EX-1016, ¶¶1-10. LWAPP is prior art to the ’384 Patent under at least §102(a)-(b).

Architecture for Control and Provisioning of Wireless Access Points (CAPWAP) (“CAPWAP”) was published by the IETF on October 2, 2003. EX-1008, 1. CAPWAP is publicly available at: <https://datatracker.ietf.org/doc/pdf/draft-mani-capwap-arch-00>, and was publicly accessible to members of the interested public as of October 22, 2003. EX-1016, ¶¶1-9, 11. CAPWAP is prior art to the ’384 Patent under at least §102(a)-(b).

V. IDENTIFICATION OF HOW THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Ground 1: Claims 1-6 are Anticipated by Calhoun

1. Calhoun (EX-1005)

a. Analogous Art

Calhoun relates to methods and systems for “facilitating the deployment and configuration of managed access points in a wireless network system” including system architectures in which “a central control element manages and controls one [or] more access elements.” EX-1005, 1:17-20, 2:1-10. EX-1012, ¶122. Calhoun is analogous art, is in the same field of endeavor, and is reasonably pertinent to the problem addressed by the ’384 Patent because Calhoun’s solution includes “a central control element” that “provides processing to dynamically configure a wireless Local Area Network,” including “functionality directed to initialization and configuration of managed access elements.” EX-1005, 3:46-49, 4:31-37; EX-1012, ¶122.

b. Overview of Calhoun

Calhoun explains that “known WLAN solutions use distributed access points to act as bridges between the wired infrastructure and the wireless clients.” *Id.*, 1:45-47. This “distributed architecture create[d] many problems affecting network management, mobility, and performance” because APs “act in their own self-interest and are not aware of the actions taken by surrounding access points” and

APs handle mobility “as a local event, which significantly increases latency.” *Id.*, 1:58-67.

Calhoun discloses a “system architecture” where a “central control element manages and controls one or more access elements,” so that the “access elements perform real-time communication functions,” while the “central control element manages the connection between the access element and one or more wireless client devices.” *Id.*, 2:1-10. Calhoun further discloses “systems facilitating deployment and configuration of managed access points in wireless network systems,” including “light-weight management protocols that reduce the management footprint” of managed APs. *Id.*, 2:24-39.

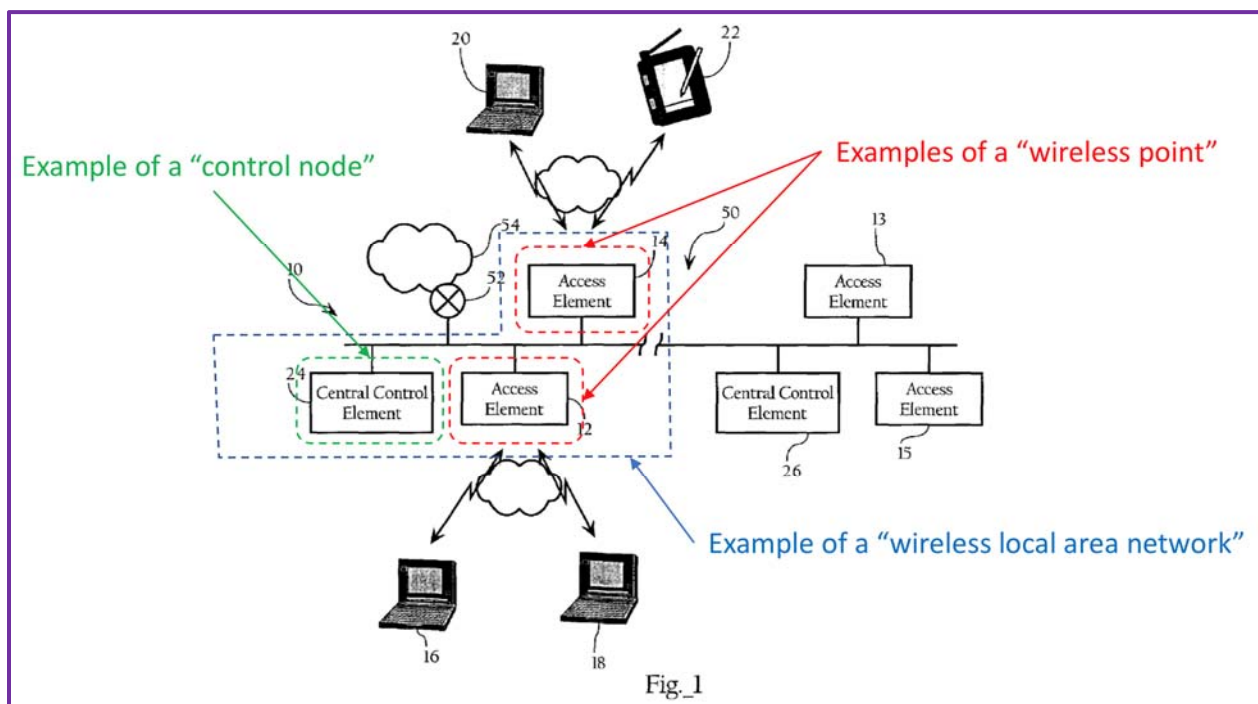
2. Detailed Application to the Challenged Claims

a. Claim 1

[1pre] A wireless point that provides for functions for a wireless local area network to be separated between said wireless point and one or more control nodes, said wireless point comprising:

If the preamble is limiting, Calhoun discloses it explicitly or inherently. Calhoun discloses an apparatuses that facilitates the deployment of managed access points in a wireless network system, with Figure 1 disclosing WLAN 10 that includes “managed access points” in the form of “access elements 12-15 for wireless communication with remote client elements 16, 18, 20, 22 and central control elements for controlling and managing the wireless connections between the access

elements 12-15 and the remote client elements.” EX-1005, 1:17-20, 3:10-18, Fig. 1 (annotated below); EX-1012, ¶274. In Calhoun’s architecture, a “central control element” manages one or more “access elements” such that the “access elements perform real-time communication functions, such as data transfer and acknowledgements, while the central control element manages the connection between the access element and one or more wireless client devices.” EX-1005, 2:6-10, 2:65-3:1; EX-1012, ¶275.



These access elements communicate using an IEEE 802.11 WLAN protocol to remote clients 16, 18, etc. EX-1005, 3:27-30. The access elements do not perform all communication functions, *e.g.*, they do not “perform link layer management functions, such as authentication and association.” EX-1005, 3:43-46, 3:51-58; EX-

1012, ¶276. Calhoun further explains that “the division of functionality between the access elements and the central control elements can be shifted,” including that “access elements can bridge network traffic associated with the remote client elements directly, while transmitting management packets to the central control element,” including when “operating in 802.11 wireless networks.” EX-1005, 9:1-2, 9:7-11; EX-1012, ¶277.

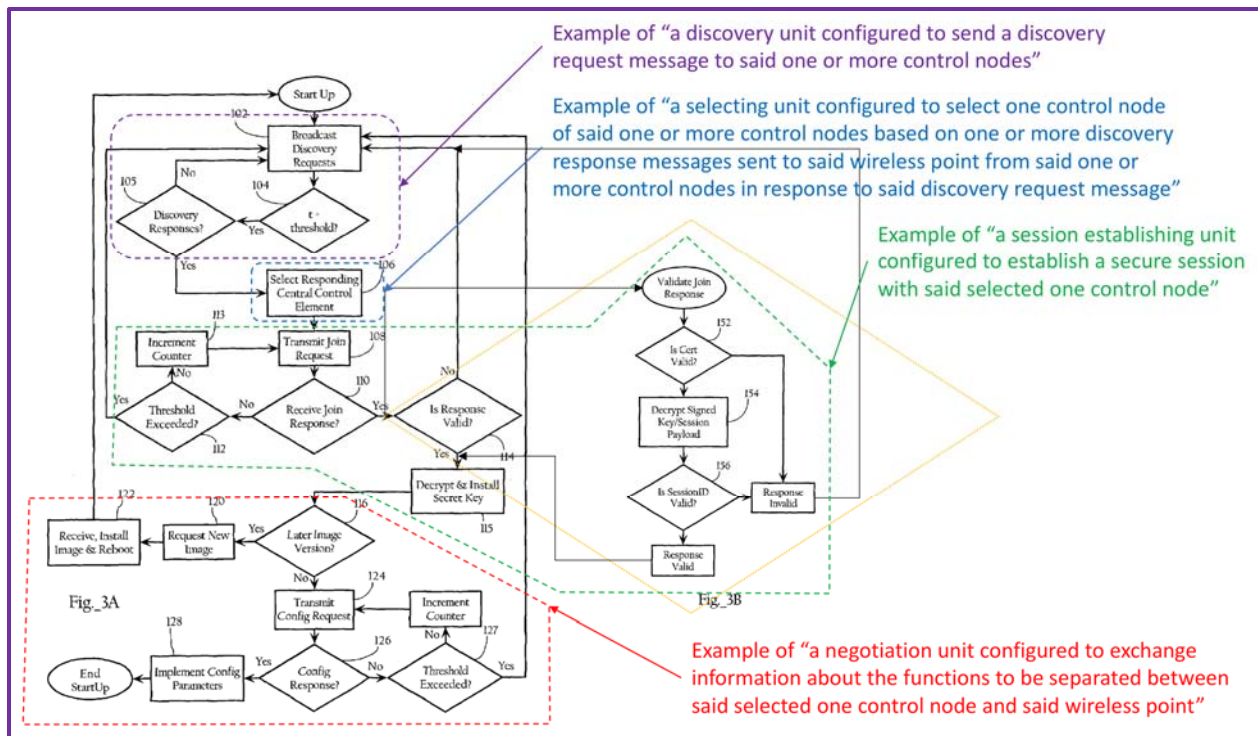
A POSA would understand that Calhoun discloses a WLAN with one or more CNs (Calhoun’s “central control elements”), and a wireless point (Calhoun’s “managed access points” or “access elements”) that “provides for functions for a wireless local area network to be separated between said wireless point and more or more control nodes (such as when the “access elements perform real-time communication functions” while the “central control element manages the connection between the access element and one or more wireless client devices” as part of a “division of functionality between the access elements and the central control elements”). EX-1012, ¶278.

[1a] a discovery unit configured to send a discovery request message to said one or more control nodes;

Calhoun discloses this limitation explicitly or inherently. Calhoun describes a “Light-Weight Access Point Protocol” that “includes functionality directed to initialization and configuration of managed access elements” across “three main phases: discovery, joinder, and configuration.” EX-1005, 4:31-37. “During the

discovery phase, the access element discovers the central control elements to which it can associate.” EX-1005, 4:37-39. Calhoun explains that, at startup, an “access element[] broadcasts or multicasts discovery requests throughout the virtual subnet implemented by the VLAN in an attempt to identify central control elements.” EX-1005, 5:20-23. This discovery request “may be a single IP packet or native link layer frame, such as an Ethernet frame.” EX-1005, 5:23-24.

Calhoun also makes explicit reference to “implementing the discovery, joiner and configuration phases of LWAPP,” as described in Figures 3A/3B. EX-1012, ¶294; EX-1005, 5:14-17. As shown in Dr. Negus’s annotations of the composite of Figures 3A/3B, Calhoun discloses a “discovery unit” that is “configured to send a discovery request message to said one or more control nodes” (such as when an “access element” “broadcasts or multicasts discovery requests throughout the virtual subnet implemented by the LAN in an attempt to identify the central control elements”). EX-1012, ¶¶294-295.



If the PO argues and the Board finds that this limitation is a means-plus-function limitation, Petitioner states that the closest structure disclosed in the '384 Patent for performing the claimed function is step 201 in Figure 2 and the applicable text at 8:59-67. EX-1001, 8:59-67; EX-1012, ¶308. The '384 Patent discloses that the way this function is performed is via an "any node discovery protocol or by the broadcast/multicast/anycast of a specific, mutually recognizable message invoking responses from available CNs," and this leads to the "result" of "discovered CNs to associate with." EX-1001, 8:59-9:2; EX-1012, ¶311.

Calhoun discloses structure for a "discovery unit," as shown in the annotated composite of Figures 3A/3B above. EX-1012, ¶310. Calhoun further discloses the claimed function of "send[ing] a discovery request message to said one or more

control nodes” when an “access element[] broadcasts or multicasts discovery requests throughout the virtual subnet [] in an attempt to identify central control elements.” EX-1005, 5:20-23. The “result” is “discovery responses” from “one or more central control elements.” EX-1005, 5:52-56; EX-1002, ¶312. A POSA would understand that the way Calhoun’s access element that “broadcasts or multicasts discovery requests throughout the virtual subnet implemented by the VLAN [] to identify central control elements” during a discovery phase is substantially similar to the ’384 Patent’s way of an “any node discovery protocol or by the broadcast/multicast/anycast of a specific, mutually recognizable message.” EX-1012, ¶313. A POSA would further recognize that Calhoun’s “result” of “discovery responses” from the “central control elements” is substantially similar to the ’384 Patent’s result of “invoking responses from available CNs” in the ’384 Patent. *Id.*

[1b] a selecting unit configured to select one control node of said one or more control nodes based on one or more discovery response messages sent to said wireless point from said one or more control nodes in response to said discovery request message, each of said one or more discovery response messages including information of functions offered by the associated control node of said one or more control nodes;

Calhoun discloses this limitation explicitly or inherently. Calhoun discloses that “central control elements[] receive the discovery requests[] and transmit discovery responses to [the] access element” and that “[e]ach discovery response comprises a central control element identifier and a load parameter.” EX-1005, 5:28-32. Calhoun explains that the “load parameter indicates the performance load

associated with the central control element” such as “the number of access elements under the management and control of a given central control element.” EX-1005, 5:34-38.

A POSA would understand that this “load parameter” is “information” that “indicates the performance load associated with the central control element” such as “the number of access elements under the management and control” of the central control element. EX-1012, ¶319. This discloses “information of functions offered by the associated control node,” such as “management and control” by the “central control element.” *Id.* Because Calhoun explains and a POSA would understand that “management and control” includes “link layer management functions, such as authentication and association,” Calhoun explicitly or inherently discloses to a POSA that “load” information, such as information about the number of access elements that the central control element is managing, is information about the capacity of link layer management functions to support additional access elements or remote client elements, *i.e.*, authentication and association the central control node performs. *Id.* A POSA, thus, would understand that this “load information” is “information of” the link layer management “functions” the central control element is currently performing and is thus “information of the functions offered by the central control node. *Id.*; EX-1005, 3:44-46.

Further, Calhoun, referencing Figure 3A, explains that an “access element [...] waits [...] for discovery responses from one or more central control elements and selects one of the responding central control elements identified in the discovery responses.” EX-1005, 5:52-56. Calhoun further explains that “selection of a given central control element can be driven by a number of different considerations” such as the “responding central control element that reports the smallest load (e.g., the smallest number of access points under management).” EX-1005, 5:60-63.

Calhoun thus discloses a “selecting unit” (shown in limitation [1a]) that is configured to select one CN based on one or more discovery response messages sent in response to said discovery request message. EX-1012, ¶321. Calhoun further discloses each discovery response message includes information of functions offered by the associated CN (such as when “[e]ach discovery response message comprises a central control element identifier and a load parameter” and the “load parameter indicates the performance load associated with the central control element” such as “the number of access elements under management” and is thus information about the functions the central control element is currently performing). *Id.*

If the Board finds this limitation is a means-plus-function limitation, Petitioner states that the closest structure disclosed in the ’384 Patent for performing the claimed function is step 203 in Figure 2 and the applicable text at 9:1-11. EX-1001, 9:1-11; EX-1012, ¶333. The ’384 Patent discloses that the way this function

is performed is to “choose which among the discovered CNs to associate with” based on “metrics” like “congestion,” and/or “manufacturer identification,” leading to the result of “CN selection.” EX-1001, 9:1-11; EX-1012, ¶336.

Calhoun discloses structure for a “selecting unit,” as shown in the annotated composite of Figures 3A/3B above. EX-1012, ¶335. Calhoun further discloses the claimed function of selecting a CN based on one or more discovery response messages sent to said wireless point in response to a discovery request message when it “selects one of the responding central control elements identified in the discovery responses” during its “discovery phase” based upon considerations such as “a central control element identifier and a load parameter,” and this leads to the result of “selection” of “one of the responding central control elements identified in the discovery responses.” EX-1012, ¶337.

A POSA would understand that the way Calhoun’s “access element” “selects one of the responding central control elements identified in the discovery responses” based upon “considerations” such as “a central control element identifier and a load parameter” during the “discovery phase” is substantially similar to the ’384 Patent’s way of “choos[ing] which among the discovered CNs to associate with” based on “metrics” such as “congestion” and/or “manufacturer identification.” EX-1012, ¶338. Further, a POSA would understand that Calhoun’s result of “selection” of “one of the responding central control elements identified in the discovery

responses” is substantially similar to the ’384 Patent’s result of a “CN selection.”

Id.

[1c] a session establishing unit configured to establish a secure session with said selected one control node; and

Calhoun discloses this limitation explicitly or inherently. Calhoun discloses that “[a]fter selection of a central control element, [the] access element[] transmits a join request to the selected central control element.” EX-1005, 6:1-6. This join request “includes an access element identifier, digital certificate and a session identifier” and may include other fields “such as WLAN MAC address, software image version.” EX-1005, 6:6-8. The “digital certificate includes a name or other identifier, a serial number, the LAN and/or WLAN MAC address associated with [the] access element[], a copy of the public key of the access element (used for encrypting messages and digital signatures)”, etc. EX-1005, 6:16-23.

The “central control element” “receives the join request[] and authenticates the digital certificate in the join request” and “composes a join response” that includes at least the “cryptographic keys” and the “digital certificate of the central control element.” EX-1005, 6:33-35, 6:47-49. The access element then receives the join response, validates it, and “assuming the join response is valid, decrypts and installs the symmetric cryptographic keys” using the procedure described in Figure 3B as annotated above. EX-1005, 6:64-7:2. As part of join response validation, the access element “validates the digital certificate associated with [the] central control

element” so that “[i]f the digital certificate is valid, [the] access element[] then verifies the signature of the signed key/session ID payload using the public key of the central control element[] and validates the session identifier.” EX-1005, 7:2-7. Then access element then “decrypts the cipher including the cryptographic keys using its private key” so that “[t]ransmission of data (e.g., configuration data, control messages, management messages, etc.) between the access element[] and the central control element[] can now be encrypted and authenticated using the shared secret cryptographic keys.” EX-1005, 7:9-13.

A POSA would understand that this “digital certificate” validation and “cryptographic keys” exchange between the access element and the selected central control element during Calhoun’s joinder phase (which follows the discovery phase) discloses that Calhoun’s access element is configured to “establish a secure session with said selected one control node.” EX-1012, ¶347. A POSA would further understand that Calhoun discloses doing so using the procedures shown in Figures 3A/3B, as annotated by Dr. Negus in limitation [1a], and this composite Figure shows a “session establishing unit.” *Id.*

Calhoun thus discloses a “session establishing unit” (the annotated portion of composite Figures 3A/3B shown in limitation [1a]) that is “configured to establish a secure session with said selected one control node.” EX-1012, ¶348.

If the Board finds this limitation is a means-plus-function limitation, Petitioner states that the closest structure disclosed in the '384 Patent for performing the claimed function is at 9:11-16. EX-1001, 9:11-16; EX-1012, ¶361. The '384 Patent discloses that the way this function is performed is via “mutual authentication” and “exchanges of security information” leading to the result of an “establishment of communication protocols.” EX-1001, 9:11-16; EX-1012, ¶364.

Calhoun’s “way” of an “access element” performing “digital certificate validation” and “cryptographic keys” exchange with the “central control element” during the joinder phase is substantially similar to the '384 Patent’s way of “mutual authentication” and “exchanges of security information.” EX-1012, ¶365. Further, Calhoun’s result of subsequent “transmission of data” between the “access element” and the “central control element” being “encrypted and authenticated using the shared secret cryptographic keys” is substantially similar to the '384 Patent’s result of “establishment of communication protocols for further exchanges.” EX-1012, ¶366.

[1d] a negotiation unit configured to exchange information about the functions to be separated between said selected one control node and said wireless point.

Calhoun discloses this limitation explicitly or inherently. As explained in [1pre], Calhoun discloses that “access elements perform real-time communication functions, such as data transfer and acknowledgements,” while the central control element “perform[s] link layer management functions, such as authentication and

association on behalf of access elements” as part of a “division of functionality between the access elements and the central control elements.” EX-1005, 2:6-10, 2:65-3:1, 3:43-46; EX-1012, ¶371. A POSA would understand that having “real-time communication functions” at the “access element” while having “link layer management functions, such as authentication and association” at the “central control element” as part of a “division of functionality between the access elements and the central control elements” is one example of “the functions to be separated between said selected one control node and said wireless point.” EX-1012, ¶372.

Calhoun explains that, during the configuration phase, the access element “composes and transmits a configuration request to [the] central control element.” EX-1005, 7:45-48. This “configuration request” includes “one or more operational parameters (such as channel, transmit power, internal v. external antenna, etc.)” that a “network administrator” can directly configure via an interface on the access element or “through an interface presented by a central control element.” EX-1005, 7:48-65. The administrator can “flag” “certain overriding parameters which a central control element can not change, except with a new ‘overriding’ parameter value.” EX-1005, 7:57-63. Calhoun disclosure explicitly or inherently discloses to a POSA that “operational parameters,” such as “channel” and “transmit power,” are information regarding the “real-time communication functions” of the WLAN that are performed by the access element, *e.g.*, the channel which the access element uses

for communication with remote client elements and the signal strength that remote client elements receive from the access element, and are thus information about the functions of the WLAN that are split into the access element. EX-1005, 2:6-7; EX-1012, ¶378.

Calhoun further explains that the “central control element[] receives the configuration request[], and generates the operational parameters for the access element[], taking into account the operational parameters identified in the configuration request,” and “transmits a configuration response including the operational parameters.” EX-1005, 7:66-8:4. The access element “receives the configuration response, . . . implements the operational parameters[], and switches to an access point mode . . . using the configuration information provided by the central control element.” EX-1005, 8:9-17. A POSA would understand that this generation of operational parameters for the access elements is part of the overall WLAN management functions performed by the central control element. EX-1005, 3:59-67 (“central control element[] may . . . process physical layer information” and “central control element[] may also transmit control messages to the access elements[] to change various operational parameters”); EX-1012, ¶379.

Calhoun further states that “wireless traffic associated with remote client elements[] . . . can be tunneled between the central control element[] and the access elements[].” EX-1005, 4:10-14. Alternatively, the “access elements[] can operate to

directly bridge network traffic between remote client elements[] and WAN[], while tunneling network management messages, such as authentication and association requests to central control element[]." EX-1005, 4:14-19. Calhoun further explains that this "division of functionality between access elements and the central control elements can be shifted," and specifically points to "bridg[ing] network traffic associated with the remote client elements directly" as an example. EX-1005, 9:9:5-15. A POSA would understand from this disclosure that functionality can be "shifted," especially in the context of "bridging" necessarily means that access elements and the central control element are exchanging information about whether bridging is performed on the access element or the central control element. EX-1012, ¶381.

A POSA would understand that Calhoun's "operational parameters"/"configuration information" exchange in the "configuration phase," as described above, disclose that Calhoun's access element is configured to "exchange information about the functions to be separated" with the "selected central control element," such as real-time communications operation at the access element and overall physical layer management at the central control element, as well as bridging between the central control element and the access element. EX-1012, ¶380. Thus, either the access element or the central control element transmits while the other receives (thus "exchange[s]") an "identifier," "parameters," and/or "information"

thus informing the other “element” about the functions at either the access element or the central control element, including real-time communication parameters, overall network management, and bridging. EX-1012, ¶¶380-381.

Calhoun explicitly (or at least inherently) discloses a “negotiation unit” (as shown in the annotated composite of Figures 3A/3B reproduced in [1a]) that is “configured to exchange information about the functions to be separated between said selected one control node and said wireless point” (such as when the access element or the central control element transmits while the other receives an “identifier,” “parameters,” and/or “information” that relate to either “real-time communication functions” at the “access element” or “link layer management functions, such as authentication and association” at the “central control element” during the “operational parameters” / “configuration information” exchange during Calhoun’s configuration phase, and when the access element and central control element necessarily exchange information about bridging). EX-1012, ¶383.

If the Board finds this limitation is a means-plus-function limitation, Petitioner states that the claimed function is “exchang[ing] information about the functions to be separated between said selected one control node and said wireless point” and the closest structure disclosed in the ’384 Patent for performing the claimed function is steps 205, 207, 209, 211, 213, 215, 219, and 221 in Figure 2 and the applicable text at 9:17-11:3. EX-1001, 9:17-11:3; EX-1012, ¶404. The ’384

Patent discloses that the way this function is by having “WAP controllers initiate by sending information regarding the functional capabilities of the associated WAPs to the chosen CN” such as “codes corresponding to the functional components that WAPs are capable of processing.” After receiving capabilities information from associated WAPs, the “CN controller[] determines an initial division of WLAN functionality” “based on a policy that allows each associated WAP to process all the functional components that they are capable of” and “only those functional components that an associated WAP cannot inherently process are left to the CN.” The CN sends the division of functionality to the associated WAPs for configuration, after which the WAP controllers “verify that the division is feasible.” This leads to the result of “a division of WLAN functionality that is consistent with the capabilities of the negotiating entities and are optimal for the operation and management of the whole WLAN.” EX-1001, 9:17-11:3; EX-1012, ¶407.

Calhoun’s “way” of performing the claimed function is via a “configuration phase” where the access element transmits a configuration request to the central control element, and this configuration request includes operational parameters and overriding parameters, which describe at least “real-time communication functions” at the access element. EX-1012, ¶408. The central control element generates operational parameters for the access element “taking into account the overriding parameters identified in the configuration request,” and then “transmits a

configuration response including operational parameters” to the “access element” which “implements the operational parameters” and “switches to an access point mode.” *Id.* This leads a “result” of a “division of functionality between the access elements and the central control elements” when “operating in 802.11 wireless networks” that uses updated “operational parameters” for such “real-time communication functions” at the “access element.” *Id.*

A POSA would understand that Calhoun’s “way” of performing the claimed function via a configuration request that includes operational and overriding parameters, followed by a configuration response from the central control element that implements the operational parameters setting the real-time communication functions at the access point during the configuration phase, is substantially similar to the ’384 Patent’s way of sending information including codes corresponding to functional components between a WAP controller and a chosen CN that determines WLAN functionality. EX-1012, ¶409. Further, Calhoun’s “result” (a “division of functionality between the access elements and the central control elements” that uses updated operational parameters for real-time communications at the access element) is substantially similar to the ’384 Patent’s result of “a division of WLAN functionality that is consistent with the capabilities of the negotiating entities and are optimal for the operation and management of the whole WLAN.” *Id.*

b. Claim 2

[2pre] The wireless point according to claim 1,

[2a] wherein said information exchange is performed by transmitting, to the selected one control node, information about functions that said wireless point has,

Calhoun discloses this limitation explicitly or inherently. As explained for [1d], Calhoun discloses an “information exchange” that is performed when the access element transmits, to the selected central control element, operational parameters such as “channel, transmit power, internal v. external antenna” for “real-time communication functions.” EX-1005, 7:45-65, 2:6-10; EX-1012, ¶419. A POSA would understand that parameters for “real-time communication functions” is “information about functions that said wireless point has,” because these parameters are information about the communication functions that the wireless point is performing. *Id.*

[2b] and receiving, from said selected one control node, information about functions that said selected one control node has.

Calhoun discloses this limitation explicitly or inherently. As discussed in [1pre], Calhoun discloses “functions said selected one control node has,” including at least “link layer management functions such as authentication and association.” EX-1012, ¶427.

Calhoun further discloses that the “information exchange,” discussed in [1d] and [2a], includes that the access element receives from the selected central control

element at least a “configuration response including the operational parameters.” EX-1005, 7:66-8:9; EX-1012, ¶428. A POSA would understand that a configuration response including the operational parameters is information about the WLAN management functions the CN is performing. EX-1012, ¶429.

c. Claim 3

The wireless point according to claim 1, wherein said functions for the wireless local area network comprise at least one of Beacon Signal Control, Power Management, Quality of Service (QoS), Scheduling, Authentication, and Encryption/Decryption.

A POSA would understand that Calhoun discloses this limitation explicitly or inherently. Calhoun discloses that the functions for the wireless local area network include “link layer management functions, such as authentication and association” for “operating in 802.11 wireless networks,” as well as encryption and decryption. EX-1005, 3:43-46, 4:54-57; 9:1-2; EX-1012, ¶448. Calhoun thus discloses authentication and encryption/decryption as listed by the claim. EX-1012, ¶449.

d. Claim 4

[4pre] A method for providing service in a wireless local area network that provides for functions for said wireless local area network to be separated between a wireless point and one or more control nodes, said method comprising:

Claim 4 is a method claim with steps that correspond to the limitations of Claim 1. A POSA would understand that Calhoun discloses this limitation explicitly or inherently for the reasons discussed for [1pre]. EX-1012, ¶¶466-467.

[4a] sending a discovery request message to said one or more control nodes;

Calhoun discloses this limitation explicitly or inherently for the reasons discussed for [1a]. EX-1012, ¶¶479-480.

[4b] selecting a control node of said one or more control nodes based on one or more discovery response messages sent to said wireless point from said one or more control nodes in response to said discovery request message, each of said one or more discovery response messages including information of functions offered by the associated control node of said one or more control nodes;

Calhoun discloses this limitation explicitly or inherently for the reasons discussed for [1b]. EX-1012, ¶¶492-493.

[4c] establishing a secure session with said selected one control node; and

Calhoun discloses this limitation explicitly or inherently for the reasons discussed for [1c]. EX-1012, ¶¶503-504.

[4d] exchanging information about the functions to be separated between said selected one control node and said wireless point.

Calhoun discloses this limitation explicitly or inherently for the reasons discussed for [1d]. EX-1012, ¶¶516-517.

e. Claim 5

[5pre] The method according to claim 4,

[5a] wherein said information exchange is performed by transmitting, to the selected one control node, information about functions that said wireless point has,

Calhoun discloses this limitation explicitly or inherently for the reasons discussed in [2pre] and [2b]. EX-1012, ¶¶533-534.

[5b] and receiving, from said selected one control node, information about functions that said selected one control node has.

Calhoun discloses this limitation explicitly or inherently for the reasons discussed for [2b]. EX-1012, ¶543.

f. Claim 6

The method according to claim 4, wherein said functions for the wireless local area network comprise at least one of Beacon Signal Control, Power Management, Quality of Service (QoS), Scheduling, Authentication, and Encryption/Decryption.

Calhoun discloses this limitation explicitly or inherently for the reasons discussed for claim 3. EX-1012, ¶¶559-560.

B. Ground II: Claims 1-6 are Obvious over Calhoun/CAPWAP/LWAPP in view of a POSA's Skill and Knowledge

1. CAPWAP

a. Analogous Art

CAPWAP, discussed in §IV.F.3, is analogous art to and in the same field as the claimed invention. CAPWAP considers WLAN functions and describes “a flexible balance of such AP (Access Point) functions as allowed in the Standards and practiced in the industry, to be meaningfully split between lightweight Access Point (LAP)” and “AP Controllers or AR (Access Router).” EX-1008, p.2; EX-1012, ¶206. CAPWAP also is pertinent to the problem addressed by the '384 Patent because it “define[s] the framework reflecting the architectural trend that delegates

and aggregates selected WLAN functions and services from APs to ARs to enhance WLAN resource management.” EX-1008, p.4; EX-1012, ¶206.

2. LWAPP

a. Analogous Art

LWAPP, discussed in §IV.F.4, is analogous art to and in the same field as the claimed invention. LWAPP describes the “Light Weight Access Point Protocol” allows a router to interoperably control and manage a collection of wireless APs. EX-1006, p.2; EX-1012, ¶154. LWAPP is pertinent to the problem addressed by the ‘384 Patent because it explains that “having a standardized, interoperable protocol could radically simplify the deployment and management of wireless networks” due to the “[c]entralization of the bridging, forwarding, authentication, encryption, and policy enforcement functions for a WLAN.” EX-1006, pp.7-8; EX-1012, ¶154.

3. Motivation to Combine Calhoun with CAPWAP and LWAPP

A POSA would be highly motivated to combine Calhoun, LWAPP and CAPWAP. EX-1012, ¶248.

First, Calhoun, LWAPP, and CAPWAP are all in the field of IEEE 802.11 WLANs. EX-1005, 1:44-57, 3:27-32; EX-1006, p.2; EX-1008, p.10; EX-1012, ¶249.

Second, Calhoun, LWAPP, and CAPWAP are directed to solving deployment challenges for the same basic system architecture of IEEE 802.11 networks and they

propose similar solutions. EX-1012, ¶¶250, 254. Calhoun’s system architecture has a “central control element” that “manages and controls one or more access elements” where the “access elements perform real-time communications functions, such as data transfer and acknowledgements, while the central control element manages the connection between the access element and one or more client devices” including during initiation and configuration phases. EX-1005, 1:6-13, 2:1-10, 4:31-37; EX-1012 ¶251. LWAPP discloses a system with “simple Access Points in 802.11 that are managed by a router or switch” that provides “[c]entralization of the bridging, forwarding, authentication, encryption and policy enforcement functions for a WLAN” including during initiation and configuration phases. EX-1006, pp.7-8, 10; EX-1012, ¶252. Similarly, CAPWAP discloses a system with “lightweight Access Point[s]” and “AP Controllers or AR (Access Router)” wherein this “new WLAN architecture” “moves much of the functions that would reside in a traditional access point (AP) to a centralized access router (AR)” including with respect to negotiation during initiation and configuration phases. EX-1008, pp.2, 9, 23; EX-1012, ¶253.

Third, Calhoun, LWAPP, and CAPWAP all share a common lineage in a similar timeframe. Calhoun was filed on March 21, 2003 and its lead inventor is Patrice Calhoun (then CTO of Airespace), and names Scott Kelly and Rohit Sori as co-inventors. EX-1012, ¶¶260-261; EX-1005, (22), (75). LWAPP was published June 28, 2003, its lead author is Patrice Calhoun, and co-authors include Bob

O'Hara, Scott Kelly, and Rohit Suri, all of whom were with Airespace. EX-1012, ¶262; EX-1006, p.1. CAPWAP, published October 20, 2003, again lists Bob O'Hara as an author, specifically acknowledges Patrice Calhoun and Scott Kelly for their contributions, and specifically references LWAPP. EX-1012, ¶263; EX-1008, pp.28, 30, 31.

Fourth, additional prior art would have motivated a POSA to combine Calhoun, LWAPP, and CAPWAP. EX-1012, ¶¶265-268. *See, e.g.*, Network World article (EX-1007, cited in §IV.F.2, *supra*) (discussing CAPWAP and LWAPP and stating that “[c]entralized security and management of wireless LANs is a rapidly growing trend in which a WLAN device such as a switch, appliance, or router is used to create and enforce policies across many streamlined, or lightweight, radio access points.”) EX-1007, p.1. In other words, the prior art specifically taught the desirability of an IEEE 802.11-based WLAN system of access points and controller nodes with the negotiable interface protocol and the various functional split architectures disclosed in Calhoun, LWAPP, and CAPWAP. EX-1007, p.2; EX-1012, ¶¶268-269.

A POSA thus would have been highly motivated to combine Calhoun, LWAPP, and CAPWAP, and would have had a reasonable expectation of success in combining their teachings. EX-1012, ¶270. For example, a POSA would have recognized that the combination of Calhoun's teaching regarding network and

device elements with protocol details taught by LWAPP and/or the network architecture details taught by CAPWAP would produce predictable and well-understood results at least because the references all disclose using a “Light Weight Access Point Protocol” for managing WLAN APs in an AP / CN system architecture that begins with discovery and transitions to dynamic configuration. EX-1012, ¶¶256-259. Further, the common authors, a common organization in Airespace, the common reference to using a “Light Weight Access Point Protocol,” and seven-month proximity in publication all strongly indicate to a POSA that the combination of the three references would produce predictable and well understood results. EX-1012, ¶259.

4. Detailed Application to the Challenged Claims

a. Claim 1

[1pre] A wireless point that provides for functions for a wireless local area network to be separated between said wireless point and one or more control nodes, said wireless point comprising:

If the preamble is limiting, Calhoun/CAPWAP/LWAPP renders it obvious.

Calhoun discloses the preamble as discussed in Ground I. §V.A.2.a.[1pre].

Likewise, LWAPP discloses a “Light Weight Access Protocol” for “allowing a router or switch to interoperably control and manage a collection of wireless Access Points.” EX-1006, p.2. LWAPP does so to “simplify the deployment and management of wireless networks” due to the “[c]entralization of the bridging,

forwarding, authentication, encryption and policy enforcement functions for a WLAN.” EX-1006, pp.7-8. Figure 1, annotated by Dr. Negus, illustrates LWAPP’s system for providing service, including a “wireless point.” EX-1012, ¶¶280-282.

LWAPP further discloses “simple Access Points in 802.11 that are managed by a router or switch (also known as an Access router, or AR).” EX-1006, p.7. LWAPP further explains that “[t]he AP forwards all 802.11 frames received to the AR via the LWAPP protocol.” EX-1006, p.7.

LWAPP thus discloses a WLAN, “one or more control nodes” (an “Access router, or AR”), and a wireless point (the “simple” or “Light Weight” “Access Points” or “APs”) that “provides for functions for a wireless local area network to be separated between said wireless point and one or more control nodes” (that “the APs can be considered as remote RF interfaces” while the “bridging, forwarding, authentication, encryption and policy enforcement functions for a WLAN”) are performed at the AR. EX-1012, ¶283.

CAPWAP also discloses a “framework” that “delegates and aggregates selected WLAN functions and services from APs to ARs to enhance WLAN resource management.” EX-1008, p.4. Figure 1, annotated by Dr. Negus, illustrates CAPWAP’s basic communications architecture between an AP and an AR. EX-1012, ¶¶285-287. CAPWAP further “describes a flexible balance of such AP (Access Point) functions as allowed in the Standards and practiced in the industry,

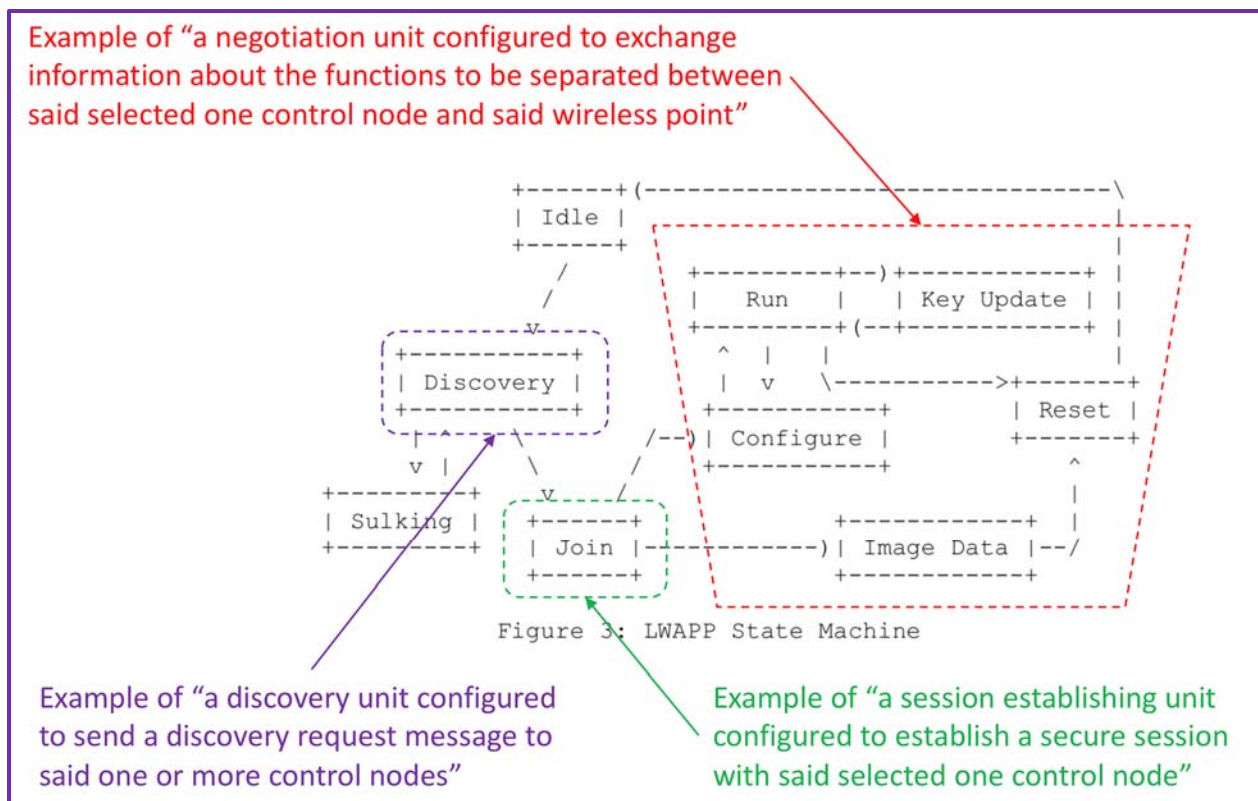
to be meaningfully split between lightweight Access Point (LAP)” and “AP Controllers or AR (Access Router).” EX-1008, p.2. The AP “Functions and Services . . . that MUST be in a lightweight AP are those that are directly related to the real-time aspects of the 802.11 MAC protocol and those related to the radio nature of an 802.11 AP.” EX-1008, p.14. CAPWAP explains that “terminating the 802.11 management frames in the AR” is called a “Split AP, where the real-time components of the 802.11 protocol are handled in the Access Point, while the access control components of the 802.11 protocol terminate in the Access Router.” EX-1008, p.10.

CAPWAP thus discloses a “wireless local area network” (the WLAN in Figure 1), “one or more control nodes” (the “AR (Access router), AC(Access Controller) and AB(Access Bridge)” that CAPWAP uses “synonymously”), and a “wireless point” (the “lightweight Access Point (LAP)”) that “provides for functions for a [WLAN] to be separated between said wireless point and one or more control nodes” (when the “functions as allowed in the Standards and practiced in the industry” are “meaningfully split” between LAP and AR with “real-time components” in the LAP and “access control components” in the AR) are performed at the AR. EX-1012, ¶288.

[1a] a discovery unit configured to send a discovery request message to said one or more control nodes;

Calhoun/CAPWAP/LWAPP renders this limitation obvious. Calhoun discloses [1a] as discussed in Ground I. §V.A.2.a.[1a].

LWAPP explains that it begins with “a discovery phase” where the “APs send a Discovery Request frame” and any Access Router “receiving that frame [] respond[s] with a Discovery Reply.” EX-1006, p.10. “Discovery Request is used by the AP to automatically discover[] potential ARs available in the network,” and this frame includes message elements including “AP Payload” and “Radio Payload (one for each radio in the AP).” EX-1006, pp.18-19. Figure 3 is a state diagram representing the “lifecycle of an AP-AR session” and, as annotated by Dr. Negus below, shows a “discovery unit” within each “Access Point” that is “configured to send a discovery request message to said one or more control nodes.” EX-1006, pp.15-16; EX-1012, ¶¶297-300.



LWAPP thus discloses a “discovery unit” (in the above annotation of Figure 3) that is “configured to send a discovery request message to said one or more control nodes” (such as when an AP “send[s] a Discovery Request frame” as a “Discovery Request message to be transmitted to a broadcast address” to “automatically discover[] potential ARs available in the network”). EX-1012, ¶301.

CAPWAP also discloses “automatic discovery” for APs that are “set up securely in the AC(AR)’s domain,” including that “Figure 1 illustrates the basic outline of communications architecture between AP & AC” including “Discovery” messages exchanged between AP and AC. EX-1008, pp.12, 21. A POSA would understand that CAPWAP’s automatic discovery using “Discovery” messages

exchanged between AP and AC/AR within the “AC(AR)’s domain” discloses that the Access Point is configured “to send a discovery request message to said one or more control nodes.” EX-1012, ¶¶303-305.

If this limitation is subject to §112, ¶6, the closest structure in the ’384 Patent for performing the claimed function “send[ing] a discovery request message to said one or more control nodes” is step 201 of Figure 2. §V.A.2.a.[1a]. As explained in Ground I, Calhoun’s Figures 3A/3B are the structure that performs the claimed functions for this limitation, and Calhoun performs the claimed functions in substantially the same way to achieve substantially the same result. EX-1012, ¶¶309-313. Further, CAPWAP discloses “automatic discovery” between the AP and the AC/AR within the AC/AR’s domain with “discovery” messages being exchanged between the AP and the AR, and so CAPWAP discloses the function of “send[ing] a discovery request message to said one or more control nodes.” EX-1012, ¶315.

A POSA would thus understand the structure in Figure 3A/3B of Calhoun, when combined with LWAPP and CAPWAP, would thus perform the same function as this limitation in the same “way” and to achieve the same “result” as the ’384 Patent (which was explained in Ground I). *Id.*

[1b] a selecting unit configured to select one control node of said one or more control nodes based on one or more discovery response messages sent to said wireless point from said one or more control nodes in response to said

discovery request message, each of said one or more discovery response messages including information of functions offered by the associated control node of said one or more control nodes;

Calhoun/CAPWAP/LWAPP renders this limitation obvious. Calhoun discloses [1b] as discussed in Ground I. §V.A.2.a.[1b].

LWAPP explains that “[f]rom the Discovery replies received, an [AP] will select an AR with which to associate.” EX-1006, p.10. An AR receiving a discovery request will respond with a “Discovery Reply [that] carries the following message elements: AR Payload” and “AR Name Payload.” EX-1006, p.19. The “AR payload message element” communicates the AR’s “current state” including its “Hardware Version,” “Software Version,” “the number of mobile stations associated with the AR,” the “maximum number of stations supported by the AR,” “the number of APs currently attached to the AR,” and the “maximum number of APs supported by the AR.” EX-1006, p.35.

A POSA would understand that at least the “number of mobile stations currently associated with the AR” and the “number of APs currently attached to the AR” discloses “information of functions offered by the associated control node” because LWAPP describes the AR as performing the “bridging, forwarding, authentication, encryption and policy enforcement functions for a WLAN.” EX-1012, ¶¶324-327; EX-1006, pp.7-8. A POSA would understand that “load” information, such as information about the number of mobile stations and APs that

the AR is managing, is information about the bridging, forwarding, authentication, encryption, and/or policy enforcement that the AR is currently performing with respect to clients attached to other WAPs in the WLAN. EX-1012, ¶327.

LWAPP further explains that an AP receiving a discovery reply “MUST wait for an interval . . . for receipt of additional discovery replies,” and after this interval lapses, “the AP enters the Joining state and will select one of the ARs that sent a discovery reply and send a Join Request to that AR.” EX-1006, pp.19-20.

A POSA would thus understand that LWAPP discloses an WAP that is “configured to select one control node of said one or more control nodes based on one or more discovery response messages sent to said wireless point from said one or more control nodes in response to said discovery request message” (when “From the Discovery Replies received, [a WAP] will select an AR with which to associate”) where “each of said one or more discovery response messages including information of functions offered by the associated control node of said one or more control nodes” (such as the “Discovery Reply” including an “AR payload message element” that includes “number of mobile stations currently associated with the AR” and/or the “number of APs currently attached to the AR”). EX-1012, ¶¶328-329.

If this limitation is subject to §112, ¶6, as stated in Ground I, the structure in the '384 Patent for performing the claimed function is step 203 of Figure 2. §V.A.2.a.[1b]. As explained in Ground I, Calhoun's Figures 3A/3B are the structure

that performs the claimed functions for this limitation, and Calhoun performs the claimed functions in substantially the same way to achieve substantially the same result. EX-1012, ¶¶334-338. Further, CAPWAP discloses “automatic discovery” between the WAP and the AC/AR within the AC/AR’s domain with “discovery” messages being exchanged between the WAP and the AR, and so CAPWAP discloses the function of “select[ing] one control node of said one or more control nodes based on one or more discovery response messages sent to said wireless point from said one or more control nodes in response to said discovery request message.” EX-1012, ¶340.

A POSA would thus understand the structure in Figure 3A/3B of Calhoun, when combined with LWAPP and CAPWAP, would thus perform the same function as this limitation in the same “way” and to achieve the same “result” as the ’384 Patent (which was explained in Ground I). *Id.*

[1c] a session establishing unit configured to establish a secure session with said selected one control node; and

Calhoun/CAPWAP/LWAPP renders this limitation obvious. Calhoun discloses [1b] as discussed in Ground I. §V.A.2.a.[1c].

LWAPP explains that, “From the Discovery Replies received, an [AP] will select an AR with which to associate, using the Join Request and Join Reply” as part of a “Join phase.” EX-1006, pp.10, 59. Further, the “Join Request” includes a “certificate message element value” as “a byte string containing a PKCS #5

certificate.” EX-1006, pp.20, 46. When the AR receives a Join Request, “[t]he AR validates the certificate found in the request” and, “if valid . . . generates a session key which will be used to secure the control frames it exchanges with the AP.” EX-1006, p. 20. When the AR sends the Join Reply, it “creates a context for the session with the AP.” EX-1006, p.20. LWAPP uses “public key cryptography to ensure trust between the AP and the AR.” EX-1006, p.59. A POSA would understand that this certificate validation and public key cryptography exchange in the Join Phase discloses that the Access Point is configured to “establish a secure session with said selected one control node.” EX-1012, ¶353. As shown in Dr. Negus’s annotation of LWAPP’s Figure 3 state diagram (shown in [1a]), LWAPP discloses a “session establishing unit” as well. EX-1012, ¶354.

A POSA would understand that LWAPP discloses a “session establishing unit” (shown in Dr. Negus’s annotation of Figure 3 shown in [1a]) that is “configured to establish a secure session with said selected one control node” (when an AP performs “PKCS #5 certificate” validation and “public key cryptography” exchange with the AR during the “Join phase”). *Id.*

CAPWAP explains that “[w]hen a[n] AP comes alive on a network, it may authenticate and register with one or more of the ARs it detects on the network it is connected to.” EX-1008, p.23. CAPWAP explains that, “for secure communications enabling automatic discovery, configuration and adaptive resource management,”

“the [APs] need to be set up securely in the AC(AR)’s domain.” EX-1008, p.21. The “[i]dentity of the AP is established reliably by cryptographically secure binding of an AP’s unique identity such one of its wireline MAC addresses to a cryptographic key.” EX-1008, p.21. A POSA would understand that this authentication via “cryptographically secure binding” within the “Capability Negotiation Phase” of CAPWAP discloses that the AP is configured to “establish a secure session with said selected one control node.” EX-1012, ¶357.

CAPWAP thus discloses a WAP that is “configured to establish a secure session with said selected one control node” (such as “authentica[ting]” by “cryptographically secure binding” during a “Capability Negotiation Phase” and becoming “set up securely in the AC(AR)’s domain”). EX-1012, ¶358.

If this limitation is subject to §112, ¶6, the closest structure in the ’384 Patent for performing the claimed function is at 9:11-16. §V.A.2.a.[1c]. As explained in Ground I, Calhoun’s Figures 3A/3B are the structure that performs the claimed functions for this limitation, and Calhoun performs the claimed functions in substantially the same way to achieve substantially the same result. EX-1012, ¶¶362-366. Further, CAPWAP discloses a “Capability Negotiation Phase” where an AP authenticates by “cryptographically secure binding” to be “set up securely in the AC(AR)’s domain” and so CAPWAP discloses the function of “establish[ing] a secure session with said selected one control node.” EX-1012, ¶368.

A POSA would thus understand the structure in Figure 3A/3B of Calhoun, when combined with LWAPP and CAPWAP, would thus perform the same function as this limitation in the same “way” and to achieve the same “result” as the ’384 Patent (which was explained in Ground I). *Id.*

[1d] a negotiation unit configured to exchange information about the functions to be separated between said selected one control node and said wireless point.

Calhoun/CAPWAP/LWAPP renders this limitation obvious. Calhoun discloses [1d] as discussed in Ground I. §V.A.2.a.[1d]. As explained in Ground I, Calhoun explains that the “division of functionality between access elements and the central control elements can be shifted,” and specifically points to “bridg[ing] network traffic associated with the remote client elements directly” as an example. EX-1005, 9:9:5-15. If the Board finds that Calhoun does not explicitly or inherently disclose exchanging information about bridging, Calhoun’s disclosure of shifting division of functionality and expressly identifying bridging renders exchanging information about how bridging is separated between an access element and a central control element would have been obvious to a POSA. EX-1012, ¶385.

LWAPP explains “APs can be considered as remote RF interfaces” while the AR performs the “bridging, forwarding, authentication, encryption and policy enforcement functions for a WLAN.” EX-1006, pp.7-8. A POSA would understand that the “remote RF interface” functions at the AP and the “bridging, forwarding, authentication, encryption and policy enforcement functions for a WLAN” at the AR

is an example of the “the functions to be separated between said selected one control node and said wireless point.” EX-1012, ¶387-388. Similarly, CAPWAP describes that the “functions as allowed in the Standards and practiced in the industry” are “meaningfully split between LAP” and “ARs” with “real-time components” in the AP and “access control components” in the AR. EX-1012, ¶396. A POSA would also understand that having “real-time” functions in the AP and “access control” functions in the AR is another example of “the functions to be separated between said selected one control node and said wireless point.” EX-1012, ¶397.

LWAPP explains that “[o]nce the AP and the AR have joined, a configuration exchange is accomplished that will . . . provision the APs” wherein such “provisioning of APs includes the typical name (802.11 Service Set Identifier, SSID), and security parameters, the data rates to be advertised and the radio channel.” EX-1006, p.10. An AP sends “Configure Requests” after “receiving a Join Reply” to “send its current configuration to its AR.” EX-1006, p.24. This request contains message elements including “Administrative State (for the AP),” “AR Name,” “Administrative State (for each radio),” “AP WLAN Radio Configuration (for each radio),” “Multi-domain Capability (for each radio),” “MAC Operation (for each radio),” “PHY TX Power (for each radio),” “PHY TX Power Level (for each Radio),” “PHY DSSS Payload or PHY OFDM Payload (for each

radio),” “Antenna (for each radio),” and “Supported Rates (for each radio).” EX-1006, p.24.

An AR that receives a Configure Request will “act upon the content of the packet and respond to the AP with a Configure Response” which “provide an opportunity for the AR to override an AP’s configuration.” EX-1006, p.25. This response contains message elements including: “Result Code,” “AP WLAN Radio Configuration (for each radio),” “Operational Rate Set (for each radio),” “Multi-domain Capability (for each radio),” “MAC Operation (for each radio),” “PHY Tx Power (for each Radio),” “PHY DSSS or PHY OFDM Payload (for each radio),” and “Antenna (for each radio).” EX-1006, p.25.

A POSA would understand that LWAPP’s “configuration exchange” for provisioning during the configuration phase discloses that the AP is configured to “exchange information about functions to be separated” with the AR because this exchange involves “message elements” (*i.e.*, “information”) about “remote RF interface” functions at the AP (*i.e.*, “about the functions to be separated between said selected one control node and said wireless point”). EX-1012, ¶392.

LWAPP thus discloses a “negotiation unit” (shown in Dr. Negus’s annotation of Figure 3 shown in [1a]) that is “configured to exchange information about the functions to be separated between said selected one control node and said wireless

point” (such as a “configuration exchange” between an AP and an AR that involves “message elements about “remote RF interface” functions). EX-1012, ¶393.

Similarly, CAPWAP explains that “[c]onfiguration of an AP includes providing the parameters necessary for the AP to advertise and provide service for one or more WLANs” where “[p]hysical parameters are related to the operation of the AP’s radio interface” and “[l]ogical parameters are related to individual WLANs that are provisioned on the AP.” EX-1008, p.21. These “physical parameters” include “the channel on which the AP is to operate, the maximum power at which the AP is to transmit, antenna selections, the supported data rates, and the timing for the periodic announcements of the WLANs provisioned on the AP.” EX-1008, p.21. “Logical parameters” include “the SSID of the WLANs, the allowed authentication methods, the allowed privacy methods, values for the contention-free period and DTIM, VLAN associations, IP addresses and netmasks, authentication server addresses, any pre-shared keys for WLANs or authentication servers, regulatory (country) information, and other 802.11-specific capabilities to be advertised for the WLANs.” EX-1008, p.21.

A POSA would understand that CAPWAP’s configuration by providing parameters based on CAPWAP’s negotiated architecture discloses that CAPWAP’s AP is configured to “exchange information about the functions to be separated” with the “AR” because providing the parameters (*i.e.*, the “exchange” of “information”)

is at least about the “real-time components” in the AP (*i.e.*, “about the functions to be separated between said selected one control node and said wireless point”). EX-1012, ¶400.

A POSA would thus understand that CAPWAP’s AP is “configured to exchange information about the functions to be separated between said selected one control node and said wireless point” (such as when “providing the parameters” to the AP from the AR about “real-time components among the “functions” within the AP). EX-1012, ¶401.

If this limitation is subject to §112, ¶6, as stated in Ground I, the structure in the ’384 Patent for performing the claimed function is steps 205, 207, 209, 211, 213, 215, 219, and 221 in Figure 2 and the applicable text at 9:17-11:3. §V.A.2.a.[1c]. As explained in Ground I, Calhoun’s Figures 3A/3B are the structure that performs the claimed functions for this limitation, and Calhoun performs the claimed functions in substantially the same way to achieve substantially the same result. EX-1012, ¶¶405-410. Further, CAPWAP discloses the AR “providing the parameters” to the AP about “real-time components” among the “functions” within the AP, and thus performing the function “exchange[ing] information about the functions to be separated between said selected one control node and said wireless point.” EX-1012, ¶411.

A POSA would thus understand the structure in Figure 3A/3B of Calhoun, when combined with LWAPP and CAPWAP, would thus perform the same function as this limitation in the same “way” and to achieve the same “result” as the ’384 Patent (which was explained in Ground I). *Id.*

b. Claim 2

[2pre] The wireless point according to claim 1,

[2a] wherein said information exchange is performed by transmitting, to the selected one control node, information about functions that said wireless point has,

Calhoun/CAPWAP/LWAPP renders this limitation obvious. Calhoun discloses [2pre] and [2a] as discussed in Ground I. §V.A.2.b.

LWAPP discloses an “information exchange” between an AP and an AR where the AP (*i.e.*, the “wireless point”) sends to the AR (*i.e.*, “transmitting, to the selected one control node”) “message elements” such as “AP WLAN Radio Configuration” or “MAC Operation” for “remote RF interfaces” (*i.e.*, “information about functions that said wireless point has”). EX-1012, ¶422.

[2b] and receiving, from said selected one control node, information about functions that said selected one control node has.

Calhoun/CAPWAP/LWAPP renders this limitation obvious. Calhoun discloses [2b] as discussed in Ground I. §V.a.2.b.[2b].

LWAPP discloses “functions that said selected one control node has” include “bridging, forwarding, authentication, encryption and policy enforcement functions

for a WLAN.” EX-1012, ¶431. Further, as explained for [1d], LWAPP discloses an “information exchange” that is performed when the AP has a “configuration exchange” to “provision the APs” that includes the AR “respond[ing]” (*i.e.*, the wireless point “receiving, from said selected one control node”) with a “Configure Response” that “includes the typical name (802.11 Service Set Identifier, SSID), and security parameters” (*i.e.*, “information about functions that said selected one control node has”). EX-1012, ¶432.

A POSA would thus understand that, because LWAPP discloses that the AR performs at least the “authentication, encryption and policy enforcement functions for a WLAN,” that the AP receiving information including the ““802.11 Service Set Identifier, SSID,” and “security parameters” in a “Configure Response” frame represents “information about functions that said selected one control node has” because “SSID” information and “security parameters” are functional information about the “authentication, encryption and policy enforcement” functions of the AR. EX-1012, ¶433.

Similarly, CAPWAP discloses “functions that said selected one control node has” include those that support CAPWAP’s architecture where “access control components of the 802.11 protocol terminate in the [AR].” EX-1012, ¶436. CAPWAP describes these “access control components” as including “Authentication,” “Deauthentication,” “Association,” “Disassociation,” and

“Reassociation.” EX-1008, pp.14-15. Further, as explained for [1d], CAPWAP discloses an “information exchange” that is performed when the AR “provid[es] the parameters” to the AP (*i.e.*, the “wireless point” is “receiving, from said selected one control node”) at least “[l]ogical parameters” including “the SSID of the WLANs,” “the allowed authentication methods,” “the allowed privacy methods,” and “any pre-shared keys for WLANs or authentication servers” (*i.e.*, “information about functions that said selected one control node has”). EX-1012, ¶437.

A POSA would thus understand that, because CAPWAP discloses an AR that performs functions including “Authentication,” “Deauthentication,” “Association,” “Disassociation,” and “Reassociation,” that “[l]ogical parameters” that include “the SSID of the WLANs,” “the allowed authentication methods,” “the allowed privacy methods,” and “any pre-shared keys for WLANs or authentication servers” is a “disclosure of information about the functions that selected one control node has” because parameters such as such “SSID,” “authentication methods,” “privacy methods,” and “pre-shared keys” are fundamental information about such “functions” of “Authentication,” “Deauthentication,” “Association,” “Disassociation,” and “Reassociation” for the AR. EX-1012, ¶438.

c. Claim 3

The wireless point according to claim 1, wherein said functions for the wireless local area network comprise at least one of Beacon Signal Control,

Power Management, Quality of Service (QoS), Scheduling, Authentication, and Encryption/Decryption.

Calhoun/CAPWAP/LWAPP renders this limitation obvious. Calhoun discloses [2b] as discussed in Ground I. §V.A.2.c.

As discussed in [1pre], LWAPP discloses that “functions for the wireless local area network” comprising at least “authentication, encryption and policy enforcement functions for a WLAN” operating “in 802.11.” EX-1012, ¶¶452-453; EX-1006, pp.7-8. Similarly, CAPWAP states that the “access control components of the 802.11 protocol include “Authentication,” “Deauthentication,” “Association,” “Disassociation,” and “Reassociation.” EX-1008, pp.14-15. CAPWAP further states that AP functions that relate to real-time aspects of 802.11 include “Privacy,” “Beaconing,” and “Power Management.” EX-1008, p.14; EX-1012, ¶¶456-458. Further, a POSA would be aware that IEEE 802.11 WLAN systems would necessarily include “scheduling.” EX-1012, ¶¶240, 461

d. Claim 4

[4pre] A method for providing service in a wireless local area network that provides for functions for said wireless local area network to be separated between a wireless point and one or more control nodes, said method comprising:

Calhoun/CAPWAP/LWAPP renders this limitation obvious for the reasons discussed in [1pre]. EX-1012, ¶¶464-465.

[4a] sending a discovery request message to said one or more control nodes;

Calhoun/CAPWAP/LWAPP renders this limitation obvious for the reasons discussed in [1a]. EX-1012, ¶¶477-478.

[4b] selecting a control node of said one or more control nodes based on one or more discovery response messages sent to said wireless point from said one or more control nodes in response to said discovery request message, each of said one or more discovery response messages including information of functions offered by the associated control node of said one or more control nodes;

Calhoun/CAPWAP/LWAPP renders this limitation obvious for the reasons discussed in [1b]. EX-1012, ¶¶490-491.

[4c] establishing a secure session with said selected one control node; and

Calhoun/CAPWAP/LWAPP renders this limitation obvious for the reasons discussed in [1c]. EX-1012, ¶¶501-502.

[4d] exchanging information about the functions to be separated between said selected one control node and said wireless point.

Calhoun/CAPWAP/LWAPP renders this limitation obvious for the reasons discussed in [1d]. EX-1012, ¶¶514-515.

e. Claim 5

[5pre] The method according to claim 4,

[5a] wherein said information exchange is performed by transmitting, to the selected one control node, information about functions that said wireless point has,

Calhoun/CAPWAP/LWAPP renders this limitation obvious for the reasons discussed in [2pre] and [2a]. EX-1012, ¶¶528-529, 531-532.

[5b] and receiving, from said selected one control node, information about functions that said selected one control node has.

Calhoun/CAPWAP/LWAPP renders this limitation obvious for the reasons discussed in [2b]. EX-1012, ¶¶541-542.

f. Claim 6

The method according to claim 4, wherein said functions for the wireless local area network comprise at least one of Beacon Signal Control, Power Management, Quality of Service (QoS), Scheduling, Authentication, and Encryption/Decryption.

Calhoun/CAPWAP/LWAPP renders this limitation obvious for the reasons discussed in claim 3. EX-1012, ¶¶557-558.

VI. THE BOARD SHOULD NOT EXERCISE ITS DISCRETION TO DENY INSTITUTION

A. The Board Should Not Deny Institution Under *Fintiv*

In *Apple Inc. v. Fintiv, Inc.*, the Board set forth six non-dispositive factors to guide whether efficiency, fairness, and the merits support the exercise of authority to deny institution in view of an earlier trial date in the parallel proceeding. On June 21, 2022, the Director issued Interim Guidance regarding application of the *Fintiv* factors stating that “the PTAB will not deny institution of an IPR or PGR under *Fintiv* [] when a petition presents compelling evidence of unpatentability.” USPTO Memorandum, Interim Procedure for Discretionary Denials in AIA PostGrant Proceedings with Parallel District Court Litigation (June 21, 2022), at 9. Here, the Petition is particularly strong and presents compelling evidence of unpatentability

of the Challenged Claims. Thus, under the Interim Guidance, the Board should not deny institution.

Likewise, the Board's decision in *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 (Dec. 1, 2020) (precedential as to § II.A) instructs that a holistic view of the remaining *Fintiv* factors also weighs in favor of institution.

Factor 1 is neutral. No request for stay was filed in the District Court (§VIII.B). *Sand Revolution II LLC v. Continental Intermodal Group – Trucking LLC*, IPR2019-01393, Paper 24 at 7 (June 16, 2020) (informative). Under factor 2, the trial date is set for September 23, 2024. Further, a Final Written Decision in this matter is expected in or around January, 2025. Considering the inherent uncertainties of litigation scheduling, particularly where multiple trials are scheduled for the same date these factors weigh against discretionary denial.

Factor 3 favors institution. The co-pending litigation is in its early stages, and the investment in it has been minimal. The parties have will not begin claim construction briefing until February 29, 2024, after the expected institution decision in this matter. EX-1014, 4. The *Markman* hearing is not until April 11, 2024; fact discovery closes in May, 2024, and expert discovery closes in June, 2024. EX-1014, 3; see *PEAG LLC v. Varta Microbattery GMBH*, IPR2020-01214, Paper 8 at 17 (Jan. 6, 2021) (little investment in the parallel proceeding where claim construction hearing had not yet been held and discovery was not complete).

Under factor 4, Petitioner stipulates that if the IPR is instituted, it will not pursue, in District Court, the same invalidity grounds for the claims challenged here. *Sand Revolution II* at 7. Thus, the grounds presented here will not be asserted in District Court against the challenged claims and this factor weighs in favor of institution. In addition to the stipulation that Petitioner issued to PO, PO has only asserted a subset of the claims that are being challenged in the present Petition. Thus, it is unlikely the district courts will be addressing the validity of all of the claims challenged by this Petition. Thus, this factor favors institution. *Sand Revolution II* at 12.

Under factor 5, while Petitioner is a defendant in District Court, nothing within *Fintiv* suggests that the same parties between the proceedings weighs in favor of discretionary denial. See *HP Inc. v. Slingshot Printing LLC*, IPR2020-01084, Paper 13 at 9 (Jan. 14, 2021) (having the “same parties as parallel proceeding” makes factor 5 “neutral”).

Under factor 6, other circumstances weigh in favor of institution. Here, the merits of the Petition are particularly strong. For example, each asserted reference, Calhoun, LWAPP, and CAPWAP, discloses the very limitation (a “*negotiation unit configured to exchange information about functions to be separated between said selected one control node and said wireless point*”) by which the ’384 Patent gained allowance. EX-1002, pp.273, 288; §IV.B.

When viewed holistically, the timing of the present Petition is reasonable; there has been relatively limited investment in the EDTX litigation; and there is minimal overlap between the present IPR and the parallel litigation. Coupling these *Fintiv* considerations with compelling evidence of unpatentability, the efficiency and integrity of the IPR process is best served by instituting review.

B. This Petition Presents Arguments Not Before the Examiner

PO may argue that the Board should deny institution because, in relying on CAPWAP for Ground 2, this Petition presents “the same or substantially the same prior art or arguments previously . . . presented to the Office.” §325(d). Such an argument would be wrong: the grounds asserted in this Petition are neither the same nor substantially the same as nor cumulative to art or arguments presented during the prosecution of the ’384 Patent. The Board uses a two-part framework in determining whether to exercise discretion under §325(d). *Advanced Bionics, LLC v. MED-L Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6 (Feb. 13, 2020) (precedential).

Under the first part of the framework, none of the references asserted in this Petition were “previously presented to the Office.” *Id.* at 7-8. Notably, CAPWAP and O’Hara are different references. And while PO may argue that CAPWAP is cumulative to O’Hara, Petitioner only presents CAPWAP in combination with Calhoun and LWAPP, which were never cited or considered by the Examiner.

Further, the Examiner relied on O’Hara as anticipating the claims and allowed the claims because O’Hara did not disclose “exchang[ing] information about functions to be separated between said selected one control node and said wireless point.” EX-1002, p.288. If the Board finds that CAPWAP is cumulative of O’Hara or does not expressly disclose this limitation, Petitioner shows how both Calhoun and LWAPP disclose this limitation and how CAPWAP renders this limitation obvious. Thus, the conditions of the first part of the *Advanced Bionics* framework are not met, and the Board should decline to exercise its discretion under §325(d) to deny institution.

Even if the Board were to consider the second part of the *Advanced Bionics* framework, the Office erred in a manner material to the patentability of the Challenged Claims. The Examiner never considered whether O’Hara rendered the claims obvious and never considered or identified any combination of O’Hara with Calhoun and LWAPP. This Petition presents extensive analysis explaining how Calhoun (Ground 1) and the combination of Calhoun, LWAPP, and CAPWAP (Ground 2) disclose the limitations of the Challenged Claims, and why a POSA would be motivated to combine the references’ teachings. This additional evidence, not considered during prosecution, warrants consideration here. Further, this Petition is supported by the expert testimony of Dr. Negus (EX-1012), who explains how a POSA would have understood the references and why a POSA would have combined their teachings. This new evidence weighs against discretionary denial.

See, e.g., Puma N. Am., Inc. v. Nike, Inc., IPR2019-01058, Paper 10, 19 (Oct. 31, 2019) (granting institution where “new non-cumulative evidence.... helpful to our consideration of a prior art combination that was not before the Examiner”).

VII. MANDATORY NOTICES UNDER 37 C.F.R. §42.8

A. Real Parties-In-Interest Under 37 C.F.R. § 42.8(b)(1)

Petitioner is Hewlett Packard Enterprise Company, which is the real party-in-interest.

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

The '384 Patent is asserted against Petitioner in *Sovereign Peak Ventures, LLC v. Hewlett Packard Enterprise Co.*, 2:23-cv-00009 (E.D. Tex.), filed on January 10, 2023.

To Petitioner’s knowledge, the '384 Patent was involved in the following pending case, which may be affected by a decision in this proceeding:

Style	Number	Tribunal	Filed
<i>Sovereign Peak Ventures, LLC v. TP-Link Corp. Ltd.</i>	6:22-cv-01273	Western District of Texas	12/09/2022

C. Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

Lead Counsel
Patrick D. McPherson, USPTO Reg. No. 46,255 DUANE MORRIS LLP 901 New York Avenue, NW, Ste. 700 East Washington, D.C. 20001 P: 202.776.5214, F: 202.776.7801; PDMcPherson@duanemorris.com
Back-Up Counsel
Patrick C. Muldoon, USPTO Reg. No. 47,343 DUANE MORRIS LLP 901 New York Avenue, NW, Ste. 700 East Washington, D.C. 20001 P: 202.776.7840, F: 202.776.7801; PCMuldoon@duanemorris.com Matthew S. Yungwirth (<i>to seek Pro Hac Vice admission</i>) DUANE MORRIS LLP 1075 Peachtree Street NE, Suite 1700 Atlanta, GA 30309 P: 404 253 6935, F: 404.745.0863; MSYungwirth@duanemorris.com

D. Service Information Under 37 C.F.R. § 42.8(b)(4)

Service via hand-delivery may be made at the postal mailing address of either lead or back-up counsel. Petitioner consents to service by e-mail at the addresses listed above.

VIII. CONCLUSION

For the foregoing reasons, Petitioner respectfully requests institution of an *inter partes* review, and cancellation of claims 1-6 of the '384 Patent.

Dated: July 31, 2023

Respectfully submitted,

/Patrick D. McPherson/

Patrick D. McPherson

USPTO Reg. No. 46,255

DUANE MORRIS LLP

901 New York Ave., NW, Ste. 700
East

Washington, D.C. 20001

P: 202.776.5214, F: 202.776.7801

PDMcPherson@duanemorris.com

ATTORNEY FOR PETITIONER

I. CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24, the undersigned attorney for the Petitioner, Hewlett Packard Enterprise Company, declares that the argument section of this petition (Sections I-VI and VIII) has a total of 13,970 words, according to the Microsoft Wordtm word count tool.

Dated: July 31, 2023

Respectfully submitted,

/Patrick D. McPherson/

Patrick D. McPherson

USPTO Reg. No. 46,255

DUANE MORRIS LLP

901 New York Ave., NW, Ste. 700

East

Washington, D.C. 20001

P: 202.776.5214, F: 202.776.7801

PDMcPherson@duanemorris.com

ATTORNEY FOR PETITIONER

CERTIFICATION OF SERVICE ON PATENT OWNER

Pursuant to 37 C.F.R. §§42.6(e), 42.8(b)(4) and 42.105, the undersigned certifies that on the 31st of July, 2023, a complete and entire copy of this Petition for Inter Partes Review of U.S. Patent 8,270,384 and all supporting exhibits were served via Federal Express, postage prepaid, to the correspondence address of record for the '384 Patent:

52989 – Dickinson Wright PLLC
1825 Eye St. N.W.
SUITE 900
Washington, DC 20006
UNITED STATES

Dated: July 31, 2023

Respectfully submitted,

/Patrick D. McPherson/
Patrick D. McPherson
USPTO Reg. No. 46,255
DUANE MORRIS LLP
901 New York Ave., NW, Ste. 700
East
Washington, D.C. 20001
P: 202.776.5214, F: 202.776.7801
PDMcPherson@duanemorris.com

ATTORNEY FOR PETITIONER