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 8,045,531 B2
Issue Date: Oct. 25, 2011

Title: SYSTEM AND METHOD FOR NEGOTIATION OF WLAN ENTITY

Inter Partes Review No.: IPR2023-01261

PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT 8,045,531 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 '531 Patent 2

B. Prosecution History 6

C. Claim Construction 7

D. Priority of the Challenged Claims 9

E. Person of Ordinary Skill in the Art 9

F. State of the Art 10

1. 802.11 10

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, 7, and 13 are Anticipated by Calhoun 15

1. Calhoun (EX-1005) 15

a. Analogous Art 15

b. Overview of Calhoun 15

2. Detailed Application to the Challenged Claims 16

a. Claim 1 16

b. Claim 7 34

c. Claim 13 40

B. Ground 2: Claims 1, 7, and 13 are Obvious over Calhoun in View of CAPWAP and LWAPP and the Knowledge of a POSA 41

1. CAPWAP 41

a. Analogous Art 41

2. LWAPP 42

a. Analogous Art 42

3. Motivation to Combine Calhoun with CAPWAP and LWAPP 43

4. Detailed Application to the Challenged Claims 45

a. Claim 1 45

a. Claim 7 60

b. Claim 13 65

VI. The Board Should Not Exercise its Discretion to Deny Institution 66

VII. Mandatory Notices under 37 C.F.R. §42.8 69

A. Real Parties-In-Interest Under 37 C.F.R. § 42.8(b)(1) 69

B. Related Matters Under 37 C.F.R. § 42.8(b)(2) 69

C. Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3) 70

D. Service Information Under 37 C.F.R. § 42.8(b)(4) 71

TABLE OF AUTHORITIES

Federal Cases

Phillips v. AWH Corp., 415 F.3d 1303 (Fed. Cir. 2005) 7

Sovereign Peak Ventures, LLC v. Hewlett Packard Enterprise Co., 2:23-cv-00009 (E.D. Tex.) 69

Sovereign Peak Ventures, LLC v. TP-Link Corp. Ltd., 6:22-cv-01273 (W.D. Tex.).....70

Regulatory Cases

Apple Inc. v. Fintiv, Inc., IPR2020-00019 66

HP Inc. v. Slingshot Printing LLC, IPR2020-01084, Paper 13 (Jan. 14, 2021) 68

PEAG LLC v. Varta Microbattery GMBH, IPR2020-01214, Paper 8 (Jan. 6, 2021).....68

Sand Revolution II LLC v. Continental Intermodal Group – Trucking LLC, IPR2019-01393, Paper 24 (June 16, 2020)..... 67-68

Sotera Wireless, Inc. v. Masimo Corp., IPR2020-01019, Paper 12 (Dec. 1, 2020).....67

Federal Statutes

35 U.S.C. §103.....1, 14

35 U.S.C. §112, ¶6.....24, 29, 57, 63

Regulations

37 C.F.R. §42.8.....69

37 C.F.R. § 42.8(b)(1).....69

37 C.F.R. § 42.8(b)(2).....69

37 C.F.R. § 42.8(b)(3).....70

37 C.F.R. § 42.8(b)(4).....70

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

Exhibit #	***Description***
1001	U.S. Patent 8,045,531 ("'531 Patent")
1002	Prosecution History of the '531 Patent
1003	[Omitted]
1004	[Omitted]
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. Aaaron, "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	IETF 802.11-1999
1010	[Omitted]
1011	IETF RFC 5412
1012	Declaration of Dr. Kevin Negus
1013	Plaintiff's Preliminary Infringement Contentions, *Sovereign Peak Ventures, LLC v. Hewlett Packard Enterprise Company*, Case No. 2:23-cv-00009 (E.D. Tex.), served on Feb. 28, 2023
1014	Amended Docket Control Order, *Sovereign Peak Ventures, LLC v. Hewlett Packard Enterprise Company*, 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 *Inter Partes* 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. 8,045,531 ("'531 Patent") (EX-1001). Petitioner respectfully submits that Claims 1, 7, and 13 ("Challenged Claims") of the '531 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 WAPs and CNs having complementary functionality, some of which the other did not have; as compared to that heavyweight WAPs that have "complete functionality." 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 in 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

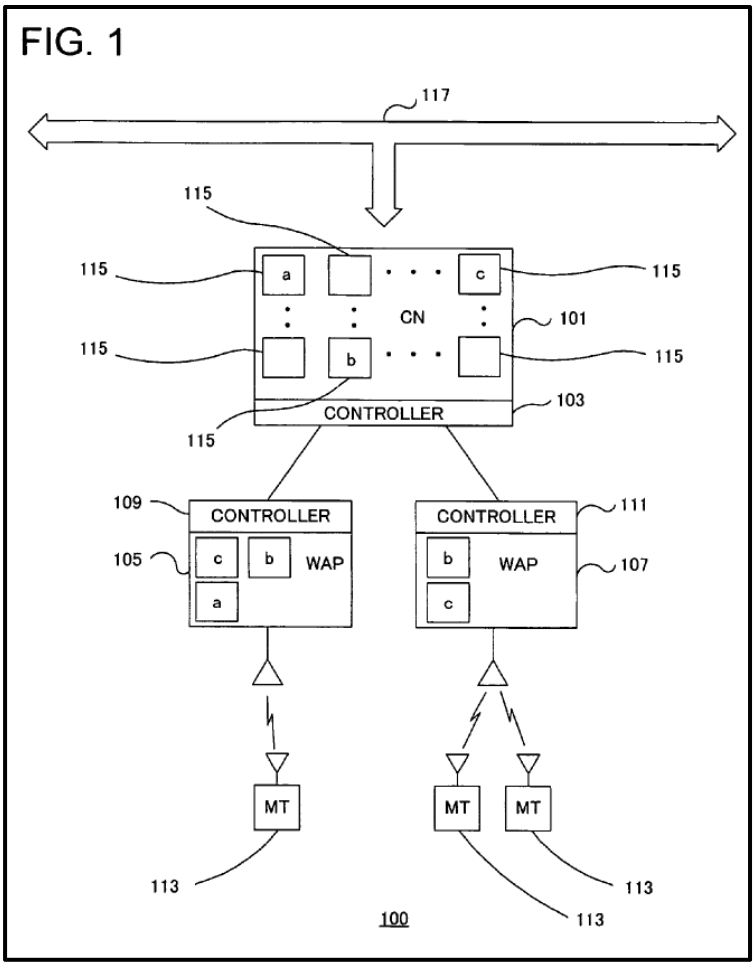
Petitioner certifies that the '531 Patent is available for IPR and Petitioner is not barred or estopped from requesting this review. 37 C.F.R. §42.104(a). This Petition is filed under 37 C.F.R. §42.106(a).

III. REASONS FOR THE REQUESTED RELIEF

As explained here and in the Declaration of Petitioner's Expert, Dr. Kevin Negus (EX-1012), the systems/methods claimed in the '531 Patent were obvious over the prior art to a person of ordinary skill in the art ("POSA") at the time of the invention.

A. Summary of the '531 Patent

The '531 Patent relates to "split architecture" WLANs, where various network functions are divided between one or more central CNs and several WAPs. EX-1001, 1:20-25, 7. In split architecture systems, certain "control aspects" of the WLAN are centralized in one or more CNs while other aspects of the WLAN are performed by the WAPs. Figure 1 illustrates this split architecture and shows a CN connected to two WAPs, which themselves serve various mobile terminals:



The ’531 Patent admits that “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 created by the Internet Engineering Task Force (“IETF”). EX-1001, 1:20-34.

The ’531 Patent states that earlier efforts did “not consider the problems of accommodating WAPs with dissimilar functional capabilities within a single WLAN” and that “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, 1:34-37, 1:64-67. The '531 Patent describes an apparatus/method for negotiations between CNs and WAPs of a WLAN, "based on policies that allow for accommodating static and dynamic differences among the WLAN entities" and "provide[s] 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, 3:13-32.

The '531 Patent references Figure 1 to explain its purported invention. 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, 7:9-26. These functional codes are logical representations 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, 7:9-16. Figure 1 shows WAP 107 with only a subset of the functional components of WAP 105, demonstrating 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, 7:38-50; Ex. 1012 ¶XX.

The ’531 Patent purports to solve the problem of WAPs with different functional capabilities by offering methods for dividing functions between WAPs and CNs. EX-1001, 5:49-51, 9:4-8. The ’531 Patent describes these negotiations in Figure 2:

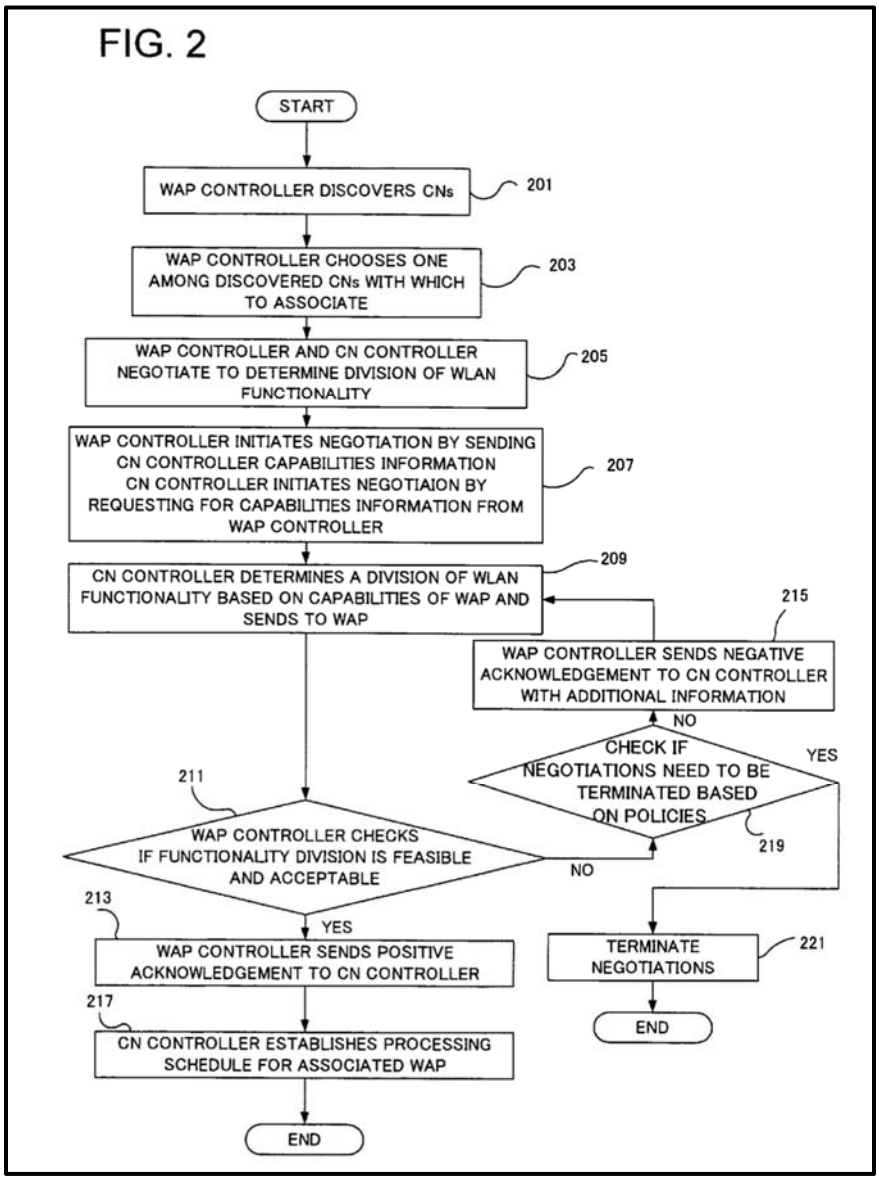


Figure 2 describes three “phases” of interaction between the WAPs and the CNs. First, in a “discovery” phase, a WAP discovers an available CN. EX-1001,

8:44-51. Second, in an "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, 8:62-67. Third, in a "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, 9:10-9:22. 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, 11:24-27.

B. Prosecution History

Application No. 10/591,184, which became the '531 Patent, was filed on May 14, 2007. EX-1001, (22), (86). Originally filed claim 1 referred to "negotiation means" and required that the WAPs and CNs be "capable" of providing a subset of complete functionality" in the WLAN. Ex. 1002, at 79; Ex. 1012 ¶XX. The Examiner rejected claim 1 as anticipated by U.S. Pub. 2003/0035464 ("Dehner"). EX-1002, pp.304-311. Claim 1 was amended to its issued form by replacing "capable of processing a subset of complete functionality" with "for processing a subset of complete functionality," replacing "negotiation means" with "negotiation unit," and making some additional conforming edits, such as removing the reference

to a CN providing "same or different complementary functionality." EX-1002, p.324. The Applicant argued that Dehner's WAPs (called "NAPs") all "have the same and complete functionality," which was different from claim 1, which "presume[s] that each WAP has a different set of functional components." EX-1002, p.335. The Applicant argued Dehner did not disclose a CN providing "complementary functionality" to a WAP because "complementary functionality" necessarily meant "providing functionality to a WAP which the WAP does not have." EX-1002, p.336 (emphasis in original). Dehner did not disclose this limitation because its "NAPs" had the "same and complete functionality." EX-1002, p.335.

The Examiner withdrew the rejections based on Applicant's arguments (EX-1002, p.373) and 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 ¶96. 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:

Limitation	**Function**	**Structure**
"negotiation unit for the single or plurality of WAPs ..." (claim 1)	"dynamically negotiate with the control node for a secure connection and function split arrangement"	Steps 205, 207, 209, 211, 213, 215, 219 and 221 in Figure 2 and the applicable text in 8:62-10:53 of the '531 Patent
"discovering unit ..." (claim 7)	"discovering an available CN within a specified domain"	Step 201 in Figure 2 and the applicable text in 8:43-51 of the '531 Patent
"a secure connection negotiating unit ..." (claim 7)	"negotiating a secure connection with a CN that may provide the complementary functionality desired by the WAP" "establishes a secure connection with the CN that provides the complementary functionality"	Steps 205, 207, 209, 211, 213, 215, 219 and 221 in Figure 2 and the applicable text in 8:62-10:53 of the '531 Patent

For these terms, Petitioner has identified the closest disclosed structure in the '531 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 functions is not sufficiently disclosed in the '531 Patent.

D. Priority of the Challenged Claims

The PCT application that led to the '531 Patent was filed March 1, 2005. EX-1001, (22). In related District Court litigation, PO has asserted that the '531 Patent is entitled to a priority date of at least as early as March 2, 2004. For this Petition, Petitioner relies on references that are prior art as of the earlier March 2, 2004 priority date alleged by PO.

E. Person of Ordinary Skill in the Art

A POSA 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, general knowledge, skill, common sense, and creativity possessed by a POSA as of March, 2004, and 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" (EX-1008, pp.7-8) knowns as a WLAN.

2. Centralized Management of WLANs

Traditional WLANs functioned on a "stand-alone basis" using "fat" APs, which contained "all wireless processing capabilities." EX-1007. However, by 2003, "centralized security and management of [WLANs] was a rapidly growing

trend." EX-1007. One 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 WLAN CNs "to create and enforce policies across many streamlined, or lightweight" APs. *Id.* An advantage of having lightweight APs paired with CNs 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.

CAPWAP Figure 1 shows the "basic outline of communications architecture between AP & [AR]." *Id.*, p.12.

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 WAP "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, 7, and 13 of the '531 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, 7, 13	§102	Calhoun
2	1, 7, 13	§103	Calhoun in view of CAPWAP and LWAPP (referred to as "Calhoun/CAPWAP/LWAPP") in view of the knowledge of a POSA

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 '531 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 '531 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 20, 2003. EX-1008, 1. CAPWAP is publicly available at: https://datatracker.ietf.org/doc/pdf/draft-mani-capwap-arch-00, and was publicly available to a member of the interested public as of at least October 22, 2003. EX-1016, ¶¶1-9, 11. CAPWAP is prior art to the '531 Patent under at least §102(a)-(b).

V. IDENTIFICATION OF HOW THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Ground 1: Claims 1, 7, and 13 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, ¶¶102-114. Calhoun is analogous art, is in the same field of endeavor, and is reasonably pertinent to the problem addressed by the '531 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, ¶115.

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

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

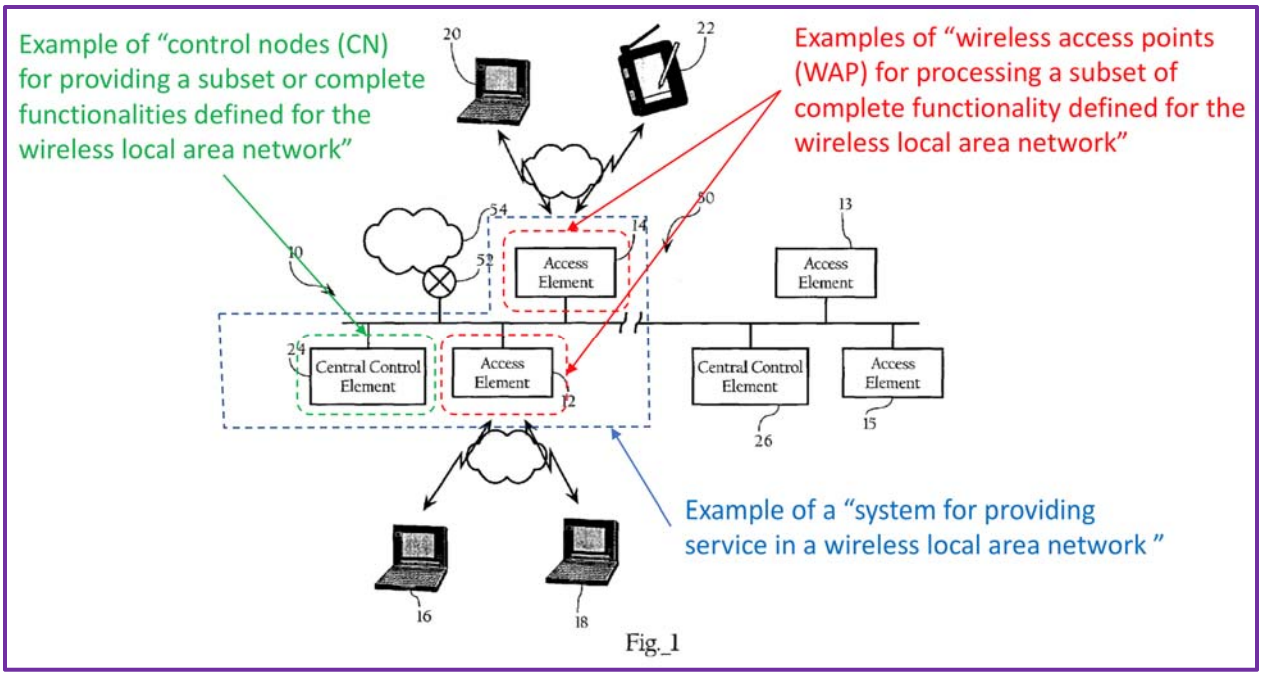
Calhoun discloses a new "system architecture" where a "central control element manages and controls one or more access elements," so that the "access elements perform real-time communication functions," while the "central control element manages the connection between the access element and one or more 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 system for providing service in a wireless local area network comprising:

If the preamble is limiting, Calhoun discloses it expressly or inherently. Calhoun discloses a system "facilitating the deployment of managed access points in a wireless network system," with Figure 1 disclosing a WLAN 10 that includes "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, ¶¶267-268.



[1a] a single or plurality of wireless access points (WAP) for processing a subset of complete functionality defined for the wireless local area network;

Calhoun discloses this limitation explicitly or inherently. Calhoun's wireless LAN includes "access elements 12-15 for wireless communication with remote client elements". EX-1005, 3:13-15. These "access elements perform real-time communication functions, such as data transfer and acknowledgements" but without "manag[ing] the connection between the access element and one or more wireless client devices." EX-1005, 2:6-10, 2:65-3:1; EX-1012, ¶279. A POSA would understand that these "access elements" are "managed access points." EX-1012, ¶278; EX-1005, 1:17-20, 2:26-32.

These access elements "are coupled via communication means using a wireless local area network (Wlan) protocol (e.g., IEEE 802.11a or 802.11b, etc.) to

the client remote elements 16, 18, 20, 22." EX-1005, 3:27-30. These access elements do not "perform link layer management functions, such as authentication and association" for "the wireless LAN management messages passed on from the client remote elements," but instead "provide immediate acknowledgement of the communication of those messages without conventional processing thereof." EX-1005, 3:43-46, 3:51-58; EX-1012, ¶280.

Thus, a POSA would understand that Calhoun discloses one or more WAPs, such as the "managed access points" or "access elements." These access elements are "for processing a subset of the complete functionality defined for the wireless local area network," such as "operating in 802.11 wireless networks" but not other network functionality, *e.g.*, "link layer management functions, such as authentication and association." EX-1012, ¶281; EX-1005, 3:43-58.

[1b] a single or plurality of control nodes (CN) for providing a subset or complete functionalities defined for the wireless local area network; and

Calhoun discloses this limitation explicitly or inherently. Calhoun's wireless LAN includes "a central control element" that "manages and controls one or more access elements." EX-1005, 2:1-6, 2:65-3:1. While the "access elements perform real-time communication functions, such as data transfer and acknowledgements, [] the central control element manages the connection between the access element and one or more wireless client devices." EX-1005, 2:6-10. For example, Calhoun discloses in Figure 1 a WLAN with "central control elements 24, 26 for controlling

and managing the wireless connections between the access elements 12-15 and the remote client elements." EX-1005, 3:10-17, Fig. 1. These "central control elements," "perform link layer management functions, such as authentication and association" for "the wireless LAN management messages passed on from the client remote elements." EX-1005, 3:44-46, 3:51-58, 9:1-2; EX-1012, ¶¶292-294.

A POSA would understand that Calhoun's "central control elements" are CNs that "provid[e] a subset or complete functionalities defined for the wireless local area network," such as "operating in 802.11 wireless networks" *e.g.*, "link layer management functions, such as authentication and association". EX-1012, ¶295.

[1c] a negotiation unit for the single or plurality of WAPs to dynamically negotiate with the control node for a secure connection and function split arrangement;

Calhoun discloses this limitation explicitly or inherently. Calhoun discloses: [(i)] a "negotiation unit" for the single or plurality of WAPs and this negotiation unit dynamically negotiates with the control node for [(ii)] a secure connection and [(iii)] a function split arrangement.

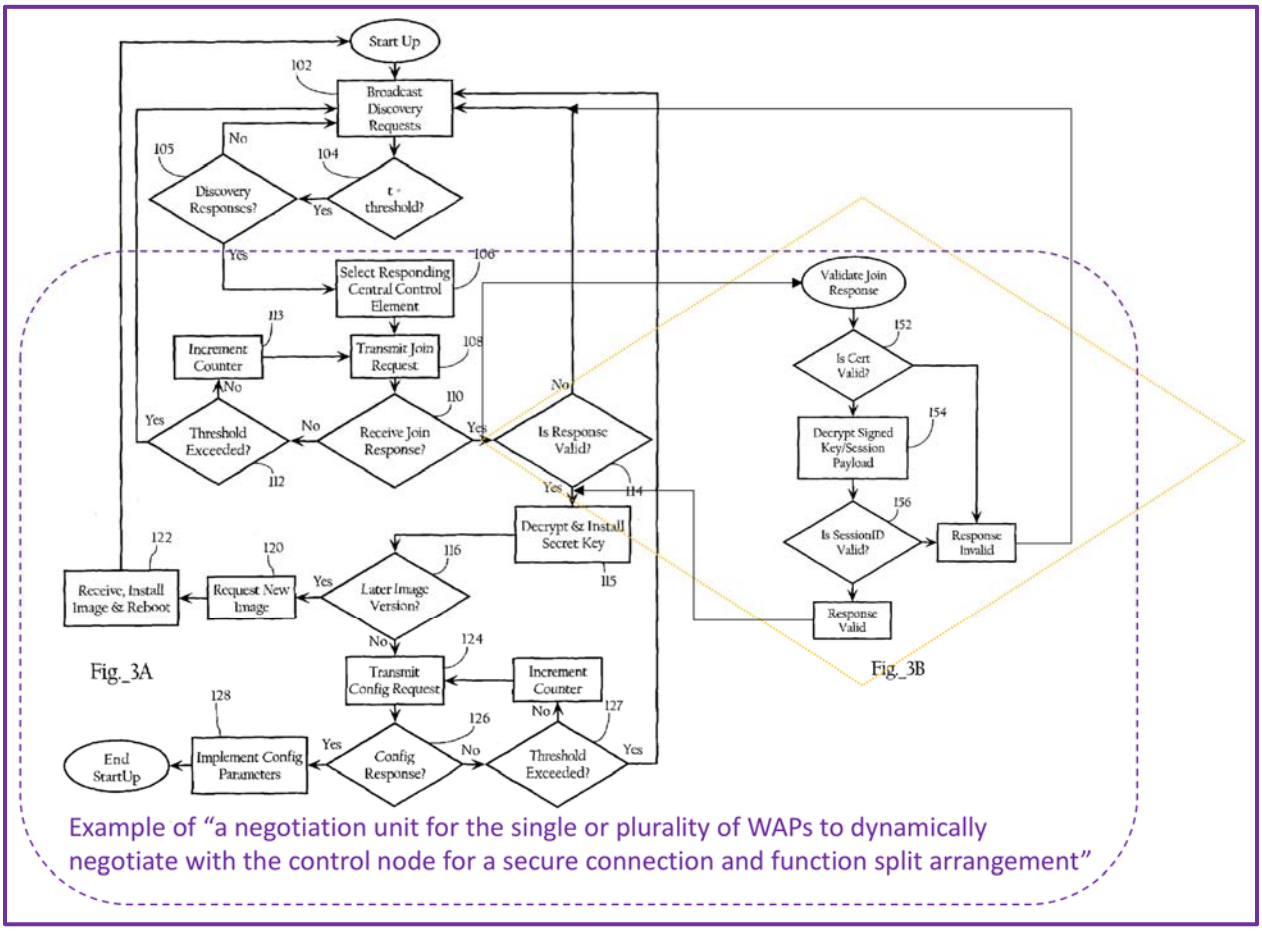
i. "negotiation unit"

Calhoun's "central control element 24 provides processing to dynamically configure a wireless Local Area Network of a system." EX-1005, 3:47-49. Calhoun describes a "Light-Weight Access Point Protocol (LWAPP)" 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," and "[d]uring the joinder phase, the access element and a selected central control element authenticate one another and establish cryptographic keys for use in encrypting subsequent communications." EX-1005, 4:37-42. The "configuration phase involves the configuration of the access element with, for example, operational parameters and, potentially, new software images." EX-1005, 4:42-45; EX-1012, ¶¶306-313, 317-319.

Calhoun also makes explicit reference to "implementing the discovery, joinder and configuration phases of LWAPP," as described in Figures 3A/3B. EX-1012, ¶¶307, 314, 324; EX-1005, 5:14-17. As shown in Dr. Negus's annotations of composite Figure 3A/3B, Calhoun discloses a "negotiation unit for the single or plurality of WAPs" within each "access element" and this negotiation unit is configured to dynamically negotiate with the control node for a secure connection and function split arrangement. EX-1012, ¶325. A POSA would understand that Calhoun's joinder and configuration phases are collectively referred to as a "Capability Negotiation Phase." EX-1008, 23. As Petitioner explains below in sub-sections [1c][(ii)] and [1c][(iii)] below, a POSA would understand that Calhoun's disclosure of dynamically configuring during these joinder and configuration phases of LWAPP is interchangeable with the term "dynamically negotiate" and that

Calhoun's disclosures in annotated Figures 3A/3B are interchangeable with a negotiation unit. EX-1012, ¶326.



If PO argues and the Board finds this limitation is a means-plus-function limitation, Petitioners contend that the closest disclosed structure for performing the claimed functions is "steps 205, 207, 209, 211, 213, 215, 219 and 221 in Figure 2 and the applicable text in 8:62-10:53."

Calhoun discloses the structure for a "negotiation unit" as shown in the annotated composite of Figures 3A/3B above. EX-1012, ¶360. Petitioner explains

below how Calhoun's Figures 3A/3B disclosures perform the claimed functions in the same way as the '531 Patent to achieve the same result.

ii. "secure connection"

Calhoun explains that, "[a]t startup, access element 15 broadcasts or multicasts discovery requests ... to identify central control elements." EX-1005, 5:20-23. The "central control elements 24, 26 receive the discovery requests" and "transmit discovery responses to access element 15," and "[e]ach discovery response comprises a central control element identifier and a load parameter." EX-1005, 5:28-32. The "load parameter includes 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; EX-1012, ¶309.

After transmitting a discovery request, each 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" based on criteria such as "the responding central control element that reports the smallest load (e.g., the smallest number of access elements under management)." EX-1005, 5:52-63; EX-1012, ¶310.

After selecting a central control element, "access element 15 transmits a join request to the selected central control element," and this request includes "an access

element identifier, a digital certificate, and a session identifier" and "other fields, such as the WLAN MAC address, [and] software image version." EX-1005, 6:1-8. The digital certificate includes "a name or other identifier, a serial number, the LAN and/or WLAN MAC address associated with access element 15, a copy of the public key of the access element (used for encrypting messages and digital signatures), [etc.]." EX-1005, 6:16-23; EX-1012, ¶311.

Next, the "central control element" receives the join request and "authenticates the digital certificate in the join request" and "composes a join response and transmits it to access element 15." EX-1005, 6:44-46. The join response includes "cryptographic keys," and the "digital certificate of the central control element". EX-1005, 6:47-51; EX-1012, ¶312. When the access element receives the join response, it validates the join response and, if valid, "decrypts and installs the symmetric cryptographic keys" using the method shown in Figure 3B. EX-1005, 6:64-7:2; EX-1012, ¶313.

A POSA would understand that the "digital certificate" validation and "cryptographic keys" exchange that follows the "discovery phase" discloses that the "access element" of Calhoun (using the "negotiation unit" of Figures 3A/3B) is configured to "dynamically negotiate with the control node for a secure connection." EX-1012 ¶314.

If this limitation is subject to §112, ¶6, the "way" the '531 Patent discloses performing "dynamically negotiat[ing] with the control node for a secure connection" is through "mutual authentication" and "exchanges of security information" between a WAP and a CN, leading the result of "establishment of communication protocols for further exchanges." EX-1001, 8:62-67; EX-1012, ¶361.

Calhoun similarly discloses "dynamically negotiat[ing] with the control node for a secure connection" via "digital certificate validation" and "cryptographic keys" exchange between the access element and the central control element during its joinder phase, leading to the result of "encrypting subsequent communications" during the configuration phase. EX-1005, 4:37-47, 6:1-8, 6:44-51; EX-1012, ¶362. A POSA would understand that Calhoun's "digital certificate validation" and "cryptographic keys" exchange is substantially similar to the '531 Patent's way of "mutual authentication" and "exchanges of security information" between a WAP controller and a CN. EX-1012, ¶363. Further, Calhoun's result of "encryption of subsequent communications" for its configuration phase is substantially similar to the '531 Patent's result of "establishment of communication protocols for further exchanges." *Id.*

iii. "function split arrangement"

Calhoun further discloses that the "negotiation unit" dynamically negotiates a function split arrangement in at least three ways: (1) shifting the division of functionality between the access elements and the central control elements, (2) determining if fragmentation and defragmentation are necessary functions, and (3) an operational parameters exchange.

First, Calhoun 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". EX-1005, 9:1-2, 9:7-11; EX-1012, ¶322. A POSA would thus understand that Calhoun's disclosure of "dynamically configur[ing]" the WLAN elements necessarily shows that the "access element" is configured to "dynamically negotiate with the control node for a ... function split arrangement." EX-1012, ¶323. For example, the access elements may bridge network traffic from remote clients directly, while transmitting management packets to the central control element instead of transmitting both data and management packets to the central control element. *Id.*

Second, Calhoun explains that "join request transmitted during the joinder phase can also be configured to determine the Maximum Transmit Unit (MTU) for

the link between access element 15 and central control element 24." EX-1005, 7:16-19. For example, the access element may "transmit[] a join request spanning 1596 bytes to determine whether the link layer supports that frame size. This frame size is chosen to determine whether a wireless packet [] can be encapsulated with additional headers and transmitted without requiring fragmentation of the native frame." EX-1005, 7:19-26. If the access element does not receive a response to the join request, it reduces the size of the join request and transmits again. If no response is received after a threshold period of time, the access element returns to the discovery phase. EX-1005, 7:26-32; EX-1012, ¶315.

A POSA would understand that this MTU determination discloses that the "access element" is configured to "dynamically negotiate with the control node for ... a function split arrangement" as recited for this claim element. EX-1012, ¶316. A POSA would understand that "to determine whether a wireless packet ... can be encapsulated with additional headers and transmitted without requiring fragmentation" determines if the "function split arrangement" between the "access element" and the "central control element" needs to include fragmentation/defragmentation. *Id*.

Third, Calhoun's access element "composes and transmits a configuration request to central control element" after updating to a current image version. 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 can be configured through a central control element interface, and further includes "overriding parameters" that the central control element cannot change. EX-1005, 7:51-65; EX-1012, ¶318.

The central control element 24 "receives the configuration request[], and generates the operational parameters for access element 15[], taking into account the overriding parameters identified in the configuration request," and "cannot change" "overriding parameters" except "with a new 'overriding' parameter value." EX-1005, 7:66-8:3, 7:57-62. The central control element then "transmits a configuration response including the operational parameters," and access element 15 receives the configuration response, "optionally stores the operational parameters in non-volatile memory, implements the operational parameters[], and switches to an access point mode" using "the configuration information provided by the central control element." EX-1005, 8:3-17.

A POSA would understand that the "operational parameters" exchange and configuration function of the configuration phase (example three) discloses that the "access element" is configured to "dynamically negotiate with the control node for a ... function split arrangement" because it involves "dynamically configur[ing]" the details of the partial WLAN functionality, as implemented in the "access element" as part of a "function split arrangement" with the "central control element." EX-

1012, ¶320. Further, a POSA would also understand that Calhoun's "operational parameters" exchange and configuration function discloses that the access element is configured to "dynamically negotiate with the control node for a … function split arrangement" because the central control element "generat[ing] the operational parameters for [the] access element" at the central control element while "taking into account the overriding parameters identified in the configuration request" from the access element is describing a management "function" of the WLAN. EX-1012, ¶321. This management function is performed within a "split arrangement" between the central control element and the access element. *Id.* Because Calhoun discloses that "overriding parameters," which the "central control element cannot change" are set at the time of each "configuration" at the access element, this configuration process specification describes a dynamic negotiation between the central control element and the access element. *Id.*

A POSA would thus understand that Calhoun discloses a "negotiation unit for the single or plurality of WAPs," such as the relevant portions of the annotated composite of Figures 3A/3B. EX-1012, ¶325. This negotiation unit is configured to dynamically negotiate with the CN for a secure connection and function split arrangement, such as when the "division of functionality" for the "access elements" and "central control elements" is "dynamically configure[d]" during the "joinder and configuration phases of LWAPP." EX-1012¶326. In the "joinder phase," a "secure

connection" is negotiated as part of the "digital certificate validation" and "cryptographic keys" exchange, and a "function split arrangement" is negotiated during the MTU determination in the joinder phase, the "operational parameters exchange," in the "configuration phase," and the "bridge network functionality" "shift" in a "division of functionality" between the "access elements" and the "central control elements" in the "configuration phase." EX-1012, ¶327.

If PO argues and the Board construes this limitation under §112, ¶6, the "way" the '531 Patent performs the function "dynamically negotiate[ing] with the control node for a ... function split arrangement" is by having "WAP controllers initiate by sending information regarding functional capabilities of the associated WAPs to the chosen CN" so that a CN controller, upon receiving capabilities information, "determines an initial division of WLAN functionality" based on, for example, "a policy that allows each associated WAP to process the functions they are capable of." EX-1001, 9:1-22. Only those functions that a WAP cannot inherently process are left to the CN, and after this division is sent to the WAPs for confirmation, the WAP controllers verify that the division is feasible. EX-1001, 9:27-31, 10:20-25. 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, 9:1-10; EX-1012, ¶364.

Similarly, Calhoun discloses performing the claimed function via a configuration phase where an access element transmits a configuration request to a central control element, and this configuration request includes operational parameters and overriding parameters that describe whether an access element is configured to "bridge network traffic associated with remote clients directly, while transmitting management packets to the central control element" as opposed to transmitting both data and management packets to the central control element. The central control element then generates operational parameters for the access element after considering the access element's parameters in the configuration request, and transmits a configuration response including these operational parameters to the access element, after which the access element implements the operational parameters and switches to an access point mode. EX-1012, ¶365. This leads to the "result" of a division of functionality between the access elements and central control elements that can be shifted when operating in 802.11 wireless networks. *Id.*

A POSA would understand that Calhoun's processing of a "configuration request" that includes operational parameters and overriding parameters including, for example, bridge network traffic functionality between an access element and the central control element, followed by a configuration response that implements configuration parameters is substantially similar to the '531 Patent's way of "sending information" including a CN that "determines an initial division of WLAN

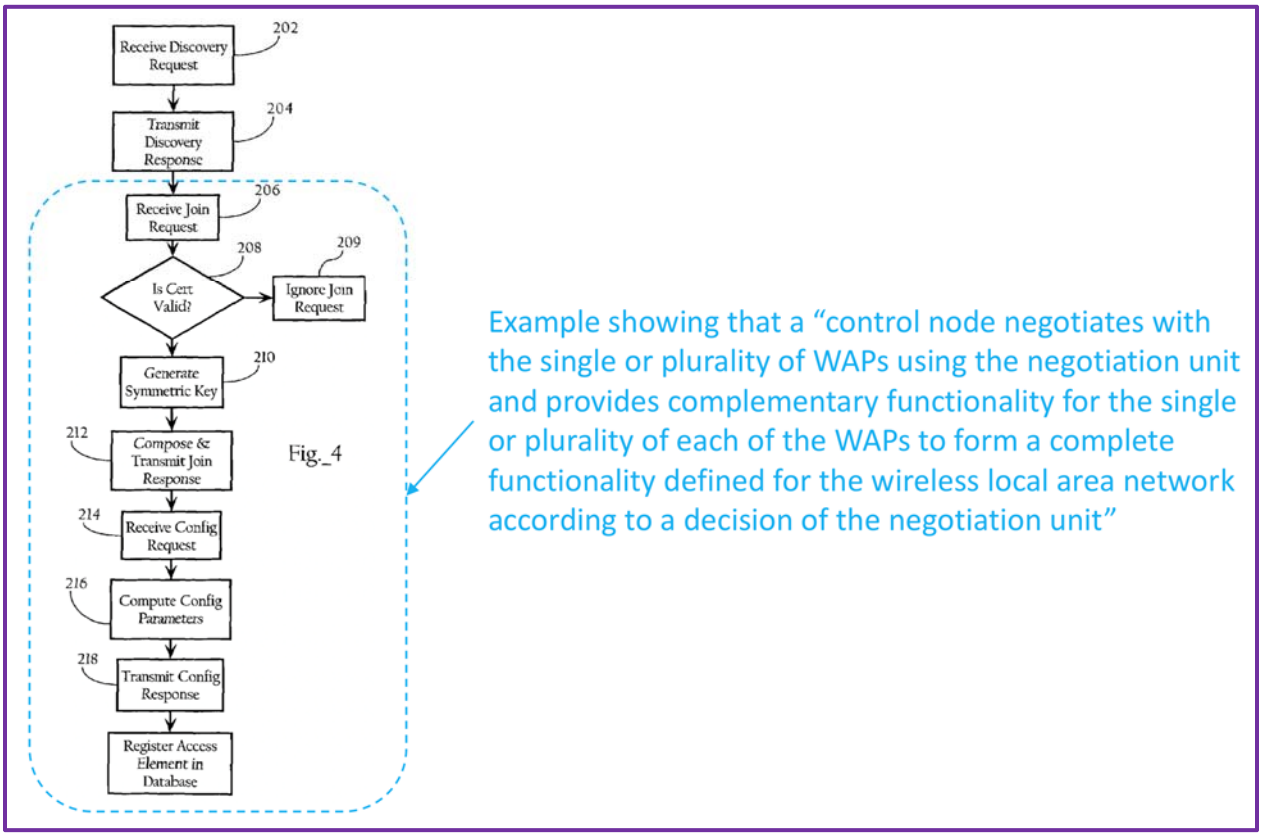
functionality" that is sent to a WAP. EX-1012, ¶366. Calhoun's result of realizing a division of functionality between the access elements and the central control elements that can be shifted is substantially similar to the '531 Patent's result of "a division of WLAN functionality that is consistent with the capabilities of the negotiating entities and are optimal for the operation and management of the whole WLAN." *Id.*

[1d] whereby the control node negotiates with the single or plurality of WAPs using the negotiation unit and provides complementary functionality for the single or plurality of each of the WAPs to form a complete functionality defined for the wireless local area network according to a decision of the negotiation unit.

Calhoun discloses this limitation explicitly or inherently. As discussed for claim [1b], the "central control element" is a CN. EX-1012, ¶372. Figure 4, annotated by Dr. Negus, reflects a method "implemented by central control elements" for supporting LWAPP functionality. EX-1005, 5:17-19. The method of Figure 4 discloses this limitation in at least three ways.

First, and as discussed above for limitation [1c].iii, a POSA would understand that Calhoun's disclosure of "dynamically configur[ing]" the elements of "802.11 wireless networks" shows that the central control element negotiates with the access elements because Calhoun discloses that the division of functionality between the access elements and the central control elements can be shifted, including whether the central control element needs to include either or both of the functions "bridge

network traffic associated with the remote client elements" and process "management packets." EX-1012, ¶376; EX-1005, 4:14-19. For example, when the access elements bridge network traffic from remote clients directly, the central control element need only perform the complementary function of process[ing] management packets to provide complete functionality defined for the wireless network. *Id.* Conversely, when the central control element is bridg[ing] network traffic from remote clients, the central control element must provide that additional complementary function to provide complete functionality defined for the wireless network. *Id.*



Second, as discussed above in limitation [1c].iii, Calhoun's "joinder phase" includes a determination of the MTU for the link between the access element and the central control element. EX-1005, 7:16-19. Identifying the MTU is done to "determine whether a wireless packet ... can be encapsulated with additional headers and transmitted without fragmentation." EX-1005, 7:22-28. This process determines if the function of fragmentation/defragmentation is necessary "to form a complete functionality defined for the wireless local area network." EX-1012, ¶374.

Third, and as discussed above in limitation [1c].iii, a POSA would understand that the "operational parameters" exchange in the configuration phase discloses that the central control element "negotiates with" the access elements to update "operational parameters," such as "channel, transmit power, internal v. external antenna." EX-1005, 7:59-60; EX-1012, ¶375. A POSA would understand that this "operational parameters" exchange involves "dynamically configur[ing]" the details of the partial WLAN functionality implemented in each access element (such as the channel the access element uses for communication with remote client elements) and also involves the complementary functionality of overall WLAN management performed by the central control element. EX-1012, ¶¶318, 375.

Calhoun thus discloses that the CN (the central control element) "negotiates with the single or plurality of WAPs" and "provides complementary functionality for the single or plurality of each of the WAPs to form a complete functionality

defined for the wireless local area network" (including, for example, the MTU determination during the joinder phase; the operational parameters exchange during the configuration phase; and the bridge network traffic shift in division of functionality between access elements and the central control elements in the configuration phase). EX-1012, ¶¶376-377. This is done according to a decision of the "negotiation unit" (the annotated portions of the composite of Figures 3A/3B discussed in [1c] above). *Id.*

b. Claim 7

[7pre] The system according to claim 1, wherein each of the WAPs further comprises:

As discussed in connection with the claim 1 analysis above, Calhoun discloses the limitations of claim 1. EX-1012, ¶¶392-393.

[7a] a discovering unit for discovering an available CN within a specified domain; ... whereby the WAP locates the CN that provides the complementary functionality with regard to defined complete wireless local area network functions with the discovering unit[1]

Calhoun discloses this limitation explicitly or inherently. Calhoun explains that LWAPP includes "functionality directed to initialization and configuration of

[1] Claim 7 recites clauses with a "discovering unit" and a "secure connection negotiating unit" followed by a whereby clause with separate functions for each unit, *i.e.*, (1) a discovering unit for locating the CN, and (2) a secure connection negotiating unit establishing a secure connection with a CN. Petitioners present their analysis of the first unit and function in the whereby clause in [7a], and the second unit and function in [7b].

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.

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. Central control elements receive discovery requests and transmit discovery responses. The access element "selects one of the responding central control elements identified in the discovery responses," and this "selection ... can be driven by a number of different considerations." EX-1005, 5:28-30, 5:52-58. A POSA would understand from this disclosure of a "discovery phase" and "discovery request"/"discovery response" messages that Calhoun discloses that the "access element" is configured for "discovering an available CN within a specified domain." EX-1012, ¶¶396-400.

Calhoun explains that the "division of functionality between the access elements and the central control elements can be shifted." EX-1005, 9:7-11. Annotated Figures 3A/3B further show the dynamically configured division of functionality between access elements and central control elements. EX-1012, ¶¶401-403. Further, as discussed above for claim limitation [1d], the "central control element" is the "CN that provides the complementary functionality with regard to

defined complete wireless local area network functions with the discovering unit." EX-1012, ¶404.

Calhoun thus discloses a "discovering unit" in each WAP (annotated above) that is for "discovering an available CN within a specified domain" such that "the WAP locates the CN ... with the discovering unit" (via the "discovery request" and "discovery response" messages between the "access element" and the "central control elements" in the same virtual subnet during the discovery phase). EX-1012, ¶405. The "central control element" is "the CN that provides the complementary functionality with regard to defined complete wireless local area network functions," as discussed for [1d]. *Id.*

If PO argues and the Board finds this limitation is a means-plus-function limitation, Petitioner states that the closest structure disclosed in the '531 Patent for performing the claimed function of "discovering an available CN within a specified domain" is step 201 in Figure 2 and the applicable text at 8:43-53. EX-1001, 8:43-51; EX-1012, ¶422. The '531 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, 8:43-53; EX-1012, ¶425.

Calhoun discloses structure for a "discovering unit" as shown in the annotated composite of Figures 3A/3B above. EX-1012, ¶424. Calhoun discloses performing the claimed function via a "discovery request" and "discovery response" exchange, leading to the result of "responding central control elements identified in the discovery responses." EX-1005, 5:20-30, 5:52-58; EX-1012, ¶426. A POSA would understand that Calhoun's "discovery request" and "discovery response" exchange is performing the claimed function in the same way as the '531 Patent's transmission of "a specific mutually recognizable message invoking responses from available CNs." EX-1012, ¶427. Further, Calhoun's disclosure of "discovered CNs to associate with" is a substantially similar to the '531 Patent's result of "responding central control elements identified in discovery responses." *Id.*

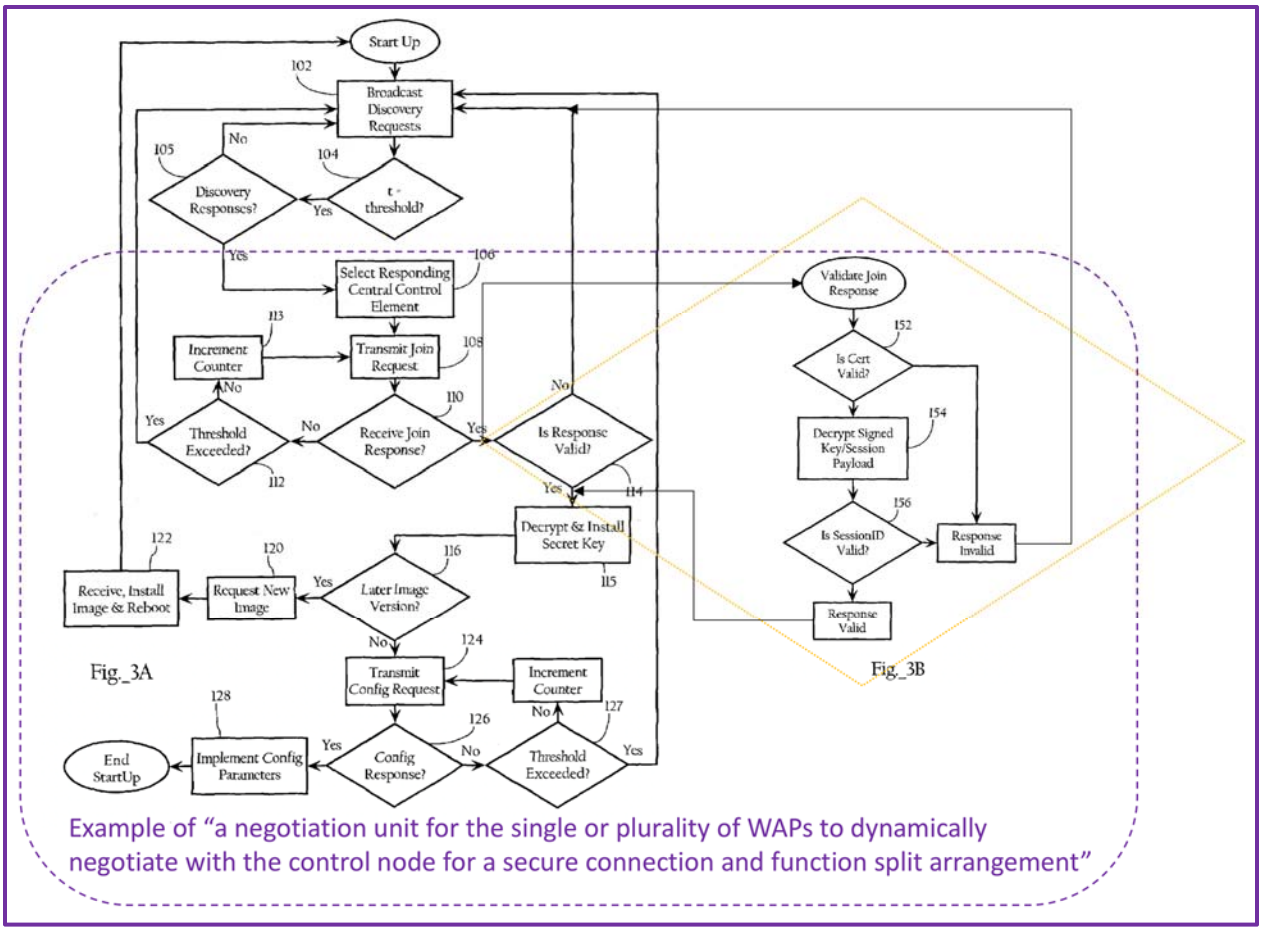
[7b] a secure connection negotiating unit for negotiating a secure connection with a CN that may provide the complementary functionality desired by the WAP; whereby the WAP ... establishes a secure connection with the CN that provides the complementary functionality with the secure connection negotiating unit.

Calhoun discloses this limitation explicitly or inherently. A POSA would understand that the claim 7[b] limitations of "negotiating a secure connection with a CN that may provide the complementary functionality desired by the WAP" and "establish[ing] a secure connection with the CN that provides the complementary functionality with the secure connection negotiating unit" are substantially similar to limitations [1c] and [1d] in claim 1, from which claim 7 depends. EX-1012, ¶431.

Claim [7b] differs in that it requires that the "secure connection negotiating unit" exist in the WAPs, whereas claim 1 did not require any location for its "negotiation unit" so long as it existed in the system. EX-1012, ¶432.[2]

As Petitioner explained for limitations [1c] and [1d] above, Calhoun discloses a "secure connection negotiating unit" in each WAP for negotiating and establishing a secure connection with a CN (such as by "digital certificate validation" and "cryptographic keys" exchange). EX-1012, ¶¶433-434. As discussed above for limitation [7a], this CN "provides the complementary functionality desired by the WAP. EX-1012, ¶435.

[2] While claim 7 also refers to a "secure connection negotiation unit", rather than just the "negotiating unit" of claim 1, the negotiation unit of claim 1 establishes a secure connection and, therefore, the "secure connection" modifying phrase does not appear to create a distinction. Notably, the '531 Patent specification does not refer to either a negotiation unit or a secure connection negotiation unit.



If PO argues and the Board finds this limitation is a means-plus-function limitation, Petitioner states that the closest structure disclosed in the '531 Patent for performing the claimed functions of "negotiating a secure connection with a CN that may provide the complementary functionality desired by the user" and "establish[ing] a secure connection with the CN that provides the complementary functionality" is steps 205, 207, 209, 211, 213, 215, 219 and 221 in Figure 2 and the applicable text at 8:62-10:53. EX-1001, 8:62-10:53; EX-1012, ¶444. As explained in [1c], the '531 Patent discloses that the way these functions are performed is via "mutual authentication" and "exchanges of security information" between a WAP

controller and a CN, leading to the result of "establishment of communications protocols for further exchanges." EX-1012, ¶¶361, 447.

Calhoun discloses structure for a "secure connection negotiating unit," identified as a "negotiating unit" in the annotated composite of Figures 3A/3B above. EX-1012, ¶446. Similarly, Calhoun performs the claimed functions via "digital certificate" validation and "cryptographic keys" exchange between access elements and the central control element, leading to the result of "encrypting subsequent communications" during Calhoun's configuration phase. EX-1012, ¶448. A POSA would understand that Calhoun's "way" of digital certificate validation and cryptographic keys exchange is substantially similar to the '531 Patent's way of mutual authentication and exchanges of security information between a WAP controller and a chosen CN. EX-1012, ¶449. A POSA would also understand that Calhoun's result of "encrypting of subsequent communications" for the subsequent configuration phase is substantially similar to the '531 Patent's result of "establishment of communication protocols for further exchanges." *Id.*

c. Claim 13

[13pre] A method for providing service in a wireless local area network (WLAN) that allows a defined WLAN function split between a wireless access point (WAP) and a single or plurality of Control Nodes (CN) comprising the steps in which:

Claim 13 is a method claim with steps that correspond to the limitations of Claim 1. If limiting, a POSA would understand that Calhoun discloses this preamble

explicitly or inherently because, as discussed for [1c] and [1d] above, Calhoun discloses "providing service" "in a wireless local area network" "that allows a defined WLAN function split between a wireless access point (WAP) and a single or plurality of control nodes." EX-1012, ¶¶457-461.

[13a] a subset of WAPs processes a total of a subset of functionality of the subset of WAPs defined for the WLAN;

Calhoun discloses this limitation explicitly or inherently for the same reasons discussed in the analysis above related to limitation [1a]. EX-1012, ¶¶472-473.

[13b] the WAP dynamically negotiates with a CN for a secure connection and function split arrangement; and

Calhoun discloses this limitation explicitly or inherently for the same reasons discussed in the analysis above related to limitation [1c]. EX-1012, ¶¶485-489.

[13c] the CN provides complementary functionality for each of the WAPs to form a complete functionality defined for the wireless local area network according to a decision in the negotiation step.

Calhoun discloses this limitation explicitly or inherently for the same reasons discussed in the analysis above related to limitation [1d]. EX-1012, ¶¶498-502.

B. Ground 2: Claims 1, 7, and 13 are Obvious over Calhoun in View of CAPWAP and LWAPP and the Knowledge of a POSA

1. CAPWAP

a. Analogous Art

CAPWAP, discussed above 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, ¶¶192-198. CAPWAP also is pertinent to the problem addressed by the '531 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, ¶199.

2. LWAPP

a. Analogous Art

LWAPP, discussed above 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" that allows a router to interoperably control and manage a collection of wireless APs. EX-1006, p.2; EX-1012, ¶¶140-146. LWAPP is pertinent to the problem addressed by the '531 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, ¶147.

3. Motivation to Combine Calhoun with CAPWAP and LWAPP

A POSA would be highly motivated to combine Calhoun, LWAPP and CAPWAP. EX-1012, ¶241.

First, Calhoun, LWAPP, and CAPWAP all relate to IEEE 802.11 networks. EX-1005, 1:44-57, 3:27-32; EX-1006, p.2; EX-1008, p.10; EX-1012, ¶242.

Second, Calhoun, LWAPP, and CAPWAP are directed to solving deployment challenges for IEEE 802.11 networks and they propose similar solutions. EX-1012, ¶¶243, 247, 248. 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 ¶¶244, 249. 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, ¶¶245, 250. Similarly, CAPWAP discloses a WLAN architecture with "lightweight Access Point[s]" and "AP Controllers or AR (Access Router)" that "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 configuration phases. EX-1008, pp.2, 9, 23; EX-1012, ¶¶246, 251.

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, ¶¶253-254, 257; 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, ¶255; 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, ¶256; EX-1008, pp.28,30, 31.

Fourth, additional prior art would have motivated a POSA to combine Calhoun, LWAPP, and CAPWAP. EX-1012, ¶258. *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-1012, ¶¶259-263.

A POSA would thus have been highly motivated to combine Calhoun, LWAPP, and CAPWAP, and would have had a reasonable expectation of success in combining their teachings. 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, ¶¶249-252. 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, ¶257.

4. Detailed Application to the Challenged Claims

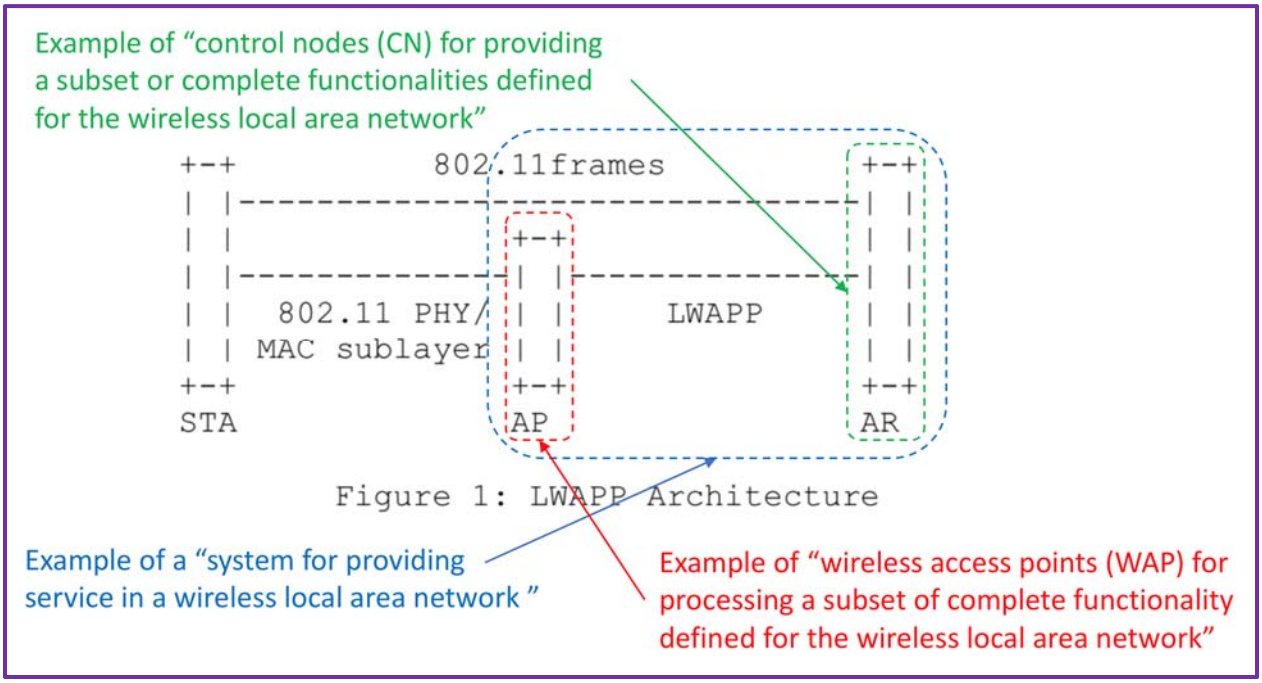
a. Claim 1

[1pre] A system for providing service in a wireless local area network comprising:

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

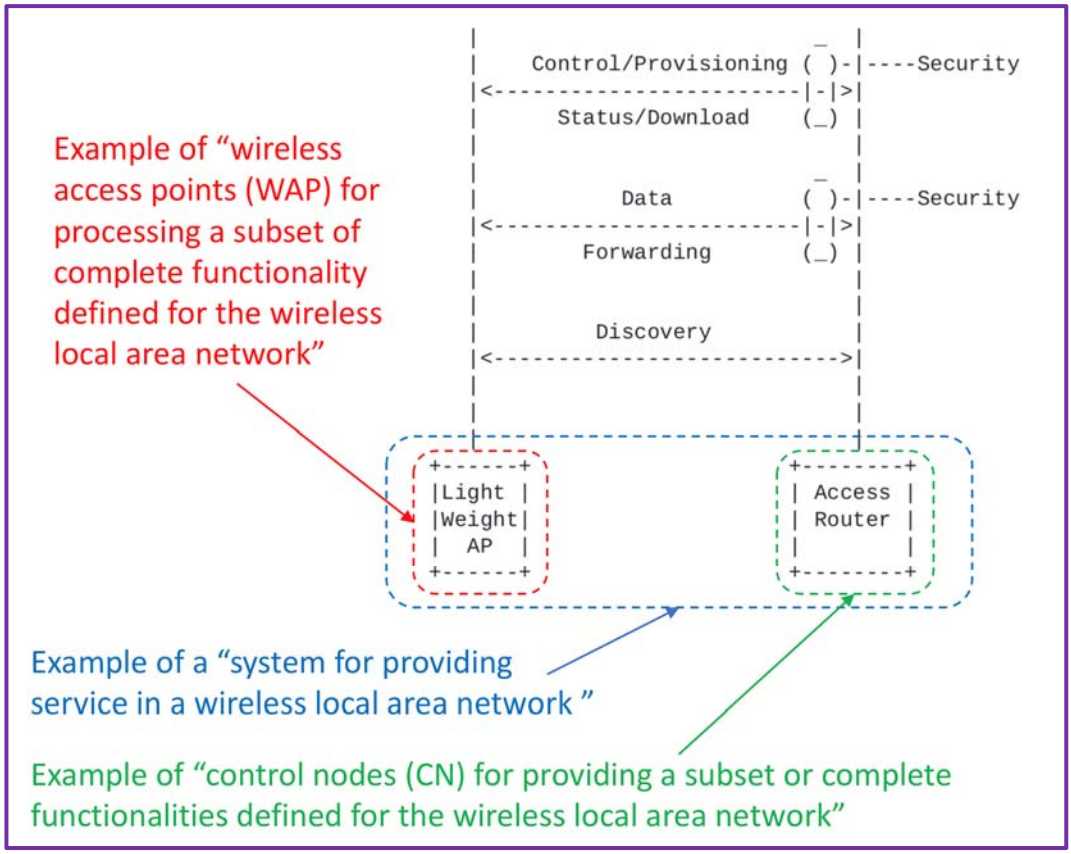
Calhoun discloses the preamble as discussed in Ground I. §V.A.2.a.[1pre].

Likewise, LWAPP discloses a 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 below by Dr. Negus, illustrates LWAPP's system for providing service. EX-1012, ¶¶270-272.



Similarly, CAPWAP's stated purpose is "to define the framework reflecting the architectural trend that delegates and aggregates the selected WLAN functions and services" from Access Points (APs) to AP Controllers (ARs) "to enhance WLAN resource management" and thus "provide a secure protocol to enable AP-to-AR communications and AP provisioning and management." EX-1008, p.4. Figure

1, annotated below by Dr. Negus, illustrates CAPWAP's system for providing service. EX-1012, ¶¶273-275.



[1a] a single or plurality of wireless access points (WAP) for processing a subset of complete functionality defined for the wireless local area network;

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

Likewise, LWAPP 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. This approach 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. LWAPP further explains that "[t]he AP forwards all 802.11 frames received to the AR via the LWAPP protocol, which processes the frames." EX-1006, p.7; EX-1012, ¶¶283-285.

CAPWAP also "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. CAPWAP explains that the "Access Point 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; EX-1012, ¶¶287-288.

LWAPP and CAPWAP thus both disclose "a single or plurality of wireless access points" ("simple APs" in LWAPP and "LAPs" in CAPWAP) for "processing a subset of complete functionality defined for the wireless local area network" (functions other than "bridging, forwarding, authentication, encryption and policy enforcement" in LWAPP and only "those [functions] 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" in CAPWAP). EX-1012, ¶¶285, 288.

[1b] a single or plurality of control nodes (CN) for providing a subset or complete functionalities defined for the wireless local area network; and

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

As discussed in [1a] above, LWAPP discloses a "single or plurality of control nodes (CN)" (the "AR" of LWAPP) that are "for providing a subset or complete functionalities defined for the wireless local area network" (such as performing, the bridging, forwarding, authentication, encryption and policy enforcement functions for a WLAN). EX-1012, ¶¶283-284, 297-298.

CAPWAP uses the terms AR, AC and AB synonymously but states that "AC is assumed to be the generic term for the entity with which an AP registers or associates." EX-1008, p.5. CAPWAP describes "a flexible balance of such [AP] functions ... to be meaningfully split between lightweight Access Point (LAP)" and "AP Controllers or AR (Access Router)." EX-1008, p.2. CAPWAP explains that "Access Controller Functions and Services" may include "those dealing with the management and control aspects of an 802.11 AP" such as "the distribution system services, in addition to authentication and deauthentication services." EX-1008, pp.14-15.

CAPWAP also discloses CNs (such as the AR, AC, and AB) that are "for providing a subset or complete functionalities defined for the wireless local area network" (such as the "management and control aspects of an 802.11AP" including

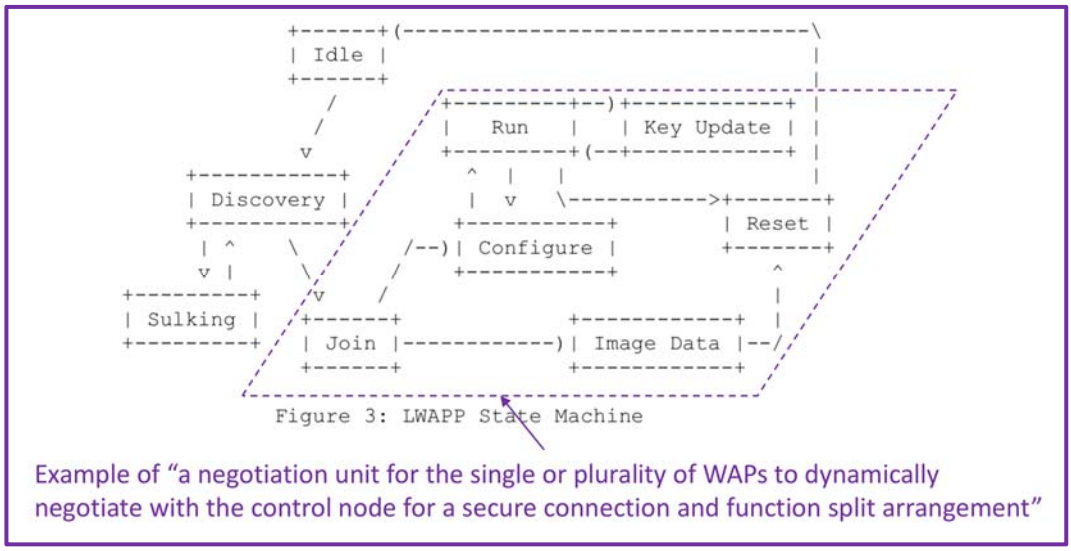
the "the distribution system services, in addition to authentication and deauthentication services"). EX-1012, ¶¶300-302.

[1c] a negotiation unit for the single or plurality of WAPs to dynamically negotiate with the control node for a secure connection and function split arrangement;

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

i. "negotiation unit"

Likewise, Figure 3 of LWAPP shows a "state diagram" that "represents the lifecycle of an AP-AR session." EX-1006, pp.15-16. A POSA would understand that this state diagram discloses a "negotiation unit for the single or plurality of WAPs" within each AP that is configured "to dynamically negotiate with the control node for a secure connection and function split arrangement." EX-1012, ¶339.



Thus, LWAPP discloses a "negotiation unit for the single or plurality of WAPs" (*see* annotated Figure 3 above). EX-1012, ¶341. As explained below, this

negotiation unit is configured to "dynamically negotiate with the control node for a secure connection and function split arrangement" (during the join phases, certificate validation, public key cryptography, and maximum transmit unit discovery, and during the configuration phase, and configuration provisioning). *Id*.

If this limitation is determined to be a means-plus-function limitation, the closest corresponding structure in the '531 Patent is "steps 205, 207, 209, 211, 213, 215, 219 and 221 in Figure 2 and the applicable text in 8:62-10:53." EX-1012, ¶358. Under that construction, Calhoun's Figures 3A/3B are the structure that performs the claimed functions for this limitation, as explained in Ground I above. EX-1012, ¶360. As explained below, LWAPP and CAPWAP also disclose the claimed functions, and a POSA would understand that Calhoun's Figures 3A/3B are structure for performing the claimed functions.

ii. "secure connection"

LWAPP discloses "a discovery phase" where the "APs send a Discovery Request frame" and any Access Router "receiving that frame [] respond[s] with a Discovery Reply." The 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. 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 "dynamically negotiate with the control node for a secure connection." EX-1012, ¶¶333-334.

CAPWAP describes "a flexible balance" of AP functions "to be meaningfully split between lightweight Access Point (LAP)" and "AP Controllers or AR (Access Router)." EX-1008, p.2. 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 "dynamically negotiate with the control node for a secure connection." EX-1012, ¶¶347-348.

If this limitation is determined to be a means-plus-function limitation, Calhoun discloses this limitation for the reasons explained in Ground I. EX-1012, ¶¶362-363.

iii. "function split arrangement"

CAPWAP explains that there is market support for a WLAN architecture that "moves much of the functions that would reside in a traditional [AP] to a centralized [AR]." EX-1008, p.9. It explains that terminating 802.11 management frames in the AR is "commonly referred to as 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. In this split AP approach, there is "a module in the AR that understands 802.11 management frames" while using the "LWAPP protocol." EX-1008, p.10; EX-1012, ¶¶343-346.

CAPWAP explains that, "based on [a] negotiated architecture" "[c]onfiguration of an AP includes providing the parameters necessary for the AP to advertise and provide service for one or more WLANs." EX-1008, p.21. These parameters are both "physical," relating to operation of the AP's radio interface, and "logical," relating to the individual WLANs that are provisioned on the AP. EX-

1008, p.21. A POSA would understand that this configuration of parameters in CAPWAP's "Capability Negotiation Phase" discloses that the AP is configured to "dynamically negotiate with the control node for a ... function split arrangement" because these parameters set the details for the partial WLAN functionality implemented in the AP as part of a "function split arrangement,' which CAPWAP describes as a "Split AP," with the "Access Controller." EX-1012, ¶¶349-350.

CAPWAP further summarizes four different architectures in which APs and ARs are linked: (i) "ARCH0" with a "self-contained controller possibly communicating with other APs," (ii) "ARCH1" with APs that "defer all WLAN functions other than real-time services" using a "vertical (real-time frontend AP and aggregated backend AC) functional distribution," (iii) ARCH2 with APs that "shift some normally real-time functions as well to the backend," and (iv) ARCH3 with an AC acting as "a single 'AP-switch'" where all connected APs are treated as smart antennas. Ex-1008, p.10. That such architectures have varied scope and limitations "underscores the argument to provide a negotiable interface protocol." EX-1008, p.11.

CAPWAP also discloses that, after the AP discovers available ARs, it "enters into a capabilities exchange phase with the candidate ACs" and "[i]f the architectural types match during the exchange – the AP registers with the AC and configures itself based on the policies it derives from the AC after mutually authenticating with the

AC." EX-1008, p.23. CAPWAP explains that the "capabilities negotiated by architectural type match will decide the applicable API's between AP and AC." EX-1008, p.23.

A POSA would understand that CAPWAP's "negotiable interface protocol" that determines the "applicable APIs between AP and AC" based upon the "capabilities negotiated by an architectural type match" during a "capabilities exchange phase" describes an "Access Point" that is configured to "dynamically negotiate with the control node ... for a function split arrangement." EX-1012, ¶354. This "Split AP" can be any one of a "classic AP" with "a self-contained controller," an AP that "defer[s] all WLAN functions other than real-time services" to the AC, or an AP/AC combination that also "shift[s] some normally real-time functions" to the AC. *Id.*

LWAPP explains that the Join Request provides an MTU discovery mechanism to determine "whether there is support for the transport of jumbo frames between the AP and [its] AR." "If support for jumbo frames is not present, the LWAPP frames will be fragmented to the maximum length discovered to be supported by the layer 2 network." EX-1006, p.10. As in Calhoun, the initial join request is set to "1596 bytes" and if a Join Reply is received, "the AP can forward frames without requiring any fragmentation." If a Join Reply is not received, the AP sends a second Join Request with a smaller payload. EX-1006, p.20. The AP keeps

retrying until either a Join Reply is received or a maximum number of retransmissions is reached. EX-1006, p.20; EX-1012, ¶331.

A POSA would understand that this MTU discovery mechanism within the "Join phase" discloses that the "Access Point" is configured to "dynamically negotiate with the control node for ... a function split arrangement" as recited for this claim element. EX-1012, ¶332. A POSA would understand that "to determine whether there is support for the transport of jumbo frames between the AP and [its] AR" determines if the "function split arrangement" between the "Access Point" and the AR needs to include "which frames will be fragmented" (and by extension, "defragmented"). *Id.*

Next, a configuration exchange "will provision the APs," and this "provisioning includes the typical name (802.11 Service Set Identifier, SSID), and security parameters, the data rates to be advertised as well as the radio channel ... to be used." EX-1006, p.10. APs send "Configure Requests ... after receiving a Join Reply" and this request includes the AP's current configuration. EX-1006, p.24. An AR receiving a Configure Request will "respond to the AP with a Configure Response," which "provides an opportunity for the AR to override an AP's configuration." *Id*.

A POSA would understand that the "provisioning" exchange aspects of LWAPP's "configuration phase" also discloses that the "Access Point" is configured

to "dynamically negotiate with the control node for a ... function split arrangement" because both aspects involve overriding the details of the partial WLAN functionality implemented in each "Access Point" as part of a "function split arrangement" with the "Access Router." EX-1012, ¶338.

Thus, Calhoun/CAPWAP/LWAPP discloses the claimed "negotiation unit" that "dynamically negotiate[s] with the control node for a ... function split arrangement" (LWAPP's MTU discovery mechanism and provisioning, as well as CAPWAP's providing configuration of parameters, and determining the "applicable APIs between AP and AC" based upon "capabilities negotiated by architectural type match" using a "negotiable interface protocol"). EX-1012, ¶¶338, 339, 350, 354.

If this limitation is subject to §112, ¶6, the "way" the '531 Patent performs the function "dynamically negotiate[ing] with the control node for a ... function split arrangement" is described in Ground I and equally applies here.

Similarly, CAPWAP discloses a "negotiable interface protocol" that determines applicable APIs between AP and AC based upon "capabilities negotiated by architectural type match" during a "capabilities exchange phase" for an AP and an AC, and this discloses the function "dynamically negotiate with the control node for ... a function split arrangement." EX-1012, ¶369. A POSA would thus understand that the structure in Calhoun for performing the claimed function, in Figures 3A/3B, when combined with LWAPP and CAPWAP, would perform the

claimed function in substantially the same way as disclosed in the '531 Patent, to achieve substantially the same result. EX-1012, ¶360, 362-363, 369.

[1d] whereby the control node negotiates with the single or plurality of WAPs using the negotiation unit and provides complementary functionality for the single or plurality of each of the WAPs to form a complete functionality defined for the wireless local area network according to a decision of the negotiation unit.

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

Likewise, as discussed in [1b] above, CAPWAP's "Access Controller" or "Access Router" is a CN. EX-1012, ¶386. A POSA would understand that the configuration of parameters in CAPWAP's "Capability Negotiation Phase," discussed in [1c], discloses that the Access Controller "negotiates with the single or the plurality of WAPs ... and provides complementary functionality for the single or plurality of each of the WAPs to form a complete functionality defined for the wireless local area network" because the parameters set the details of the partial WLAN functionality in the AP as part of a "Split AP" with the AC that "moves much of the functions that would reside in a traditional access point (AP) to a centralized access router (AR)." EX-1012 ¶387.

Further, CAPWAP's "negotiable interface protocol" that determines the "applicable API's between AP and AC" based upon "capabilities negotiated by architectural type match" during a "capabilities exchange phase" describes that the

AC "negotiates with the single or the plurality of WAPs ... and provides complementary functionality for the single or plurality of each of the WAPs to form a complete functionality defined for the wireless local area network." EX-1012, ¶389. This also is disclosed in CAPWAP through its disclosure of a variable architecture, *i.e.*, Split AP with a self-contained controller, an AP that defers all non-real-time services to the AC, and an AP/AC combination that shifts some normally real-time functions to the AC. EX-1012, ¶388.

As discussed in [1b] above, LWAPP's "AR" is a CN. EX-1012, ¶380. A POSA would thus understand that the "MTU discovery mechanism," discussed in [1c], discloses that the AR "negotiates with the single or plurality of WAPs" to "provide[] complementary functionality for the single or plurality of each of the WAPs to form a complete functionality defined for the wireless local area network" because determining "whether there is support for the transport of jumbo frames between the AP and [its] AR" determines if forming "a complete functionality defined for the wireless local area network" needs to include the functions of "fragmentation" and "defragmentation" as "complementary functionality for the single or plurality of each of the WAPs." EX-1012, ¶381.

Further, the "provisioning" exchange in LWAPP's "configuration phase" discussed above in [1c] discloses that the AR "negotiates with the single or plurality of WAPs" to "provide[] complementary functionality for the single or plurality of

each of the WAPs to form a complete functionality defined for the wireless local area network." EX-1012, ¶382. The provisioning exchange involve overriding the details of the partial WLAN functionality implemented in the AP "to form a complete functionality defined for the wireless local area network" that includes "complementary functionality for the single or plurality of each of the WAPs." EX-1012, ¶382. This provisioning exchange comes via application of LWAPP's Figure 3 state machine which Petitioner previously explained contained the "negotiation unit." EX-1012, ¶383.

a. Claim 7

[7pre] The system according to claim 1, wherein each of the WAPs further comprises:

For the reason explained in [1pre], Calhoun/CAPWAP/LWAPP renders this claim limitation obvious. EX-1012, ¶392.

[7a] a discovering unit for discovering an available CN within a specified domain; [...] whereby the WAP locates the CN that provides the complementary functionality with regard to defined complete wireless local area network functions with the discovering unit

Calhoun/CAPWAP/LWAPP renders this limitation obvious. Calhoun discloses [7a] as discussed in claim [7a] Ground I. §V.A.2.b.[7a].

Likewise, LWAPP's protocol begins with a "discovery phase" where "APs send a Discovery Request frame, causing any Access Router (AR)[], receiving that frame to respond with a Discovery Reply." EX-1006, p. 10. The AP "will select an AR with which to associate" from the Discovery Replies received. EX-1006, p. 10.

LWAPP explains that the "Discovery Request is used by the AP to automatically discovery potential ARs available in the network." EX-1006, p. 18. The AR responds with a "Discovery Reply sent to the address in the source address of the received discovery request." EX-1006, p. 19.

Further, "[w]hen an AP receives a Discovery Reply, it MUST wait for an interval ... for receipt of additional discovery replies." EX-1006, pp. 19-20. After that internal 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. LWAPP further explains that, "when run over Ethernet, the LWAPP protocol is restricted to a specific Ethernet segment" and the "AR discovery mechanism" is "for the Discovery Request message to be transmitted to a broadcast address." EX-1006, p. 54.

A POSA would understand that the Discovery Request/Discovery Response exchange between AP and AC within a specific Ethernet segment discloses that the AP is configured for "discovering an available CN within a specified domain." EX-1012, ¶412. Further, as discussed in [1c], Figure 3 provides a state diagram that represents the lifecycle of an AP-AR session. A POSA would understand that Figure 3 discloses a "discovering unit" within each AP, as shown in the below annotation by Dr. Negus. *Id*.

LWAPP thus discloses a "discovering unit" that "each of the WAPs further comprises" (in the above annotation of Figure 3) that is for "discovering an available CN within a specified domain" such that the "WAP locates the CN ... with the discovering unit" (such as the Discovery Request/Discovery Response exchange between AP and AC within a "specific Ethernet segment during the "discovery phase"), where the "CN ... provides the complementary functionality with regard to defined complete wireless local area network functions" (the AC discussed above in claim [1d]). EX-1012, ¶415.

CAPWAP 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. CAPWAP explains that, after discovering "available ARs[,] the AP enters into a capabilities exchange phase with the candidate ACs." EX-1008, p. 23. If "architectural types match during the exchange, the AP registers with the AC and configures itself based on the policies it derives from the AC after mutually authenticating with the AC." EX-1008, p. 23.

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 AP is configured for discovering an available CN within a specified domain. EX-1012, ¶419.

If this limitation is subject to §112, ¶6, as stated in Ground I, the structure in the '531 patent for performing the claimed function of "discovering an available CN within a specified domain" is step 201 in Figure 2 and the applicable text at 8:43-51. EX-1001, 8:43-51; EX-1012, ¶422.

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, ¶424. Further, CAPWAP discloses "automatic discovery" between the AP and the AC/AR within the AC/AR's domain, and so Calhoun discloses the function of "discovering an available CN within a specified domain." EX-1012, ¶429. A POSA would thus understand that the structure in Calhoun for performing the claimed function, in Figures 3A/3B, when combined with LWAPP and CAPWAP, would perform the claimed function in substantially the same way as disclosed in the '531 Patent, to achieve substantially the same result. EX-1012, ¶¶426-429.

[7b] a secure connection negotiating unit for negotiating a secure connection with a CN that may provide the complementary functionality desired by the WAP; whereby the WAP [...] establishes a secure connection with the CN that provides the complementary functionality with the secure connection negotiating unit.

Calhoun/CAPWAP/LWAPP renders this limitation obvious.

Calhoun discloses [7b] for the reasons discussed with respect to limitations [1c] and [1d] in Ground I. §V.A.2.b.[7b].

Likewise, as discussed above in [1c], LWAPP discloses a "Join phase" with certificate validation and "public key cryptography" exchange between an AP and a CN. As discussed above in [1d], LWAPP discloses an "MTU discovery mechanism," and a "provisioning exchange." A POSA would understand that LWAPP discloses a "secure connection negotiating unit" (such as the annotated negotiation unit in Figure 3) that is for "negotiating a secure connection with a CN" and/or for "establish[ing] a secure connection with the CN" (via certificate validation and "public key cryptography exchange" in the Join phase), where the "CN" is both "a CN that may provide the complementary functionality desired by the WAP" and "the CN that provides the complementary functionality" (such as AR described in [1d] for the MTU discovery mechanism, and provisioning exchange). EX-1012, ¶¶437-438.

As discussed above in [1c], CAPWAP discloses a "Capability Negotiation Phase" that includes at least "authenticat[ing]" by "cryptographically secure binding." As discussed above in [1d], CAPWAP discloses that the AC determines the "applicable API's between AP and AC" based upon "capabilities negotiated by architectural type match." A POSA would understand that CAPWAP discloses an "Access Point" that is for "negotiating a secure connection with a CN" and/or establish[ing] a secure connection with the CN" (such as the "Capabilities Negotiation Phase" that includes "authenticat[ing]" by "cryptographically secure

binding"), where the "CN" is both "a CN that may provide the complementary functionality desired by the WAP" and "the CN that provides the complementary functionality" (such as the AC determining "applicable API's between AP and AC" based upon "capabilities negotiated by architectural type match"). EX-1012, ¶440-441.

As explained in limitations [1c] and [1d] of 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, ¶¶444-446. Further, CAPWAP discloses a "negotiable interface protocol" that determines applicable APIs between AP and AC based upon "capabilities negotiated by architectural type match" during a "capabilities exchange phase" for an AP and an AC. EX-1012, ¶455. A POSA would thus understand that the structure in Calhoun for performing the claimed function, in Figures 3A/3B, when combined with LWAPP and CAPWAP, would perform the claimed function in substantially the same way as disclosed in the '531 Patent, to achieve substantially the same result. EX-1012, ¶¶448-449, 455.

b. Claim 13

[13pre] A method for providing service in a wireless local area network (WLAN) that allows a defined WLAN function split between a wireless access

point (WAP) and a single or plurality of Control Nodes (CN) comprising the steps in which:

If the preamble is limiting, Calhoun/CAPWAP/LWAPP renders it obvious for the reasons explained with respect to limitations [1pre], [1c] and [1d] above, EX-1012, ¶¶462-469.

[13a] a subset of WAPs processes a total of a subset of functionality of the subset of WAPs defined for the WLAN;

Calhoun/CAPWAP/LWAPP renders this limitation obvious for the reasons discussed in [1a]. EX-1012, ¶¶477-482.

[13b] the WAP dynamically negotiates with a CN for a secure connection and function split arrangement; and

Calhoun/CAPWAP/LWAPP renders this limitation obvious for the reasons discussed in [1c]. EX-1012, ¶¶490-495.

[13c] the CN provides complementary functionality for each of the WAPs to form a complete functionality defined for the wireless local area network according to a decision in the negotiation step.

Calhoun/CAPWAP/LWAPP renders this limitation obvious for the reasons discussed in [1d]. EX-1012, ¶¶503-507.

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

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. Specifically, the Petition explains how the primary reference, Calhoun, alone and in combination with the other references, discloses the claimed limitations. The evidence presented, if unrebutted in trial, would plainly lead to a conclusion that one or more claims are unpatentable by a preponderance of the evidence. 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 because no request for stay has been filed in the District Court Litigation (§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 has been 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 this factor weighs 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 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. *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) ("same parties as parallel proceeding" makes factor 5 "neutral").

Under factor 6, other circumstances weigh in favor of institution. The merits of the Petition are particularly strong. For example, each prior art reference discloses the very limitation by which the '531 Patent gained allowance. EX-1002, pp.324, 439; §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.

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 '531 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 '531 Patent was involved in the following pending case, which may be affected by a decision in this proceeding:

Style	Number	Tribunal	Filed
Sovereign Peak Ventures, LLC v. TP-Link Corp. Ltd.	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 (*to seek Pro Hac Vice admission*) 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, 7, and 13 of the '531 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 13,990 words, according to the Microsoft Word[tm] 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 8,045,531 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