

**EXPERT DECLARATION OF DR. KEVIN NEGUS
FOR
INTER PARTES REVIEW OF U.S. PATENT NO. 8,270,384**

TABLE OF CONTENTS

I. INTRODUCTION	3
II. QUALIFICATIONS	5
III. PERSON OF ORDINARY SKILL IN THE ART	12
IV. LEGAL UNDERSTANDING	14
V. THE ‘384 PATENT	20
A. Overview of the ‘384 Patent	20
B. Prosecution File History of the ‘384 Patent	30
C. Asserted Claims and Priority Date	38
D. Objective Indicia of Non-obviousness	38
VI. CLAIM CONSTRUCTION	39
VII. STATE OF THE ART	41
A. Calhoun (Ex. 1005)	42
B. LWAAP (Ex. 1006)	58
C. Network World (Ex. 1007)	71
D. CAPWAP (Ex. 1008)	74
E. IEEE 802.11-1999 (Ex. 1009)	84
VIII. ANTICIPATION AND/OR OBVIOUSNESS OF THE ‘384 PATENT UNDER 35 U.S.C. §§ 102, 103 DUE TO CALHOUN, LWAPP AND/OR CAPWAP	91
IX. CONCLUSION	160

I. INTRODUCTION

1. I, Dr. Kevin Negus, submit this declaration in support of a Petition for *Inter Partes* Review of United States Patent Nos. 8,270,384 (the “384 Patent”), owned by Sovereign Peak Ventures, LLC (“SPV” or “Patent Owner”). I have been retained in this matter by counsel for Hewlett-Packard Enterprise Company (“HP” or “Petitioner”). I understand that Petitioner is the Real Party-in-Interest to this Petition.

2. I make this declaration based upon my personal knowledge. I am over the age of 21 and am competent to make this declaration.

3. The statements herein include my opinions and the bases for those opinions, which relate to at least the following documents of the pending *inter partes* review petition:

- U.S. Patent No. 8,270,384 by H. Cheng et al., entitled “Wireless point that provides functions for a wireless local area network to be separated between the wireless point and one or more control nodes, and method for providing service in a wireless local area network having functions separated between a wireless point and one or more control nodes” (the “384 Patent”) (Ex. 1001).
- File History for U.S. Patent No. 8,270,384 (Ex. 1002).
- U.S. Patent No. 8,045,531 by H. Cheng et al., entitled “System and method for negotiation of WLAN entity” (the “531 Patent”) (Ex. 1003).
- File History for U.S. Patent No. 8,045,531 (Ex. 1004).
- U.S. Patent No. 7,508,801 by P. Calhoun et al., entitled “Light-weight Access Point Protocol” (“Calhoun”) (Ex. 1005).
- Internet-Draft draft-calhoun-seamoby-lwapp-03 by P. Calhoun et al., entitled “Light Weight Access Point Protocol (LWAPP)” (“LWAPP”) (Ex. 1006).

- Network World article by P. Calhoun et al., entitled “LWAPP brings harmony to WLANs” (“Network World”) (Ex. 1007).
- Internet-Draft draft-mani-ietf-capwap-arch-00 by M. Mani et al., entitled “Architecture for Control and Provisioning of Wireless Access Points (CAPWAP)” (“CAPWAP”) (Ex. 1008).
- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, ANSI/IEEE Std 802.11, 1999 Edition (“IEEE 802.11-1999”) (Ex. 1009).
- IETF RFC 5412 by P. Calhoun et al., entitled “Lightweight Access Point Protocol” (Ex. 1011).
- Plaintiff’s Preliminary Infringement Contentions, Case No. 2:23-cv-00009, Feb. 28, 2023 (Ex. 1013).
- Amended Docket Control Order, Case No. 2:23-cv-00009, Apr. 13, 2023 (Ex. 1014).
- Expert Declaration of Dr. Sylvia Hall-Ellis with respect to Inter Partes Review (Ex. 1015).
- Declaration of Alexa Morris (Ex. 1016).

4. My materials considered for forming my opinions herein have included at least the above-referenced documents.

5. Although I am being compensated for my time at my normal and customary rate in preparing this declaration, the opinions herein are my own, and I have no stake in the outcome of the review proceeding. My compensation does not depend in any way on the outcome of the Petitioner’s petition.

II. QUALIFICATIONS

6. I am qualified by education and experience to testify as an expert in the field of telecommunications. Attached, as Attachment A, is a copy of my resume detailing my experience and education. Additionally, I provide the following overview of my background as it pertains to my qualifications for providing expert testimony in this matter.

7. I am currently a Full Professor of Electrical Engineering at Montana Tech University in Butte, MT. I lead research programs at Montana Tech that include developing communications solutions for extremely low power sensors in challenging locations such as alpine mountains and watersheds including federally-designated wilderness areas and for control of critical infrastructure distributed continentally and globally. I mentor, supervise and teach both senior undergraduate and graduate students of Electrical Engineering in the general fields of telecommunications and networking with an emphasis on wireless systems.

8. In 1988, I received my Ph.D. in Engineering from the University of Waterloo in Canada. The Departments of Electrical Engineering and Mechanical Engineering jointly supervised my Ph.D. research on the modeling of bipolar semiconductor devices. My graduate course work was primarily in Electrical Engineering and included such subjects as semiconductor device physics and fabrication, wireless circuit design, and wireless propagation analysis. For my Ph.D. work, I received the Faculty Gold Medal in 1988 for the best Ph.D. thesis in the entire Faculty of Engineering across all Departments for that year. My Ph.D. thesis research also formed the basis of a paper published in 1989 that won the award for Best Paper in 1989 for the IEEE (Institute of Electrical and Electronic Engineers) journal in which it was published.

9. In 1984 and 1985, respectively, I received the B.A.Sc. and M.A.Sc. Degrees in Mechanical Engineering from the University of Waterloo in Canada. My coursework and research work included, amongst many other topics, extensive embedded firmware development for automation applications and implementation of networks and communications protocols. For my M.A.Sc. Degree research and academic achievements, I received the prestigious University Gold Medal in 1985 for the best Masters thesis in the entire University of Waterloo for that year.

10. In 1986, I joined the Palo Alto Research Center of Fairchild Semiconductor in Palo Alto, CA. At Fairchild, I participated in the development of devices and products for high-speed applications such as wired networking, RISC microprocessors and wireless communications.

11. In 1988, I took the position of Member of the Technical Staff at Avantek, Inc. in Newark, CA. I was hired to develop products for both wireless and wired data networking applications. Some of the components I developed early in my career at Avantek were used for 1st generation wireless local area network (WLAN) products, voice band modem equipment, wired data networking both in the LAN and WAN and 1st generation cellular handsets and base stations based on AMPS or TACS.

12. In 1991, the Hewlett-Packard Company purchased Avantek, Inc. I continued to work for Hewlett-Packard until 1998 in such roles as IC Design Manager, Director of Chipset Development and Principal System Architect. In 1992, Hewlett-Packard assigned me to work on the “Field of Waves” project, which was a major multi-division effort to build WLAN products for mobile computers. The project was cancelled in 1993. However, the work I did on the project was leveraged into producing the world’s first IEEE 802.11 chipset, which my division at Hewlett-Packard first offered for sale in 1994. I led the project to develop and market this

chipset for many early WLAN product companies including Proxim, Symbol (now part of Motorola) and Aironet (now part of Cisco). I also helped coordinate efforts within Hewlett-Packard to guide extensive research projects on WLAN protocols and technology at Hewlett-Packard's central research laboratories in Palo Alto, CA and Bristol, U.K.

13. In 1998, I joined Proxim, Inc. in Mountain View, CA. At that time, Proxim was engaged in the development and sale of wired and wireless products for home and enterprise networking applications based on several different wired and wireless networking protocols. I stayed at Proxim through 2002 and was the Chief Technology Officer for this publicly-traded company at the time of my departure. During my career at Proxim, I led or participated in the development of many WLAN and WWAN products and/or chipsets for network adapters, OEM design-in modules, access points, bridges, switches, and routers that used a wide variety of bus, LAN, or WAN wired interfaces. I have supervised many engineers including those responsible for embedded firmware development to implement various wired and wireless networking, reservation, and security protocols at the MAC layer and above, those responsible for HDL code creation of baseband chips to implement PHY and MAC algorithms, as well as other engineers that developed hardware reference designs, modem algorithms and chipsets.

14. I note that specific to this matter that while I was Chief Technology Officer at Proxim that we developed the world's first WLAN access point controller system, which used the system architecture disclosed in the '384 Patent. This system was sold in the USA starting in 2001.

15. Since 2002, I have been an independent consultant and have provided services to a number of companies including some that have developed IEEE 802.11 products. In particular, from 2002 until 2007 I was Chairman of WiDeFi, Inc. – a company that developed chips and

embedded firmware for 802.11 repeater products based on 802.11a, b, g and draft n amendments. From 2007-2011, I was Chairman of Tribal Shout – a company that delivered IP voice and audio streaming media using VoIP to any cellular or landline phone including those reachable only by the circuit-switched connections such as the PSTN and 2nd generation cellular radio. From 2010-2016, I was Chairman and Chief Technology Officer of CBF Networks, Inc. (dba Fastback Networks) – a company that developed fiber extension products for backhaul of data networks including Wi-Fi, HSPA, CDMA2000, WiMAX and LTE cellular radio systems.

16. I have been a Board Observer on behalf of the venture capital firm Camp Ventures at two companies that develop semiconductor components including one that developed technology specifically to improve the system performance of HSPA and LTE cellular radio systems (Quantance) and another that provides system on a chip (SOC) microcontrollers, OEM design-in modules and firmware with 802.11 and wired interfaces for embedded applications (GainSpan). I have also been a technology and/or business strategy advisor to multiple early stage companies that are developing such products as new wireless communications security systems (AirTight), RFID radio systems (Mojix), time/frequency reference components (SiTime), and application of machine learning to wireless communications (Aira).

17. I have actively monitored or participated in the IEEE 802.11 standards process continuously since 1989. I am a listed contributor to the highly successful IEEE 802.11g standard published in 2003 that describes a wireless communications protocol in use worldwide by over 5 billion devices. In 2002 and 2003, I participated in the IEEE 802.11 Wireless Next Generation Committee that was responsible for launching the 802.11n standards development process.

18. I am an author or co-author of many papers that have been published in distinguished engineering journals or conferences such as those of the IEEE or ASME. An exemplary list of these publications is included in my resume.

19. I am also a former member of the Federal Communication Commission's Technological Advisory Committee as an appointee of then Chairman Michael Powell. I have also served on the Wyoming Telecommunications Council as an appointee of then Governor Jim Geringer after confirmation by the Wyoming State Senate.

20. I am named as an inventor on numerous U.S. patents all of which have related in at least some way to products for wired and/or wireless networks. I believe that the following is a complete list as of this date for my approximately 88 issued U.S. Patents: 4,839,717, 5,111,455, 5,150,364, 5,436,595, 5,532,655, 6,587,453, 7,035,283, 7,085,284, 7,187,904, 8,095,067, D704174, 8,238,318, 8,300,590, 8,311,023, 8,385,305, 8,422,540, 8,467,363, 8,502,733, 8,638,839, 8,649,418, 8,761,100, 8,811,365, 8,824,442, 8,830,943, 8,872,715, 8,897,340, 8,928,542, 8,942,216, 8,948,235, 8,982,772, 8,989,762, 9,001,809, 9,049,611, 9,055,463, 9,178,558, 9,179,240, 9,226,295, 9,226,315, 9,252,857, 9,282,560, 9,313,674, 9,325,398, 9,345,036, 9,350,411, 9,374,822, 9,408,215, 9,474,080, 9,490,918, 9,572,163, 9,577,700, 9,577,733, 9,578,643, 9,609,530, 9,655,133, 9,712,216, 9,713,019, 9,713,155, 9,713,157, 9,876,530, 10,051,643, 10,063,363, 10,129,888, 10,135,501, 10,237,760, 10,284,253, 10,306,635, 10,313,898, 10,356,782, 10,506,611, 10,548,132, 10,700,733, 10,708,918, 10,716,111, 10,720,969, 10,735,979, 10,736,110, 10,764,891, 10,785,754, 10,932,267, 10,966,201, 11,134,491, 11,160,078, 11,166,280, 11,271,613, 11,283,192, 11,303,322, 11,343,060, 11,343,684.

21. I have provided expert testimony, reports or declarations in the cases of *Agere v. Sony* (on behalf of plaintiff Agere), *Linex v. Belkin et al.* (on behalf of defendant Cisco), *CSIRO v. Toshiba et al.* (multiple related cases on behalf of plaintiff CSIRO), *Freedom Wireless v. Cingular et al.* (on behalf of plaintiff Freedom Wireless), *Rembrandt v. HP et al.* (on behalf of defendant HP), *DNT v. Sprint et al.* (on behalf of the defendants Sprint, T-Mobile, US Cellular, Verizon and Novatel), *Teles v. Cisco* (on behalf of defendant Cisco), *WiAV v. HP* (on behalf of defendant HP), *SPH v. Acer et al.* (on behalf of defendants Sony, Nokia, Motorola, Novatel, Sierra and Dell), *LSI v. Funai* (on behalf of plaintiff LSI), *WiAV v. Dell and RIM* (on behalf of the defendants Dell and RIM), *Wi-LAN v. RIM* (on behalf of defendant RIM), *LSI v. Barnes & Noble* (on behalf of plaintiff LSI), *Novatel v. Franklin and ZTE* (on behalf of plaintiff Novatel), *LSI v. Realtek* (on behalf of plaintiff LSI), *Wi-LAN v. Apple et al.* (on behalf of defendants Apple, Sierra and Novatel), *EON v. Sensus et al.* (on behalf of defendants Motorola, US Cellular and Sprint), *M2M/Blackbird v Sierra et al.* (multiple related cases on behalf of defendants Sierra and Novatel), *Intellectual Ventures v. AT&T et al.* (on behalf of defendants AT&T, T-Mobile and Sprint), *Intellectual Ventures v. Motorola* (on behalf of defendant Motorola), *TQ Beta v. DISH et al.* (on behalf of defendant DISH), *Qurio v. DISH et al.* (on behalf of defendant DISH), *Fatpipe v. Talari* (on behalf of the defendant Talari), *EON v. Apple* (on behalf of defendant Apple), *Chrimar v. Dell* (on behalf of defendant Dell), *Nokia v. LGE* (on behalf of plaintiff Nokia), *PanOptis v. Blackberry* (on behalf of defendant Blackberry), *Customedia v. DISH et al.* (on behalf of defendant DISH), *Blackberry v. BLU* (on behalf of plaintiff Blackberry), *MTel v. Charter et al.* (on behalf of defendants Charter, Time Warner, Cox and Bright House), *Huawei v. Samsung* (on behalf of plaintiff Huawei), *Alacritech v. Wistron* (on behalf of defendant Wistron), *IPA v. DISH et al.* (on behalf of defendant DISH), *XR v. Ruckus et al.* (on behalf of defendants

Ruckus, Netgear and Belkin), *Twilio v. Telesign* (on behalf of plaintiff Twilio), *Hera/Sisvel v. Arris et al.* (on behalf of defendants Arris/Ruckus, Netgear, Amazon, Roku and Belkin), *Intellectual Ventures v. Ericsson et al.* (on behalf of defendants Ericsson, T-Mobile and Sprint), *Sol IP v. AT&T et al.* (on behalf of defendants AT&T, Verizon and Sprint), *Soundview v DISH et al.* (on behalf of defendants DISH and Sling Media), *DISH v Peloton, iFIT and MIRROR* (on behalf of plaintiffs DISH and Sling Media) and *XR v. D-Link et al.* (on behalf of defendants D-Link, HP, Netgear and Belkin). I believe that the preceding list includes all cases that I have testified in as an expert at trial or by deposition at least during the past four years.

III. PERSON OF ORDINARY SKILL IN THE ART

22. I understand that the content of a patent (including its claims) and prior art should be interpreted the way a person of ordinary skill in the art (or “POSITA”) would have interpreted the material at the alleged time of invention.

23. I understand that the “alleged time of invention” here is no earlier than the date that the applicants for the ‘384 Patent first filed an application related to the ‘384 Patent, namely, Mar. 2, 2004.

24. A person of ordinary skill in the art (referred to herein as a “POSITA”) at the alleged time of invention for the ‘384 Patent would have been a person familiar with wireless communications networks and equipment, and would have had at least a working knowledge of the applicable standards-based protocols and architectures for common wireless communications networks at the time as well as an understanding of the components and subsystems within available wireless communication equipment.

25. For example, such a POSITA would have had at least a Bachelor’s degree in Electrical Engineering or an equivalent field, and at least two years of work experience in wireless communications. Alternatively, a POSITA 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 communications.

26. In addition to my testimony as an expert, I am prepared to testify as someone who actually practiced in the field from 1986 to present, who actually possessed at least the knowledge of a POSITA within that time period including at the alleged time of invention, and who actually worked with others possessing at least the knowledge of a POSITA within that time period including at the alleged time of invention.

27. I understand that the POSITA is a hypothetical person who is assumed to be aware of all the pertinent information that qualifies as prior art. In addition, the POSITA makes inferences and takes creative steps.

IV. LEGAL UNDERSTANDING

28. I have a general understanding of validity based on my experience with patents and my discussions with counsel.

29. I understand that the claims of a patent are presumed valid. I understand that one factor to be considered in challenging this presumption of validity is whether or not prior art references cited by Petitioner are cumulative to one or more prior art references considered by the U.S. Patent and Trademark Office (the “PTO”) in allowing the claims at issue. I understand that prior art references not specifically considered by the PTO are presumed to be non-cumulative. I understand that if Patent Owner contends that certain prior art references are cumulative to one or more prior art references considered by the PTO, then Patent Owner has the burden to prove this contention with specificity, and further that Petitioner and/or its experts will be allowed to rebut the Patent Owner’s contention.

30. I have a general understanding of prior art and priority date based on my experience with patents and my discussions with counsel.

31. I understand that inventors may be entitled to a priority date earlier than an actual date of filing of a patent application that provides written description support for a particular claim to the extent that they can show complete possession of such a particular claimed invention at such an earlier priority date and reasonable diligence to reduce such a particular claimed invention to practice between such an earlier priority date and such an actual date of filing. I understand that if Patent Owner contends that particular claims are entitled to such an earlier priority date than such an actual date of filing, then Patent Owner has the burden to prove this contention with specificity.

32. I understand that an invention by another must be made before the priority date of a particular patent claim in order to qualify as “prior art” under 35 U.S.C. § 102 or § 103, that a printed publication must be publicly available before the priority date of a particular patent claim in order to qualify as “prior art” under 35 U.S.C. § 102(a), that a printed publication must be publicly available more than one year prior to the actual date of filing of a patent application that provides written description support for a particular claim in the United States in order to qualify as “prior art” under 35 U.S.C. § 102(b), or that the invention by another must be described in an application for patent filed in the United States before the priority date of a particular patent claim in order to qualify as “prior art” under 35 U.S.C. § 102(e). I understand that Petitioner has the burden of proving that any particular reference or product usage or offer for sale is prior art.

33. I have a general understanding of anticipation based on my experience with patents and my discussions with counsel.

34. I understand that anticipation analysis is a two-step process. The first step is to determine the meaning and scope of the asserted claims. Each claim must be viewed as a whole, and it is improper to ignore any element of the claim. For a claim to be anticipated under U.S. patent law: (1) each and every claim element must be identically disclosed, either explicitly or inherently, in a single prior art reference; (2) the claim elements disclosed in the single prior art reference must be arranged in the same way as in the claim; and (3) the identical invention must be disclosed in the single prior art reference, in as complete detail as set forth in the claim. Where even one element is not disclosed in a reference, the anticipation contention fails. Moreover, to serve as an anticipatory reference, the reference itself must be enabled, i.e., it must provide enough information so that a person of ordinary skill in the art can practice the subject matter of the reference without undue experimentation.

35. I further understand that where a prior art reference fails to explicitly disclose a claim element, the prior art reference inherently discloses the claim element only if the prior art reference must necessarily include the undisclosed claim element. Inherency may not be established by probabilities or possibilities. The fact that an element may result from a given set of circumstances is not sufficient to prove inherency. I have applied these principles in forming my opinions in this matter.

36. I have a general understanding of obviousness based on my experience with patents and my discussions with counsel.

37. I understand that a patent claim is invalid under 35 U.S.C. § 103 as being obvious only if the differences between the claimed invention and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person of ordinary skill in that art. An obviousness analysis requires consideration of four factors: (1) scope and content of the prior art relied upon to challenge patentability; (2) differences between the prior art and the claimed invention; (3) the level of ordinary skill in the art at the time of the invention; and (4) the objective evidence of non-obviousness, such as commercial success, unexpected results, the failure of others to achieve the results of the invention, a long-felt need which the invention fills, copying of the invention by competitors, praise for the invention, skepticism for the invention, or independent development.

38. I understand that a prior art reference is proper to use in an obviousness determination if the prior art reference is analogous art to the claimed invention. I understand that a prior art reference is analogous art if at least one of the following two considerations is met. First a prior art reference is analogous art if it is from the same field of endeavor as the claimed invention, even if the prior art reference addresses a different problem and/or arrives at a

different solution. Second, a prior art reference is analogous art if the prior art reference is reasonably pertinent to the problem faced by the inventor, even if it is not in the same field of endeavor as the claimed invention.

39. I understand that it must be shown that a person of ordinary skill in the art at the time of the invention would have had a reasonable expectation that a modification or combination of one or more prior art references would have succeeded. Furthermore, I understand that a claim may be obvious in view of a single prior art reference, without the need to combine references, if the elements of the claim that are not found in the reference can be supplied by the knowledge or common sense of a person of ordinary skill in the relevant art. However, I understand that it is inappropriate to resolve obviousness issues by a retrospective analysis or hindsight reconstruction of the prior art and that the use of “hindsight reconstruction” is improper in analyzing the obviousness of a patent claim.

40. I further understand that the law recognizes several specific guidelines that inform the obviousness analysis. First, I understand that a reconstructive hindsight approach to this analysis, i.e., the improper use of post-invention information to help perform the selection and combination, or the improper use of the listing of elements in a claim as a blueprint to identify selected portions of different prior art references in an attempt to show that the claim is obvious, is not permitted. Second, I understand that any prior art that specifically teaches away from the claimed subject matter, i.e., prior art that would lead a person of ordinary skill in the art to a specifically different solution than the claimed invention, points to non-obviousness, and conversely, that any prior art that contains any teaching, suggestion, or motivation to modify or combine such prior art reference(s) points to the obviousness of such a modification or combination. Third, while many combinations of the prior art might be “obvious to try”, I

understand that any obvious to try analysis will not render a patent invalid unless it is shown that the possible combinations are: (1) sufficiently small in number so as to be reasonable to conclude that the combination would have been selected; and (2) such that the combination would have been believed to be one that would produce predictable and well understood results. Fourth, I understand that if a claimed invention that arises from the modification or combination of one or more prior art references uses known methods or techniques that yield predictable results, then that factor also points to obviousness. Fifth, I understand that if a claimed invention that arises from the modification or combination of one or more prior art references is the result of known work in one field prompting variations of it for use in the same field or a different one based on design incentives or other market forces that yields predictable variations, then that factor also points to obviousness. Sixth, I understand that if a claimed invention that arises from the modification or combination of one or more prior art references is the result of routine optimization, then that factor also points to obviousness. Seventh, I understand that if a claimed invention that arises from the modification or combination of one or more prior art references is the result of a substitution of one known prior art element for another known prior art element to yield predictable results, then that factor also points to obviousness.

41. I understand that a dependent claim incorporates each and every limitation of the claim from which it depends. Thus, my understanding is that if a prior art reference fails to anticipate an independent claim, then that prior art reference also necessarily fails to anticipate all dependent claims that depend from the independent claim. Similarly, my understanding is that if a prior art reference or combination of prior art references fails to render obvious an independent claim, then that prior art reference or combination of prior art references also necessarily fails to render obvious all dependent claims that depend from the independent claim.

42. I understand that claim elements may be expressed as a means for performing a recited function as set out in 35 U.S.C. § 112, ¶ 6. I further understand that for such a means-plus-function element, the element is to be construed to cover the corresponding structure, material, or acts described in the patent specification for performing that function and equivalents thereof. Thus, I understand that in the case of a means-plus-function element that the scope of the claim element is limited to only structure that is both actually disclosed in the patent specification and clearly linked to the claimed function(s).

43. I understand that a claim including a means-plus-function element is literally disclosed if the prior art is found to have a structure that performs the identical recited function wherein that structure is identical or equivalent to structure disclosed in the patent for performing the identical recited function. I further understand that structures are deemed equivalent if they are insubstantially different. One way of determining whether structures are equivalent is to determine whether each performs the identical recited function in a substantially similar way to obtain a substantially similar result. I understand that a structural equivalence analysis must be supported by specific evidence, and that a conclusory statement alleging that a structure within prior art is equivalent to structure disclosed in the patent for performing the identical recited function is insufficient.

44. I also understand that when construing means-plus-function limitations that concern a computer or a microprocessor that is programmed to carry out an algorithm, the structure is to be construed as the algorithm as disclosed in the patent specification. I further understand that disclosure of a means-plus-function claim limitation directed to a computer programmed to perform an algorithm requires that the software in the prior art uses an algorithm that performs the same steps as the algorithm disclosed in the patent specification.

V. THE '384 PATENT

45. The '384 Patent, entitled "Wireless point that provides functions for a wireless local area network to be separated between the wireless point and one or more control nodes, and method for providing service in a wireless local area network having functions separated between a wireless point and one or more control nodes" relates "to the field of wireless local area networks and in particular to the operation of such networks in heterogeneous environments" (see, for example, Ex. 1001 at 1:22-24).

A. Overview of the '384 Patent

46. In the "Background Art" section, the '384 Patent notes that at the time of the invention that "many WLAN equipment manufacturers have addressed large-scale deployments by introducing new split architecture" wherein "control aspects" are "centralized at controller nodes (CNs) while other aspects are distributed to numerous wireless access points (WAPs)" (emphasis added, see, for example, Ex. 1001 at 1:36-41).

47. For example, the '384 Patent observes that "There are currently some efforts to provide standardized means for managing large-scale WLANs in the Internet Engineering Task Forces (IETF) Control and Provisioning of Wireless Access Point (CAPWAP) working group" but alleges that "these efforts do not consider the problems of accommodating WAPs with dissimilar functional capabilities within a single WLAN" (emphasis added, see, for example, Ex. 1001 at 1:45-52).

48. The '384 Patent predicts that "future deployments of WLANs will feature dynamic wireless networks" wherein "network topologies will change during the operational lifecycle of the WLAN" (emphasis added, see, for example, Ex. 1001 at 1:54-57).

49. The '384 Patent contends that "WLAN entities currently available from various vendors are incapable of interoperation in a single WLAN and are also incapable of operation in

a dynamic topology WLAN” due to both “*static differences* between WLAN entities” and “*dynamic differences* between WLAN entities” (emphasis added, see, for example, Ex. 1001 at 2:13-20).

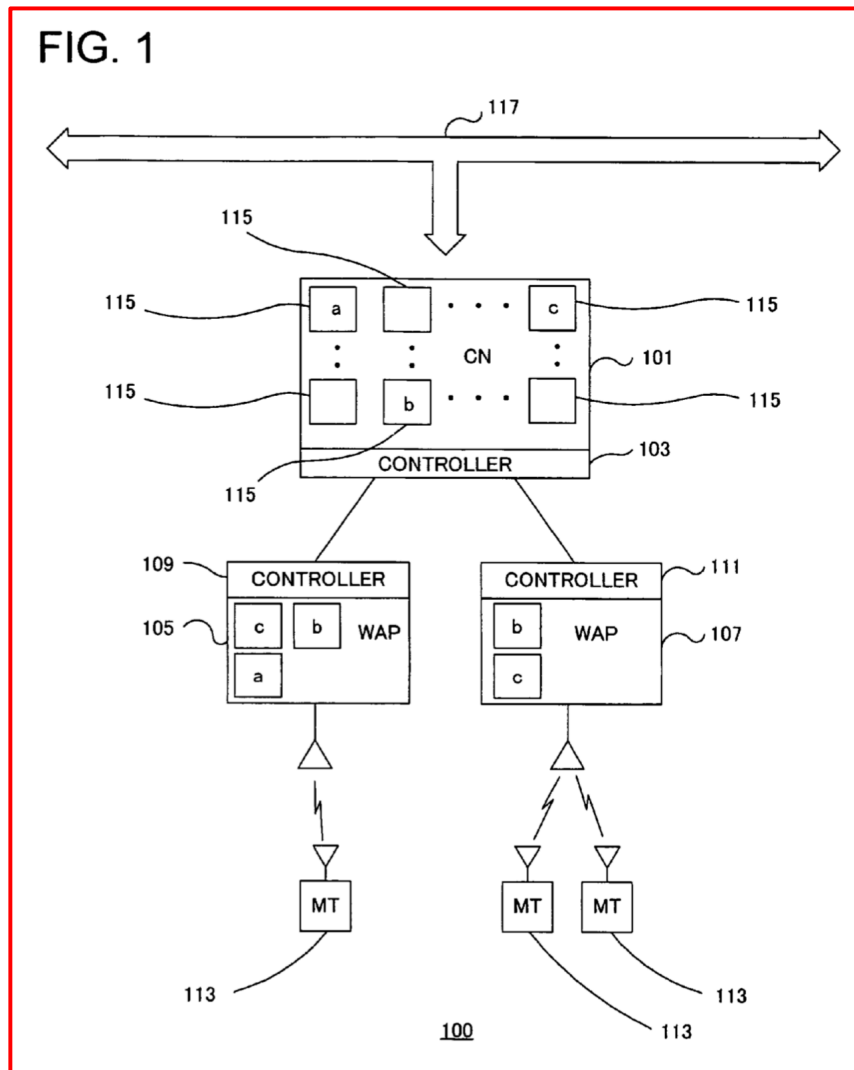
50. More specifically, the ‘384 Patent contends that “during the functioning of a WLAN, the *processing load at a WAP can become substantially high* even exceeding the processing capacity of the WAP” which “could be *due to increases in the number of associated mobile terminals (MTs)* or due to increases in the *volume of traffic* from the associated MTs” (emphasis added, see, for example, Ex. 1001 at 2:21-26).

51. In the “**Disclosure of the Invention**” section, the ‘384 Patent states that “In view of the above discussed problems, it is the objective of the present invention to provide an *apparatus and method for negotiations between controlling nodes (CNs) and wireless access points (WAPs)* of a WLAN based on policies that allow for *accommodating static and dynamic differences* among the WLAN entities including *dynamic changes in WLAN topologies* within a single WLAN” (emphasis added, see, for example, Ex. 1001 at 3:29-35).

52. More specifically, the ‘384 Patent purports “to provide a method and policy for *negotiations between WLAN entities* for the purpose of *determining selected subsets of functional, load or other components to be processed* by each of said WLAN entities so as to accommodate *variations in system design, processing load or network topology*” (emphasis added, see, for example, Ex. 1001 at 3:36-41).

53. In the “**Best Mode for Carrying Out the Invention**” section, the ‘384 Patent describes “FIG. 1” as a “diagram” that “illustrates a *WLAN system 100* comprising a *controller node (CN) 101*, a number of *wireless access points (WAPs) 105 and 107*, a plurality of *mobile terminals (MTs) 113* and a network backbone *117*” wherein “The CN 101 provides *support and*

control to the WAPs 105 and 107 that associate with it” and thus “A new WAP in the WLAN system must first choose and establish association relationships with one or more CNs before it receives support and control from the one or more CNs” (emphasis added, see, for example, Ex. 1001 at 6:55-7:5, FIG. 1 as reproduced below).



54. In reference to FIG. 1 shown above, the ‘384 Patent explains that “Each functional operation is logically represented by one of the functional components 115” which “may include encryption, decryption, medium access control protocol data unit (MAC PDU)

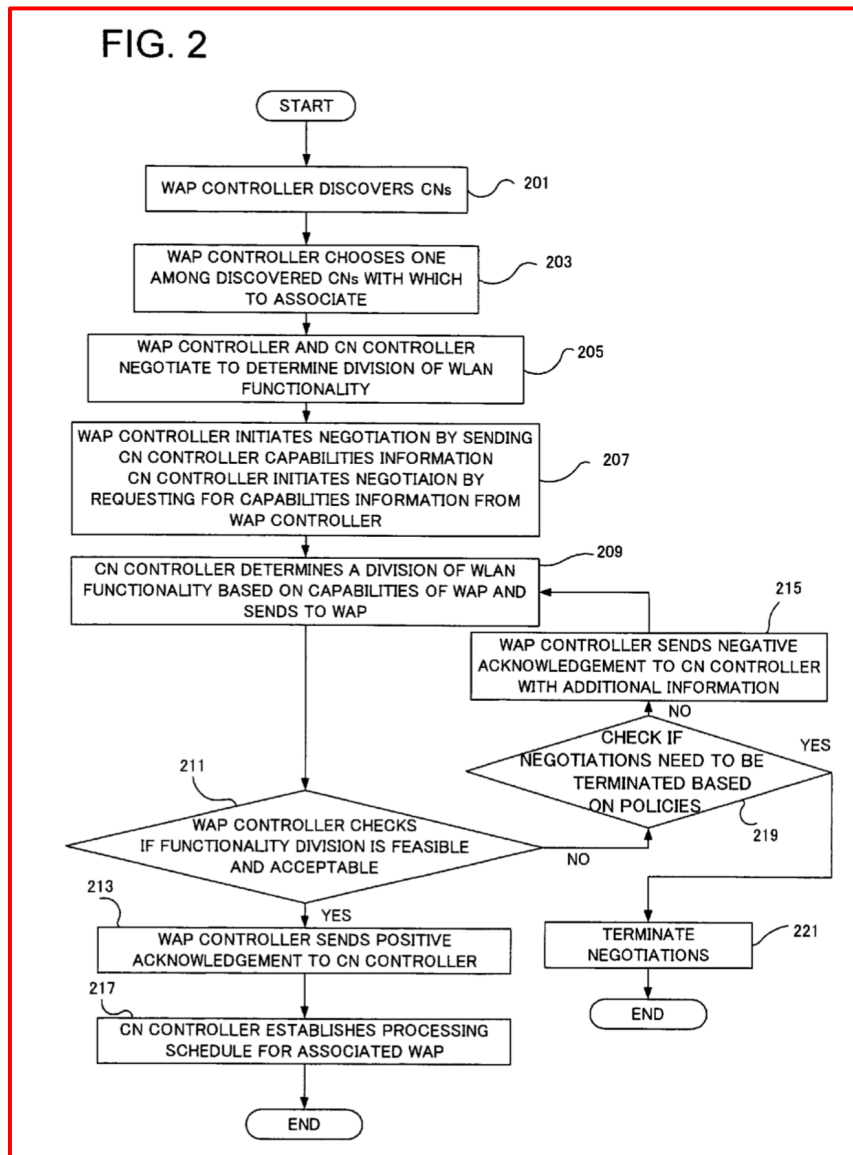
processing, authentication, association, quality of service (QoS) processing, Internet Protocol (IP) processing etc.” (emphasis added, see, for example, Ex. 1001 at 7:25-31).

55. For example, the ‘384 Patent explains that “some of the functional components in FIG. 1 are represented by functional component codes ‘a’, ‘b’ and ‘c’” such that “functional component ‘a’ may denote the processing required for a certain type of encryption, for example Wi-Fi Protected Access (WPA) or Advanced Encryption Standard (AES), functional component ‘b’ for QoS processing, for example priority handling, while functional component ‘c’ may be that for power control during radio transmission and reception” (emphasis added, see, for example, Ex. 1001 at 7:33-41).

56. Additionally, the ‘384 Patent explains that “Since the WAPs may be from different manufacturers or of different implementations, they may incorporate among them varying degrees of WLAN functional components” such as in reference to FIG. 1 shown above, “WAP **105** is shown to be capable of processing functional components ‘a’, ‘b’ and ‘c’ whereas WAP **107** is only capable of processing functional components ‘b’ and ‘c’” and thus accordingly, “These differences between the WAP and CN entities represent the static differences that are to be accommodated by each other WLAN entity by means of the disclosed method for negotiations” (emphasis added, see, for example, Ex. 1001 at 7:53-65).

57. In further reference to FIG. 1 shown above, the ‘384 Patent explains that “Each WLAN entity is controlled in general by a controller entity” wherein “CN controller 103, WAP controllers 109 and 111 are responsible for the overall operations of CN **101**, WAPs **105** and **107**, respectively” and also that “While the WLAN system **100** shows the controllers to be integral to the WLAN entities, the controllers may also be separate entities” ” (emphasis added, see, for example, Ex. 1001 at 8:29-34).

58. According to the '384 Patent, "FIG. 2 is a diagram depicting the general operational steps involved in a first aspect of the present invention dealing with policies for negotiations between a CN and WAP" (emphasis added, see, for example, Ex. 1001 at 5:65-67, FIG. 2 as reproduced below).



59. In reference to FIG. 2 shown above, the '384 Patent explains that "WAP controllers 109 and 111 for WAPs 105 and 107, respectively, first perform a step 201 in the figure of discovering CNs" which "may be accomplished based on any node discovery protocol

or by the broadcast/multicast/anycast of a specific, mutually recognizable message invoking responses from available CNs” (emphasis added, see, for example, Ex. 1001 at 8:60-67).

60. The ‘384 Patent states that “Next the WAP controllers choose which among the discovered CNs to associate with in a step **203**” wherein “One possible metric for this choice may be the round-trip latency between the WAPs and CNs” while “Other metrics that may be used for CN selection include network status, congestion, subset of WLAN functions offered by CN, cost of using the CN, the vendor of the CN, the characteristics of the connection to the CN, link status, random selection, cost of using the link, manufacturer identification and a weighted sum of these metrics” (emphasis added, see, for example, Ex. 1001 at 9:1-11).

61. Next, the ‘384 Patent states that “Having chosen a CN 101 with which to associate, WAP controllers 109 and 111 then enter an association phase with the CN” wherein “This phase may include mutual authentication, exchanges of security information and the establishment of communication protocols for further exchanges” (emphasis added, see, for example, Ex. 1001 at 9:11-16).

62. In further reference to FIG. 2 shown above, the ‘384 Patent explains that “Then, in a step **205**, WAP controllers **109** and **111** enter a negotiation phase with CN controller **103** for the purpose of establishing means to accommodate the possible differences in their respective functional capabilities” in order “to establish 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” wherein such “negotiations may be initiated by either a WAP controller or a CN controller” (emphasis added, see, for example, Ex. 1001 at 9:17-26).

63. More specifically, the ‘384 Patent explains that “in a step **207**” of FIG. 2 that “WAP controllers initiate by sending information regarding the functional capabilities of the

associated WAPs to the chosen CN” such as “the appropriate codes corresponding to the functional components that the WAPs are capable of processing” or alternatively, “A CN controller initiates negotiations by requesting for functional capabilities information from the associated WAPs” (emphasis added, see, for example, Ex. 1001 at 9:26-33).

64. In further reference to FIG. 2 shown above, the ‘384 Patent explains that “Upon receiving capabilities information from the associated WAPs and based on established policies, CN controller 103 determines an initial division of WLAN functionality” which “is then enforced between CN 101 and the associated WAPs 105 and 107 as in step 209” (emphasis added, see, for example, Ex. 1001 at 9:34-38).

65. For example, the ‘384 Patent discloses one embodiment wherein “the initial division of functionality is based on a policy that allows each associated WAP to process all the functional components that they are capable of” such that “only those functional components that an associated WAP cannot inherently process are left to the CN” (emphasis added, see, for example, Ex. 1001 at 9:43-47).

66. Alternatively, the ‘384 Patent discloses another embodiment wherein “the initial division of functionality is based on a policy in which the CN controller first determines a subset of functional components that are common across all associated WAPs” which “then process only the determined subset of functional components even if they are capable of processing other functional components” such that “the remaining set of functional components required to be processed for each associated WAP will be common to all of them” and “can then be processed by the CN” (emphasis added, see, for example, Ex. 1001 at 9:57-66).

67. In further reference to FIG. 2 shown above, the ‘384 Patent next explains that “having determined an initial division of WLAN functionality, the division is then sent to the

associated WAPs for confirmation as in a step **209**” such that “The WAP controllers in turn verify that the division is feasible and upon verification return a positive acknowledgement to the CN as in steps **211** and **213**” (emphasis added, see, for example, Ex. 1001 at 10:37-42).

68. However, the ‘384 Patent notes that “some WAPs may implement functional components in a non-partitioned manner, for example in a hardwire system” and accordingly, “such WAPs may not be able to adhere to the specified initial functionality division” such that these “WAPs send a negative acknowledgement to the CN with an updated processing schedule that indicates operational dependencies between their functional components as in a step **215**” and then “The CN controller then takes this new processing schedule into account and formulates another functionality division that may be compatible with the WAPs” such that “If the new division is feasible, the WAPs return a positive acknowledgement and if not, the negotiations continue in a similar fashion” (emphasis added, see, for example, Ex. 1001 at 10:43-54).

69. Finally, in reference to FIG. 2 shown above, the ‘384 Patent explains that “Once a functionality division is acceptable to all participating WLAN entities, CN controller 103 establishes appropriate processing schedules for associated WAPs **105** and **107** as in a step **217**” in order to “define the sequence of functional components that are to be processed by CN 101 for control and data units received from associated WAPs **105** and **107**” and “Then, CN controller 103 manages each associated WAP in a manner consistent with the processing schedules” (emphasis added, see, for example, Ex. 1001 at 11:4-11).

70. The ‘384 Patent also discloses one embodiment wherein “WLAN functionality may be divided into four functional components that may be denoted by functional component codes 1, 2, 3 and 4” and wherein “code **1** relates to ... the radio aspects”, “code **2** ... relates to

security aspects”, “code 3 deals with ... control and data protocol data units (PDUs)” and “code 4 ... relates to the general control and management of the WLAN” (emphasis added, see, for example, Ex. 1001 at 11:12-31).

71. Accordingly, in this embodiment, the ‘384 Patent explains that “Negotiations between various WLAN entities may then be based on these classifications” such that “a WAP implementing only radio aspects of WLAN may be referred to as a type 1 entity which will then require a CN capable of the remaining functional components 2, 3 and 4” (emphasis added, see, for example, Ex. 1001 at 11:35-40).

72. Alternatively, the ‘384 Patent discloses another embodiment wherein “a WAP controller need not explicitly send its functional capabilities information to a CN controller” because “the CN controller infers the capabilities of an associated WAP” which “allows for easier determination of functional capabilities without requiring the explicit exchange of functional component codes between a CN and associated WAPs” (emphasis added, see, for example, Ex. 1001 at 11:41-48).

73. For example, the ‘384 Patent discloses “a CN controller simulating a data unit as if it was a mobile terminal and sending the simulated data unit to an associated WAP” with the “destination address of the simulated data unit” being “set to be the CN itself” and then “Upon receiving the data unit, the WAP performs its processing based on its capabilities and forwards the processed data unit back to the CN” so that “The CN controller then infers the functional capabilities of the associated WAP from the processed data unit” (emphasis added, see, for example, Ex. 1001 at 11:59-67).

74. The ‘384 Patent also states that “dynamics changes in WLAN topologies is addressed” based upon “the general aspects of a CAPWAP based dynamic WLAN system” such

that “In one embodiment based on the IEEE802.11 specifications and CAPWAP framework, Operational Association state information is exchanged between the network entities accommodating topology changes and network entities effecting topology changes via the central controlling node” (emphasis added, see, for example, Ex. 1001 at 13:18-20, 15:11-15).

B. Prosecution File History of the ‘384 Patent

75. I understand that on May 14, 2007 that U.S. Patent Application No. 10/591,184 by H. Cheng et al., entitled “System and method for negotiation of WLAN entity” was filed (see, for example, Ex. 1003 at [86]).

76. I understand the following to be original claim 1 of U.S. Patent Application No. 10/591,184 (from Ex. 1004 at p. 285):

1. (Original) A system for providing service in a wireless local area network comprising

- i. a single or plurality of wireless access points (WAP) capable of processing a subset of complete functionality defined for the wireless local area network;
- ii. a single or plurality of control nodes (CN) capable of providing a subset or complete functionalities defined for the wireless local area network; and
- iii. negotiation means for the wireless access points to dynamically negotiate with the control node for a secure connections and function split arrangement;

whereby, in use, the control node would negotiate with the WAPs using the negotiation means and provide same or different complementary functionality for each of the WAPs to form a complete functionality defined for the wireless local area network according to decision of the negotiation means.

77. I understand that in Jan. 2010 that the US PTO rejected all pending claims of U.S. Patent Application No. 10/591,184 wherein original claim 1 shown above was rejected as anticipated by U.S. Patent Publication No. 2003/0035464 (“Dehner”) (see, for example, Ex. 1004 at pp. 302-314).

78. I understand that applicants provided amended claims for U.S. Patent Application No. 10/591,184 and remarks in response to the above noted rejection in Jun 2010 (see, for example, Ex. 1004 at pp. 323-343, amended claim 1 as shown below).

1. (Currently Amended) A system for providing service in a wireless local area network comprising:

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

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

[[iii.]] a negotiation unit means for the single or plurality of WAPs ~~wireless access points~~ to dynamically negotiate with the control node for a secure connection ~~connections~~ and function split arrangement;

whereby, ~~in use~~, the control node negotiates ~~would negotiate~~ with the single or plurality of WAPs using the negotiation unit means and provides ~~provide~~ ~~same or different~~ 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 means.

79. I understand that applicants informed the PTO regarding U.S. Patent Application No. 10/591,184 in the above noted Jun 2010 correspondence that “in the methods and apparatuses recited by claims 1-32, it is presumed that a Wireless Access Point (WAP) does not have complete functionality defined for a wireless local area network, and instead has only a subset of complete functionality” and “Therefore, the methods and apparatuses recited by claims 1-32 have as an objective to provide complementary functionality to a WAP which has only a subset of complete functionality to form complete functionality” (emphasis added, see, for example, Ex. 1004 at pp. 334-335).

80. Additionally, I understand that applicants informed the PTO that “In the methods and apparatuses recited by claims 1-32, it is presumed that each WAP has a different set of

functional components” and “Similarly, each Control Node (CN) has a different set of functional components” (emphasis added, see, for example, Ex. 1004 at p. 335).

81. Moreover, I understand that applicants also informed the PTO that “in the methods and apparatuses recited by claims 1-32, the term “providing complementary functionality” can be understood to mean providing some functionalities which a given WAP does not have from another entity which has those functionalities”, or “More specifically, the term “providing complementary functionality” can be understood to mean providing service in a wireless local area network to a radio communication terminal by forming complete functionality defined for the wireless local area network by negotiation and cooperation between WAPs, between a WAP and a CN, and so on” (emphasis added, see, for example, Ex. 1004 at p. 335).

82. I further understand that in view of the above remarks that applicants distinguished at least pending claims 1-8, 12 and 23 of U.S. Patent Application No. 10/591,184 from Dehner by informing the PTO that “By way of review, according to Dehner, all Network Access Points (“NAP”, see FIG. 1, 103 and 105) have the same and complete functionality” (emphasis added, see, for example, Ex. 1004 at p. 335). I also note that applicants emphasized this distinction in remarks for other claims of U.S. Patent Application No. 10/591,184 when stating that “On the contrary, it is assumed in Dehner that all WAPs have the same and complete functionality” (emphasis in original, see, for example, Ex. 1004 at p. 339).

83. I understand that applicants further remarked that “Dehner fails to disclose, either expressly or inherently, each of the recited features of claim 1” by which “the system of claim 1 solves various problems associated with the prior art, including the problem of incompatibility of WAPs of different functionalities, WLAN operations in dynamic topology environments, and

accommodating dissimilar volumes of processing loads over time” (emphasis added, see, for example, Ex. 1004 at p. 336).

84. I understand that in Sep. 2010 that the US PTO notified the applicants of U.S. Patent Application No. 10/591,184 that “Applicant's arguments, see pages 12-20 of the remarks, filed June 28, 2010, with respect to Claims 1-31 have been fully considered and are persuasive” and accordingly all “rejections have been withdrawn” (emphasis added, see, for example, Ex. 1004 at p. 373). However, I understand that the US PTO also informed the applicants that the then-pending claims are “are subject to restriction and/or election requirement” (see, for example, Ex. 1004 at p. 372).

85. I understand that in Oct. 2010 that the applicants informed the USPTO regarding U.S. Patent Application No. 10/591,184 that “In response to the pending Restriction Requirement, Applicants hereby elect Group I, Claims 1-8, 12-14,23,25-27,32, and 33(newly added)” (see, for example, Ex. 1004 at p. 393).

86. I understand that in Dec. 2010 that the US PTO notified the applicants of U.S. Patent Application No. 10/591,184 that pending claims 1-8, 12, 23 and 33 were allowed, that claim 14 was allowable if re-written in independent form and that claims 13 and 32 were anticipated by U.S. Patent Publication No. 2005/0059396 (“Chuah”) (see, for example, Ex. 1004 at pp. 399-406).

87. I understand that in Apr. 2011 that the applicants informed the USPTO regarding U.S. Patent Application No. 10/591,184 that “Chuah fails to disclose, either expressly or inherently, each of the features of claim 1” and further noted in contrast that “Chuah discloses that an access point discovers gateways at which the access point is not registered by broadcasting a gateway query message, and registers its basic information, such as its address

and radio characteristics, at a selected gateway, among the discovered gateways” (emphasis added, see, for example, Ex. 1004 at pp. 425-426).

88. I understand that in Jun. 2011 that the US PTO notified the applicants of U.S. Patent Application No. 10/591,184 that then pending “Claims 1-8, 12-14, 23 and 32-35 are allowed” and also that the “examiner's statement of reasons for allowance” were “Regarding claim 1, the instant invention discloses a negotiation unit for the single or plurality of wireless access points WAPs to dynamically negotiate with the control node for a secure connection and function split arrangement; 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” (emphasis in original, see, for example, Ex. 1004 at pp. 438-442).

89. I understand that U.S. Patent Application No. 10/591,184 issued as U.S. Patent No. 8,045,531 on Oct. 25, 2011 (see, for example, Ex. 1003 at [45]).

90. I understand that on Sep. 19, 2011 that U.S. Patent Application No. 13/235,912 by H. Cheng et al., entitled “Wireless point that provides functions for a wireless local area network to be separated between the wireless point and one or more control nodes, and method for providing service in a wireless local area network having functions separated between a wireless point and one or more control nodes” was filed (see, for example, Ex. 1001 at [22]).

91. I understand the following to be original claims 1 and 2 of U.S. Patent Application No. 13/235,912 (from Ex. 1002 at p. 60):

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

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

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

a session establishing unit configured to establish a secure session with said selected one control node.

2. The wireless point according to claim 1, further comprising:

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

92. I understand that in Feb. 2012 that the US PTO rejected all pending claims of U.S. Patent Application No. 13/235,912 as anticipated by “O'Hara et al. "Architecture for Control and Provisioning of Wireless Access Points (CAPWAP), "draft-ietf-capwap-arch-OO.txt", IETF standard-working-draft, IETF, CH, vol. capwap, 8 February 2004” (“O’Hara”) (see, for example, Ex. 1002 at p. 244).

93. I understand that applicants informed the PTO regarding U.S. Patent Application No. 13/235,912 in a May 2012 correspondence that “O'Hara does not disclose that the discovered ARs send information about their functions to the AP during the AR discovery” and thus “fails to disclose that the ARs send “...discovery response messages including information of functions offered by the associated control node of said one or more control nodes,” as recited by claim 1” (emphasis in original, see, for example, Ex. 1002 at p. 267).

94. I understand that in Jun. 2012 that applicants filed a supplemental amendment subsequent to a telephone interview with the PTO wherein original claims 1 and 2 of U.S. Patent Application No. 13/235,912 were combined to form amended claim 1 as follows (from Ex. 1002 at p. 273):

Please amend the claims to read as follows:

Listing of Claims

1. (Currently Amended) A wireless point that provides for functions for a wireless local area network to be separated between said wireless point and one or more control nodes, said wireless point comprising:

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

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

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

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

2. (Canceled).

95. I understand that in Jun. 2012 that the US PTO notified the applicants of U.S. Patent Application No. 13/235,912 that then pending “Claims 1, 3-5, 7 and 8 are allowed” and also that the “examiner's statement of reasons for allowance” were “Regarding claims 1 and 5, the instant invention discloses "a negotiation unit configured to exchange information about

functions to be separated between said selected one control node and said wireless point””

(emphasis in original, see, for example, Ex. 1002 at p. 288).

96. I understand that U.S. Patent Application No. 13/235,912 issued as U.S. Patent No. 8,270,384 on Sep. 18, 2012 (see, for example, Ex. 1001 at [45]).

C. Asserted Claims and Priority Date

97. The ‘384 Patent includes 6 claims. I understand that Claims 1, 3-4 and 6 of the ‘384 Patent are asserted in the District Court litigation (see, for example, Ex. 1013 at p. 2) and are subject to this *Inter Partes* Review petition. I also note that Claims 2 and 5 of the ‘384 Patent are also subject to this *Inter Partes* Review petition. Accordingly, I may refer to Claims 1-6 of the ‘384 Patent as the “challenged claims” herein.

98. The ‘384 Patent was filed on Sep. 19, 2005 (see, for example, Ex. 1001 at [22]). However, I understand that in the District Court litigation that the Patent Owner alleges the priority date of the ‘384 Patent to be Mar. 2, 2004 (see, for example, Ex. 1013 at p. 4). For purposes of this declaration, I assume Mar. 2, 2004 as the priority date of the ‘384 Patent.

D. Objective Indicia of Non-obviousness

99. I understand that in the District Court litigation, Patent Owner has not yet provided any information regarding this topic. As of this writing, I am unaware of any information that would provide objective indicia of non-obviousness for any of the challenged claims of the ‘384 Patent. However, to the extent that Patent Owner (or its expert) provides opinions and/or analysis with respect to this topic, I reserve the right to supplement my opinions and analyses on this topic.

VI. CLAIM CONSTRUCTION

100. I understand that claim construction is a matter of law. I further understand that in a *Inter Partes* Review proceeding that the claims are to be given their ordinary and customary (or “plain and ordinary”) meaning, as would be understood by a POSITA in the context of the entire disclosure and intrinsic record. I also understand that limitations from the specification of the patent are not to be read into the claims, and that conversely, not all claims necessarily encompass all material disclosed within the specification. The specification, however, can inform a POSITA as to the plain and ordinary meaning of the claims. In addition, I understand that a POSITA would look to statements made by the applicants during the prosecution file history to inform as to the plain and ordinary meaning of the claims.

101. I understand that at least indefiniteness and lack of written description and/or enablement are potential invalidity issues that cannot be addressed as part of an *Inter Partes* Review proceeding. Therefore, solely for the purposes of my prior art invalidity analyses herein as relevant to this *Inter Partes* Review proceeding, I have assumed claim constructions as appropriate for an *Inter Partes* Review proceeding even for such claims and/or claim elements that I may otherwise believe to be indefinite, lacking written description and/or non-enabled as may be set forth in the District Court litigation.

102. I understand that in the District Court litigation involving the Petitioner that Patent Owner has not, as of this writing, identified any claim terms alleged to require constructions nor proposed any claim constructions thereof for the ‘384 Patent. However, Patent Owner has provided an allegation of infringement for at least Claims 1, 3-4 and 6 of the ‘384 Patent. Thus, Patent Owner appears to believe that the claim terms of the challenged claims of

the ‘384 Patent are at least as broad as would be necessary for such allegation of infringement to apply.

103. I have applied a plain and ordinary meaning to all claim terms for the purposes of this *Inter Partes* Review proceeding. In my opinion, my analyses of anticipation and obviousness herein would apply to any reasonable construction of the claim terms as well.

104. I have also been asked to consider, in the alternative, that certain claim elements may be subject to interpretation as a means for performing a recited function as set out in 35 U.S.C. § 112, ¶ 6. I have not been asked to opine as to which claim elements, if any, should be subject to such interpretation. I have also not been asked to opine as to what, if anything, within the specification of the ‘384 Patent may constitute sufficient disclosure of structure linked to performing the recited functions for such claim elements.

105. However, I am informed by counsel for the Petitioner that claim elements of the challenged claims of the ‘384 Patent that may be subject to interpretation as a means for performing a recited function as set out in 35 U.S.C. § 112, ¶ 6 may include at least the **“discovery unit”**, the **“selecting unit”**, the **“session establishing unit”**, and the **“negotiation unit”** of Claim 1.

106. Accordingly, I have also considered in my analyses herein, in the alternative, each of the above listed claim elements as subject to interpretation as a means for performing a recited function as set out in 35 U.S.C. § 112, ¶ 6.

107. In the event that one or more of these constructions is changed, or in the event that additional terms not specifically construed herein receive a proposed construction, I reserve the right to revisit my analysis under such additional construction(s).

VII. STATE OF THE ART

108. As of Mar. 2, 2004, which the Patent Owner alleges to be the priority date of the ‘384 Patent, the state of the art in the field of wireless local area networks using a “split architecture” of “controller nodes” and “wireless access points” already fully encompassed the elements of the asserted claims of the ‘384 Patent, as evidenced in even the small sample of the art described herein.

A. Calhoun (Ex. 1005)

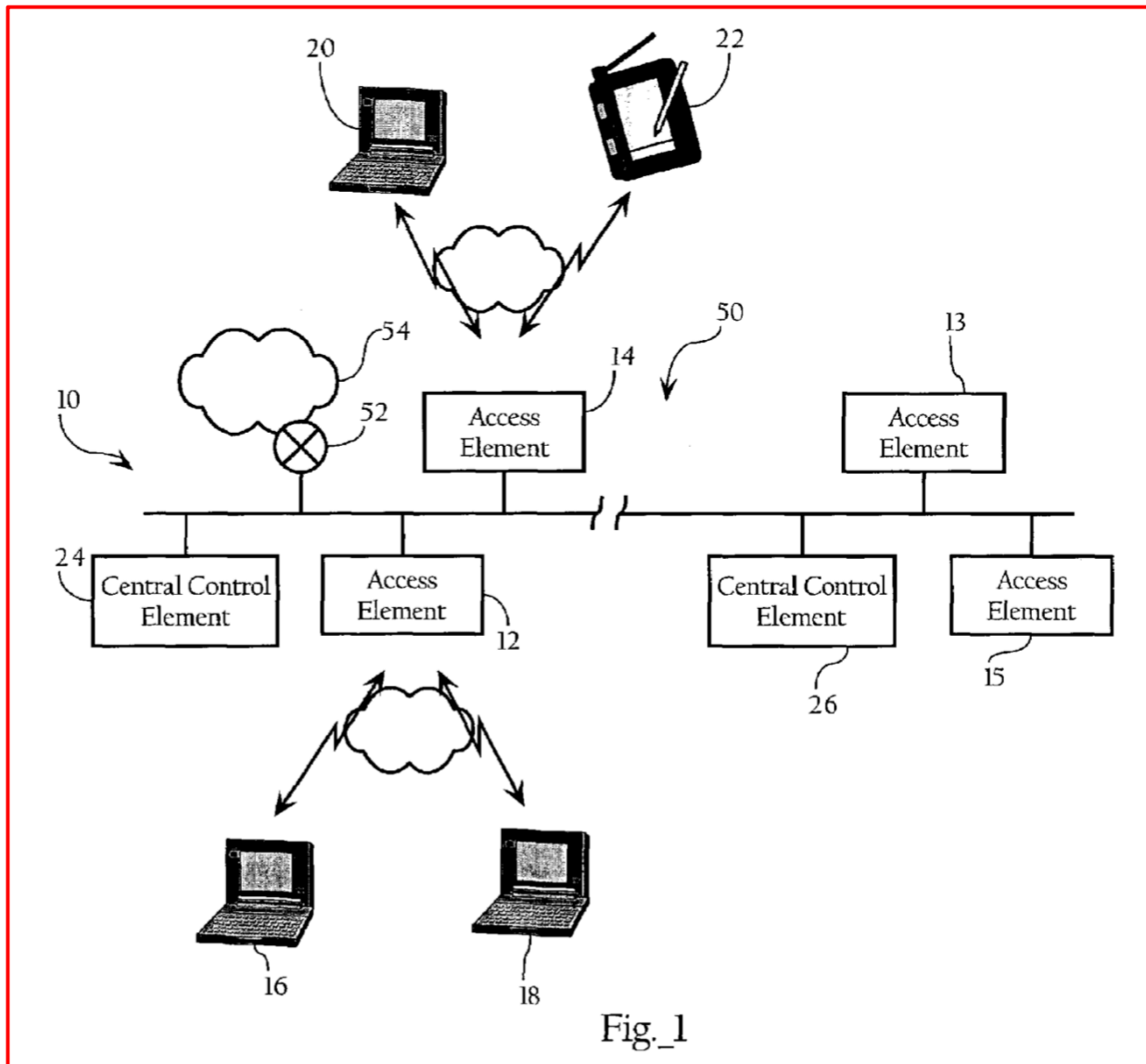
109. For example, amongst the numerous prior art references in this field, U.S. Patent No. 7,508,801 by Patrice Calhoun, Scott Kelly and Rohit Suri, entitled “Light-weight Access Point Protocol” (“Calhoun”) was filed on Mar. 21, 2003 and assigned to Cisco (see, for example, Ex. 1005 at [10], [22], [73], [75]). Thus, I understand that Calhoun qualifies as prior art to the ‘384 Patent at least under 35 U.S.C. § 102(e).

110. Calhoun “relates to wireless networks and, more particularly, to methods, apparatuses and systems facilitating the deployment and configuration of managed access points in a wireless network system” (emphasis added, see, for example, Ex. 1005 at 1:17-20).

111. In the “**Background of the Invention**” section, Calhoun explains that “Unlike centrally-managed cellular wireless systems, known WLAN solutions use distributed access points to act as bridges between the wired infrastructure and the wireless clients” wherein such “An uncoordinated system of access points makes it difficult to manage a large number of access points” and thus “known prior art wireless network systems such as conventional 802.11 systems provide the initial handshaking, access authentication and access association at a remote node without attention to overall network loading and signal quality” (emphasis added, see, for example, Ex. 1005 at 1:44-57).

112. However, Calhoun describes that “U.S. patent application Ser. No. 10/155,938”, which Calhoun incorporates in its entirety, discloses a “system architecture” in which “a central control element manages and controls one more access elements” wherein such “access elements perform real-time communication functions, such as data transfer and acknowledgements, while the central control element manages the connection between the access element and one or more wireless client devices” (emphasis added, see, for example, Ex. 1005 at 1:6-13, 2:1-10).

113. In the “**Description of Preferred Embodiment(s)**” section, Calhoun describes “FIG. 1” as showing a “block diagram of a wireless Local Area Network (LAN) 10” that includes “access elements 12-15 for wireless communication with remote client elements 16, 18, 20, 22 and central control elements 24, 26 for controlling and managing the wireless connections between the access elements 12-15 and the remote client elements” (emphasis added, see, for example, Ex. 1005 at 3:10-17, FIG. 1 as reproduced below).



114. In reference to FIG. 1 shown above, Calhoun explains that “The access elements 12-15 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” while “The LAN segment 10 connecting the access elements 12, 14 and the central control element 24 is typically an Ethernet network” (emphasis added, see, for example, Ex. 1005 at 3:27-32).

115. More specifically, Calhoun discloses that “the central control element 24 provides processing to dynamically configure a wireless Local Area Network of a system according to the invention” (emphasis added, see, for example, Ex. 1005 at 3:46-49).

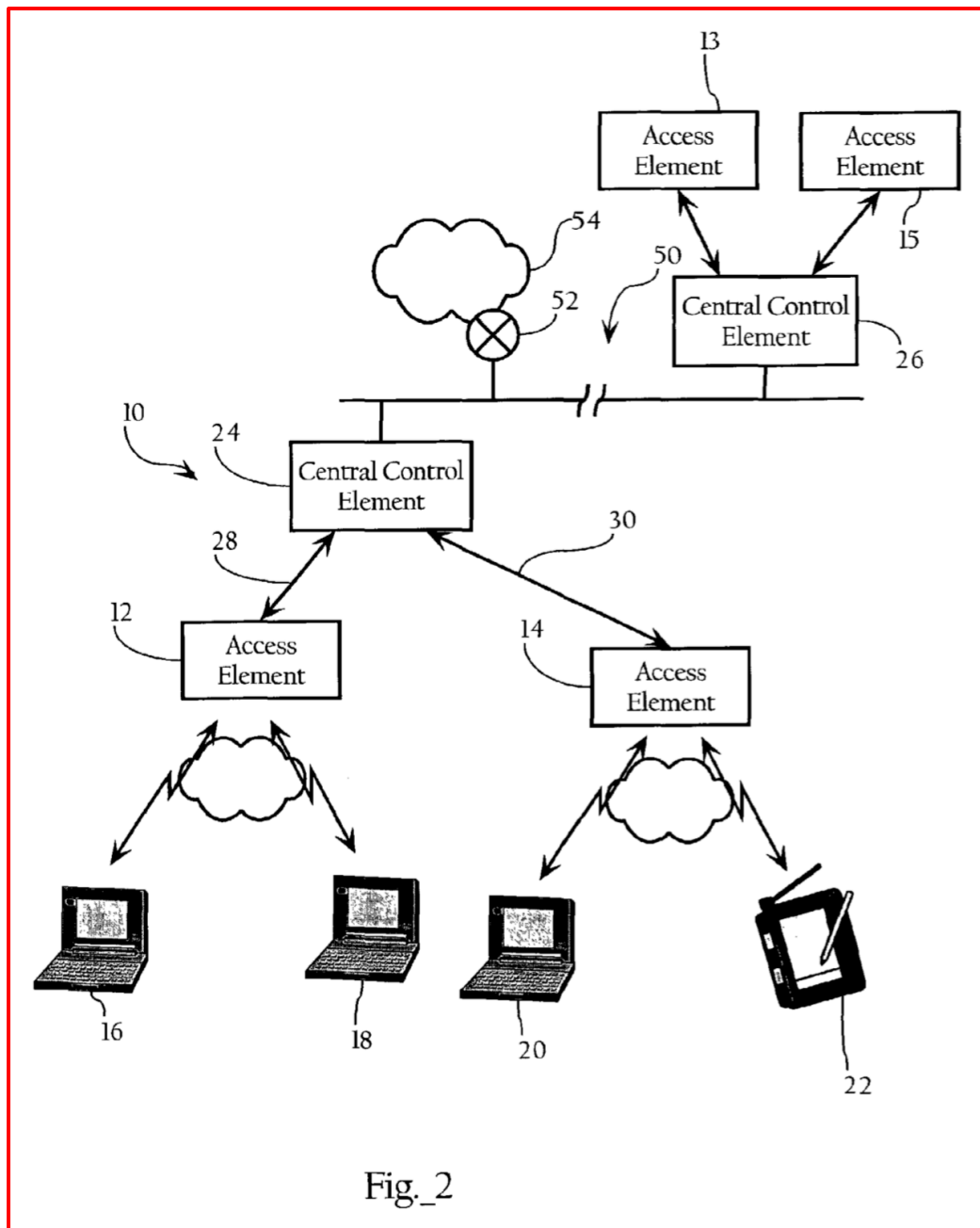
116. For example, Calhoun describes that “central control element 24 operates to perform link layer management functions, such as authentication and association on behalf of access elements 12, 14” and thus “The central control element 24 may for example process the wireless LAN management messages passed on from the client remote elements 16, 18; 20, 22 via the access elements 12, 14” even though “the access elements 12, 14 provide immediate acknowledgment of the communication of those messages without conventional processing thereof” (emphasis added, see, for example, Ex. 1005 at 3:44-46, 3:51-58).

117. As further examples, Calhoun discloses that “the central control element 24 may for example process physical layer information” that is “collected at the access elements 12, 14 on channel characteristic, propagation, and interference or noise” and that “Central control element 24 may also transmit control messages to the access elements 12, 14 to change various operational parameters, such as frequency channel and transmit power” (emphasis added, see, for example, Ex. 1005 at 3:60-66).

118. For example, Calhoun discloses a “deployment architecture” where “wireless traffic associated with remote client elements 16, 18; 20, 22” “can be tunneled between the

central control element 24 and the access elements 12, 14” but also discloses “another embodiment” where “access elements 12, 14 can operate to directly bridge network traffic between remote client elements 16, 18; 20, 22 and WAN 50, while tunneling network management messages, such as authentication and association requests from remote client elements to central control element 24” (emphasis added, see, for example, Ex. 1005 at 4:10-19).

119. Additionally, Calhoun discloses “an alternative deployment architecture where the access elements 12-15 are connected to their respective central control elements 24, 26 via direct access lines 28, 30” as illustrated in FIG. 2 (emphasis added, see, for example, Ex. 1005 at 4:26-29, FIG. 2 as reproduced below).

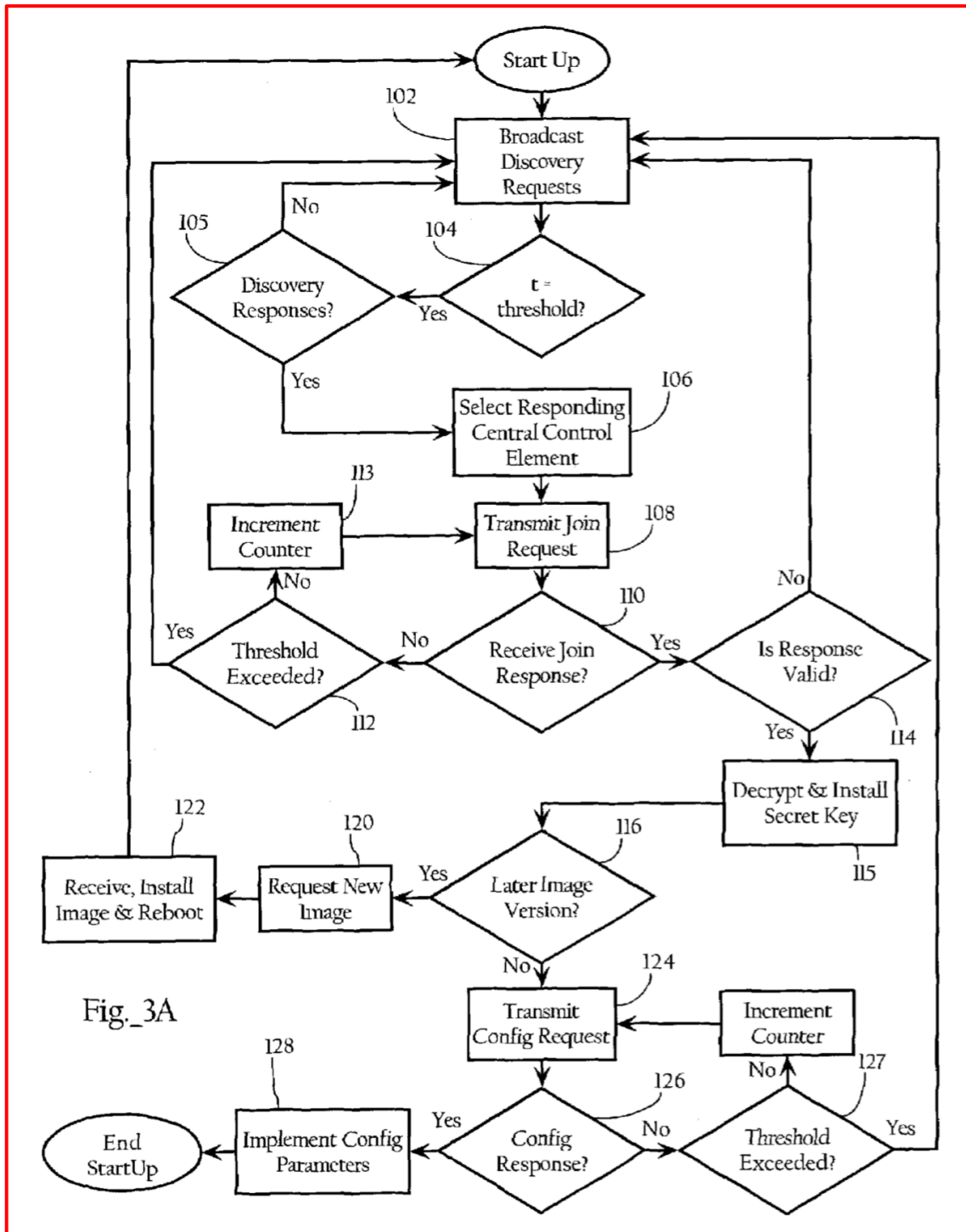


120. Calhoun introduces a “Light-Weight Access Point Protocol (LWAPP)” as including “functionality directed to initialization and configuration of managed access elements” across “three main phases: discovery, joinder, and configuration” (emphasis added, see, for example, Ex. 1005 at 4:31-37).

121. For example, Calhoun explains that “During the discovery phase, the access element discovers the central control elements to which it can associate” while “During 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” and then “Lastly, the configuration phase involves the configuration of the access element with, for example, operational parameters and, potentially, new software images” wherein “The access elements and the central control elements can communicate using a variety of protocols, such as IEEE 802.3, IEEE 802.2, IP, UDP, TCP, etc.” (emphasis added, see, for example, Ex. 1005 at 4:37-47).

122. Therefore, in my opinion, a POSITA would understand even before considering the detailed disclosure of Calhoun to follow that Calhoun is from the same field of endeavor as the ‘384 Patent and that Calhoun is reasonably pertinent to the problem faced by the ‘384 Patent (see, for example, ¶¶ 46-52 above regarding the ‘384 Patent in comparison with the above-summarized introduction to Calhoun). Accordingly, Calhoun is analogous art to the ‘384 Patent.

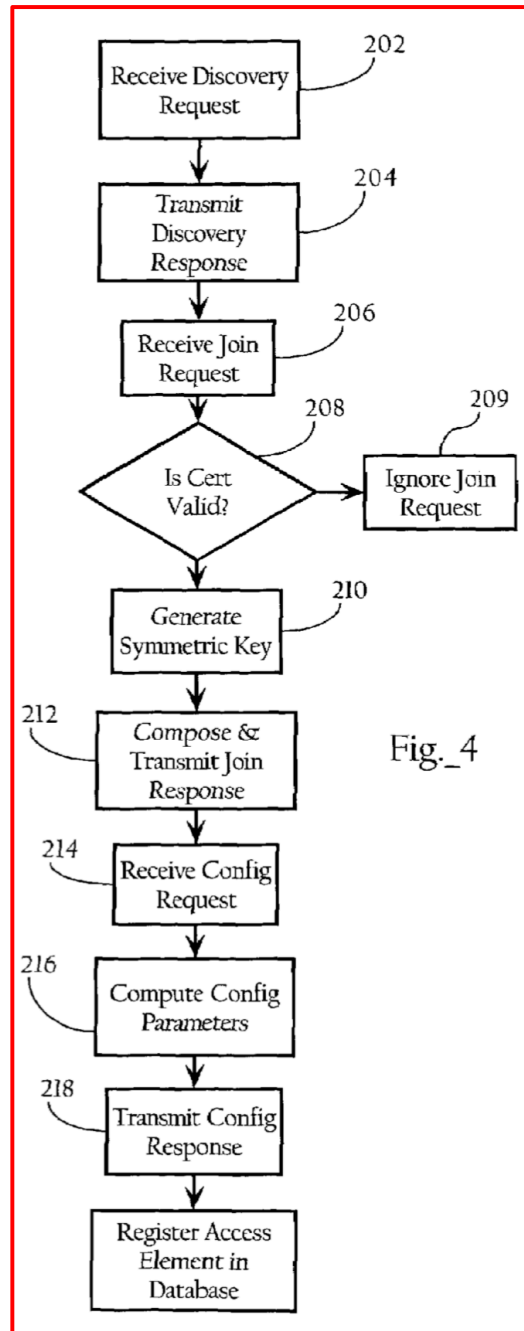
123. According to Calhoun, “FIG. 3A is a flow chart diagram providing a method directed to the initialization and configuration of an access element” thereby “implementing the discovery, joinder and configuration phases of LWAPP” (emphasis added, see, for example, Ex. 1005 at 2:49-51, 5:14-17, FIG. 3A as reproduced below).



124. In reference to FIG. 3A shown above, Calhoun explains that “At startup, access element 15 broadcasts or multicasts discovery requests throughout the virtual subnet implemented by the VLAN in an attempt to identify central control elements (102)” wherein

such “discovery request may be a single IP packet or native link layer frame, such as an Ethernet frame” and then “access element 15 waits a threshold period of time for the receipt of discovery responses (104, 105) before broadcasting or multicasting additional discovery requests” (emphasis added, see, for example, Ex. 1005 at 5:20-27).

125. According to Calhoun, “FIG. 4 provides a method, implemented by central control elements, supporting the LWAPP functionality” and illustrates, for example, that “central control elements 24, 26 receive the discovery requests (202) and transmit discovery responses to access element 15 (204)” wherein “Each discovery response comprises a central control element identifier and a load parameter” (emphasis added, see, for example, Ex. 1005 at 5:17-19, 5:28-32, FIG. 4 as reproduced below).



126. More specifically, Calhoun discloses that “The load parameter indicates the performance load associated with the central control element” such as “the number of access elements under the management and control of a given central control element” (emphasis added, see, for example, Ex. 1005 at 5:34-38).

127. In further reference to FIG. 3A shown above, Calhoun also explains that “access element 15 waits a threshold period of time (104, 105) for discovery responses from one or more central control elements and selects one of the responding central control elements identified in the discovery responses (106)” wherein “The selection of a given central control element can be driven by a number of different considerations” such as “the responding central control element that reports the smallest load (e.g., the smallest number of access elements under management)” (emphasis added, see, for example, Ex. 1005 at 5:52-62).

128. Next, Calhoun explains that “After selection of a central control element, access element 15 transmits a join request to the selected central control element” wherein such “join request” includes “an access element identifier, a digital certificate and a session identifier” and/or “other fields, such as the WLAN MAC address, software image version, etc.” (emphasis added, see, for example, Ex. 1005 at 6:1-8).

129. More specifically, Calhoun discloses that “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), and the digital signature of the certificate-issuing authority (in one embodiment, the manufacturer of the access element) so that central control elements can verify that the digital certificate is authentic” (emphasis added, see, for example, Ex. 1005 at 6:16-23).

130. In further reference to FIG. 3A shown above, Calhoun next explains that “access element 15 waits for a predetermined period of time for a join response (110)” but “If no join response is received within this period of time, access element 15 retransmits the join request (112, 113)” and then “After a threshold number of failed attempts, access element 15” either “restarts the discovery process to locate other central control elements” or “attempts to join with

another central control element identified during the previous discovery process” (emphasis added, see, for example, Ex. 1005 at 6:23-32).

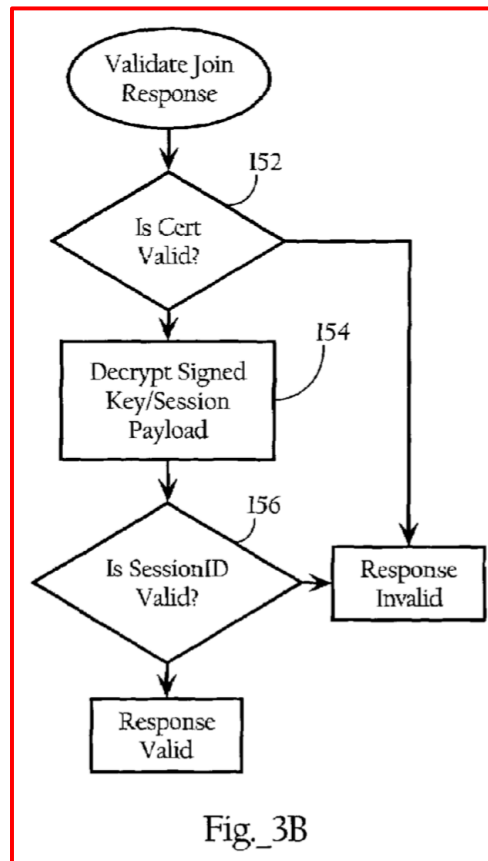
131. Next, in reference to FIG. 4 shown above, Calhoun explains that “Central control element 24 (in this example) receives the join request (206) and authenticates the digital certificate in the join request (208)” and then “generates a secret, shared cryptographic keys” that “will be used to encrypt and authenticate messages between it and access element 15 (210)” and also “composes a join response and transmits it to access element 15 (212)” (emphasis added, see, for example, Ex. 1005 at 6:33-46).

132. More specifically, Calhoun discloses that this “join response” includes not only the “cryptographic keys” and the “digital certificate of the central control element” but also the “software image version supported and implemented by central control element 24” (emphasis added, see, for example, Ex. 1005 at 6:47-51).

133. Furthermore, Calhoun explains that “Similar to the access element, the digital certificate associated with the central control element includes a name or other identifier, a serial number, a MAC address, a copy of the public key of the central control element, and the digital signature of the certificate-issuing authority (in one embodiment, the manufacturer of the access element) so that access elements can verify that the digital certificate is authentic” and also that “central control element 24 encrypts the cryptographic keys with the public key of access element 15 using an asymmetric encryption algorithm, adds the session identifier to the enciphered cryptographic keys, and digitally signs the resulting string with its private key” (emphasis added, see, for example, Ex. 1005 at 6:51-63).

134. In further reference to FIG. 3A shown above, Calhoun next explains that “When access element 15 receives the join response, it validates the join response (114) and, assuming

the join response is valid, decrypts and installs the symmetric cryptographic keys (115)” as shown in FIG. 3B which sets forth “a method directed to the validation of a join response transmitted by a central control element” (emphasis added, see, for example, Ex. 1005 at 2:52-54, 6:64-7:2, FIG. 3B as reproduced below).



135. In reference to FIG. 3B shown above, Calhoun explains that “Access element 15 validates the digital certificate associated with central control element **24 (152)**” such that “If the digital certificate is valid, access element **15** then verifies the signature of the signed key/sessionID payload using the public key of the central control element **24 (154)** and validates the session identifier (156)” and “then decrypts the cipher including the cryptographic keys using its private key **(115)**” so that accordingly, “Transmission of data (e.g., configuration data, control messages, management messages, etc.) between the access element 15 and central control

element 24 can now be encrypted and authenticated using the shared secret cryptographic keys” (emphasis added, see, for example, Ex. 1005 at 7:3-12).

136. Calhoun further discloses that “the join request transmitted during the joiner phase can also be configured to determine the Maximum Transmit Unit (MTU) for the link between access element **15** and central control element **24**” such as for an “embodiment employing Ethernet protocols, access element **15** transmits a join request spanning 1596 bytes to determine whether the link layer supports that frame size” wherein “This frame size is chosen to determine whether a wireless packet (typically the size of a standard Ethernet frame) can be encapsulated with additional headers and transmitted without requiring fragmentation of the native frame” but “If access element 15 does not receive a response to the join request, it reduces the size of the join request to 1500 bytes (standard Ethernet) and transmits it again” and further “If no response is received after a threshold period of time, access element **15** returns to the discovery phase” (emphasis added, see, for example, Ex. 1005 at 7:16-32).

137. In further reference to FIG. 3A shown above, Calhoun next explains that “access element 15 begins the configuration phase, in one embodiment, by comparing the image version identifier in the join response to the image version installed on access element **15 (116)**” such that “If the image version in the join response is later than the image version associated with access element **15**, access element requests the new image version from central control element **24 (120)**” and then subsequently “Access element **15** receives the new image version, installs it and reboots (122), thereby restarting the initialization process described herein” (emphasis added, see, for example, Ex. 1005 at 7:33-42).

138. In continued reference to FIG. 3A shown above, Calhoun explains that “Access element 15, assuming it has a current image version (at least relative to central control element

24), composes and transmits a configuration request to central control element 24 (124)” and “retries the configuration request a threshold number of times, after which it returns to the discovery phase (126, 127)” (emphasis added, see, for example, Ex. 1005 at 7:45-51).

139. More specifically, Calhoun discloses that this “configuration request” from a particular “access element” includes “one or more operational parameters (such as channel, transmit power, internal v. external antenna, etc.)” that a “network administrator” can “directly configure” via “a command line interface, browser interface, etc.” on the “access element” or “through an interface presented by a central control element” wherein such “network administrator” can also “flag” at least “certain overriding parameters which a central control element can not change, except with a new “overriding” parameter value” (emphasis added, see, for example, Ex. 1005 at 7:51-65).

140. Next, in further reference to FIG. 4 shown above, Calhoun explains that “central control element 24 receives the configuration request (214), and generates the operational parameters for access element 15 (216), taking into account the overriding parameters identified in the configuration request” and “then transmits a configuration response including the operational parameters (218), and registers the access element 15 in a database (e.g., a single table, or a relational database), including identifying information (e.g., LAN MAC address, WLAN MAC address, access element identifier, etc.) and the operational parameters associated with the access element (220)” (emphasis added, see, for example, Ex. 1005 at 7:66-8:9).

141. In continued reference to FIG. 3A shown above, Calhoun next explains that “Access element 15 receives the configuration response (126), optionally stores the operational parameters in non-volatile memory, implements the operational parameters (128), and switches to an access point mode” using “the configuration information provided by the central control

element”, and then subsequently “transmits a message indicating the start up event to the central control element” (emphasis added, see, for example, Ex. 1005 at 8:9-17).

142. Calhoun observes that “embodiments of the present invention have been described as operating in 802.11 wireless networks” (emphasis added, see, for example, Ex. 1005 at 9:1-2).

143. Additionally, Calhoun discloses that “the division of functionality between the access elements and the central control elements can be shifted” wherein “For example, the access elements can bridge network traffic associated with the remote client elements directly, while transmitting management packets to the central control element” (emphasis added, see, for example, Ex. 1005 at 9:7-11).

144. Moreover, Calhoun further discloses that “the managed access point protocol can be implemented, as discussed above, in connection with substantially autonomous access elements managed and configured by a central management server or appliance” (emphasis added, see, for example, Ex. 1005 at 9:12-15).

145. I note that Calhoun also recites 16 claims. Exemplary claims 13 and 15 are shown below (from Ex. 1005 at 10:49-12:7):

13. A wireless network system, comprising
a plurality of access elements for wireless communication with at least one remote client element and for communication with a central control element;
a plurality of central control elements for supervising the access elements, wherein the central control elements are each operative to
manage wireless connections between the access elements and corresponding remote client elements,
exchange validating information with access elements,
and
exchange configuration information with validated access elements;
wherein the access elements are each operative to
discover one or more central control elements, wherein the one or more central control elements each provide a central control element identifier and a load parameter identifying the number of access elements associated with the corresponding central control element,
select a central control element from the discovered central control elements wherein the selected central control element reporting the lowest load parameter,

exchange validating information with the selected central control element by transmitting a first joint request having a first byte size to the selected central control element; if a join response to the first joint request is not received, transmitting a second joint request having a second byte size, wherein the second byte size is less than the first byte size; and validating a join response received from the selected control element,
exchange configuration information with the validated central control element, and
establish and maintain, in connection with the validated central control element, wireless connections with remote client elements.

15. The wireless network system of claim **13** wherein the plurality of central control elements are each operative to
generate cryptographic keys,
provide at least one cryptographic key to validated access elements, and
wherein communication of management data between the plurality of access elements and the plurality of central control elements is encrypted using the at least one cryptographic key.

B. LWAAP (Ex. 1006)

146. For example, amongst the numerous prior art references in this field, Internet-Draft draft-calhoun-seamoby-lwapp-03 by P. Calhoun, B. O'Hara, S. Kelly, R. Suri (all four from Airespace) et al., entitled "Light Weight Access Point Protocol (LWAPP)" ("LWAPP") was published by the Internet Engineering Task Force (IETF) of the Internet Society on Jun. 28, 2003 (see, for example, Ex. 1006 at p. 1). This document is publicly available at <https://datatracker.ietf.org/doc/draft-calhoun-seamoby-lwapp/>. Thus, I understand that LWAPP qualifies as prior art to the '384 Patent at least under 35 U.S.C. § 102(a).

147. In its "**Abstract**" section, LWAPP discloses that "This document describes the *Light Weight Access Point Protocol* which is a protocol allowing a router or switch *to interoperably control and manage a collection of wireless Access Points*" wherein "an *802.11 binding* is provided" (emphasis added, see, for example, Ex. 1006 at p. 2).

148. In its "**Introduction**" section, LWAPP discloses that "The emergence of *simple Access Points in 802.11* that are *managed by a router or switch* (also known as an *Access router, or AR*) suggests that having a *standardized, interoperable protocol* could radically *simplify the deployment and management of wireless networks*" due to the "*Centralization* of the *bridging, forwarding, authentication, encryption and policy enforcement functions* for a *WLAN*" (emphasis added, see, for example, Ex. 1006 at pp. 7-8).

149. LWAPP explains that "The *APs can be considered as remote RF interfaces*, being *controlled by the AR* (see Figure 1)" wherein "The *AP forwards all 802.11 frames* received *to the AR* via the LWAPP protocol, *which processes the frames*" and thus "*packets from authorized mobiles are forwarded by the AP to the AR* via this protocol" (emphasis added, see, for example, Ex. 1006 at p. 7, Figure 1 as reproduced below).

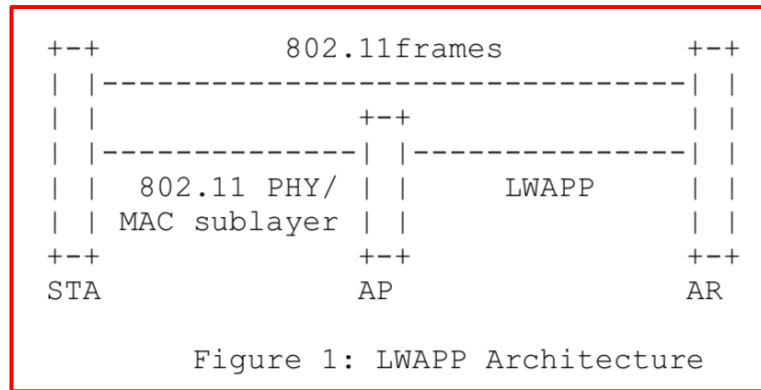


Figure 1: LWAPP Architecture

150. In its “**Protocol Overview**” section, LWAPP discloses that “The Light Weight Access Protocol (LWAPP) begins with a discovery phase, whereby the APs send a Discovery Request frame, causing any Access Router (AR) [9], receiving that frame to respond with a Discovery Reply” such that “From the Discovery Replies received, an Access Point (AP) will select an AR with which to associate, using the Join Request and Join Reply” (emphasis added, see, for example, Ex. 1006 at p. 10).

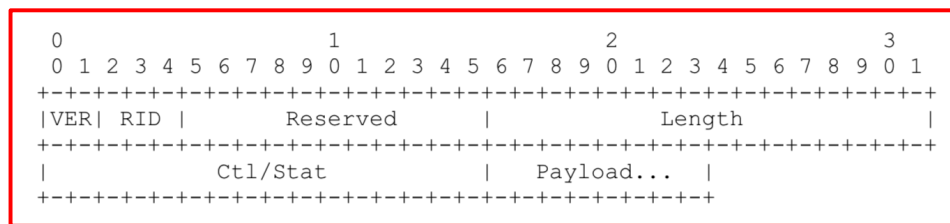
151. More specifically, LWAPP explains that “The Join Request also provides an MTU discovery mechanism, to determine whether there is support for the transport of jumbo frames between the AP and it's AR” wherein “If support for jumbo frames is not present, the LWAPP frames will be fragmented to the maximum length discovered to be supported by the layer 2 network” (emphasis added, see, for example, Ex. 1006 at p. 10).

152. Next, LWAPP discloses that “Once the AP and the AR have joined, a configuration exchange is accomplished that will upgrade the version of the code running on the AP to match that of the AR, if necessary, and will provision the APs” wherein such “provisioning of APs includes the typical name (802.11 Service Set Identifier, SSID), and security parameters, the data rates to be advertised as well as the radio channel (channels), if the AP is capable of operating more than one 802.11 MAC and PHY simultaneously) to be used” and then “Finally, the APs are enabled for operation” (emphasis added, see, for example, Ex. 1006 at p. 10).

153. LWAPP further discloses that “When the AP and AR have one or more WLANs provisioned and enabled, the LWAPP encapsulates the 802.11 Data and Management frames, to transport them between the AP and AR”, “LWAPP also provides for the delivery of commands from the AR to the AP for the management of 802.11 devices that are communicating with the AP”, and “LWAPP provides the ability for the AR to obtain any statistical information collected by the AP” (emphasis added, see, for example, Ex. 1006 at pp. 10-11).

154. Therefore, in my opinion, a POSITA would understand even before considering the detailed disclosure of LWAPP to follow that LWAPP is from the same field of endeavor as the ‘384 Patent and that LWAPP is reasonably pertinent to the problem faced by the ‘384 Patent (see, for example, ¶¶ 46-52 above regarding the ‘384 Patent in comparison with the above-summarized introduction to LWAPP). Accordingly, LWAPP is analogous art to the ‘384 Patent.

155. In its “**LWAPP Packet Format**” section, LWAPP discloses the “general packet header format” in view of an “LWAPP Message Format” (emphasis added, see, for example, Ex. 1006 at p. 13, excerpt as reproduced below).



156. More specifically, LWAPP explains for the depicted “Control/Status” field (or “Ctl/Stat” field in the excerpt above) that “The interpretation of this field depends on the direction of transmission of the packet” such that it is a “Status” field “When an LWAPP packet is transmitted from an AP to a AR” and it is a “Control” field “When an LWAPP packet is transmitted from an AR to an AP” that “indicates on which WLANs the encapsulated 802.11

frame is to be transmitted” (emphasis added, see, for example, Ex. 1006 at p. 14, excerpt as reproduced below).

The Control field is encoded in the following manner:

```

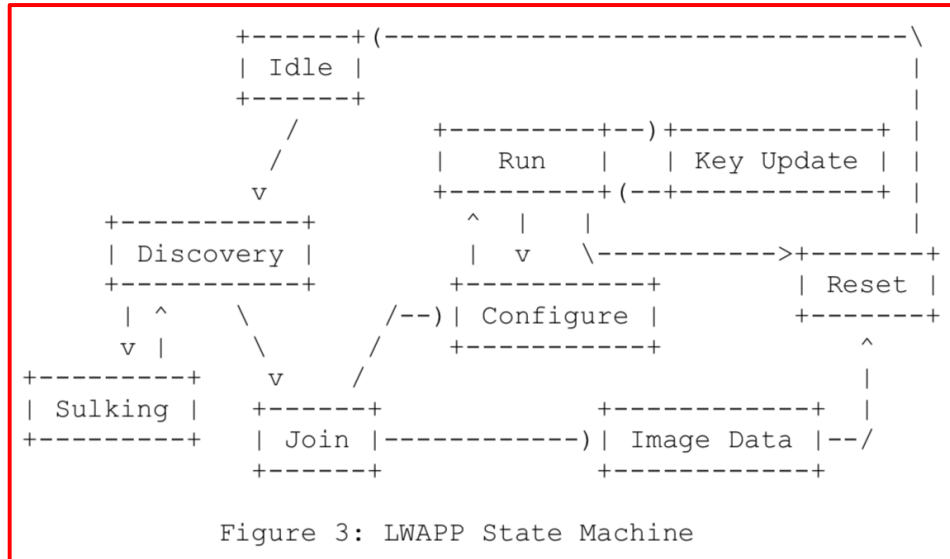
      0                               1
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-----+-----+-----+-----+
|               WLAN ID(s)               |
+-----+-----+-----+-----+

```

157. Additionally, LWAPP explains that “The Payload field contains data”, such as “the encapsulated 802.11 frame” noted above, that is “equal in size to the value of the Length field, found within the LWAPP header” (emphasis added, see, for example, Ex. 1006 at p. 15).

158. In its “**LWAPP Control Messages**” section, LWAPP discloses that “The LWAPP Control protocol provides a communication channel between the AP and the AR and falls into the following distinct messages types” which include at least “Control Channel Management: Messages that fall within this classification are used for the discovery of ARs by the APs as well as the establishment and maintenance of an LWAPP control channel”, “AR Configuration messages” that “are used by the AR to push a specific configuration to the APs it has a control channel with”, and “Firmware Management: Messages in this category are used by the AR to push a new firmware image down to the AP” (emphasis added, see, for example, Ex. 1006 at p. 15).

159. Additionally, LWAPP provides a “state diagram” that “represents the lifecycle of an AP-AR session” wherein “Each of the states” depicted “correspond to an LWAPP control message type” (emphasis added, see, for example, Ex. 1006 at pp. 15-16, Figure 3 as reproduced below).



160. More specifically, LWAPP discloses a “Control Message Format” that includes a “Message Type” field in its “header” that “identifies the function of the LWAPP control message” according to a list of “valid values for Message Type” (emphasis added, see, for example, Ex. 1006 at pp. 16-17, excerpt as reproduced below).

Discovery Request	1
Discovery Reply	2
Join Request	3
Join Reply	4
Configure Request	5
Configure Response	6
Configuration Update Request	7
Configuration Update Response	8
Statistics Report	9
Statistics Report Response	10
Reserved	11-16
Echo Request	17
Echo Response	18
Image Data Request	19
Image Data Response	20
Reset Request	21
Reset Response	22
Key Update Request	23
Key Update Response	24
Reserved	25-26
Key Update Trigger	27

161. LWAPP also discloses that this “Control Message Format” may include “message element(s)” that “carry the information pertinent to each of the control message types” including at least a list of “supported message elements” each with “allowable values for the

Type field” (emphasis added, see, for example, Ex. 1006 at pp. 17, 32 excerpt as reproduced below).

Description	Type
Result Code	1
AR Address	2
AP Payload	3
AP Name	4
AR Payload	5
Reserved	6
AP WLAN Radio Configuration	7
Rate Set	8
Multi-domain capability	9
MAC Operation	10
Reserved	11
Tx Power Level	12
Direct Sequence Control	13
OFDM Control	14
Supported Rates	15
Reserved	16
Test	17
Reserved	18-25
Administrative State	26
Delete WLAN	27
Reserved	28-29
AR Name	30
Image Download	31
Image Data	32
Reserved	33
Location Data	34
Reserved	35
Statistics Timer	36
Statistics	37
Reserved	38-42
Certificate	43
Session	44
Session key	45
Reserved	46-49
WLAN Payload	50
Vendor Specific	51
Tx Power	52
Add Mobile	53
Delete Mobile	54
Mobile Session key	55

162. For example, LWAPP explains that “The Discovery Request is used by the AP to automatically discovery potential ARs available in the network” and mandates that “An AP must transmit this command even if it has a statically configured AR, as it is a required step in the LWAPP state machine” (emphasis added, see, for example, Ex. 1006 at p. 18).

163. LWAPP further explains that “The Discovery Request carries the following message elements: AP Payload” and “Radio Payload (one for each radio in the AP)” (also

denoted as “AP WLAN Radio Configuration” in the list above) (emphasis added, see, for example, Ex. 1006 at p. 19).

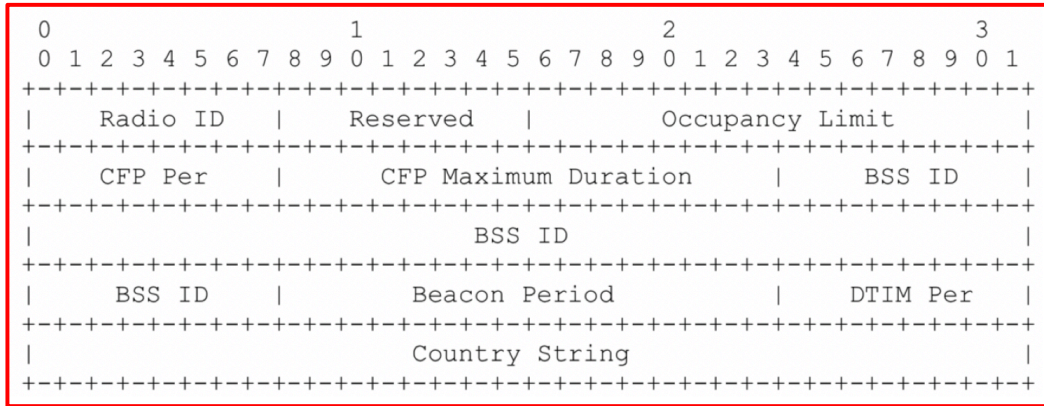
164. More specifically, LWAPP describes the format of this “AP payload message element” as including the “current hardware/firmware configuration” of the AP as well as information on the number of “Radios” and the “Encryption Capabilities” of the AP (emphasis added, see, for example, Ex. 1006 at pp. 33-34, excerpt as reproduced below).

0	1	2	3
0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1
+	+	+	+
	Hardware	Version	
+	+	+	+
	Software	Version	
+	+	+	+
	Boot	Version	
+	+	+	+
	Max Radios	Radios in use	
+	+	+	+
	Encryption Capabilities		
+	+	+	+

165. In further detail, LWAPP describes the format of this “Encryption Capabilities” field within the “AP payload message element” as a “16-bit field” that “is used by the AP to communicate its capabilities to the AR” because “most APs support link layer encryption” and thus, “the AR may opt to make use of these services” which include “1 - Encrypt WEP 104”, “2 - Encrypt WEP 40”, “3 - Encrypt WEP 128”, “4 - Encrypt AES-OCB 128”, and “5 - Encrypt TKIP-MIC” (emphasis added, see, for example, Ex. 1006 at p. 34).

166. Additionally, LWAPP describes the format of the “Radio Payload” or “AP WLAN Radio Configuration” “message element” that is “used by the AR to configure a Radio on the AP” as including at least the fields “Radio ID: An 8-bit value representing the radio to configure”, “BSSID: The WLAN Radio's MAC Address”, “Beacon Period: This attribute specifies the number of TU that a station uses for scheduling Beacon transmissions”, “DTIM Period: This attribute specifies the number of beacon intervals that elapses between transmission

of Beacons frames containing a TIM element whose DTIM Count field is 0” and multiple “point coordinator” and “contention free period” (or “CFP”) fields (emphasis added, see, for example, Ex. 1006 at pp. 35-36, excerpt as reproduced below).



167. For example, LWAPP explains that “Upon receiving a discovery request, the AR will respond with a Discovery Reply sent to the address in the source address of the received discovery request” wherein “The Discovery Reply carries the following message elements: AR Payload” and “AR Name Payload” (emphasis added, see, for example, Ex. 1006 at p.19).

168. More specifically, LWAPP describes the format of this “AR payload message element” as being “used by the AR to communicate it's current state” and as including the “Hardware Version” and “Software Version”, the “number of mobile stations currently associated with the AR” and the “maximum number of stations supported by the AR”, and the “number of APs currently attached to the AR” and the “maximum number of APs supported by the AR” (emphasis added, see, for example, Ex. 1006 at p. 35, excerpt as reproduced below).

0										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1								
Reserved										Hardware Version ...																													
HW Ver										Software Version ...																													
SW Ver										Stations										Limit																			
Limit										Radios										Max Radio																			
Max Radio																																							

169. For example, LWAPP explains that “When an AP receives a Discovery Reply, it MUST wait for an interval not less than DiscoveryInterval for receipt of additional discovery replies” such that “After the DiscoveryInterval elapses, 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” (emphasis added, see, for example, Ex. 1006 at pp. 19-20).

170. Additionally, LWAPP explains that “The initial Join Request is padded with the Test message element to 1596 bytes” such that “If a Join Reply is received, the AP can forward frames without requiring any fragmentation” but “If no Join Reply is received, it issues a second Join Request padded with the Test Payload to a total of 1500 bytes” wherein “The AP continues to cycle from large (1596) to small (1500) packets until a Join Reply has been received, or until both packets sizes have been retransmitted 3 times” and then “If the Join Reply is not received after the maximum number of retransmissions, the AP MUST abandon the AR and restart the discovery phase” (emphasis added, see, for example, Ex. 1006 at p. 20).

171. LWAPP further explains that “The Join Request carries the following message elements: AR Address Payload”, “AP Payload”, “AP Name Payload”, “Location Data”, “Radio Payload (one for each radio)” (also denoted as “AP WLAN Radio Configuration” as noted

above), “Certificate”, “Session ID”, and “Test” (emphasis added, see, for example, Ex. 1006 at p. 20).

172. More specifically, LWAPP describes the format of this “certificate message element value” as “a byte string containing a PKCS #5 certificate” (emphasis added, see, for example, Ex. 1006 at p. 46).

173. For example, LWAPP explains that “When an AR receives a Join Request” that then “The AR validates the certificate found in the request” such that “If valid, the AR generates a session key which will be used to secure the control frames it exchanges with the AP” and then “When the AR issues the Join Reply, the AR creates a context for the session with the AP” (emphasis added, see, for example, Ex. 1006 at p. 20).

174. More specifically, LWAPP explains that “The Join Reply is sent by the AR to indicate to an AP whether it is capable and willing to provide service to it” wherein “The Join Reply carries the following message elements: Result Code” (with “values” that are either “0 Success” or “1 Failure”), “Certificate” (described above) and “Session Key” (which is “A 128-bit value randomly generated session key” that is “used to protect the LWAPP control messages”) (emphasis added, see, for example, Ex. 1006 at pp. 21, 33, 46-47).

175. For example, LWAPP explains that “Configure Requests are sent by an AP after receiving a Join Reply” in order to “send its current configuration to its AR” wherein such “Configure Request carries the following message elements: Administrative State (for the AP)”, “AR Name”, “Administrative State (for each radio)”, “AP WLAN Radio Configuration (for each radio)”, “Multi-domain Capability (for each radio)”, “MAC Operation (for each radio)”, “PHY TX Power (for each radio)”, “PHY TX Power Level (for each Radio)”, “PHY DSSS Payload or

PHY OFDM Payload (for each radio)”, “Antenna (for each radio)” and “Supported Rates (for each radio)” (emphasis added, see, for example, Ex. 1006 at p. 24).

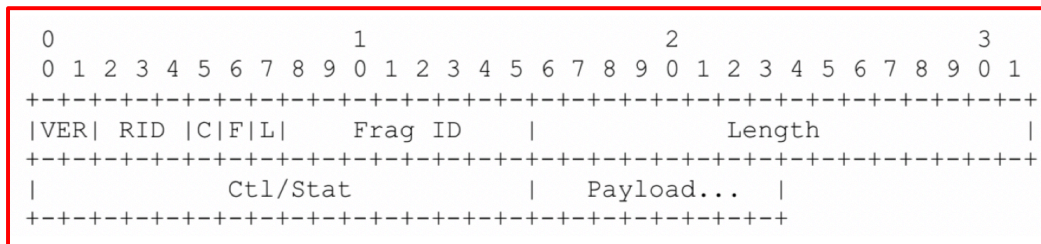
176. For example, LWAPP explains that “When an AR receives a Configure Request it will act upon the content of the packet and respond to the AP with a Configure Response” which “provides an opportunity for the AR to override an AP's configuration” wherein such “Configure Response carries the following message elements: Result Code”, “AP WLAN Radio Configuration (for each radio)”, “Operational Rate Set (for each radio)”, “Multi-domain Capability (for each radio)”, “MAC Operation (for each radio)”, “PHY Tx Power (for each Radio)”, “PHY DSSS or PHY OFDM Payload (for each radio)” and “Antenna (for each radio)” (emphasis added, see, for example, Ex. 1006 at p. 25).

177. For example, LWAPP explains that “When an AP receives a Configure Response it acts upon the content of the packet, as appropriate” (emphasis added, see, for example, Ex. 1006 at p. 25).

178. In its “**LWAPP Transport Layer**” section, LWAPP discloses that “The LWAPP protocol can operate at layer 2 or 3” wherein “For layer 2 support, the LWAPP frames are carried in a native Ethernet frame” and wherein “Layer 3 support is provided by encapsulating the LWAPP frames within UDP” (emphasis added, see, for example, Ex. 1006 at p. 54).

179. For example, LWAPP explains that “When run over Ethernet, the LWAPP protocol is restricted to a specific Ethernet segment” such that “The AR discovery mechanism used with this transport is for the Discovery Request message to be transmitted to a broadcast address” and then “The ARs will receive this message and reply based on their policy” (emphasis added, see, for example, Ex. 1006 at p. 54).

180. Additionally, LWAPP discloses an “Extended LWAPP Message Format” and explains that “When LWAPP is run over a layer 2 interface, the base LWAPP header is extended to include fields that are only useful when run over this transport” wherein the “Reserved” field shown in ¶ 155 above is populated with a “C Bit” field that “indicates whether this packet carries data or control information” as well as other fields that describe fragmentation if applicable (emphasis added, see, for example, Ex. 1006 at pp. 54-55, excerpt as reproduced below).



181. Alternatively, for “Layer 3”, LWAPP explains that “Communication between AP and AR is established according to the standard UDP client/server model” wherein “The connection is initiated by the AP (client) to the well-known UDP port of the AR (server) used for control messages” and “the transport layer uses IP fragmentation to fragment and reassemble LWAPP messages that are longer than MTU size used by either AP or AR” (emphasis added, see, for example, Ex. 1006 at p. 56).

182. More specifically, LWAPP explains that because “LWAPP messages convey control information between AP and AR, as well as, 802.11 data frames or 802.11 management frames” and thus “LWAPP messages needs to be multiplexed in the transport sub-layer”, then “In case of Layer 3 connection, multiplexing is achieved by use of different UDP ports for control and data packets” (emphasis added, see, for example, Ex. 1006 at p. 56).

183. Accordingly, in view of the above requirement, LWAPP teaches that “As part of Join procedure, the AP and AR may negotiate different UDP ports, as well as, different IP

addresses for data or session management messages” (emphasis added, see, for example, Ex. 1006 at p. 56).

184. LWAPP further explains that “When LWAPP is run over routed IP network, the AP and the AR do not need to reside in the same IP subnet (broadcast domain)” and thus accordingly, “The AP may send the Discovery Request message to either limited broadcast IP address (255.255.255.255) or to the unicast IP address of the AR” so that “Upon receipt of the message, the AR issues a Discovery Reply message to the IP address of the AP, regardless of whether Discovery Request was sent as a broadcast or unicast message” (emphasis added, see, for example, Ex. 1006 at pp. 56-57).

185. In its “**Security Considerations**” section, LWAPP discloses that “LWAPP uses public key cryptography to ensure trust between the AP and the AR” wherein “During the Join phase, the AR generates a session key, which is used to secure all future control messages” and thus because “The AP does not participate in the key generation”, then “A secured delivery mechanism to place the certificate in the devices is required” (emphasis added, see, for example, Ex. 1006 at p. 59).

C. Network World (Ex. 1007)

186. For example, amongst the numerous prior art references in this field, the Network World article by P. Calhoun et al., entitled “LWAPP brings harmony to WLANs” (“Network World”) was published by Network World on Dec. 1, 2003 (see, for example, Ex. 1007 at p. 1). This document is publicly available at <https://www.networkworld.com/article/2328757/lwapp-brings-harmony-to-wlans.html>. Thus, I understand that Network World qualifies as prior art to the ‘384 Patent at least under 35 U.S.C. § 102(a).

187. Network World states that “Centralized 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” (emphasis added, see, for example, Ex. 1007 at p. 1).

188. Network World states that “Lightweight Access Point Protocol (LWAPP)” is “a draft standard” that “the Internet Engineering Task Force is considering as part of the Control and Provisioning of Wireless Access Points (CAPWAP), which is in the preliminary stages of becoming an IETF working group” (emphasis added, see, for example, Ex. 1007 at p. 1).

189. Network World states that “Traditional WLANs” are “based on a device known as a fat access point, which contains all wireless processing capabilities”, which “doesn't let different vendors' equipment interoperate” (emphasis added, see, for example, Ex. 1007 at p. 1).

190. In contrast, Network World describes that “LWAPP's goal is to provide consistent behavior across WLAN devices, ensure multi-vendor WLAN interoperability, protect WLAN hardware investments and create a foundation for delivering advanced WLAN functionality in enterprise environments” (emphasis added, see, for example, Ex. 1007 at p. 1).

191. For example, Network World describes that “An LWAPP-managed network consists of multiple access points connected via Layer 2 (Ethernet) or Layer 3 (IP) to an access controller” such as “WLAN appliances or WLAN switches” and “With LWAPP, access points are essentially remote radio frequency interfaces that no longer house all the mandatory wireless processing capabilities and are controlled by the access controller” (emphasis added, see, for example, Ex. 1007 at p. 2).

192. Network World also explains that “LWAPP governs how access points and access controllers communicate with each other by defining” certain “activities” including “Access point device discovery and authentication”, “Access point information exchange, configuration and software control”, and “Communications control and management between access point and wireless system devices” (emphasis added, see, for example, Ex. 1007 at p. 2).

193. More specifically, Network World explains that “When an access point is plugged into a wireless network, it uses LWAPP to discover available access controllers” so that “After the access point is certified as a valid network device, it associates with the best available WLAN switch/appliance” (emphasis added, see, for example, Ex. 1007 at p. 2).

194. Additionally, Network World explains that once associated that “The access point is updated with the most recent software load and configured with appropriate WLAN system information, such as Service Set Identifiers, channel assignments and security parameters” and then “LWAPP handles packet encapsulation, fragmentation and formatting of data being transferred between access points and access controllers” (emphasis added, see, for example, Ex. 1007 at p. 2).

195. Network World states that “LWAPP has several practical benefits” which include that it “lets the limited computing resources on the access point focus on wireless access, rather

than filtering and policy enforcement” because “The protocol centralizes traffic handling, authentication, encryption and policy enforcement (quality of service and security) capabilities within the access controller” (emphasis added, see, for example, Ex. 1007 at p. 2).

196. Additionally, Network World states that “LWAPP lets network administrators use an array of interoperable access points and wireless system devices from multiple vendors” such that “they can make purchasing decisions based on the functionalities of individual access points and access controllers” (emphasis added, see, for example, Ex. 1007 at p. 2).

197. Finally, Network World states that “LWAPP is expected to move to a working group within the IETF in the first half of next year” and then “Standardization is projected to take approximately 18 to 24 months, but early vendor implementations exist today” with the additional information that “Calhoun is CTO of Airespace and one of the co-authors of the LWAPP protocol” (emphasis added, see, for example, Ex. 1007 at p. 3).

D. CAPWAP (Ex. 1008)

198. For example, amongst the numerous prior art references in this field, Internet-Draft draft-mani-ietf-capwap-arch-00 by M. Mani (Avaya), B. O'Hara (Airespace) et al., entitled “Architecture for Control and Provisioning of Wireless Access Points (CAPWAP)” (“CAPWAP”) was published by the Internet Engineering Task Force (IETF) of the Internet Society on Oct. 20, 2003 (see, for example, Ex. 1008 at p. 1). This document is publicly available at <https://datatracker.ietf.org/doc/draft-mani-capwap-arch/>. Thus, I understand that CAPWAP qualifies as prior art to the ‘384 Patent at least under 35 U.S.C. § 102(a).

199. CAPWAP starts by stating that “This Document analyzes WLAN (Wireless LAN) functions and services” and thereby “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)” (emphasis added, see, for example, Ex. 1008 at p. 2).

200. CAPWAP informs that “The purpose of CAPWAP work is to define the framework reflecting the architectural trend that delegates and aggregates selected WLAN functions and services from APs to ARs to enhance WLAN resource management” and thus “to provide a secure protocol to enable AP-to-AR communications and AP provisioning & management” (emphasis added, see, for example, Ex. 1008 at p. 4).

201. CAPWAP states that “Throughout the document the terminologies of AR (Access Router), AC (Access Controller) and AB (Access Bridge) are used synonymously in contexts of allowable network topology arguments” but “AC is to be assumed the generic term for the entity with which an AP registers or associates” (emphasis added, see, for example, Ex. 1008 at p. 5).

202. CAPWAP describes as “Motivation” that “As evidenced over the past few months, there is overwhelming support in the market for a new WLAN architecture” which “moves much of the functions that would reside in a traditional access point (AP) to a centralized access router (AR)”, thereby providing “benefits” that include “Ease of Use”, “Increased Security”, “Enhanced Mobility”, and “Quality of Service” (emphasis added, see, for example, Ex. 1008 at p. 9).

203. More specifically, with regard to “Quality of Service”, CAPWAP explains that “allowing the centralized AR manage the RF links” offers a “systemic perspective to perform efficient load balancing across multiple Access Points - thus increasing the efficiency of the wireless network” (emphasis added, see, for example, Ex. 1008 at p. 9).

204. Additionally, CAPWAP explains that such “benefits” described above are provided by “terminating the 802.11 management frames in the AR” wherein “This approach is also 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” using “a module in the AR that understands 802.11 management frames” while using the “LWAPP protocol and CAPWAP architecture” (emphasis added, see, for example, Ex. 1008 at p. 10).

205. I note that with respect to the disclosure of the “LWAPP protocol” for the “CAPWAP architecture” that CAPWAP observes that “LWAPP is a domain specific protocol with some messages assuming 802.11 semantics” (emphasis added, see, for example, Ex. 1008 at p. 28) and that CAPWAP specifically references for the “LWAPP protocol” as “[4]” the prior art reference I have referred to herein as LWAPP as shown in this excerpt from CAPWAP below (from Ex. 1008 at p. 31):

References

- [1] "IEEE WLAN MAC and PHY Layer Specifications", August 1999, <IEEE 802.11-99>.
- [2] "Advanced Encryption Standard (AES)", November 2001, <FIPS PUB 197>.
- [3] "Counter with CBC-MAC (CCM)", September 2003, <[RFC 3610](#)>.
- [4] "Light Weight Access Point Protocol (LWAPP)", June 2003, <<http://www.ietf.org/internet-drafts/draft-calhoun-seamoby-lwapp-03.txt>>.
- [5] "Security Requirements for a Light Weight Access Point Protocol", August 2003, <<http://www.ietf.org/internet-drafts/draft-kelly-ietf-lwapp-sec-00.txt>>.

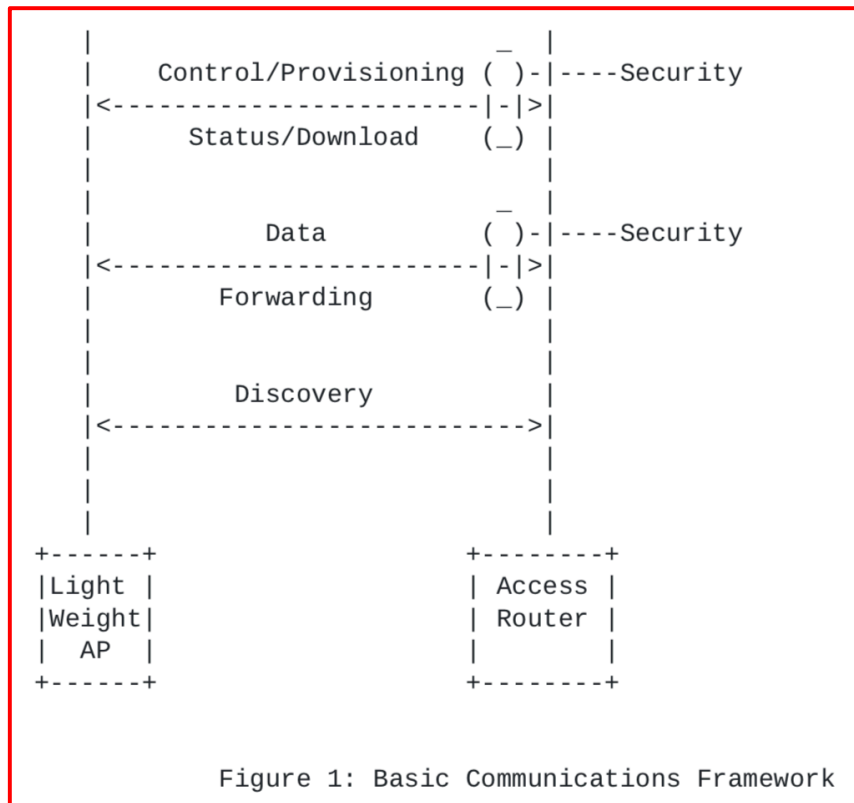
206. Therefore, in my opinion, a POSITA would understand even before considering the detailed disclosure of CAPWAP to follow that CAPWAP is from the same field of endeavor as the '384 Patent and that CAPWAP is reasonably pertinent to the problem faced by the '384 Patent (see, for example, ¶¶ 46-52 above regarding the '384 Patent in comparison with the above-summarized introduction to CAPWAP). Accordingly, CAPWAP is analogous art to the '384 Patent.

207. CAPWAP summarizes four different "architectures" in which "APs and ARs are linked" including "ARCH0" wherein the "classic AP" has "a self-contained controller possibly communicating with other APs", "ARCH1" wherein "APs" will "defer all WLAN functions other than real-time services" by using a "vertical (real-time frontend AP and aggregated backend AC) functional distribution", "ARCH2" wherein "APs" also "shift some normally real-time functions as well to the backend" with benefits such as extending OTA (over-the-air) protection for AP-AR", and "ARCH3" wherein "AC" becomes "a single "AP-switch" treating all connected APs as smart antennae" (emphasis added, see, for example, Ex. 1008 at p. 10).

208. Accordingly, CAPWAP teaches that "to allow for all such architectures to have a role with varying scope and limitations" in view of "varied market requirements" that include

“deployment scope”, “scalability”, “performance” and “end-end security demands” that “This further underscores the argument to provide a negotiable interface protocol” (emphasis added, see, for example, Ex. 1008 at p. 11).

209. CAPWAP explains that in view of the “three primary architecture types (and a fourth variant)” described above that “Figure 1 illustrates the basic outline of communications architecture between AP & AC” (emphasis added, see, for example, Ex. 1008 at p. 12, Figure 1 as reproduced below).



210. In reference to Figure 1 shown above, CAPWAP explains for the “Access Point Functions and Services” that “The services that MUST be in a lightweight AP are those that are directly related to the real-time aspects of the 802.11 MAC protocol and those related to the radio nature of an 802.11 AP” wherein “These functions are:” given in the list below (emphasis added, see, for example, Ex. 1008 at p. 14, excerpt as reproduced below).

- a) Privacy
- b) MSDU Delivery
- c) Beaconsing
- d) Synchronization
- e) Power Management
- f) Channel Assignment
- g) Transmit Power Control
- h) Clear Channel Assignment
- i) Radio Resource Measurement
- j) RADAR detection

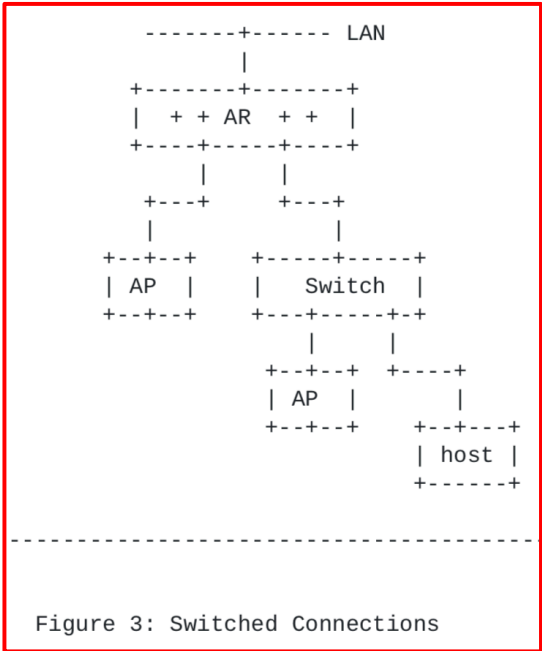
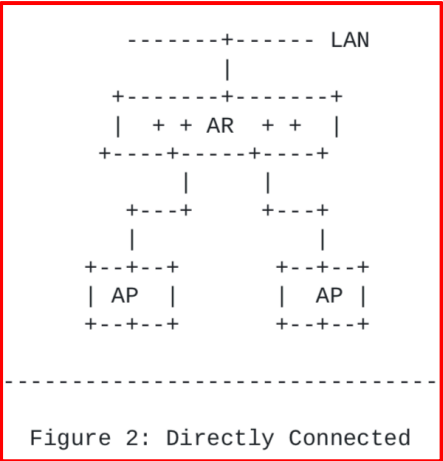
211. Additionally, CAPWAP explains for the “Access Controller Functions and Services” that “The functions that MAY be moved from the lightweight AP and located in the AR are those dealing with the management and control aspects of an 802.11 AP” such as “the distribution system services, in addition to authentication and deauthentication services” wherein “These functions are:” given in the list below (emphasis added, see, for example, Ex. 1008 at pp. 14-15, excerpt as reproduced below).

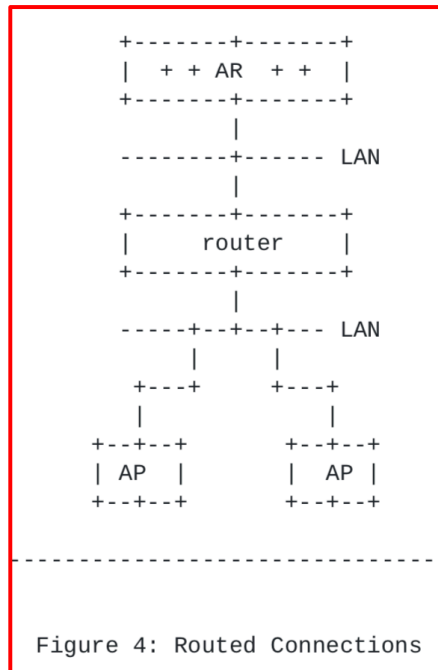
- a) Authentication
- b) Deauthentication
- c) Association
- d) Disassociation
- e) Reassociation
- f) Distribution
- g) Integration
- h) Dynamic Channel Selection
- i) Dynamic Control of transmit power

212. CAPWAP notes that for “Access Points” described as “Conventional” or “Heavy” that these “normally” also “support various services and protocols that provide seamless connectivity of WLAN clients to the wired network such as” given in the list below but that “Based on the definition of lightweight access points these services SHOULD qualify for offloading to the AR” (emphasis added, see, for example, Ex. 1008 at p. 15, excerpt as reproduced below).

- a) Port and Protocol-based VLANs
- b) SNMP
- c) QoS (DiffServ and 802.1Q) mapping
- d) IP routing
- e) DHCP relay/server
- f) RADIUS client/proxy
- g) MobileIP (client proxy)

213. CAPWAP also notes that the above “Functional distribution of WLAN services” described in earlier sub-sections are partly an artifact of the architecture types ARCH0-3” and “assumes that the AR and AP are within the same administrative domain” as shown in “several topologies” including Figures 2-4 (emphasis added, see, for example, Ex. 1008 at pp. 16-18, Figures 2-4 as reproduced below).





214. CAPWAP discloses that “for secure communications enabling automatic discovery, configuration and adaptive resource management” that “the AP's need to be set up securely in the AC(AR)'s domain” wherein “Identity 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” (emphasis added, see, for example, Ex. 1008 at p. 21).

215. For example, CAPWAP explains that “Configuration of an AP includes providing the parameters necessary for the AP to advertise and provide service for one or more WLANs” wherein such “parameters are both physical and logical” (emphasis added, see, for example, Ex. 1008 at p. 21).

216. More specifically, CAPWAP describes that these “Physical parameters are related to the operation of the AP's radio interface” and “include the channel on which the AP is to operate, the maximum power at which the AP is to transmit, antenna selections, the supported data rates, and the timing for the periodic announcements of the WLANs provisioned on the AP” (emphasis added, see, for example, Ex. 1008 at p. 21).

217. Additionally, CAPWAP describes that these “Logical parameters are related to the individual WLANs that are provisioned on the AP” and “include the SSID of the WLANs, the allowed authentication methods, the allowed privacy methods, values for the contention-free period and DTIM, VLAN associations, IP addresses and netmasks, authentication server addresses, any pre-shared keys for WLANs or authentication servers, regulatory (country) information, and other 802.11-specific capabilities to be advertised for the WLANs” (emphasis added, see, for example, Ex. 1008 at p. 21).

218. CAPWAP describes for the “discovery context” that “as part of provisioning an AP” and “based on negotiated architecture” that “one may configure the ability to offer redundancy of ACs” (emphasis added, see, for example, Ex. 1008 at p. 21).

219. More specifically, CAPWAP describes that “When a AP comes alive on a network it may authenticate and register with one or more ARs it detects on the network it is connected to” wherein this “identification of ARs is only dependent on the L2 or IP protocol used but is expected to be architecture-agnostic” such that “It is the Capability Negotiation Phase” that “follows which resolves the mutual capabilities of AP and AC which lets them decide to AP register with one or more AC” (emphasis added, see, for example, Ex. 1008 at p. 23).

220. Additionally, CAPWAP specifically describes this “Capabilities Negotiation” wherein “Upon having discovered available ARs the AP enters into a capabilities exchange phase with the candidate ACs” such that “If 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” and thus “The capabilities negotiated by architectural type match will decide the applicable API's between AP and AC” (emphasis added, see, for example, Ex. 1008 at p. 23).

221. As a “Summary”, CAPWAP states that it “allows for a set of flexible architectures” in order “to achieve the Security, Ease of Management, Enhanced QoS and Mobility objectives across the WLAN domain” based upon a “set of CAPWAP services” which include “AC Discovery”, “Capability Negotiation”, “Mutual Authentication of AP and AC”, “Secure Encapsulation Protocol based on Secure Key Management”, “Secure AP Configuration from AC”, and “Secure Encapsulation of Control and/or Data between AP & AC” (emphasis added, see, for example, Ex. 1008 at p. 24).

222. I note that CAPWAP provides “Acknowledgements” to “Pat Calhoun” and “Scott Kelly” for “completion of this document in a very short time” and “consenting to let us adapt from their topological and architectural analysis” (see, for example, Ex. 1008 at p. 30). I also note that CAPWAP continued with multiple versions within the IETF standards organization and eventually released as a completed standard RFC 5412 entitled “Lightweight Access Point Protocol” by P. Calhoun et al. in Feb. 2010 (see, for example, <https://datatracker.ietf.org/doc/rfc5412/> or Ex. 1011 at p. 1).

E. IEEE 802.11-1999 (Ex. 1009)

223. For example, amongst the numerous prior art references in this field, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, ANSI/IEEE Std 802.11, 1999 Edition (“IEEE 802.11-1999”) was published Aug. 20, 1999 (see, for example, Ex. 1009 at p. iii). Thus, I understand that IEEE 802.11-1999 qualifies as prior art to the ‘384 Patent at least under §§ 102(a) and 102(b).

224. IEEE 802.11-1999 describes that “The scope of this standard is to develop a medium access control (MAC) and physical layer (PHY) specification for wireless connectivity for fixed, portable, and moving stations within a local area” (emphasis added, see, for example, Ex. 1009 at §§ 1.1, 1.2).

225. IEEE 802.11-1999 describes that “the addressable unit is a station (STA)”, “Mobile stations actually address the LAN while in motion”, and “The basic service set (BSS) is the basic building block of an IEEE 802.11 LAN” wherein “a BSS may also form a component of an extended form of network that is built with multiple BSSs” wherein “The architectural component used to interconnect BSSs is the distribution system (DS)” (emphasis added, see, for example, Ex. 1009 at §§ 5.1.1.1, 5.1.1.3, 5.2, 5.2.2).

226. Additionally, IEEE 802.11-1999 describes that “The association between a STA and a BSS is dynamic (STAs turn on, turn off, come within range, and go out of range)” and “To become a member of an infrastructure BSS, a station shall become “associated”” wherein such “associations are dynamic and involve the use of the distribution system service (DSS)” as provided by “An access point (AP)” that “is a STA that provides access to the DS by providing DS services in addition to acting as a STA” such that “Data move between a BSS and the DS via

an AP” (emphasis added, see, for example, Ex. 1009 at §§ 5.2.1.1, 5.2.2, Figure 2 as reproduced below).

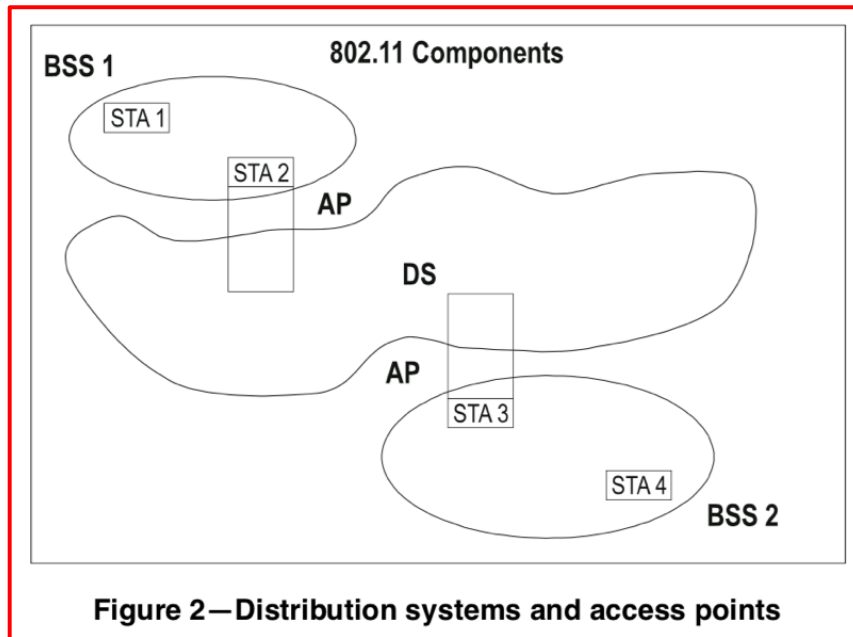
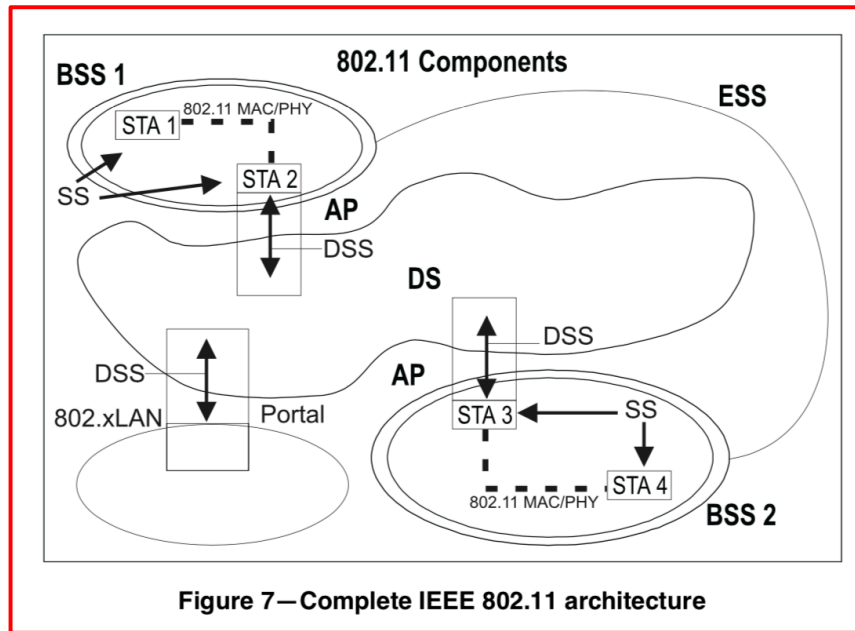


Figure 2—Distribution systems and access points

227. According to IEEE 802.11-1999, “IEEE 802.11 explicitly does not specify the details of DS implementations” but “Instead, IEEE 802.11 specifies services” for which “There are two categories of IEEE 802.11 service—the station service (SS) and the distribution system service (DSS)” with both “used by the IEEE 802.11 MAC sublayer” (bold emphasis in original, other emphasis added, see, for example, Ex. 1009 at § 5.3).

228. More specifically, IEEE 802.11-1999 discloses that the “station service (SS)” is “present in every IEEE 802.11 station (including APs, as APs include station functionality)” and includes “Authentication”, “Deauthentication”, “Privacy”, and “MSDU delivery” while the “distribution system service (DSS)” are provided by an “AP” and include “Association”, “Disassociation”, “Distribution”, “Integration”, and “Reassociation” wherein “Figure 7 combines the components from previous figures with both types of services to show the complete

IEEE 802.11 architecture” (emphasis added, see, for example, Ex. 1009 at §§ 5.3.1, 5.3.2, Figure 7 as reproduced below).



229. In reference to the above-noted “nine services specified by IEEE 802.11”, IEEE 802.11-1999 explains that “Six of the services are used to support MSDU delivery between STAs” while “Three of the services are used to control IEEE 802.11 LAN access and confidentiality” and further that “Each of the services is supported by one or more MAC frame types” (emphasis added, see, for example, Ex. 1009 at § 5.4).

230. Additionally, IEEE 802.11-1999 discloses that “The IEEE 802.11 MAC sublayer uses three types of messages—data, management, and control (see Clause 7)” wherein “The data messages are handled via the MAC data service path”, “MAC management messages are used to support the IEEE 802.11 services and are handled via the MAC management service data path”, and “MAC control messages are used to support the delivery of IEEE 802.11 data and management messages” (emphasis added, see, for example, Ex. 1009 at § 5.4).

231. For example, IEEE 802.11-1999 discloses that “At any given instant, a STA may be associated with no more than one AP” and that “Association is always initiated by the mobile STA, not the AP” while conversely, “An AP may be associated with many STAs at one time” (emphasis added, see, for example, Ex. 1009 at § 5.4.2.2).

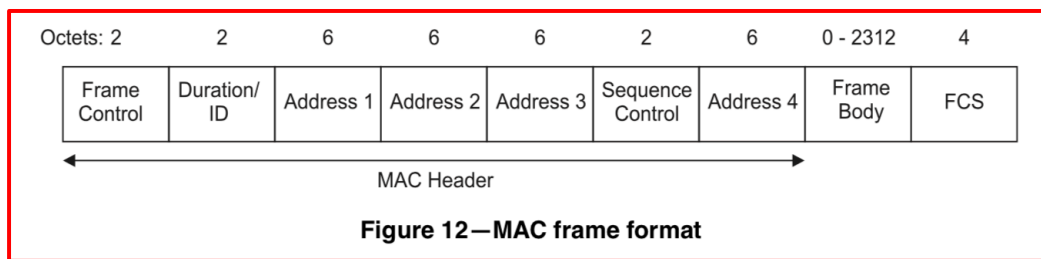
232. Also, IEEE 802.11-1999 discloses that “The disassociation service is invoked whenever an existing association is to be terminated” which “may be invoked by either party to an association (non-AP STA or AP)” wherein “Disassociation is a notification, not a request” and “cannot be refused by either party to the association” but “the MAC protocol does not depend on STAs invoking the disassociation service” (emphasis added, see, for example, Ex. 1009 at § 5.4.2.4).

233. According to IEEE 802.11-1999, “Two services are provided to bring the IEEE 802.11 functionality in line with wired LAN assumptions; authentication and privacy” wherein “Authentication is used instead of the wired media physical connection” and “Privacy is used to provide the confidential aspects of closed wired media” (emphasis added, see, for example, Ex. 1009 at § 5.4.3).

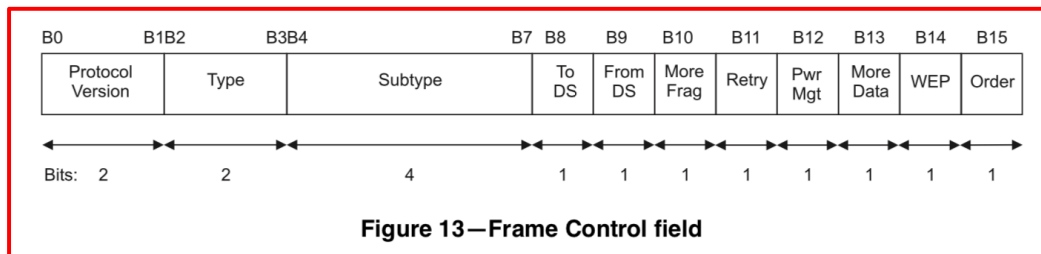
234. More specifically, “IEEE 802.11 provides the ability to control LAN access via the authentication service” which “is used by all stations to establish their identity to stations with which they will communicate” such that “If a mutually acceptable level of authentication has not been established between two stations, an association shall not be established” but “A STA may be authenticated with many other STAs at any given instant” (emphasis added, see, for example, Ex. 1009 at § 5.4.3.1).

235. Additionally, “IEEE 802.11 provides the ability to encrypt the contents of messages” wherein “This functionality is provided by the privacy service” that will “perform the actual encryption of messages” (emphasis added, see, for example, Ex. 1009 at § 5.4.3.3).

236. According to IEEE 802.11-1999, “Each frame consists of the following basic components: a) A **MAC header**, which comprises frame control, duration, address, and sequence control information; b) A variable length **frame body**, which contains information specific to the frame type; c) A **frame check sequence** (FCS), which contains an IEEE 32-bit cyclic redundancy code (CRC)” wherein “Figure 12 depicts the general MAC frame format” (bold emphasis in original, emphasis added, see, for example, IEEE 802.11-1999 at §§ 7.1, 7.1.2, Figure 12 as reproduced below).



237. More specifically, in reference to Figure 12 shown above, IEEE 802.11-1999 discloses that “The format of the Frame Control field is illustrated in Figure 13” (emphasis added, see, for example, IEEE 802.11-1999 at § 7.1.3.1, Figure 13 as reproduced below).



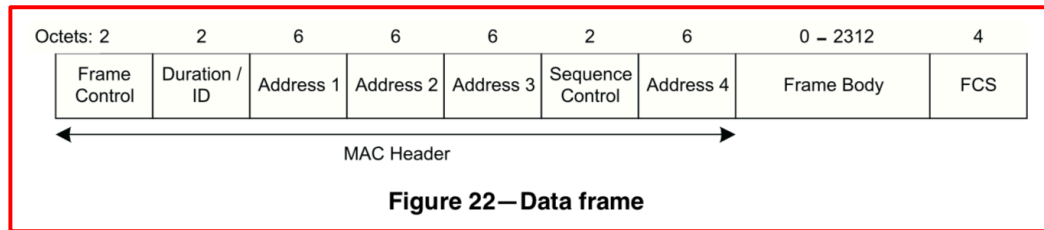
238. In reference to Figure 13 shown above, IEEE 802.11-1999 discloses that “The Type and Subtype fields together identify the function of the frame” among “three frame types:

control, data, and management” wherein “Table 1 defines the valid combinations of type and subtype” (emphasis added, see, for example, IEEE 802.11-1999 at § 7.1.3.1.2, Table 1 as reproduced below).

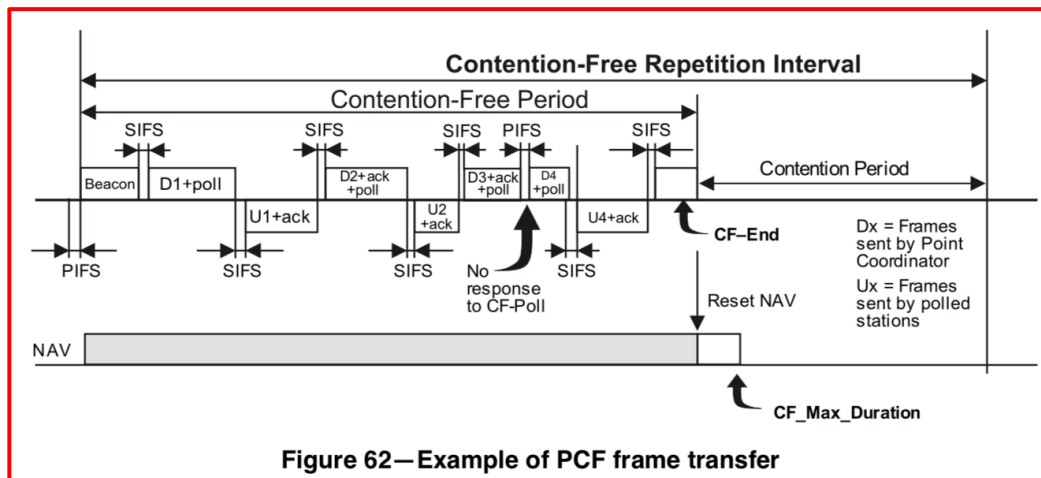
Table 1—Valid type and subtype combinations			
Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110–0111	Reserved
00	Management	1000	Beacon
00	Management	1001	Announcement traffic indication message (ATIM)
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101–1111	Reserved
01	Control	0000–1001	Reserved
01	Control	1010	Power Save (PS)-Poll
01	Control	1011	Request To Send (RTS)
01	Control	1100	Clear To Send (CTS)
01	Control	1101	Acknowledgment (ACK)
01	Control	1110	Contention-Free (CF)-End
01	Control	1111	CF-End + CF-Ack
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-Ack + CF-Poll
10	Data	0100	Null function (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000–1111	Reserved
11	Reserved	0000–1111	Reserved

239. According to IEEE 802.11-1999, “The frame format for a Data frame is independent of subtype and is as defined in Figure 22” wherein “The content of the Address

fields of the data frame is dependent upon the values of the To DS and From DS bits” (emphasis added, see, for example, IEEE 802.11-1999 at § 7.2.2, Figure 22 as reproduced below).



240. According to IEEE 802.11-1999, the “Point Coordination Function” or “PCF provides contention-free frame transfer” wherein “Frame transfers under the PCF typically consist of frames alternately sent from the AP/PC and sent to the AP/PC” such that “During the CFP, the ordering of these transmissions, and the STA allowed to transmit frames to the PC at any given point in time, shall be controlled by the PC” wherein “Figure 62 depicts a frame transfer during a typical CFP” (emphasis added, see, for example, IEEE 802.11-1999 at §§ 9.3, 9.3.3, , Figure 62 as reproduced below).



VIII. ANTICIPATION AND/OR OBVIOUSNESS OF THE ‘384 PATENT UNDER 35 U.S.C. §§ 102, 103 DUE TO CALHOUN, LWAPP AND/OR CAPWAP

241. In my opinion, Calhoun anticipates at least Claims 1, 3-4 and 6 of the ‘384 Patent for at least the reasons described herein.

242. In my opinion, Calhoun enabled a POSITA to practice Claims 1, 3-4 and 6 of the ‘384 Patent at least to the same extent that the specification of the ‘384 Patent is considered to enable a POSITA to practice Claims 1, 3-4 and 6 of the ‘384 Patent.

243. In my opinion, Calhoun in view of LWAPP and CAPWAP renders obvious at least Claims 1-6 of the ‘384 Patent for at least the reasons described herein.

244. Calhoun is analogous art to the ‘384 Patent (see ¶ 122 above). Similarly, LWAPP is also analogous art to the ‘384 Patent (see ¶ 154 above). Additionally, CAPWAP is analogous art to the ‘384 Patent (see ¶ 206 above).

245. A general overview of Calhoun is given at ¶¶ 109-145 above.

246. A general overview of LWAPP is given at ¶¶ 146-185 above.

247. A general overview of CAPWAP is given at ¶¶ 198-221 above.

248. In my opinion, a POSITA at the alleged time of invention for the ‘384 Patent would have been highly motivated to combine Calhoun, LWAPP and CAPWAP for at least the following reasons.

249. First, each of Calhoun, LWAPP and CAPWAP addresses the same wireless communications field of art specifically for IEEE 802.11 wireless local area networking (see, for example, ¶¶ 110-114, 147-149 and 199-204 above).

250. Second, each of Calhoun, LWAPP and CAPWAP are directed to solving deployment challenges for the same basic system architecture of IEEE 802.11 wireless local area networks.

251. For example, Calhoun discloses a “system architecture” in which “a central control element manages and controls one more access elements” wherein such “access elements perform real-time communication functions, such as data transfer and acknowledgements, while the central control element manages the connection between the access element and one or more wireless client devices” (see, for example, ¶ 112 above).

252. Similarly, LWAPP is directed to a system with “simple Access Points in 802.11 that are managed by a router or switch (also known as an Access router, or AR)” that provides “Centralization of the bridging, forwarding, authentication, encryption and policy enforcement functions for a WLAN” (see, for example, ¶ 148 above).

253. And also similarly, CAPWAP is directed to a system with “lightweight Access Point (LAP)” and “AP Controllers or AR (Access Router)” wherein this “new WLAN architecture” “moves much of the functions that would reside in a traditional access point (AP) to a centralized access router (AR)” (see, for example, ¶¶ 199 and 202 above).

254. Accordingly, in my opinion, a POSITA would have been highly motivated to combine Calhoun, LWAPP and CAPWAP at least because each is directed to solving deployment challenges for the AP controller system architecture that was becoming popular in the industry at the alleged time of invention for the ‘384 Patent (see also ¶ 14 above).

255. Third, each of Calhoun, LWAPP and CAPWAP propose similar and related solutions for these deployment challenges for the AP controller system architecture.

256. For example, Calhoun discloses a “Light-Weight Access Point Protocol (LWAPP)” as including “functionality directed to initialization and configuration of managed access elements” across “three main phases: discovery, joinder, and configuration” (see, for example, ¶ 120 above).

257. Similarly, LWAPP discloses that “the Light Weight Access Point Protocol” allows “a router or switch to interoperably control and manage a collection of wireless Access Points” and “begins with a discovery phase” such that “Once the AP and the AR have joined, a configuration exchange is accomplished” (see, for example, ¶¶ 147, 150 and 152 above).

258. And also similarly, CAPWAP discloses use of this same “LWAPP protocol” as a “secure protocol to enable AP-to-AR communications and AP provisioning & management” such that “Upon having discovered available ARs the AP enters into a capabilities exchange phase with the candidate ACs” wherein “the AP registers with the AC and configures itself based on the policies it derives from the AC” (see, for example, ¶¶ 200, 205 and 220 above).

259. Accordingly, in my opinion, a POSITA would have been highly motivated to combine Calhoun, LWAPP and CAPWAP at least because each discloses using the Light Weight Access Point Protocol for management of WLAN access points in an AP controller system architecture by beginning with discovery and then transitioning to configuration, thereby teaching a POSITA that the combination would produce predictable and well understood results.

260. Fourth, Calhoun, LWAPP and CAPWAP share a common lineage in a similar timeframe for addressing a similar problem, thereby further suggesting to a POSITA that the combination would produce predictable and well understood results.

261. For example, the lead inventor for Calhoun, dated Mar. 21, 2003, is Patrice Calhoun, who was known to be the CTO of Airespace (later acquired by Cisco), the co-inventors

are Scott Kelly and Rohit Suri (also with Airespace), and the invention is entitled “Light-weight Access Point Protocol” (see, for example, ¶¶ 109 and 197 above).

262. Similarly, the lead author for LWAPP is also Patrice Calhoun and co-authors for LWAPP include Bob O’Hara, Scott Kelly and Rohit Suri, all four of which are with Airespace, and this Internet-Draft is entitled “Light Weight Access Point Protocol” and dated Jun. 28, 2003 (see, for example, ¶ 146 above).

263. And also similarly, one author for CAPWAP is Bob O’Hara with specific acknowledgment to contributions by Patrice Calhoun and Scott Kelly, all three of which are with Airespace, and this Internet-Draft is dated Oct. 20, 2003 and references the LWAPP prior art as the source of the “LWAPP protocol” on which CAPWAP is based (see, for example, ¶¶ 198, 205 and 222 above).

264. Accordingly, in my opinion, a POSITA would have been highly motivated to combine Calhoun, LWAPP and CAPWAP at least because the common authors such as Patrice Calhoun, Bob O’Hara and Scott Kelly, the common organization such as Airespace, the common reference to using a “Light Weight Access Point Protocol”, and the short timeframe of approximately 7 months in 2003 in which all three references were dated provides a strong indication to a POSITA that the combination would produce predictable and well understood results.

265. Fifth, additional prior art also would have highly motivated a POSITA to combine Calhoun, LWAPP and CAPWAP.

266. For example, Network World states that “Centralized 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” (see, for example, ¶ 187 above), which teaches a POSITA of the desirability of the AP controller system architecture that was becoming popular in the industry at the alleged time of invention for the ‘384 Patent (see also ¶ 14 above).

267. For example, Network World states “Lightweight Access Point Protocol (LWAPP)” is “a draft standard” that “the Internet Engineering Task Force is considering as part of the Control and Provisioning of Wireless Access Points (CAPWAP), which is in the preliminary stages of becoming an IETF working group” (see, for example, ¶ 188 above), which teaches a POSITA that CAPWAP is the emerging relevant standard for the AP controller system architecture and that CAPWAP is based upon the “Light Weight Access Point Protocol” currently being developed by at least Patrice Calhoun, Bob O’Hara and Scott Kelly per the Calhoun and LWAPP prior art references.

268. For example, Network World states “LWAPP has several practical benefits” which include that “The protocol centralizes traffic handling, authentication, encryption and policy enforcement (quality of service and security) capabilities within the access controller” and that “LWAPP lets network administrators use an array of interoperable access points and wireless system devices from multiple vendors” (see, for example, ¶¶ 195-196 above), which teaches a POSITA that the known AP controller system architecture benefits by adopting the specific capabilities described by the Calhoun, LWAPP and CAPWAP prior art references.

269. Accordingly, in my opinion, a POSITA would have been highly motivated to combine Calhoun, LWAPP and CAPWAP at least because the prior art specifically teaches the desirability of this combination to address market forces such as centralized management of WLANs with interoperable devices from multiple vendors.

270. In my opinion, a POSITA at the alleged time of invention for the ‘384 Patent would have combined Calhoun, LWAPP and CAPWAP to create an IEEE 802.11-based WLAN system of access points and controller nodes that realizes the benefits described by Network World based upon at least the network and device elements as disclosed in Calhoun combined with at least the specific interface protocol details as disclosed in LWAPP in order to at least implement the negotiable interface protocol and various functional split architectures for such access points and controller nodes as disclosed collectively in Calhoun, LWAPP and CAPWAP.

271. My specific analyses of Calhoun and of Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA, with respect to every claim element of Claims 1-6 of the ‘384 Patent is given herein.

272. Note that for purposes of my analysis herein that I have provided subsection headings for claim elements in the form “1(a)”, “1(b)”, etc. for the convenience of the reader even though such headings do not exist in the actual ‘384 Patent claims themselves.

'384 Patent: Claim 1

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

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

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

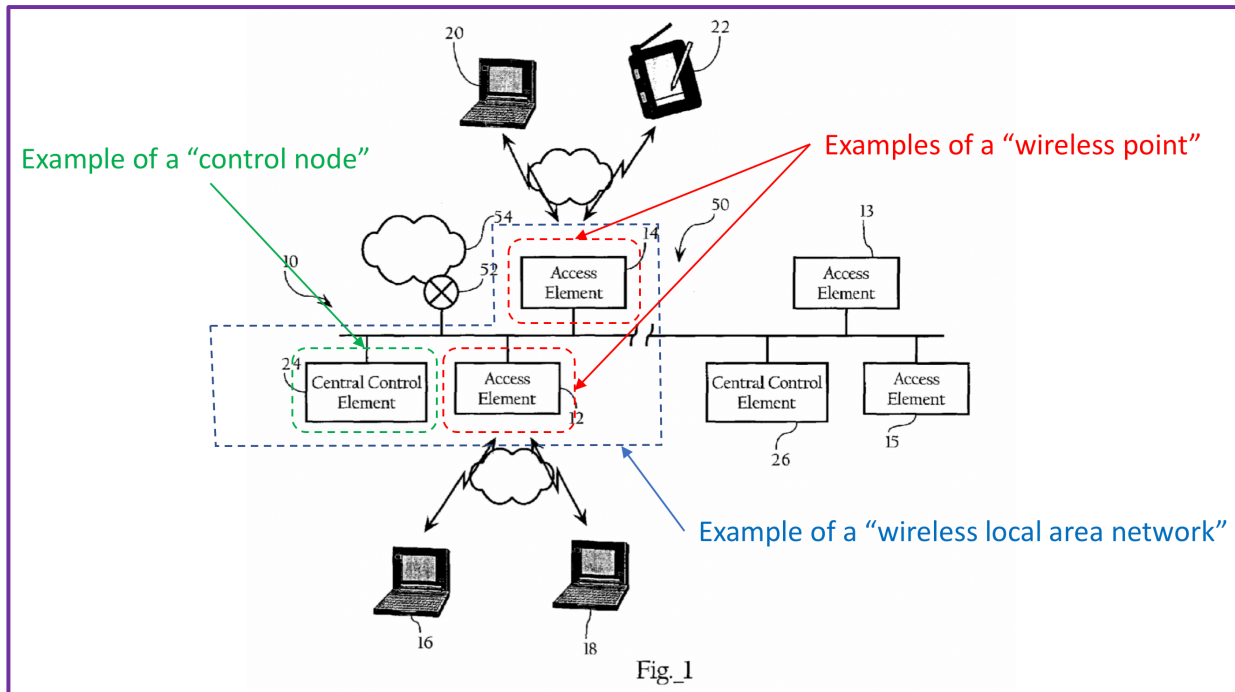
 a session establishing unit configured to establish a secure session with said selected one control node; and

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

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

273. I have considered that this preamble claim element may be limiting.

274. Calhoun discloses “methods, apparatuses and systems facilitating the deployment and configuration of managed access points in a wireless network system” wherein “FIG. 1” shows a “block diagram of a wireless Local Area Network (LAN) 10” that includes such “managed access points” in the form of “access elements 12-15 for wireless communication with remote client elements 16, 18, 20, 22” (see, for example, ¶¶ 110, 113 and 145 above, and annotated FIG. 1 shown below).



275. For example, Calhoun discloses a “system architecture” in which “a central control element manages and controls one more access elements” wherein such “access elements perform real-time communication functions, such as data transfer and acknowledgements, while the central control element manages the connection between the access element and one or more wireless client devices” (see, for example, ¶¶ 112 and 145 above).

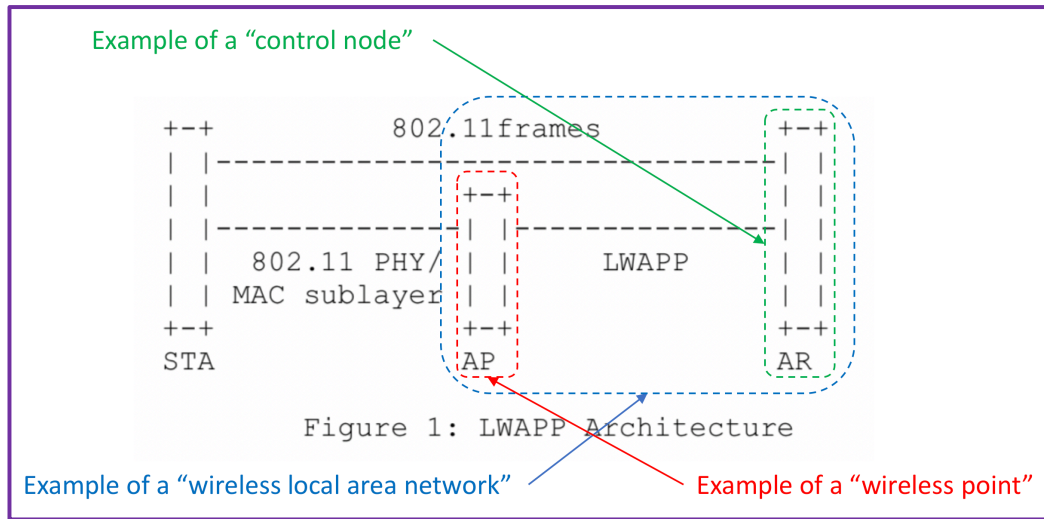
276. For example, Calhoun discloses that although “The access elements 12-15 are coupled via communication means using a wireless local area network (WLAN) protocol (e.g., IEEE 802.11a or 802.11b, etc.) to the client remote elements 16, 18, 20, 22” and “have been described as operating in 802.11 wireless networks” that 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 acknowledgment of the communication of those messages without conventional processing thereof” (see, for example, ¶¶ 114, 116 and 142 above).

277. For example, Calhoun discloses that when “operating in 802.11 wireless networks” that “the division of functionality between the access elements and the central control elements can be shifted” wherein “For example, the access elements can bridge network traffic associated with the remote client elements directly, while transmitting management packets to the central control element” (see, for example, ¶¶ 142-143 above).

278. Thus, Calhoun discloses a “**wireless local area network**” (for example, the “**wireless Local Area Network (LAN)**” as also depicted in FIG. 1 of Calhoun), “**one or more control nodes**” (for example, the “**central control elements**” of Calhoun), and a “**wireless point**” (for example, the “**managed access points**” or “**access elements**” of Calhoun) that “**provides for functions for a wireless local area network to be separated between said wireless point and one or more control nodes**” (for example, when “**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**” in order to “**perform link layer management functions, such as authentication and association**” as part of a “**division of functionality between the access elements and the central control elements**”).

279. Therefore, in my opinion, Calhoun discloses the limitations of this claim element, if any.

280. LWAPP discloses “the Light Weight Access Point Protocol which is a protocol allowing a router or switch to interoperably control and manage a collection of wireless Access Points” in order to “simplify the deployment and management of wireless networks” as shown in the “LWAPP Architecture” diagram (see, for example, ¶¶ 147-148 above, and annotated Figure 1 shown below).



281. For example, LWAPP discloses “simple Access Points in 802.11 that are managed by a router or switch (also known as an Access router, or AR)” such that “The APs can be considered as remote RF interfaces, being controlled by the AR (see Figure 1)” (see, for example, ¶¶ 148-149 above).

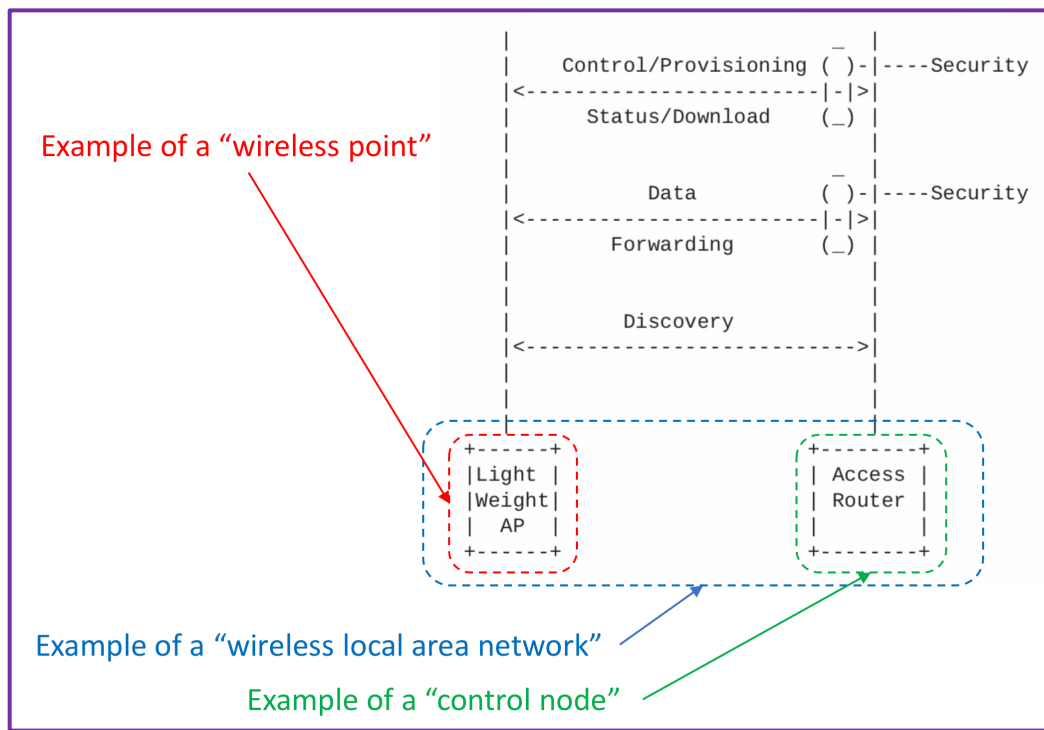
282. For example, LWAPP discloses that “The AP forwards all 802.11 frames received to the AR via the LWAPP protocol, which processes the frames” including, for example, the “bridging, forwarding, authentication, encryption and policy enforcement functions for a WLAN” (see, for example, ¶¶ 148-149 above).

283. Thus, LWAPP discloses a “**wireless local area network**” (for example, the “**WLAN**” as also depicted in Figure 1 of LWAPP), “**one or more control nodes**” (for example, the “**Access router, or AR**” of LWAPP), and a “**wireless point**” (for example, the “**simple**” or “**Light Weight**” “**Access Points**” or “**APs**” of LWAPP) that “**provides for functions for a wireless local area network to be separated between said wireless point and one or more control nodes**” (for example, when operating “**in 802.11**” the “**APs can be considered as remote RF interfaces**” while the “**bridging, forwarding, authentication, encryption and policy**

enforcement functions for a WLAN” are performed at the “**Access router, or AR**” per the disclosures of LWAPP).

284. Therefore, in my opinion, LWAPP discloses the limitations of this claim element, if any.

285. CAPWAP informs that “The purpose of CAPWAP work is to define the framework reflecting the architectural trend that delegates and aggregates selected WLAN functions and services from APs to ARs to enhance WLAN resource management” wherein “Figure 1 illustrates the basic outline of communications architecture between AP & AC” (see, for example, ¶¶ 199 and 209 above, and annotated Figure 1 shown below).



286. CAPWAP “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)” and explains for the “Access Point Functions and Services” that “The services that MUST be in a lightweight AP

are those that are directly related to the real-time aspects of the 802.11 MAC protocol and those related to the radio nature of an 802.11 AP” (see, for example, ¶¶ 199 and 210 above).

287. For example, CAPWAP explains that “terminating the 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” (see, for example, ¶ 204 above).

288. Thus, CAPWAP discloses a “**wireless local area network**” (for example, the “**WLAN**” as also depicted in Figure 1 of CAPWAP), “**one or more control nodes**” (for example, the “**AR (Access Router), AC (Access Controller) and AB (Access Bridge)**” that “**are used synonymously**” in CAPWAP), and a “**wireless point**” (for example, the “**lightweight Access Point (LAP)**” of CAPWAP) that “**provides for functions for a wireless local area network to be separated between said wireless point and one or more control nodes**” (for example, when the “**functions as allowed in the Standards and practiced in the industry**” are “**meaningfully split between lightweight Access Point (LAP)**” and “**AP Controllers or AR (Access Router)**” with “**real-time components**” in the “**Access Point**” and “**access control components**” in the “**Access Router**” per the disclosures of CAPWAP).

289. Therefore, in my opinion, CAPWAP discloses the limitations of this claim element, if any.

290. See at least ¶¶ 248-270 above regarding the combination of Calhoun, LWAPP and CAPWAP.

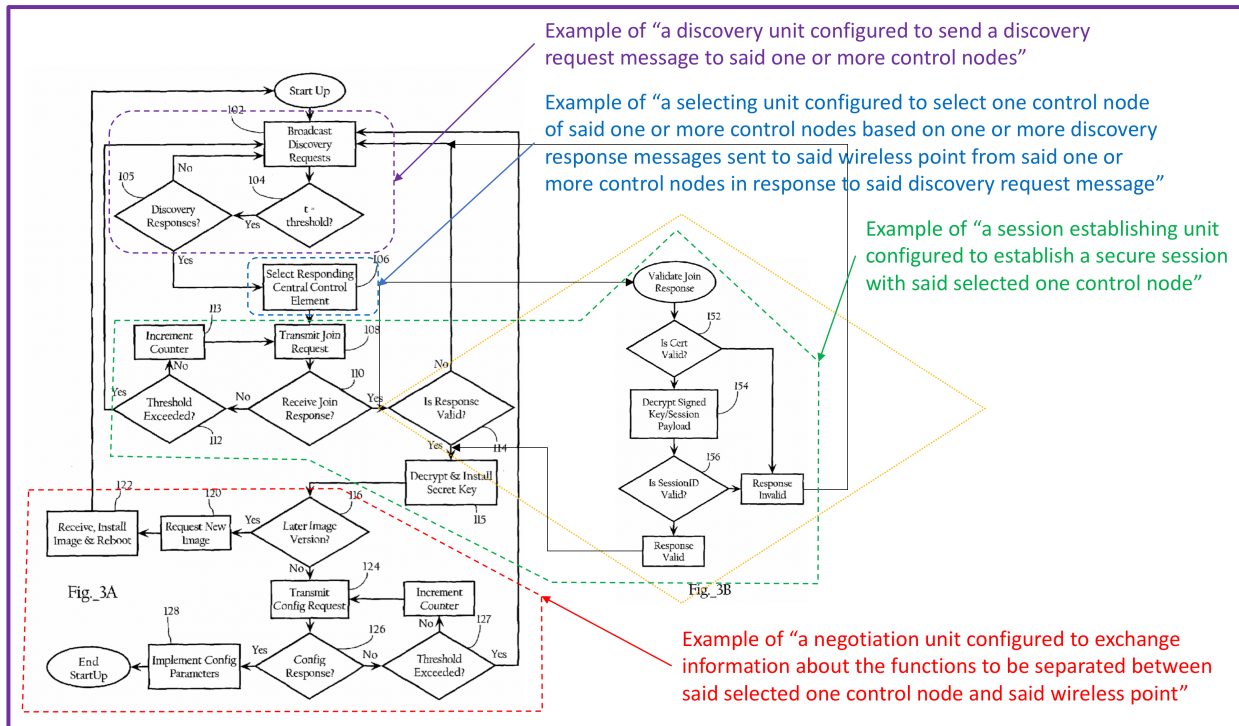
291. At least because each of Calhoun, LWAPP and CAPWAP discloses the limitations of this claim element, if any, then Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA also renders obvious the limitations of this claim element, if any.

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

292. Calhoun discloses a “Light-Weight Access Point Protocol (LWAPP)” as including “functionality directed to initialization and configuration of managed access elements” across “three main phases: discovery, joinder, and configuration” such that “During the discovery phase, the access element discovers the central control elements to which it can associate” (see, for example, ¶¶ 120-121 above).

293. Calhoun explains that “At startup, access element 15 broadcasts or multicasts discovery requests throughout the virtual subnet implemented by the VLAN in an attempt to identify central control elements (102)” wherein such “discovery request may be a single IP packet or native link layer frame, such as an Ethernet frame” and then “access element 15 waits a threshold period of time for the receipt of discovery responses (104, 105) before broadcasting or multicasting additional discovery requests” (see, for example, ¶ 124 above).

294. Calhoun discloses that such “***implementing the discovery, joinder and configuration phases of LWAPP***” is also shown by the “***flow chart diagrams***” FIG. 3A and FIG. 3B of Calhoun (see, for example, ¶¶ 123 and 134 above, and annotated composite FIG. 3A and FIG. 3B shown below).



295. Thus, Calhoun discloses a “**discovery unit**” (for example, the above annotated portion of composite FIG. 3A and FIG. 3B of Calhoun) that is “**configured to send a discovery request message to said one or more control nodes**” (for example, when an “*access element*” “*broadcasts or multicasts discovery requests throughout the virtual subnet implemented by the VLAN in an attempt to identify central control elements*”).

296. Therefore, in my opinion, Calhoun discloses the limitations of this claim element.

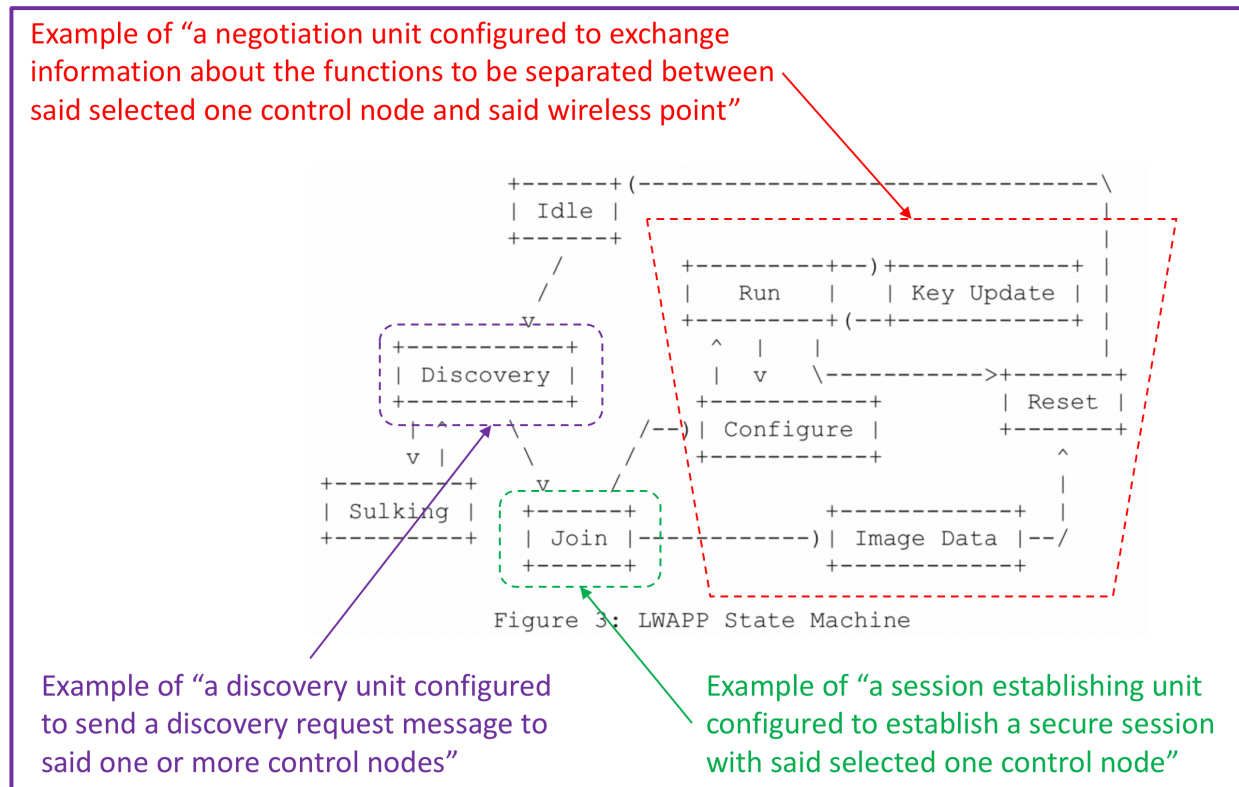
297. LWAPP discloses that “The *Light Weight Access Protocol* (LWAPP) *begins with a discovery phase*, whereby the *APs send a Discovery Request frame*, causing any *Access Router (AR)* [9], receiving that frame to *respond with a Discovery Reply*” (see, for example, ¶ 150 above).

298. For example, LWAPP explains that “The *Discovery Request* is *used by the AP* to automatically *discovery potential ARs* available in the network” wherein such “*Discovery*

Request carries the following *message elements*: *AP Payload*” and “*Radio Payload* (one for each radio in the AP)” (see, for example, ¶¶ 162-163 above).

299. For example, LWAPP explains that “*When run over Ethernet*, the LWAPP protocol is *restricted to a specific Ethernet segment*” such that “The *AR discovery mechanism* used with this transport is for the *Discovery Request message to be transmitted to a broadcast address*” (see, for example, ¶ 179 above).

300. LWAPP provides a “*state diagram*” that “represents the *lifecycle of an AP-AR session*” in Figure 3 (see, for example, ¶ 159 above), which, in my opinion, a POSITA would understand discloses a “**discovery unit**” within each “**Access Point**” that is “**configured to send a discovery request message to said one or more control nodes**” per the recited limitations of this claim element as discussed above and shown by my annotated version of Figure 3 of LWAPP:



301. Thus, LWAPP discloses a **“discovery unit”** (for example, the above annotated portions of Figure 3 of LWAPP) that is **“configured to send a discovery request message to said one or more control nodes”** (for example, when an *“Access Point”* **“send[s] a Discovery Request frame”** as a **“Discovery Request message to be transmitted to a broadcast address”** to **“automatically discovery potential ARs available in the network”**).

302. Therefore, in my opinion, LWAPP discloses the limitations of this claim element.

303. CAPWAP discloses “automatic discovery” for “AP’s” that are “set up securely in the AC(AR)’s domain” (see, for example, ¶ 214 above). CAPWAP also discloses that “Figure 1 illustrates the basic outline of communications architecture between AP & AC” which includes “Discovery” messages being exchanged between AP and AC (see, for example, ¶ 209 above).

304. Accordingly, a POSITA would understand that this **“automatic discovery”** using **“Discovery”** messages being exchanged between the *“Access Point”* and the *“Access Controller”* or *“Access Router”* within the *“AC(AR)’s domain”* of CAPWAP discloses at least that the *“Access Point”* of CAPWAP is configured **“to send a discovery request message to said one or more control nodes”** as recited for this claim element.

305. Thus, CAPWAP discloses an *“Access Point”* that is **“configured to send a discovery request message to said one or more control nodes”** (for example, when an *“Access Point”* uses **“Discovery”** messages being exchanged with the *“Access Controller”* or *“Access Router”* within the *“AC(AR)’s domain”*).

306. See at least ¶¶ 248-270 above regarding the combination of Calhoun, LWAPP and CAPWAP.

307. At least because each of Calhoun and LWAPP discloses the limitations of this claim element, and because CAPWAP also discloses at least certain limitations of this claim

element, then Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA also renders obvious the limitations of this claim element.

308. As an alternative claim construction, I have been asked by Counsel for the Petitioner to also analyze this claim while assuming that this claim element may be construed as a matter of law as a means for performing a recited function as set out in 35 U.S.C. § 112, ¶ 6, wherein the recited function would be “**send[ing] a discovery request message to said one or more control nodes**” and the proposed structure in the specification of the ‘384 Patent for performing such function as a “**discovery unit**” that the “**wireless point compris[es]**” would be described by the “operational step” denoted as “**201**” in FIG. 2 as well as the applicable text in 8:59-67 of the ‘384 Patent (see, for example, ¶¶ 58-59 above).

309. Under the alternative claim construction of ¶ 308 above, I note that Calhoun discloses identically the recited function of “**send[ing] a discovery request message to said one or more control nodes**” as I have described herein (see, for example, ¶¶ 292-296 above).

310. Calhoun also discloses structure for a “**discovery unit**” that the “**wireless point compris[es]**” by at least the “*flow chart diagrams*” FIG. 3A and FIG. 3B of Calhoun as I have annotated herein (see, for example, ¶ 294 above).

311. Under the alternative claim construction of ¶ 308 above, I believe a POSITA would understand the “way” that the proposed structure in the specification of the ‘384 Patent would be deemed to perform the function of “**send[ing] a discovery request message to said one or more control nodes**” is by “*any node discovery protocol*” or by the *broadcast/multicast/anycast of a specific, mutually recognizable message*”, thereby leading to the “result” of “*invoking responses from available CNs*” (see, for example, ¶ 59 above).

312. Similarly, the “way” that the structure for a **“discovery unit”** that the **“wireless point compris[es]”** in Calhoun performs the function of **“send[ing] a discovery request message to said one or more control nodes”** is when it *“broadcasts or multicasts discovery requests throughout the virtual subnet implemented by the VLAN in an attempt to identify central control elements”* during the *“discovery phase”*, thereby leading to the “result” of *“discovery responses”* from the *“central control elements”* (see, for example, ¶¶ 292-293 above).

313. In my opinion, a POSITA would understand that the “way” that an **“access element”** *“broadcasts or multicasts discovery requests throughout the virtual subnet implemented by the VLAN in an attempt to identify central control elements”* during the *“discovery phase”* in Calhoun is substantially similar to (at least by being one example thereof) the “way” of *“any node discovery protocol* or by the *broadcast/multicast/anycast of a specific, mutually recognizable message”* in the ‘384 Patent, and that such “result” of **“discovery responses”** from the *“central control elements”* in Calhoun is substantially similar to the “result” of *“invoking responses from available CNs”* in the ‘384 Patent, or thus that the structure in Calhoun for performing the function of **“send[ing] a discovery request message to said one or more control nodes”** is at least equivalent to the proposed structure in the specification of the ‘384 Patent under the alternative claim construction of ¶ 308 above.

314. Therefore, in my opinion, Calhoun discloses the limitations of this claim element under the alternative claim construction of ¶ 308 above.

315. Additionally, I note that per my analysis herein that CAPWAP discloses at least *“automatic discovery”* using **“Discovery”** messages being exchanged between the **“Access Point”** and the **“Access Controller”** or **“Access Router”** within the **“AC(AR)’s domain”**, or

hence the function of “**send[ing] a discovery request message to said one or more control nodes**” as recited for this claim element, thereby further informing a POSITA that the structure in Calhoun for performing the function of “**send[ing] a discovery request message to said one or more control nodes**” when combined as noted herein to implement at least the “*negotiable interface protocol*” of CAPWAP would similarly include a “way” and a “result” that are each substantially similar to those of the proposed structure in the specification of the ‘384 Patent under the alternative claim construction of ¶ 308 above.

316. Therefore, in my opinion, Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA renders obvious the limitations of this claim element under the alternative claim construction of ¶ 308 above.

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

317. Calhoun discloses that “*central control elements 24, 26 receive the discovery requests (202) and transmit discovery responses* to access element **15 (204)**” wherein “Each discovery response comprises a *central control element identifier and a load parameter*” (see, for example, ¶ 125 above).

318. More specifically, Calhoun discloses that “The *load parameter indicates* the performance *load associated with the central control element*” such as “the *number of access elements under the management and control* of a given central control element” (see, for example, ¶ 126 above).

319. Accordingly, a POSITA would understand that this “*load parameter*”, which is “**information**”, that “*indicates the performance load associated with the central control element*” such as “*the number of access elements under the management and control*”

discloses “**information of functions offered by the associated control node**” at least because Calhoun describes such “*management and control*” by a “*central control element*” of an “*access element*” as including “*link layer management functions, such as authentication and association*” (see, for example, ¶¶ 275-276 above), or hence, “**functions offered by the associated control node**”. Similarly, a POSITA would understand from the disclosures of Calhoun, either explicitly or inherently, that such “*load*” information about “*the number of access elements*” under the management of the central control element is “**information**” of the “*link layer management functions*” the central control element is currently performing and thus also “**information of**” the capacity of the central control element to perform additional “*link layer management functions, such as authentication and association*” (see, for example, ¶¶ 275-276 above), or hence, “**functions offered by the associated control node**”.

320. In reference to FIG. 3A, Calhoun discloses that “*access element 15 waits a threshold period of time (104, 105) for discovery responses from one or more central control elements and selects one of the responding central control elements identified in the discovery responses (106)*” wherein “The *selection of a given central control element* can be *driven by a number of different considerations*” such as “the *responding central control element* that *reports the smallest load* (e.g., the *smallest number of access elements under management*)” (see, for example, ¶ 127 above, and annotated FIG. 3A shown at ¶ 294 above).

321. Thus, Calhoun discloses a “**selecting unit**” (for example, the annotated portion of composite FIG. 3A and FIG. 3B of Calhoun shown at ¶ 294 above) that is “**configured to select one control node of said one or more control nodes based on one or more discovery response messages sent to said wireless point from said one or more control nodes in response to said discovery request message**” (for example, when an “*access element*” “*selects*

one of the responding central control elements identified in the discovery responses” wherein the “*selection of a given central control element*” is based upon “*the smallest load (e.g., the smallest number of access elements under management)*” as reported in the “*discovery responses*”), and wherein “**each of said one or more discovery response messages including information of functions offered by the associated control node of said one or more control nodes**” (for example, when “*Each discovery response comprises a central control element identifier and a load parameter*” and this “*load parameter indicates the performance load associated with the central control element*” such as “*the number of access elements under the management and control*”).

322. Therefore, in my opinion, Calhoun discloses the limitations of this claim element.

323. See ¶ 297 above regarding LWAPP, which applies also to this claim element.

324. LWAPP further discloses that “From the Discovery Replies received, an Access Point (AP) will select an AR with which to associate” (see, for example, ¶ 150 above).

325. For example, LWAPP explains that “Upon receiving a discovery request, the AR will respond with a Discovery Reply sent to the address in the source address of the received discovery request” wherein “The Discovery Reply carries the following message elements: AR Payload” and “AR Name Payload” (see, for example, ¶ 167 above).

326. More specifically, LWAPP describes the format of this “AR payload message element” as being “used by the AR to communicate it's current state” and as including the “Hardware Version” and “Software Version”, the “number of mobile stations currently associated with the AR” and the “maximum number of stations supported by the AR”, and the “number of APs currently attached to the AR” and the “maximum number of APs supported by the AR” (see, for example, ¶ 168 above).

327. Accordingly, a POSITA would understand that at least the “***number of mobile stations currently associated with the AR***” and/or the “***number of APs currently attached to the AR***”, which are “**information**”, as disclosing “**information of functions offered by the associated control node**” at least because LWAPP describes such the “***bridging, forwarding, authentication, encryption and policy enforcement functions for a WLAN***” as being performed at the “**AR**” (see, for example, ¶ 282 above) and because such “**load**” information is information about the volume of the “***bridging, forwarding, authentication, encryption and policy enforcement functions***” that the “**AR**” is currently performing with respect to the WLAN, or hence, “**functions offered by the associated control node**”, which is analogous to the disclosure of this process provided in Calhoun (see, for example, ¶¶ 317-320 above).

328. Additionally, LWAPP explains that “When an AP receives a Discovery Reply, it ***MUST wait*** for an interval not less than DiscoveryInterval for ***receipt of additional discovery replies***” such that “After the DiscoveryInterval elapses, 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***” (see, for example, ¶ 169 above).

329. Thus, LWAPP discloses an “**Access Point**” that is “**configured to select one control node of said one or more control nodes based on one or more discovery response messages sent to said wireless point from said one or more control nodes in response to said discovery request message**” (for example, when “***From the Discovery Replies received, an Access Point (AP) will select an AR with which to associate***”), and wherein “**each of said one or more discovery response messages including information of functions offered by the associated control node of said one or more control nodes**” (for example, when the “**Discovery Reply**” carries the “**AR payload message element**” which includes at least the

“number of mobile stations currently associated with the AR” and/or the “number of APs currently attached to the AR”).

330. See ¶ 303 above regarding CAPWAP, which applies also to this claim element.

331. See at least ¶¶ 248-270 above regarding the combination of Calhoun, LWAPP and CAPWAP.

332. At least because Calhoun discloses the limitations of this claim element, and because LWAPP also discloses at least certain limitations of this claim element, then Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA also renders obvious the limitations of this claim element.

333. As an alternative claim construction, I have been asked by Counsel for the Petitioner to also analyze this claim while assuming that this claim element may be construed as a matter of law as a means for performing a recited function as set out in 35 U.S.C. § 112, ¶ 6, wherein the recited function would be **“select[ing] one control node of said one or more control nodes based on one or more discovery response messages sent to said wireless point from said one or more control nodes in response to said discovery request message”** and the proposed structure in the specification of the ‘384 Patent for performing such function as a **“selecting unit”** that the **“wireless point compris[es]”** would be described by the “operational step” denoted as **“203”** in FIG. 2 as well as the applicable text in 9:1-11 of the ‘384 Patent (see, for example, ¶¶ 58 and 60 above).

334. Under the alternative claim construction of ¶ 333 above, I note that Calhoun discloses identically the recited function of **“select[ing] one control node of said one or more control nodes based on one or more discovery response messages sent to said wireless point**

from said one or more control nodes in response to said discovery request message” as I have described herein (see, for example, ¶¶ 317-322 above).

335. Calhoun also discloses structure for a **“selecting unit”** that the **“wireless point compris[es]”** by at least the **“flow chart diagrams”** FIG. 3A and FIG. 3B of Calhoun as I have annotated herein (see, for example, ¶ 294 above).

336. Under the alternative claim construction of ¶ 333 above, I believe a POSITA would understand the “way” that the proposed structure in the specification of the ‘384 Patent would be deemed to perform the function of **“select[ing] one control node of said one or more control nodes based on one or more discovery response messages sent to said wireless point from said one or more control nodes in response to said discovery request message”** is to **“choose which among the discovered CNs to associate with”** based on **“metrics”** such as **“congestion”**, and/or **“manufacturer identification”**, thereby leading to the “result” of a **“CN selection”** (see, for example, ¶ 60 above).

337. Similarly, the “way” that the structure for a **“selecting unit”** that the **“wireless point compris[es]”** in Calhoun performs the function of **“select[ing] one control node of said one or more control nodes based on one or more discovery response messages sent to said wireless point from said one or more control nodes in response to said discovery request message”** is when it **“selects one of the responding central control elements identified in the discovery responses”** during the **“discovery phase”** based upon **“considerations”** such as **“a central control element identifier and a load parameter”**, thereby leading to the “result” of a **“selection”** of **“one of the responding central control elements identified in the discovery responses”** (see, for example, ¶¶ 317-320 above).

338. In my opinion, a POSITA would understand that the “way” that an “*access element*” “*selects one of the responding central control elements identified in the discovery responses*” based upon “*considerations*” such as “*a central control element identifier and a load parameter*” during the “*discovery phase*” in Calhoun is substantially similar to (at least by being one example thereof) the “way” to “*choose which among the discovered CNs to associate with*” based on “*metrics*” such as “*congestion*”, and/or “*manufacturer identification*” in the ‘384 Patent, and that such “result” of a “*selection*” of “*one of the responding central control elements identified in the discovery responses*” in Calhoun is substantially similar to the “result” of a “*CN selection*” in the ‘384 Patent, or thus that the structure in Calhoun for performing the function of “**select[ing] one control node of said one or more control nodes based on one or more discovery response messages sent to said wireless point from said one or more control nodes in response to said discovery request message**” is at least equivalent to the proposed structure in the specification of the ‘384 Patent under the alternative claim construction of ¶ 333 above.

339. Therefore, in my opinion, Calhoun discloses the limitations of this claim element under the alternative claim construction of ¶ 333 above.

340. Additionally, I note that per my analysis herein that CAPWAP discloses at least “*automatic discovery*” using “*Discovery*” messages being exchanged between the “*Access Point*” and the “*Access Controller*” or “*Access Router*” within the “*AC(AR)’s domain*”, or hence the function of “**select[ing] one control node of said one or more control nodes based on one or more discovery response messages sent to said wireless point from said one or more control nodes in response to said discovery request message**” as recited for this claim element, thereby further informing a POSITA that the structure in Calhoun for performing the

function of “select[ing] one control node of said one or more control nodes based on one or more discovery response messages sent to said wireless point from said one or more control nodes in response to said discovery request message” when combined as noted herein to implement at least the “*negotiable interface protocol*” of CAPWAP would similarly include a “way” and a “result” that are each substantially similar to those of the proposed structure in the specification of the ‘384 Patent under the alternative claim construction of ¶ 333 above.

341. Therefore, in my opinion, Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA renders obvious the limitations of this claim element under the alternative claim construction of ¶ 333 above.

1(c) a session establishing unit configured to establish a secure session with said selected one control node;

342. See ¶ 292 above regarding Calhoun, which applies also to this claim element.

343. Calhoun further discloses that “*After selection* of a central control element, *access element 15 transmits a join request* to the *selected central control element*” wherein such “join request” includes “an *access element identifier*, a *digital certificate* and a *session identifier*” and/or “*other fields*, such as the *WLAN MAC address*, *software image version*, etc.” and more specifically, such “*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), and the *digital signature of the certificate-issuing authority*” (see, for example, ¶¶ 128-129 above).

344. For example, Calhoun explains for this “*joinder phase*” that “*Central control element 24* (in this example) *receives the join request (206)* and *authenticates the digital certificate* in the join request (208)” and “*composes a join response*” that includes at least the

“cryptographic keys” and the “digital certificate of the central control element” (see, for example, ¶¶ 131-132 above).

345. Calhoun next explains that “When access element 15 receives the join response, it validates the join response (114) and, assuming the join response is valid, decrypts and installs the symmetric cryptographic keys (115)” using the procedure described in reference to FIG. 3B (see, for example, ¶ 134 above).

346. Calhoun further explains that “Access element 15 validates the digital certificate associated with central control element 24 (152)” such that “If the digital certificate is valid, access element 15 then verifies the signature of the signed key/sessionID payload using the public key of the central control element 24 (154) and validates the session identifier (156)” and “then decrypts the cipher including the cryptographic keys using its private key (115)” so that accordingly, “Transmission of data (e.g., configuration data, control messages, management messages, etc.) between the access element 15 and central control element 24 can now be encrypted and authenticated using the shared secret cryptographic keys” (see, for example, ¶ 135 above).

347. Accordingly, a POSITA would understand that this “**digital certificate**” validation and “**cryptographic keys**” exchange between the “**access element**” and the “**selected central control element**” during the “**joinder phase**” of Calhoun which follows the “**discovery phase**” as described above discloses at least that the “**access element**” of Calhoun is configured to “**establish a secure session with said selected one control node**” as recited for this claim element as disclosed by the procedures shown in and described for FIG. 3A and FIG. 3B of Calhoun (see, for example, ¶¶ 123, 130 and 134 above) using the elements of the “**flow chart diagrams**” of FIG. 3A and FIG. 3B as I have annotated herein as a “**session establishing unit**”

(see, for example, ¶ 294 above), thereby enabling that subsequent “*Transmission of data (e.g., configuration data, control messages, management messages, etc.)*” between the “*access element*” and the “*central control element*” will be “*encrypted and authenticated using the shared secret cryptographic keys*”.

348. Thus, Calhoun discloses a “**session establishing unit**” (for example, the annotated portion of composite FIG. 3A and FIG. 3B of Calhoun shown at ¶ 294 above) that is “**configured to establish a secure session with said selected one control node**” (for example, when an “*access element*” performs the “*digital certificate*” validation and “*cryptographic keys*” exchange with the “*selected central control element*” during the “*joinder phase*” such that subsequent “*Transmission of data (e.g., configuration data, control messages, management messages, etc.)*” between the “*access element*” and the “*central control element*” will be “*encrypted and authenticated using the shared secret cryptographic keys*”).

349. Therefore, in my opinion, Calhoun discloses the limitations of this claim element.

350. See ¶ 297 above regarding LWAPP, which applies also to this claim element.

351. LWAPP further discloses that “From the Discovery Replies received, an Access Point (AP) will select an AR with which to associate, using the Join Request and Join Reply” as part of a “Join phase” (see, for example, ¶¶ 150 and 185 above).

352. For example, LWAPP explains that “The Join Request” includes a “certificate message element value” as “a byte string containing a PKCS #5 certificate” such that “When an AR receives a Join Request” that then “The AR validates the certificate found in the request” such that “If valid, the AR generates a session key which will be used to secure the control frames it exchanges with the AP” and then “When the AR issues the Join Reply, the AR creates a

context for the session with the AP” so that “LWAPP uses public key cryptography to ensure trust between the AP and the AR” (see, for example, ¶¶ 171-173 and 185 above).

353. Accordingly, a POSITA would understand that this “**PKCS #5 certificate**” validation and “**public key cryptography**” exchange “**between the AP and the AR**” within the “**Join phase**” of LWAPP which follows the “**discovery phase**” as described above discloses at least that the “**Access Point**” of LWAPP is configured to “**establish a secure session with said selected one control node**” as recited for this claim element as disclosed by procedures described for the “**state diagram**” that “**represents the lifecycle of an AP-AR session**” in Figure 3 of LWAPP as I have annotated herein as a “**session establishing unit**” (see, for example, ¶ 300 above), which is analogous to the disclosure of this process provided in Calhoun (see, for example, ¶¶ 342-347 above).

354. Thus, LWAPP discloses a “**session establishing unit**” (for example, the annotated portion of Figure 3 of LWAPP shown at ¶ 300 above) that is “**configured to establish a secure session with said selected one control node**” (for example, when an “**Access Point**” performs the “**PKCS #5 certificate**” validation and “**public key cryptography**” exchange with the “**AR**” during the “**Join phase**”).

355. Therefore, in my opinion, LWAPP discloses the limitations of this claim element.

356. CAPWAP describes that “When a AP comes alive on a network it may authenticate and register with one or more ARs it detects on the network it is connected to” wherein “for secure communications enabling automatic discovery, configuration and adaptive resource management” then “the AP's need to be set up securely in the AC(AR)'s domain” such that “Identity 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” as part of the

“Capability Negotiation Phase” that “resolves the mutual capabilities of AP and AC” and “lets them decide to AP register with one or more AC” (see, for example, ¶¶ 214 and 219 above).

357. Accordingly, a POSITA would understand that this “*authenticate*” by “*cryptographically secure binding*” to be “*set up securely in the AC(AR)’s domain*” within the “*Capability Negotiation Phase*” of CAPWAP as described above discloses at least that the “*Access Point*” of CAPWAP is configured to “**establish a secure session with said selected one control node**” as recited for this claim element, which is analogous to the disclosure of this process provided in Calhoun (see, for example, ¶¶ 342-347 above).

358. Thus, CAPWAP discloses an “*Access Point*” that is “**configured to establish a secure session with said selected one control node**” (for example, as shown during the “*Capability Negotiation Phase*” as described specifically above at least to “*authenticate*” by “*cryptographically secure binding*” and become “*set up securely in the AC(AR)’s domain*”).

359. See at least ¶¶ 248-270 above regarding the combination of Calhoun, LWAPP and CAPWAP.

360. At least because each of Calhoun and LWAPP discloses the limitations of this claim element, and because CAPWAP also discloses at least certain limitations of this claim element, then Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA also renders obvious the limitations of this claim element.

361. As an alternative claim construction, I have been asked by Counsel for the Petitioner to also analyze this claim while assuming that this claim element may be construed as a matter of law as a means for performing a recited function as set out in 35 U.S.C. § 112, ¶ 6, wherein the recited function would be “**establish[ing] a secure session with said selected one control node**” and the proposed structure in the specification of the ‘384 Patent for performing

such function as a “**session establishing unit**” that the “**wireless point compris[es]**” would be described at 9:11-16 of the ‘384 Patent (see, for example, ¶ 61 above).

362. Under the alternative claim construction of ¶ 361 above, I note that Calhoun discloses identically the recited function of “**establish[ing] a secure session with said selected one control node**” as I have described herein (see, for example, ¶¶ 342-347 above).

363. Calhoun also discloses structure for a “**session establishing unit**” that the “**wireless point compris[es]**” by at least the “*flow chart diagrams*” FIG. 3A and FIG. 3B of Calhoun as I have annotated herein (see, for example, ¶ 294 above).

364. Under the alternative claim construction of ¶ 361 above, I believe a POSITA would understand the “way” that the proposed structure in the specification of the ‘384 Patent would be deemed to perform the function of “**establish[ing] a secure session with said selected one control node**” is via “*mutual authentication*” and “*exchanges of security information*”, thereby leading to the “result” of an “*establishment of communication protocols* for further exchanges” (see, for example, ¶ 61 above).

365. Similarly, the “way” that the structure for a “**session establishing unit**” that the “**wireless point compris[es]**” in Calhoun performs the function of “**establish[ing] a secure session with said selected one control node**” is by the “*digital certificate*” validation and “*cryptographic keys*” exchange with the “*selected central control element*” during the “*joinder phase*”, thereby leading to the “result” subsequent “*Transmission of data (e.g., configuration data, control messages, management messages, etc.)*” between the “*access element*” and the “*central control element*” will be “*encrypted and authenticated using the shared secret cryptographic keys*” (see, for example, ¶¶ 342-347 above).

366. In my opinion, a POSITA would understand that the “way” that an “*access element*” performs the “*digital certificate*” validation and “*cryptographic keys*” exchange with the “*selected central control element*” during the “*joinder phase*” in Calhoun is substantially similar to (at least by being one example thereof) the “way” of “*mutual authentication*” and “*exchanges of security information*” in the ‘384 Patent, and that such “result” of subsequent “*Transmission of data (e.g., configuration data, control messages, management messages, etc.)*” between the “*access element*” and the “*central control element*” will be “*encrypted and authenticated using the shared secret cryptographic keys*” in Calhoun is substantially similar to (at least by being one example thereof) the “result” of “*establishment of communication protocols* for further exchanges” in the ‘384 Patent, or thus that the structure in Calhoun for performing the function of “**establish[ing] a secure session with said selected one control node**” is at least equivalent to the proposed structure in the specification of the ‘384 Patent under the alternative claim construction of ¶ 361 above.

367. Therefore, in my opinion, Calhoun discloses the limitations of this claim element under the alternative claim construction of ¶ 361 above.

368. Additionally, I note that per my analysis herein that CAPWAP discloses at least a “*Capability Negotiation Phase*” wherein an “*Access Point*” would “*authenticate*” by “*cryptographically secure binding*” and thus “*set up securely in the AC(AR)'s domain*”, or hence the function of “**establish[ing] a secure session with said selected one control node**” as recited for this claim element, thereby further informing a POSITA that the structure in Calhoun for performing the function of “**establish[ing] a secure session with said selected one control node**” when combined as noted herein to implement at least the “*negotiable interface protocol*” of CAPWAP would similarly include a “way” and a “result” that are each substantially similar to

those of the proposed structure in the specification of the ‘384 Patent under the alternative claim construction of ¶ 361 above.

369. Therefore, in my opinion, Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA renders obvious the limitations of this claim element under the alternative claim construction of ¶ 361 above.

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

370. See ¶¶ 275-278 above regarding Calhoun, which applies also to this claim element particularly regarding **“the functions to be separated between said selected one control node and said wireless point”**.

371. More specifically, Calhoun describes that ***“real-time communication functions”*** are performed at the ***“access element”*** while ***“link layer management functions, such as authentication and association”*** are performed at the ***“selected central control element”*** as part of a ***“division of functionality between the access elements and the central control elements”***.

372. Accordingly, a POSITA would understand that ***“real-time communication functions”*** at the ***“access element”*** and ***“link layer management functions, such as authentication and association”*** at the ***“selected central control element”*** as part of a ***“division of functionality between the access elements and the central control elements”*** is one example of **“the functions to be separated between said selected one control node and said wireless point”** as recited for this claim element.

373. See ¶ 292 above regarding Calhoun, which applies also to this claim element.

374. Calhoun explains that ***“access element 15 begins the configuration phase”*** by ***“comparing the image version identifier in the join response to the image version installed on access element 15 (116)”*** such that ***“If the image version in the join response is later*** than the

image version associated with access element **15**, access element requests the new image version from central control element **24 (120)**” and then subsequently “Access element **15** receives the new image version, installs it and reboots (122), thereby restarting the initialization process described herein” (see, for example, ¶ 137 above).

375. Additionally, Calhoun explains that after updating to the “**current image version**” as described above that this “**configuration phase**” continues when “Access element 15” next “composes and transmits a configuration request to central control element **24 (124)**” wherein this “**configuration request**” includes “one or more operational parameters (such as channel, transmit power, internal v. external antenna, etc.)” that a “network administrator” can “directly configure” via “a command line interface, browser interface, etc.” on the “access element” or “through an interface presented by a central control element” wherein such “network administrator” can also “flag” at least “certain overriding parameters which a central control element can not change, except with a new “overriding” parameter value” (see, for example, ¶¶ 138-139 above).

376. Calhoun next explains that “central control element 24 receives the configuration request (214), and generates the operational parameters for access element 15 (216), taking into account the overriding parameters identified in the configuration request” and “then transmits a configuration response including the operational parameters (218)” so that “Access element 15 receives the configuration response (126), optionally stores the operational parameters in non-volatile memory, implements the operational parameters (128), and switches to an access point mode” using “the configuration information provided by the central control element” (see, for example, ¶¶ 140-141 above).

377. Calhoun also explains that “wireless traffic associated with remote client elements 16, 18; 20, 22” “can be tunneled between the central control element 24 and the access elements 12, 14” but also discloses that “access elements 12, 14 can operate to directly bridge network traffic between remote client elements 16, 18; 20, 22 and WAN 50, while tunneling network management messages, such as authentication and association requests from remote client elements to central control element 24” and further discloses that “the division of functionality between the access elements and the central control elements can be shifted” wherein “For example, the access elements can bridge network traffic associated with the remote client elements directly, while transmitting management packets to the central control element” (see, for example, ¶¶ 118 and 143 above).

378. Accordingly, a POSITA would understand that “**operational parameters**”, such as “**channel**,” “**transmit power**,” and “**internal vs. external antenna**”, which, for example, would represent respectively the frequency channel, the radiated power and the chosen antenna at which the access element transmits to and receives from remote client elements, are “**information**” regarding the “**real-time communication functions**” of the WLAN that are performed by the access element, and are thus “**information about the functions**” at the access element of Calhoun (see, for example, ¶ 375 above).

379. Similarly, a POSITA would understand that by their generation at the central control element of Calhoun, such “**operational parameters**” including “**channel**,” “**transmit power**,” and “**internal vs. external antenna**” for such access elements are also “**information**” about the WLAN management functions performed by such central control element of Calhoun (see, for example, ¶ 376 above).

380. Accordingly, a POSITA would understand that either or both of this “*image version*” update aspect and this “*operational parameters*”/“*configuration information*” exchange aspect of the “*configuration phase*” of Calhoun as described above also discloses at least that the “*access element*” of Calhoun is configured to “**exchange information about the functions to be separated**” with the “*selected central control element*” of Calhoun as recited for this claim element because for each such aspect one of the “*access element*” or the “*selected central control element*” “*transmits*” while the other “*receives*” (or thus “**exchange[s]**”) such “*identifier*”, “*parameters*” and/or “*information*” (or thus “**information**”), thereby informing the other “*element*” something “**about the functions**” at either the “*access element*” or the “*selected central control element*” (or thus “**about the functions to be separated between said selected one control node and said wireless point**” as I also explained at ¶¶ 370-372 above).

381. Additionally, a POSITA would understand that this “*shift[ing]*” of “*division of functionality*” aspect of Calhoun wherein the “*access element*” may be configured to “*bridge network traffic associated with remote clients directly, while transmitting management packets to the central control element*” such that this configuration may be “*shifted*” from “*wireless traffic associated with remote client elements*” to being “*tunneled between the central control element*” and the “*access elements*” discloses at least that the “*access element*” of Calhoun is configured to “**exchange information about the functions to be separated**” with the “*selected central control element*” of Calhoun as recited for this claim element because for such “*division of functionality*” to be “*shifted*” requires that for each such “*shift*” one of the “*access element*” or the “*selected central control element*” “*transmits*” while the other “*receives*” such information about “*shift[ing]*” the “*division of functionality*” (or thus “**about the functions to**

be separated between said selected one control node and said wireless point” as I also noted at ¶ 377 above).

382. Note also that the claims of Calhoun recite the above described process disclosed in Calhoun as being to “*exchange configuration information*” between “*access elements*” and “*central control elements*” (see, for example, ¶ 145 above).

383. Thus, Calhoun discloses a “**negotiation unit**” (for example, the annotated portion of composite FIG. 3A and FIG. 3B of Calhoun shown at ¶ 294 above) that is “**configured to exchange information about the functions to be separated between said selected one control node and said wireless point**” (for example, when the “*access element*” or the “*selected central control element*” “*transmits*” while the other “*receives*” the “*identifier*”, “*parameters*” and/or “*information*” that relate to either “*real-time communication functions*” at the “*access element*” or “*link layer management functions, such as authentication and association*” at the “*selected central control element*” or “*shifting*” the “*division of functionality*” during either or both of the “*image version*” update aspect and the “*operational parameters*”/“*configuration information*” exchange aspect of the “*configuration phase*” of Calhoun).

384. Therefore, in my opinion, Calhoun discloses the limitations of this claim element.

385. Additionally, to the extent that Patent Owner may allege that Calhoun’s disclosure of “*shifting*” the “*division of functionality*” does not literally disclose, either explicitly or inherently, the limitations of this claim element, then, in my opinion, Calhoun renders obvious the limitations of this claim element to a POSITA that an “*access element*” and a “*central control element*” “**exchange information about the functions to be separated**” in order to effectuate such a “*shift*” in the “*division of functionality*” when the shift is from access elements that “*bridge network traffic associated with remote clients directly*” to “*wireless traffic*”

associated with remote client elements” being *“tunneled between the central control element”* and *“access elements”* or vice versa.

386. See ¶¶ 281-283 above regarding LWAPP, which applies also to this claim element particularly regarding **“the functions to be separated between said selected one control node and said wireless point”**.

387. More specifically, LWAPP describes that the *“APs can be considered as remote RF interfaces”* while the *“bridging, forwarding, authentication, encryption and policy enforcement functions for a WLAN”* are performed at the *“Access router, or AR”*.

388. Accordingly, a POSITA would understand that *“remote RF interface”* functions at the *“AP”* and the *“bridging, forwarding, authentication, encryption and policy enforcement functions”* at the *“Access router, or AR”* is one example of **“the functions to be separated between said selected one control node and said wireless point”** as recited for this claim element.

389. LWAPP explains that *“Once the AP and the AR have joined, a configuration exchange is accomplished that will ... provision the APs”* wherein such “provisioning of APs includes the *typical name (802.11 Service Set Identifier, SSID)*, and *security parameters*, the *data rates* to be advertised as well as the *radio channel (channels)*, if the AP is capable of operating *more than one 802.11 MAC and PHY simultaneously*) to be used” (see, for example, ¶ 152 above).

390. LWAPP further explains that *“Configure Requests are sent by an AP after receiving a Join Reply”* in order to “send its *current configuration to its AR*” such that *“When an AR receives a Configure Request it will act upon the content of the packet and respond to the AP”*

with a Configure Response” which “provides an *opportunity for the AR to override an AP's configuration*” (see, for example, ¶¶ 175-176 above).

391. More specifically, LWAPP discloses that this “*Configure Request* carries the following *message elements*: Administrative State (for the AP)”, “AR Name”, “Administrative State (for each radio)”, “AP WLAN Radio Configuration (for each radio)”, “Multi-domain Capability (for each radio)”, “MAC Operation (for each radio)”, “PHY TX Power (for each radio)”, “PHY TX Power Level (for each Radio)”, “PHY DSSS Payload or PHY OFDM Payload (for each radio)”, “Antenna (for each radio)” and “Supported Rates (for each radio)” while this “*Configure Response* carries the following *message elements*: Result Code”, “AP WLAN Radio Configuration (for each radio)”, “Operational Rate Set (for each radio)”, “Multi-domain Capability (for each radio)”, “MAC Operation (for each radio)”, “PHY Tx Power (for each Radio)”, “PHY DSSS or PHY OFDM Payload (for each radio)” and “Antenna (for each radio)” (see, for example, ¶¶ 175-176 above).

392. Accordingly, a POSITA would understand that this “*configuration exchange*” for “*provisioning*” during the “*configuration phase*” of LWAPP as described above also discloses at least that the “*Access Point*” of LWAPP is configured to “**exchange information about the functions to be separated**” with the “*Access Router*” of LWAPP as recited for this claim element because this “*exchange*” involves “*message elements*” (or thus “**information**”) about “*remote RF interface*” functions at the “*AP*” (or thus “**about the functions to be separated between said selected one control node and said wireless point**” as I also explained at ¶¶ 386-388 above), which is analogous to the disclosure of this process provided in Calhoun (see, for example, ¶¶ 370-382 above).

393. Thus, LWAPP discloses a “**negotiation unit**” (for example, the annotated portion of Figure 3 of LWAPP shown at ¶ 300 above) that is “**configured to exchange information about the functions to be separated between said selected one control node and said wireless point**” (for example, during a “*configuration exchange*” between an “*Access Point*” and an “*Access Router*” that involves “*message elements*” about “*remote RF interface*” functions).

394. Therefore, in my opinion, LWAPP discloses the limitations of this claim element.

395. See ¶¶ 286-288 above regarding CAPWAP, which applies also to this claim element particularly regarding “**the functions to be separated between said selected one control node and said wireless point**”.

396. More specifically, CAPWAP describes that the “*functions as allowed in the Standards and practiced in the industry*” are “*meaningfully split between lightweight Access Point (LAP)*” and “*AP Controllers or AR (Access Router)*” with “*real-time components*” in the “*Access Point*” and “*access control components*” in the “*Access Router*”.

397. Accordingly, a POSITA would understand that having “*real-time*” “*functions*” at the “*Access Point*” and the “*access control*” “*functions*” at the “*AP Controller*” is one example of “**the functions to be separated between said selected one control node and said wireless point**” as recited for this claim element.

398. CAPWAP explains that “based on negotiated architecture” then “Configuration of an AP includes providing the parameters necessary for the AP to advertise and provide service for one or more WLANs” wherein “Physical parameters are related to the operation of the AP's radio interface” and “Logical parameters are related to the individual WLANs that are provisioned on the AP” (see, for example, ¶¶ 215-218 above).

399. More specifically, CAPWAP describes that these “Physical parameters” include “the channel on which the AP is to operate, the maximum power at which the AP is to transmit, antenna selections, the supported data rates, and the timing for the periodic announcements of the WLANs provisioned on the AP” while these “Logical parameters” include “the SSID of the WLANs, the allowed authentication methods, the allowed privacy methods, values for the contention-free period and DTIM, VLAN associations, IP addresses and netmasks, authentication server addresses, any pre-shared keys for WLANs or authentication servers, regulatory (country) information, and other 802.11-specific capabilities to be advertised for the WLANs” (see, for example, ¶¶ 216-217 above).

400. Accordingly, a POSITA would understand that this “**configuration**” by “**providing the parameters**” based on the “**negotiated architecture**” of CAPWAP as described above also discloses at least that the “**Access Point**” of CAPWAP is configured to “**exchange information about the functions to be separated**” with the “**AP Controller**” of CAPWAP as recited for this claim element because this “**providing the parameters**” (or thus “**exchange**” of “**information**”) is at least about “**real-time components**” in the “**Access Point**” (or thus “**about the functions to be separated between said selected one control node and said wireless point**” as I also explained at ¶¶ 395-397 above), which is analogous to the disclosure of this process provided in Calhoun (see, for example, ¶¶ 370-382 above).

401. Thus, CAPWAP discloses an “**Access Point**” that is “**configured to exchange information about the functions to be separated between said selected one control node and said wireless point**” (for example, when “**providing the parameters**” to the “**Access Point**” from the “**AP Controller**” about “**real-time components**” among the “**functions**” within the “**Access Point**”).

402. See at least ¶¶ 248-270 above regarding the combination of Calhoun, LWAPP and CAPWAP.

403. At least because each of Calhoun and LWAPP discloses the limitations of this claim element, and because CAPWAP also discloses at least certain limitations of this claim element, then Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA also renders obvious the limitations of this claim element.

404. As an alternative claim construction, I have been asked by Counsel for the Petitioner to also analyze this claim while assuming that this claim element may be construed as a matter of law as a means for performing a recited function as set out in 35 U.S.C. § 112, ¶ 6, wherein the recited function would be **“exchange[ing] information about the functions to be separated between said selected one control node and said wireless point”** and the proposed structure in the specification of the ‘384 Patent for performing such function as a **“negotiation unit”** that the **“wireless point compris[es]”** would be described by the “operational steps” denoted as **“205, 207, 209, 211, 213, 215, 219 and 221”** in FIG. 2 as well as the applicable text in 9:17-11:3 of the ‘384 Patent (see, for example, ¶¶ 58 and 62-68 above).

405. Under the alternative claim construction of ¶ 404 above, I note that Calhoun discloses identically the recited function of **“exchange[ing] information about the functions to be separated between said selected one control node and said wireless point”** as I have described herein (see, for example, ¶¶ 370-382 above).

406. Calhoun also discloses structure for a **“negotiation unit”** that the **“wireless point compris[es]”** by at least the **“flow chart diagrams”** FIG. 3A and FIG. 3B of Calhoun as I have annotated herein (see, for example, ¶ 294 above).

407. Under the alternative claim construction of ¶ 404 above, I believe a POSITA would understand the “way” that the proposed structure in the specification of the ‘384 Patent would be deemed to perform the function of **“exchange[ing] information about the functions to be separated between said selected one control node and said wireless point”** is by having *“WAP controllers initiate by sending information regarding the functional capabilities of the associated WAPs to the chosen CN”* such as *“the appropriate codes corresponding to the functional components that the WAPs are capable of processing”* so that *“Upon receiving capabilities information from the associated WAPs and based on established policies, CN controller 103 determines an initial division of WLAN functionality”* which is *“based on a policy that allows each associated WAP to process all the functional components that they are capable of”* such that *“only those functional components that an associated WAP cannot inherently process are left to the CN”* and next *“the division is then sent to the associated WAPs for confirmation”* such that *“The WAP controllers in turn verify that the division is feasible”*, thereby leading 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”* (see, for example, ¶¶ 62-67 above).

408. Similarly, one exemplary “way” that the structure for a **“negotiation unit”** that the **“wireless point compris[es]”** in Calhoun performs the function of **“exchange[ing] information about the functions to be separated between said selected one control node and said wireless point”** is by a **“configuration phase”** wherein the **“access element”** **“composes and transmits a configuration request to central control element”** wherein this **“configuration request”** includes **“operational parameters”** and **“overriding parameters”** that describe at least the **“real-time communication functions”** at the **“access element”** and then subsequently the

“central control element” “generates the operational parameters for access element” after “taking into account the overriding parameters identified in the configuration request” and “then transmits a configuration response including the operational parameters” to the “access element” which “implements the operational parameters” and “switches to an access point mode”, thereby leading to the “result” of a “division of functionality between the access elements and the central control elements” when “operating in 802.11 wireless networks” that uses updated “operational parameters” for such “real-time communication functions” at the “access element” (see, for example, ¶¶ 370-382 above).

409. In my opinion, a POSITA would understand that the “way” of such *“configuration request”* that includes *“operational parameters”* and *“overriding parameters”* to describe at least the *“real-time communication functions”* at the *“access element”* followed by such *“configuration response”* from the *“central control element”* that *“implements the operational parameters”* that set the *“real-time communication functions”* at the *“access element”* during the *“configuration phase”* in Calhoun is substantially similar to the “way” of *“sending information”* including *“codes corresponding to the functional components”* to and/or from a *“WAP controller”* and a *“chosen CN”* which *“determines ... WLAN functionality”* in the ‘384 Patent, and that such “result” of realizing a *“division of functionality between the access elements and the central control elements”* that uses updated *“operational parameters”* for such *“real-time communication functions”* at the *“access element”* in Calhoun is substantially similar 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”* in the ‘384 Patent, or thus that the structure in Calhoun for performing the function of **“exchange[ing] information about the functions to be separated between said selected one**

control node and said wireless point” is at least equivalent to the proposed structure in the specification of the ‘384 Patent under the alternative claim construction of ¶ 404 above.

410. Therefore, in my opinion, Calhoun discloses the limitations of this claim element under the alternative claim construction of ¶ 404 above.

411. Additionally, I note that per my analysis herein that CAPWAP discloses at least *“providing the parameters”* to the *“Access Point”* from the *“AP Controller”* about *“real-time components”* among the *“functions”* within the *“Access Point”*, or hence the function of **“exchange[ing] information about the functions to be separated between said selected one control node and said wireless point”** as recited for this claim element, thereby further informing a POSITA that the structure in Calhoun for performing the function of **“exchange[ing] information about the functions to be separated between said selected one control node and said wireless point”** when combined as noted herein to implement at least the *“negotiable interface protocol”* of CAPWAP would similarly include a “way” and a “result” that are each substantially similar to those of the proposed structure in the specification of the ‘384 Patent under the alternative claim construction of ¶ 404 above.

412. Therefore, in my opinion, Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA renders obvious the limitations of this claim element under the alternative claim construction of ¶ 404 above.

‘384 Patent: Claim 2

2. The wireless point according to claim 1, wherein said information exchange is performed by transmitting, to the selected one control node, information about functions that said wireless point has, and receiving, from said selected one control node, information about functions that said selected one control node has.

2. The wireless point according to claim 1,

413. Per my analysis for Claim 1 as summarized above, Calhoun discloses the **“wireless point according to claim 1”**.

414. Therefore, in my opinion, Calhoun discloses this preamble claim element.

415. Per my analysis for Claim 1 as summarized above, Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA renders obvious the “**wireless point according to claim 1**”.

416. Therefore, in my opinion, Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA renders obvious this preamble claim element.

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

417. I note that “**said information exchange**” has an antecedent basis from at least claim element 1(d) which recites a limitation “**to exchange information about the functions to be separated between said selected one control node and said wireless point**”.

418. See ¶¶ 370-384 above regarding Calhoun, which applies also to this claim element.

419. Accordingly, my analysis for claim element 1(d) shows that a POSITA would understand that Calhoun discloses “**said information exchange**” as being performed when the “*access element*” (or “**wireless point according to claim 1**”) “*transmits*” to the “*selected central control element*” that “*receives*” (or “**transmitting, to the selected one control node**”) at least “*operational parameters*” such as “*channel, transmit power, internal v. external antenna*” for the “*real-time communication functions*” that the “*access element*” is currently performing (or “**information about functions that said wireless point has**”).

420. Therefore, in my opinion, Calhoun discloses the limitations of this claim element.

421. See ¶¶ 386-394 above regarding LWAPP, which applies also to this claim element.

422. Accordingly, my analysis for claim element 1(d) shows that a POSITA would understand that LWAPP discloses “**said information exchange**” as being performed when the “**Access Point**” (or “**wireless point according to claim 1**”) has “**sent**” to the “**Access Router**” that “**receives**” (or “**transmitting, to the selected one control node**”) at least “**message elements**” such as the “**AP WLAN Radio Configuration**” or the “**MAC Operation**” for the “**remote RF interfaces**” (or “**information about functions that said wireless point has**”).

423. Therefore, in my opinion, LWAPP discloses the limitations of this claim element.

424. See at least ¶¶ 248-270 above regarding the combination of Calhoun, LWAPP and CAPWAP.

425. At least because Calhoun and LWAPP each disclose the limitations of this claim element, then Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA also renders obvious the limitations of this claim element.

2(b) wherein said information exchange is performed by ... receiving, from said selected one control node, information about functions that said selected one control node has.

426. See ¶¶ 370-384 above regarding Calhoun, which applies also to this claim element.

427. As I noted in my analysis above, Calhoun discloses that the “**functions that said selected one control node has**” include at least “**link layer management functions, such as authentication and association**” (see, for example, ¶ 276 above).

428. Additionally, as I noted in my analysis above, Calhoun discloses “**said information exchange**” as being performed when the “**access element**” (or “**wireless point according to claim 1**”) “**receives**” from the “**selected central control element**” that “**transmits**” (or “**receiving, from said selected one control node**”) at least a “**configuration response including the operational parameters**” (or “**information about functions**”).

429. I further note from my analysis of claim element 1(b) (see, for example, ¶¶ 317-322 above) that Calhoun also discloses that “*central control elements*” “*transmit discovery responses to access element*” that include a “*load parameter*” that “*indicates the performance load associated with the central control element*” such as “*the number of access elements under the management and control of a given central control element*” which is information about the functions the “*central control element*” is currently performing (or “**information about functions that said wireless point has**”).

430. See ¶¶ 386-394 above regarding LWAPP, which applies also to this claim element.

431. As I noted in my analysis above, LWAPP discloses that the “**functions that said selected one control node has**” include at least the “*bridging, forwarding, authentication, encryption and policy enforcement functions for a WLAN*” (see, for example, ¶ 282 above).

432. Additionally, as I noted in my analysis above, LWAPP discloses “**said information exchange**” as being performed when the “*Access Point*” (or “**wireless point according to claim 1**”) has a “*configuration exchange*” to “*provision the APs*” that includes wherein the “*Access Router*” will “*respond*” (or “**receiving, from said selected one control node**”) at least a “*Configure Response*” that “*includes the typical name (802.11 Service Set Identifier, SSID), and security parameters*” (or “**information about functions that said selected one control node has**”).

433. In my opinion, at least because LWAPP discloses that the “*Access Router*” performs at least the “*authentication, encryption and policy enforcement functions for a WLAN*”, which is analogous to the disclosure of Calhoun (see, for example, ¶ 427 above) and to the disclosure of CAPWAP (see, for example, ¶ 436 below), then a POSITA would understand

that such “**802.11 Service Set Identifier, SSID**” and “**security parameters**” being received at the “**Access Point**” from the “**Access Router**” in the “**Configure Response**” during the “**configuration exchange**” represents a disclosure of “**information about functions that said selected one control node has**” because such “**SSID**” and “**security parameters**” are fundamental information about such “**authentication, encryption and policy enforcement functions**” of the “**Access Router**”.

434. Therefore, in my opinion, LWAPP discloses the limitations of this claim element.

435. See ¶¶ 395-401 above regarding CAPWAP, which applies also to this claim element.

436. As I noted in my analysis above, CAPWAP discloses that the “**functions that said selected one control node has**” include at least those to support that the “**access control components of the 802.11 protocol terminate in the Access Router**” (see, for example, ¶ 287 above). I further note that CAPWAP describes such “**access control components of the 802.11 protocol**” as including at least the “**functions**” of “**Authentication**”, “**Deauthentication**”, “**Association**”, “**Disassociation**”, and “**Reassociation**” (see, for example, ¶ 211 above).

437. Accordingly, my analysis for claim element 1(d) shows that a POSITA would understand that CAPWAP discloses “**said information exchange**” as being performed when “**providing the parameters**” to the “**Access Point**” from the “**AP Controller**” (or “**wireless point according to claim 1**” is “**receiving, from said selected one control node**”) at least “**Logical parameters**” that include at least “**the SSID of the WLANs**”, “**the allowed authentication methods**”, “**the allowed privacy methods**” and “**any pre-shared keys for WLANs or authentication servers**” (or “**information about functions that said selected one control node has**”).

438. In my opinion, at least because CAPWAP discloses that the “*AP Controller*” performs at least the “*functions*” of “*Authentication*”, “*Deauthentication*”, “*Association*”, “*Disassociation*”, and “*Reassociation*”, which is analogous to the disclosure of Calhoun (see, for example, ¶ 427 above) and to the disclosure of LWAPP (see, for example, ¶ 431 above), then a POSITA would understand that such “*Logical parameters*” that include at least “*the SSID of the WLANs*”, “*the allowed authentication methods*”, “*the allowed privacy methods*” and “*any pre-shared keys for WLANs or authentication servers*” represents a disclosure of “**information about functions that said selected one control node has**” because such “*SSID*”, “*authentication methods*”, “*privacy methods*” and “*pre-shared keys*” are fundamental information about such “*functions*” of “*Authentication*”, “*Deauthentication*”, “*Association*”, “*Disassociation*”, and “*Reassociation*” for the “*AP Controller*”.

439. Therefore, in my opinion, CAPWAP discloses the limitations of this claim element.

440. See at least ¶¶ 248-270 above regarding the combination of Calhoun, LWAPP and CAPWAP.

441. At least because LWAPP and CAPWAP each disclose the limitations of this claim element, and because Calhoun discloses at least certain limitations of this claim element, then Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA also renders obvious the limitations of this claim element.

‘384 Patent: Claim 3

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

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

442. Per my analysis for Claim 1 as summarized above, Calhoun discloses the **“wireless point according to claim 1”**.

443. Therefore, in my opinion, Calhoun discloses this preamble claim element.

444. Per my analysis for Claim 1 as summarized above, Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA renders obvious the **“wireless point according to claim 1”**.

445. Therefore, in my opinion, Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA renders obvious this preamble claim element.

446. I note that **“said functions for the wireless local area network”** has an antecedent basis from at least the preamble of Claim 1 which recites **“functions for a wireless local area network to be separated between said wireless point and one or more control nodes”**.

447. See ¶¶ 273-279 above regarding Calhoun, which applies also to this claim element.

448. Accordingly, my analysis for the preamble of Claim 1 shows that a POSITA would understand that Calhoun discloses **“said functions for the wireless local area network”** as comprising at least **“link layer management functions, such as authentication and association”** for **“operating in 802.11 wireless networks”** (or thus at least **“Authentication”** and **“Encryption/Decryption”** per ¶¶ 233-235 above).

449. Thus, Calhoun discloses **“The wireless point according to claim 1”** (for example, the **“access element”** of Calhoun), wherein **“said functions for the wireless local area network”** (for example, the **“link layer management functions, such as authentication and association”** for **“operating in 802.11 wireless networks”** of Calhoun) comprise **“at least one of**

Beacon Signal Control, Power Management, Quality of Service (QoS), Scheduling, Authentication, and Encryption/Decryption” (for example, the “*802.11*” “*management functions*” of “*authentication and association*” in Calhoun).

450. Therefore, in my opinion, Calhoun discloses the limitations of this claim element.

451. See ¶¶ 280-284 above regarding LWAPP, which applies also to this claim element.

452. Accordingly, my analysis for the preamble of Claim 1 shows that a POSITA would understand that LWAPP discloses “**said functions for the wireless local area network**” as comprising at least “*authentication, encryption and policy enforcement functions for a WLAN*” operating “*in 802.11*” (or thus at least “**Authentication**” and “**Encryption/Decryption**” per ¶¶ 233-235 above).

453. Thus, LWAPP discloses “**The wireless point according to claim 1**” (for example, the “*Access Point*” of LWAPP), wherein “**said functions for the wireless local area network**” (for example, the “*authentication, encryption and policy enforcement functions for a WLAN*” operating “*in 802.11*” of LWAPP) comprise “**at least one of Beacon Signal Control, Power Management, Quality of Service (QoS), Scheduling, Authentication, and Encryption/Decryption**” (for example, the “*802.11*” “*functions*” of “*authentication, encryption*” in LWAPP).

454. Therefore, in my opinion, LWAPP discloses the limitations of this claim element.

455. See ¶¶ 285-289 above regarding CAPWAP, which applies also to this claim element.

456. I further note that CAPWAP describes that the “*access control components of the 802.11 protocol*” include at least the “*functions*” of “*Authentication*”, “*Deauthentication*”,

“Association”, *“Disassociation”*, and *“Reassociation”* (see, for example, ¶ 211 above) while the *“Access Point Functions”* that relate to *“real-time aspects”* for *“802.11”* include at least *“Privacy”*, *“Beaconing”*, and *“Power Management”* (see, for example, ¶ 210 above).

457. Accordingly, my analysis for the preamble of Claim 1 shows that a POSITA would understand that CAPWAP discloses **“said functions for the wireless local area network”** as comprising at least the *“functions”* of *“Authentication”*, *“Deauthentication”*, *“Association”*, *“Disassociation”*, *“Reassociation”*, *“Privacy”*, *“Beaconing”*, and *“Power Management”* according to *“the 802.11 protocol”* (or thus at least **“Beacon Signal Control”**, **“Power Management”**, **“Authentication”** and **“Encryption/Decryption”** per ¶¶ 228, 233-235, 238 and 240 above).

458. Thus, CAPWAP discloses **“The wireless point according to claim 1”** (for example, the *“Access Point”* of CAPWAP), wherein **“said functions for the wireless local area network”** (for example, the *“functions”* of *“Authentication”*, *“Deauthentication”*, *“Association”*, *“Disassociation”*, *“Reassociation”*, *“Privacy”*, *“Beaconing”*, and *“Power Management”* according to *“the 802.11 protocol”* of CAPWAP) comprise **“at least one of Beacon Signal Control, Power Management, Quality of Service (QoS), Scheduling, Authentication, and Encryption/Decryption”** (for example, the *“802.11” “functions”* of *“Authentication”*, *“Privacy”*, *“Beaconing”*, and *“Power Management”* in CAPWAP).

459. Therefore, in my opinion, CAPWAP discloses the limitations of this claim element.

460. See at least ¶¶ 248-270 above regarding the combination of Calhoun, LWAPP and CAPWAP.

461. Additionally, I note that the common knowledge of a POSITA at the alleged time of invention would also include for IEEE 802.11 compatible WLAN systems such as Calhoun, LWAPP and CAPWAP that yet another one of the **“functions for the wireless local area network”** would necessarily include **“Scheduling”** (see, for example, ¶ 240 above).

462. At least because each of Calhoun, LWAPP and CAPWAP discloses the limitations of this claim element, and the knowledge of a POSITA further discloses the limitations of this claim element, then Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA also renders obvious the limitations of this claim element.

‘384 Patent: Claim 4

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

- sending a discovery request message to said one or more control nodes;
- selecting a control node of said one or more control nodes based on one or more discovery response messages sent to said wireless point from said one or more control nodes in response to said discovery request message, each of said one or more discovery response messages including information of functions offered by the associated control node of said one or more control nodes;
- establishing a secure session with said selected one control node; and
- exchanging information about the functions to be separated between said selected one control node and said wireless point.

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

463. I have considered that this preamble claim element may be limiting.

464. In my opinion, a POSITA would understand that the limitations of **“A method ... that provides for functions for said wireless local area network to be separated between a wireless point and one or more control nodes”** for this claim element are substantially similar to limitations expressed in the preamble for Claim 1.

465. Accordingly, my analysis of Calhoun, LWAPP, and CAPWAP for the preamble for Claim 1 above already applies to this the preamble for Claim 4.

466. Additionally, my analysis of Calhoun for the preamble for Claim 1 above is also applicable for this preamble of Claim 4 for the limitation of “**A method for providing service in a wireless local area network**” (see, for example, ¶¶ 273-279 above).

467. Thus, Calhoun discloses “**A method for providing service in a wireless local area network**” (for example, the “*wireless Local Area Network (LAN)*” as also depicted in FIG. 1 of Calhoun) that comprises “**one or more control nodes**” (for example, the “*central control elements*” of Calhoun), and a “**wireless point**” (for example, the “*managed access points*” or “*access elements*” of Calhoun) wherein such “**method ... provides for functions for said wireless local area network to be separated between a wireless point and one or more control nodes**” (for example, when “*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*” in order to “*perform link layer management functions, such as authentication and association*” as part of a “*division of functionality between the access elements and the central control elements*”).

468. Therefore, in my opinion, Calhoun discloses the limitations of this claim element, if any.

469. My analysis of LWAPP for the preamble for Claim 1 above is also applicable for this preamble of Claim 4 for the limitation of “**A method for providing service in a wireless local area network**” (see, for example, ¶¶ 280-284 above).

470. Thus, LWAPP discloses “**A method for providing service in a wireless local area network**” (for example, the “*WLAN*” as also depicted in Figure 1 of LWAPP) that comprises “**one or more control nodes**” (for example, the “*Access router, or AR*” of LWAPP), and a “**wireless point**” (for example, the “*simple*” or “*Light Weight*” “*Access Points*” or “*APs*”

of LWAPP) wherein such **“method ... provides for functions for said wireless local area network to be separated between a wireless point and one or more control nodes”** (for example, when operating *“in 802.11”* the *“APs can be considered as remote RF interfaces”* while the *“bridging, forwarding, authentication, encryption and policy enforcement functions for a WLAN”* are performed at the *“Access router, or AR”* per the disclosures of LWAPP).

471. Therefore, in my opinion, LWAPP discloses the limitations of this claim element, if any.

472. My analysis of CAPWAP for the preamble for Claim 1 above is also applicable for this preamble of Claim 4 for the limitation of **“A method for providing service in a wireless local area network”** (see, for example, ¶¶ 285-289 above).

473. Thus, CAPWAP discloses **“A method for providing service in a wireless local area network”** (for example, the *“WLAN”* as also depicted in Figure 1 of CAPWAP) that comprises **“one or more control nodes”** (for example, the *“AR (Access Router), AC (Access Controller) and AB (Access Bridge)”* that *“are used synonymously”* in CAPWAP), and a **“wireless point”** (for example, the *“lightweight Access Point (LAP)”* of CAPWAP) wherein such **“method ... provides for functions for said wireless local area network to be separated between a wireless point and one or more control nodes”** (for example, when the *“functions as allowed in the Standards and practiced in the industry”* are *“meaningfully split between lightweight Access Point (LAP)”* and *“AP Controllers or AR (Access Router)”* with *“real-time components”* in the *“Access Point”* and *“access control components”* in the *“Access Router”* per the disclosures of CAPWAP).

474. Therefore, in my opinion, CAPWAP discloses the limitations of this claim element, if any.

475. See at least ¶¶ 248-270 above regarding the combination of Calhoun, LWAPP and CAPWAP.

476. At least because each of Calhoun, LWAPP and CAPWAP discloses the limitations of this claim element, if any, then Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA also renders obvious the limitations of this claim element, if any.

4(a) sending a discovery request message to said one or more control nodes;

477. In my opinion, a POSITA would understand that the limitations of “**sending a discovery request message to said one or more control nodes**” for this claim element are substantially similar to limitations expressed in claim element 1(a) above for Claim 1.

478. Accordingly, my analysis of Calhoun, LWAPP, and CAPWAP for claim element 1(a) above already applies to this claim element 4(a).

479. My analysis of Calhoun for claim element 1(a) above is also applicable for this claim element 4(a) (see, for example, ¶¶ 292-296 above).

480. Thus, Calhoun discloses “**sending a discovery request message to said one or more control nodes**” (for example, when an “*access element*” “*broadcasts or multicasts discovery requests throughout the virtual subnet implemented by the VLAN in an attempt to identify central control elements*”).

481. Therefore, in my opinion, Calhoun discloses the limitations of this claim element.

482. My analysis of LWAPP for claim element 1(a) above is also applicable for this claim element 4(a) (see, for example, ¶¶ 297-302 above).

483. Thus, LWAPP discloses “**sending a discovery request message to said one or more control nodes**” (for example, when an “*Access Point*” “*send[s] a Discovery Request frame*” as a “*Discovery Request message to be transmitted to a broadcast address*” to “*automatically discovery potential ARs available in the network*”).

484. Therefore, in my opinion, LWAPP discloses the limitations of this claim element.

485. My analysis of CAPWAP for claim element 1(a) above is also applicable for this claim element 4(a) (see, for example, ¶¶ 303-305 above).

486. Thus, CAPWAP discloses “**sending a discovery request message to said one or more control nodes**” (for example, when an “*Access Point*” uses “*Discovery*” messages being exchanged with the “*Access Controller*” or “*Access Router*” within the “*AC(AR)’s domain*”).

487. Therefore, in my opinion, CAPWAP discloses the limitations of this claim element.

488. See at least ¶¶ 248-270 above regarding the combination of Calhoun, LWAPP and CAPWAP.

489. At least because each of Calhoun, LWAPP and CAPWAP discloses the limitations of this claim element, then Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA also renders obvious the limitations of this claim element.

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

490. In my opinion, a POSITA would understand that the limitations of “**selecting a control node of said one or more control nodes based on one or more discovery response messages sent to said wireless point from said one or more control nodes in response to said discovery request message, each of said one or more discovery response messages including information of functions offered by the associated control node of said one or more control nodes**” for this claim element are substantially similar to limitations expressed in claim element 1(b) above for Claim 1.

491. Accordingly, my analysis of Calhoun, LWAPP, and CAPWAP for claim element 1(b) above already applies to this claim element 4(b).

492. My analysis of Calhoun for claim element 1(b) above is also applicable for this claim element 4(b) (see, for example, ¶¶ 317-322 above).

493. Thus, Calhoun discloses “**selecting a control node of said one or more control nodes based on one or more discovery response messages sent to said wireless point from said one or more control nodes in response to said discovery request message**” (for example, when an “*access element*” “*selects one of the responding central control elements identified in the discovery responses*” wherein the “*selection of a given central control element*” is based upon “*the smallest load (e.g., the smallest number of access elements under management)*” as reported in the “*discovery responses*”), and wherein “**each of said one or more discovery response messages including information of functions offered by the associated control node of said one or more control nodes**” (for example, when “*Each discovery response comprises a central control element identifier and a load parameter*” and this “*load parameter indicates the performance load associated with the central control element*” such as “*the number of access elements under the management and control*”).

494. Therefore, in my opinion, Calhoun discloses the limitations of this claim element.

495. My analysis of LWAPP for claim element 1(b) above is also applicable for this claim element 4(b) (see, for example, ¶¶ 323-329 above).

496. Thus, LWAPP discloses “**selecting a control node of said one or more control nodes based on one or more discovery response messages sent to said wireless point from said one or more control nodes in response to said discovery request message**” (for example, when “*From the Discovery Replies received, an Access Point (AP) will select an AR with*

which to associate”), and wherein “each of said one or more discovery response messages including information of functions offered by the associated control node of said one or more control nodes” (for example, when the “*Discovery Reply*” carries the “*AR payload message element*” which includes at least the “*number of mobile stations currently associated with the AR*” and/or the “*number of APs currently attached to the AR*”).

497. Therefore, in my opinion, LWAPP discloses the limitations of this claim element.

498. See ¶ 303 above regarding CAPWAP, which applies also to this claim element.

499. See at least ¶¶ 248-270 above regarding the combination of Calhoun, LWAPP and CAPWAP.

500. At least because each of Calhoun and LWAPP discloses the limitations of this claim element, then Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA also renders obvious the limitations of this claim element.

4(c) establishing a secure session with said selected one control node;

501. In my opinion, a POSITA would understand that the limitations of “**establishing a secure session with said selected one control node**” for this claim element are substantially similar to limitations expressed in claim element 1(c) above for Claim 1.

502. Accordingly, my analysis of Calhoun, LWAPP, and CAPWAP for claim element 1(c) above already applies to this claim element 4(c).

503. My analysis of Calhoun for claim element 1(c) above is also applicable for this claim element 4(c) (see, for example, ¶¶ 342-349 above).

504. Thus, Calhoun discloses “**establishing a secure session with said selected one control node**” (for example, when an “*access element*” performs the “*digital certificate*” validation and “*cryptographic keys*” exchange with the “*selected central control element*” during the “*joinder phase*” such that subsequent “*Transmission of data (e.g., configuration*

data, control messages, management messages, etc.)” between the “*access element*” and the “*central control element*” will be “*encrypted and authenticated using the shared secret cryptographic keys*”).

505. Therefore, in my opinion, Calhoun discloses the limitations of this claim element.

506. My analysis of LWAPP for claim element 1(c) above is also applicable for this claim element 4(c) (see, for example, ¶¶ 350-355 above).

507. Thus, LWAPP discloses “**establishing a secure session with said selected one control node**” (for example, when an “*Access Point*” performs the “*PKCS #5 certificate*” validation and “*public key cryptography*” exchange with the “*AR*” during the “*Join phase*”).

508. Therefore, in my opinion, LWAPP discloses the limitations of this claim element.

509. My analysis of CAPWAP for claim element 1(c) above is also applicable for this claim element 4(c) (see, for example, ¶¶ 356-358 above).

510. Thus, CAPWAP discloses “**establishing a secure session with said selected one control node**” (for example, as shown during the “*Capability Negotiation Phase*” as described specifically above at least to “*authenticate*” by “*cryptographically secure binding*” and become “*set up securely in the AC(AR)’s domain*”).

511. Therefore, in my opinion, CAPWAP discloses the limitations of this claim element.

512. See at least ¶¶ 248-270 above regarding the combination of Calhoun, LWAPP and CAPWAP.

513. At least because each of Calhoun, LWAPP and CAPWAP discloses the limitations of this claim element, then Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA also renders obvious the limitations of this claim element.

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

514. In my opinion, a POSITA would understand that the limitations of “**exchanging information about the functions to be separated between said selected one control node and said wireless point**” for this claim element are substantially similar to limitations expressed in claim element 1(d) above for Claim 1.

515. Accordingly, my analysis of Calhoun, LWAPP, and CAPWAP for claim element 1(d) above already applies to this claim element 4(d).

516. My analysis of Calhoun for claim element 1(d) above is also applicable for this claim element 4(d) (see, for example, ¶¶ 370-384 above).

517. Thus, Calhoun discloses “**exchanging information about the functions to be separated between said selected one control node and said wireless point**” (for example, when the “*access element*” or the “*selected central control element*” “*transmits*” while the other “*receives*” the “*identifier*”, “*parameters*” and/or “*information*” that relate to either “*real-time communication functions*” at the “*access element*” or “*link layer management functions, such as authentication and association*” at the “*selected central control element*” during either or both of the “*image version*” update aspect and the “*operational parameters*”/“*configuration information*” exchange aspect of the “*configuration phase*” of Calhoun).

518. Therefore, in my opinion, Calhoun discloses the limitations of this claim element.

519. My analysis of LWAPP for claim element 1(d) above is also applicable for this claim element 4(d) (see, for example, ¶¶ 386-394 above).

520. Thus, LWAPP discloses “**exchanging information about the functions to be separated between said selected one control node and said wireless point**” (for example,

during a “*configuration exchange*” between an “*Access Point*” and an “*Access Router*” that involves “*message elements*” about “*remote RF interface*” functions).

521. Therefore, in my opinion, LWAPP discloses the limitations of this claim element.

522. My analysis of CAPWAP for claim element 1(d) above is also applicable for this claim element 4(d) (see, for example, ¶¶ 395-401 above).

523. Thus, CAPWAP discloses “**exchanging information about the functions to be separated between said selected one control node and said wireless point**” (for example, when “*providing the parameters*” to the “*Access Point*” from the “*AP Controller*” about “*real-time components*” among the “*functions*” within the “*Access Point*”).

524. Therefore, in my opinion, CAPWAP discloses the limitations of this claim element.

525. See at least ¶¶ 248-270 above regarding the combination of Calhoun, LWAPP and CAPWAP.

526. At least because each of Calhoun, LWAPP and CAPWAP discloses the limitations of this claim element, then Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA also renders obvious the limitations of this claim element.

‘384 Patent: Claim 5

5. The method according to claim 4, wherein said information exchange is performed by transmitting, to the selected one control node, information about functions that said wireless point has, and receiving, from said selected one control node, information about functions that said selected one control node has.

5. The method according to claim 4,

527. Per my analysis for Claim 4 as summarized above, Calhoun discloses the “**method according to claim 4**”.

528. Therefore, in my opinion, Calhoun discloses this preamble claim element.

529. Per my analysis for Claim 4 as summarized above, Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA renders obvious the “**method according to claim 4**”.

530. Therefore, in my opinion, Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA renders obvious this preamble claim element.

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

531. In my opinion, a POSITA would understand that the limitations of “**wherein said information exchange is performed by transmitting, to the selected one control node, information about functions that said wireless point has**” for this claim element are substantially similar to limitations expressed in claim element 2(a) above for Claim 2.

532. Accordingly, my analysis of Calhoun, LWAPP, and CAPWAP for claim element 2(a) above already applies to this claim element 5(a).

533. My analysis of Calhoun for claim element 2(a) above is also applicable for this claim element 5(a) (see, for example, ¶¶ 418-420 above).

534. Accordingly, my analysis for claim element 2(a) shows that a POSITA would understand that Calhoun discloses “**said information exchange**” as being performed when the “*access element*” (or “**wireless point**”) “*transmits*” to the “*selected central control element*” that “*receives*” (or “**transmitting, to the selected one control node**”) at least “*operational parameters*” such as “*channel, transmit power, internal v. external antenna*” for the “*real-time communication functions*” (or “**information about functions that said wireless point has**”).

535. Therefore, in my opinion, Calhoun discloses the limitations of this claim element.

536. My analysis of LWAPP for claim element 2(a) above is also applicable for this claim element 5(a) (see, for example, ¶¶ 421-423 above).

537. Accordingly, my analysis for claim element 2(a) shows that a POSITA would understand that LWAPP discloses “**said information exchange**” as being performed when the “*Access Point*” (or “**wireless point**”) has “*sent*” to the “*Access Router*” that “*receives*” (or “**transmitting, to the selected one control node**”) at least “*message elements*” such as the “*AP WLAN Radio Configuration*” or the “*MAC Operation*” for the “*remote RF interfaces*” (or “**information about functions that said wireless point has**”).

538. Therefore, in my opinion, LWAPP discloses the limitations of this claim element.

539. See at least ¶¶ 248-270 above regarding the combination of Calhoun, LWAPP and CAPWAP.

540. At least because Calhoun and LWAPP each disclose the limitations of this claim element, then Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA also renders obvious the limitations of this claim element.

5(b) wherein said information exchange is performed by ... receiving, from said selected one control node, information about functions that said selected one control node has.

541. In my opinion, a POSITA would understand that the limitations of “**wherein said information exchange is performed by ... receiving, from said selected one control node, information about functions that said selected one control node has**” for this claim element are substantially similar to limitations expressed in claim element 2(b) above for Claim 2.

542. Accordingly, my analysis of Calhoun, LWAPP, and CAPWAP for claim element 2(b) above already applies to this claim element 5(b).

543. My analysis of Calhoun for claim element 2(b) above is also applicable for this claim element 5(b) (see, for example, ¶¶ 426-429 above).

544. My analysis of LWAPP for claim element 2(b) above is also applicable for this claim element 5(b) (see, for example, ¶¶ 430-434 above).

545. Accordingly, my analysis for claim element 2(b) shows that a POSITA would understand that LWAPP discloses “**said information exchange**” as being performed when the “*Access Point*” (or “**wireless point**”) has a “*configuration exchange*” to “*provision the APs*” that includes wherein the “*Access Router*” will “*respond*” (or “**receiving, from said selected one control node**”) at least a “*Configure Response*” that “*includes the typical name (802.11 Service Set Identifier, SSID), and security parameters*” (or “**information about functions that said selected one control node has**”).

546. Therefore, in my opinion, LWAPP discloses the limitations of this claim element.

547. My analysis of CAPWAP for claim element 2(b) above is also applicable for this claim element 5(b) (see, for example, ¶¶ 435-439 above).

548. Accordingly, my analysis for claim element 2(b) shows that a POSITA would understand that CAPWAP discloses “**said information exchange**” as being performed when “*providing the parameters*” to the “*Access Point*” from the “*AP Controller*” (or “**wireless point**” is “**receiving, from said selected one control node**”) at least “*Logical parameters*” that include at least “*the SSID of the WLANs*”, “*the allowed authentication methods*”, “*the allowed privacy methods*” and “*any pre-shared keys for WLANs or authentication servers*” (or “**information about functions that said selected one control node has**”).

549. Therefore, in my opinion, CAPWAP discloses the limitations of this claim element.

550. See at least ¶¶ 248-270 above regarding the combination of Calhoun, LWAPP and CAPWAP.

551. At least because LWAPP and CAPWAP each disclose the limitations of this claim element, and because Calhoun discloses at least certain limitations of this claim element,

then Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA also renders obvious the limitations of this claim element.

‘384 Patent: Claim 6

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

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

552. Per my analysis for Claim 4 as summarized above, Calhoun discloses the **“method according to claim 4”**.

553. Therefore, in my opinion, Calhoun discloses this preamble claim element.

554. Per my analysis for Claim 4 as summarized above, Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA renders obvious the **“method according to claim 4”**.

555. Therefore, in my opinion, Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA renders obvious this preamble claim element.

556. I note that **“said functions for the wireless local area network”** has an antecedent basis from at least the preamble of Claim 4 which recites **“functions for a wireless local area network to be separated between said wireless point and one or more control nodes”**.

557. In my opinion, a POSITA would understand that the limitations of **“wherein said functions for the wireless local area network comprise at least one of Beacon Signal Control, Power Management, Quality of Service (QoS), Scheduling, Authentication, and Encryption/Decryption”** for this claim element are substantially similar to limitations expressed for Claim 3.

558. Accordingly, my analysis of Calhoun, LWAPP, and CAPWAP for Claim 3 above already applies to this Claim 6.

559. My analysis of Calhoun for Claim 3 above is also applicable for this Claim 6 (see, for example, ¶¶ 447-450 above).

560. Thus, Calhoun discloses wherein “**said functions for the wireless local area network**” (for example, the “*link layer management functions, such as authentication and association*” for “*operating in 802.11 wireless networks*” of Calhoun) comprise “**at least one of Beacon Signal Control, Power Management, Quality of Service (QoS), Scheduling, Authentication, and Encryption/Decryption**” (for example, the “*802.11*” “*management functions*” of “*authentication and association*” in Calhoun).

561. Therefore, in my opinion, Calhoun discloses the limitations of this claim element.

562. My analysis of LWAPP for Claim 3 above is also applicable for this Claim 6 (see, for example, ¶¶ 451-454 above).

563. Thus, LWAPP discloses wherein “**said functions for the wireless local area network**” (for example, the “*authentication, encryption and policy enforcement functions for a WLAN*” operating “*in 802.11*” of LWAPP) comprise “**at least one of Beacon Signal Control, Power Management, Quality of Service (QoS), Scheduling, Authentication, and Encryption/Decryption**” (for example, the “*802.11*” “*functions*” of “*authentication, encryption*” in LWAPP).

564. Therefore, in my opinion, LWAPP discloses the limitations of this claim element.

565. My analysis of CAPWAP for Claim 3 above is also applicable for this Claim 6 (see, for example, ¶¶ 455-459 above).

566. Thus, CAPWAP discloses wherein “**said functions for the wireless local area network**” (for example, the “*functions*” of “*Authentication*”, “*Deauthentication*”, “*Association*”, “*Disassociation*”, “*Reassociation*”, “*Privacy*”, “*Beaconing*”, and “*Power Management*” according to “*the 802.11 protocol*” of CAPWAP) comprise “**at least one of Beacon Signal Control, Power Management, Quality of Service (QoS), Scheduling, Authentication, and Encryption/Decryption**” (for example, the “*802.11*” “*functions*” of “*Authentication*”, “*Privacy*”, “*Beaconing*”, and “*Power Management*” in CAPWAP).

567. Therefore, in my opinion, CAPWAP discloses the limitations of this claim element.

568. See at least ¶¶ 248-270 above regarding the combination of Calhoun, LWAPP and CAPWAP.

569. See also ¶ 461 above.

570. At least because each of Calhoun, LWAPP and CAPWAP discloses the limitations of this claim element, and the knowledge of a POSITA further discloses the limitations of this claim element, then Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA also renders obvious the limitations of this claim element.

IX. CONCLUSION

571. In my opinion, the claims of the '384 Patent are invalid for at least the reasons stated above.

572. I reserve the right to supplement my opinions in the future to respond to any arguments raised by Patent Owner or its experts and to take into account new information that becomes available to me.

573. I declare under penalty of perjury that all statements made herein are of my own knowledge and are true and correct and were made with the knowledge that willful false statements are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "K. J. Negus", written over a horizontal line.

Kevin J. Negus

Date: July 31, 2023