EXPERT DECLARATION OF DR. KEVIN NEGUS
FOR
INTER PARTES REVIEW OF U.S. PATENT NO. 8,045,531

TABLE OF CONTENTS

I. INTRODUCTION

1. I, Dr. Kevin Negus, submit this declaration in support of a Petition for *Inter Partes* Review of United States Patent Nos. 8,045,531 (the "'531 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. 8,045,531 by H. Cheng et al., entitled "System and method for negotiation of WLAN entity" (the "'531 Patent") (Ex. 1001).
- File History for U.S. Patent No. 8,045,531 (Ex. 1002).
- 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 '531 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 '531 Patent first filed an application related to the '531 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 '531 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 predicable 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 '531 PATENT

45. The '531 Patent, entitled "System and method for negotiation of WLAN entity" 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 1:6-8).

A. Overview of the '531 Patent

46. In the "**Background Art**" section, the '531 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 1:20-25).

47. For example, the '531 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 1:29-36).

48. The '531 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 1:38-41).

49. The '531 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 1:64-2:4).

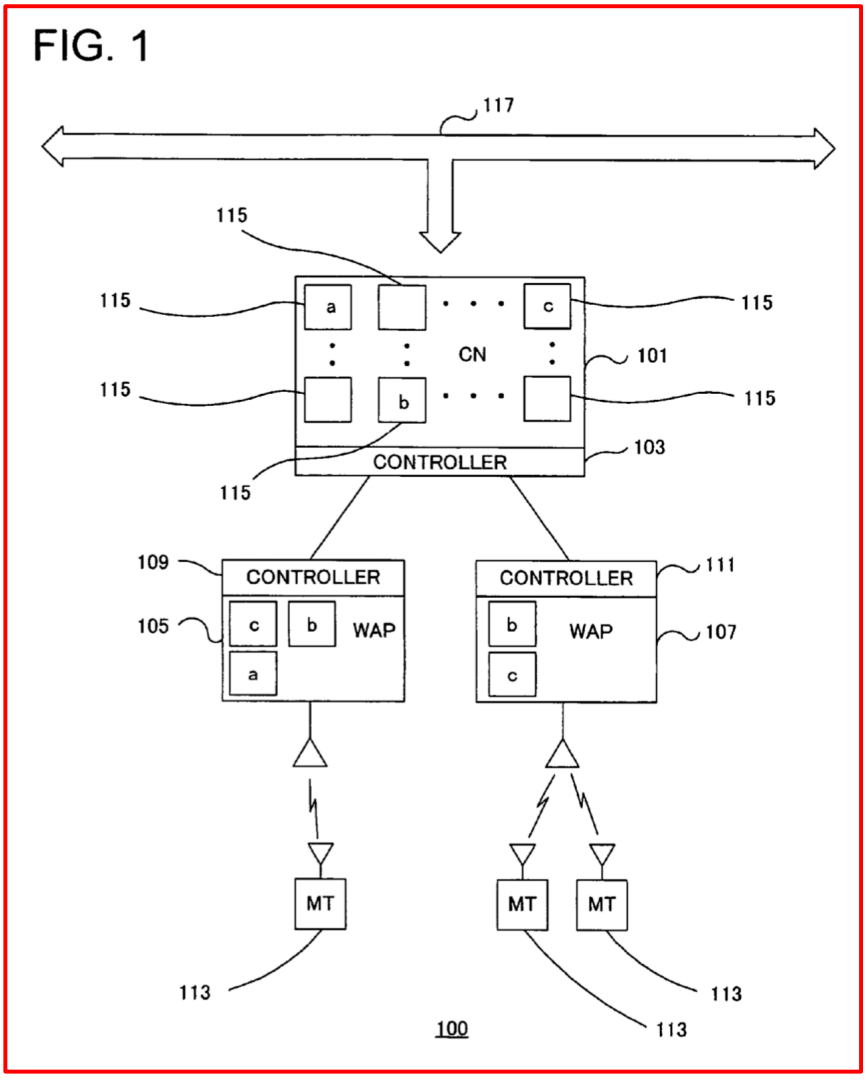
50. More specifically, the '531 Patent contends that "during the functioning of a WLAN, the *processing load at a WAP can become substantially high* even exceeding the processing capacity of the WAP" which "could be *due to increases in the number of associated mobile terminals (MTs)* or due to increases in the *volume of traffic* from the associated MTs" (emphasis added, see, for example, Ex. 1001 at 2:5-10).

51. In the "**Disclosure of the Invention**" section, the '531 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 3:14-20).

52. More specifically, the '531 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 3:21-26).

53. In the "**Best Mode for Carrying Out the Invention**" section, the '531 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 6:39-56, FIG. 1 as reproduced below).



54. In reference to FIG. 1 shown above, the '531 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 7:9-16).

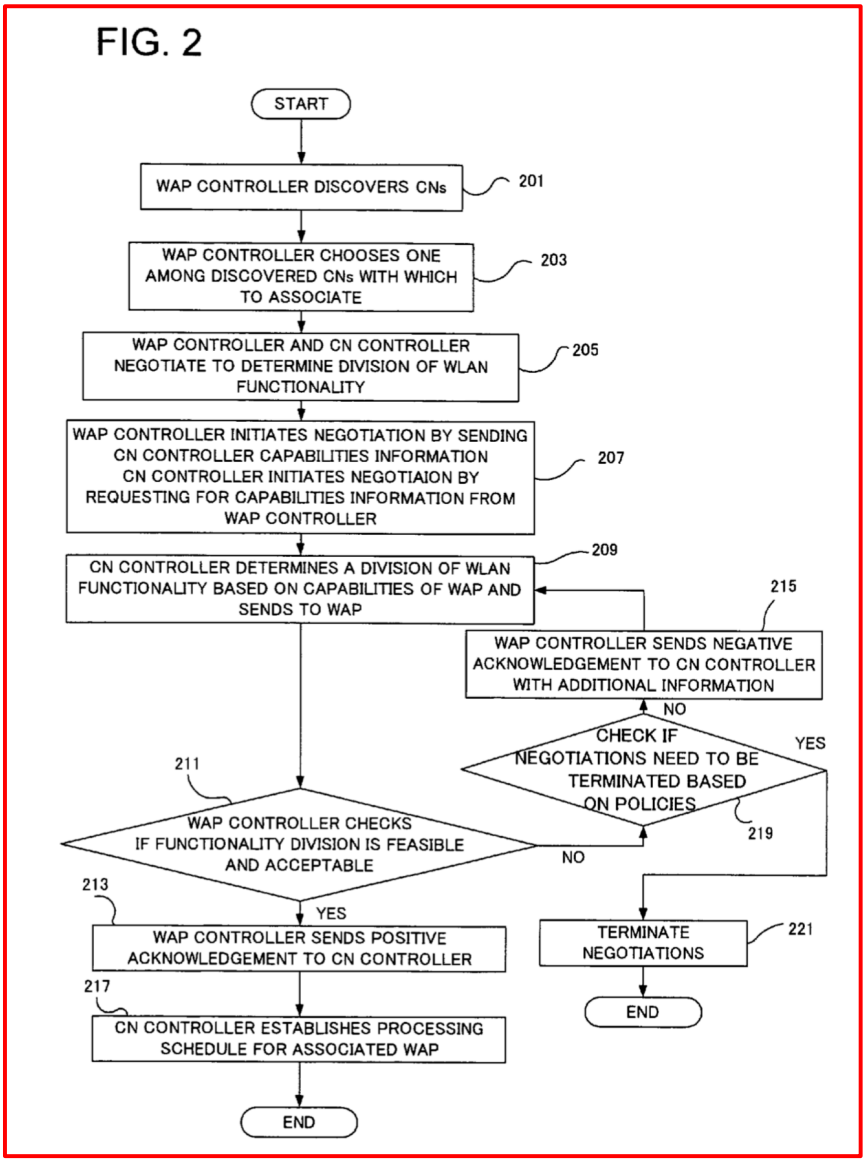
55. For example, the '531 Patent explains that "some of the *functional components* in FIG. 1 are represented by functional *component codes* 'a', 'b' and 'c'" such that "functional component 'a' may denote the *processing required for a certain type of encryption*, for example Wi-Fi Protected Access (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 7:18-26).

56. Additionally, the '531 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 7:38-50).

57. In further reference to FIG. 1 shown above, the '531 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 8:13-18).

58. According to the '531 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 5:49-51, FIG. 2 as reproduced below).



59. In reference to FIG. 2 shown above, the '531 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 8:44-51).

60. The '531 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 8:52-62).

61. Next, the '531 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 8:62-67).

62. In further reference to FIG. 2 shown above, the '531 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 9:1-10).

63. More specifically, the '531 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 9:10-17).

64. In further reference to FIG. 2 shown above, the '531 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 9:18-22).

65. For example, the '531 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 9:27-31).

66. Alternatively, the '531 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 9:41-50).

67. In further reference to FIG. 2 shown above, the '531 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 10:20-25).

68. However, the '531 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 10:26-37).

69. Finally, in reference to FIG. 2 shown above, the '531 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 10:54-61).

70. The '531 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 10:62-11:14).

71. Accordingly, in this embodiment, the '531 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 11:18-23).

72. Alternatively, the '531 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 11:24-31).

73. For example, the '531 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 11:42-50).

74. The '531 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 13:1-4, 14:63-67).

B. Prosecution File History of the '531 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. 1001 at [86]).

76. I understand the following to be original claim 1 of U.S. Patent Application No. 10/591,184 (from Ex. 1002 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. 1002 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. 1002 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. 1002 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. 1002 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. 1002 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. 1002 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. 1002 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. 1002 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. 1002 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. 1002 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. 1002 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. 1002 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. 1002 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. 1002 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. 1001 at [45]).

C. Asserted Claims and Priority Date

90. The '531 Patent includes 16 claims. I understand that Claims 1, 7 and 13 of the '531 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. Accordingly, I may refer to Claims 1, 7 and 13 of the '531 Patent as the "challenged claims" herein.

91. The '531 Patent was filed on Mar. 1, 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 '531 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 '531 Patent.

D. Objective Indicia of Non-obviousness

92. 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 '531 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

93. 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.

94. 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.

95. 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 '531 Patent. However, Patent Owner has provided an allegation of infringement for at least Claims 1, 7 and 13 of the '531 Patent. Thus, Patent Owner appears to believe that the claim terms of the challenged claims of

the '531 Patent are at least as broad as would be necessary for such allegation of infringement to apply.

96. 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.

97. 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 '531 Patent may constitute sufficient disclosure of structure linked to performing the recited functions for such claim elements.

98. However, I am informed by counsel for the Petitioner that claim elements of the challenged claims of the '531 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 "**negotiation unit**" of Claim 1 as well as the "**discovering unit**" and the "**secure connection negotiating unit**" of Claim 7.

99. 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.

100. 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

101. As of Mar. 2, 2004, which the Patent Owner alleges to be the priority date of the '531 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 '531 Patent, as evidenced in even the small sample of the art described herein.

A. Calhoun (Ex. 1005)

102. 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 '531 Patent at least under 35 U.S.C. § 102(e).

103. 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).

104. 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).

105. 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).

106. 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).

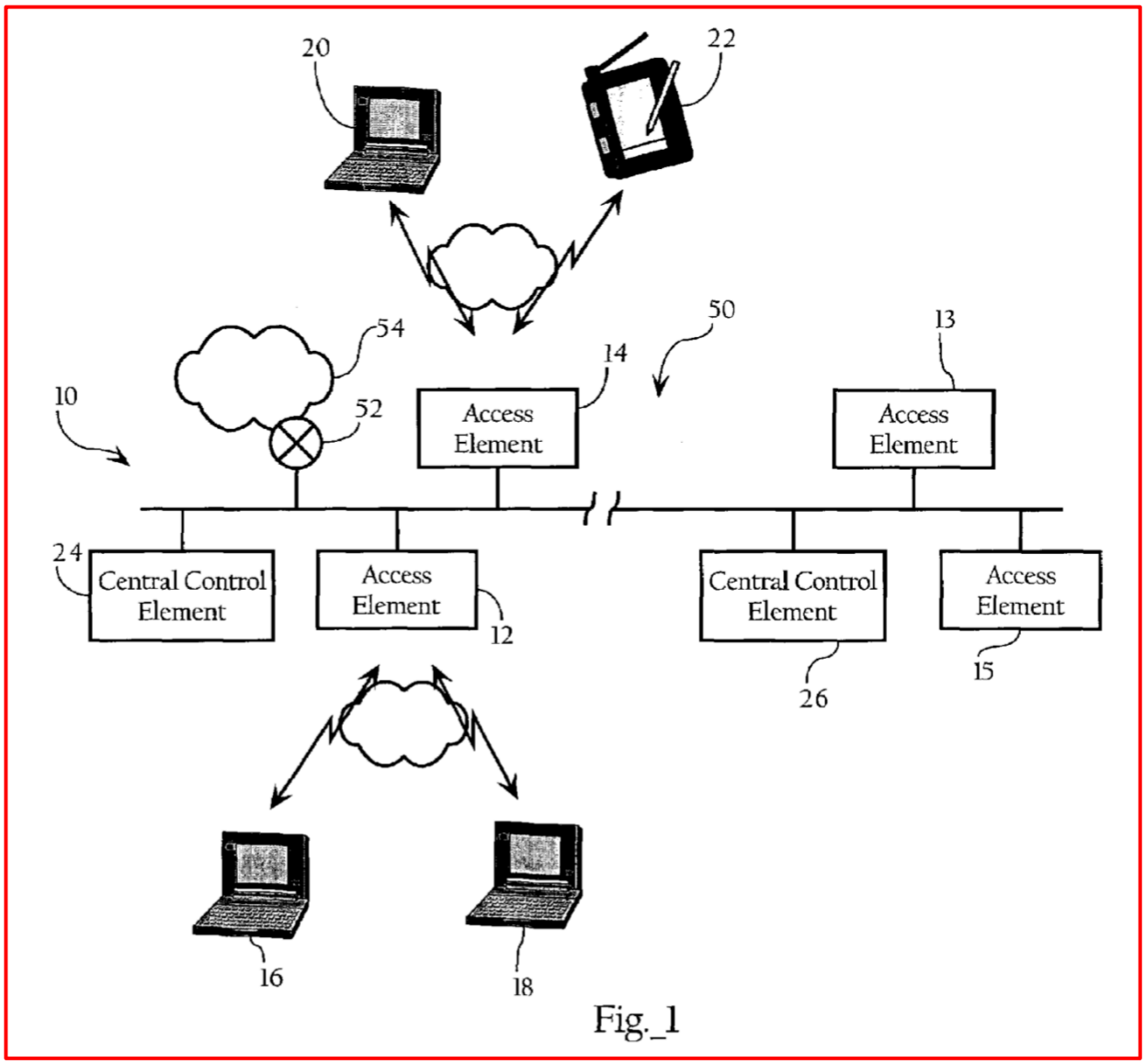


Fig._1

107. 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 (WIAN) 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).

108. 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).

109. 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).

110. 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).

111. 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).

112. 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).

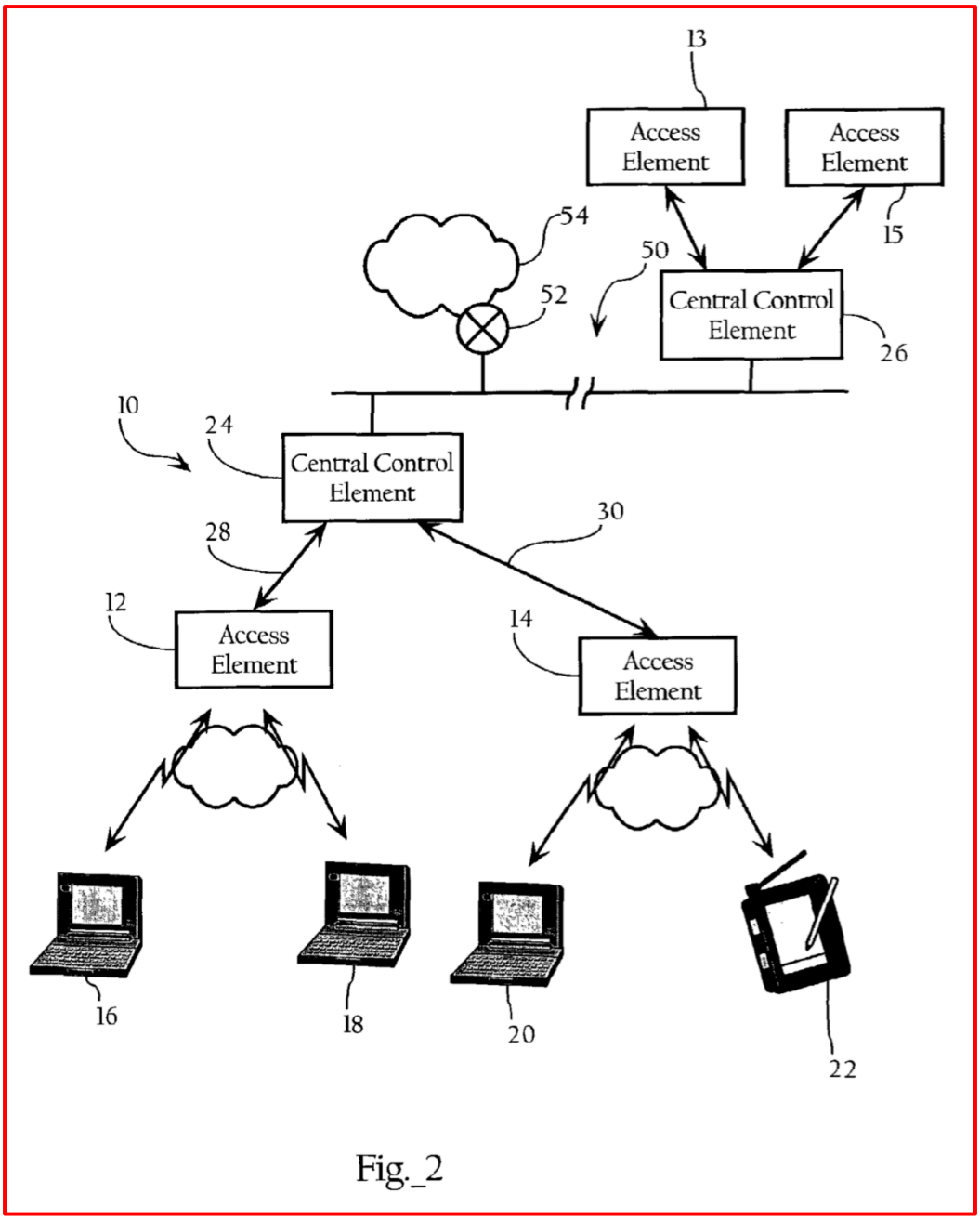


Fig._2

113. 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).

114. 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).

115. 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 '531 Patent and that Calhoun is reasonably pertinent to the problem faced by the '531 Patent (see, for example, ¶¶ 46-52 above regarding the '531 Patent in comparison with the above-summarized introduction to Calhoun). Accordingly, Calhoun is analogous art to the '531 Patent.

116. 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).

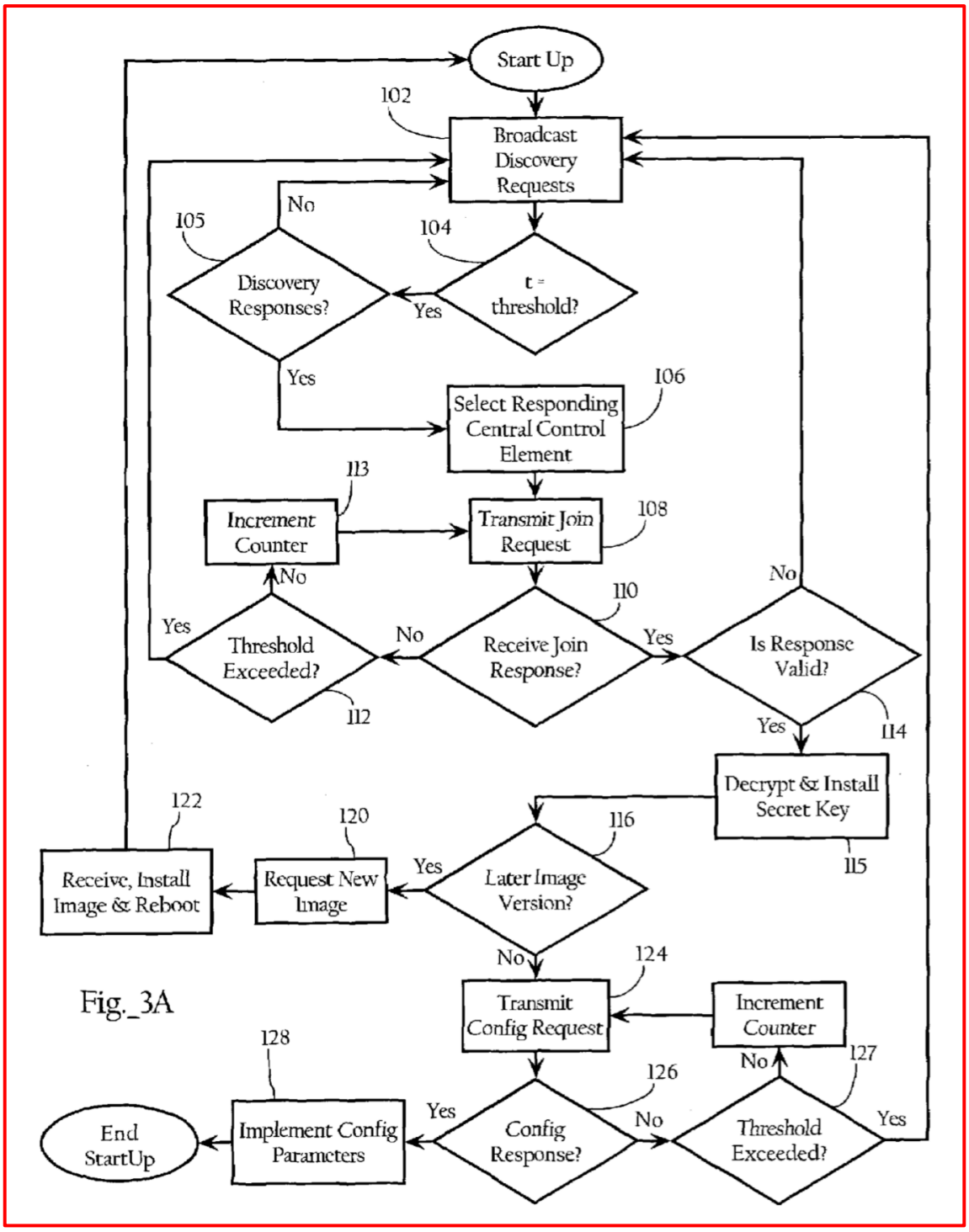


Fig._3A

117. 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).

118. 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).

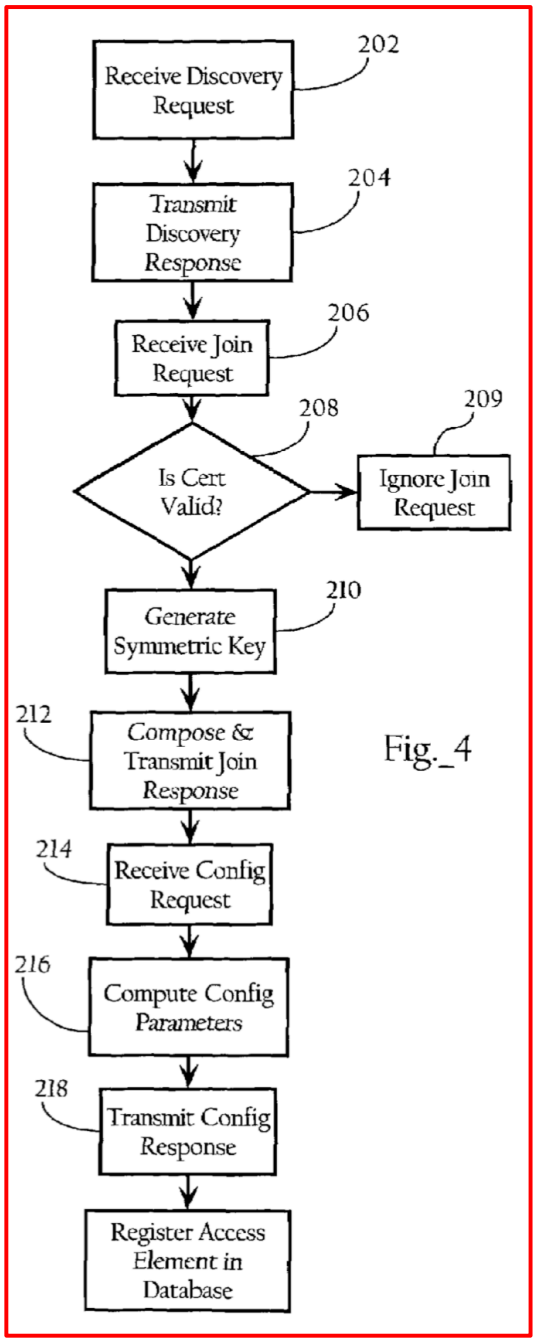


Fig._4

119. 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).

120. 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).

121. 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).

122. 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).

123. 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).

124. 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).

125. 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).

126. 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).

127. 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).

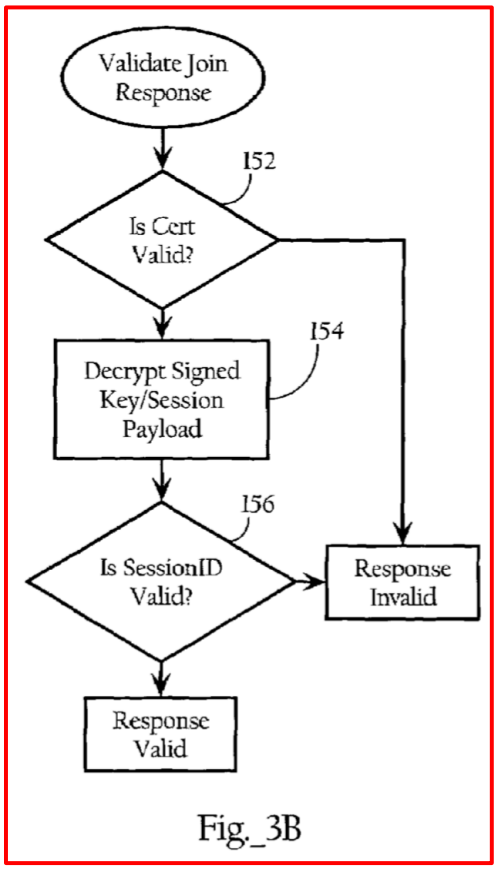


Fig._3B

128. 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).

129. Calhoun further discloses that "the *join request* transmitted during the joinder phase can also be *configured to determine the Maximum Transmit Unit* (MTU) for the link between access element **15** and central control element **24**" 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).

130. 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).

131. 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).

132. 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).

133. 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).

134. 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).

135. 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).

136. 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).

137. 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).

138. 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 join request is not received, transmitting a second join 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)

139. 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 '531 Patent at least under 35 U.S.C. § 102(a).

140. 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).

141. 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).

142. 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).

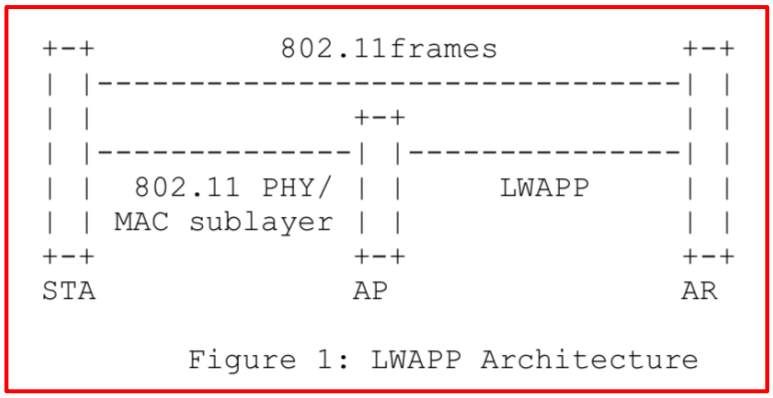


Figure 1: LWAPP Architecture

143. 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).

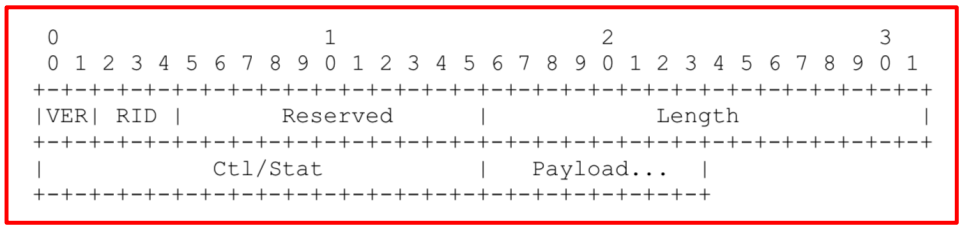
144. More specifically, LWAPP explains that "The *Join Request* also provides an *MTU discovery mechanism*, to determine whether there is *support for the transport of jumbo frames* between the AP and it's AR" wherein "*If support for jumbo frames is not present*, the LWAPP *frames will be fragmented*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

145. 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).

146. 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).

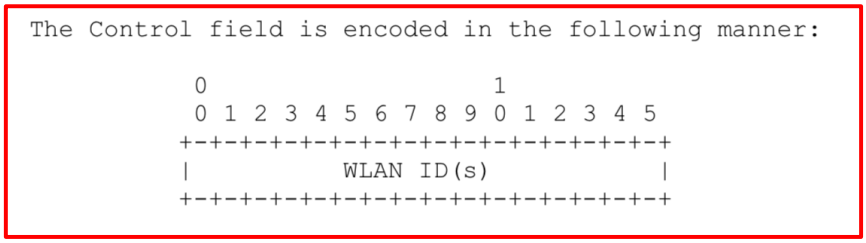
147. Therefore, in my opinion, a POSITA would understand even before considering the detailed disclosure of LWAPP to follow that LWAPP is from the same field of endeavor as the '531 Patent and that LWAPP is reasonably pertinent to the problem faced by the '531 Patent (see, for example, ¶¶ 46-52 above regarding the '531 Patent in comparison with the above-summarized introduction to LWAPP). Accordingly, LWAPP is analogous art to the '531 Patent.

148. 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).



149. 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).



150. 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).

151. 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).

152. 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).

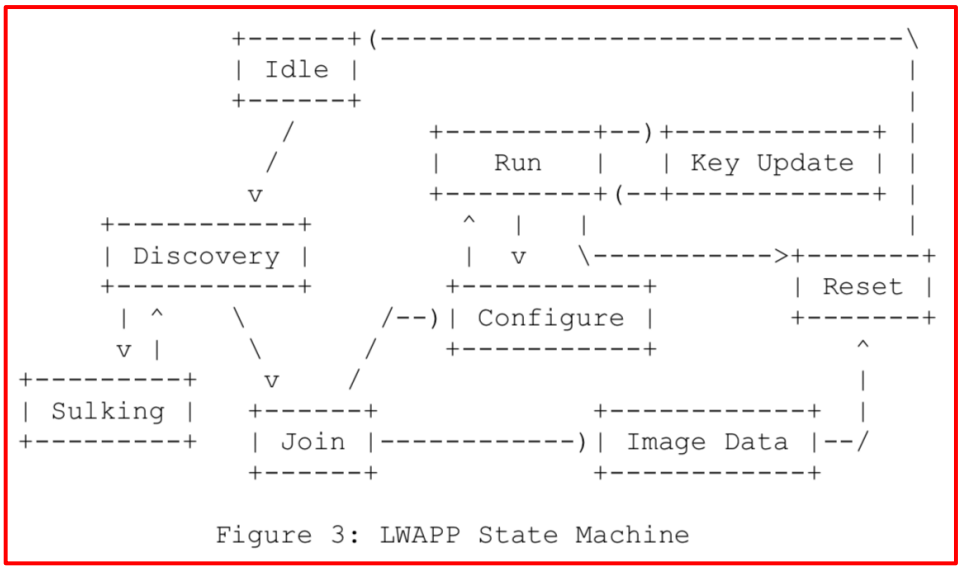


Figure 3: LWAPP State Machine

153. 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

154. 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).

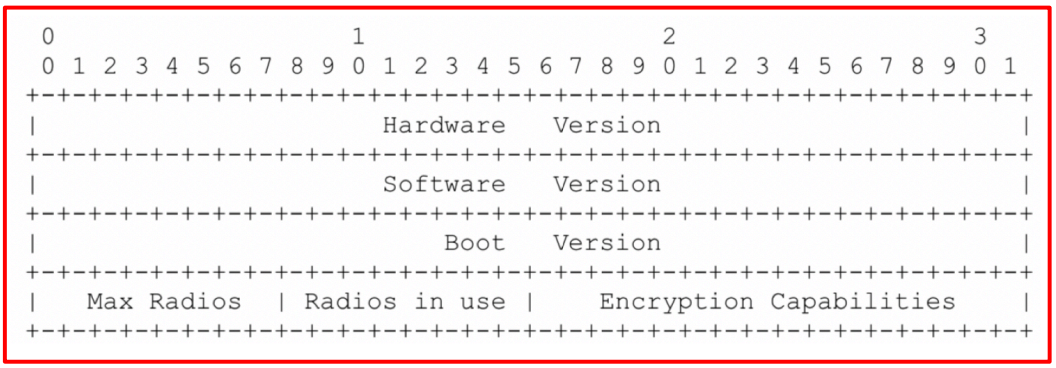
Description	Type
Result Code	1
AR Address	2
AP Payload	3
AP Name	4
AR Payload	5
Reserved	6
AP WLAN Radio Configuration	7
Rate Set	8
Multi-domain capability	9
MAC Operation	10
Reserved	11
Tx Power Level	12
Direct Sequence Control	13
OFDM Control	14
Supported Rates	15
Reserved	16
Test	17
Reserved	18-25
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

155. 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).

156. 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).

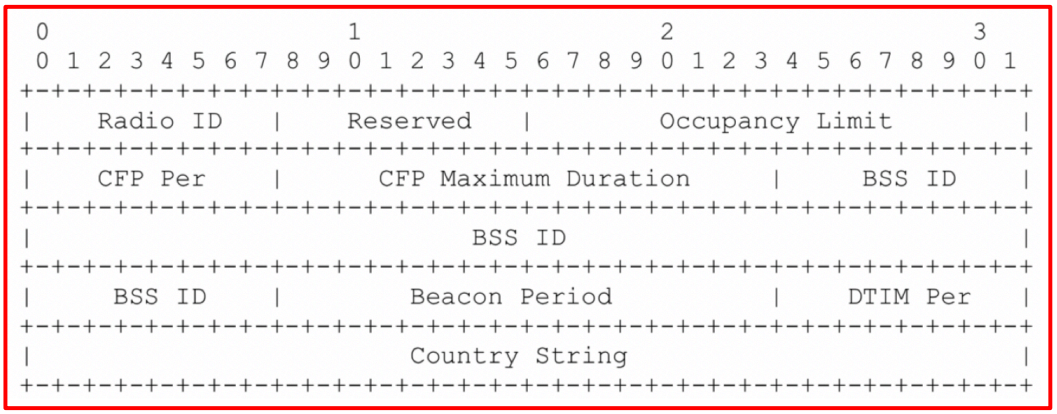
157. More specifically, LWAPP describes the format of this "*AP payload* message element" as including the "*current hardware/firmware configuration*" of the AP as well as information on the number of "*Radios*" and the "*Encryption Capabilities*" of the AP (emphasis added, see, for example, Ex. 1006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



158. 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* it's *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).

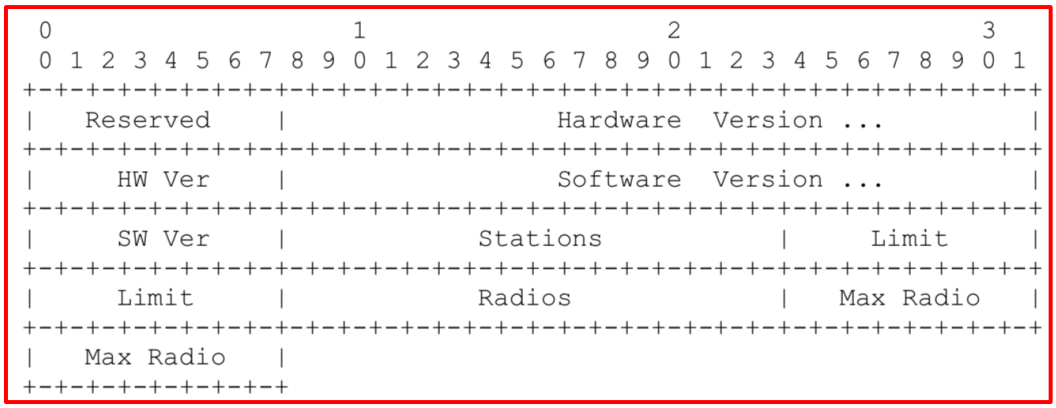
159. Additionally, LWAPP describes the format of the "*Radio Payload*" or "*AP WLAN Radio Configuration*" "message element" that is "*used by the AR to configure a Radio on the AP*" as including at least the fields "*Radio ID*: An 8-bit value representing the radio to configure", "*BSSID*: The WLAN Radio's 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).



160. 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).

161. 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).



162. 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).

163. 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).

164. 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).

165. 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).

166. 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).

167. 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).

168. 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).

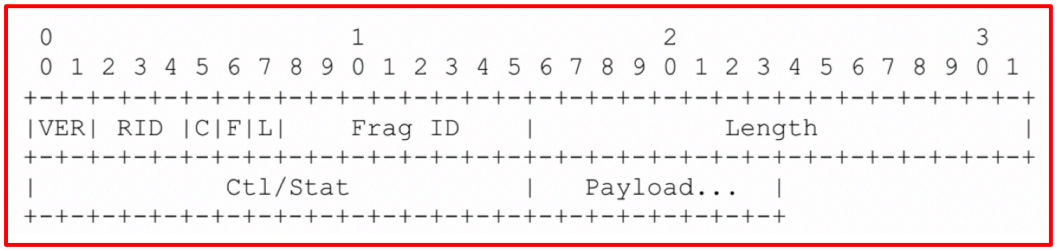
169. For example, LWAPP explains that "*When an AR receives a Configure Request* it will act upon the content of the packet and *respond to the AP with a Configure Response*" which "provides an *opportunity for the AR to override an AP's configuration*" wherein such "*Configure Response* carries the 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).

170. 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).

171. 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).

172. 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).

173. 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 ¶ 148 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).



174. 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).

175. 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).

176. 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).

177. 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).

178. 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 s*ecured 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)

179. 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 '531 Patent at least under 35 U.S.C. § 102(a).

180. 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).

181. 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).

182. 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).

183. 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).

184. 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).

185. 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).

186. 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).

187. 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).

188. 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).

189. 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).

190. 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)

191. 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 '531 Patent at least under 35 U.S.C. § 102(a).

192. 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).

193. 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).

194. 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).

195. 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).

196. 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).

197. 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).

198. 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>.

199. 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 '531 Patent and that CAPWAP is reasonably pertinent to the problem faced by the '531 Patent (see, for example, ¶¶ 46-52 above regarding the '531 Patent in comparison with the above-summarized introduction to CAPWAP). Accordingly, CAPWAP is analogous art to the '531 Patent.

200. 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).

201. 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).

202. 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).

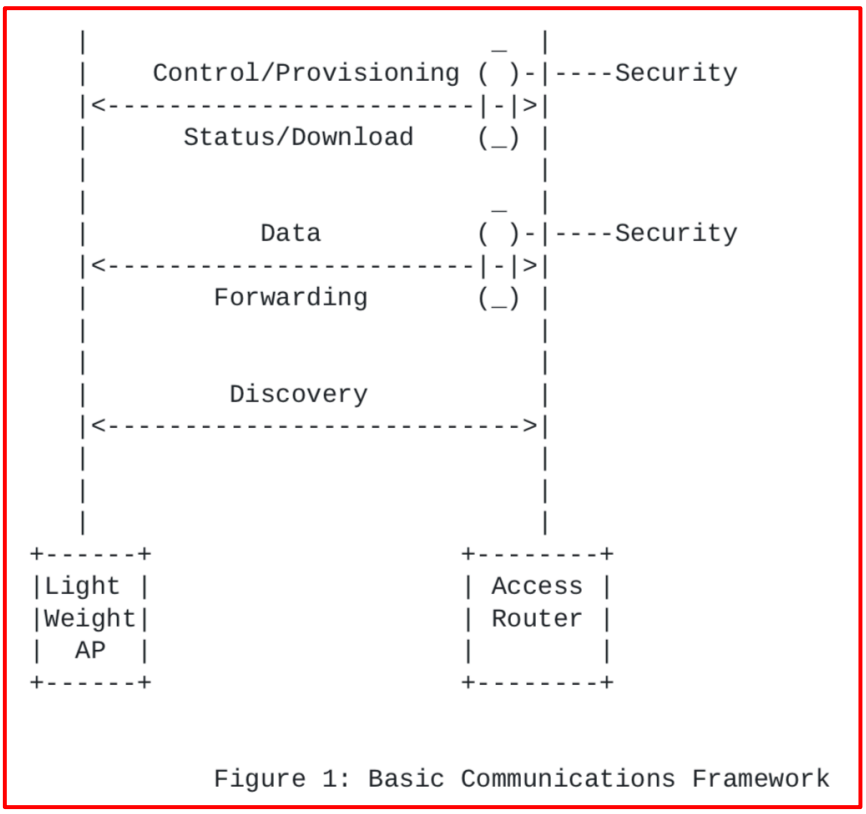


Figure 1: Basic Communications Framework

203. 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) Beaconing

d) Synchronization

e) Power Management

f) Channel Assignment

g) Transmit Power Control

h) Clear Channel Assignment

i) Radio Resource Measurement

j) RADAR detection

204. 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

205. 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)

206. 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).

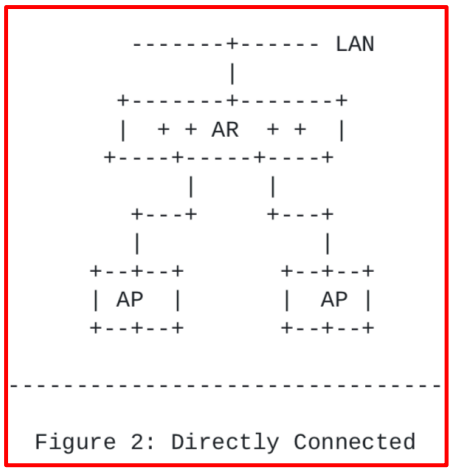


Figure 2: Directly Connected

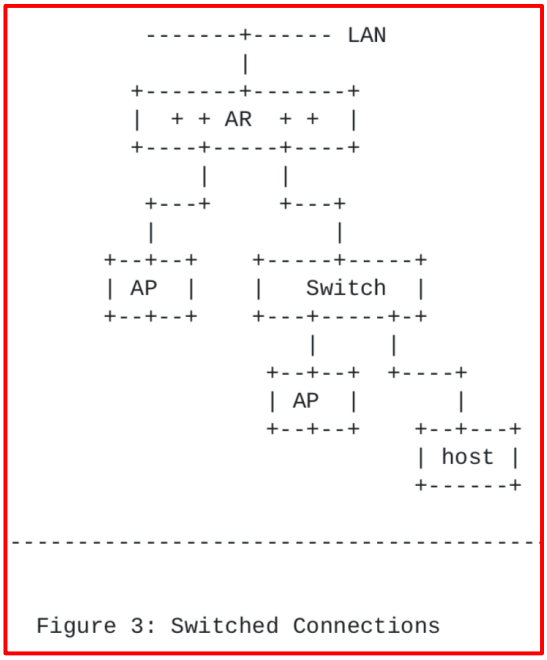


Figure 3: Switched Connections

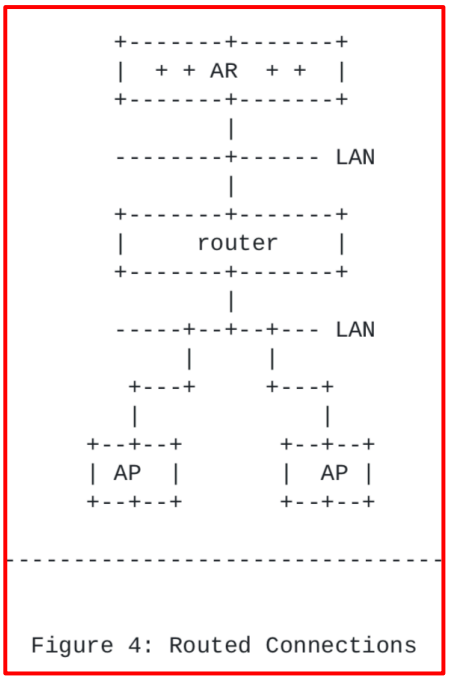


Figure 4: Routed Connections

207. 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).

208. 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).

209. 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).

210. 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).

211. 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).

212. 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).

213. 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).

214. 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).

215. 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)

216. 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 '531 Patent at least under §§ 102(a) and 102(b).

217. 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).

218. 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).

219. 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).

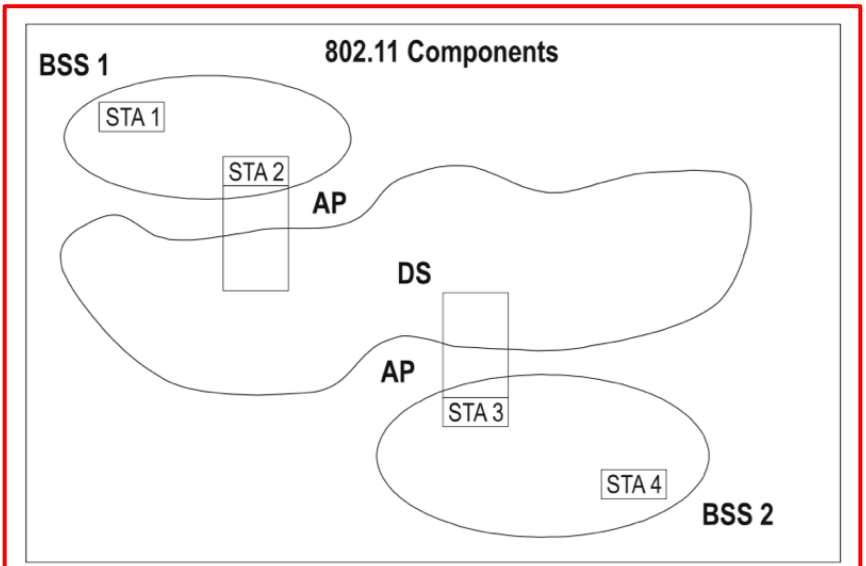


Figure 2—Distribution systems and access points

220. 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).

221. 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).

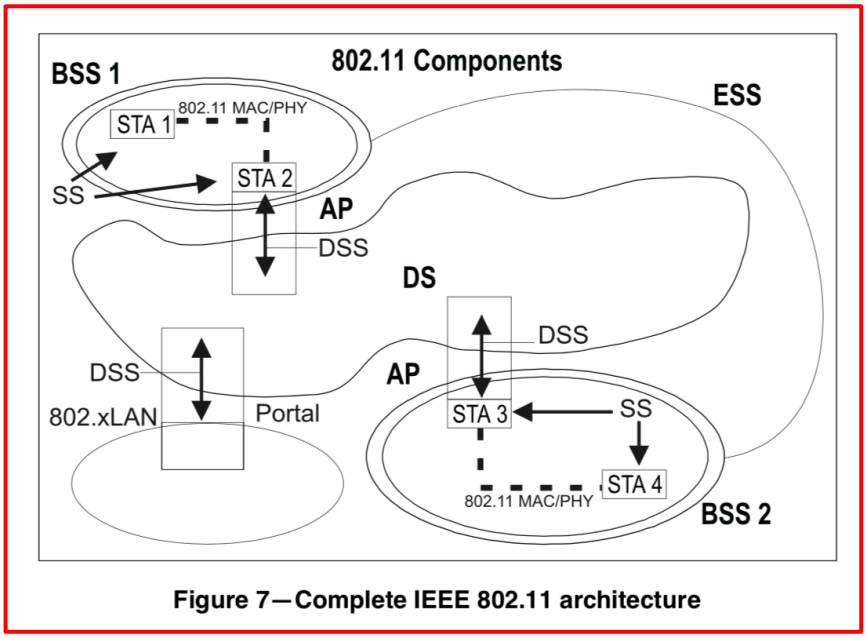


Figure 7—Complete IEEE 802.11 architecture

222. 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).

223. 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).

224. 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).

225. 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).

226. 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).

227. 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).

228. 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).

229. 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).

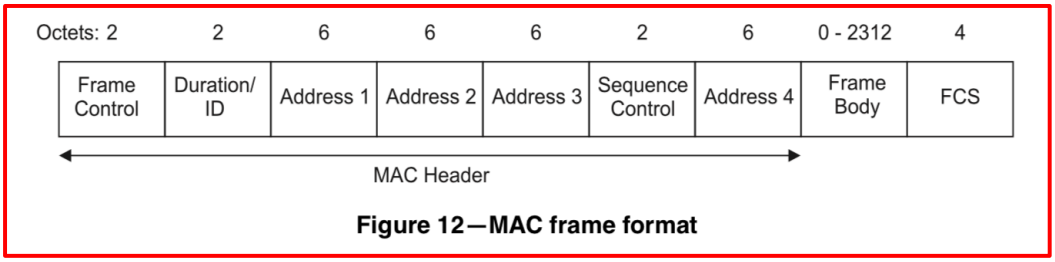


Figure 12—MAC frame format

230. 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).

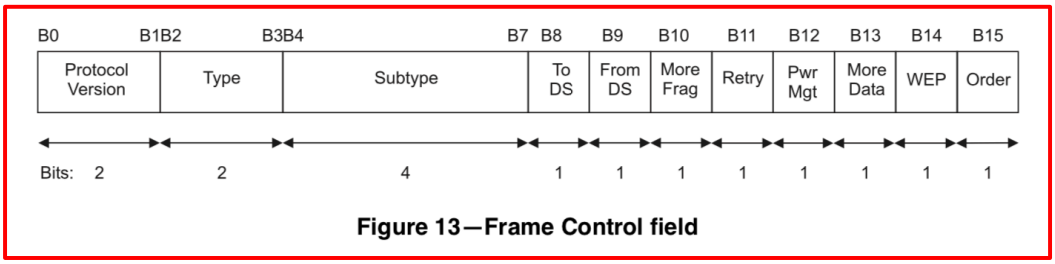


Figure 13—Frame Control field

231. 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

232. 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).

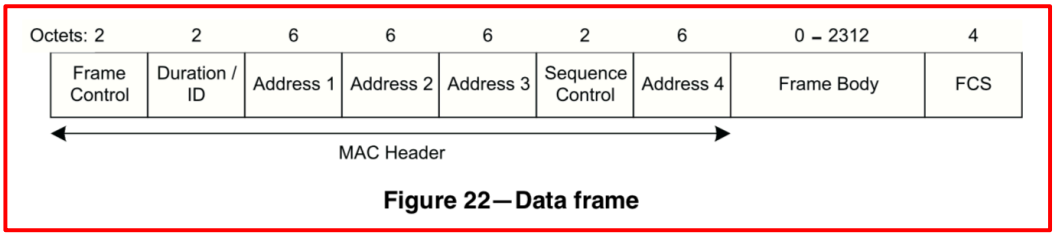


Figure 22—Data frame

233. 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).

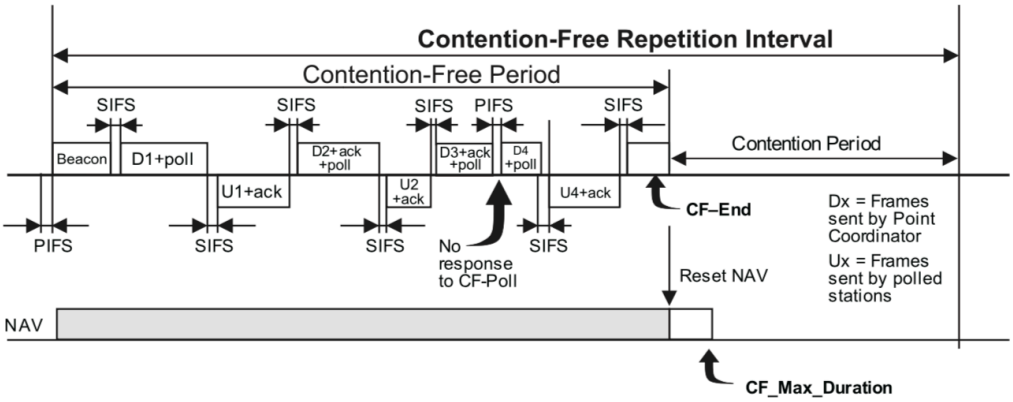


Figure 62—Example of PCF frame transfer

VIII. ANTICIPATION AND/OR OBVIOUSNESS OF THE '531 PATENT UNDER 35 U.S.C. §§ 102, 103 DUE TO CALHOUN, LWAPP AND/OR CAPWAP

234. In my opinion, Calhoun anticipates at least Claims 1, 7 and 13 of the '531 Patent for at least the reasons described herein.

235. In my opinion, Calhoun enabled a POSITA to practice Claims 1, 7 and 13 of the '531 Patent at least to the same extent that the specification of the '531 Patent is considered to enable a POSITA to practice Claims 1, 7 and 13 of the '531 Patent.

236. In my opinion, Calhoun in view of LWAPP and CAPWAP renders obvious at least Claims 1, 7 and 13 of the '531 Patent for at least the reasons described herein.

237. Calhoun is analogous art to the '531 Patent (see ¶ 115 above). Similarly, LWAPP is also analogous art to the '531 Patent (see ¶ 147 above). Additionally, CAPWAP is analogous art to the '531 Patent (see ¶ 199 above).

238. A general overview of Calhoun is given at ¶¶ 102-138 above.

239. A general overview of LWAPP is given at ¶¶ 139-178 above.

240. A general overview of CAPWAP is given at ¶¶ 191-214 above.

241. In my opinion, a POSITA at the alleged time of invention for the '531 Patent would have been highly motivated to combine Calhoun, LWAPP and CAPWAP for at least the following reasons.

242. 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, ¶¶ 103-107, 140-142 and 192-197 above).

243. 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.

244. 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, ¶ 105 above).

245. 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, ¶ 141 above).

246. 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, ¶¶ 192 and 195 above).

247. 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 '531 Patent (see also ¶ 14 above).

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

249. 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, ¶ 113 above).

250. 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, ¶¶ 140, 143 and 145 above).

251. 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, ¶¶ 193, 198 and 213 above).

252. 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.

253. 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.

254. 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, ¶¶ 102 and 190 above).

255. 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, ¶ 139 above).

256. 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, ¶¶ 191, 198 and 215 above).

257. 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.

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

259. 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, ¶ 180 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 '531 Patent (see also ¶ 14 above).

260. 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, ¶ 181 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.

261. 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, ¶¶ 188-189 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.

262. 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.

263. In my opinion, a POSITA at the alleged time of invention for the '531 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.

264. 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 1-16 of the '531 Patent is given herein.

265. 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 '531 Patent claims themselves.

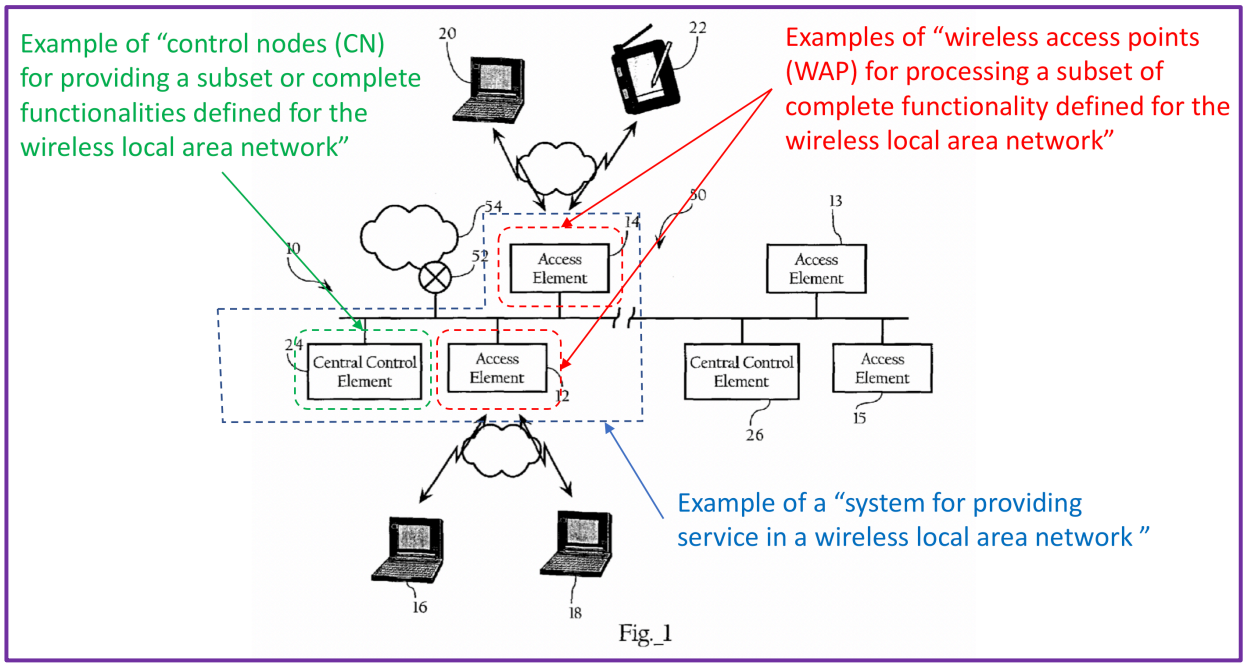
'531 Patent: Claim 1

1. A system for providing service in a wireless local area network comprising:
a single or plurality of wireless access points (WAP) for processing a subset of complete functionality defined for the wireless local area network;
a single or plurality of control nodes (CN) for providing a subset or complete functionalities defined for the wireless local area network; and
a negotiation unit for the single or plurality of WAPs to dynamically negotiate with the control node for a secure connection and function split arrangement;
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.

1. A system for providing service in a wireless local area network comprising:

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

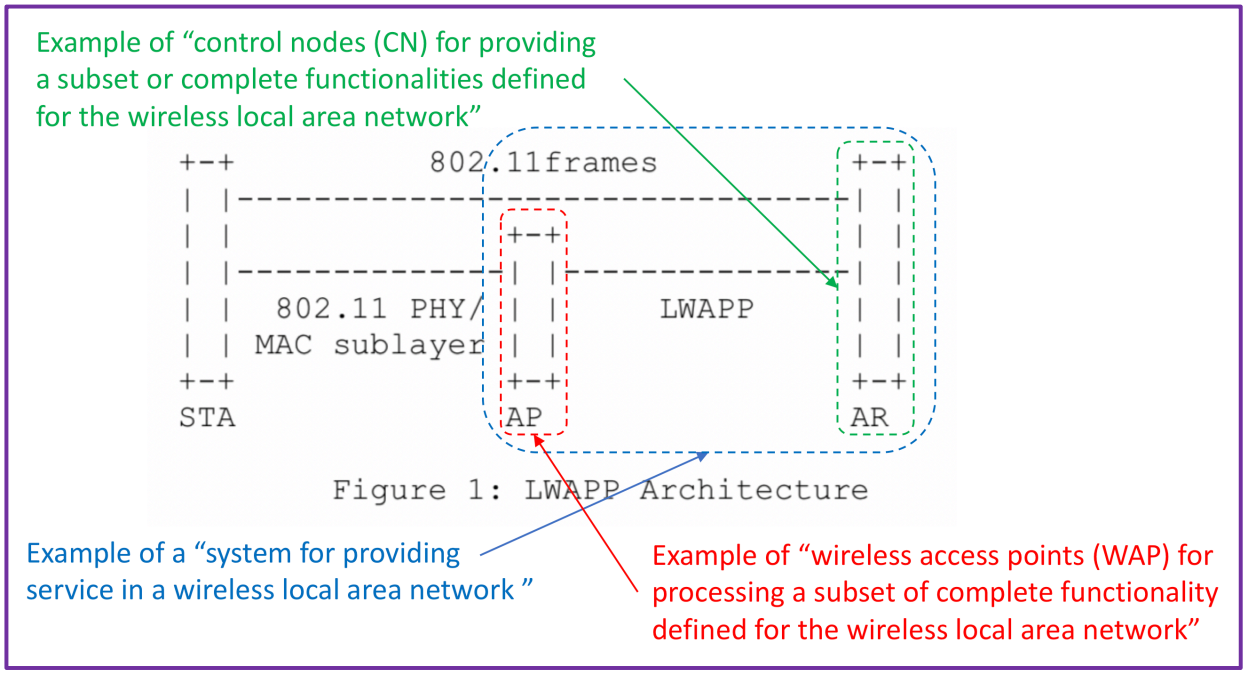
267. Calhoun discloses "methods, apparatuses and systems facilitating the *deployment and configuration of managed access points in a wireless network system*" wherein "FIG. 1" shows a "block diagram of a *wireless Local Area Network (LAN)* **10**" (see, for example, ¶¶ 103, 106 and 138 above, and annotated FIG. 1 shown below).



268. Thus, Calhoun discloses a "**system for providing service**" (for example, the "***wireless network system***" of Calhoun) that is "**in a wireless local area network**" (for example, a "***wireless Local Area Network (LAN)***" as also depicted in FIG. 1 of Calhoun).

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

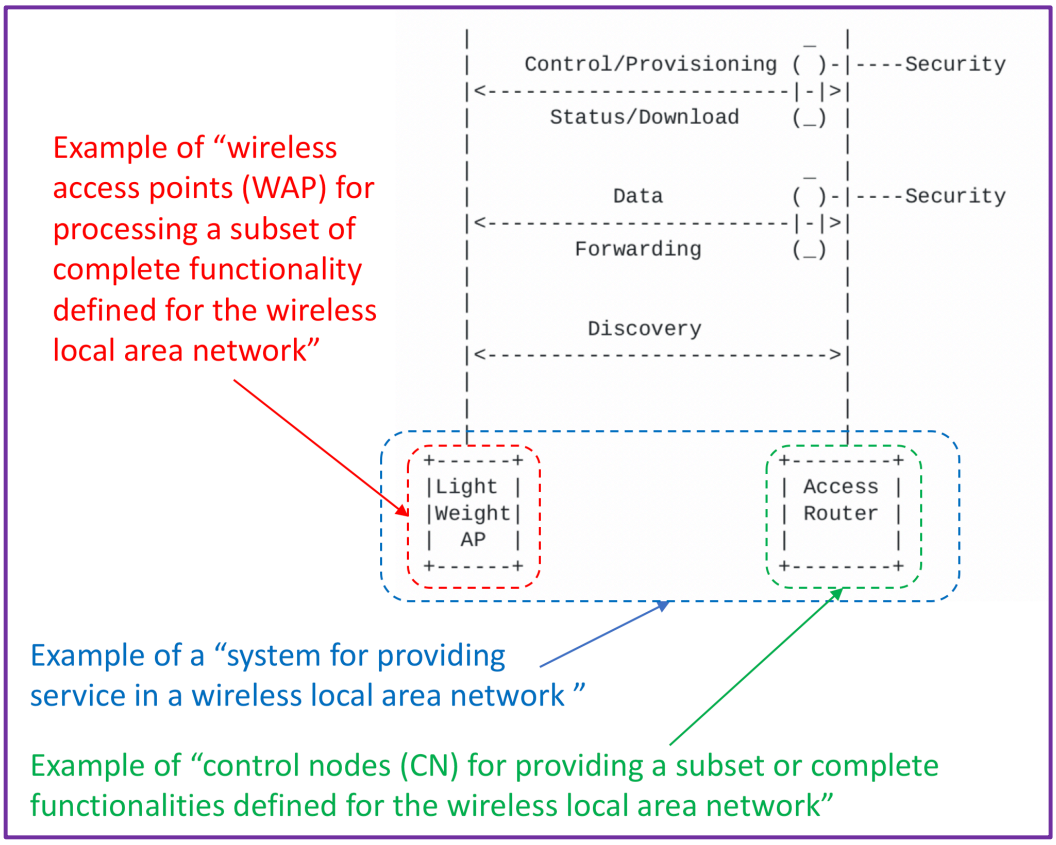
270. LWAPP discloses "the *Light Weight Access Point Protocol* which is a protocol allowing a router or switch *to interoperably control and manage a collection of wireless Access Points*" in order to "*simplify the deployment and management of wireless networks*" due to the "*Centralization* of the *bridging, forwarding, authentication, encryption and policy enforcement functions* for a *WLAN*" as shown in the "LWAPP Architecture" diagram (see, for example, ¶¶ 140-141 above, and annotated Figure 1 shown below).



271. Thus, LWAPP discloses a "**system for providing service**" (for example, the "***wireless networks***" of LWAPP) that is "**in a wireless local area network**" (for example, a "***WLAN***" as also depicted in Figure 1 of LWAPP).

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

273. 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*" wherein "*Figure 1* illustrates the basic outline of *communications architecture between AP & AC*" (see, for example, ¶¶ 192 and 202 above, and annotated Figure 1 shown below).



274. Thus, CAPWAP discloses a "**system for providing service**" (for example, the "***communications architecture***" of CAPWAP) that is "**in a wireless local area network**" (for example, a "***WLAN***" as also depicted in Figure 1 of CAPWAP).

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

276. See at least ¶¶ 241-263 above regarding the combination of Calhoun, LWAPP and CAPWAP.

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

278. Calhoun discloses a "block diagram of a *wireless Local Area Network (LAN)* **10**" that includes "*managed access points*" in the form of "*access elements* **12-15** for wireless communication with *remote client elements* **16**, **18**, **20**, **22**" (see, for example, ¶¶ 103, 106 and 138 above, and annotated FIG. 1 shown at ¶ 267 above).

279. For example, Calhoun discloses that such "*access elements* perform *real-time communication functions*, such as data transfer and acknowledgements" without "*manag[ing] the connection between the access element and one or more wireless client devices*" (see, for example, ¶ 105 above).

280. For example, Calhoun discloses that although "The *access elements* **12-15** are coupled via communication means *using a wireless local area network (WIAN) 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, ¶¶ 107, 109 and 135 above).

281. Thus, Calhoun discloses "**a single or plurality of wireless access points (WAP)**" (for example, the "***managed access points***" or "***access elements***" of Calhoun) that are "**for processing a subset of complete functionality defined for the wireless local area network**" (for example, "***operating in 802.11 wireless networks***" according to "***IEEE 802.11a or 802.11b, etc.***" without "***perform[ing] link layer management functions, such as authentication and association***" per the disclosures of Calhoun).

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

283. LWAPP discloses for the "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*)" that "The *APs can be considered as remote RF interfaces*, being *controlled by the AR* (see Figure 1)" (see, for example, ¶¶ 141-142 above, and annotated Figure 1 shown at ¶ 270 above).

284. LWAPP further 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, ¶¶ 141-142 above).

285. Thus, LWAPP discloses "**a single or plurality of wireless access points (WAP)**" (for example, the "***simple***" or "***Light Weight***" "***Access Points***" or "***APs***" of LWAPP) that are "**for processing a subset of complete functionality defined for the wireless local area network**" (for example, operating "***in 802.11***" without performing the "***bridging, forwarding,***

authentication, encryption and policy enforcement functions for a WLAN" per the disclosures of LWAPP).

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

287. 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, ¶¶ 192 and 203 above, and annotated Figure 1 shown at ¶ 273 above).

288. Thus, CAPWAP discloses "**a single or plurality of wireless access points (WAP)**" (for example, the "***lightweight Access Point (LAP)***" of CAPWAP) that are "**for processing a subset of complete functionality defined for the wireless local area network**" (for example, operating in "***802.11***" while performing the "***AP (Access Point) functions***" that are "***directly related to the real-time aspects of the 802.11 MAC protocol and those related to the radio nature of an 802.11 AP***" per the disclosures of CAPWAP).

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

290. See at least ¶¶ 241-263 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 then Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA also renders obvious the limitations of this claim element.

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

292. 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, ¶¶ 105 and 138 above).

293. For example, Calhoun discloses a "block diagram of a *wireless Local Area Network (LAN)* **10**" that includes "*central control elements* **24**, **26** for controlling and managing the wireless connections between the access elements **12-15** and the remote client elements" (see, for example, ¶¶ 106 and 138 above, and annotated FIG. 1 shown at ¶ 267 above).

294. For example, Calhoun discloses such "*central control elements*" that "have been *described as operating in 802.11 wireless networks*" do "perform *link layer management functions*, such as *authentication and association*" for "*the wireless LAN management messages passed on from the client remote elements*" (see, for example, ¶¶ 109 and 135 above).

295. Thus, Calhoun discloses "**a single or plurality of control nodes (CN)**" (for example, the "***central control elements***" of Calhoun) that are "**for providing a subset or complete functionalities defined for the wireless local area network**" (for example, "***operating in 802.11 wireless networks***" while "***perform[ing] link layer management functions, such as authentication and association***" per the disclosures of Calhoun).

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

297. See ¶¶ 283-284 above.

298. Thus, LWAPP discloses "**a single or plurality of control nodes (CN)**" (for example, the "***Access router, or AR***" of LWAPP) that are "**for providing a subset or complete**

functionalities defined for the wireless local area network" (for example, operating "***in 802.11***" while performing the "***bridging, forwarding, authentication, encryption and policy enforcement functions for a WLAN***" per the disclosures of LWAPP).

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

300. 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" (see, for example, ¶ 194 above).

301. 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 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*" (see, for example, ¶¶ 192 and 204 above, and annotated Figure 1 shown at ¶ 273 above).

302. Thus, CAPWAP discloses "**a single or plurality of control nodes (CN)**" (for example, the "***AR (Access Router), AC (Access Controller) and AB (Access Bridge)***" that "***are used synonymously***" in CAPWAP) that are "**for providing a subset or complete functionalities defined for the wireless local area network**" (for example, operating "***in 802.11***" while performing the "***management and control aspects of an 802.11 AP***" such as "***the distribution system services, in addition to authentication and deauthentication services***" per the disclosures of CAPWAP).

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

304. See at least ¶¶ 241-263 above regarding the combination of Calhoun, LWAPP and CAPWAP.

305. 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.

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

306. 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*" (see, for example, ¶ 108 above).

307. 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*" (see, for example, ¶ 113 above).

308. 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*" (see, for example, ¶ 114 above).

309. Calhoun explains that "*At startup*, *access element* **15** *broadcasts or multicasts discovery requests* … to *identify central control elements* (**102**)" and then subsequently "*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*" 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* of a given central control element" (see, for example, ¶¶ 117-119 above).

310. 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**)" 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, ¶ 120 above).

311. 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." 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, ¶¶ 121-122 above).

312. In the next step of this "*joinder phase*", 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 "*composes a join response*" that 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**" and then "*transmits it to access element* **15** (**212**)" (see, for example, ¶¶ 124-125 above).

313. 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, ¶ 127 above).

314. Accordingly, a POSITA would understand that this "***digital certificate***" validation and "***cryptographic keys***" exchange within 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 "**dynamically negotiate with the control node for a secure connection**" as recited for this claim element particularly in view of the disclosure in Calhoun that "***After a threshold number of failed attempts, access element***" 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***" as disclosed by the procedures shown in and described for FIG. 3A and FIG. 3B of Calhoun (see, for example, ¶¶ 116, 123 and 127 above).

315. For example, Calhoun further explains for this "***joinder phase***" that "the *join request* transmitted during the joinder phase can also be *configured to determine the Maximum Transmit Unit* (MTU) for the link between access element **15** and central control element **24**" 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*" (see, for example, ¶ 129 above).

316. Accordingly, a POSITA would understand that this "***Maximum Transmit Unit***" determination aspect of the "***joinder phase***" of Calhoun which follows the "***discovery phase***" as described above also discloses at least that the "***access element***" of Calhoun is configured to "**dynamically negotiate with the control node for a … function split arrangement**" as recited for this claim element because "***to determine whether a wireless packet … can be encapsulated with additional headers and transmitted without requiring fragmentation***" using the process disclosed in Calhoun determines if the "**function split arrangement**" between the "***access element***" and the "***central control element***" of Calhoun needs to include or not include the functions of "***fragmentation***" (and hence also "***defragmentation***") in each "***element***".

317. For example, 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, ¶ 130 above).

318. For example, 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, ¶¶ 131-132 above).

319. 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, ¶¶ 133-134 above).

320. Accordingly, a POSITA would understand that either or both of this "***image version***" update aspect and this "***operational parameters***" exchange aspect of the "***configuration phase***" of Calhoun as described above also discloses at least that the "***access element***" of Calhoun is configured to "**dynamically negotiate with the control node for a … function split arrangement**" as recited for this claim element because each such aspect involves "***dynamically configur[ing]***" the details of the partial WLAN functionality as implemented in the "***access element***" as part of a "**function split arrangement**" with the "***central control element***".

321. Furthermore, a POSITA would understand that this "***operational parameters***" exchange aspect of the "***configuration phase***" of Calhoun discloses to "**dynamically negotiate with the control node for a … function split arrangement**" as recited for this claim element at least because "***generat[ing] the operational parameters for access element***" at the "***central control element***" while "***taking into account the overriding parameters identified in the configuration request***" from the "***access element***" describes a management "**function**" of the WLAN that is performed specifically within a "**split arrangement**" among both the "***central control element***" and the "***access element***" of Calhoun, and because the disclosure in Calhoun of "***overriding parameters***" being set at each time of "***configuration***" at the "***access element***" such that the "***central control element can not change***" specifically describes a "**dynamic negotiation**" between the "***central control element***" and the "***access element***" of Calhoun.

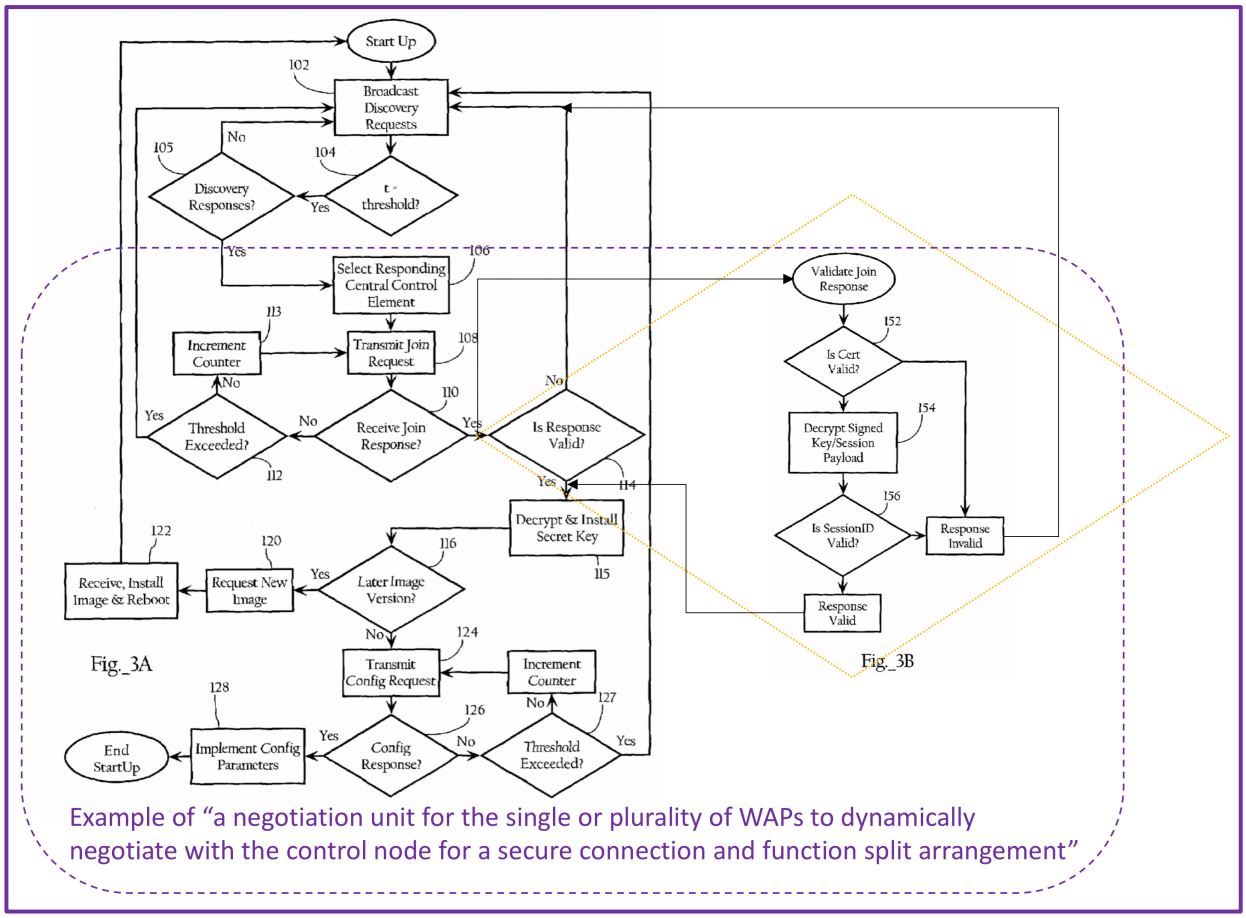
322. Additionally, Calhoun explains that when "*operating in 802.11 wireless networks*" that "the *division of functionality between the access elements and the central control elements can be shifted*" wherein "For example, the *access elements can bridge network traffic* associated with the remote client elements directly, *while transmitting management packets to the central control element*" (see, for example, ¶¶ 135-136 above).

323. Accordingly, a POSITA would understand that Calhoun's disclosure to "***dynamically configure***" the "***elements***" of "***802.11 wireless networks***" also shows at least that the "***access element***" of Calhoun is configured to "**dynamically negotiate with the control node for a … function split arrangement**" as recited for this claim element because this "***division of functionality between the access elements and the central control elements can be shifted***" with a specific example being when the "***access elements***" are configured to "***bridge network traffic associated with the remote client elements directly, while transmitting***

management packets to the central control element" instead of "***transmitting***" both "***data***" and "***management packets to the central control element***".

324. Calhoun also discloses that "***implementing the discovery, joinder and configuration phases of LWAPP***" by which the "***division of functionality***" for the "***access elements***" and the "***central control elements***" becomes "***dynamically configure[d]***" is also shown by the "***flow chart diagrams***" FIG. 3A and FIG. 3B of Calhoun (see, for example, ¶¶ 116 and 127 above).

325. Accordingly, a POSITA would understand that Calhoun also discloses a "**negotiation unit for the single or plurality of WAPs**" within each one of the "***access elements***" and is configured "**to dynamically negotiate with the control node for a secure connection and function split arrangement**" per the recited limitations of this claim element as shown by my annotated composite below for FIG. 3A and FIG. 3B of Calhoun:



326. I also note that a POSITA would know that the prior art at the alleged time of invention of the '531 Patent specifically teaches that the "***joinder and configuration phases of LWAPP***" as described by Calhoun, which follow the "***discovery phase***", are collectively referred to as a "***Capability Negotiation Phase***" (see, for example, ¶¶ 212-214 above), thereby affirming that Calhoun's disclosure to "***dynamically configure***" during these "***joinder and configuration phases of LWAPP***" is interchangeable with the term to "**dynamically negotiate**", and similarly, that the teachings of Calhoun for implementing the "***joinder and configuration phases of LWAPP***" as described by FIG. 3A and FIG. 3B of Calhoun as annotated above is interchangeable with the term "**negotiation unit**".

327. Thus, Calhoun discloses a "**negotiation unit for the single or plurality of WAPs**" (for example, the above annotated portions of composite FIG. 3A and FIG. 3B of Calhoun) that is configured "**to dynamically negotiate with the control node for a secure connection and function split arrangement**" (for example, as shown when the "***division of functionality***" for the "***access elements***" and the "***central control elements***" becomes "***dynamically configure[d]***" during the "***joinder and configuration phases of LWAPP***" as described specifically above for at least the "***digital certificate***" validation and "***cryptographic keys***" exchange aspect of the "***joinder phase***", the "***Maximum Transmit Unit***" determination aspect of the "***joinder phase***", the "***image version***" update aspect and the "***operational parameters***" exchange aspects of the "***configuration phase***", and the "***bridge network traffic***" "***shift***" in "***division of functionality***" between "***access elements***" and the "***central control elements***" aspects of the "***configuration phase***").

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

329. 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*" as part of a "*Join phase*" (see, for example, ¶¶ 143 and 178 above).

330. 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" (see, for example, ¶ 144 above).

331. For example, LWAPP describes for this "*MTU discovery mechanism*" 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*" (see, for example, ¶ 163 above).

332. Accordingly, a POSITA would understand that this "***MTU discovery mechanism***" within the "***Join phase***" of LWAPP which follows the "***discovery phase***" as described above also discloses at least that the "***Access Point***" of LWAPP is configured to "**dynamically negotiate with the control node for a … function split arrangement**" as recited for this claim element because "***to determine whether there is support for the transport of jumbo frames between the AP and it's AR***" using the process disclosed in LWAPP determines if the "**function split arrangement**" between the "***Access Point***" and the "***Access Router***" of LWAPP needs to include or not include the functionality by which "***frames will be fragmented***" (and hence also "***defragmented***") in each of the "***Access Point***" and the "***Access Router***", which is analogous to the disclosure of this process provided in Calhoun (see, for example, ¶¶ 315-316 above).

333. For example, LWAPP further 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, ¶¶ 164-166 and 178 above).

334. Accordingly, a POSITA would understand that this "***PKCS #5 certificate***" validation and "***public key cryptography***" exchange 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 "**dynamically negotiate with the control node for a secure connection**" as recited for this claim element, which is analogous to the disclosure of this process provided in Calhoun (see, for example, ¶¶ 308-314 above).

335. For example, LWAPP also explains 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" via an "*LWAPP Control protocol*" message exchange that is "used by the *AR to push a new firmware image down to the AP*" wherein an "*AP payload* message element" includes its "*current hardware/firmware configuration*" and an "*AR payload* message element" includes its "*Hardware Version*" and "*Software Version*" for such "*code running on the AP*" (see, for example, ¶¶ 145, 151, 157 and 161 above).

336. For example, LWAPP further 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, ¶ 145 above).

337. More specifically, 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*" 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, ¶¶ 168-169 above).

338. Accordingly, a POSITA would understand that either or both of this "***firmware image***" update aspect and this "***provisioning***" exchange aspect of the "***configuration phase***" of LWAPP as described above also discloses at least that the "***Access Point***" of LWAPP is configured to "**dynamically negotiate with the control node for a … function split arrangement**" as recited for this claim element because each such aspect involves "***overrid [ing]***" the details of the partial WLAN functionality as implemented in the "***Access Point***" as part of a "**function split arrangement**" with the "***Access Router***", which is analogous to the disclosure of this process provided in Calhoun (see, for example, ¶¶ 317-320 above).

339. Additionally, LWAPP provides a "*state diagram*" that "represents the *lifecycle of an AP-AR session*" in Figure 3 (see, for example, ¶ 152 above), which, in my opinion, a POSITA would understand discloses a "**negotiation unit for the single or plurality of WAPs**" within each "***Access Point***" and is configured "**to dynamically negotiate with the control node for a secure connection and function split arrangement**" per the recited limitations of this claim element as discussed above and shown by my annotated version of Figure 3 of LWAPP:

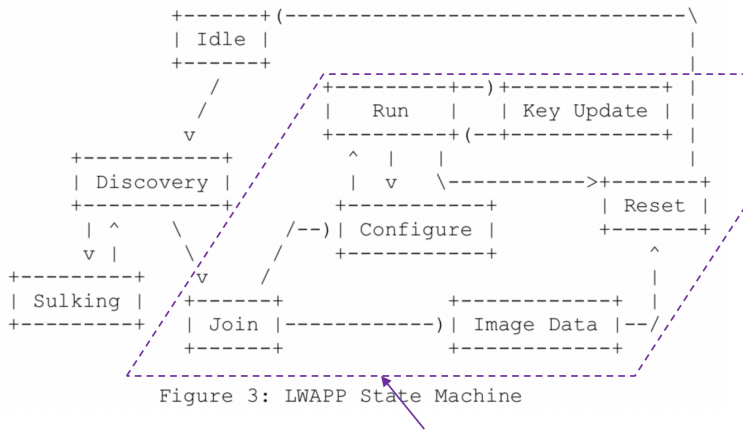


Figure 3: LWAPP State Machine

Example of "a negotiation unit for the single or plurality of WAPs to dynamically negotiate with the control node for a secure connection and function split arrangement"

340. See also ¶ 326 above, which is applicable to LWAPP as well as Calhoun.

341. Thus, LWAPP discloses a "**negotiation unit for the single or plurality of WAPs**" (for example, the above annotated portions of Figure 3 of LWAPP) that is configured "**to dynamically negotiate with the control node for a secure connection and function split arrangement**" (for example, as shown during the "***join and configuration phases of LWAPP***" as described specifically above for at least the "***PKCS #5 certificate***" validation and "***public key cryptography***" exchange within the "***Join phase***", the "***MTU discovery mechanism***" within the "***Join phase***", and the "***firmware image***" update aspect and this "***provisioning***" exchange aspect of the "***configuration phase***").

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

343. 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)" (see, for example, ¶ 192 above).

344. 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)*" (see, for example, ¶ 195 above).

345. 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, ¶ 197 above).

346. More specifically, CAPWAP explains that for this "*Split AP*" approach in the "*CAPWAP architecture*" that there is "a *module in the AR that understands 802.11 management frames*" while using the "*LWAPP protocol*", such usage of the term "*LWAPP protocol*" as "*a domain specific protocol* with some *messages assuming 802.11 semantics*" is specifically referring to the LWAPP prior art reference described and analyzed herein (see, for example, ¶¶ 197-198 above).

347. 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, ¶¶ 207 and 212 above).

348. Accordingly, a POSITA would understand that this "***authenticate***" by "***cryptographically secure binding***" within the "***Capability Negotiation Phase***" of CAPWAP as described above discloses at least that the "***Access Point***" of CAPWAP is configured to

"**dynamically negotiate with the control node for a secure connection**" as recited for this claim element, which is analogous to the disclosure of this process provided in Calhoun (see, for example, ¶¶ 308-314 above).

349. For example, 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, ¶¶ 208-211 above).

350. Accordingly, a POSITA would understand that this "***Configuration***" of "***parameters***" exchange aspect of the "***Capability Negotiation Phase***" of CAPWAP as described above also discloses at least that the "***Access Point***" of CAPWAP is configured to "**dynamically negotiate with the control node for a … function split arrangement**" as recited for this claim element because such "***parameters***" set the details of the partial WLAN functionality as implemented in the "***Access Point***" as part of a "**function split arrangement**", which CAPWAP describes as "***Split AP***", with the "***Access Controller***", which is analogous to the disclosure of this process provided in Calhoun (see, for example, ¶¶ 317-320 above).

351. For example, 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*" (see, for example, ¶ 200 above).

352. Additionally, CAPWAP teaches that because "such *architectures*" have "*varying scope and limitations*" that this "underscores the argument to *provide a negotiable interface protocol*" (see, for example, ¶ 201 above).

353. Additionally, CAPWAP specifically describes that "*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" (see, for example, ¶ 213 above).

354. Accordingly, a POSITA would understand that the "***negotiable interface protocol***" of CAPWAP that determines the "***applicable API's between AP and AC***" based upon "***capabilities negotiated by architectural type match***" during a "***capabilities exchange phase***" describes an "***Access Point***" that is configured to "**dynamically negotiate with the control node for a … function split arrangement**" as recited for this claim element because this "***Split AP***" can be any one of a "***classic AP***" with "***a self-contained controller***", an "***AP***" that will "***defer all WLAN functions other than real-time services***" to the "***AC***" (for example, "***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***"), or an "***AP***" and "***AC***" combination that will also "***shift some normally real-time functions***" to the "***AC***", which is analogous to the disclosure of this process provided in Calhoun (see, for example, ¶¶ 322-323 above).

355. Thus, CAPWAP discloses an "***Access Point***" that is configured "**to dynamically negotiate with the control node for a secure connection and function split arrangement**" (for example, as shown during the "***Capability Negotiation Phase***" as described specifically above at least to "***authenticate***" by "***cryptographically secure binding***", to provide "***Configuration***" of "***parameters***", and to determine the "***applicable API's between AP and AC***" based upon "***capabilities negotiated by architectural type match***" using a "***negotiable interface protocol***").

356. See at least ¶¶ 241-263 above regarding the combination of Calhoun, LWAPP and CAPWAP.

357. 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.

358. 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 "**dynamically negotiat[ing] with the control node for a secure connection and function split arrangement**" and the proposed structure in the specification of the '531 Patent for performing such function as a "**negotiation unit for the single or plurality of WAPs**" 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 8:62-10:53 of the '531 Patent (see, for example, ¶¶ 58-68 above).

359. Under the alternative claim construction of ¶ 358 above, I note that Calhoun discloses identically the recited function of "**dynamically negotiat[ing] with the control node for a secure connection and function split arrangement**" as I have described herein (see, for example, ¶¶ 306-323 above).

360. Calhoun also discloses structure for a "**negotiation unit for the single or plurality of WAPs**" by at least the "***flow chart diagrams***" FIG. 3A and FIG. 3B of Calhoun as I have annotated herein (see, for example, ¶¶ 324-325 above).

361. Under the alternative claim construction of ¶ 358 above, I believe a POSITA would understand the "way" that the proposed structure in the specification of the '531 Patent would be deemed to perform the function of "**dynamically negotiat[ing] with the control node for a secure connection**" is by "*mutual authentication*" and "*exchanges of security information*" between a "*WAP controller*" and a "*chosen CN*", thereby leading to the "result" of "the *establishment of communication protocols* for further exchanges" (see, for example, ¶ 61 above).

362. Similarly, the "way" that the structure for a "**negotiation unit for the single or plurality of WAPs**" in Calhoun performs the function of "**dynamically negotiat[ing] with the control node for a secure connection**" is by "***digital certificate***" validation and "***cryptographic keys***" exchange between the "***access element***" and the "***central control element***" during the "***joinder phase***", thereby leading to the "result" of "***encrypting subsequent communications***" for the "***configuration phase***" (see, for example, ¶¶ 308-314 above).

363. In my opinion, a POSITA would understand that the "way" of such "***digital certificate***" validation and "***cryptographic keys***" exchange between the "***access element***" and the "***central control element***" during the "***joinder phase***" in Calhoun is substantially similar to the "way" of "*mutual authentication*" and "*exchanges of security information*" between a "*WAP*

controller" and a "*chosen CN*" in the '531 Patent, and that such "result" of "***encrypting subsequent communications***" for the "***configuration phase***" in Calhoun is substantially similar to the "result" of "the *establishment of communication protocols* for further exchanges" in the '531 Patent, or thus that the structure in Calhoun for performing the function of "**dynamically negotiat[ing] with the control node for a secure connection**" is at least equivalent to the proposed structure in the specification of the '531 Patent under the alternative claim construction of ¶ 358 above.

364. Additionally, under the alternative claim construction of ¶ 358 above, I believe a POSITA would understand that one exemplary "way" that the proposed structure in the specification of the '531 Patent would be deemed to perform the function of "**dynamically negotiat[ing] with the control node for a … function split arrangement**" 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).

365. Similarly, one exemplary "way" that the structure for a "**negotiation unit for the single or plurality of WAPs**" in Calhoun performs the function of "**dynamically negotiat[ing] with the control node for a … function split arrangement**" 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 if the "***access element***" is configured to "***bridge network traffic associated with the remote client elements directly, while transmitting management packets to the central control element***" instead of "***transmitting***" both "***data***" and "***management packets to the central control 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***" that "***can be shifted***" when "***operating in 802.11 wireless networks***" (see, for example, ¶¶ 318-323 above).

366. In my opinion, a POSITA would understand that the "way" of such "***configuration request***" that includes "***operational parameters***" and "***overriding parameters***" to describe the "***bridge network traffic***" functionality location between the "***access element***" and the "***central control element***" followed by such "***configuration response***" from the "***central control element***" that "***implements the operational parameters***" that set the "***bridge network traffic***" functionality location 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" from a "*WAP controller*" to a "*chosen CN*" which "*determines an initial division of WLAN functionality*" that is "*sent to the associated WAP*" in the '531 Patent, and that such "result" of realizing a "***division of functionality between the access elements and the central control elements***" that "***can be shifted***" 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 '531 Patent, or thus that the structure in Calhoun for performing the function of "**dynamically negotiat[ing] with the control node for a … function split arrangement**" is at least equivalent to the proposed structure in the specification of the '531 Patent under the alternative claim construction of ¶ 358 above.

367. Therefore, in my opinion, Calhoun discloses the limitations of this claim element under the alternative claim construction of ¶ 358 above.

368. See at least ¶¶ 241-263 above regarding the combination of Calhoun, LWAPP and CAPWAP.

369. Additionally, I note that per my analysis herein that CAPWAP discloses at least a "***negotiable interface protocol***" that determines the "***applicable API's between AP and AC***" based upon "***capabilities negotiated by architectural type match***" during a "***capabilities exchange phase***" for an "***Access Point***" and an "***Access Controller***" that is configured to "**dynamically negotiate with the control node for a … function split arrangement**" as recited for this claim element, thereby further informing a POSITA that the structure in Calhoun for performing the function of "**dynamically negotiat[ing] with the control node for a … function split arrangement**" when combined as noted herein to implement the various functional split architectures 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 '531 Patent under the alternative claim construction of ¶ 358 above.

370. 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 ¶ 358 above.

1(d) 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.

371. My analysis of Calhoun for claim element 1(c) above is also applicable for this claim element 1(d) (see, for example, ¶¶ 306-328 and 359-367 above).

372. For example, I have specifically noted and/or analyzed various aspects of the "***central control element***" of Calhoun in at least ¶¶ 308-309, 312, 314-316, 319-323, 326-327, 362 and 365 above, which I also incorporate herein.

373. Additionally, Calhoun discloses that "FIG. 4 provides a method, implemented by *central control elements*, supporting the *LWAPP functionality*" " (see, for example, ¶ 118 above, and annotated Figure 4 shown below).

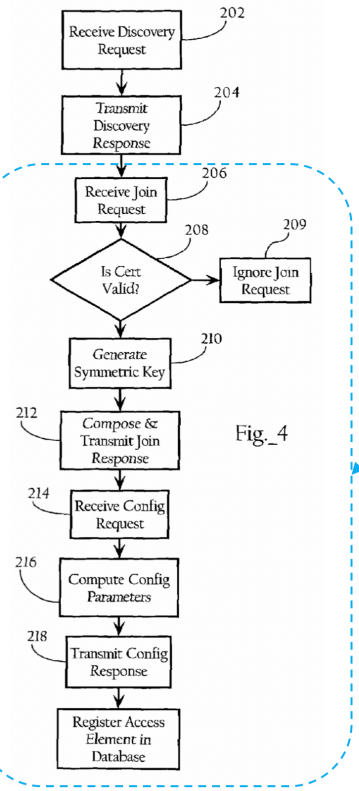


Fig. 4

Example showing that a "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"

374. Accordingly, a POSITA would understand that this "***Maximum Transmit Unit***" determination aspect of the "***joinder phase***" of Calhoun which follows the "***discovery phase***" as described above also discloses at least that the "***central control element***" of Calhoun is configured such that it "**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**" as recited for this claim element because "***to determine whether a wireless packet … can be encapsulated with additional headers and transmitted without requiring fragmentation***" using the process disclosed in Calhoun determines if "**to form a complete functionality defined for the wireless local area network**" between the "***access element***" and the "***central control element***" of Calhoun that such "***central control element***" needs to include or not include the functions of "***fragmentation***" (and hence

also "***defragmentation***") as "**complementary functionality for the single or plurality of each of the WAPs**" according to the "***Maximum Transmit Unit***" determination (or hence, "**a decision of the negotiation unit**").

375. Additionally, a POSITA would understand that either or both of this "***image version***" update aspect and this "***operational parameters***" exchange aspect of the "***configuration phase***" of Calhoun as described above also discloses at least that the "***central control element***" of Calhoun is configured such that it "**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**" as recited for this claim element because each such aspect involves "***dynamically configur[ing]***" the details of the partial WLAN functionality as implemented in the "***access element***" in order "**to form a complete functionality defined for the wireless local area network**" that includes the "**complementary functionality for the single or plurality of each of the WAPs**" within the "***central control element***" and at least since my analysis shows such "***image version***" update and "***operational parameters***" exchange comes about through the elements of Calhoun in FIG. 3A and FIG. 3B as shown above (or hence, "**a decision of the negotiation unit**").

376. Moreover, a POSITA would understand that Calhoun's disclosure to "***dynamically configure***" the "***elements***" of "***802.11 wireless networks***" also shows at least that the "***central control element***" of Calhoun is configured such that it "**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**" as recited for

this claim element because this "***division of functionality between the access elements and the central control elements can be shifted***" using the process disclosed in Calhoun determines if "**to form a complete functionality defined for the wireless local area network**" between the "***access element***" and the "***central control element***" of Calhoun that such "***central control element***" needs to include or not include either or both of the functions to "***bridge network traffic associated with the remote client elements***" or process "***management packets***" as "**complementary functionality for the single or plurality of each of the WAPs**" according to the described process to "***dynamically configure***" such "***access elements***" using the elements of Calhoun in FIG. 3A and FIG. 3B as shown above (or hence, "**a decision of the negotiation unit**").

377. Thus, Calhoun discloses "**whereby the control node negotiates with the single or plurality of WAPs using the negotiation unit**" (for example, the above annotated portion of FIG. 4 of Calhoun and its description as summarized above) and "**whereby the control node … 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**" (for example, as shown when the "***division of functionality***" for the "***access elements***" and the "***central control elements***" becomes "***dynamically configure[d]***" during the "***joinder and configuration phases of LWAPP***" as described specifically above for at least the "***Maximum Transmit Unit***" determination aspect of the "***joinder phase***", the "***image version***" update aspect and the "***operational parameters***" exchange aspects of the "***configuration phase***", and the "***bridge network traffic***" "***shift***" in "***division of functionality***" between "***access elements***" and the "***central control elements***" aspects of the "***configuration phase***") according to "**a decision of**

the negotiation unit" (for example, according to the above annotated portions of composite FIG. 3A and FIG. 3B of Calhoun and its description as summarized above).

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

379. My analysis of LWAPP for claim element 1(c) above is also applicable for this claim element 1(d) (see, for example, ¶¶ 329-342 above).

380. For example, I have specifically noted and/or analyzed various aspects of the "***Access Router***" of LWAPP in at least ¶¶ 330-331 and 335-337 above, which I also incorporate herein.

381. Accordingly, a POSITA would understand that this "***MTU discovery mechanism***" within the "***Join phase***" of LWAPP which follows the "***discovery phase***" as described above also discloses at least that the "***Access Router***" of LWAPP is configured such that it "**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**" as recited for this claim element because "***to determine whether there is support for the transport of jumbo frames between the AP and it's AR***" using the process disclosed in LWAPP determines if "**to form a complete functionality defined for the wireless local area network**" between the "***Access Point***" and the "***Access Router***" of LWAPP that such "***Access Router***" needs to include or not include the functions of "***fragmentation***" (and hence also "***defragmentation***") as "**complementary functionality for the single or plurality of each of the WAPs**" according to the "***MTU discovery mechanism***" determination (or hence, "**a decision of the negotiation unit**"), which is analogous to the disclosure of this process provided in Calhoun (see, for example, ¶ 374 above).

382. Additionally, a POSITA would understand that either or both of this "***firmware image***" update aspect and this "***provisioning***" exchange aspect of the "***configuration phase***" of LWAPP as described above also discloses at least that the "***Access Router***" of LWAPP is configured such that it "**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**" as recited for this claim element because each such aspect involves "***overrid [ing]***" the details of the partial WLAN functionality as implemented in the "***Access Point***" in order "**to form a complete functionality defined for the wireless local area network**" that includes the "**complementary functionality for the single or plurality of each of the WAPs**" within the "***Access Router***" and at least since my analysis shows such "***firmware image***" update and "***provisioning***" exchange comes about through application of the "***State Machine***" for LWAPP in Figure 3 as shown above (or hence, "**a decision of the negotiation unit**"), which is also analogous to the disclosure of this process provided in Calhoun (see, for example, ¶ 375 above).

383. Thus, LWAPP discloses "**whereby the control node negotiates with the single or plurality of WAPs using the negotiation unit**" (for example, the application of the "***State Machine***" at the "***Access Router***" for the above annotated portion of Figure 3 of LWAPP and its description as summarized above) and "**whereby the control node … 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**" (for example, during the "***Join phase***" of LWAPP and the "***configuration phase***" of LWAPP as described specifically above for at least the "***MTU discovery mechanism***" determination aspect and the "***firmware image***" update

and "***provisioning***" exchange) according to "**a decision of the negotiation unit**" (for example, according to the application of the "***State Machine***" at the "***Access Point***" for the above annotated portion of Figure 3 of LWAPP and its description as summarized above).

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

385. My analysis of Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA for claim element 1(c) above is also applicable for this claim element 1(d) (see, for example, ¶¶ 343-357 and 368-370 above).

386. For example, I have specifically noted and/or analyzed various aspects of the "***Access Controller***" or "***Access Router***" of CAPWAP in at least ¶¶ 343-347 and 351-353 above, which I also incorporate herein.

387. Accordingly, a POSITA would understand that this "***Configuration***" of "***parameters***" exchange aspect of the "***Capability Negotiation Phase***" of CAPWAP as described above also discloses at least that the "***Access Controller***" of CAPWAP is configured such that it "**negotiates with the single or plurality of WAPs … and provides complementary functionality for the single or plurality of each of the WAPs to form a complete functionality defined for the wireless local area network**" as recited (in part) for this claim element because such "***parameters***" set the details of the partial WLAN functionality as implemented in the "***Access Point***" as part of a "***Split AP***" with the "***Access Controller***" that "***moves much of the functions that would reside in a traditional access point (AP) to a centralized access router (AR)***", which is also analogous to the disclosure of this process provided in Calhoun (see, for example, ¶ 375 above).

388. Additionally, a POSITA would understand that the "***negotiable interface protocol***" of CAPWAP that determines the "***applicable API's between AP and AC***" based upon

"***capabilities negotiated by architectural type match***" during a "***capabilities exchange phase***" describes at least that the "***Access Controller***" of CAPWAP is configured such that it "**negotiates with the single or plurality of WAPs … and provides complementary functionality for the single or plurality of each of the WAPs to form a complete functionality defined for the wireless local area network**" as recited (in part) for this claim element because this "***Split AP***" can be any one of a "***classic AP***" with "***a self-contained controller***", an "***AP***" that will "***defer all WLAN functions other than real-time services***" to the "***AC***" (for example, "***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***"), or an "***AP***" and "***AC***" combination that will also "***shift some normally real-time functions***" to the "***AC***", which is analogous to the disclosure of this process provided in Calhoun (see, for example, ¶ 376 above).

389. Thus, CAPWAP discloses "**whereby the control node negotiates with the single or plurality of WAPs**" (for example, the application of the "***negotiable interface protocol***" of CAPWAP at the "***Access Controller***" and its description as summarized above) and "**whereby the control node … 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**" (for example, as shown during the "***Capability Negotiation Phase***" as described specifically above for the "***Access Controller***" at least to provide "***Configuration***" of "***parameters***", and to determine the "***applicable API's between AP and AC***" based upon "***capabilities negotiated by architectural type match***").

390. See at least ¶¶ 241-263 above regarding the combination of Calhoun, LWAPP and CAPWAP.

391. 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.

‘531 Patent: Claim 7

> 7. The system according to claim 1, wherein each of the WAPs further comprises:
> a discovering unit for discovering an available CN within a specified domain; and
> a secure connection negotiating unit for negotiating a secure connection with a CN that may provide the complementary functionality desired by the WAP;
> whereby the WAP locates the CN that provides the complementary functionality with regard to defined complete wireless local area network functions with the discovering unit and establishes a secure connection with the CN that provides the complementary functionality with the secure connection negotiating unit.

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

392. Per my analysis for Claim 1 as summarized above, Calhoun discloses the “**system according to claim 1**” including one or more “**WAPs**” within such “**system**”.

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

394. Per my analysis for Claim 1 as summarized above, Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA renders obvious the “**system according to claim 1**” including one or more “**WAPs**” within such “**system**”.

395. Therefore, in my opinion, Calhoun in view of LWAPP, CAPWAP and the knowledge of a POSITA renders obvious the additional limitations of this preamble claim element, if any.

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

396. 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*” (see, for example, ¶ 108 above).

397. Calhoun also 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, ¶¶ 113-114 above).

398. 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, ¶ 117 above).

399. Calhoun further explains that subsequently "*central control elements* **24**, **26** *receive the discovery requests* (**202**) and *transmit discovery responses* to access element **15** (**204**)" so that "*access element* **15** … *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*" (see, for example, ¶¶ 118 and 120 above).

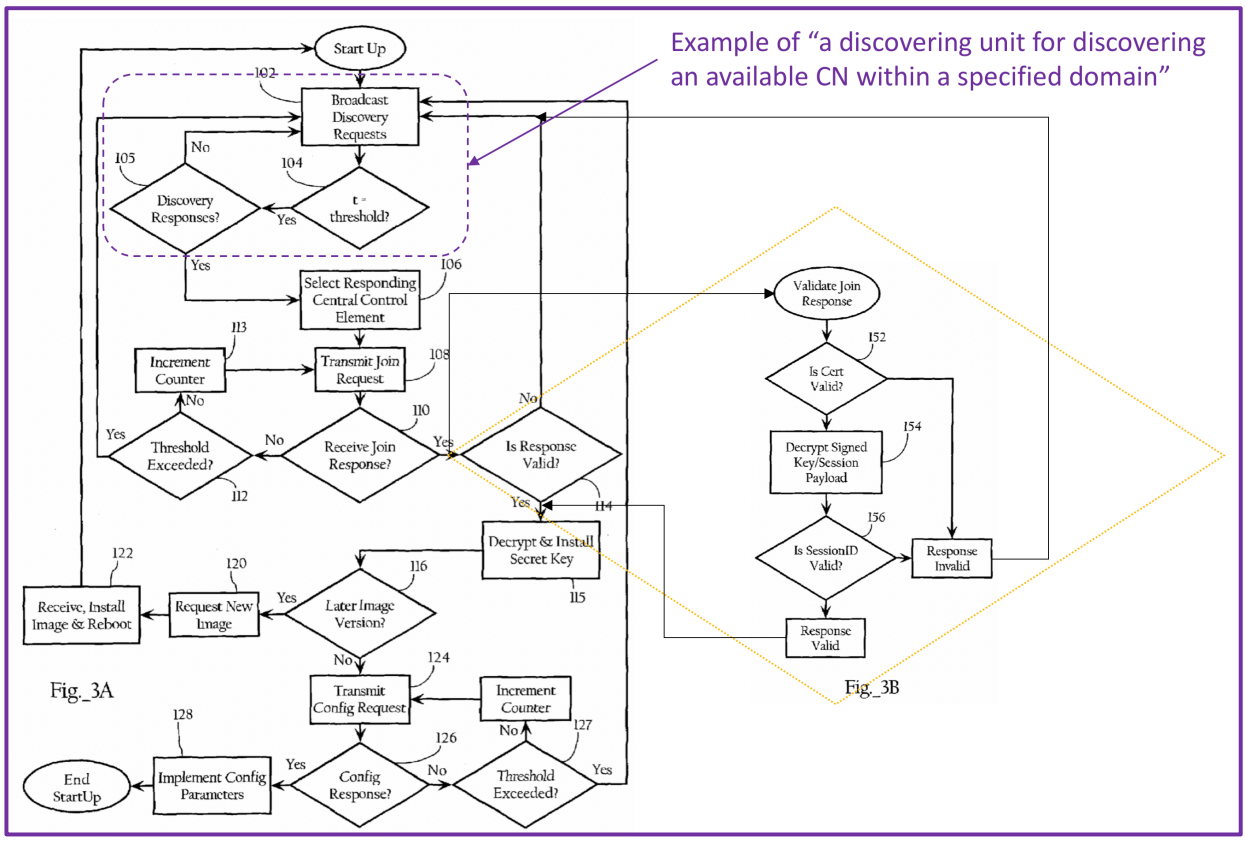
400. Accordingly, a POSITA would understand that this "***discovery request***" and "***discovery response***" exchange between the "***access element***" and the "***central control elements***" within the "***virtual subnet***" during the "***discovery phase***" of Calhoun as described above discloses at least that the "***access element***" of Calhoun is configured for "**discovering an available CN within a specified domain**" as recited for this claim element.

401. Calhoun discloses that "the *division of functionality between the access elements and the central control elements can be shifted*" (see, for example, ¶ 136 above).

402. As I noted herein for claim element 1(c) above, Calhoun also discloses that "***implementing the discovery, joinder and configuration phases of LWAPP***" by which the

"***division of functionality***" for the "***access elements***" and the "***central control elements***" becomes "***dynamically configure[d]***" is also shown by the "***flow chart diagrams***" FIG. 3A and FIG. 3B of Calhoun (see, for example, ¶¶ 116 and 127 above).

403. Accordingly, a POSITA would understand that Calhoun also discloses a "**discovering unit**" within each one of the "***access elements***" that is for "**discovering an available CN within a specified domain**" per the recited limitations of this claim element as shown by my annotated composite below for FIG. 3A and FIG. 3B of Calhoun:



404. Additionally, I note that my analysis for claim element 1(d) above also shows that the "***central control element***" of Calhoun, which the "***access element***" discovers within the "***virtual subnet***" during the "***discovery phase***", discloses at least a "**CN that provides the**

complementary functionality with regard to defined complete wireless local area network functions" (see, for example, ¶¶ 371-378 above).

405. Thus, Calhoun discloses a "**discovering unit**" that "**each of the WAPs further comprises**" (for example, the above annotated portions of composite FIG. 3A and FIG. 3B of Calhoun) that is for "**discovering an available CN within a specified domain**" whereby "**the WAP locates the CN … with the discovering unit**" (for example, as shown by the "***discovery request***" and "***discovery response***" exchange between the "***access element***" and the "***central control elements***" within the "***virtual subnet***" during the "***discovery phase***" of Calhoun), such "**CN**" being "**the CN that provides the complementary functionality with regard to defined complete wireless local area network functions**" (for example, the "***central control element***" of Calhoun as shown by my analysis for claim element 1(d) above).

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

407. 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*" (see, for example, ¶ 143 above).

408. 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, ¶¶ 155-156 above).

409. 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

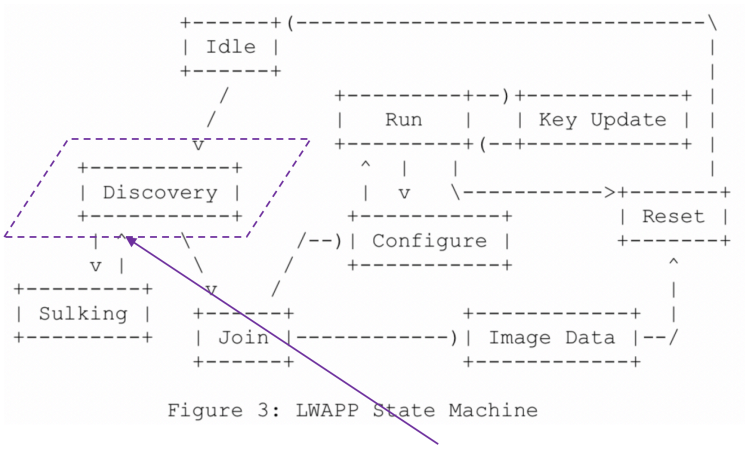
discovery request" wherein "The *Discovery Reply* carries the following *message elements*: *AR Payload*" and "*AR Name Payload*" (see, for example, ¶ 160 above).

410. 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*" (see, for example, ¶ 162 above).

411. 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, ¶ 172 above).

412. Accordingly, a POSITA would understand that this "***Discovery Request***" and "***Discovery Response***" exchange between the "***Access Point***" and the "***Access Controller***" within the "***specific Ethernet segment***" during the "***discovery phase***" of LWAPP as described above discloses at least that the "***Access Point***" of LWAPP is configured for "**discovering an available CN within a specified domain**" as recited for this claim element.

413. As I noted herein for claim element 1(c) above, LWAPP provides a "*state diagram*" that "represents the *lifecycle of an AP-AR session*" in Figure 3 (see, for example, ¶ 152 above), which, in my opinion, a POSITA would understand discloses a "**discovering unit**" within each "***Access Point***" that is for "**discovering an available CN within a specified domain**" per the recited limitations of this claim element as discussed above and shown by my annotated version of Figure 3 of LWAPP:



Example of "a discovering unit for discovering an available CN within a specified domain"

414. Additionally, I note that my analysis for claim element 1(d) above also shows that the "***Access Controller***" of LWAPP, which the "***Access Point***" discovers within the "***specific Ethernet segment***" during the "***discovery phase***", discloses at least a "**CN that provides the complementary functionality with regard to defined complete wireless local area network functions**" (see, for example, ¶¶ 379-384 above).

415. Thus, LWAPP discloses a "**discovering unit**" that "**each of the WAPs further comprises**" (for example, the above annotated portions of Figure 3 of LWAPP) that is for "**discovering an available CN within a specified domain**" whereby "**the WAP locates the CN … with the discovering unit**" (for example, as shown by the "***Discovery Request***" and "***Discovery Response***" exchange between the "***Access Point***" and the "***Access Controller***" within the "***specific Ethernet segment***" during the "***discovery phase***" of LWAPP), such "**CN**" being "**the CN that provides the complementary functionality with regard to defined complete wireless local area network functions**" (for example, the "***Access Controller***" of LWAPP as shown by my analysis for claim element 1(d) above).

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

417. CAPWAP discloses "*automatic discovery*" for "*AP's*" that are "*set up securely in the AC(AR)'s domain*" (see, for example, ¶ 207 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, ¶ 202 above).

418. CAPWAP further discloses that "*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" (see, for example, ¶ 213 above).

419. 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 as described above discloses at least that the "***Access Point***" of CAPWAP is configured for "**discovering an available CN within a specified domain**" as recited for this claim element.

420. See at least ¶¶ 241-263 above regarding the combination of Calhoun, LWAPP and CAPWAP.

421. 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.

422. 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 "**discovering an available CN within a specified domain**" and the proposed structure in the specification of the '531 Patent for performing such function as a "**discovering unit**" that "**each of the WAPs further comprises**" would be described by the "operational step" denoted as "**201**" in FIG. 2 as well as the applicable text in 8:43-51 of the '531 Patent (see, for example, ¶¶ 58-59 above).

423. Under the alternative claim construction of ¶ 422 above, I note that Calhoun discloses identically the recited function of "**discovering an available CN within a specified domain**" as I have described herein (see, for example, ¶¶ 396-400 above).

424. Calhoun also discloses structure for a "**discovering unit**" that "**each of the WAPs further comprises**" by at least the "***flow chart diagrams***" FIG. 3A and FIG. 3B of Calhoun as I have annotated herein (see, for example, ¶¶ 402-403 above).

425. Under the alternative claim construction of ¶ 422 above, I believe a POSITA would understand the "way" that the proposed structure in the specification of the '531 Patent would be deemed to perform the function of "**discovering an available CN within a specified domain**" is by "*any node discovery protocol* or by the *broadcast/multicast/anycast of a specific, mutually recognizable message* invoking responses from available CNs", thereby leading to the "result" of "*discovered CNs to associate with*" (see, for example, ¶¶ 59-60 above).

426. Similarly, the "way" that the structure for a "**discovering unit**" that "**each of the WAPs further comprises**" in Calhoun performs the function of "**discovering an available CN within a specified domain**" is by "***discovery request***" and "***discovery response***" exchange between the "***access element***" and the "***central control elements***" within the "***virtual subnet***"

during the "***discovery phase***", thereby leading to the "result" of "***responding central control elements identified in the discovery responses***" (see, for example, ¶¶ 396-399 above).

427. In my opinion, a POSITA would understand that the "way" of such "***discovery request***" and "***discovery response***" exchange between the "***access element***" and the "***central control elements***" within the "***virtual subnet***" 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* invoking responses from available CNs" in the '531 Patent, and that such "result" of "***responding central control elements identified in the discovery responses***" in Calhoun is substantially similar to the "result" of "*discovered CNs to associate with*" in the '531 Patent, or thus that the structure in Calhoun for performing the function of "**discovering an available CN within a specified domain**" is at least equivalent to the proposed structure in the specification of the '531 Patent under the alternative claim construction of ¶ 422 above.

428. Therefore, in my opinion, Calhoun discloses the limitations of this claim element under the alternative claim construction of ¶ 422 above.

429. Additionally, I note that per my analysis herein that CAPWAP discloses at least "***automatic discovery***" between the "***Access Point***" and the "***Access Controller***" or "***Access Router***" within the "***AC(AR)'s domain***", or hence the function of "**discovering an available CN within a specified domain**" as recited for this claim element, thereby further informing a POSITA that the structure in Calhoun for performing the function of "**discovering an available CN within a specified domain**" 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 '531 Patent under the alternative claim construction of ¶ 422 above.

430. 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 ¶ 422 above.

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

431. In my opinion, a POSITA would understand that the limitations of "**negotiating a secure connection with a CN that may provide the complementary functionality desired by the WAP**" and "**establish[ing] a secure connection with the CN that provides the complementary functionality**" for this claim element are substantially similar to limitations expressed in claim elements 1(c) and 1(d) above for Claim 1 from which this Claim 7 depends.

432. Additionally, in my opinion, a POSITA would understand that the fundamental differentiation of this claim element relative to Claim 1 from which this Claim 7 depends is that "**each of the WAPs further comprises**" the "**secure connection negotiating unit**" of this claim element, whereas in Claim 1 a "**negotiation unit**" could be comprised within "**each of the WAPs**" but could also be comprised within some other element of the claimed "**system**" and/or could be common for multiple such "**WAPs**".

433. However, in my analysis above for claim elements 1(c) and 1(d), including under the alternative claim construction of ¶ 358 above, I specifically considered the case where the "**negotiation unit**" is comprised within "**each of the WAPs**". Accordingly, my analysis of Calhoun, LWAPP, and CAPWAP for claim elements 1(c) and 1(d) above already applies to this claim element 7(b).

434. My analysis of Calhoun for claim elements 1(c) and 1(d) above is also applicable for this claim element 7(b) (see, for example, ¶¶ 306-328 and 371-378 above).

435. Thus, Calhoun discloses a "**secure connection negotiating unit**" that "**each of the WAPs further comprises**" (for example, the annotated portions of composite FIG. 3A and FIG. 3B for the "***access element***" of Calhoun as shown at ¶ 325 above) that is for "**negotiating a secure connection with a CN**" and/or for "**establish[ing] a secure connection with the CN**" (for example, by at least the "***digital certificate***" validation and "***cryptographic keys***" exchange aspect of the "***joinder phase***" of Calhoun), such "**CN**" being "**a CN that may provide the complementary functionality desired by the WAP**" and "**the CN that provides the complementary functionality**" (for example, as shown by the "***central control element***" of Calhoun when the "***division of functionality***" for the "***access elements***" and the "***central control elements***" becomes "***dynamically configure[d]***" during the "***joinder and configuration phases of LWAPP***" as described specifically above for at least the "***Maximum Transmit Unit***" determination aspect of the "***joinder phase***", the "***image version***" update aspect and the "***operational parameters***" exchange aspects of the "***configuration phase***", and the "***bridge network traffic***" "***shift***" in "***division of functionality***" between "***access elements***" and the "***central control elements***" aspects of the "***configuration phase***").

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

437. My analysis of LWAPP for claim elements 1(c) and 1(d) above is also applicable for this claim element 7(b) (see, for example, ¶¶ 329-342 and 379-384 above).

438. Thus, LWAPP discloses a "**secure connection negotiating unit**" that "**each of the WAPs further comprises**" (for example, the above annotated portions of Figure 3 for the "***Access Point***" of LWAPP as shown at ¶ 339 above) that is for "**negotiating a secure**

connection with a CN" and/or for "**establish[ing] a secure connection with the CN**" (for example, by at least the "***PKCS #5 certificate***" validation and "***public key cryptography***" exchange within the "***Join phase***" of LWAPP), such "**CN**" being "**a CN that may provide the complementary functionality desired by the WAP**" and "**the CN that provides the complementary functionality**" (for example, as shown by the "***Access Router***" of LWAPP as described specifically above for at least the "***MTU discovery mechanism***" determination aspect and the "***firmware image***" update and "***provisioning***" exchange).

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

440. My analysis of CAPWAP for claim elements 1(c) and 1(d) above is also applicable for this claim element 7(b) (see, for example, ¶¶ 343-357 and 385-390 above).

441. Thus, CAPWAP discloses an "***Access Point***" that is for "**negotiating a secure connection with a CN**" and/or for "**establish[ing] a secure connection with the CN**" (for example, as shown during the "***Capability Negotiation Phase***" as described specifically above at least to "***authenticate***" by "***cryptographically secure binding***"), such "**CN**" being "**a CN that may provide the complementary functionality desired by the WAP**" and "**the CN that provides the complementary functionality**" (for example, as shown by the "***Access Controller***" of CAPWAP that determines the "***applicable API's between AP and AC***" based upon "***capabilities negotiated by architectural type match***").

442. See at least ¶¶ 241-263 above regarding the combination of Calhoun, LWAPP and CAPWAP.

443. 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.

444. 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 functions would be "**negotiating a secure connection with a CN that may provide the complementary functionality desired by the WAP**" and "**establish[ing] a secure connection with the CN that provides the complementary functionality**" and the proposed structure in the specification of the '531 Patent for performing such functions as a "**secure connection negotiating unit**" that "**each of the WAPs further comprises**" 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 8:62-10:53 of the '531 Patent (see, for example, ¶¶ 58-68 above).

445. Under the alternative claim construction of ¶ 444 above, I note that Calhoun discloses identically the recited functions of "**negotiating a secure connection with a CN that may provide the complementary functionality desired by the WAP**" and "**establish[ing] a secure connection with the CN that provides the complementary functionality**" as I have described herein (see, for example, ¶¶ 434-436 above).

446. Calhoun also discloses structure for a "**secure connection negotiating unit**" that "**each of the WAPs further comprises**" by at least the "***flow chart diagrams***" FIG. 3A and FIG. 3B of Calhoun as I have annotated herein (see, for example, ¶¶ 324-325 above).

447. Under the alternative claim construction of ¶ 444 above, I believe a POSITA would understand the "way" that the proposed structure in the specification of the '531 Patent would be deemed to perform the functions of "**negotiating a secure connection with a CN …**"

and "**establish[ing] a secure connection with the CN …**" is by "*mutual authentication*" and "*exchanges of security information*" between a "*WAP controller*" and a "*chosen CN*", thereby leading to the "result" of "the *establishment of communication protocols* for further exchanges" (see, for example, ¶ 61 above).

448. Similarly, the "way" that the structure for a "**secure connection negotiating unit**" that "**each of the WAPs further comprises**" in Calhoun performs the functions of "**negotiating a secure connection with a CN …**" and "**establish[ing] a secure connection with the CN …**" is by "***digital certificate***" validation and "***cryptographic keys***" exchange between the "***access element***" and the "***central control element***" during the "***joinder phase***", thereby leading to the "result" of "***encrypting subsequent communications***" for the "***configuration phase***" (see, for example, ¶¶ 308-314 above).

449. In my opinion, a POSITA would understand that the "way" of such "***digital certificate***" validation and "***cryptographic keys***" exchange between the "***access element***" and the "***central control element***" during the "***joinder phase***" in Calhoun is substantially similar to the "way" of "*mutual authentication*" and "*exchanges of security information*" between a "*WAP controller*" and a "*chosen CN*" in the '531 Patent, and that such "result" of "***encrypting subsequent communications***" for the "***configuration phase***" in Calhoun is substantially similar to the "result" of "the *establishment of communication protocols* for further exchanges" in the '531 Patent, or thus that the structure in Calhoun for performing the functions of "**negotiating a secure connection with a CN …**" and "**establish[ing] a secure connection with the CN …**" is at least equivalent to the proposed structure in the specification of the '531 Patent under the alternative claim construction of ¶ 444 above.

450. Additionally, under the alternative claim construction of ¶ 444 above, I believe a POSITA would understand that one exemplary "way" that the proposed structure in the specification of the '531 Patent would be deemed to perform the functions of "**negotiating … with a CN that may provide the complementary functionality desired by the WAP**" and "**establish[ing] … with the CN that provides the complementary functionality**" 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).

451. Similarly, one exemplary "way" that the structure for a "**secure connection negotiating unit**" that "**each of the WAPs further comprises**" in Calhoun performs the functions of "**negotiating … with a CN that may provide the complementary functionality desired by the WAP**" and "**establish[ing] … with the CN that provides the complementary functionality**" 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 if the "***access element***" is configured to "***bridge network traffic associated with the remote client elements directly, while transmitting management packets to the central control element***" instead of "***transmitting***" both "***data***" and "***management packets to the central control 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***" that "***can be shifted***" when "***operating in 802.11 wireless networks***" (see, for example, ¶¶ 318-323 above).

452. In my opinion, a POSITA would understand that the "way" of such "***configuration request***" that includes "***operational parameters***" and "***overriding parameters***" to describe the "***bridge network traffic***" functionality location between the "***access element***" and the "***central control element***" followed by such "***configuration response***" from the "***central control element***" that "***implements the operational parameters***" that set the "***bridge network traffic***" functionality location 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*" from a "*WAP controller*" to a "*chosen CN*" which "*determines an initial division of WLAN functionality*" that is "*sent to the associated WAP*" in the '531 Patent, and that such "result" of realizing a "***division of functionality between the access elements and the central control elements***" that "***can be shifted***" 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 '531 Patent, or thus that the structure in Calhoun for performing the functions of "**negotiating … with a CN that may provide the complementary functionality desired by the WAP**" and "**establish[ing] … with the CN that provides the complementary functionality**" is at least equivalent to the proposed structure in the specification of the '531 Patent under the alternative claim construction of ¶ 444 above.

453. Therefore, in my opinion, Calhoun discloses the limitations of this claim element under the alternative claim construction of ¶ 444 above.

454. See at least ¶¶ 241-263 above regarding the combination of Calhoun, LWAPP and CAPWAP.

455. Additionally, I note that per my analysis herein that CAPWAP discloses at least a "***negotiable interface protocol***" that determines the "***applicable API's between AP and AC***" based upon "***capabilities negotiated by architectural type match***" during a "***capabilities exchange phase***" for an "***Access Point***" and an "***Access Controller***" that is for "**negotiating … with a CN that may provide the complementary functionality desired by the WAP**" and "**establish[ing] … with the CN that provides the complementary functionality**" as recited for this claim element, thereby further informing a POSITA that the structure in Calhoun for performing the functions of "**negotiating a secure connection with a CN that may provide the complementary functionality desired by the WAP**" and "**establish[ing] a secure connection with the CN that provides the complementary functionality**" when combined as noted herein to implement the various functional split architectures 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 '531 Patent under the alternative claim construction of ¶ 444 above.

456. 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 ¶ 444 above.

‘531 Patent: Claim 13

> 13. A method for providing service in a wireless local area network (WLAN) that allows a defined. WLAN function split between a wireless access point (WAP) and a single or plurality of Control Nodes (CN) comprising the steps in which:
>
> a subset of WAPs processes a total of a subset of functionality of the subset of WAPs defined for the WLAN;
>
> the WAP dynamically negotiates with a CN for a secure connection and function split arrangement; and
>
> the CN provides complementary functionality for each of the WAPs to form a complete functionality defined for the wireless local area network according to a decision in the negotiation step.

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

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

458. My analysis of Calhoun for the preamble of Claim 1 above is also applicable for this preamble of Claim 13 at least for the limitation of “**providing service in a wireless local area network (WLAN)**” (see, for example, ¶¶ 266-269 above).

459. Additionally, my analysis of Calhoun for claim elements 1(c) and 1(d) above is also applicable for this preamble of Claim 13 at least for the limitation of “**that allows a defined WLAN function split between a wireless access point (WAP) and a single or plurality of Control Nodes (CN)**” (see, for example, ¶¶ 306-328 and 371-378 above).

460. Thus, Calhoun discloses “**providing service**” (for example, with the “***wireless network system***” of Calhoun) that is “**in a wireless local area network**” (for example, a “***wireless Local Area Network (LAN)***” as also depicted in annotated FIG. 1 of Calhoun as shown at ¶ 267 above) that “**allows a defined WLAN function split between a wireless access point (WAP) and a single or plurality of Control Nodes (CN)**” (for example, by a “***division of functionality***” for one or more “***access elements***” and one or more “***central control elements***”).

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

462. My analysis of LWAPP for the preamble of Claim 1 above is also applicable for this preamble of Claim 13 at least for the limitation of "**providing service in a wireless local area network (WLAN)**" (see, for example, ¶¶ 270-272 above).

463. Additionally, my analysis of LWAPP for claim elements 1(c) and 1(d) above is also applicable for this preamble of Claim 13 at least for the limitation of "**that allows a defined WLAN function split between a wireless access point (WAP) and a single or plurality of Control Nodes (CN)**" (see, for example, ¶¶ 329-342 and 379-384 above).

464. Thus, LWAPP discloses a "**providing service**" (for example, with the "***wireless networks***" of LWAPP) that is "**in a wireless local area network**" (for example, a "***WLAN***" as also depicted in Figure 1 of LWAPP as shown at ¶ 270 above) that "**allows a defined WLAN function split between a wireless access point (WAP) and a single or plurality of Control Nodes (CN)**" (for example, by the "***Join phase***" of LWAPP and the "***configuration phase***" of LWAPP as described specifically above for at least the "***MTU discovery mechanism***" determination and the "***firmware image***" update and "***provisioning***" exchange).

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

466. My analysis of CAPWAP for the preamble of Claim 1 above is also applicable for this preamble of Claim 13 at least for the limitation of "**providing service in a wireless local area network (WLAN)**" (see, for example, ¶¶ 273-275 above).

467. Additionally, my analysis of CAPWAP for claim elements 1(c) and 1(d) above is also applicable for this preamble of Claim 13 at least for the limitation of "**that allows a defined WLAN function split between a wireless access point (WAP) and a single or plurality of Control Nodes (CN)**" (see, for example, ¶¶ 343-357 and 385-390 above).

468. Thus, CAPWAP discloses a "**system for providing service**" (for example, the "***communications architecture***" of CAPWAP) that is "**in a wireless local area network**" (for example, a "***WLAN***" as also depicted in Figure 1 of CAPWAP as shown at ¶ 273 above) that "**allows a defined WLAN function split between a wireless access point (WAP) and a single or plurality of Control Nodes (CN)**" (for example, by the "***applicable API's between AP and AC***" based upon "***capabilities negotiated by architectural type match***" using a "***negotiable interface protocol***").

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

470. See at least ¶¶ 241-263 above regarding the combination of Calhoun, LWAPP and CAPWAP.

471. 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.

13(a) a subset of WAPs processes a total of a subset of functionality of the subset of WAPs defined for the WLAN;

472. In my opinion, a POSITA would understand that the limitations of "**a subset of WAPs processes a total of a subset of functionality of the subset of WAPs defined for the WLAN**" for this claim element are substantially similar to limitations expressed in claim element 1(a) above for Claim 1.

473. Accordingly, my analysis of Calhoun, LWAPP, and CAPWAP for claim element 1(a) above already applies to this claim element 13(a).

474. My analysis of Calhoun for claim element 1(a) above is also applicable for this claim element 13(a) (see, for example, ¶¶ 278-282 above).

475. Thus, Calhoun discloses "**a subset of WAPs**" (for example, the "***managed access points***" or "***access elements***" of Calhoun) that "**processes a total of a subset of functionality of the subset of WAPs defined for the WLAN**" (for example, "***operating in 802.11 wireless networks***" according to "***IEEE 802.11a or 802.11b, etc.***" without "***perform[ing] link layer management functions, such as authentication and association***" per the disclosures of Calhoun).

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

477. My analysis of LWAPP for claim element 1(a) above is also applicable for this claim element 13(a) (see, for example, ¶¶ 283-286 above).

478. Thus, LWAPP discloses "**a subset of WAPs**" (for example, the "***simple***" or "***Light Weight***" "***Access Points***" or "***APs***" of LWAPP) that "**processes a total of a subset of functionality of the subset of WAPs defined for the WLAN**" (for example, operating "***in 802.11***" without performing the "***bridging, forwarding, authentication, encryption and policy enforcement functions for a WLAN***" per the disclosures of LWAPP).

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

480. My analysis of CAPWAP for claim element 1(a) above is also applicable for this claim element 13(a) (see, for example, ¶¶ 287-289 above).

481. Thus, CAPWAP discloses "**a subset of WAPs**" (for example, the "***lightweight Access Point (LAP)***" of CAPWAP) that "**processes a total of a subset of functionality of the subset of WAPs defined for the WLAN**" (for example, operating in "***802.11***" while performing the "***AP (Access Point) functions***" that are "***directly related to the real-time aspects of the 802.11 MAC protocol and those related to the radio nature of an 802.11 AP***" per the disclosures of CAPWAP).

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

483. See at least ¶¶ 241-263 above regarding the combination of Calhoun, LWAPP and CAPWAP.

484. 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.

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

485. In my opinion, a POSITA would understand that the limitations of "**the WAP dynamically negotiates with a CN for a secure connection and function split arrangement**" for this claim element are substantially similar to limitations expressed in claim element 1(c) above for Claim 1, subject to the additional limitations of claim element 7(b) as I discussed at ¶¶ 432-433 above and explained that I had already incorporated into my analysis of claim element 1(c).

486. Accordingly, my analysis of Calhoun, LWAPP, and CAPWAP for claim element 1(c) above already applies to this claim element 13(b).

487. My analysis of Calhoun for claim element 1(c) above is also applicable for this claim element 13(b) (see, for example, ¶¶ 306-328 above).

488. Thus, Calhoun discloses that "**the WAP**" (for example, the annotated portions of composite FIG. 3A and FIG. 3B for the "***access element***" of Calhoun as shown at ¶ 325 above) "**dynamically negotiates with a CN for a secure connection and function split arrangement**" (for example, as shown when the "***division of functionality***" for the "***access elements***" and the "***central control elements***" becomes "***dynamically configure[d]***" during the "***joinder and***

configuration phases of LWAPP" as described specifically above for at least the "***digital certificate***" validation and "***cryptographic keys***" exchange aspect of the "***joinder phase***", the "***Maximum Transmit Unit***" determination aspect of the "***joinder phase***", the "***image version***" update aspect and the "***operational parameters***" exchange aspects of the "***configuration phase***", and the "***bridge network traffic***" "***shift***" in "***division of functionality***" between "***access elements***" and the "***central control elements***" aspects of the "***configuration phase***").

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

490. My analysis of LWAPP for claim element 1(c) above is also applicable for this claim element 13(b) (see, for example, ¶¶ 329-342 above).

491. Thus, LWAPP discloses that "**the WAP**" (for example, the above annotated portions of Figure 3 for the "***Access Point***" of LWAPP as shown at ¶ 339 above) "**dynamically negotiates with a CN for a secure connection and function split arrangement**" (for example, as shown during the "***join and configuration phases of LWAPP***" as described specifically above for at least the "***PKCS #5 certificate***" validation and "***public key cryptography***" exchange within the "***Join phase***", the "***MTU discovery mechanism***" within the "***Join phase***", and the "***firmware image***" update aspect and this "***provisioning***" exchange aspect of the "***configuration phase***").

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

493. My analysis of CAPWAP for claim element 1(c) above is also applicable for this claim element 13(b) (see, for example, ¶¶ 343-357 above).

494. Thus, CAPWAP discloses that "**the WAP**" (for example, the "***Access Point***" of CAPWAP) "**dynamically negotiates with a CN for a secure connection and function split arrangement**" (for example, as shown during the "***Capability Negotiation Phase***" as described specifically above at least to "***authenticate***" by "***cryptographically secure binding***", to provide

"***Configuration***" of "***parameters***", and to determine the "***applicable API's between AP and AC***" based upon "***capabilities negotiated by architectural type match***" using a "***negotiable interface protocol***").

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

496. See at least ¶¶ 241-263 above regarding the combination of Calhoun, LWAPP and CAPWAP.

497. 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.

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

498. In my opinion, a POSITA would understand that the limitations of "**the CN provides complementary functionality for each of the WAPs to form a complete functionality defined for the wireless local area network according to a decision in the negotiation step**" for this claim element are substantially similar to limitations expressed in claim element 1(d) above for Claim 1.

499. Accordingly, my analysis of Calhoun, LWAPP, and CAPWAP for claim element 1(d) above already applies to this claim element 13(c).

500. My analysis of Calhoun for claim element 1(d) above is also applicable for this claim element 13(c) (see, for example, ¶¶ 371-378 above).

501. Thus, Calhoun discloses "**the CN**" (for example, the above annotated portion of FIG. 4 for the "***central control element***" of Calhoun as shown at ¶ 373 above) "**provides complementary functionality for each of the WAPs to form a complete functionality**

defined for the wireless local area network" (for example, as shown when the "***division of functionality***" for the "***access elements***" and the "***central control elements***" becomes "***dynamically configure[d]***" during the "***joinder and configuration phases of LWAPP***" as described specifically above for at least the "***Maximum Transmit Unit***" determination aspect of the "***joinder phase***", the "***image version***" update aspect and the "***operational parameters***" exchange aspects of the "***configuration phase***", and the "***bridge network traffic***" "***shift***" in "***division of functionality***" between "***access elements***" and the "***central control elements***" aspects of the "***configuration phase***") according to "**a decision in the negotiation step**" (for example, according to the annotated portions of composite FIG. 3A and FIG. 3B of Calhoun as shown at ¶ 325 above).

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

503. My analysis of LWAPP for claim element 1(d) above is also applicable for this claim element 13(c) (see, for example, ¶¶ 379-384 above).

504. Thus, LWAPP discloses "**the CN**" (for example, the "***Access Router***" of LWAPP) "**provides complementary functionality for each of the WAPs to form a complete functionality defined for the wireless local area network**" (for example, as shown during the "***Join phase***" of LWAPP and the "***configuration phase***" of LWAPP as described specifically above for at least the "***MTU discovery mechanism***" determination aspect and the "***firmware image***" update and "***provisioning***" exchange) according to "**a decision in the negotiation step**" (for example, according to the application of the "***State Machine***" at the "***Access Point***" for the annotated portion of Figure 3 of LWAPP as shown at ¶ 339 above).

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

506. My analysis of CAPWAP for claim element 1(d) above is also applicable for this claim element 13(c) (see, for example, ¶¶ 385-391 above).

507. Thus, CAPWAP discloses "**the CN**" (for example, the "***Access Controller***" of CAPWAP) "**provides complementary functionality for each of the WAPs to form a complete functionality defined for the wireless local area network**" (for example, as shown during the "***Capability Negotiation Phase***" as described specifically above for the "***Access Controller***" at least to provide "***Configuration***" of "***parameters***", and to determine the "***applicable API's between AP and AC***" based upon "***capabilities negotiated by architectural type match***").

508. See at least ¶¶ 241-263 above regarding the combination of Calhoun, LWAPP and CAPWAP.

509. 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.

IX. CONCLUSION

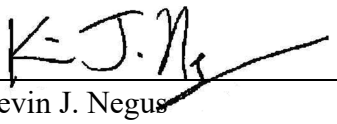
510. In my opinion, the claims of the '531 Patent are invalid for at least the reasons stated above.

511. 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.

512. 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,

Date: July 31, 2023



Kevin J. Negus