

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD.
and
SAMSUNG ELECTRONICS AMERICA, INC.,
PETITIONER,

v.

SECURE WI-FI LLC,

PATENT OWNER.

U.S. PATENT NO. 10,694,384
ISSUED: JUNE 23, 2020

ENTITLED: SCHEMES FOR CONNECTING TO WIRELESS NETWORK

Inter Partes Review No.: IPR2024-01367

PETITION FOR *INTER PARTES* REVIEW

TABLE OF CONTENTS

	Page
I. Mandatory Notices.....	1
A. Real Parties-In-Interest Pursuant to 37 C.F.R. § 42.8(b)(1).....	1
B. Related Matters Pursuant to 37 C.F.R. § 42.8(b)(2)	1
C. Lead and Back-Up Counsel Pursuant to 37 C.F.R. § 42.8(b)(3)	2
D. Service Information Pursuant to 37 C.F.R. § 42.8(b)(4).....	2
E. Payment of Fees under 37 C.F.R. §§ 42.15(a) and 42.103.....	3
II. Grounds for Standing.....	3
III. Introduction	4
IV. The '384 Patent.....	6
A. Summary of the Disclosure	6
B. Prosecution History.....	9
C. Level of Ordinary Skill in the Art	10
V. Claim Construction	10
VI. Prior Art and Grounds for Relief.....	11
A. Printed Publications Relied Upon for Grounds of Invalidity	11
1. <i>Vardi</i> (US8,126,476).....	11
2. <i>Yun</i> (WO2007/086705).....	12
3. <i>IEEE802.11</i> (IEEE 802.11 Standard TM - 2012)	14
4. <i>Satish</i> (US7,885,639).....	16
5. <i>Jalfon</i> (US2012/0076072).....	17
B. Relief Requested and Statutory Grounds of Invalidity	17
VII. Ground 1: <i>Vardi-IEEE802.11-Yun</i>	18
A. Motivation to Combine	18
B. Invalidity of Claims 1-24	22
1. Claim 1:.....	22
2. Claim 9:.....	41

3.	Claim 2:	45
4.	Claims 3 and 10:	46
5.	Claims 4 and 11:	46
6.	Claims 5 and 16:	47
7.	Claim 6:	47
8.	Claims 7 and 15:	51
9.	Claim 8:	51
10.	Claim 12:	52
11.	Claim 13:	52
12.	Claim 14:	53
13.	Claim 17:	55
14.	Claim 18:	59
15.	Claim 19:	59
16.	Claim 20:	60
17.	Claim 21:	60
18.	Claim 22:	61
19.	Claim 23:	61
20.	Claim 24:	62
VIII.	Ground 2: <i>Vardi-Yun-IEEE802.11-Satish</i>	62
A.	Motivation to Combine	62
B.	Invalidity of Claims 17-24	64
1.	Claim 17:	64
2.	Claim 18:	68
3.	Claim 19:	68
4.	Claim 20:	68
5.	Claim 21:	68
6.	Claim 22:	69
7.	Claim 23:	69
8.	Claim 24:	69

IX.	Ground 3: <i>Vardi-IEEE802.11-Jalfon</i>	69
A.	Motivation to Combine <i>Vardi-IEEE802.11-Jalfon</i>	69
B.	Invalidity of Claims 1-24	73
1.	Claim 1:	73
2.	Claim 9:	77
3.	Claim 2:	79
4.	Claims 3 and 10:	79
5.	Claims 4 and 11:	79
6.	Claims 5 and 16:	80
7.	Claim 6:	80
8.	Claims 7 and 15:	81
9.	Claim 8:	81
10.	Claim 12:	81
11.	Claim 13:	81
12.	Claim 14:	81
13.	Claim 17:	81
14.	Claim 18:	88
15.	Claim 19:	88
16.	Claim 20:	88
17.	Claim 21:	89
18.	Claim 22:	90
19.	Claim 23:	91
20.	Claim 24:	91
X.	No Discretionary Denial Is Warranted	91
A.	<i>Fintiv</i> Factors	91
B.	<i>Becton Dickinson</i> – Not the Same or Substantially the Same Art	93
XI.	Conclusion	95

TABLE OF AUTHORITIES

Page(s)

Cases

<i>Comm’ns Techs., Inc. v. Samsung Elecs. Am., Inc.</i> , No. 2:21-cv-00444-JRG (E.D. Tex. Feb. 2, 2023).....	92
<i>KSR Int’l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007).....	18, 69
<i>Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.</i> , 868 F.3d 1013 (Fed. Cir. 2017).....	10

LISTING OF EXHIBITS

<u>Exhibit No.</u>	<u>Exhibit Title</u>
Exhibit 1001	U.S. Patent 10,694,384, filed Mar. 30, 2018
Exhibit 1002	Declaration of Dr. Harry Bims
Exhibit 1003	Prosecution File History for U.S. Patent 10,694,384
Exhibit 1004	WO 2007/086705 (Yun), filed January 26, 2007
Exhibit 1005	[Reserved]
Exhibit 1006	US Application Publication 2012/0076072 (Jalfon), filed September 24, 2010
Exhibit 1007	U.S. Patent 8,126,476 (Vardi), filed July 25, 2008
Exhibit 1008	[Reserved]
Exhibit 1009	IEEE Std 802.11TM-2012 (<i>IEEE802.11</i>), dated March 29, 2012
Exhibit 1010	[Reserved]
Exhibit 1011	Infringement Contentions for U.S. Patent 10,694,384
Exhibit 1012	U.S. Patent 7,885,639 (Satish), filed June 29, 2006
Exhibit 1013	[Reserved]
Exhibit 1014	Prosecution File History for U.S. Patent 9,717,005
Exhibit 1015	Merriam-Webster's Collegiate Dictionary, 10 th Edition, 1999 (Excerpts)

CLAIM LISTING

Element Designation	Claim Language
Claim 1	
1[pre]	A method performed under control of an end device, the method comprising:
1[a]	generating, by the end device, a fake media access control (MAC) address for the end device;
1[b]	transmitting, by the end device to an access point, a probe request that includes the fake MAC address;
1[c]	receiving, by the end device from the access point, a probe response that includes information regarding the access point;
1[d]	determining, by the end device, that the access point is an authenticated access point based, at least in part, on the information in the probe response being indicative that the access point was connected with the end device previous to when the access point received the probe request transmitted by the end device; and
1[e]	transmitting, by the end device to the access point determined to be the authenticated access point, a connection request that includes an authentic device identifier for the end device.
Claim 2	
Claim 2	The method of claim 1, wherein the fake MAC address is distinct from an actual original MAC address of a hardware network interface of the end device.
Claim 3	
Claim 3	The method of claim 1, wherein information in the probe request is insufficient to identify the end device, so as to prevent leakage of present location information of the end device to non-authenticated access points.
Claim 4	
Claim 4	The method of claim 1, wherein generating the fake MAC address includes generating the fake MAC address from one or more characters that are selected randomly.
Claim 5	
Claim 5	The method of claim 1, wherein the authentic device identifier for the end device includes an authentic MAC address for a hardware network interface of the end device.

Claim 6	
6[pre]	The method of claim 1, further comprising:
6[a]	receiving, by the end device from the access point, an approval of the connection request; and
6[b]	connecting, by the end device, to a wireless local area network provided by the access point.
Claim 7	
Claim 7	The method of claim 6, wherein the access point includes a Wi-Fi access point, and wherein the wireless local area network includes a Wi-Fi network.
Claim 8	
8[pre]	The method of claim 1, further comprising:
8[a]	receiving, by the end device, a list of authenticated access points that includes information regarding one or more access points,
8[b]	wherein determining that the access point is the authenticated access point is further based on determining that the access point is included in the list of authenticated access points.
Claim 9	
9[pre]	A method performed by an end device, the method comprising:
9[a]	obtaining, by the end device, an authenticated access point list that includes information regarding one or more access points;
9[b]	generating, by the end device, a media access control (MAC) address for the end device that is distinct from an actual MAC address for a hardware network interface of the end device;
9[c]	transmitting, by the end device to at least one access point, a probe request that includes the generated MAC address;
9[d]	receiving, by the end device from the at least one access point in response to the probe request, a probe response that includes information regarding the at least one access point;
9[e]	determining, by the end device based at least, in part, on the information regarding the at least one access point, that the at least one access point is an authenticated access point,
9[f]	wherein determining that the at least one access point is the authenticated access point includes determining that the information regarding the at least one access point is included in the authenticated access point list; and

9[g]	transmitting, by the end device to the at least one access point after determining that the at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the end device.
Claim 10	
Claim 10	The method of claim 9, wherein information in the probe request is insufficient to identify the end device, so as to prevent leakage of present location information of the end device to non-authenticated access points.
Claim 11	
Claim 11	The method of claim 9, wherein generating the MAC address includes generating the MAC address from one or more characters that are selected randomly.
Claim 12	
Claim 12	The method of claim 9, wherein the information regarding the one or more access points includes at least one of a MAC address of each of the one or more access points, or a service set identifier (SSID) of each of the one or more access points.
Claim 13	
Claim 13	The method of claim 9, wherein determining that the at least one access point is the authenticated access point further includes determining that the at least one access point is the authenticated access point if the end device was previously-connected to the at least one access point.
Claim 14	
Claim 14	The method of claim 9, further comprising: receiving, by the end device from the at least one access point, an approval of the connection request; transmitting, by the end device to the at least one access point after receiving the approval of the connection request, an association request; receiving, by the end device from the at least one access point, an association response to the association request; and connecting to a communication network via the at least one access point in accordance with the association response.
Claim 15	
Claim 15	The method of claim 14, wherein the at least one access point includes a Wi-Fi access point, and wherein the communication network includes a Wi-Fi network that is accessible through the Wi-Fi access point.

Claim 16	
Claim 16	The method of claim 9, wherein the authentic device identifier for the end device includes the actual MAC address for the hardware network interface of the end device.
Claim 17	
17[pre]	An end device, comprising:
17[a]	a hardware network interface associated with an actual media access control (MAC) address;
17[b]	a processor coupled to the hardware network interface and operable to generate a MAC address for the end device that is distinct from the actual MAC address;
17[c]	a transmitter coupled to the processor and operable to transmit to an access point, a probe request that includes the generated MAC address; and
17[d]	a receiver coupled to the processor and operable to receive, from the access point, a probe response that includes information regarding the access point,
17[e]	wherein the processor is further operable to determine that the access point is an authenticated access point based, at least in part, on the information regarding the access point being indicative that the access point was connected with the end device previous to when the access point received the probe request transmitted from the transmitter, and
17[f]	wherein the hardware network interface is operable to connect, in response to determination that the access point is the authenticated access point, the end device to a wireless local area network provided by the access point.
Claim 18	
Claim 18	The end device of claim 17, wherein the access point includes a Wi-Fi access point, and wherein the wireless local area network includes a Wi-Fi network.
Claim 19	
Claim 19	The end device of claim 17, wherein the processor is operable to generate the MAC address from one or more characters that are selected randomly.

Claim 20	
20[pre]	The end device of claim 17, wherein:
20[a]	the transmitter is further operable to transmit, to the access point in response to the determination that the access point is the authenticated access point, a connection request that includes an authentic device identifier for the end device,
20[b]	The receiver is further operable to receive, from the access point, an approval of the connection request, and
20[c]	The hardware network interface is operable to connect the end device to the wireless local area network after the receiver receives the approval of the connection request.
Claim 21	
Claim 21	The end device of claim 20, wherein the authentic device identifier for the end device includes the actual MAC address.
Claim 22	
Claim 22	The end device of claim 17, further comprising a memory coupled to the processor and operable to store a list of authenticated access points that includes the information regarding the access point, wherein the information regarding the access point includes at least one of a MAC address of the access point, or a service set identifier (SSID) of the access point.
Claim 23	
Claim 23	The end device of claim 17, wherein the end device includes one of a cell phone, a personal data assistant (PDA), a personal media player device, a wireless web-watch device, a personal headset device, an application specific device, or a hybrid device.
Claim 24	
Claim 24	The end device of claim 17, wherein information in the probe request is insufficient to identify the end device, so as to prevent leakage of present location information of the end device to non-authenticated access points.

I. MANDATORY NOTICES

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

Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (collectively, “Petitioner”) are the real parties-in-interest.

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

Secure Wi-Fi LLC (“PO”) filed a complaint alleging infringement of U.S. Patents 10,694,384 (the “’384 Patent”), 9,961,552 (the “’552 Patent”), and 9,971,005 (the “’005 Patent”) (collectively, the “Texas Asserted Patents”) against Petitioner on January 25, 2024. That matter, *Secure Wi-Fi LLC v. Samsung Elecs. Co. Ltd. et al.*, No. 2:24-cv-00047-JRG in the Eastern District of Texas (the “Texas Action”), is currently pending. The Texas Action may affect, or be affected by, a decision in this proceeding.

The Texas Asserted Patents are a family of patents sharing a specification. Petitioner is concurrently petitioning for *inter partes* review against the ’005 Patent and ’552 Patents in the following matters:

- IPR2024-01366 – ’005 Patent, Claims 1-17;
- IPR2024-01368 – ’552 Patent, Claims 1-9; and
- IPR2024-01369 – ’552 Patent, Claims 10-28.

Decisions in the ’552 and ’005 Patents’ *inter partes* review proceedings may affect, or be affected by, a decision in this proceeding.

Currently, there are no other judicial or administrative matters that would affect, or be affected by, a decision in this proceeding.

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

Petitioner identifies Walter D. Davis, Jr. (Reg. No. 45,137) as Lead Counsel and Dipu A. Doshi (Reg. No. 60,073), Jonathan W.S. England (Reg. No. 71,223), Sean D. Damon (*pro hac* forthcoming), and Arun Paradkar (Reg. No. 72,236) as Backup Counsel. Pursuant to 37 C.F.R. § 42.10(b), a Power of Attorney accompanies this Petition.

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

Petitioner identifies the following contact information of counsel in this proceeding.

Lead Counsel	
Walter D. Davis, Jr., (Reg. No. 45,137) BLANK ROME LLP 1825 Eye Street NW Washington, D.C. 20006 Telephone: (202) 420-4847 Facsimile: (202) 478-0914 Email: walter.davis@blankrome.com	
Backup Counsel	Backup Counsel
Dipu A. Doshi (Reg. No. 60,073) Telephone: (202) 420-2604 Facsimile: (202) 420-2201 Email: dipu.doshi@blankrome.com	Sean D. Damon (<i>pro hac</i> to be filed) Telephone: (202) 420-4879 Facsimile: (202) 379-9380 Email: sean.damon@blankrome.com
Jonathan W.S. England (Reg. No. 71,223) Telephone: (202) 420-2747 Facsimile: (202) 420-2201	Arun Paradkar (Reg. No. 72,236) Telephone: (202) 772-5849 Facsimile: (202) 572-8439

Email: jonathan.england@blankrome.com BLANK ROME LLP 1825 Eye Street NW Washington, D.C. 20006	Email: arun.paradkar@blankrome.com BLANK ROME LLP 1825 Eye Street NW Washington, D.C. 20006
---	--

Petitioner agrees to electronic service at the following email address:

Email: samsung-swf-ipsr@blankrome.com

E. Payment of Fees under 37 C.F.R. §§ 42.15(a) and 42.103

The required fees are submitted herewith. If additional fees are owed during this proceeding, the PTO is authorized to charge Deposit Account No. [23-2185].

II. GROUNDS FOR STANDING

Pursuant to 37 C.F.R. § 42.104(a), Petitioner certifies that the '384 Patent is available for *inter partes* review. Petitioner is not barred or estopped from requesting *inter partes* review challenging the patent claims on the grounds set forth herein.

III. INTRODUCTION

The '384 Patent discloses a known problem solved in a known manner associated with connecting mobile devices wirelessly to networks through access points (“AP”) according to the available Institute of Electrical Engineers (“IEEE”) telecommunications and information exchange wireless local area network standard (IEEE Std 802.11TM-2012) (“*IEEE802.11*”) (EX1009).

As shown in the annotated figures below, the '384 Patent (left) simply builds on *IEEE802.11* (right) connection procedures.

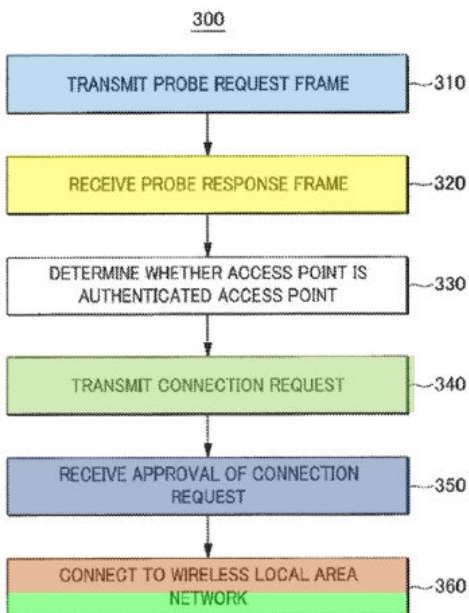


FIG. 3

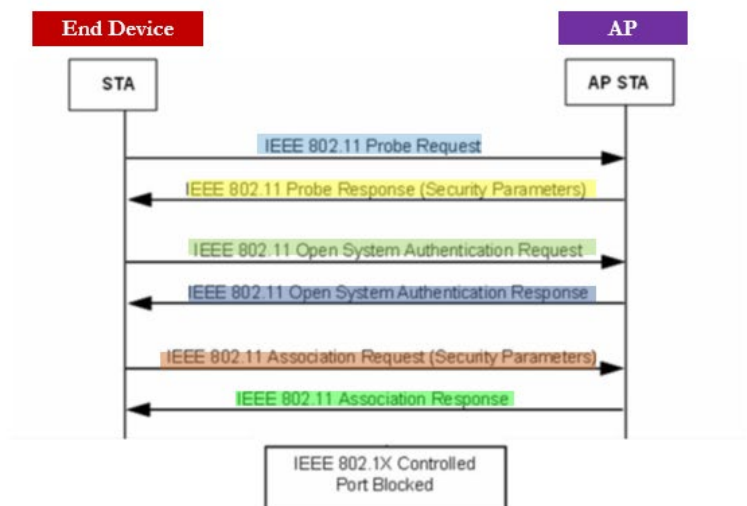


Figure 4-17—Establishing the IEEE 802.11 association

The '384 Patent identifies two alleged problems with the *IEEE802.11* process.

First, *IEEE802.11* defines a probe request, which includes unique identifying information of the end device, specifically, the media address control (“MAC”)

address, sent to all proximal APs to identify available APs for connection. Thus, undesired APs receive the unique MAC address and can use the information to potentially identify the end device based on that MAC address and proximity to the AP.

Second, *IEEE802.11* does not define selection criteria for choosing an AP for connection among the available APs. But it was known that malicious APs sought to intercept connections to obtain data sent over the network.

To solve the '384 Patent's identified problems, the '384 Patent identified two solutions, but those solutions were already known:

First, the '384 Patent modifies the probe request defined in *IEEE802.11* to include a fake MAC address instead of the authentic MAC address. However, this solution was already known in the industry; International Patent WO 2007/086705 ("Yun") (EX1004) substitutes an arbitrary MAC address in a probe request *instead of* the actual MAC address. Similarly, U.S. Patent Publication 2012/0076072 ("Jalfon") (EX1006) includes a random MAC address *instead of* the allocated MAC address of the end device in the probe request.

Second, the '384 Patent describes a method on selecting APs for connection by determining the AP was previously connected to the end device by simply matching the AP information ("API") received in a probe response to API stored on the device of previously-connected APs. Selecting APs for connection based on

prior successful connections was known and disclosed in, for example, U.S. Patent 8,126,476 (“*Vardi*”) (EX1007), which teaches scanning for APs according to *IEEE802.11* and selecting an AP for connection based on prior connection between the AP and the end device.

IV. THE ’384 PATENT

A. Summary of the Disclosure

The ’384 Patent describes secured wireless network communications between an end device and a network through a wireless AP. *Id.*, 3:1-4. End device (130) and method (300) are shown in Figs. 3 and 4 (below).

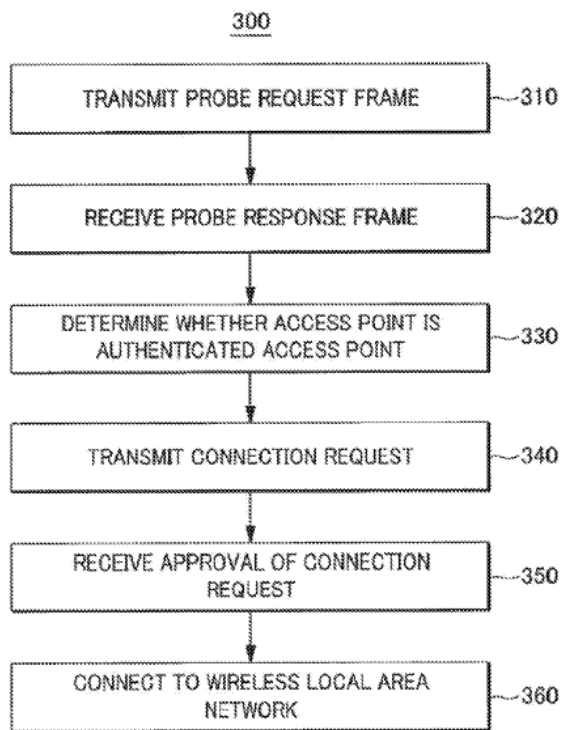


FIG. 3

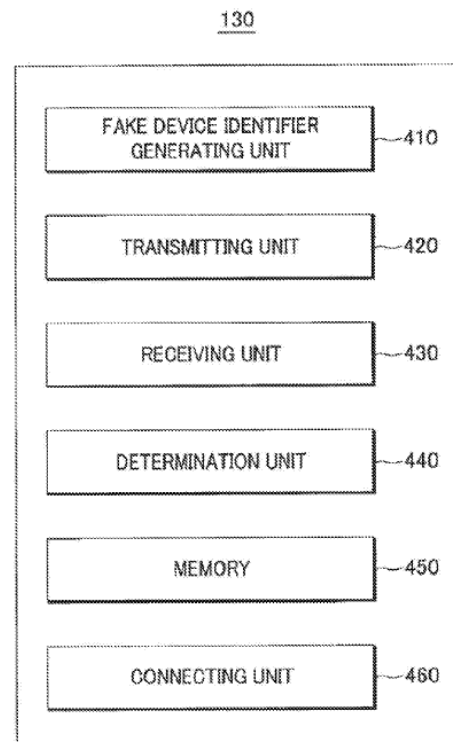


FIG. 4

The process (annotated below—left) aligns with the connection process defined in *IEEE802.11* (annotated below—right). EX1001, Fig. 3; EX1009, 182 (Fig. 4-17). Each process step except (330) correlates to *IEEE802.11*'s defined connection procedures.

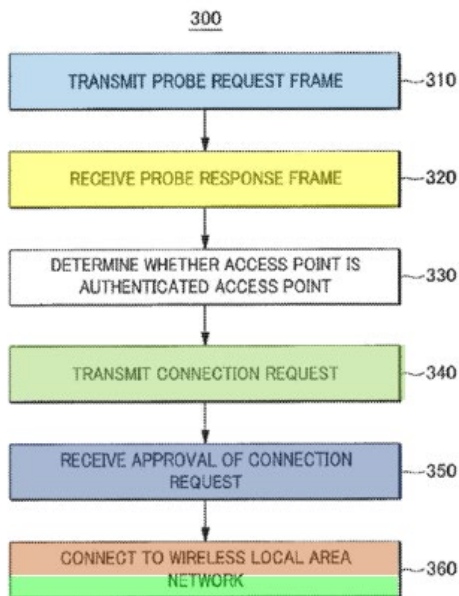


FIG. 3

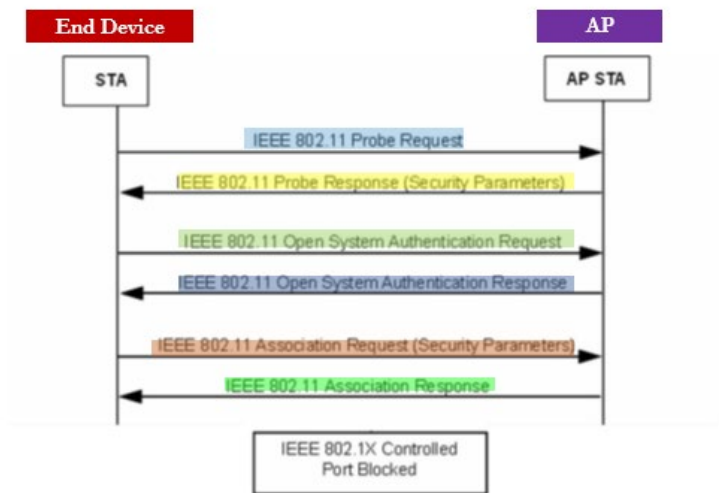


Figure 4-17—Establishing the IEEE 802.11 association

The end device transmits a probe request frame (310) to all proximate APs. EX1001, 3:8-17, 5:19-22; EX1009, 182 (Fig. 4-17). Previously, probe requests included authentic MAC addresses for the end device. *Id.*, 3:15-17. However, by using the authentic MAC address in the probe request, present location information could be exposed to undesired APs. *Id.*, 3:17-23.

Instead, the '384 Patent generates and includes a fake device identifier (fake MAC address) instead of the authentic device identifier in the probe request. EX1001, 3:24-27, 4:4-16, 5:19-22.

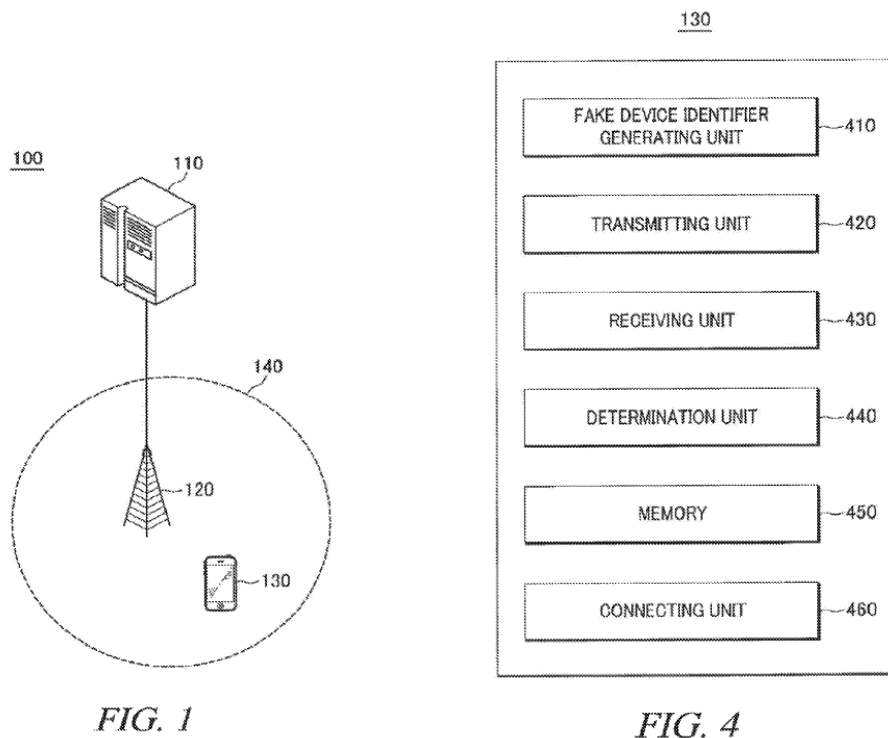
Next, the end device receives probe responses (320). *Id.*, 5:26-28; EX1009, 182 (Fig. 4-17). The probe responses include API of the respective APs, including MAC addresses and/or service set identifiers ("SSID"). EX1001, 4:19-23, 5:28-32.

The '384 Patent describes methods to determine a preferred AP, or authenticated AP ("AAP"), based on the API received in the probe response (330). *Id.*, 4:24-42, 5:34-52. One way compares received API to an authenticated AP list ("AAPL") by determining whether the received API is included in the AAPL. *Id.*, 3:35-42. The AAPL may contain a list of AAPs that are APs previously connected with the end device. *Id.* Alternatively, an AAP can be identified by determining whether an AP was previously connected with the end device. *Id.*

After selecting an AP, the end device sends a connection request (340) including the actual MAC address. *Id.*, 4:52-61, 5:53-60; EX1009, 182 (Fig. 4-17) (Authentication Request). The end device proceeds to connection by receiving an approval of the connection request and associating with the AP through association requests-response (360). *Id.*, 4:62-5:4, 5:61-64; EX1009, 182 (Fig. 4-17) (Authentication-Association). Following receipt of an association response, the end

device is connected to the wireless local area network (“WLAN”). EX1001, 5:3-4, 5:65-67.

A device to perform the above method is also described (Figs. 1, 4). End device 130 includes generic components. *Id.*, 6:12-18. Notably, no algorithms or specialized components are described.



B. Prosecution History

The reasons for allowance state:

The combination of limitations including “a fake media access control (MAC) address...transmitting, by the end device to an access point” and “determining, by the end device, that the access point is an authenticated access point”.

EX1003, 19.

C. Level of Ordinary Skill in the Art

Petitioner submits that a person of ordinary skill in the art (“POSITA”) for the ’384 Patent would have possessed at least a four-year degree in computer engineering, computer science, or a similar discipline, along with 2 years of professional experience in the fields of networking and network-based systems or applications, or an equivalent level of skill, knowledge, and experience. And would be aware of and generally knowledgeable about how devices were provisioned onto wireless networks, along with standards applicable to well-known methods for communication such as Wi-Fi, Bluetooth, and 3G available at the time the ’384 Patent was filed. EX1002, ¶36. Relevant graduate education could substitute for professional work experience. *Id.*

V. CLAIM CONSTRUCTION

Claims must be construed only to the extent necessary to resolve a controversy. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017). Here, no terms need construction to resolve the controversy in this forum.

VI. PRIOR ART AND GROUNDS FOR RELIEF

A. Printed Publications Relied Upon for Grounds of Invalidity

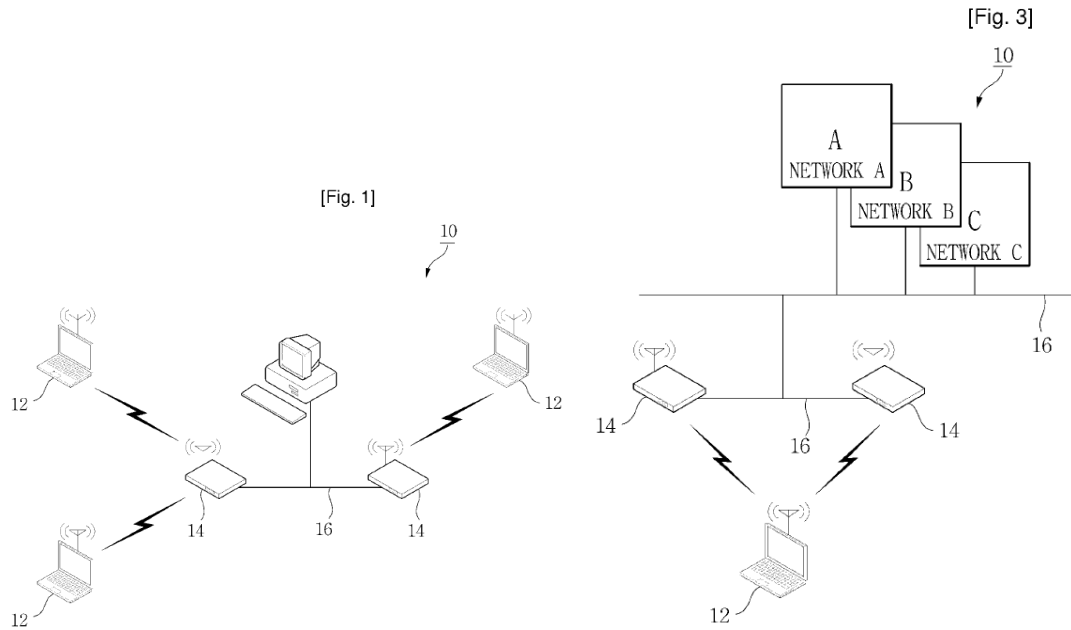
There is at least a reasonable likelihood that the claims of the '384 Patent will be found unpatentable. The '384 Patent claims priority to November 21, 2012; therefore, it is subject to pre-AIA §§102 and 103.

1. *Vardi* (US8,126,476)

Vardi published February 28, 2012, and is prior art under 35 U.S.C. § 102(a). EX1007, (22). *Vardi* describes a system and method for user terminals (“UT”) to connect to APs using a server provided database. *Id.*, 3:4-6, 4:18-25, 4:43-57. The database of APs stores and collates information corresponding to the APs for its “clients” (i.e., UTs) to utilize in real-time. *Id.*, 7:10-20, 7:33-36. The databases’ information is from prior connections between clients and APs and includes API (MAC address and SSID). *Id.*, 3:21-30, 11:41-42. Clients update the server based on their connections with APs, which then updates the database and sends the updates to clients. *Id.*, 3:4-6, 4:18-25, 8:7-21. IEEE 802.11 scans are used to identify APs and obtain API for both database and real-time connections. *Id.*, 10:34-36, 11:35-36, 13:4-7, 14:52-57. UTs compares that API to the API in the database to select APs for preferred connections. *Id.*

2. Yun (WO2007/086705)

Yun published August 2, 2007, and is prior art under 35 U.S.C. § 102(b). EX1004, (22). *Yun* describes wireless network systems and communication methods for wireless networks. *Id.*, (54).



Figures 1 and 3 (above) illustrate *Yun*'s wireless network systems. Specifically, stations(12) connected to WLANs(10) through APs(14) and distribution system(16). *Id.*, ¶[17], ¶[20], ¶[22], ¶[25]. The stations include network interface cards (NIC) to connect to the WLAN in accordance with IEEE 802.11 standard. *Id.*, ¶[17].

Figures 4 and 5 (annotated below) illustrate the connection process for connecting the station to the WLAN, corresponding to the *IEEE802.11* connection protocol. *Id.*, Figs. 4-5; EX1009, 182 (Fig. 4-17).

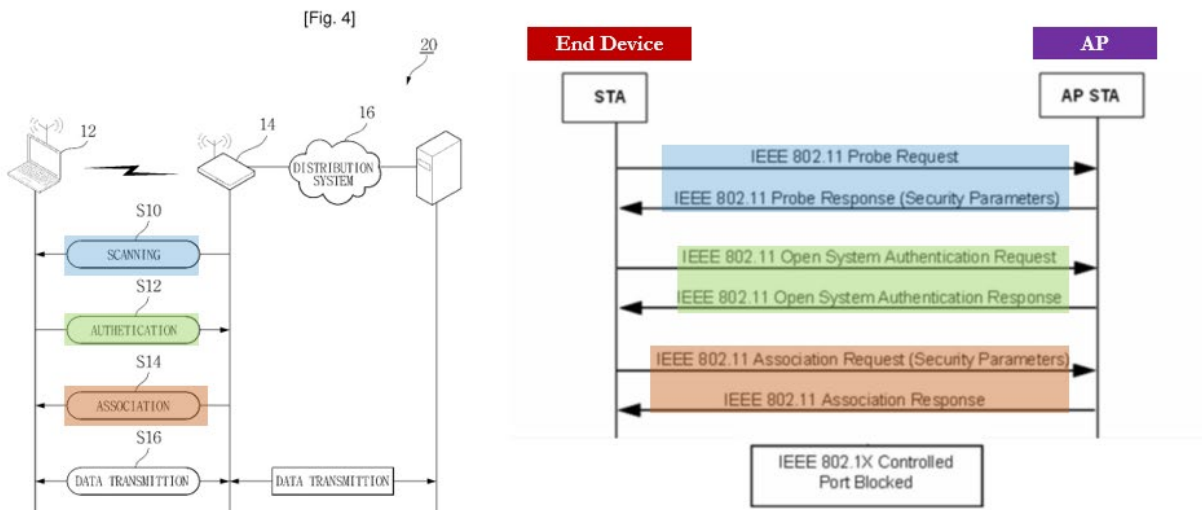
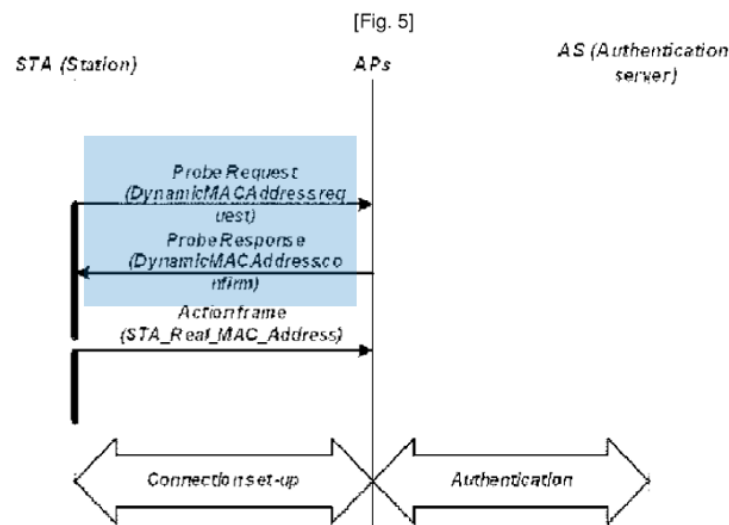


Figure 4-17—Establishing the IEEE 802.11 association



Scanning(S10) includes active scanning to identify available APs by broadcasting probe requests. EX1004, ¶¶[31]-[32]. The station receives probe responses from the APs including API such as SSID. *Id.*, ¶[32].

To provide MAC address anonymity during probe requests transmissions, *Yun* describes using arbitrary MAC addresses, e.g., AMID or dynamic MAC address, instead of the actual MAC address. *Id.*, ¶¶[144]-[145], ¶¶[154]-[156]. The station

generates the arbitrary MAC address and then transmits it in a probe request to the AP. *Id.*, ¶¶146], ¶¶154]-[156].

After scanning, *Yun* proceeds with IEEE 802.11 authentication(S12) and association(S14) to connect to the WLAN. *Id.*, ¶¶35]-[38].

3. ***IEEE802.11* (IEEE 802.11 Standard™- 2012)**

IEEE802.11 was published as a standard by IEEE in March 2012, and bears a 2012 Copyright date. EX1009, 1, 4. The 2012 edition “gives users, in one document, the IEEE 802.11 standard for wireless local area networks (WLANS) with all the amendments...” *Id.*, 11. By early 2012, *IEEE802.11* was publicly available, known, and widely available to POSITAs. EX1002, ¶80 (explaining how “[a]t the time of its publication and afterwards, *IEEE802.11* was a well-known standard in the wireless industry specifying aspects of wireless local area networks (‘LAN’)”); EX1009, 1880 n.51. Thus, *IEEE802.11* is prior art under at least § 102(a).

IEEE802.11 specifies “[t]he medium access control (MAC) and physical characteristics for wireless local area networks (LANs).” *Id.*, 4. It describes the procedure by which mobile devices join and communicate with other stations. *Id.*, 1076. Specifically, the mobile device can use “Active scanning[, which] involves the generation of Probe frames and the subsequent processing of received Probe Response frames.” *Id.*

A typical broadcast probe request frame seeks a response from any basic service set (“BSS”), a synchronized set of stations, and does not include the address of a specific SSID. *Id.*, 105, 1076-78. This is shown, in part, in Figure 10-3 below (*id.*, 1078), which shows the scanning station issuing a broadcast probe message, and responder stations 1 and 2 issuing probe response messages:

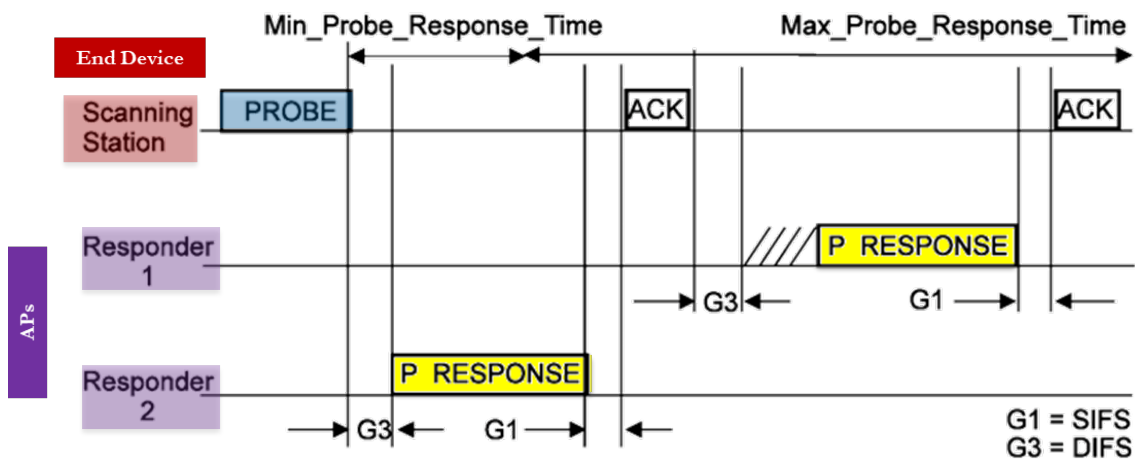


Figure 10-3—Probe response

If a device wishes to probe a specific BSS, for example a previously connected AP, then it appends to the probe request message the SSID of the specifically-targeted BSS during the active scanning procedure. *Id.*, 1076-78. Generally speaking, stations “receiving Probe Request frames shall respond with a probe response only if” the SSID in the probe request is the broadcast SSID or matches the specific SSID of the STA.” *Id.*, 1077.

IEEE802.11 further defines the general transmissions required to connect a station to the network provided by the AP. As shown below, scanning (probe request-response), authentication, and association between the station and AP occur in order to result in a connection. EX1002, ¶82; EX1009, 182 (Fig. 4-17).

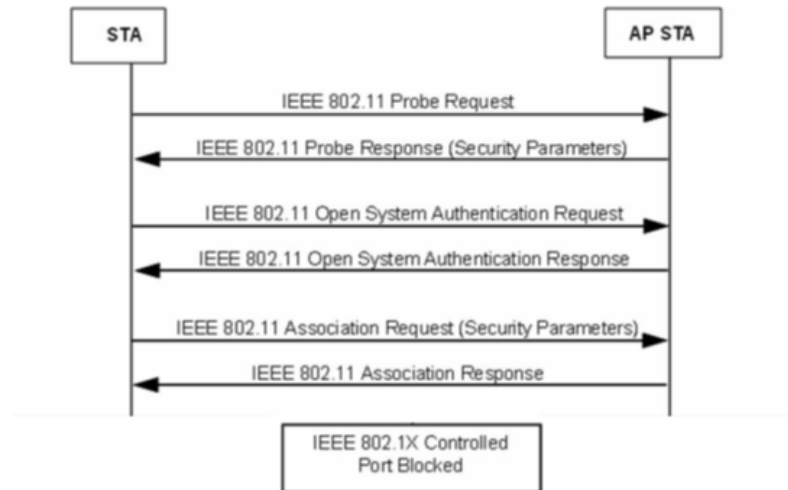


Figure 4-17—Establishing the IEEE 802.11 association

4. *Satish* (US7,885,639)

U.S. Patent 7,885,639 (“*Satish*”) issued February 8, 2011, and is prior art under 35 U.S.C. § 102(b). EX1012, (22). *Satish* discloses methods and systems for authenticating wireless APs. *Id.*, Abs., Fig. 2, 1:8-10, 2:58-59, 3:15-24, 6:22-26, 8:2-40, 9:13-53, 10:23-63. The methods include connecting to an AP, storing an SSID associated with the AP, storing a MAC address for the AP, and associating the MAC address with the SSID. *Id.*, 2:25-43, 9:13-53. *Satish* also discloses comparing API to previously-connected APs and selecting previously-connected APs for connection. *Id.*, 5:39-48, 6:49-58.

5. Jalfon (US2012/0076072)

Jalfon published March 29, 2012, and is prior art under 35 U.S.C. § 102(a). EX1006, (22) (43). *Jalfon* teaches systems and methods performed by wireless communication devices for maintaining wireless network privacy in the context of IEEE 802.11. *Id.*, (57), ¶[7], ¶[11], ¶[17]. The wireless devices transmit a probe request to APs including a randomized MAC address instead of the allocated MAC address, and subsequently receive probe responses from an AP. *Id.*, ¶¶[0016]-[0020], ¶[0029], ¶¶[0034]-[0036], Fig. 4. Then, the device sends an authentication request including the allocated MAC address to initiate a link to the network. *Id.*, ¶[0016], ¶[0033], ¶[0036], ¶[0039], Fig. 4.

B. Relief Requested and Statutory Grounds of Invalidity

Petitioner requests *inter partes* review of Claims 1-24 under 35 U.S.C. §§ 311 – 318 and 37 C.F.R. §§ 42.100 – 42.123, and cancellation of Claims 1-24 as unpatentable under 35 U.S.C. § 103.

Petitioner submits the following grounds of invalidity:

<u>#</u>	<u>Grounds</u>
1	<i>Vardi-Yun-IEEE802.11</i> renders obvious claims 1-24
2	<i>Vardi-Yun-IEEE802.11-Satish</i> renders obvious claims 17-24
3	<i>Vardi-IEEE802.11-Jalfon</i> renders obvious claims 1-24

VII. GROUND 1: *VARDI-IEEE802.11-YUN*

A. Motivation to Combine

Vardi, *Yun*, and *IEEE802.11* are all directed to the same field of endeavor in establishing secure wireless connections between a terminal and a network through a wireless AP according to IEEE 802.11 standard. EX1002, ¶87-88. Accordingly, a POSITA would be motivated to combine the references with an expectation of achieving a successful wireless connection to a network through an AP. *Id.* *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007).

Vardi discloses or suggests all the claimed IEEE 802.11 connection steps and components to perform those steps between a mobile device and AP—probing/scanning, authentication, and association. Although *Vardi* does not detail the underlying implementation of, for example, performing an “IEEE 802.11 scan,” “probing,” or “IEEE 802.11 association,” *Vardi* does explicitly disclose using IEEE 802.11 to connect a mobile device and AP. EX1002, ¶89. It therefore would have been obvious to a POSITA to look to IEEE 802.11 to provide underlying details of *Vardi*’s “scan,” “probing,” and “association.” *Id.* Indeed, *Vardi and Yun* explicitly direct a POSITA to the standard to implement their disclosed systems and methods. *Id.*; EX1007, 7:36-40, 10:25-28, 10:34-53, 11:35-36, 13:4-7, 14:52-57; EX1004, ¶[17], ¶[35], ¶[138], ¶[147], ¶[230].

Vardi also discloses or at least renders obvious the well-known components required by Claims 17-24. *Vardi* discloses that a “user terminal can be a device that executes a program...to find usable...wireless APs,” “clients can continuously collect radio resource information about AP’s [*sic*] detected by the wireless terminal. These clients can be executed on laptops, handheld[] devices (PDA[s]), cellphones, or other devices that incorporate radio facility for wireless communication, such as WiFi,” a POSITA would understand this disclosure satisfies the claimed processor and hardware communication interface including a transmitter and receiver. EX1007, 7:10-14, 9:54-59; EX1002, ¶90. *Vardi* also discloses “user’s clients can store... information in the memory of the wireless user terminal” and “can compare [received] scan result with its radio resource database to determine which APs are preferred for connection and roaming.” A POSITA would have readily understood these disclosures as satisfying the claimed “memory” and “processor” components of the claims. EX1007, 7:31-32, 14:55-57; EX1002, ¶90.

It would have been obvious to a POSITA to apply *Yun*’s generated arbitrary MAC address and anonymous probe request transmission (compliant with *IEEE802.11*), to the *Vardi* system. EX1002, ¶91. Additionally, to the extent *Vardi*’s hardware interface component is not explicit, *Yun*’s is explicit, and it would have been obvious to a POSITA to implement *Vardi*’s system using the well-known components of *Yun* compliant with *IEEE802.11*. *Id.*

Yun similarly describes a wireless communication network for a wireless connection between a station and network through a wireless AP, including a NIC to facilitate IEEE 802.11 communications and using IEEE 802.11 terminology. EX1004, ¶[25], ¶[17], ¶¶[30]-[38]; EX1002, ¶92. To ensure proper formatting of probe request/response messages that *Vardi* and *Yun* disclose, a POSITA would have turned to *IEEE802.11*, which defines these formats. EX1002, ¶92.

Moreover, *Yun* extends the IEEE 802.11 standard, identifying a problem, and solving the problem while remaining IEEE 802.11 compliant. EX1004, ¶[17], ¶[147]. Specifically, *Yun* identifies that stations previously used “their actual MAC address for communications with the access point,” but that allowed others to identify the station when receiving the MAC address. *Id.*, ¶[143], ¶[154]; EX1002, ¶93. To solve the problem, *Yun* teaches using an arbitrary MAC address distinct from the station’s in the probe request, which provides for “MAC address anonymity” and “makes an identity of the station(12) not presumed through the MAC address.” EX1006, ¶¶[154]-[156]; EX1002, ¶93.

As described above, *IEEE802.11* is foundational to both of *Vardi* and *Yun*’s teachings. Because each system shares a foundational standard, it ensures interoperability between *Vardi* and *Yun* for a POSITA with minimum effort and no undue experimentation. EX1002, ¶94. Indeed, a POSITA would have a reasonable expectation of success in applying *Yun*’s probe request into *Vardi*’s wireless

communication system because *Vardi*'s system already transmits probe request messages, including the MAC address as defined and taught by *IEEE802.11*. The modification would merely exchange a probe request including an actual MAC address with a probe request including a generated arbitrary MAC address. EX1002, ¶87, ¶94. Configuring *Vardi* to substitute the "actual" MAC address for an "arbitrary" MAC address would have been a routine application of well-known techniques in wireless communication. *Id.*; EX1007, 7:59-60; EX1004, ¶¶[144]-[146], ¶¶[154]-[156].

Yun additionally teaches improving *IEEE802.11* active scanning by generating and replacing the stations actual MAC address with an arbitrary MAC address to provide MAC address anonymity during the probe request broadcast. EX1004, ¶¶[144]-[146], ¶¶[154]-[156]. The use of arbitrary MAC addresses prevents the identity of the station from being disclosed through the MAC address; and therefore, prevents undesired APs from identifying the particular station. EX1002, ¶95; EX1004, ¶¶[154]-[156]. Thus, a POSITA would have been motivated to substitute the authentic MAC address of *Vardi* compliant with *IEEE802.11* probe request with the arbitrary generated MAC address of *Yun* to protect the identity of the station. *Id.* Since all references are compliant with *IEEE802.11*, a POSITA would have expected to successfully incorporate the arbitrary MAC address in a

probe request and receive a probe response, as taught by *Yun*. EX1002, ¶95, ¶87; EX1004, ¶[146], ¶[156].

B. Invalidity of Claims 1-24

1. Claim 1:

Vardi-IEEE802.11-Yun render obvious Claim 1. EX1002, ¶97.

- i. 1[pre]: *A method performed under control of an end device, the method comprising:*

Vardi discloses a method performed under control of a UT for connecting to a network via an AP. EX1007, 7:10-20 (“Each user’s wireless user terminal can be a device that executes a program (e.g., a client) that uses the combined data to find usable radio resources or wireless access points and establish network connections through them...”), 3:11-13, 4:18-27, 4:42-48, 6:34-35, 6:49-54, 8:7-21, Figs. 1-3; EX1002, ¶¶98-99.

- ii. 1[a]: *generating, by the end device, a fake media access control (MAC) address for the end device;*

Vardi-IEEE802.11-Yun render obvious Element 1[a]. EX1002, ¶100.

Yun discloses generating and using an AP MAC Identifier (“AMID”) by the station or a dynamic MAC address. EX1004, ¶¶[144]-[146] (“After the station(12) generates the trial AMID, the probe request including the generated AMID value is transmitted to the access point(14).”), ¶¶[154]-[156]. The AMID is an “arbitrary” (fake) MAC address for the station distinct from the fixed MAC address of the

station, and provides MAC anonymity during probe requests. *Id.*, ¶¶[144]-[145] (“AMID instead of the fixed MAC address...”), ¶[155]; EX1002, ¶101.

It would have been obvious to a POSITA to include *Yun*’s generating the AMID or dynamic MAC address into *Vardi*’s process for use in the probe request, as taught by *Yun*. EX1002, ¶102; §VII.A; *infra* §VII.B.1.iii.

- iii. 1[b]: *transmitting, by the end device to an access point, a probe request that includes the fake MAC address;*

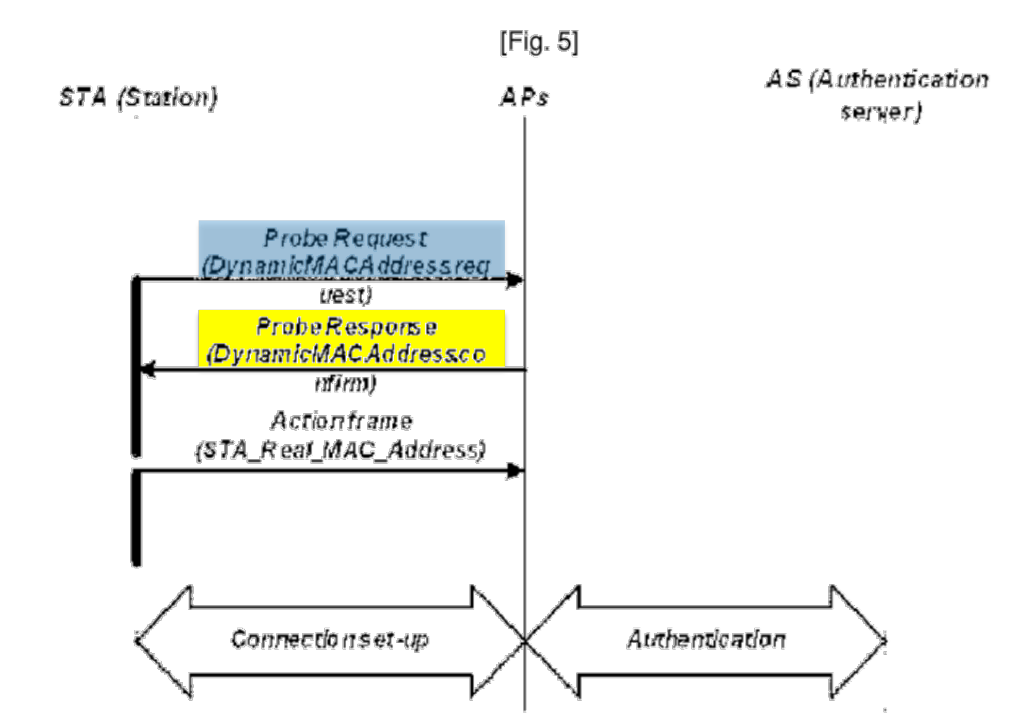
Vardi-IEEE802.11-Yun render obvious Element 1[b]. EX1002, ¶103.

Vardi discloses “[c]onnecting to a wireless network starts by scanning the neighborhood for candidate AP connections (IEEE 802.11 scan). The IEEE 802.11 scan can produce a list of access points in reach.” EX1007, 13:4-7. An IEEE 802.11 scan is a well-understood term of art encompassing “probe request-response.” EX1002, ¶104, ¶¶52-54. The UT attempting to connect to a wireless network issues a probe request (begins “active scan”), and APs in the area receive the probe request and subsequently transmit a probe response (APs respond “produc[ing] a list of access points”). EX1007, 13:4-8, 13:52-57 (“When client becomes active it executes an IEEE 802.11 scan for APs in reach and determines the SSID, MAC address, RSSI and security status.”). *Id.*

In this communication, a POSITA knows the UT transmits its MAC address to the AP—the alleged problem the ’384 patent is trying to solve. EX1001, 3:12-20

(“When searching, the end device may transmit a probe request frame that may include a device identifier, for the end device such as a media access control (MAC) address of the end device....since the probe request frame that includes the device identifier is transmitted to access points around the end device, present location of the end device may be exposed...”); EX1002, ¶105, ¶¶46-50.

Vardi does not disclose transmitting a fake MAC address in the probe request, but *Yun* does. “After the station(12) generates the trial AMID, the probe request including the generated AMID value is transmitted to the access point(14).” EX1004, ¶[146], ¶[156] (“the station(12) transmits the data including the MAC address request such as the probe request(‘Dynamic MAC address request’) to the access points(14).”), Fig. 5; EX1002, ¶106.



It would have been obvious to a POSITA to add *Yun*'s arbitrary MAC address generation capabilities to the UT of *Vardi* and for *Vardi*'s UT to transmit the arbitrary MAC address in the probe request “to supply MAC address anonymity,” thus preventing identification of the station from the probe request. EX1002, ¶107; EX1004, ¶¶[144]-[145], ¶¶[154]-[155]. The inclusion of *Yun*'s generation and use of arbitrary MAC address would also not alter the process of *Vardi* because *Yun* explicitly discloses a probe request including the arbitrary MAC address still triggers a probe response including API. *Id.*

To the extent transmitting a MAC address is disputed in the scan of *Vardi*, a POSITA would have readily known that or could have read—as instructed by *Vardi* and *Yun*—*IEEE802.11* to understand that the *IEEE802.11* probe request includes transmitting a MAC address. As identified below and *infra* §VII.B.1.vi, the *IEEE802.11* probe request includes transmitting a MAC address—source/origin IEEE MAC address in Address 2 field (SA field)—within the probe request sent by the device to the AP. EX1002, ¶108; EX1009, 97 (SA), 182 (Fig. 4-17), 516 (Fig. 8-34), 1078 (Fig. 10-3), 486. As §VII.A explains, a POSITA would have readily looked to *IEEE802.11* to provide the implementation details regarding *Vardi*'s “IEEE 802.11 scan,” and “probing.”

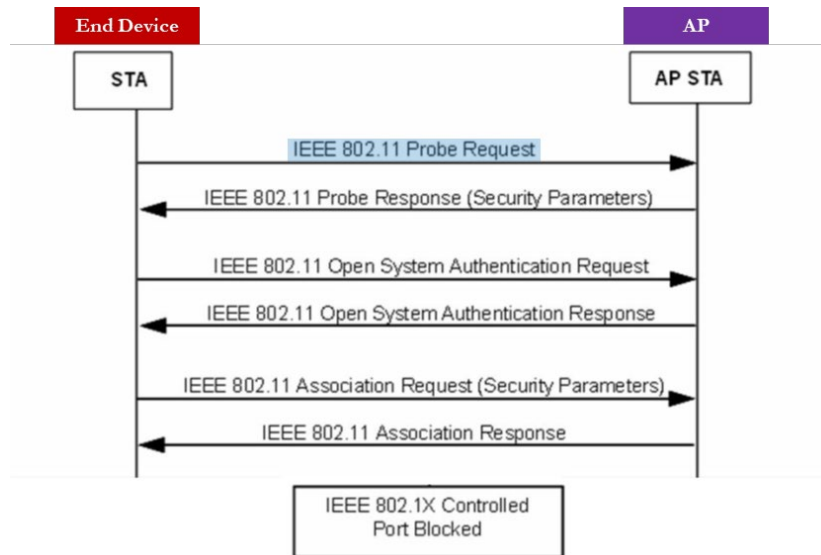
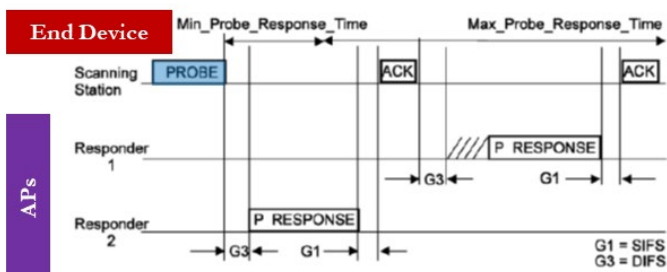
10.1.4.3.3 Active scanning procedure

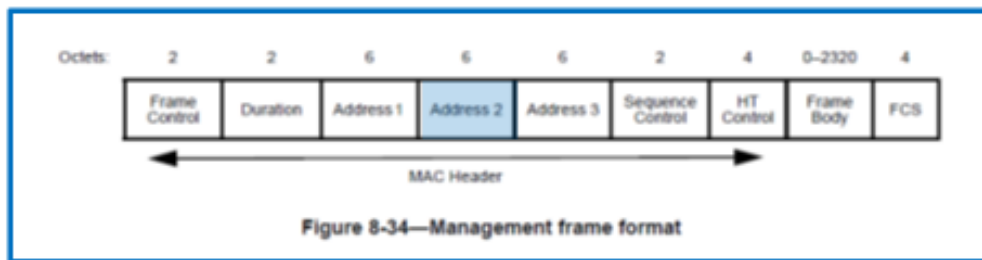
Upon receipt of the MLME-SCAN.request primitive with ScanType indicating an active scan, a STA shall use the following procedure:

For each channel to be scanned:

- Wait until the ProbeDelay time has expired or a PHYRxStart.indication primitive has been received.
- Perform the Basic Access procedure as defined in 9.3.4.2.
- Send a probe request to the broadcast destination address, with the SSID and BSSID from the MLME-SCAN.request primitive. When the SSID List is present in the MLME-SCAN.request primitive, send one or more probe request frames, each with an SSID indicated in the SSID List and the BSSID from the MLME-SCAN.request primitive.
- Set to 0 and start a ProbeTimer.
- If PHY-CCA.indication (busy) primitive has not been detected before the ProbeTimer reaches MinChannelTime, then set NAV to 0 and scan the next channel, else when ProbeTimer reaches MaxChannelTime, process all received probe responses.
- Set NAV to 0 and scan the next channel.

See Figure 10-3.





The address fields for all management frames except Multihop Action frames are as follows:

- a) The Address 1 field of the management frame is the RA (=DA) and is determined as the destination of the frame.
- b) The Address 2 field of the management frame is the TA (=SA) and is determined as the address of the STA transmitting the frame.
- c) The Address 3 field of the management frame is set and determined as follows:

8.2.4.3.6 SA field

The SA field contains an IEEE MAC individual address that identifies the MAC entity from which the transfer of the MSDU (or fragment thereof) or A-MSDU, as defined in 8.3.2.1, contained in the frame body field was initiated. The individual/group bit is always transmitted as a 0 in the source address.

- iv. 1[c]: receiving, by the end device from the access point, a probe response that includes information regarding the access point;

Vardi-IEEE802.11-Yun render obvious Element 1[c]. EX1002, ¶109.

The *Vardi-IEEE802.11-Yun* UT receives a probe response from APs including API—SSID and MAC address of the AP.

The UT of *Vardi* performs a “Basic IEEE 802.11 association procedure... using...probing to get association information” and “information acquired as part of the standard 802.11 scan, i.e., [Network or AP name (SSID...); and, AP Radio Mac address]” is included in the response from the AP. EX1007, 10:25-36, 13:4-7 (“Connecting to a wireless network starts by scanning the neighborhood for candidate AP connections (IEEE 802.11 scan). The IEEE 802.11 scan can produce

a list of access points in reach.”), 14:52-57 (“When client becomes active it executes an IEEE 802.11 scan for APs in reach and determines the SSID, MAC address...”), 7:10-46, 9:54-64 10:34-36, EX1002, ¶110.

As illustrated below, *Vardi* teaches additional information received within the probe response.

i. Network name;	xii. User Terminal Location;
ii. MAC address;	xiii. Access Point Location;
iii. Received signal strength and variance over time;	xiv. Mapping Type—how an access point location was determined.
iv. Encryption status;	The data base of data can comprise the above information as well as:
v. Internet connection available capacity;	i. Location
vi. Access protocol response times;	ii. Internet accessibility
vii. Gateway IP address;	iii. Long term behavioral statistics comprising:
viii. DNS address;	Percentage of availability
ix. Occupied IP addresses;	Signal strength variance
x. Captive portal credentials;	Available bandwidth
xi. Connection Technology;	iv. Name of owner;
	v. Owner profile;
	vi. Password.

Element 1[b] *supra* explains that a POSITA would have readily understood that *IEEE802.11* active scan encompass the probe request and response communication between the device and APs. §VII.B.1.iii; EX1002, ¶112.

But to the extent PO contends *Vardi* does not explicitly disclose the “probe response frame,” *IEEE802.11* defines the communication and frame (illustrated below). *IEEE802.11* explains that APs receiving a probe request frame will respond by issuing a probe response frame. EX1009, 1077-78, 528-31 (Table 8-27); EX1002, ¶113, ¶54. The probe response frame’s MAC header, as explained

supra §VII.B.1.iii, and frame body includes the AP's SSID and MAC Address.

Id., ¶¶46-50, ¶54.

10.1.4.3.3 Active scanning procedure

Upon receipt of the MLME-SCAN.request primitive with ScanType indicating an active scan, a STA shall use the following procedure:

For each channel to be scanned:

- Wait until the ProbeDelay time has expired or a PHYRxStart.indication primitive has been received.
- Perform the Basic Access procedure as defined in 9.3.4.2.
- Send a probe request to the broadcast destination address, with the SSID and BSSID from the MLME-SCAN.request primitive. When the SSID List is present in the MLME-SCAN.request primitive, send one or more probe request frames, each with an SSID indicated in the SSID List and the BSSID from the MLME-SCAN.request primitive.
- Set to 0 and start a ProbeTimer.
- If PHY-CCA.indication (busy) primitive has not been detected before the ProbeTimer reaches MinChannelTime, then set NAV to 0 and scan the next channel, else when ProbeTimer reaches MaxChannelTime, process all received probe responses.
- Set NAV to 0 and scan the next channel.

See Figure 10-3.

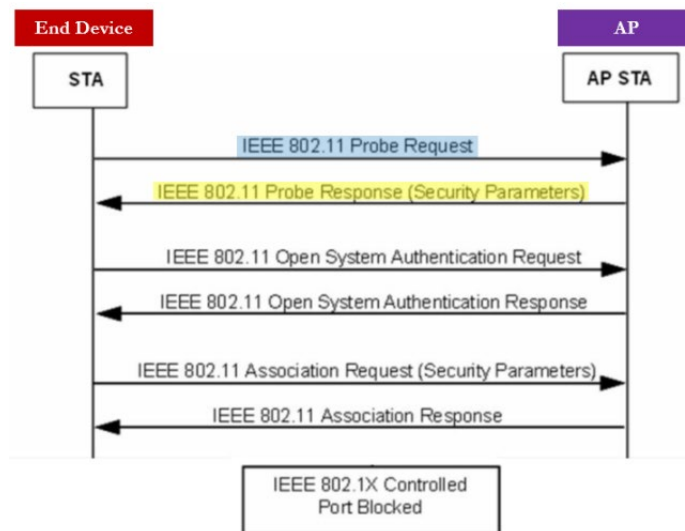
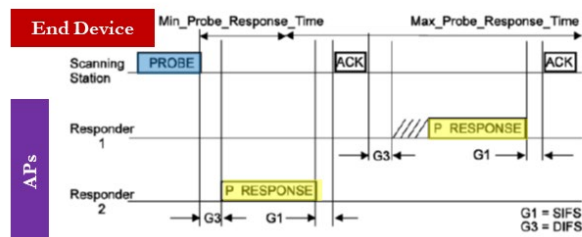


Table 8-27—Probe Response frame body

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability	

Table 8-27—Probe Response frame body (continued)

Order	Information	Notes
4	SSID	If dot11MeshActivated is true, the SSID element is the wildcard value as described in 8.4.2.2.
5	Supported rates	
6	FH Parameter Set	The FH Parameter Set element is present within Probe Response frames generated by STAs using FH PHYs.
7	DSSS Parameter Set	The DSSS Parameter Set element is present within Probe Response frames generated by STAs using Clause 16, Clause 17, and Clause 19 PHYs. The DSSS Parameter Set element is present within Probe Response frames generated by STAs using a Clause 20 PHY in the 2.4 GHz band.
8	CF Parameter Set	The CF Parameter Set element is present only within Probe Response frames generated by APs supporting a PCF.

Table 8-27—Probe Response frame body (continued)

Order	Information	Notes
23	Measurement Pilot Transmission	The Measurement Pilot Transmission element is present if dot11RMMeasurementPilotActivated is between 2 and 7.
24	Multiple BSSID	One or more Multiple BSSID elements are present if dot11RMMeasurementPilotActivated is between 2 and 7 and the AP is a member of a Multiple BSSID Set (see 10.11.14) with two or more members, or if dot11MgmtOptionMultiBSSIDActivated is true, or if dot11InterworkingServiceActivated is true and the AP is a member of a Multiple BSSID Set with two or more members and at least one dot11GASAdvertisementID MIB attribute exists.
25	RM Enabled Capabilities	The RM Enabled Capabilities element is present if dot11RadioMeasurementActivated is true.

As §VII.A explains, a POSITA would have readily looked to *IEEE802.11* to provide the implementation details regarding *Vardi*'s "IEEE 802.11 scan," and "probing." The POSITA would have a likelihood of success applying the implementation details to the *Vardi* system. EX1002, ¶114.

- v. 1[d]: *determining, by the end device, that the access point is an authenticated access point based, at least in part, on the information in the probe response being indicative that the access point was connected with the end device previous to when the access point received the probe request transmitted by the end device; and*

Vardi-IEEE802.11-Yun renders obvious Element 1[d]. EX1002, ¶115.

The '384 Patent identifies that an authenticated AP ("AAP") can be an AP previously connected with the end device. EX1001, 4:39-42. PO's infringement contentions agree, because PO asserts an AP is an AAP by being a previously-connected AP. EX1011, 30 (annotated below). PO also contends matching a list of previously-connected APs with the API received in the probe response meets this limitation. *Id.*

EXHIBIT A-INFRINGEMENT CONTENTIONS FOR U.S. PATENT NO. 10,694,384

The Accused Products determine that the access point is an authenticated access point (e.g., a whitelisted and/or previously connected Wi-Fi access point) based, at least in part, on the information in the probe response being indicative that the access point was connected with the end device previous to when the access point received the probe request transmitted by the end device.

Vardi teaches that "it was well known in prior art computing systems" for devices to store API of previously-connected APs facilitating devices to

“*automatically* reconnect to that AP. The cache [memory] normally includes the [SSID] and MAC address of the AP.” EX1007, 12:24-30. *Vardi* further teaches to compare the scanning data to stored MAC address to determine which APs are preferred for connection. EX1007, 14:52-57 (“When client becomes active it executes an IEEE 802.11 scan for APs in reach and determines the SSID, MAC address... Using the MAC address, the client can compare this scan result with its radio resources database to determine which APs are preferred for connection...”), 4:22-23, 12:24-30, 13:19-23; EX1002, ¶117.

Thus, *Vardi* teaches, or at least renders obvious, storing API of previously-connected APs, and then upon subsequent probing, comparing the datasets and *automatically* selecting and connecting to an AP because the API matches the cached list of previously-connected APs. EX1002, ¶118.

Additionally, *Vardi* teaches comparing the API received in the probe response to information in a radio resource database [AP list], previously obtained from a server and stored in the UT’s memory to select a favorable AP. EX1007, 3:21-54, 13:4-12, 7:10-20, 7:33-36, 14:52-57; EX1002, ¶119. The API from the server is collected based on prior connections between the UT and APs, and includes API—MAC address and SSID. *Id.*, 3:4-6, 3:21-30, 4:18-25, 8:7-21, 11:41-42. The UTs compare the stored API with the API received from an *IEEE802.11* scan to determine whether the AP is the preferred AP—the preferred

AP being an AAP—and automatically connects to that AP when the UT determines that the SSID or MAC address from the *IEEE802.11* scan matches that of the received database stored in memory. EX1007, 14:52-57; EX1002, ¶119.

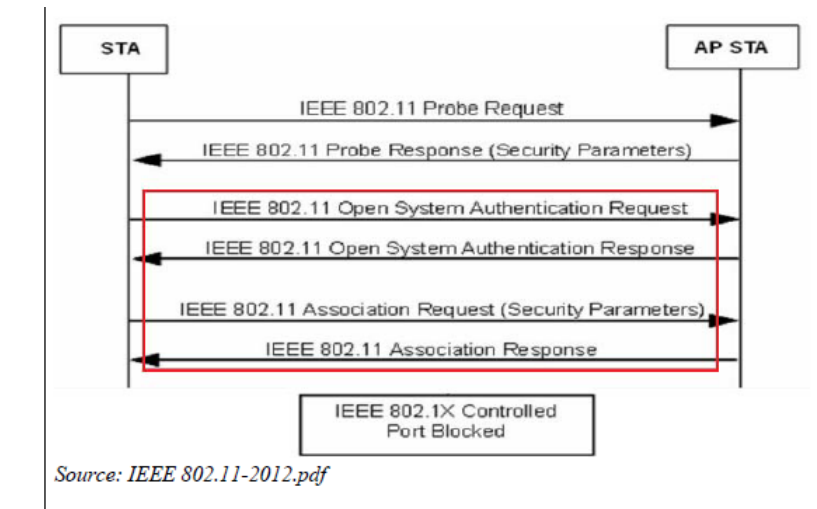
Vardi further explicitly determines an AP as a “most favorable [AP]” for connection if an available AP is included in the database distributed by the server or if the available AP is included in “a list of *previously successfully* used [APs].” EX1007, 13:13-23; EX1002, ¶120. Because *Vardi* teaches selecting an AP based on matching API received during *IEEE802.11* scanning to a list of previously successfully used APs to select the AP for connection (EX1007, 13:19-23), *Vardi* discloses or at least renders obvious the API received in the probe response being indicative that the AP was connected with the UT previously. EX1002, ¶120.

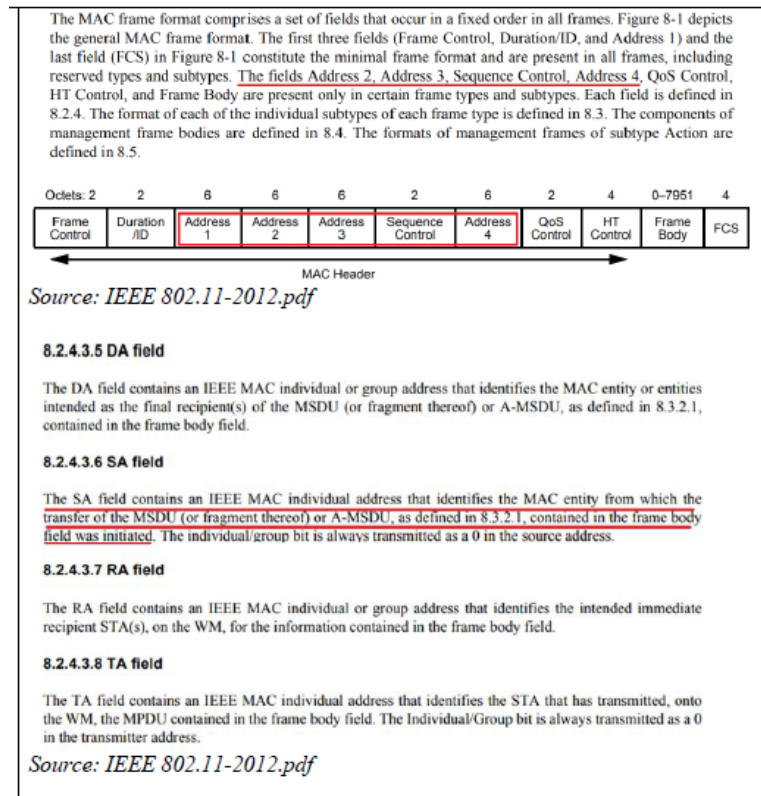
Specifically, for the API of the probe request to match API in list of previously-connected APs, the API of the probe request must *indicate* that AP was previously connected to the UT, for example, by being able to be matched to the list API. *Id.*

- vi. 1[e]: *transmitting, by the end device to the access point determined to be the authenticated access point, a connection request that includes an authenticated device identifier for the end device.*

Vardi-IEEE802.11-Yun renders obvious Element 1[e]. EX1002, ¶121. *Vardi* discloses connecting to the preferred AP. See §VII.B.1.v; EX1007, 14:52-57 (“preferred for connection...”).

The '384 Patent states a connection request may include an original MAC address of the device and an authentication request, which is followed by authentication response and association request and response. EX1001, 4:54-5:4. PO's infringement contentions cite *IEEE802.11* specification as evidence of infringement. PO draws a red box around the *IEEE802.11* authentication and association steps and cites the "MAC header."





Ex.1011, 36-37 (annotations in original).

Vardi discloses this. The UT, when “[c]onnecting to a wireless network starts by scanning the neighborhood for candidate AP connections (IEEE 802.11 scan)... the connection process will exploit the radio resource information in its memory.” EX1007, 13:4-10. For example, “If a ‘favorite’ AP (AP is called favorite if it is part of radio resource database that had been distributed to client...) is detected by the IEEE 802.11 scan...the client can select this AP for connection, or If a list of previously successfully used access points is available (locally stored) and some APs on the list are available...the client can select the AP...for connection.” *Id.*, 13:13-23. EX1002, ¶123.

Vardi explains that the UT and AP performs an “IEEE 802.11 association procedure” to establish connection. EX1007, 7:36-40 (“establishing a WiFi connection to the Internet requires a sequence of steps, starting with the **IEEE 802.11 association**, continuing with security exchange, essential network IP information acquisition .”), 10:34-35 (“F1—**Basic IEEE 802.11 association procedure** (inclusive of WEP, if needed)”), 10:50 (“F2—**IEEE 802.11 authentications**, (WPA, WPA2...)”); EX1002, ¶124.

A POSITA would understand that the IEEE 802.11 association procedure includes: (1) device discovery (‘probing’); (2) device authentication (WEP, checking capabilities); and (3) establishing connection (association). *Id.* Each of these steps involves transmitting management frames, including a “MAC header” as defined in *IEEE802.11*. *Id.*, ¶124, ¶¶46-57; §VII.B.1.iii. A POSITA would understand the MAC header used while establishing the connection to include the original MAC address of the transmission source. *Id.* Thus, a POSITA would have readily understood at the time of the alleged invention that *Vardi* teaches or at least renders obvious transmitting a “connection request” comprising the original MAC address of the transmission source, *i.e.*, the UT, to the AP for connection with the MAC header. *Id.*

To the extent PO contends that *Vardi*’s *IEEE802.11* association procedure does not explicitly disclose the “authentic device identifier”, *IEEE802.11* does.

IEEE802.11 dictates that a “STA shall be able properly to construct a subset of the frames specified in this clause for transmission and to decode.... All STAs shall be able to validate every received frame...and to interpret certain fields from the MAC headers of all frames.” EX1009, 478. *IEEE802.11* further explains that “[e]ach frame consists of the following...*MAC header*.... A variable-length *frame body*, which contains information specific to the frame *type* and *subtype*...” *Id.* (emphasis in original). *IEEE802.11* sets forth the general frame format, which includes a *MAC header* and *frame body*. *Id.* (8.2 MAC frame formats). Specifically, the “MAC frame format comprises a set of fields that occur in a fixed order in all frames.” *Id.*, 479 (Fig. 8-1 (below)). While Figure 8-2 identifies, for example, “The Type and Subtype fields together identify the function of the frame.” Thus, as identified in Table 8-1 of *IEEE802.11*, fields “Type and Subtype” identify whether the communication is an “Association” request/response, “Probe” request/response, or “Authentication,” which are transmitted with the MAC header. EX1002, ¶125, ¶¶46-50, ¶¶55-57. And the MAC header includes the MAC address—claimed authentic device identifier—during the connection request. *Id.*

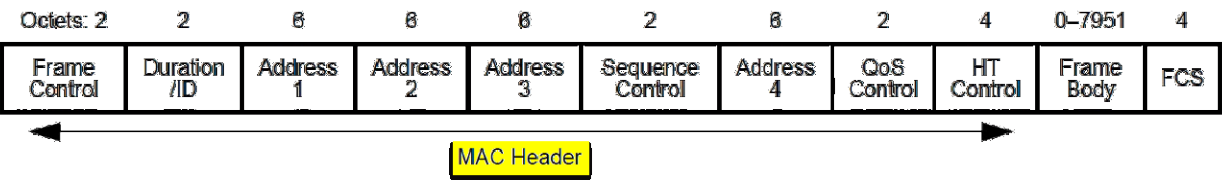


Figure 8-1—MAC frame format

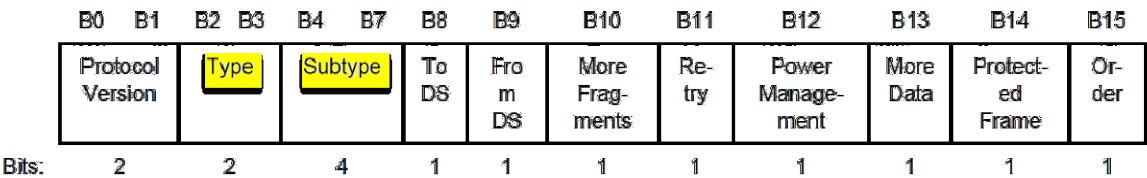


Figure 8-2—Frame Control field

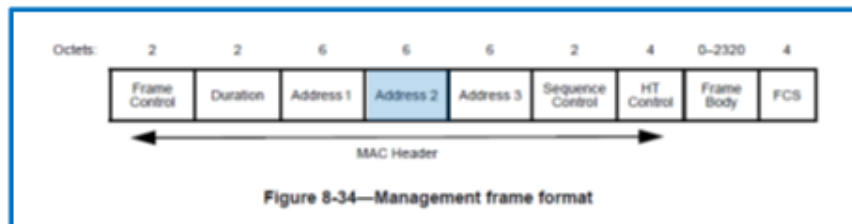
Table 8-1—Valid type and subtype combinations

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	Timing Advertisement

Table 8-1—Valid type and subtype combinations (continued)

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication

As shown below, after the device selects the “preferred AP,” it performs an exchange comprising at least four management frames (shown in the red dotted box). *IEEE802.11* expressly discloses that the MAC address in the MAC header ((SA field) Address field 2 (*supra* §VII.B.1.iii))—authentic device identifier—is transmitted as part of each message Type and SubType for connection. EX1002, ¶126, ¶¶46-50, ¶¶55-57; EX1009, 182 (Fig. 4-17 – Establishing the IEEE 802.11 association), 516 (Fig. 8-34), 486 (8.2.4.3.6 SA field). As stated above, a POSITA would understand the MAC header used while establishing the connection includes the original MAC address of the transmission source. *Id.*



The address fields for all management frames except Multihop Action frames are as follows:

- The Address 1 field of the management frame is the RA (=DA) and is determined as the destination of the frame.
- The Address 2 field of the management frame is the TA (=SA) and is determined as the address of the STA transmitting the frame.
- The Address 3 field of the management frame is set and determined as follows:

8.2.4.3.6 SA field

The SA field contains an IEEE MAC individual address that identifies the MAC entity from which the transfer of the MSDU (or fragment thereof) or A-MSDU, as defined in 8.3.2.1, contained in the frame body field was initiated. The individual/group bit is always transmitted as a 0 in the source address.

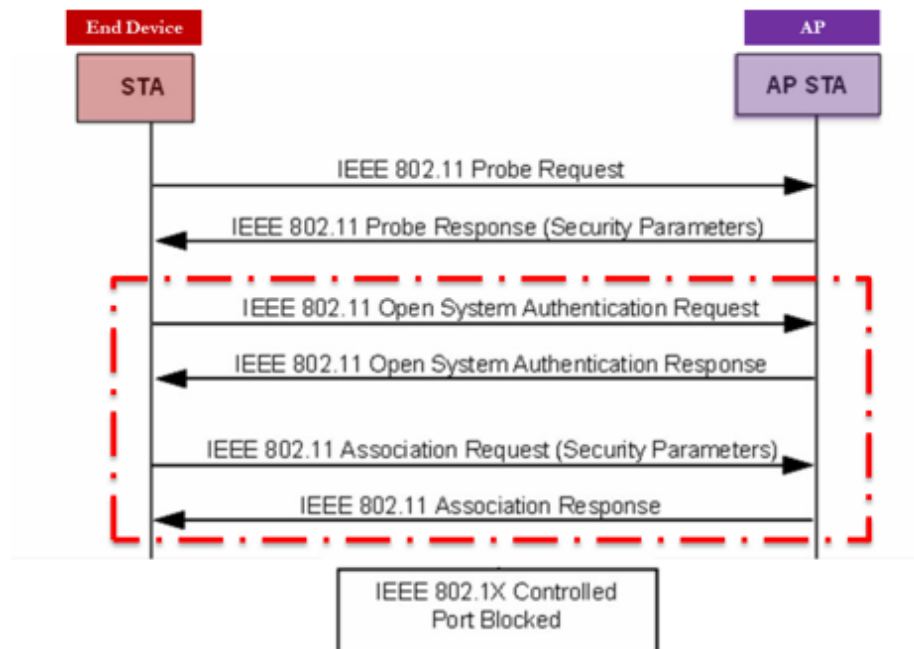


Figure 4-17—Establishing the IEEE 802.11 association

8.2.4.3.5 DA field

The DA field contains an IEEE MAC individual or group address that identifies the MAC entity or entities intended as the final recipient(s) of the MSDU (or fragment thereof) or A-MSDU, as defined in 8.3.2.1, contained in the frame body field.

8.2.4.3.6 SA field

The SA field contains an IEEE MAC individual address that identifies the MAC entity from which the transfer of the MSDU (or fragment thereof) or A-MSDU, as defined in 8.3.2.1, contained in the frame body field was initiated. The individual/group bit is always transmitted as a 0 in the source address.

8.2.4.3.7 RA field

The RA field contains an IEEE MAC individual or group address that identifies the intended immediate recipient STA(s), on the WM, for the information contained in the frame body field.

8.2.4.3.8 TA field

The TA field contains an IEEE MAC individual address that identifies the STA that has transmitted, onto the WM, the MPDU contained in the frame body field. The Individual/Group bit is always transmitted as a 0 in the transmitter address.

8.2.3 General frame format

The MAC frame format comprises a set of fields that occur in a fixed order in all frames. Figure 8-1 depicts the general MAC frame format. The first three fields (Frame Control, Duration/ID, and Address 1) and the last field (FCS) in Figure 8-1 constitute the minimal frame format and are present in all frames, including reserved types and subtypes. The fields Address 2, Address 3, Sequence Control, Address 4, QoS Control, HT Control, and Frame Body are present only in certain frame types and subtypes. Each field is defined in 8.2.4. The format of each of the individual subtypes of each frame type is defined in 8.3. The components of management frame bodies are defined in 8.4. The formats of management frames of subtype Action are defined in 8.5.

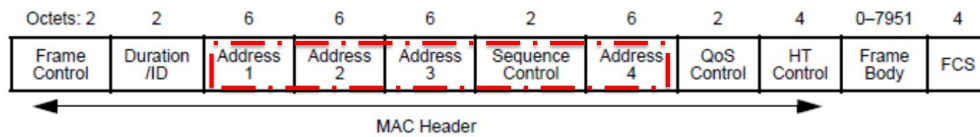


Figure 8-1—MAC frame format

As explained herein, a POSITA would have looked to *IEEE802.11* to implement the necessary components of a connection request. EX1002, ¶127; §VII.A.

2. Claim 9:

Vardi-IEEE802.11-Yun renders obvious Claim 9. EX1002, ¶128.

- i. 9[pre]: *A method performed by an end device, the method comprising:*

Vardi discloses a UT performing a method for connecting to a network via an AP. EX1007, 7:10-20 (“Each user’s wireless user terminal can be a device that executes a program (e.g., a client) that uses the combined data to find usable radio resources or wireless access points and establish network connections through them....”), 3:11-13, 4:18-27, 4:42-48, 6:34-35, 6:49-54, 8:7-21, Figs. 1-3; EX1002, ¶129.

- ii. 9[a]: *obtaining, by the end device, an authenticated access point list that includes information regarding one or more access points;*

Vardi-IEEE802.11-Yun renders obvious Element 9[a]. EX1002, ¶132.

The '384 Patent states the AAPL may include information about AAPs—MAC address or SSID. EX1001, 4:45-51, Fig. 2. AAPs include APs previously connected with the end device. *Id.*, 4:39-42. Thus, a database including API of APs previously connected to the end device meets this limitation. EX1002, ¶131. PO's infringement contentions agree. EX1011, 60 (“the memory stores a list of previously-connected access points”).

Vardi teaches or renders obvious caching a list of previously-connected APs by UTs for use in future connections. EX1007, 12:24-29; EX1002, ¶132. The cached list includes the SSID and MAC address of the AP. EX1007, 12:29-30, 13:19-23. Therefore, *Vardi* teaches obtaining by the UT a list of previously-connected to APs including MAC address and SSID of the APs. EX1002, ¶132. Thus, *Vardi* renders obvious Element 9[a]. *Id.*

Vardi discloses UTs “execute[] a program (*e.g.*, a client) that uses the combined data to find usable radio resources or wireless APs and establishes network connections through them....” EX1007, 7:10-14. *Vardi*'s UTs utilize the received API to compare with the stored API to select and connect to their preferred AP—AAP. Specifically, *Vardi*'s “clients receive updates about relevant

access points from the server and use the information to select and connect to the preferred access point.” *Id.*, 3:4-6. The API “can include access point connectivity information that can be used by the wireless user terminal to connect to the access point.” *Id.*, 3:21-59 (API illustrated below), 7:23-32 (AP data stored in memory), 12:24-30 (cache information of previously-connected APs), 13:13-23 (compare received API with stored API to connect to “‘favorite’ AP”), 11:41-42; EX1002, ¶133.

i. Network name;	xii. User Terminal Location;
ii. MAC address;	xiii. Access Point Location;
iii. Received signal strength and variance over time;	xiv. Mapping Type—how an access point location was determined.
iv. Encryption status;	The data base of data can comprise the above information as well as:
v. Internet connection available capacity;	i. Location
vi. Access protocol response times;	ii. Internet accessibility
vii. Gateway IP address;	iii. Long term behavioral statistics comprising:
viii. DNS address;	Percentage of availability
ix. Occupied IP addresses;	Signal strength variance
x. Captive portal credentials;	Available bandwidth
xi. Connection Technology;	iv. Name of owner;
	v. Owner profile;
	vi. Password.

- iii. 9[b]: *generating, by the end device, a MAC address for the end device that is distinct from an actual MAC address for a hardware network interface of the end device.*

Vardi-IEEE802.11-Yun teach Element 9[b]. EX1002, ¶134.

Vardi-Yun discloses generating arbitrary MAC addresses for the end device, explained *supra* §VII.B.1.ii. EX1002, ¶135.

Yun's stations include NICs—hardware network interfaces—for the WLAN and facilitating connections based on IEEE 802.11. EX1004, ¶[17]; EX1002, ¶136. It was widely known that NICs are allocated unique and fixed MAC addresses from manufacturers, which become the origin address of transmissions arising out of the station, and thus the MAC address of the station. EX1002, ¶136.

The generated arbitrary MAC address is distinct from the fixed MAC address of the station. EX1004, ¶[145] (teaching use of arbitrary MAC address “*instead of* the fixed MAC address”). Indeed, MAC address anonymity as taught by *Yun* requires the distinction. EX1004, ¶[145], ¶[154]; EX1002, ¶137.

It would have been obvious to generate a MAC address distinct from the NIC's actual MAC address of the end device, including as explained *supra* §VII.B.1.ii, §VII.A. EX1002, ¶138.

- iv. 9[c]: *transmitting, by the end device to at least one access point, a probe request that includes the generated MAC address;*

Vardi-IEEE802.11-Yun teach Element 9[c] for the same reasons as Element 1[b]. §VII.B.1.iii; EX1002, ¶¶139-40.

- v. 9[d]: *receiving, by the end device from the at least one access point in response to the probe request, a probe response that includes information regarding the at least one access point;*

Vardi-IEEE802.11-Yun teach Element 9[d] for the same reasons as Element 1[c]. §VII.B.1.iv; EX1002, ¶¶141-42.

- vi. 9[e] / 9[f]: *determining, by the end device based at least, in part, on the information regarding the at least one access point, that the at least one access point is an authenticated access point; wherein determining that the at least one access point is the authenticated access point includes determining that the information regarding the at least one access point is included in the authenticated access point list;*

Vardi-IEEE802.11-Yun teach Claim Elements 9[e], 9[f]. EX1002, ¶143.

The claim language dictates that determining an AP is included in the AAPL of previously-connected to APs satisfies determining that an AP is an AAP. EX1002, ¶144. PO's infringement contentions agree. EX1011, 87, 92.

As explained *supra* §VII.B.1.v, *Vardi* teaches the UT determining, based on API received in the probe response, that an AP is an AAP by matching the API received in the probe response to the API included in the database of previously-connected APs or cached storage (AAPL). EX1002, ¶145; §VII.B.2.ii.

- vii. 9[g]: *transmitting, by the end device to the at least one access point after determining that the at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the end device.*

Vardi-IEEE802.11-Yun render obvious Element 9[g] for the same reasons as Element 1[e]. §VII.B.1.vi, §VII.B.2.iii; EX1002, ¶¶146-47.

3. Claim 2:

Vardi-IEEE802.11-Yun render Claim 2 obvious. EX1002, ¶148.

Vardi-IEEE802.11-Yun teach generating a fake MAC address for the UT as explained *supra* §VII.B.1.ii.

Vardi-IEEE802.11-Yun further teach generating a MAC address distinct from the actual MAC address of the end device (NIC) as explained in Element 9[b]. §VII.B.2.iii; EX1002, ¶149.

4. Claims 3 and 10:

Vardi-IEEE802.11-Yun render obvious Claims 3 and 10. EX1002, ¶150.

The '384 Patent describes preventing leakage of the present location information *by transmitting the fake MAC address in the probe request*. EX1001, 3:24-45. PO's infringement contentions agree. EX1011, 41.

Yun teaches this. By using arbitrary MAC addresses instead of fixed MAC addresses, MAC anonymity is obtained obfuscating identifying the station. EX1004, ¶[145]. ¶[154]; EX1002, ¶151. Since *Vardi-IEEE802.11-Yun* teach including a fake or distinct MAC address in the probe request (§VII.B.1.iii, §VII.B.2.iv), the “fake MAC address is insufficient to identify the end device. As such, user privacy is increased because the present location of the end-device...is not leaked, as the device MAC address is not identified” (EX1011, 41). EX1002, ¶151.

5. Claims 4 and 11:

Vardi-IEEE802.11-Yun render obvious Claims 4 and 11. EX1002, ¶152.

Yun teaches generating an arbitrary MAC address. EX1004, ¶[144], [146], [154], [155]. A POSITA understands “arbitrary” means “existing or coming about seemingly at random or by chance....” EX1015. Therefore, it would have been obvious to generate the arbitrary MAC address of *Yun* using characters selected at random because a known method of achieving an arbitrary address coming about at random or by chance is to include at least one character selected at random. EX1002, ¶153.

6. Claims 5 and 16:

Vardi-IEEE802.11-Yun teach, explained *supra* §VII.B.1.vi and §VII.B.2.vii, the connection request includes the authentic MAC address for the UT/NIC, and therefore render obvious Claims 5 and 16. EX1002, ¶¶154-55.

7. Claim 6:

Vardi-IEEE802.11-Yun render obvious Claim 6. §VII.B.1.vi; EX1002, ¶156.

- i. 6[a]: *receiving, by the end device from the access point, an approval of the connection request;*
- ii. 6[b]: *connecting, by the end device, to a wireless local area network provided by the access point;*

Vardi discloses a UT connecting through the preferred AP via *IEEE802.11* authentication-association protocol to a WLAN. EX1007, 4:42-48 (searching for and connecting to AP), 7:10-20 (“wireless user terminal can be a device that

executes a program (e.g., client) that uses the combined data to find usable radio resources or wireless APs and ***establish network connections*** through them, for example, connections to the internet.”), 7:36-43 (“establishing a ***WiFi connection*** to the Internet requires a sequence of steps, starting with the IEEE 802.11 association, continuing with security exchange, essential network IP information acquisition and accessing specific network location.”), 10:34-39, 10:50-53; EX1002, ¶157.

To the extent PO contends that *Vardi*’s disclosure connecting the UT and AP via the “IEEE 802.11 association, continuing with security exchange, essential network IP information acquisition” procedure does not explicitly disclose or teach Claim 6, *IEEE802.11* does. EX1009, 182 (FIG.4-17) (below); EX1002, ¶158. Claim 6 merely recites the steps required by an IEEE 802.11 connection procedure. EX1002, ¶158. As shown below, *IEEE802.11* defines the connection procedure between a station (“STA”) and an AP (“AP STA”). *Id.* *IEEE802.11* illustrates that after the STA and AP exchange probe request and response messages, the STA receives an authentication response, transmits an associate request to the AP, and the STA receives the AP’s association response, at which point the STA and AP are connected to the WLAN via the AP. EX1002, ¶158.

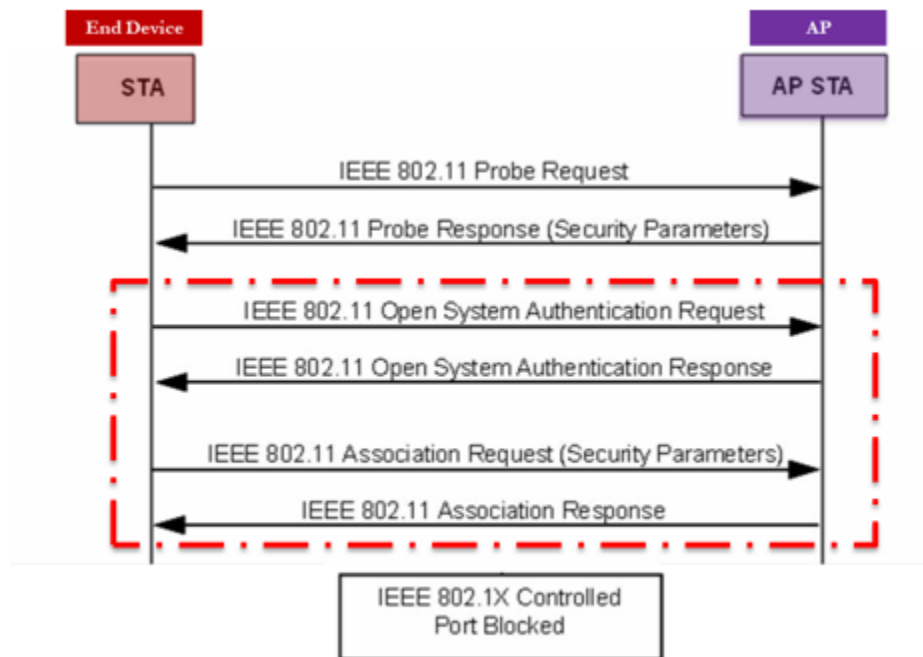


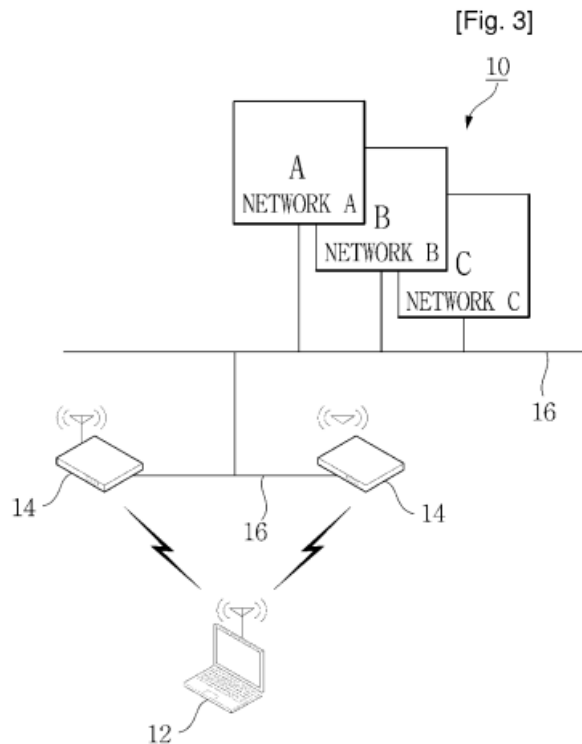
Figure 4-17—Establishing the IEEE 802.11 association

A POSITA would have found it obvious to review the underlying implementation provided by the *IEEE802.11* standard to establish a connection of its UT to the network because *Vardi* expressly instructs its connections are based on *IEEE802.11* and a POSITA would have been familiar with the standard. EX1002, ¶159; §VII.A.

Thus, *Vardi-IEEE802.11-Yun* teach performing the authentication-association protocol according to *IEEE802.11* to connect to the network, and *Vardi-IEEE802.11-Yun* teach the UT receiving an approval of the connection response including receiving an authentication response. EX1002, ¶160.

To the extent PO disputes *Vardi* connects to a WLAN, *Yun* also teaches connecting its station to a WLAN provided by an AP. FIG. 3 shows station(12)

connecting to WLAN(10) provided by AP(14). EX1004, ¶¶[15]-[17], ¶20, ¶22, ¶¶[29]-[38]; EX1002, ¶161.



To the extent necessary, it would have been obvious to a POSITA to connect the UT to a wireless LAN system as described by *Yun*, because *Yun* teaches a wireless connection to LAN compliant with *IEEE802.11* that permits a station to advantageously connect to a plurality of different networks through a single AP. EX1002, ¶[25]; EX1002, ¶162. And a POSITA would seek to provide users of the APs access to the Internet or more than peer-to-peer connection and thus, it would be obvious to provide WLAN connectivity in a wireless system as disclosed by *Vardi* and *Yun*. EX1002, ¶162.

8. Claims 7 and 15:

Vardi-IEEE802.11-Yun renders obvious Claims 7 and 15. EX1002, ¶163.

Vardi discloses compliance with *IEEE802.11* (§VII.A) and APs providing Wi-Fi . EX1007, 14:66-15:1 (“FIG. 3... radio access points 370*a-d* are connected to a network 305, such as the Internet.”); 7:6-43. Additionally, *Vardi*’s UTs are configured to communicate via *Wi-Fi* with the APs. EX1007, 9:54-59 (“clients continuously collect radio resources information about APs detected by the wireless user terminal. These clients can be executed on laptops, handheld devices (PDA’s), cellphones, or any other devices that incorporates a radio facility for wireless communication, such as WiFi.”); 5:11-16 (“Wifi enabled mobile telephones”); 7:36-40; FIG. 3; EX1002, ¶164.

9. Claim 8:

Vardi-IEEE802.11-Yun renders obvious Claim 8. EX1002, ¶165.

- i. 8[a]: *receiving, by the end device, a list of authenticated access points that includes information regarding one or more access points,*

Vardi discloses Element 8[a] for the same reasons as Element 9[a]; and specifically, because *Vardi* teaches obtaining an AAPL from a server containing a database of previously-connected APs including MAC addresses and/or SSIDs. §VII.B.2.ii; EX1002, ¶166.

- ii. 8[b]: *wherein determining that the access point is the authenticated access point is further based on determining that the access point is included in the list of authenticated access points.*

Vardi discloses determining the AP is an AAP based on determining that the AP is included in the AAP list, as explained above. *Vardi* selects a favorable AP for connection based upon comparing real-time AP API to a stored list of API for previously connected to APs from the server. §VII.B.2.vi; EX1002, ¶167.

10. Claim 12:

Vardi-IEEE802.11-Yun renders obvious Claim 12. EX1002, ¶168.

Vardi discloses receiving an AAPL from the server including the MAC address or SSID of each of the APs. VI.B.2.ii. For “each radio source” the database includes SSID and MAC address. EX1007, 3:25-30; EX1002, ¶169.

11. Claim 13:

Vardi-IEEE802.11-Yun renders obvious Claim 13. EX1002, ¶170.

It would have been obvious to a POSITA to further determine the AP is an AAP by determining if the UT was previously connected to the AP as explained above, including because *Vardi* discloses making the AP selection based on comparing API obtained from available APs to a previously stored database of previously-connected APs and selecting a match. §VII.B.2.vi, §VII.B.9.ii; EX1007, 13:19-23; EX1002, ¶127.

12. Claim 14:

Vardi-IEEE802.11-Yun renders obvious Claim 14. VII.B.2.vii; EX1002, ¶172.

- i. 14[a]: *receiving, by the end device from the at least one access point, an approval of the connection request;*
- ii. 14[b]: *transmitting, by the end device to the at least one access point after receiving the approval of the connection request, an association request;*
- iii. 14[c]: *receiving, by the end device from the at least one access point, an association response to the association request; and*
- iv. 14[d]: *connecting to a communication network via the at least one access point in accordance with the association response.*

Vardi discloses a UT connecting with the preferred AP via *IEEE802.11* authentication-association protocol. EX1007, 4:42-48 (searching for and connecting to AP), 7:10-20 (“wireless user terminal can be a device that executes a program (e.g., client) that uses the combined data to find usable radio resources or wireless APs and establish network connections through them....”), 7:36-43 (“establishing a WiFi connection to the Internet requires a sequence of steps, starting with the IEEE 802.11 association, continuing with security exchange, essential network IP information acquisition and accessing specific network location.”); EX1002, ¶173.

If PO contends that *Vardi*'s disclosure connecting the UT and AP via the "IEEE 802.11 association, continuing with security exchange, essential network IP information acquisition" procedure does not explicitly disclose or teach claim 14, *IEEE802.11* does. EX1002, ¶174. Claim 14 recites the steps required by an IEEE 802.11 connection procedure. *Id.* Shown below, *IEEE802.11* defines the connection procedure between a STA and an AP ("AP STA"). EX1009, 182 (FIG.4-17) (below); EX1002, ¶174. *IEEE802.11* illustrates that after the STA and AP exchange probe request and response messages, the STA transmits an association request, and the STA receives the AP's transmitted association response, at which point the STA and AP are connected to the network via the AP. EX1002, ¶174. Indeed, PO asserts the accused devices' compliance with *IEEE802.11* authentication and association procedures meet these limitations. EX1011, 117-19.

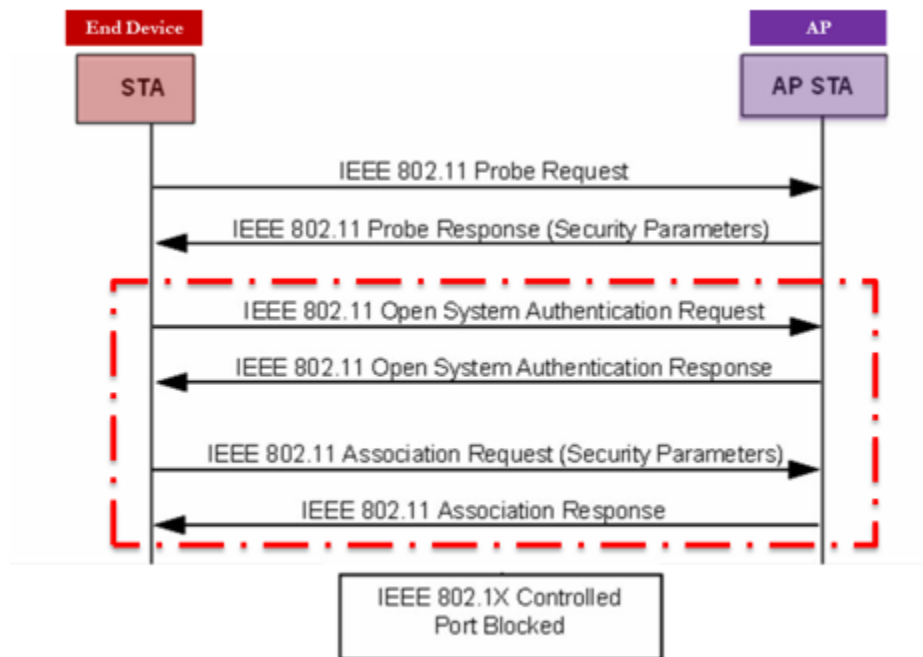


Figure 4-17—Establishing the IEEE 802.11 association

A POSITA would have found it obvious to review the underlying implementation provided by the *IEEE802.11* to establish a connection of the UT to the network because, as explained above, *Vardi* expressly instructs a POSITA that its communications and connections are compliant with *IEEE802.11*. EX1002, ¶175; §VII.B.2.vii, §VII.A, §VII.B.7.

13. Claim 17:

- i. 17[pre]: *An end device, comprising:*

Vardi discloses a UT as an end device. EX1007, 7:10-20, 3:11-13, Figs. 1, 3; EX1002, ¶177.

- ii. 17[a]: *a hardware network interface associated with an actual media access control (MAC) address;*

Vardi-IEEE802.11-Yun renders obvious Element 17[a]. EX1002, ¶178.

Vardi-IEEE802.11-Yun render obvious a hardware network interface associated with an actual MAC address for the reasons explained *supra* §VII.B.2.ii. EX1002, ¶179. Specifically, *Yun* discloses stations including NICs as hardware network interfaces for connecting to WLANs based on IEEE 802.11. EX1004, ¶[17]; EX1002, ¶179; §VII.A.

- iii. 17[b]: *a processor coupled to the hardware network interface and operable to generate a MAC address for the end device that is distinct from the actual MAC address;*
- iv. 17[c]: *a transmitter coupled to the processor and operable to transmit to an access point, a probe request that includes the generated MAC address;*
- v. 17[d]: *a receiver coupled to the processor and operable to receive, from the access point, a probe response that includes information regarding the access point,*

Vardi-IEEE802.11-Yun render obvious Elements 17[b]-[d]. EX1002, ¶180.

Elements 17[b]-[d] add nothing more to Claim 9 than well-known mobile device components: (1) processor, (2) transmitter, and (3) receiver to perform the method steps of claim 9. *Id.*; §VII.B.2.iii-v. Each of these well-known mobile device components are disclosed by *Vardi*. *Id.*

Processor: *Vardi* discloses a “processor” executes a client program for finding usable APs and establishing network connections through them. *Vardi* further explains that the system can employ a client/server architecture where the

client is a software program executed on the device. EX1007, 7:10-20; EX1002, ¶181.

Transmitter and Receiver: *Vardi* discloses “clients continuously collect radio resource information about APs detected by the wireless user terminal... clients can be executed on laptops, handheld devices (PDA’s), cellphones, or any other devices that incorporates a radio facility for wireless communication, such as WiFi.” EX1007, 9:54-62; Figs. 1, 3 (depicting UT in wireless communication—transmitting and receiving—with server and APs to connect to the Internet); EX1002, ¶182. Thus, *Vardi* discloses that each of these mobile devices incorporate “a radio facility for wireless communication,” which a POSITA would have readily understood performed both transmitting and receiving. EX1007, 3:11-13 (“connecting a wireless user terminal to a network, such as the internet,”), 3:62-63 (the device “transmitting the first set of data to a server over a network or the Internet,”), 3:4-6, 5:12-15, 9:54-62, 14:52-57 (“When client becomes active it executes an IEEE 802.11 scan for APs in reach and determines the SSID, MAC address...”), 17:61-63, Figs. 1, 3; EX1002, ¶182.

It would have been obvious to a POSITA to couple the processor, NIC, receiver, and transmitter together to facilitate the wireless transmissions disclosed by *Vardi-IEEE802.11-Yun*. EX1002, ¶183; §VII.B.2.iii-v. It would have been obvious to a POSITA to couple the components to fulfill *Vardi-IEEE802.11-Yun*’s

method and generate the arbitrary MAC address in the processor, facilitate and transmit the probe request by the NIC and transmitter, and to receive the probe response by the receiver. EX1002, ¶183. Such a combination would have been simply connecting the components to achieve the disclosed process of *Vardi-IEEE802.11-Yun*. A POSTIA would have expected to succeed in such arrangement because coupling components together then sharing information is known and routine in the computing industry. *Id*; EX1007, 20:6-18.

- vi. 17[e]: *wherein the processor is further operable to determine that the access point is an authenticated access point based, at least in part, on the information regarding the access point being indicative that the access point was connected with the end device previous to when the access point received the probe request transmitted from the transmitter,*

Vardi-IEEE802.11-Yun renders obvious Element 17[e]. EX1002, ¶184.

Element 17[e] adds nothing more to Claim 1 than a well-known mobile device component—a “processor.” §VII.B.1.v; §VII.B.13.iii (processor); EX1002, ¶185. As explained above, for Element 17[b], *Vardi* discloses the claimed “processor.” And as explained in Element 1[e], *Vardi-IEEE802.11-Yun*’s UT determines an AP is an AAP. §VII.B.1.v; EX1002, ¶185.

- vii. 17[f]: *wherein the hardware network interface is operable to connect, in response to determination that the access point is the authenticated access point, the end device to a wireless local area network provided by the access point.*

Vardi-IEEE802.11-Yun renders obvious Element 17[f]. EX1002, ¶186.

Element 17[f] adds nothing more to Claims 1, 9, 6, and 14 than a well-known mobile device component—a “hardware network interface.” §VII.B.1.vi, §VII.B.2.iii, §VII.B.7, §VII.B.12; EX1002, ¶187. As explained above, for Elements 1[e], 9[b], 6[b], 14[d], *Vardi-IEEE802.11-Yun*’s UT connects, in response to selecting an AP for connection, to a WLAN provided by the AP. *Id.*

14. Claim 18:

Vardi-IEEE802.11-Yun renders obvious Claim 18. EX1002, ¶188.

Vardi-IEEE802.11-Yun renders obvious this limitations for the same reasons explained *supra* §VII.B.8. EX1002, ¶189.

15. Claim 19:

Vardi-IEEE802.11-Yun render obvious Claim 19. EX1002, ¶190.

Claim 19 adds nothing more to Claims 4 and 11 than a well-known device component—a “processor.” §VII.B.5; EX1002, ¶191. As explained above, for Element 17[b], *Vardi* discloses the claimed “processor.” And as explained in Claims 4 and 11, *Vardi-IEEE802.11-Yun*’s UT generates the MAC address from one or more characters that are selected randomly. §VII.B.1.v; EX1002, ¶191.

16. Claim 20:

Vardi-IEEE802.11-Yun renders obvious Claim 20. EX1002, ¶192.

- i. 20[a]: *the transmitter is further operable to transmit, to the access point in response to the determination that the access point is the authenticated access point, a connection request that includes an authentic device identifier for the end device,*
- ii. 20[b]: *the receiver is further operable to receive, from the access point, an approval of the connection request, and*
- iii. 20[c]: *the hardware network interface is operable to connect the end device to the wireless LAN after the receiver receives the approval of the connection request*

Claim 20 adds nothing more respectively to Elements 1[e], 6[a], and 6[b] than well-known mobile device components—a “transmitter,” “receiver,” and “hardware network interface.” §VII.B.1vi, §VII.B.7; EX1002, ¶193. As explained above, for Elements 17[b]-[d], *Vardi-IEEE802.11-Yun* teach the claimed “transmitter,” “receiver,” and “hardware network interface.” §VII.B.13.iii-v; EX1002, ¶193. And as explained in Element 1[e] and Claim 6, *Vardi-IEEE802.11-Yun*’s UT transmits a connection request including an authentic device identifier for the end device, receives an approval of the connection request, and connects the UT to WLAN. §VII.B.1vi, §VII.B.7; EX1002, ¶193.

17. Claim 21:

Vardi-IEEE802.11-Yun renders obvious Claim 21. EX1002, ¶194.

Vardi-IEEE802.11-Yun teach connection requests includes the authentic MAC address, as explained regarding Element 20[a]. §VII.B.16.i, §VII.B.6; EX1002, ¶195.

18. Claim 22:

Vardi-IEEE802.11-Yun renders obvious Claim 22. EX1002, ¶196.

Vardi teaches obtaining a database of AAPL including information about the AAP—MAC address and SSID. §VII.B.9.i, §VII.B.2.ii, §VII.B.10; EX1007, 3:25-30; EX1002, ¶197.

Vardi teaches its UT includes a memory and storing the database information in the memory. EX1007, 7:31-36, 13:9-10; EX1002, ¶198.

It would have been obvious to a POSITA that the processor be coupled to the memory with the stored database of AAPL to provide the process access to the information in the database to facilitate the AP selection process described in *Vardi*. EX1007, 13:4-23; EX1002, ¶199; §VII.B.2.ii. A POSITA would have understood the processor required access to the database stored in the memory to perform its AP selections. EX1002, ¶199.

19. Claim 23:

Vardi discloses its UTs can be PDAs and cellphones, rendering Claim 23 obvious. EX1007, 9:54-62; EX1002, ¶¶200-201.

20. Claim 24:

Vardi-IEEE802.11-Yun teach a transmitter operable to transmit a fake MAC address. §VII.B.13.iv. Therefore, *Vardi-IEEE802.11-Yun* render obvious Claim 24 for similar reasons as Claim 3 and 10. EX1002, ¶¶202-03; §VII.B.4.

VIII. GROUND 2: *VARDI-YUN-IEEE802.11-SATISH*

A. Motivation to Combine

As explained above, the *Vardi-IEEE802.11-Yun* system renders obvious Claims 1-24. Despite explicit disclosures above regarding well-known components of mobile devices at the time of alleged invention, PO may contend the references do not disclose component connections within the mobile device. *Satish* does. EX1012, Fig. 1. A POSITA would have looked to and for components that support secure IEEE 802.11 standard communications when deploying mobile devices in an IEEE 802.11 WLAN, as taught by *Vardi*. EX1002, ¶204; EX1007, 20:6-18.

Satish satisfies the inquiry. *Satish* discloses selecting APs for connection based on matching the results of a discovery scan to a stored list of API of previously-connected APs. EX1012, 2:25-35. The information used to select the desired AP includes MAC address and SSID. *Id.*, 5:46-48, 6:13-18. *Satish* discloses its methods and systems in the context of IEEE 802.11 transmissions. EX1012, 3:55-57 (“wireless NIC 116 may comply with any wireless network standard, such as 802.11a, b, g, and n”). *Satish* also discloses a computing device that can select

APs based on comparing API of APs to stored API. *Id.*, 5:46-48, 6:13-18; EX1002, ¶205. *Satish* teaches suitable computing devices capable of performing the above-describes processes including a CPU, NIC, and memory (shown below) coupled together. EX1012, 1:33-44, 2:35-43, Fig. 1; EX1002, ¶205.

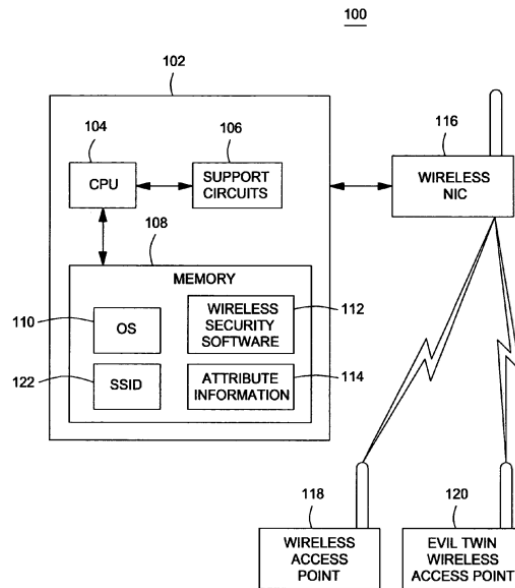


FIG. 1

Like *Vardi*, *IEEE802.11*, and *Yun*, *Satish* is in the same field of endeavor as the '384 Patent. EX1002, ¶206. The proposed combination would have been nothing more than (1) using known components, (2) inside known devices, (3) for their known purpose, (4) implementing a known standard for WLAN communication—the same IEEE 802.11 standard. It was known to a POSITA that standard compliant systems are more useful and valuable because they allow for interoperability of devices and components. EX1002, ¶206.

A POSITA would have had a reasonable expectation of success because using standardized supported components would have been common and expected, as taught by *Vardi*. EX1007, 20:6-18; EX1002, ¶207. Moreover, as explained above, *Vardi* discloses the same components and instructs a POSTIA that the components need to be operable with *IEEE802.11*. EX1002, ¶207.

B. Invalidity of Claims 17-24

1. Claim 17:

Vardi-IEEE802.11-Yun-Satish render obvious Claim 17. EX1002, 209.

- i. 17[pre]:
- ii. 17[a]:
- iii. 17[b]:
- iv. 17[c]:
- v. 17[d]:

Vardi-IEEE802.11-Yun-Satish render obvious Elements 17[pre] (to the extent its limiting) and 17[a]-[d]. EX1002, ¶210. Limitations 17[pre] and 17[a]-[d] add nothing more to Claims 1 and 9 than well-known mobile device components: (1) hardware network interface, (2) processor, (3) transmitter, and (4) receiver to perform the method steps recited in claims 1 and 9. EX1002, ¶210. Each of these well-known computing device components and corresponding claimed operations are disclosed by *Vardi-IEEE802.11-Yun* as detailed above in §VII.B.13.i-v;

however, to the extent otherwise contended, *Satish* teaches these well-known components. EX1002, ¶210.

Satish discloses a “computing device” (EX1012, 3:33) including a “central processing unit,” (*id.*, 3:35-37) and a “wireless NIC...[providing] wireless access to a communications network such as the Internet or a LAN” that can “comply with any wireless network standard, such as 802.11a, b, g and n” (*id.*, 3:49-57). EX1002, ¶211; EX1012, Fig. 1.

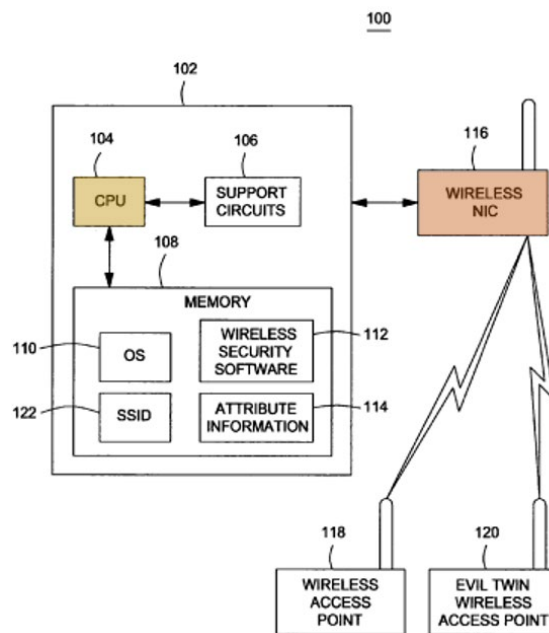


FIG. 1

As explained herein, a POSITA would have looked to and for components that support *IEEE802.11* standard communications when deploying mobile devices in *IEEE802.11* WLAN. EX1002, ¶212; §VIII.A; EX1007, 20:6-28; EX1012, 3:25-

42, 3:49-57. As described above, it would have been obvious to a POSITA to implement the computing architecture disclosed in Satish, *e.g.*, the CPU, wireless NIC, transmitter, and receiver into the UT of Vardi. §VIII.A. Satish teaches IEEE 802.11 standard compliant devices operable to scan and obtain API and use programs comparing the API to stored lists of API to select APs for connection, which a POSITA would recognize as suitable to execute the client program of Vardi. EX1002, ¶212; EX1012, 6:13-48; §VIII.A. *Satish* also discloses an IEEE 802.11 standard compliant wireless NIC, which a POSITA would understand includes transmitters/receivers to facilitate its transmissions, and also recognize as evident by the transmission lines of FIG. 1, which a POSITA would recognize as *IEEE802.11* complaint for facilitating the *IEEE802.11* communications of *Vardi*. EX1002, ¶212; EX1012, 3:49-57.

vi. 17[e]:

Vardi-IEEE802.11-Yun-Satish renders obvious limitations 17[e]. EX1002, ¶213.

Element 17[e] adds nothing more to Claim 1 than a well-known mobile device component—a “processor.” §VII.B.1.v; §VII.B.13.iii (processor), §VIII.B.1.iii (processor); EX1002, ¶214. As explained above, for Element 17[b], *Vardi* discloses the claimed “processor.” And as explained in Element 1[e], *Vardi-IEEE802.11-Yun*’s UT determines an AP is an AAP. §VII.B.1.v; EX1002, ¶214.

To the extent that PO contends *Vardi*'s processor is not explicitly disclosed, as explained in Element 17[b], it would have been obvious to implement *Satish*'s processor as part of *Vardi*'s UT to execute the client software performing the determination whether the AP is the preferred AP. EX1002, ¶¶216.

vii. 17[f]:

Vardi-IEEE802.11-Yun-Satish renders obvious limitations 17[e]. EX1002, ¶216.

Element 17[f] adds nothing more to Claims 1, 9, 6, and 14 than a well-known mobile device component—a “hardware network interface.” §VII.B.1.vi, §VII.B.2.iii, §VII.B.7, §VII.B.12; EX1002, ¶217. As explained above, for Elements 1[e], 9[b], 6[b], 14[d], *Vardi-IEEE802.11-Yun*'s UT connects, in response to selecting an AP for connection, the to a WLAN provided by the AP. *Id.*

To the extent that PO contends *Vardi-IEEE802.11-Yun*'s hardware network interface or NIC is not explicitly disclosed, as explained in Element 17[a], it would have been obvious to implement *Satish*'s wireless NIC as part of *Vardi*'s UT to send and receive transmissions, including IEEE 802.11 scanning, authentication and association, because *Vardi* teaches a POSITA to seek suitable components to enact its methods and *Satish* teaches a suitable IEEE 802.11 standard compliant NIC. EX1002, ¶218. A POSITA would seek *Satish*'s IEEE 802.11 standard

compliant NIC to maintain desired compliance with the standard, as described above. *Id.*; §VIII.A.

2. Claim 18:

Vardi-IEEE802.11-Yun-Satish teach Claim 18 for the same reasons as *Vardi-IEEE802.11-Yun* teach Claim 18. §VII.B.14; EX1002, ¶¶219-220.

3. Claim 19:

Vardi-IEEE802.11-Yun-Satish render obvious Claim 19. EX1002, ¶221.

Claim 19 adds nothing more to Claims 4 and 11 than a well-known mobile device component—a “processor.” §VII.B.5; EX1002, ¶222. As explained above, for Element 17[b], *Vardi-IEEE802.11-Yun-Satish* disclose the claimed “processor.” And as explained in Claims 4 and 11, *Vardi-IEEE802.11-Yun*’s UT generates the MAC address from one or more characters that are selected randomly. §VII.B.1.v; EX1002, ¶222.

4. Claim 20:

Vardi-IEEE802.11-Yun-Satish teach a UT including a transmitter, receiver, and NIC. §VIII.B.1.ii, §VIII.B.1.iv, §VIII.B.1.v; EX1002, ¶¶223-24. Claim 20 would have been obvious for *Vardi-IEEE802.11-Yun-Satish* for the same reasons explained above (§VII.B.16). EX1002, ¶¶223-24.

5. Claim 21:

Vardi-IEEE802.11-Yun-Satish render obvious Claim 21. EX1002, ¶225.

Claim 21 is obvious for the same reasons explained above. §VII.B.17;
EX1002, ¶¶225-26; EX1012, 5:14-24.

6. Claim 22:

Vardi-IEEE802.11-Yun-Satish render obvious Claim 22. EX1002, ¶227.

Vardi teaches a memory coupled to a processor and operable to store an AAPL including API which includes MAC address and SSID of the APs. §VII.B.18.

7. Claim 23:

Vardi teaches its device can be a PDA. EX1007, 9:56-59; §VII.B.19;
EX1012, 3:33-35. Therefore, *Vardi-IEEE802.11-Yun-Satish* renders obvious Claim
23. EX1002, ¶229-30.

8. Claim 24:

Claim 24 is obvious for the same reasons explained above. §VII.B.20.
EX1002, ¶231-32.

IX. GROUND 3: *VARDI-IEEE802.11-JALFON*

A. Motivation to Combine *Vardi-IEEE802.11-Jalfon*

Vardi, *IEEE802.11*, and *Jalfon* are all directed to the same field of endeavor in establishing secure wireless connections between a mobile device and a network through a wireless AP in accordance with IEEE 802.11. EX1002, ¶¶233-34; *KSR*, 550 U.S. at 417.

For the reasons discussed above, it would have been obvious to a POSITA to seek out or read *IEEE802.11* in view of *Vardi* because *Vardi* discloses compliance

and application of *IEEE802.11* and it would have been within the skill and knowledge of a POSITA to apply the teachings of *IEEE802.11* to implement the underlying teachings of *Vardi*. §XII.A; EX1002, ¶235.

Vardi also discloses or at least renders obvious the well-known components required by Claims 17-24, as explained above. However, to the extent it is disputed, *Jalfon* cures any deficiencies. A POSITA would have looked to and for components that support secure IEEE 802.11 standard communications when deploying mobile devices in an IEEE 802.11 WLAN, as taught by *Vardi*. EX1002, ¶236; EX1007, 20:6-18.

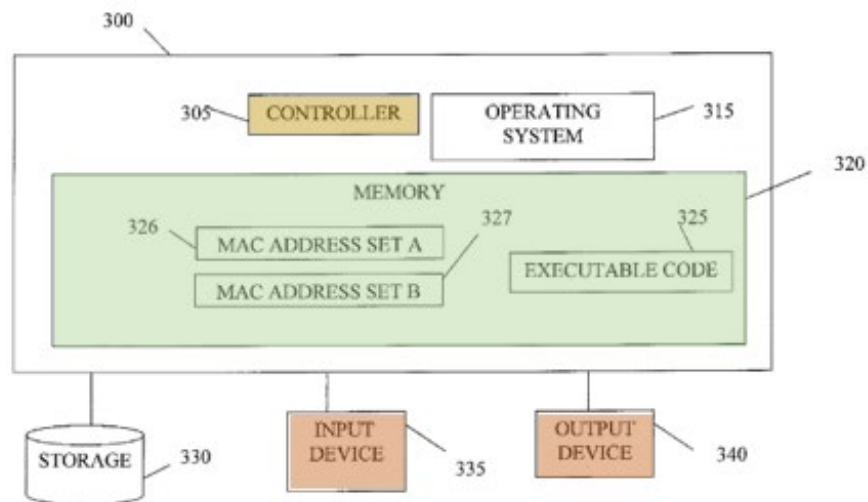
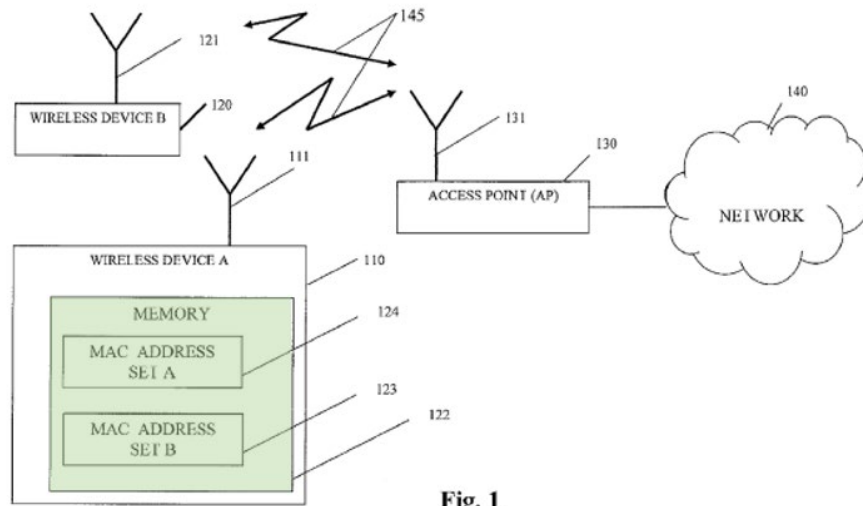
Jalfon satisfies the inquiry. EX1002, ¶237. *Jalfon* describes improving security and privacy in wireless network connections strictly in accordance with IEEE 802.11. EX1006, Abs., ¶[0017]. *Jalfon* teaches solutions to known security issues of broadcasting authentic MAC addresses in probe requests according to *IEEE802.11*. EX1006, ¶[0025]-[0026]. To solve, *Jalfon* substitutes a random MAC address in the IEEE 802.11 probe request, to prevent disclosure of the sensitive unique allocated MAC address of the device to hostile or other wireless communication devices. *Id.*, ¶[0014], ¶¶[0016]-[0020], ¶¶[0035]-[0036]. Only after the mobile device has connected with the AP *during the probe request-response* phase, does *Jalfon* further describes using the actual MAC address for the authentication phase. *Id.*, ¶¶[0020]-[0021].

It would have been obvious to a POSITA to apply *Jalfon*'s random generated MAC address and anonymous probe request transmission (compliant with *IEEE802.11*), to the *Vardi* system. EX1002, ¶238. Additionally, to the extent *Vardi*'s hardware interface component, processor, transmitter, and receiver are not explicit, *Jalfon*'s are explicit, and it would have been obvious to a POSITA to implement *Vardi*'s system using the well-known components of *Jalfon* compliant with *IEEE802.11*. To ensure proper formatting of probe request/response messages that *Vardi* discloses, a POSITA would have turned to *IEEE802.11* specification, which defines these formats, and *Jalfon* which teaches an IEEE 802.11 standard complaint transmission. *Id.*

As described above, the IEEE 802.11 is foundational to both of *Vardi* and *Jalfon*'s teachings. EX1002, ¶239. Because each system shares a foundational standard, it ensures interoperability between *Vardi* and *Jalfon* for a POSITA with minimum effort and no undue experimentation. Indeed, a POSITA would have a reasonable expectation of success in applying *Jalfon*'s probe request into *Vardi*'s wireless communication system because *Vardi*'s system already transmits probe request messages, including the MAC address as defined and taught by *IEEE802.11*. The modification would merely exchange a probe request including an actual MAC address with a probe request including a generated random MAC address. *Id.* Configuring *Vardi* to substitute the “actual” MAC address for a “random” MAC

address would have been a routine application of well-known techniques in wireless communication. *Id.*; EX1007, 7:36-40, 20:6-18; EX1006, ¶¶[0016]-[0020], ¶¶[0035]-[0036]; EX1002, ¶239.

Additionally, as noted above, it would be obvious to combine the communication device (110) of *Jalfon* with the UT of *Vardi* because *Jalfon* teaches a suitable communication device and architecture (shown below) compliant with *IEEE802.11* to perform the methods of *Vardi*, and *Vardi* invites the combination. EX1002, ¶240; EX1006, ¶[0017], ¶¶[0027]-[0029], ¶¶[0037]-[0041], Fig. 1, 3; EX1007, 20:6-18. A POSITA would look to incorporate *IEEE802.11* compliant components into the UT of *Vardi* to ensure compliance with *IEEE802.11*. EX1002, ¶240. Indeed, a POSITA would further have an expectation of success because *Jalfon* similarly teaches wireless networking according to *IEEE802.11*, including transmitting and receiving probe requests-responses and other transmissions. EX1002, ¶240, ¶233.



B. Invalidity of Claims 1-24

1. Claim 1:

Vardi-IEEE802.11-Jalfon renders obvious Claim 1. EX1002, ¶242.

i. 1[Pre]:

Vardi discloses Element 1[pre]. §VII.B.1.i.

ii. 1[a]:

Vardi-IEEE802.11-Jalfon renders obvious Element 1[a]. EX1002, ¶244.

Jalfon teaches a communication device generating a random MAC address for the device. EX1006, ¶[0035]. The random MAC address is expressly different from the allocated MAC address of the end device, and is a fake MAC address for the end device. EX1006, ¶¶[0014]-[0015]; EX1002, ¶245.

As explained (§IX.A), it would have been obvious to combine *Vardi* and *Jalfon* to include generating random MAC addresses for the UT for use in probe requests according to *Vardi-IEEE802.11*. EX1002, ¶246; *infra* §IX.B.1.iii. *Jalfon* teaches the benefits of including a random MAC address in the probe request to improve security of sensitive information (§XI.A); thus, a POSITA would have been motivated for the UT to generate a random MAC address for the end device for use in a probe request as needed. *Id.*; §VII.B.1.iii (*Vardi-IEEE802.11* teaching transmitting probe requests).

iii. 1[b]:

Vardi-IEEE802.11 teaches transmitting probe requests including a MAC address but does not disclose including a fake MAC address. §VII.B.1.iii. EX1002, ¶248.

It would have been obvious to replace the authentic MAC address of *Vardi-IEEE802.11* in the probe request with the random MAC address for the end device

taught by *Jalfon*. *Jalfon* expressly teaches transmitting a probe request including the randomized MAC (410), as shown in FIG. 4 (reproduced below). EX1006, ¶[0035], Fig. 4; EX1002, ¶249. A POSITA would have been motivated to make such a substitution to improve security during a *Vardi-IEEE802.11* probe request to protect sensitive MAC address unique to the end device. EX1006, Abs., ¶[0025], ¶[0014], ¶[0021]; EX1002, ¶249; §IX.A.

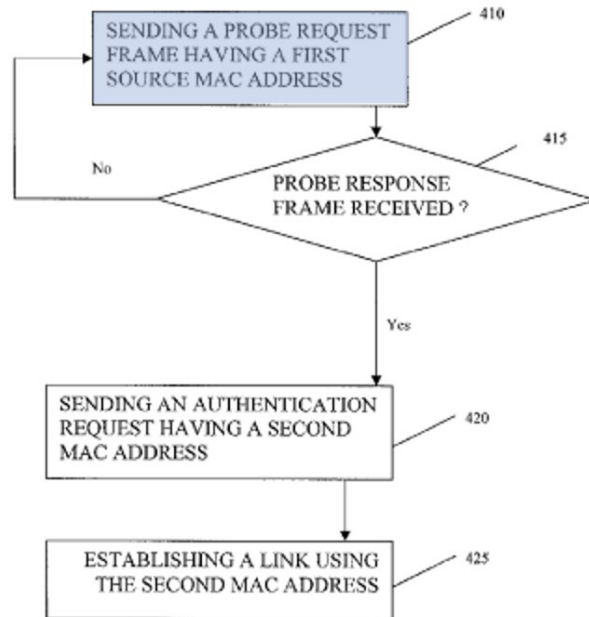


Fig. 4

A POSITA would have expected to successfully make the substitution as it would have maintained *IEEE802.11* compliance, as taught by *Jalfon*, and it would not have required additional modifications to *Vardi*'s system to substitute one

compliant MAC address for another compliant MAC address in the probe response.

EX1012, ¶250; §IX.A.

Vardi-IEEE802.11-Jalfon render obvious Element 1[b]. EX1002, ¶247.

iv. 1[c]:

Vardi-IEEE802.11 teaches Element 1[c]. §VII.B.1.iv; EX1002, ¶¶251-52.

Therefore, for the same reasons, *Vardi-IEEE802.11-Jalfon* renders obvious Element 1[c]. *Id.*

v. 1[d]:

Vardi-IEEE802.11-Jalfon renders obvious Element 1[d] for the reasons discussed above. §VII.B.1.ii. EX1002, ¶¶253-54.

vi. 1[e]:

Vardi-IEEE802.11-Jalfon render obvious Element 1[e] for the reasons discussed above. §VII.B.1.vi. EX1002, ¶¶255-56.

Alternatively, *Jalfon* discloses transmitting a connection request that includes an authentic device identifier for the end device. Specifically, *Jalfon* discloses “sending an authentication request having a second MAC address [block 420]” and “establishing a link using the second MAC address...which may be an allocated and unique address...” EX1006, ¶[0036]. Because the authentication and linking requests of *Jalfon* are IEEE 802.11 compliant and transmitted to a targeted AP (EX1006, ¶[0033], ¶[0019], ¶[0036]) “in order to establish a link”

(EX1006, ¶[0036]), a POSITA would have been motivated to substitute *Jalfon*'s IEEE 802.11 compliant authentication request with allocated/authenticated MAC address into *Vardi*, which also teaches a IEEE 802.11 compliant authentication request and provides additional implementation instructions. EX1002, ¶257.

2. Claim 9:

Vardi-IEEE802.11-Jalfon renders obvious Claim 9. EX1002, ¶258.

i. 9[pre]:

Vardi-IEEE802.11-Jalfon teaches a method under control of a UT. §VII.B.2.i; EX1002, ¶¶259-60.

ii. 9[a]:

Vardi-IEEE802.11-Jalfon renders obvious Element 9[a], as explained above. §VII.B.1.ii; EX1002, ¶¶260-61.

iii. 9[b]:

Jalfon teaches a communication device generating a random MAC address for the device. EX1006, ¶[0035] (“a MAC address...may be randomly, pseudo-randomly, or otherwise generated.”). The device includes a wireless NIC as the input/output device, as shown in Fig. 3 below (*Id.*, ¶[0040]), which is allocated a MAC address by manufacturers from IEEE and becomes the origin address of transmissions from the device, *e.g.*, the MAC address of the device (*Id.*, ¶¶[0014]-[0015]). EX1002, ¶264. The random MAC address is “distinguish[able]” from the

allocated MAC address, and therefore is distinct from the allocated MAC address of the device/NIC. EX1006, ¶¶[0014]-[0015]; EX1002, ¶264.

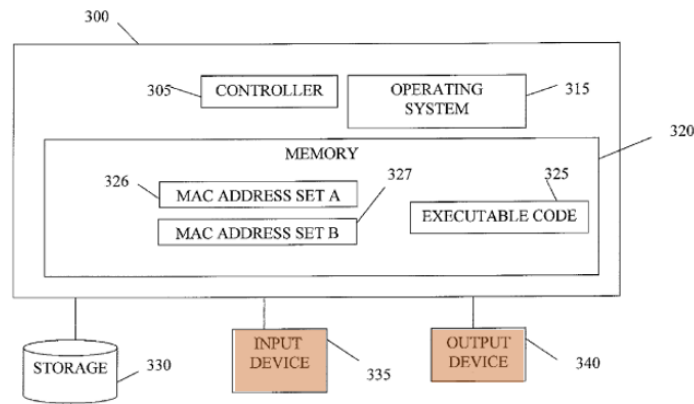


Fig. 3

It would have been obvious to combine *Vardi* and *Jalfon* to generate a fake MAC address distinct from an allocated MAC address of the UT/NIC based on the teachings of *Jalfon* for the same reasons explained above regarding obtaining a fake MAC address for probe requests. §IX.B.1.ii; EX1002, ¶265.

Vardi-IEEE802.11-Jalfon render obvious Element 9[b]. EX1002, ¶263.

iv. 9[c]:

Element 9[c] is obvious over *Vardi-IEEE802.11-Jalfon* for the same reasons as Element 1[b]. IX.B.1.iii; EX1002, ¶¶266-67.

v. 9[d]:

Element 9[d] is obvious over *Vardi-IEEE802.11-Jalfon* for the same reasons as Element 1[c]. IX.B.1.iv; EX1002, ¶¶268-69.

vi. 9[e] / 9[f]:

For the reasons explained above, Elements 9[e] and 9[f] are obvious over *Vardi-IEEE802.11-Jalfon*. §VI.B.2.vi; EX1002, ¶¶270-71.

vii. 9[g]:

Element 9[d] is obvious over *Vardi-IEEE802.11-Jalfon* for the same reasons as Element 1[e]. IX.B.1.vi; EX1002, ¶¶272-73.

3. Claim 2:

Vardi-IEEE802.11-Jalfon teaches generating a fake MAC address distinct from an actual allocated MAC address of a NIC. §VIII.B.2.iii; EX1002, ¶¶274-75.

For the same reasons explained in Element 9[b], *Vardi-IEEE802.11-Jalfon* render obvious Claim 2. EX1002, ¶¶274-75.

4. Claims 3 and 10:

Vardi-IEEE802.11-Jalfon teach including a random/fake MAC address in the probe request. §IX.B.1.iii, §IX.B.2.iv. The '384 Patent and PO's infringement allegations identify including a fake MAC address in the probe response prevents leakage of present location information. EX1001, 3:24-45, EX1011, 41. *Vardi-IEEE802.11-Jalfon* renders obvious Claims 3 and 10. EX1002, ¶¶276-77.

5. Claims 4 and 11:

Jalfon teaches generating the random MAC address includes generating the MAC address from one or more characters that are selected randomly. EX1006, ¶[0035]; EX1002, ¶279. A POSITA would understand that generating a random

MAC address includes generating the random MAC address from one or more characters selected randomly. EX1002, ¶279.

Vardi-IEEE802.11-Jalfon render obvious Claims 4 and 11. EX1002, ¶278.

6. Claims 5 and 16:

Vardi-IEEE802.11-Jalfon teach the UT transmitting connection requests including the authentic MAC address of the end device. §XI.B.1.vi, §VII.B.6 §IX.B.2.vii; EX1002, ¶281.

Vardi-IEEE802.11-Jalfon renders obvious Claims 5 and 16. EX1002, ¶280.

7. Claim 6:

Vardi-IEEE802.11-Jalfon renders obvious Claim 6, explained above. §VII.B.7; §VII.B.12; EX1002, ¶¶282-83.

To the extent it is disputed that *Vardi* discloses connecting to a wireless LAN provided by the AP, *Jalfon* explicitly discloses wireless connections with LAN. EX1006, ¶[0022] (“in order to join a wireless network, a STA connects to an AP.”); EX1002, ¶284. A POSITA would seek to provide users of the APs access to the Internet or more than peer-to-peer connection, and thus, it would be obvious to provide WLAN connectivity in a wireless system as disclosed by *Jalfon* and *Vardi*. *Id.*

8. Claims 7 and 15:

Vardi-IEEE802.11-Jalfon renders obvious Claims 7 and 15, as explained above. §VII.B.8; §VII.B.12; EX1002, ¶¶285-86.

9. Claim 8:

Vardi renders obvious Claim 8 for the same reasons explained above (§IX.B.2.ii; §VII.B.9). EX1002, ¶¶287-88.

10. Claim 12:

Vardi renders obvious Claim 12 for the same reasons explained above. §VII.B.10; EX1002, ¶¶289-90.

11. Claim 13:

Vardi renders obvious Claim 13 for the same reasons explained above. §VII.B.11; EX1002, ¶¶291-92.

12. Claim 14:

Vardi and *IEEE802.11* render obvious Claim 14 for the same reasons explained above. §VII.B.12; EX1002, ¶¶293-94.

13. Claim 17:

Vardi-IEEE802.11-Jalfon renders obvious Claim 17. EX1002, ¶295.

i. 17[pre]:

Vardi teaches a UT. §IX.B.13; EX1002, ¶296.

ii. 17[a]:

Vardi discloses a hardware network interface. §VII.B.13.ii.

To the extent PO disputes *Vardi*'s disclosure, *Jalfon* discloses a NIC (hardware network interface) as input/output (335/340) (Fig. 3, below) with an allocated (authentic) MAC address for the end device. EX1006, ¶¶[0014]-[0015], ¶[0040]. The device (110) (Fig. 1, below) can include the components of computing device 300, and therefore includes the NIC. *Id.*, ¶[0040]. It would be obvious to combine *Vardi-IEEE802.11-Jalfon* to obtain a NIC with an allocated MAC address to facilitate wireless communications of *Vardi*, as explained above. §IX.A; §IX.B.13; EX1002, ¶299. Indeed, *Jalfon* discloses an end device including an allocated MAC address and further discloses such allocations can be assigned to network interfaces. EX1006, ¶¶[0014]-[0015], ¶[0040], Figs. 1, 3; EX1002, ¶299. It would have been obvious to a POSITA to combine *Jalfon* to obtain suitable wireless transmission components for use in *Vardi* because *Vardi* teaches obtaining such components (EX1007, 20:6-18), and *Jalfon* teaches such components for use in *IEEE802.11* compliant transmissions. Such a POSITA would have been expected to succeed because *Jalfon* also teaches standard compliant components and transmissions. EX1002, ¶299.

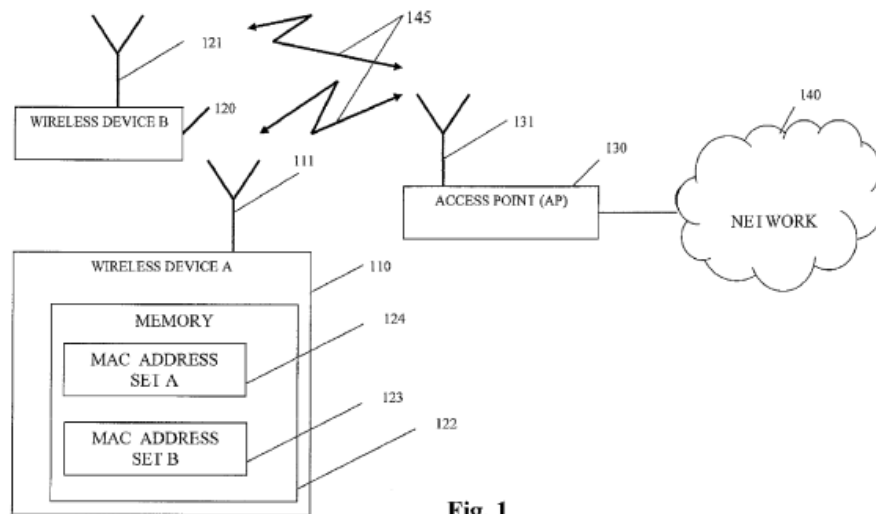


Fig. 1

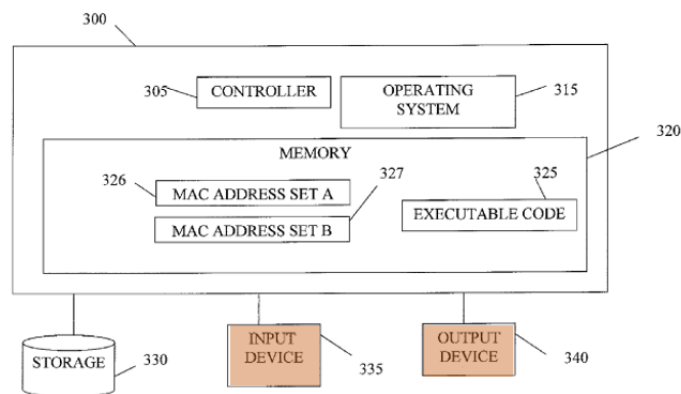


Fig. 3

Vardi-IEEE802.11-Jalfon renders obvious Element 17[a]. EX1002, ¶297.

iii. 17[b]:

Jalfon teaches processor (CPU) (305) coupled to the NIC (Fig. 3, below). EX1006, ¶[0037]; EX1002, ¶301. To the extent that Fig. 3 does not explicitly show controller 305 is coupled to NIC (335, 340), it would have been obvious to a POSITA to couple the CPU to the NIC to provide instructions to the NIC for facilitating

wireless connections with networks, as described by *Jalfon* and *Vardi*. EX1002, ¶301.

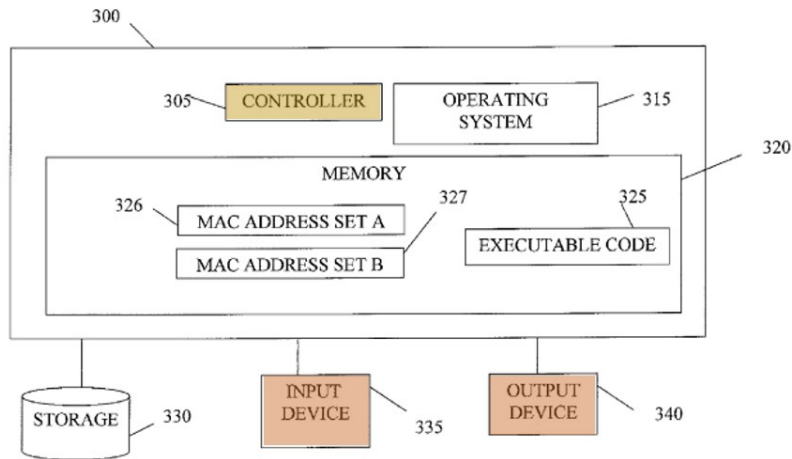


Fig. 3

Vardi-IEEE802.11-Jalfon further teach a processor adapted to generate a random MAC address distinct from the MAC address of the NIC/device, as explained above. §IX.B.2.iii; EX1002, ¶302. It would have been obvious that the CPU of *Jalfon* be operable to generate the random MAC address taught by *Jalfon* because it would have been a known component used for its intended use as disclosed by *Jalfon. Id.* In addition, a POSITA would incorporate the processor to execute its client program of *Vardi*. EX1007, 7:10-14. EX1002, ¶302; §IX.A.

Vardi-IEEE802.11-Jalfon teach Element 17[b]. EX1002, ¶300.

iv. 17[c]:

Vardi-IEEE802.11-Jalfon teach the UT transmitting to an AP a probe request including the generated MAC address for at least the reasons explained above. §IX.B.2.iv.

Jalfon teaches devices including transmitters configured to transmit probe requests. EX1006, ¶[0028]; EX1002, ¶305. It would have been obvious to a POSITA to couple the transmitter to the processor for the processor to provide the generated MAC address to the transmitter (EX1006, ¶[0028], ¶[0035]), and instruct the transmitter to send the probe request including the generated MAC address, as taught by *Jalfon* (EX1006, ¶[0028]). EX1002, ¶305. Indeed, a POSITA would have been motivated as taught by *Vardi* to seek suitable *IEEE802.11* compliant components for inclusion in the UT, and *Jalfon* expressly teaches a suitable device including components to transmit and receive probe requests and probe responses in accordance with *IEEE802.11*. EX1002, ¶305; §IX.A.

Vardi-IEEE802.11-Jalfon render obvious Element 17[c]. EX1002, ¶303.

v. 17[d]:

Vardi-IEEE802.11-Jalfon teach receiving by the UT from an AP a probe response that includes API of at least one AP. §IX.B.2.v.

Additionally, *Jalfon* teaches that wireless communication devices can include a receiver configured to receive a probe response and other messages. EX1006,

¶[0028]; EX1002, ¶308. It would have been obvious to a POSITA to couple the receiver to the processor in order for the processor to access API in probe responses, as taught by *Jalfon* (EX1006, ¶[0028], ¶¶[0035]-[0036], Fig. 4). EX1002, ¶308. Indeed, a POSITA would have been motivated as taught by *Vardi* to seek suitable *IEEE802.11* compliant components for inclusion in the UT to promote interoperability, and *Jalfon* expressly teaches a suitable device including components to transmit and receive probe requests and probe responses in accordance with *IEEE802.11*. EX1002, ¶308; §IX.A.

Vardi-IEEE802.11-Jalfon renders obvious Element 17[d]. EX1002, ¶306.

vi. 17[e]:

Vardi-IEEE802.11-Jalfon teach a processor. §IX.B.13.iii.

Vardi discloses determining an AP is an AAP as recited in Element 17[e]. §VII.B.13.vi.

Element 17[e] contributes nothing beyond Element 1[e] except the inclusion of a well-known component—a “processor.” It would have been obvious for the processor to be operable to perform the selecting functions described in *Vardi*, including determining an AP is an AAP by comparing API obtained in the probe response to stored API of previously-connected APs, because a POSITA understands comparing sets of information is a known function of processors and it

would have been using a generic component for its intended purpose as explicitly taught by *Jalfon*. EX1002, ¶312; EX1007, 20:6-18.

Vardi-IEEE802.11-Jalfon renders obvious Element 17[e]. EX1002, ¶309.

vii. 17[f]:

Vardi-IEEE802.11-Jalfon renders obvious Element 17[f]. EX1002, ¶313.

Vardi-IEEE802.11-Jalfon teach a NIC having an allocated MAC address.

IX.B.13.ii.

Vardi-IEEE802.11-Jalfon also teach connecting the UT to a WLAN communication network provided by the AP in response to determining the AP is an AAP. §IX.B.1.vi, §IX.B.7, §IX.B.12.

It was known that NICs facilitate wireless connections, including to wireless LANs provided by APs. EX1002, ¶316. *Vardi-IEEE802.11-Jalfon* teaches transmitting a connection request to the AP determined to be an AAP and then connecting to the WLAN provided by the AAP. §VII.B.1.vi, §VI.B.7. It would have been obvious to a POSITA for the NIC to be adapted to perform the methods described in *Vardi* and be operable to connect to a WLAN provided by the AP, because it is using a known component for its intended use to achieve an expected result. EX1002, ¶316.

14. Claim 18:

Vardi-IEEE802.11-Jalfon teach a Wi-Fi AP providing access to a Wi-Fi network for the reasons explained above. §IX.B.8; EX1002, ¶318. *Vardi-IEEE802.11-Jalfon* render obvious Claim 18. EX1002, ¶317.

15. Claim 19:

Vardi-IEEE802.11-Jalfon teach a processor. §IX.B.13.iii.

Generating MAC addresses from one or more characters selected randomly was known. §IX.B.5; EX1002, ¶321. Therefore, it would have been obvious for the processor to be operable to generate a MAC address from one or more characters that are selected randomly, as taught by *Jalfon*, including as being a known and obvious variant. §XI.B.13.iii, §XI.B.5; EX1002, ¶321.

Vardi-IEEE802.11-Jalfon renders obvious Claim 19. EX1002, ¶319.

16. Claim 20:

Vardi-IEEE802.11-Jalfon renders obvious Claim 20. EX1002, ¶322.

i. 20[a]:

Vardi-IEEE802.11-Jalfon teach a UT transmitting to an AP in response to a determination that the AP is the AAP, a connection request that includes the actual MAC address of the UT/NIC. §IX.B.1.vi.

Vardi-IEEE802.11-Jalfon further teaches a UT including a transmitter operable to transmit. §IX.B.13.iv.

Therefore, it would have been obvious to a POSITA to adapt the transmitter to transmit the connection request of *Vardi-IEEE802.11-Jalfon* because it is using a known component for a known function to achieve an expected result. §IX.B.1.vi; EX1002, ¶¶323-25; EX1007, 20:6-18.

ii. 20[b]/20[c]:

Vardi-IEEE802.11-Jalfon teach receiving from an AP an approval of the connection request and connecting the UT to the WLAN after receiving the approval of the connection request. §IX.B.7; §IX.B.12.

Vardi-IEEE802.11-Jalfon further teaches a receiver operable to receive (§IX.B.13.v) and a NIC operable to connect to a WLAN provided by the AP (§IX.B.13.vii).

It would have been obvious to a POSITA to adapt the receiver and NIC to further perform the methods of *Vardi* because such functionality is a known and obvious variation to the methods above from *Vardi-IEEE802.11-Jalfon* (§IX.B.7; §IX.B.12). EX1002, ¶328; EX1007, 20:6-18.

17. Claim 21:

Vardi-IEEE802.11-Jalfon render obvious Claim 21 by teaching the authentic device identifier in the connection request includes an actual MAC address of the UT. §IX.B.16.i, §IX.B.6; EX1002, ¶¶329-30.

18. Claim 22:

Vardi teaches a memory coupled to the processor and operable to store an AAPL including API regarding APs, wherein the API includes the MAC address and/or SSID of the APs. §VII.B.18.

Jalfon also discloses a memory (320) coupled to a processor and operable to store MAC addresses, shown below in FIG. 3. EX1006, ¶¶[0028]-[0029], ¶¶[0037]-[0038], Fig. 3; EX1002, ¶333.

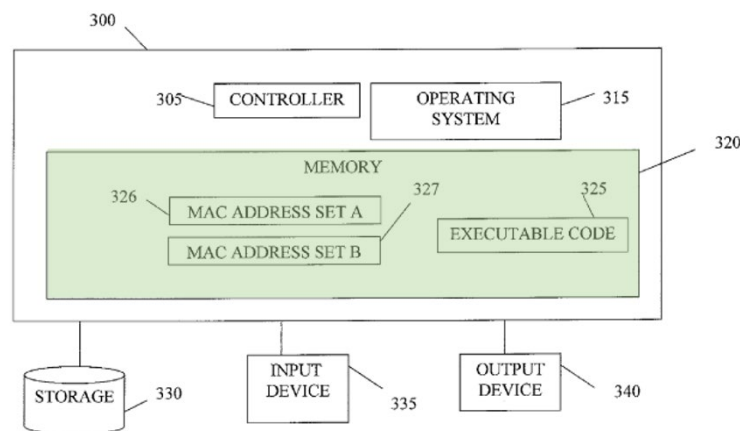


Fig. 3

It would have been obvious to a POSITA for the memory of *Vardi-IEEE802.11-Jalfon* be operable to store an AAPL of API regarding APs including the MAC address and/or SSID of the APs because *Jalfon* teaches its memory is configured to store information, and because *Vardi* explicitly teaches storing such AAPL information in a memory (EX1007, 7:31-36, 13:9-10). EX1002, ¶334.

Further, *Vardi* teaches accessing the information for processing functions, thus, it would have been obvious to couple the memory to the processor. EX1002, ¶334.

Vardi-IEEE802.11-Jalfon render obvious Claim 22. EX1002, ¶331.

19. Claim 23:

Vardi-IEEE802.11-Jalfon teaches the UT can be a PDA; and therefore, renders obvious Claim 23. EX1007, 9:54-62; EX1002, ¶¶335-36.

20. Claim 24:

Vardi-IEEE802.11-Jalfon teach a transmitter operable to transmit a probe request including a fake MAC address instead of the actual MAC address of the UT. §IX.B.13.iii; EX1002, ¶¶337-38.

Therefore, for the same reasons as Claims 3 and 10, Claim 24 is obvious. *Id.*

X. NO DISCRETIONARY DENIAL IS WARRANTED

A. *Fintiv* Factors

Discretionary denial is not favored because, if instituted, there will be limited, if any, overlap between the issues presented in here and the Texas Action.

Likelihood of a stay is neutral. The Texas Asserted Patents are at issue in the Texas action. Petitioner is simultaneously challenging all claims of the Texas Asserted Patents, including unasserted claims. Institution of the four IPR petitions would thus enable the Board to resolve core issues in, if not completely moot, the Texas Action. As such, the District Court likely would stay the case pending the

outcome of the IPRs in view of potentially substantial judicial efficiencies to be gained. Indeed, Judge Gilstrap—presiding over the Texas Litigation—granted a stay in a similar patent infringement case where all claims of the asserted patent, including the non-asserted claims, were subject to IPR. *Comm’ns Techs., Inc. v. Samsung Elecs. Am., Inc.*, No. 2:21-cv-00444-JRG (E.D. Tex. Feb. 2, 2023).

Trial is currently scheduled in the Texas Action for November 3, 2025, just ahead of the Board’s projected statutory deadline of February, 2026. Therefore, due to likelihood of slippage of dates, this factor is neutral.

At the time of filing, there has been minimal investment in the Texas Action. Discovery is just beginning, and the parties are yet to file any dispositive motions, brief claim construction, or conduct expert discovery. Therefore, the lack of investment between the parties and the court in the Texas Action weighs heavily against discretionary denial.

Overlap between issues weighs against discretionary denial. Petitioner stipulates that, if IPR is instituted, Petitioner will not pursue in the Texas Action the same grounds asserted in this Petition. Moreover, this Petition challenges all claims not just the Asserted Claims, such that their validity will not be addressed at all in that proceeding.

As demonstrated in the above three Grounds, although Petitioner and PO are the parties in the Texas Action, the exceptionally strong merits presented herein warrant the Board to not discretionarily deny institution.

B. *Becton Dickinson* – Not the Same or Substantially the Same Art

The only reference cited herein previously before the USPTO is *Jalfon* (EX1006), which is part of Ground 3. *Jalfon* was not discussed or cited during the prosecution of the '384 Patent.

Instead, *Jalfon* was discussed as a primary reference during the prosecution of a parent application resulting in the '005 Patent. EX1014. There, applicant was unable to distinguish the limitations the Examiner identified as being taught by *Jalfon*, but instead narrowed a different portion of the claim; particularly, the AP determination, to overcome the secondary reference (not cited herein). The reasons for allowance reflect this and do not describe any limitation the present Petition, or the Examiner during '005 Patent prosecution, cites *Jalfon* as teaching. EX1014, 402.

In contrast, during prosecution for the '384 Patent, *Jalfon* was never referenced, but is only identified on the face of the '384 Patent. EX1001, (56). Additionally, the notice of allowance for the '384 Patent similarly identified the determining that the AP is an AAP as a point of novelty. EX1003, 19. To the extent the Notice of Allowance identified the limitation a fake [MAC]

address...transmitting, by the end device to an access point,” as shown herein, that was already known to POSITAs by, for example, *Yun*. §VII.B.1.ii.

Here, the Petition relies on *Jalfon* for only one Ground. Importantly, *Jalfon* is being presented in a new light as being used as a secondary reference proving POSITA’s motivations to modify *Vardi-IEEE802.11* disclosures to specifically address limitations that were not overcome during the prosecution of ’005 Patent or cited for the ’384 Patent. *Vardi* was never before the USPTO and is cited as teaching the specific limitations identified in both the ’005 and ’552 Patent’s reasons for allowance. Thus, the art being considered by the PTO in this proceeding has not been considered previously – specifically, a separate reference (*Vardi*) being modified by *Jalfon* to achieve an obvious method or apparatus. Therefore, Petitioner is presenting *Jalfon* in a never before considered manner that is distinct from the examiner’s assessment of *Jalfon* as a primary reference.

Thus, the new ground, and proposed prior art as a whole, was never presented before to the USPTO and due to the strength of the ground and the newly identified reference (*Vardi*), discretionary denial is not warranted.

XI. CONCLUSION

Since there is a reasonable likelihood that Petitioner would prevail, this
Petition should be granted.

Respectfully submitted,

Dated: September 4, 2024

By: /Walter D. Davis, Jr/

Walter D. Davis, Jr.
Registration No.: 45,137
BLANK ROME LLP
1825 Eye Street, NW
Washington, DC 20006-5403
Tel: (202) 420-4847
Fax: (202) 478-0914
Email: walter.davis@blankrome.com

Counsel for Petitioner

CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24, the undersigned attorney for Petitioner certifies that the document contains 13,991 words in 14-point Times New Roman font, excluding the parts of the document that are exempted by 37 C.F.R. §42.24(a)(1), according to the word count tool in Microsoft Word.

Dated: September 4, 2024

By: /Walter D. Davis, Jr./

Walter D. Davis, Jr.
Registration No.: 45,137
BLANK ROME LLP
1825 Eye Street, NW
Washington, DC 20006-5403
Tel: (202) 420-2200

Counsel for Petitioner

CERTIFICATE OF SERVICE

I hereby certify that on September 4, 2024, a true and correct copy of the foregoing *PETITION FOR INTER PARTES REVIEW* including exhibits was filed with the Patent Trial and Appeal Board Case Tracking System (P-TACTS) and served via overnight FedEx to the Patent Owner at the correspondence addresses of record as follows:

154241 – IP Spring – A1
161 N. Clark St.
Suite 1700
Chicago, IL
United States

A courtesy copy was also served on PO's counsel of record in the Texas Action via email.

By: /Walter D. Davis, Jr./

Walter D. Davis, Jr.
Registration No.: 45,137
BLANK ROME LLP
1825 Eye Street, NW
Washington, DC 20006-5403
Tel: (202) 420-2200

Counsel for Petitioner