

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.

IPR2024-01369
Patent 9,961,552

PETITIONER'S REPLY TO
PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

	Page
I. Patent Owner Interprets “‘Authenticated’ Access Point” in a way that is Inconsistent with its Interpretation of that Term in its Infringement Contentions	1
II. Two Petitions Challenging the Same Patent is Warranted.....	4
III. Patent Owner’s Characterization of the Co-Pending Litigation is Misleading	5

TABLE OF AUTHORITIES

Page(s)

Cases

<i>Amazon.com, Inc. v. Barnesandnoble.com, Inc.</i> , 239 F.3d 1343 (Fed. Cir. 2001)	3
<i>Solas OLED Ltd. v. Samsung Display Co., Ltd.</i> , No. 2:19-CV-00152- JRG, 2020 WL 4040716 (E.D. Tex. Mar. 17, 2020)	6

LISTING OF EXHIBITS

<u>Exhibit No.</u>	<u>Exhibit Title</u>
Exhibit 1001	U.S. Patent 9,961,552, filed May 01, 2018
Exhibit 1002	Declaration of Dr. Harry Bims
Exhibit 1003	Prosecution File History for U.S. Patent 9,961,552
Exhibit 1004	WO 2007/086705 (Yun), filed January 26, 2007
Exhibit 1005	US Patent Application Publication 2003/0177267 (Orava), filed December 5, 2002
Exhibit 1006	[RESERVED]
Exhibit 1007	U.S. Patent 8,126,476 (Vardi), filed July 25, 2008
Exhibit 1008	Microsoft Computer Dictionary 5 th Edition (Excerpts)
Exhibit 1009	IEEE Std 802.11TM-2012 (IEEE802.11), dated March 29, 2012
Exhibit 1010	US Application Publication 2012/0257536 (Kholaf), filed April 8, 2011
Exhibit 1011	Infringement Contentions for U.S. Patent 9,961,552
Exhibit 1012	[RESERVED]
Exhibit 1013	[RESERVED]
Exhibit 1014	[RESERVED]
Exhibit 1015	[RESERVED]
Exhibit 1016	Email from Trials@uspto.gov, dated January 23, 2025, Re: IPR2024-01368, -01369
Exhibit 1017	Patent Owner Secure Wi-Fi's P.R. 4-2 Disclosure of Proposed Claim Constructions

Exhibit 1018	Petitioner Samsung's P.R. 4-2 Disclosure of Proposed Claim Constructions
--------------	--

CLAIM LISTING

Element Designation	Claim Language
Independent Claim 10	
10[pre]	A method performed by a device, the method comprising:
10[a]	receiving, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;
10[b]	receiving, from the server, a fake device identifier for the device, wherein the received fake device identifier includes at least one of one or more random numbers or one or more random characters to falsely identify the device in a probe request frame;
10[c]	transmitting, to at least one access point, the probe request frame that includes the received fake device identifier;
10[d]	receiving, from the at least one access point in response to the transmitting the probe request frame, a probe response frame that includes information regarding the at least one access point;
10[e]	determining, in response to the receiving the probe response frame and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point, wherein the determining whether the at least one access point is the authenticated access point includes determining whether the information regarding the at least one access point is included in the authenticated access point list that is received from the server; and
10[f]	transmitting, to the at least one access point in response to a determination that the at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the device.
Claim 11	
Claim 11	The method of claim 10, wherein the receiving the fake device identifier includes receiving a fake media access control (MAC) address.
Claim 12	
Claim 12	The method of claim 10, wherein the determining whether the information regarding the at least one access point is included in the authenticated access point list comprises determining whether the at least one access point is under control of the server.
Claim 13	

Claim 13	The method of claim 10, further comprising: storing the authenticated access point list in a memory.
Claim 14	
14[pre]	The method of claim 10, further comprising:
14[a]	receiving, from the at least one access point, an approval of the connection request;
14[b]	transmitting, to the at least one access point in response to the receiving the approval of the connection request, an association request;
14[c]	receiving, from the at least one access point, an association response to the association request; and
14[d]	connecting to a communication network via the at least one access point in accordance with the association response.
Independent Claim 15	
15[pre]	A method performed by a device, the method comprising:
15[a]	receiving, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;
15[b]	generating a fake device identifier for the device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters;
15[c]	transmitting, to at least one access point, a probe request frame that includes the fake device identifier;
15[d]	receiving, from the at least one access point in response to the transmitting the probe request frame, a probe response frame that includes information regarding the at least one access point;
15[e]	determining, in response to the receiving the probe response frame and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point, wherein the determining whether the at least one access point is the authenticated access point includes determining whether the information regarding the at least one access point is included in the authenticated access point list that is received from the server, and wherein the determining whether the information regarding the at least one access point is included in the authenticated access point list includes determining whether the at least one access point is under control of the server; and

15[f]	transmitting, to the at least one access point in response to a determination that the at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the device.
Claim 16	
Claim 16	The method of claim 15, wherein the generating the fake device identifier includes generating a fake media access control (MAC) address.
Claim 17	
Claim 17	The method of claim 15, wherein the information regarding the at least one access point includes at least one of a media access control (MAC) address of the at least one access point or a service set identifier (SSID) of the at least one access point.
Claim 18	
Claim 18	The method of claim 15, wherein the determining whether the at least one access point is the authenticated access point further includes determining whether the at least one access point was previously connected with the device.
Claim 19	
Claim 19	The method of claim 15, further comprising: storing the authenticated access point list, received from the server, in a memory.
Claim 20	
20[pre]	The method of claim 15, further comprising:
20[a]	receiving, from the at least one access point, an approval of the connection request
20[b]	transmitting, to the at least one access point in response to the receiving the approval of the connection request, an association request;
20[c]	receiving, from the at least one access point, an association response to the association request; and
20[d]	connecting to a communication network via the at least one access point in accordance with the association response.
Independent Claim 21	
21[pre]	A method performed by a device, the method comprising:
21[a]	receiving, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;

21[b]	generating a collection that includes at least one of one or more random numbers or one or more random characters to provide a fake device identifier for the device to falsely identify the device in a probe request frame;
21[c]	transmitting, in a search for at least one available access point around the device, the probe request frame that includes the fake device identifier;
21[d]	receiving, from at least one access point around the device in response to the transmitting the probe request frame, a probe response frame that includes information regarding the at least one access point;
21[e]	determining, in response to the receiving the probe response frame and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point, wherein the determining whether the at least one access point is the authenticated access point includes determining whether the information regarding the at least one access point is included in the authenticated access point list, and wherein the determining whether the information regarding the at least one access point is included in the authenticated access point list includes determining whether the at least one access point is under control of the server; and
21[f]	transmitting, to the at least one access point in response to a determination that the at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the device.
Claim 22	
22[pre]	The method of claim 21, wherein:
22[a]	the generating the collection that includes the at least one of one or more random numbers or one or more random characters comprises configuring the collection as a fake media access control (MAC) address, and
22[b]	the fake device identifier includes the fake media access control (MAC) address.
Claim 23	
Claim 23	The method of claim 21, further comprising: storing the fake device identifier in a memory.
Independent Claim 24	
24[pre]	A system, comprising:

24[a]	a processor;
24[b]	at least one communication interface;
24[c]	a transmitter to transmit, to at least one access point via the at least one communication interface, a probe request frame that includes a fake device identifier for a device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters;
24[d]	a receiver to:
24[d][i]	receive, from the at least one access point via the at least one communication interface, a probe response frame that includes information regarding the at least one access point; and
24[d][ii]	receive, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;
24[e]	a memory to store the information regarding the at least one access point, and the authenticated access point list; and
24[f]	a determination unit to determine, under control of the processor and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point and is under control of the server,
24[g]	wherein to determine whether the at least one access point is the authenticated access point and is under control of the server, the determination unit determines whether the information regarding the at least one access point is included in the authenticated access point list, and
24[h]	wherein the transmitter further transmits to the at least one access point, a connection request that includes an authentic device identifier for the device, in response to a determination by the determination unit that the at least one access point is the authenticated access point and is under control of the server.
Claim 25	
Claim 25	The system of claim 24, wherein the fake device identifier includes a fake media access control (MAC) address.
Claim 26	
Claim 26	The system of claim 24, further comprising: a fake device identifier generation unit to generate, under control of the processor, the fake device identifier.
Claim 27	

Claim 27	The system of claim 24, wherein the memory further stores the fake device identifier.
Claim 28	
Claim 28	The system of claim 24, wherein the at least one access point includes a Wi-Fi access point, and wherein the at least one communication interface is configured for communication with a Wi-Fi network

Pursuant to the Board's January 23, 2025, authorization (EX1016), Petitioner hereby files this Reply to address Patent Owner's arguments regarding the construction of the term "'authenticated' access point," Petitioner's filing of two Petitions challenging the same patent, and the record for the parallel district court action between Patent Owner and Petitioner ("Co-Pending Litigation") (*see* Paper 1 at 1 (Related Matters)).

I. PATENT OWNER INTERPRETS "'AUTHENTICATED' ACCESS POINT" IN A WAY THAT IS INCONSISTENT WITH ITS INTERPRETATION OF THAT TERM IN ITS INFRINGEMENT CONTENTIONS

In the current IPR proceeding, with validity at issue, Patent Owner proposes interpreting "'authenticated' access point" as an access point that has been "authenticated" by a "process of verifying the identity of an entity, using known, trusted, and verifiable information, before granting access to a resource" or that has been proved to be "real, true, or what people say it is." Paper 7 at 21-22. And according to Patent Owner, *Vardi* does not disclose such an "authenticated access point." Paper 7 at 22-29. But Patent Owner interpreted the same term much

differently in its infringement contentions from the Co-Pending Litigation.¹

The Accused Product confirms the received SSID information and/or other information from probe responses with access point information stored in its memory. Once confirmed that there is a probe response from an access point with which the Accused Product was connected previously, the Accused Product initiates a connection to

the access point using an authenticated device identifier, such as a persistent MAC address that was used for a prior connection with the access point.

The Accused Products maintain a list of previously-connected access points which is matched to the access point's SSID received in the probe response. Each previously-connected access point is linked to a persistent MAC address for connecting to that access point.

EX1011 at 45-57 (annotated). As demonstrated in the above excerpt from Patent Owner's infringement contentions, Patent Owner explicitly stated that determining an access point is an authenticated access point only requires "confirm[ing]" the SSID and/or other information from the probe response with access point information stored in its memory. *Id.*, 52. That is, an end device checks its memory using the received SSID and other information to see whether the access point previously provided connectivity to the end device. Patent Owner identified no further step was necessary to "verify the identity of an entity, using known, trusted, and verifiable information" or "to prove that something is real, true, or what people say it is."

¹ To provide a complete record, Petitioner hereby includes Patent Owner's and Petitioner's respective Disclosures of Proposed Claim Construction exchanged in the Co-Pending Litigation. *See* EX1017 (Patent Owner); EX1018 (Petitioner).

Patent Owner cannot interpret a claim term one way for infringement and another for validity. *Amazon.com, Inc. v. Barnesandnoble.com, Inc.*, 239 F.3d 1343, 1351 (Fed. Cir. 2001) (“A patent may not, like a ‘nose of wax,’ be twisted one way to avoid anticipation and another to find infringement.”). When applying Patent Owner's infringement contentions logic to *Vardi*, it is clear that *Vardi* teaches an “authenticated access point.”

For example, *Vardi* discloses its user terminal obtains and stores lists of access points that previously provided connectivity to the end device, including MAC addresses and/or SSIDs of those access points. *See* Paper 1 at 25-34 (Claim Element 10[a]); EX1007, 4:37-45, 7:23-32, 12:24-30, 14:52-57, 13:4-23; EX1002, ¶¶330-75. The information on the list is generated through scans from the user terminal by caching information from previous connections or by conducting scans of available access points, providing the information to a server, and receiving the list back from the server. *Id.*, 25-27; EX1007, 12:24-30, 14:52-57, 13:4-23. Then, during a network connection process, the information obtained from the IEEE 802.11 scan is compared to the list of access points that provided connectivity to the end device and is used to confirm the access point had previously provided connectivity to the user terminal, based on, for example MAC address and SSID. *See, e.g.*, EX1007, 12:24-30, 14:42-57, 13:4-18, 13:19-23 (“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 with the highest RSSI value for connection"); EX1002, ¶¶414-77;

Paper 1 at 51-56 (Claim Elements 10[e], 10[f]). In that sense, applying Patent Owner's infringement-motivated interpretation, *Vardi* authenticates the access point before using it to provide connectivity to the user terminal.

II. TWO PETITIONS CHALLENGING THE SAME PATENT IS WARRANTED

Patent Owner contends that the Board should exercise its discretion to deny institution, because Petitioner filed two Petitions to challenge the '552 Patent. *See* Paper 7 at 43. Notably, Patent Owner argues that Petitioner failed to rank the two petitions or explain why the Board should institute two petitions challenging the same patent. Petitioner asserts that the ranking and explanation was at least implicitly included in the Petition. For example, the Petition explained that institution should not be denied due to the *Fintiv* factors and the Co-Pending Litigation. The *Fintiv* factors are relevant because all the claims involved in the Co-Pending Litigation are challenged in this Petition. Paper 1 at 97 (explaining this Petition challenges more than Co-Pending Litigation's Asserted Claims). Thus, the Petition suggests that claims at issue in the Co-Pending Litigation, as identified in the infringement contentions, are more important than independent claims not asserted against Petitioner. *See* EX1011.

Implicitness aside, Petitioner hereby affirms that this Petition (IPR2024-01369) ranks first, because it covers all of the claims identified in Patent Owner's

Infringement Contentions. *See* EX1011 (identifying independent claims 10, 15, 21, and 24 and claims depending therefrom). IPR2024-01368 ranks second, because it covers claims that have not been asserted against Petitioner in the Co-Pending Litigation, and due to those claims focus on the perspective of a server or access point, do not appear to have any chance of being asserted.

The Petitions are focused on different sides of a three-way exchange with each side performing unique actions based on its perspective. Although the three-way exchange involves the same connection process between an end device and a network, the Petitions do not include any overlap in the perspective of the actions. For example, this Petition focuses on the perspective of the end device and its method steps, while IPR2024-01368 focuses on the perspective of the server and the access points and the steps each separate device performs. Finally, the separate Petitions should both be instituted because Judge Gilstrap (Co-Pending Litigation Judge) found the fact that all claims of the asserted patent were instituted in an IPR pertinent in granting a stay in a similarly disposed case. *See* Paper 1 at 95-96.

III. PATENT OWNER'S CHARACTERIZATION OF THE CO-PENDING LITIGATION IS MISLEADING

As detailed below, Patent Owner's arguments regarding Fintiv factors 1 and 3 are misleading.

Factor 1: Patent Owner wrongly asserts that it is unlikely the district court will grant a stay due to the previously rejected stay motion. Paper 7 at 45-46. This

mischaracterizes the issue. The initial stay motion was filed within a week of the Petition. As recognized by the Court, it is not unusual for courts to deny a motion to stay without prejudice before institution. EX2001 at 2. But the Co-Pending Litigation Court still invites parties to file early motions to stay because the Court awards weight to the timing of the moving party's *initial* motion to stay making the renewed post-institution stay more likely to be granted. *See Solas OLED Ltd. v. Samsung Display Co., Ltd.*, No. 2:19-CV-00152-JRG, 2020 WL 4040716, at *2 (E.D. Tex. Mar. 17, 2020) (acknowledging that “the Court must accord some weight to the timing of Samsung’s Original Motion”).

Factor 3: The parties’ investment in the parallel proceedings is not as extensive as Patent Owner asserts. The parties’ claim constructions were just exchanged this week, with opening briefs not due until March 31, 2025, which ultimately will result in a *Markman* order after **May 12, 2025** (hearing). And only after *Markman* will the parties be submitting Final Infringement and Invalidity Contentions. Indeed, Patent Owner has yet to even serve its necessary supplemental infringement contentions based on Petitioner’s confidential information. Significant work remains by the parties in the Co-Pending Litigation, including fact discovery, *Markman*, Final Invalidity Contentions, and expert discovery. All to occur after the Board’s **March 26, 2025** Institution Decision deadline.

Respectfully submitted,

Dated: January 30, 2025

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 SERVICE

I hereby certify that on January 30, 2025, a true and correct copy of the foregoing *PETITIONER'S REPLY TO PATENT OWNER'S PRELIMINARY RESPONSE* including exhibits was filed with the Patent Trial and Appeal Board Case Tracking System (P-TACTS), with a copy served via electronic mail to the following email addresses, as authorized in Patent Owner's Mandatory Notice (Paper 5):

jtice@bdiplaw.com

SecureWiFi_Samsung@bdiplaw.com

Dated: January 30, 2025

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