

EXHIBIT A

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

As set forth below, the Accused Products and their referenced structures and functions are designed to and do operate in an infringing manner and perform the claimed systems and methods each and every time an Accused Product is used as intended (i.e., to connect to a Wi-Fi network). The following claim chart sets forth exemplary evidence demonstrating Secure Wi-Fi's infringement theories, and showing where in the Accused Products each element of the asserted claims is found. The evidence included below for particular Accused Product(s) is exemplary, and is representative of infringement by other Accused Products, including those that use Android OS 10 or above or Wear OS 3 or above, as those products employ the same or similar structures and functionality in the same manner.

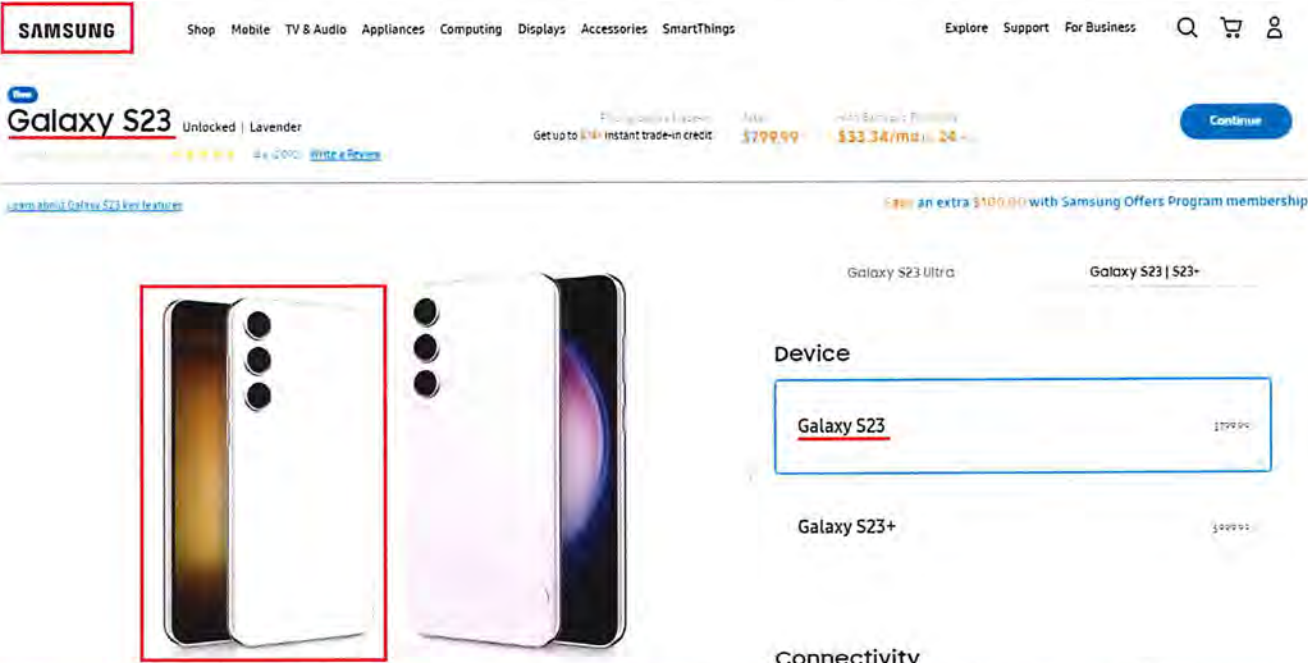
This claim chart specifically addresses infringement of the asserted claims by Samsung's Accused Products using Android OS 10 or above or Wear OS 3 or above. These infringement contentions are illustrative rather than exhaustive. Although the Samsung Accused Products may differ in some respects, for example use of different operating systems, SOCs, mobile platforms, chipsets, and/or connectivity systems, any differences are not relevant with respect to the asserted claims of the '384 patent or Secure Wi-Fi's infringement allegations. On information and belief, the evidence cited in this claim chart is representative of how the other accused products would operate under similar conditions. Excerpts below may be annotated to highlight certain information, aid in readability, or for some other purpose. The annotations are not limiting.

The Accused Products listed herein are not exhaustive. Secure Wi-Fi accuses any Samsung products with substantially similar MAC Randomization functionality to the expressly listed Accused Products. Moreover, it may be that the same underlying products have multiple identification numbers based on, *inter alia*, differences in geographic sales locations, customers, product colors, or other features that do not affect the structure and operation of such products and the infringement allegations herein. Secure Wi-Fi asserts that any such products infringe the asserted claims for the same reasons as identified herein.

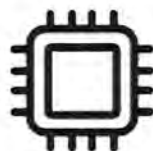
This infringement analysis is preliminary, and Secure Wi-Fi's investigation into Samsung's infringement is ongoing. Secure Wi-Fi reserves the right to provide additional theories under which Samsung products infringe this patent.

Secure Wi-Fi reserves the right to supplement or modify these contentions as appropriate upon receipt of further information and discovery, or as otherwise permitted by the Court. Secure Wi-Fi has not completed its investigation of the facts in this case. For example, Defendant Samsung has not yet made complete production of technical documents for the Accused Products and algorithms discussed herein. Secure Wi-Fi reserves the right to provide additional theories under which Samsung products infringe this patent. This chart is being provided pursuant to the schedule in this case, and Secure Wi-Fi specifically reserves all rights to amend or supplement this claim chart with further evidence obtained during the further course of discovery.

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

U.S. Patent No. 10,694,384	Samsung Accused Products
1. A method performed under control of an end device, the method comprising:	To the extent the preamble is limiting, the Accused Products practice a method performed under control of an end device. The Accused Products include Android OS 10 or above or Wear OS 3 or above. Each Accused Product includes an SoC and Wi-Fi connection functionality. As a specific example shown below, the Galaxy S23 includes the Android 13 operating system, which includes randomized MAC for Wi-Fi connections. It comprises an SoC, Snapdragon 8 Gen 2, a Wi-Fi chipset, and FastConnect. It connects to a Wi-Fi network using the Wi-Fi chipset.  https://www.samsung.com/us/smartphones/galaxy-s23/buy/galaxy-s23-128gb-unlocked-sm-s911ulixaa/

Galaxy S23



Super fast processing

Snapdragon® 8 Gen 2

Octa-Core

<https://www.samsung.com/us/smartphones/galaxy-s23/specs/>

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

Phone	<u>Galaxy S23</u>	Galaxy S23+	Galaxy S23 Ultra
Chipset	Snapdragon 8 Gen 2 for Galaxy	Snapdragon 8 Gen 2 for Galaxy	Snapdragon 8 Gen 2 for Galaxy
RAM & Storage	8+128GB, 8+256GB (UFS 3.1)	8+256GB, 8+512GB (UFS 4.0)	8+256GB, 12+512GB, 12GB+1TB (UFS 4.0)
Display	6.1" FHD+ Dynamic AMOLED 2x, 120Hz Adaptive Refresh Rate, 425ppi, 1,750nit (outdoor peak)	6.6" FHD+ Dynamic AMOLED 2x, 120Hz Adaptive Refresh Rate, 393ppi, 1,750nit (outdoor peak)	6.8" QHD+ Dynamic AMOLED 2x, 120Hz Adaptive Refresh Rate, 500ppi, 1,750nit (outdoor peak)
<u>Software</u>	<u>Android 13 / One UI 5.1</u>	Android 13 / One UI 5.1	Android 13 / One UI 5.1
https://www.androidpolice.com/samsung-galaxy-s23/			
			
https://www.youtube.com/watch?v=BadWvxWe8y8			

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

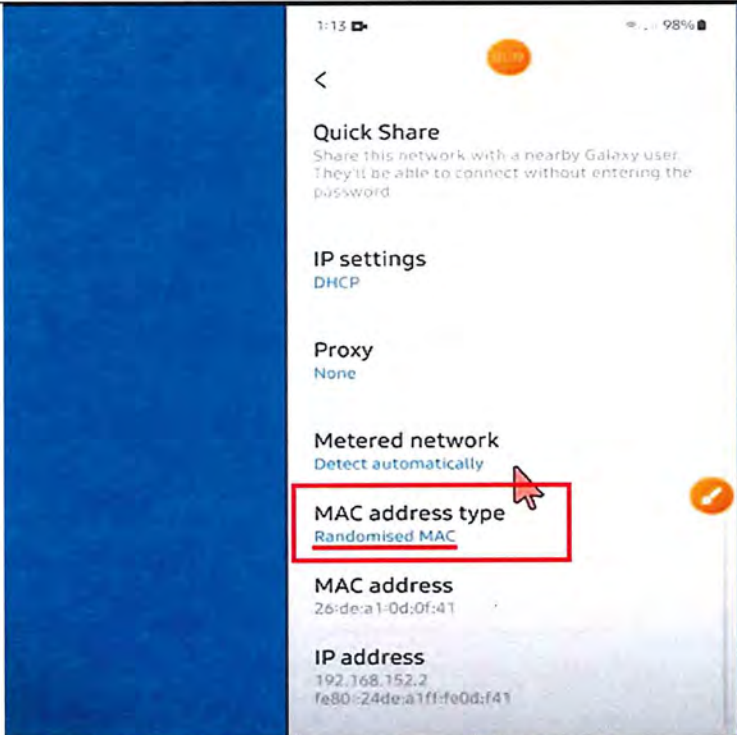
	 The screenshot shows the 'Quick Share' settings on a Galaxy S23 Plus. The 'MAC address type' is set to 'Randomised MAC', which is highlighted with a red box and a red arrow. Other settings visible include 'IP settings' (DHCP), 'Proxy' (None), 'Metered network' (Detect automatically), 'MAC address' (26:de:a1:0d:0f:41), and 'IP address' (192.168.152.2). <u>GALAXY S23, PLUS</u> <u>Set MAC Address Type to</u> <u>Randomized</u> <u>MAC/Phone MAC</u> https://www.youtube.com/watch?v=dT63df6nnqU
--	---

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

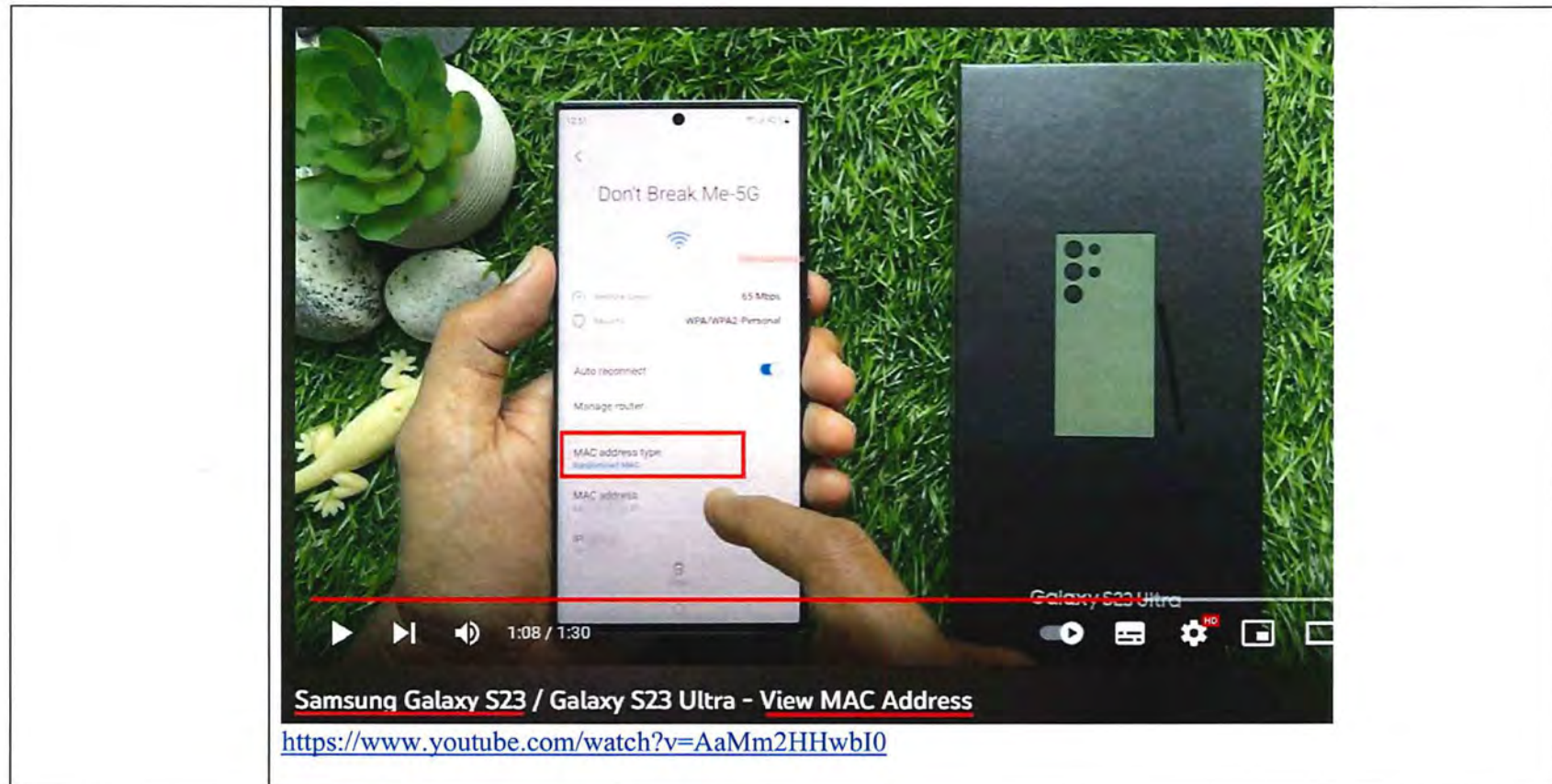


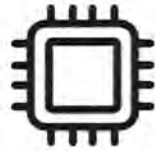
EXHIBIT A-INFRINGEMENT CONTENTIONS FOR U.S. PATENT NO. 10,694,384

	Featuring the Snapdragon X70 5G Modem RF System, <u>Snapdragon 8 Gen 2</u> is the world's first and only mobile platform with a dedicated 5G AI processor. Plus, gaming, streaming, and communication from home soar via Wi-Fi 7 (the industry's lowest latency offering), all brought to you by the <u>Qualcomm® FastConnect™ 7800 Mobile Connectivity System</u>. • 5G Dual-SIM Dual-Active (DSDA) enables the simultaneous use of two 5G+5G or 5G+4G SIM cards for ultimate user flexibility • Blazing Wi-Fi speeds of up to 5.8 Gbps—more than double Wi-Fi 6 • World's first commercial Wi-Fi 7 SoC, with advanced High Band Simultaneous Multi-Link https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/Snapdragon-8-Gen-2-Product-Brief.pdf • <u>The Samsung Galaxy S23 series features Qualcomm Technologies' leading connectivity solutions</u>, including the Snapdragon® X70 Modem-RF System, the world's fastest and smartest 5G modem-RF system, and <u>Qualcomm® FastConnect™ for high-speed and ultra-low latency Wi-Fi</u>, and the latest Bluetooth audio enhancements. https://www.qualcomm.com/news/releases/2023/02/qualcomm-and-samsung-partner-to-bring-the-fastest-snapdragon-eve MAC Randomization is implemented in devices running the Android OS since at least Android OS 10 as well as WearOS 3.0.
--	--

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

	In Android 10, MAC randomization is enabled by default for client mode, SoftAp, and Wi-Fi Direct. MAC randomization prevents listeners from using MAC addresses to build a history of device activity, thus increasing user privacy. Additionally, MAC addresses are randomized as part of Wi-Fi Aware and Wi-Fi RTT operations. For more information, see MAC Randomization Behavior. https://source.android.com/docs/core/connect/wifi-mac-randomization WearOS, including WearOS 3.0, is based on Android. See https://developer.android.com/training/wearables/wear-v-mobile#:~:text=Wear%20OS%20is%20based%20on,design%20a%20Wear%20OS%20app. Devices operating on WearOS 3.0 implement MAC randomization. See https://www.reddit.com/r/GalaxyWatch/comments/pcmkj1/galaxy_watch_4_wifi_mac_address/
[1a] generating, by the end device, a fake media access control (MAC) address for the end device;	The Accused Products generate a fake media access control (MAC) address (e.g., randomized MAC address) for the end device. As shown below, an example of the Accused Products comprises an SoC, Snapdragon 8 Gen 2. It also includes the Android OS 10 or higher (e.g., Android 13 operating system) and has randomized MAC for Wi-Fi connections. The operating system is used to generate a randomized MAC address to be used for when scanning or searching for access points, such as for Wi-Fi probe requests. The operating system runs on a CPU of the SoC (e.g., the Kryo CPU) of the Accused Product.

Galaxy S23



Super fast processing

Snapdragon® 8 Gen 2

Octa-Core

<https://www.samsung.com/us/smartphones/galaxy-s23/specs/>

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

Phone	<u>Galaxy S23</u>	Galaxy S23+	Galaxy S23 Ultra
Chipset	Snapdragon 8 Gen 2 for Galaxy	Snapdragon 8 Gen 2 for Galaxy	Snapdragon 8 Gen 2 for Galaxy
RAM & Storage	8+128GB, 8+256GB (UFS 3.1)	8+256GB, 8+512GB (UFS 4.0)	8+256GB, 12+512GB, 12GB+1TB (UFS 4.0)
Display	6.1" FHD+ Dynamic AMOLED 2x, 120Hz Adaptive Refresh Rate, 425ppi, 1,750nit (outdoor peak)	6.6" FHD+ Dynamic AMOLED 2x, 120Hz Adaptive Refresh Rate, 393ppi, 1,750nit (outdoor peak)	6.8" QHD+ Dynamic AMOLED 2x, 120Hz Adaptive Refresh Rate, 500ppi, 1,750nit (outdoor peak)
<u>Software</u>	<u>Android 13 / One UI 5.1</u>	Android 13 / One UI 5.1	Android 13 / One UI 5.1

<https://www.androidpolice.com/samsung-galaxy-s23/>



CPU

Kryo CPU

- 64-bit Architecture
- 1 Prime core, up to 3.36 GHz²
 - Arm Cortex-X3 technology
- 4 Performance cores, up to 2.8 GHz
- 3 Efficiency cores, up to 2.0 GHz

<https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/Snapdragon-8-Gen-2-Product-Brief.pdf>

Phone	<u>Galaxy S23</u>	Galaxy S23+	Galaxy S23 Ultra
<u>Connectivity</u>	5G, <u>Wi-Fi 6E</u> , Bluetooth 5.3, NFC	5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband	5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband

<https://www.androidpolice.com/samsung-galaxy-s23/>

Galaxy S23



Wi-Fi 6E

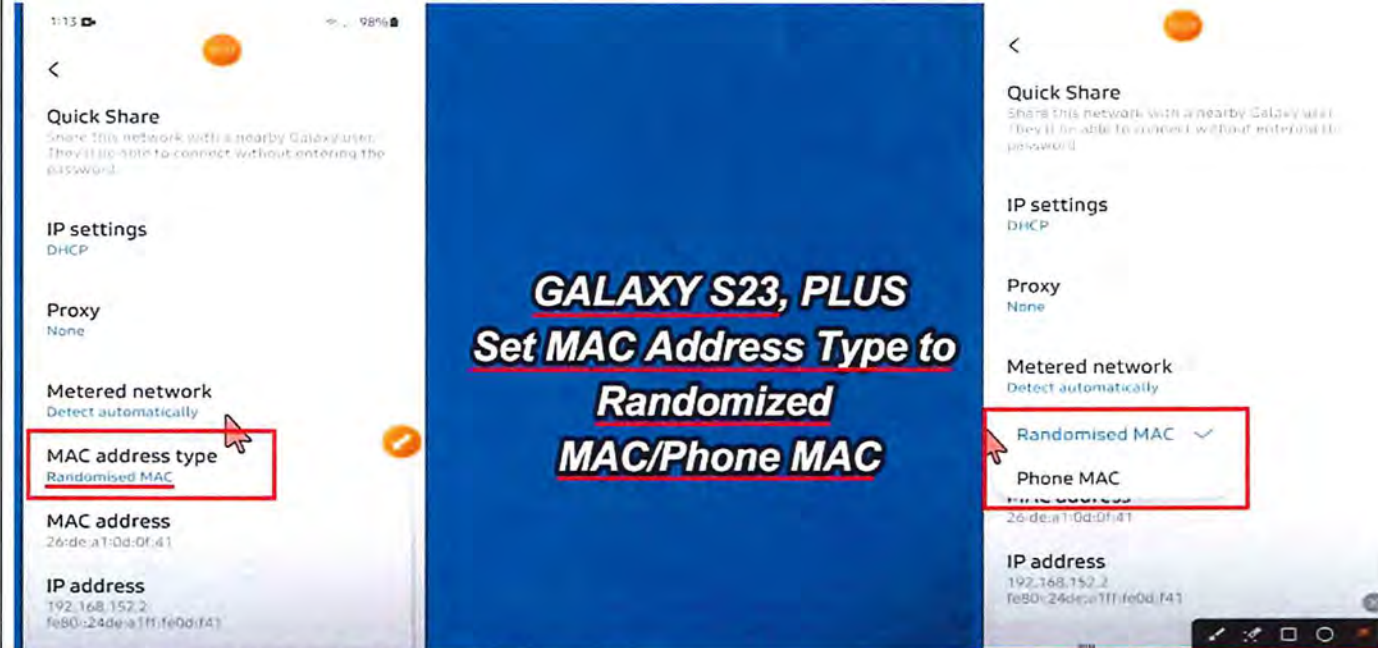
802.11 a/b/g/n/ac/ax

<https://www.samsung.com/us/smartphones/galaxy-s23/specs/>

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

- **Connectivity:** The Galaxy S23 series boasts unparalleled Snapdragon Connect technologies across 5G, Wi-Fi, and Bluetooth®. Featuring the multiple-award-winning Snapdragon X70 5G Modem-RF System with the Qualcomm® 5G AI Processor, the Galaxy S23 series harnesses the power of AI to enable breakthrough 5G coverage, power efficiency, speeds, and latency. These new devices also support 5G+5G/4G Dual-SIM Dual-Active³, which harnesses the power and flexibility of two 5G SIMs at once. Additionally, all Galaxy S23 series variants feature the Qualcomm® FastConnect™ 6900 and 7800 systems delivering multi-gigabit Wi-Fi speeds, ultra-low latency, and deeply immersive Bluetooth Audio experiences.

<https://www.qualcomm.com/news/releases/2023/02/qualcomm-and-samsung-partner-to-bring-the-fastest-snapdragon-eve>



<https://www.youtube.com/watch?v=dT63df6nnqU>

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

The Accused Products support the Wi-Fi standard. According to the standard, the Accused Products (each a UE) inquire about available Wi-Fi access points using a probe request that includes a MAC address. For a probe request the Accused Products use a randomized MAC address, which is a fake MAC address.

MAC Randomization Behavior

The MAC randomization feature allows devices to use a randomized MAC address when connecting to a Wi-Fi network. For implementation instructions, see [Implementing MAC Randomization](#). This page describes the behavior of MAC randomization in Android.

MAC addresses are used by devices when connecting to a Wi-Fi network or an access point. Because these MAC addresses are transmitted without encryption, they can be captured and used to potentially track a user's location. Historically, devices use the factory MAC address to associate to a Wi-Fi network. The factory MAC address is globally unique and static, allowing the device to be tracked and individually identified.

The MAC randomization feature increases user privacy by using a randomized MAC address when connecting to a Wi-Fi network.

MAC addresses are 48 bits long and usually represented by 12 hex digits (6 octets as each octet is 8 bits) such as 00:11:22:AA:BB:CC. The MAC randomization feature randomizes the address by setting the locally administered bit to 1, and the unicast bit to 0. The other 46 bits are randomized.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

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

	For devices running Android 10 or higher, the framework uses randomized MAC address by default. Users can enable or disable MAC randomization for individual networks through an option in the Network details screen in Settings, as shown in Figure 1. If a user disables MAC randomization for a network, the framework uses the factory MAC address (globally unique address).  Figure 1. MAC randomization option. https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
[1b] transmitting, by the end device to an access point, a probe request that includes the fake MAC address;	The Accused Products transmit to an access point (e.g., Wi-Fi access point), a probe request that includes the fake MAC address (e.g., randomized MAC address). The Accused Products support the Wi-Fi standard. According to the standard, the Accused Products (each a UE) send probe requests to access points to inquire about available Wi-Fi access points. The probe request comprises a sender address field (e.g., device identifier). The Accused Products utilize a random MAC address as the sender address in a probe request. The end user device transmits probe requests to identify available access points:

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

	The reason for client scanning is to determine a suitable AP to which the client may need to roam now or in the future. <u>A client can use two scanning methods: active and passive. During an active scan, the client radio transmits a probe request and listens for a probe response from an AP.</u> With a passive scan, the client radio listens on each channel for beacons sent periodically by an AP. A passive scan generally takes more time, since the client must listen and wait for a beacon versus actively probing to find an AP. Another limitation with a passive scan is that if the client does not wait long enough on a channel, then the client may miss an AP beacon. https://www.wi-fi.org/knowledge-center/faq/what-are-passive-and-active-scanning
--	--

CWAP 802.11- Probe Request/Response

POSTED BY NAYARASI IN CWAP

≈ 27 COMMENTS

Discovering the network by scanning all possible channels & listening to beacons is not considered to be very efficient (**passive scanning**). To enhance this discovery process, stations often use what is called **active scanning**.

In Active scanning, stations still go through each channel in turn, but instead of passively listening to the signals on that frequency, station send a **Probe Request** management frame asking what network is available on that channel.

Probe Request are sent to the broadcast DA address (ff:ff:ff:ff:ff:ff). Once a Probe sent, STA starts a ProbeTimer countdown & wait for answers. At the end of the timer, STA process the answer it has received. If no answers received, STA moves to next channel & repeats the discovery process.

STA sending Probe Request may specify the SSID they looking (called **directed probe request**). Then only IBSS STA or AP support that SSID will answer. **The SSID value can also be set to 0** (ie **SSID field is present, but empty**). This is called **Wildcard SSID** or **Null Probe Request**.

<https://mrnciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

A Wi-Fi probe request includes the end device's MAC address:

Probe requests are packets broadcasted in plain text by Wi-Fi mobile devices to discover 802.11 Access Points (APs) in their proximity [1]. These unencrypted messages contain information about their sources (i.e., MAC address and supported data rate and supported connection to an AP). The operation of capturing data on a

<https://www.sciencedirect.com/science/article/abs/pii/S1389128622000196>

The Wi-Fi probe request of the Accused Products includes a randomized MAC address, which is a fake MAC address.

MAC Randomization Behavior

The MAC randomization feature allows devices to use a randomized MAC address when connecting to a Wi-Fi network. For implementation instructions, see [Implementing MAC Randomization](#). This page describes the behavior of MAC randomization in Android.

MAC addresses are used by devices when connecting to a Wi-Fi network or an access point. Because these MAC addresses are transmitted without encryption, they can be captured and used to potentially track a user's location. Historically, devices use the *factory MAC address* to associate to a Wi-Fi network. The factory MAC address is globally unique and static, allowing the device to be tracked and individually identified.

The MAC randomization feature increases user privacy by using a randomized MAC address when connecting to a Wi-Fi network.

MAC addresses are 48 bits long and usually represented by 12 hex digits (6 octets as each octet is 8 bits) such as 00:11:22:AA:BB:CC. The MAC randomization feature randomizes the address by setting the *locally administered* bit to 1, and the *unicast* bit to 0. The other 46 bits are randomized.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

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

For devices running Android 10 or higher, the framework uses randomized MAC address by default. Users can enable or disable MAC randomization for individual networks through an option in the **Network details** screen in **Settings**, as shown in Figure 1. If a user disables MAC randomization for a network, the framework uses the factory MAC address (globally unique address).

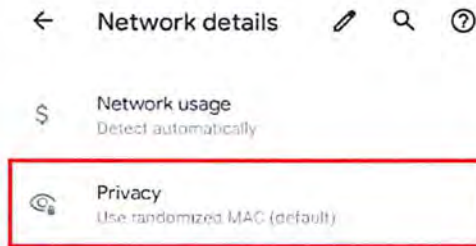
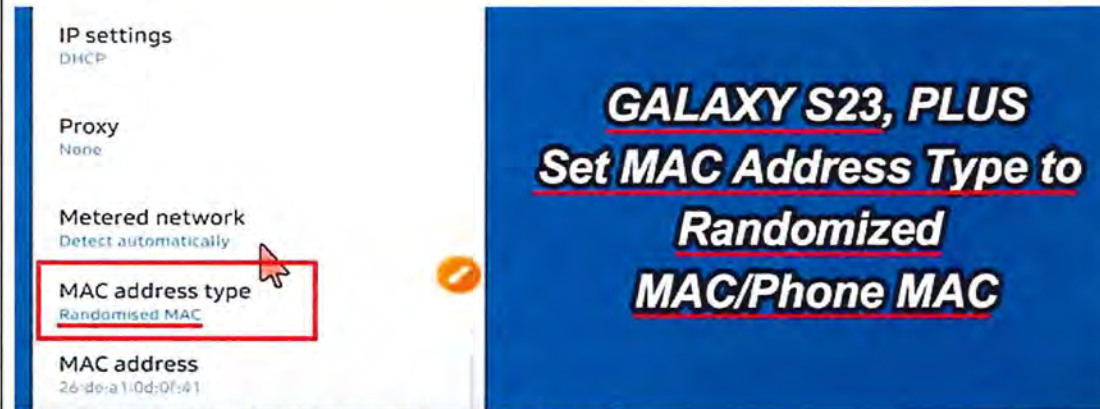


Figure 1. MAC randomization option.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>



<https://www.youtube.com/watch?v=dT63df6nnqU>

An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.

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

[1c] receiving, by the end device from the access point, a probe response that includes information regarding the access point;	The Accused Products receive from the access point, a probe response that includes information regarding the access point. As an example, a probe response from a Wi-Fi access point includes the SSID (wireless network name), supported data rates, encryption types, capabilities, etc. of the access point. The Accused Products support the Wi-Fi standard. The Accused Products receive probe responses from multiple available access points. As an example, an access point responds with the probe response when the SSID in the probe request is the wildcard SSID or matches the specific SSID of the access point or when the specific SSID of the access point is included in the SSID List element. As a further example, an AP responds to a probe request when it supports data rates or other requirements of the Accused Products. 2. APs receiving the probe request check to see if the mobile station has at least one common supported data rate. If they have compatible data rates, a probe response is sent advertising the SSID (wireless network name), supported data rates, encryption types if required, and other 802.11 capabilities of the AP. https://documentation.meraki.com/MR/Wi-Fi Basics and Best Practices/802.11 Association Process Explained <u>Persistent randomization</u> <u>Android uses the persistent randomization type by default when the MAC randomization feature is enabled. Android generates a persistent randomized MAC address based on the parameters of the network profile including SSID, security type, or FQDN (for Passpoint networks). This MAC address remains the same until factory reset. The MAC address does not get re-randomized if the user forgets and re-adds the Wi-Fi network since the MAC addressed depends on the parameters of the network profile.</u> https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior
--	---

MAC Randomization Behavior

The MAC randomization feature allows devices to use a randomized MAC address when connecting to a Wi-Fi network. For implementation instructions, see [Implementing MAC Randomization](#). This page describes the behavior of MAC randomization in Android.

MAC addresses are used by devices when connecting to a Wi-Fi network or an access point. Because these MAC addresses are transmitted without encryption, they can be captured and used to potentially track a user's location. Historically, devices use the factory MAC address to associate to a Wi-Fi network. The factory MAC address is globally unique and static, allowing the device to be tracked and individually identified.

The MAC randomization feature increases user privacy by using a randomized MAC address when connecting to a Wi-Fi network.

MAC addresses are 48 bits long and usually represented by 12 hex digits (6 octets as each octet is 8 bits) such as `00:11:22:AA:BB:CC`. The MAC randomization feature randomizes the address by setting the *locally administered* bit to 1, and the *unicast* bit to 0. The other 46 bits are randomized.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

For devices running Android 10 or higher, the framework uses randomized MAC address by default. Users can enable or disable MAC randomization for individual networks through an option in the **Network details** screen in **Settings**, as shown in Figure 1. If a user disables MAC randomization for a network, the framework uses the factory MAC address (globally unique address).

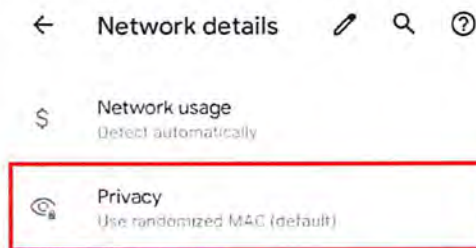


Figure 1. MAC randomization option.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

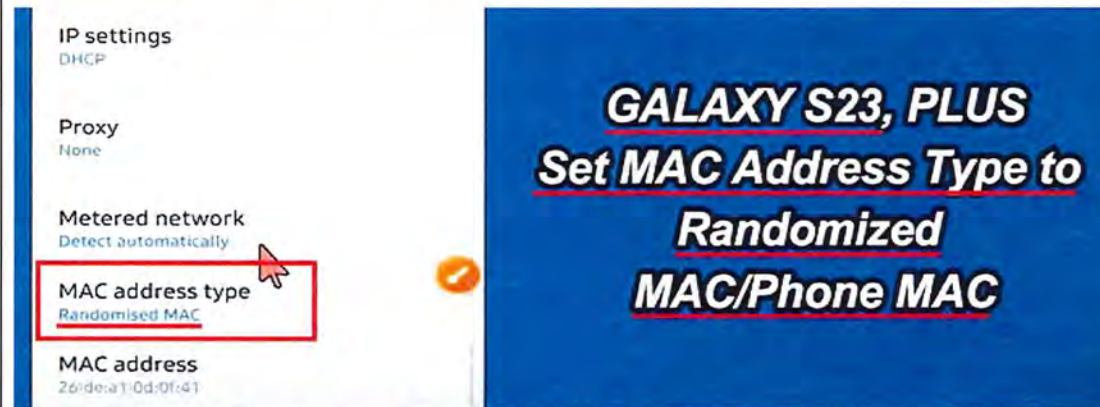
MAC Randomization Behavior

The MAC randomization feature allows devices to use a randomized MAC address when connecting to a Wi-Fi network. For implementation instructions, see [Implementing MAC Randomization](#). This page describes the behavior of MAC randomization in Android.

MAC addresses are used by devices when connecting to a Wi-Fi network or an access point. Because these MAC addresses are transmitted without encryption, they can be captured and used to potentially track a user's location. Historically, devices use the factory MAC address to associate to a Wi-Fi network. The factory MAC address is globally unique and static, allowing the device to be tracked and individually identified.

The MAC randomization feature increases user privacy by using a randomized MAC address when connecting to a Wi-Fi network.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>



<https://www.youtube.com/watch?v=dT63df6nnqU>

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

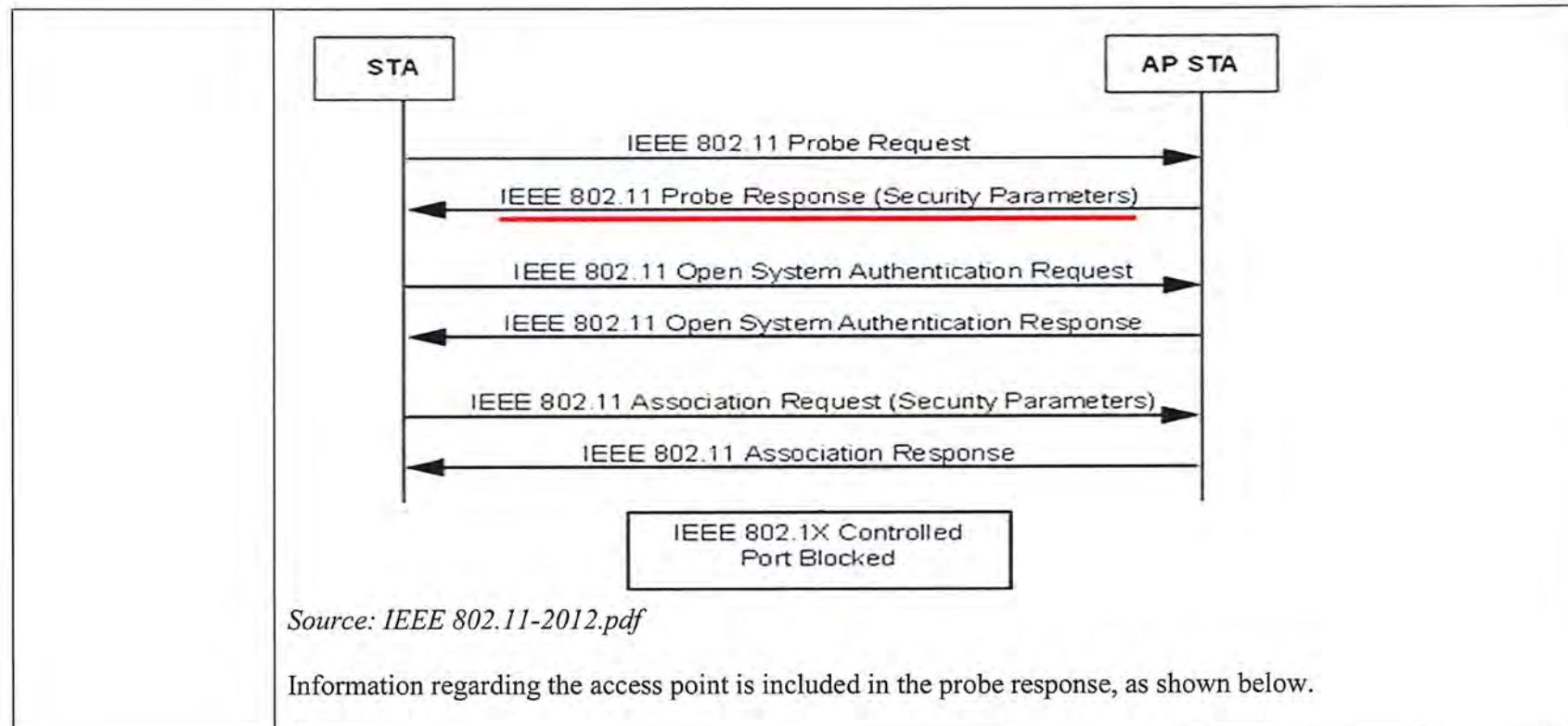


EXHIBIT A-INFRINGEMENT CONTENTIONS FOR U.S. PATENT NO. 10,694,384

Table 8-27—Probe Response frame body		
Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability	
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 PHY's.
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 PHY's. 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.
9	IBSS Parameter Set	The IBSS Parameter Set element is present only within Probe Response frames generated by STAs in an IBSS.
10	Country	The Country element is present if dot11MultiDomainCapabilityActivated is true or dot11SpectrumManagementRequired is true or dot11RadioMeasurementActivated is true.
11	FH Parameters	The FH Parameters element, as specified in 8.4.2.11, is optionally present if dot11MultiDomainCapabilityActivated is true.
12	FH Pattern Table	The FH Pattern Table element, as specified in 8.4.2.12, is optionally present if dot11MultiDomainCapabilityActivated is true.
13	Power Constraint	The Power Constraint element is present if dot11SpectrumManagementRequired is true and is optionally present if dot11RadioMeasurementActivated is true.
14	Channel Switch Announcement	The Channel Switch Announcement element is optionally present if dot11SpectrumManagementRequired is true.
15	Quiet	The Quiet element is optionally present if dot11SpectrumManagementRequired is true or if dot11RadioMeasurementActivated is true.
16	IBSS DFS	The IBSS DFS element is present if dot11SpectrumManagementRequired is true in an IBSS.
17	TPC Report	The TPC Report element is present if dot11SpectrumManagementRequired is true or dot11RadioMeasurementActivated is true.
18	ERP	The ERP element is present within Probe Response frames generated by STAs using ERPs and is optionally present otherwise.
19	Extended Supported Rates	The Extended Supported Rates element is present if there are more than eight supported rates, and it is optionally present otherwise.
20	RSN	The RSNE is present only if dot11RSNAActivated is true.
21	BSS Load	The BSS Load element is present if dot11QoSOptionImplemented and dot11QBSSLoadImplemented are both true.
22	EDCA Parameter Set	The EDCA Parameter Set element is present if dot11QoSOptionImplemented is true and dot11MeshActivated is true.

<https://mmcciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

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

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.
26	AP Channel Report	If dot11RMAPChannelReportActivated is true, one AP Channel Report element is optionally present for each operating class that has at least 1 channel to report.
27	BSS Average Access Delay	The BSS Average Access Delay element is optionally present if dot11RMBSSAverageAccessDelayActivated is true and the value of the AP Average Access Delay field is not equal to 255 (measurement not available).
28	Antenna	The Antenna element is optionally present if dot11RMAntennaInformationActivated is true and the value of the Antenna ID field is not equal to 0 (unknown antenna).
29	BSS Available Admission Capacity	The BSS Available Admission Capacity element is optionally present if dot11RMBSSAvailableAdmissionCapacityActivated is true with the following exceptions: 1) when Available Admission Capacity Bitmask equals 0 (Available Admission Capacity List contains no entries), or 2) when the BSS Load element is present and the Available Capacity Bitmask equals 256 (Available Admission Capacity List contains only the AC_VO entry).
30	BSS AC Access Delay	The BSS AC Access Delay element is optionally present if dot11RMBSSAverageAccessDelayActivated is true and at least one field of the element is not equal to 255 (measurement not available).
31	Mobility Domain	The MDE is present if dot11FastBSSTransitionActivated is true.
32	DSE registered location	The DSE Registered Location element is present if dot11LCIDSERequired is true.
33	Extended Channel Switch Announcement	The Extended Channel Switch Announcement element is optionally present if dot11ExtendedChannelSwitchActivated is true.
34	Supported Operating Classes	The Supported Operating Classes element is present if dot11ExtendedChannelSwitchActivated is true.
35	HT Capabilities	The HT Capabilities element is present when dot11HighThroughputOptionImplemented attribute is true.
36	HT Operation	The HT Operation element is included by an AP and a mesh STA when dot11HighThroughputOptionImplemented attribute is true.
37	20/40 BSS Coexistence	The 20/40 BSS Coexistence element is optionally present when the dot112040BSSCoexistenceManagementSupport attribute is true.
38	Overlapping BSS Scan Parameters	The Overlapping BSS Scan Parameters element is optionally present if the dot11FortyMHzOptionImplemented attribute is true.
39	Extended Capabilities	The Extended Capabilities element is optionally present if any of the fields in this element are nonzero.

<https://mrcciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

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

40	QoS Traffic Capability	The QoS Traffic Capability element is optionally present if dot11MgmtOptionACStationCountActivated is true.
41	Channel Usage	The Channel Usage element is present if the Channel Usage element is present in the Probe Request frame and dot11MgmtOptionChannelUsageActivated is true.
42	Time Advertisement	The Time Advertisement element is present if dot11MgmtOptionUTCSTSOOffsetActivated is true.
43	Time Zone	The Time Zone element is present if dot11MgmtOptionUTCSTSOOffsetActivated is true.
44	Interworking	The Interworking element is present if dot11InterworkingServiceActivated is true.
45	Advertisement Protocol	Advertisement Protocol element is present if dot11InterworkingServiceActivated is true and at least one dot11GASAdvertisementID MIB attribute exists.
46	Roaming Consortium	The Roaming Consortium element is present if dot11InterworkingServiceActivated is true and the dot11RoamingConsortiumTable has at least one entry.
47	Emergency Alert Identifier	One or more Emergency Alert Identifier elements are present if dot11EASActivated is true and there are one or more EAS message(s) active in the network.
48	Mesh ID	The Mesh ID element is present if dot11MeshActivated is true.
49	Mesh Configuration	The Mesh Configuration element is present if dot11MeshActivated is true.
50	Mesh Awake Window	The Mesh Awake Window element is optionally present if dot11MeshActivated is true.
51	Beacon Timing	The Beacon Timing element is optionally present if both dot11MeshActivated and dot11MBCAActivated are true.
52	MCCAOP Advertisement Overview	The MCCAOP Advertisement Overview element is optionally present if both dot11MeshActivated and dot11MCCAActivated are true.
53	MCCAOP Advertisement	One or more MCCAOP Advertisement elements are optionally present if both dot11MeshActivated and dot11MCCAActivated are true.
54	Mesh Channel Switch Parameters	The Mesh Channel Switch Parameters element is present if dot11MeshActivated is true and either Channel Switch Announcement element or Extended Channel Switch Announcement element is present.
Last-1	Vendor Specific	One or more vendor-specific elements are optionally present. These elements follow all other elements, except the Requested elements.
Last-n	Requested elements	Elements requested by the Request element of the Probe Request frame are present if dot11MultiDomainCapabilityActivated is true. See 10.1.4.3.2.

<https://mrncciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

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

4.3.13.15 SSID list

The SSID List element enables the non-AP STA to request information on a list of SSIDs. This is intended to reduce the number of Probe Request frames sent by the non-AP STA.

Source: IEEE 802.11-2012.pdf

In an infrastructure BSS or in an IBSS, STAs receiving Probe Request frames shall respond with a probe response when the SSID in the probe request is the wildcard SSID or matches the specific SSID of the STA or when the specific SSID of the STA is included in the SSID List element. Furthermore, a STA with dot11RadioMeasurementActivated true receiving a probe request with a DSSS Parameter Set element containing a Current Channel field value that is not the same as the value of dot11CurrentChannel shall not respond with a probe response. An AP shall respond to all probe requests meeting the above criteria. In an IBSS a STA that transmitted a Beacon frame since the last TBTT shall respond to group addressed Probe Request frames. A STA in an IBSS shall respond to Probe Request frames sent to the individual address of the STA.

Source: IEEE 802.11-2012.pdf

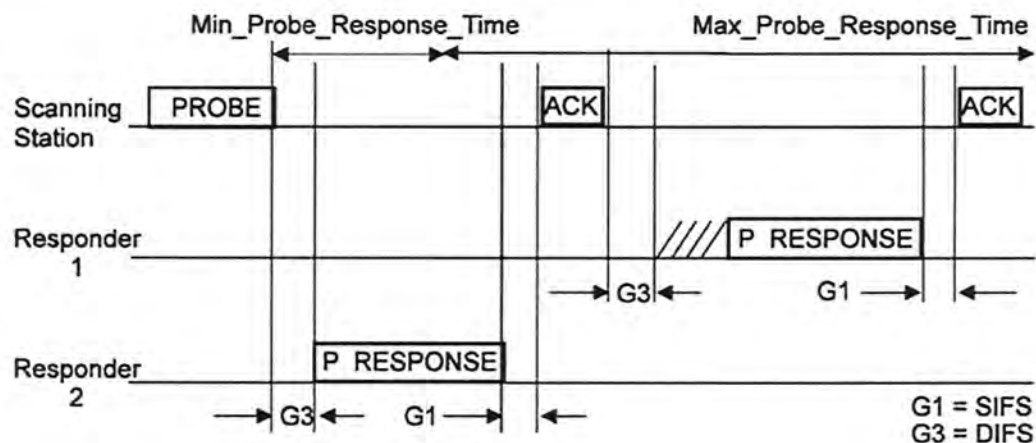


Figure 10-3—Probe response

Source: IEEE 802.11-2012.pdf

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

Before answering the question, let us first understand what a preferred network list is. The PNL is a historical record of all the network names (SSIDs) that a device has previously connected to, and trusts to automatically connect to again in the future.

User devices trying to connect to a Wi-Fi network watch for access points (APs) broadcasting its availability for a device to connect to its network. Within that information contains the network name, or Service Set Identifier (SSID). Wi-Fi enabled devices trying to connect to a wireless network, and using Active Service Discovery, will then broadcast its interest in connecting to the AP if the network name is in its PNL, which increases the connection speed.

For instance, if you connect to a **Starbucks** Wi-Fi network once, your device will remember and try to automatically connect to any network with the SSID Starbucks. This is true whether you go to the same Starbucks in the future, or a Starbucks 1,000 miles away. All the user device knows is the network name; no additional data is stored. Auto-connecting to wireless networks in PNL saves time and is convenient for the user, but it is a security risk. Therefore, it is important to identify all networks in the PNL and stop connecting automatically to Wi-Fi to stay safe.

<https://blog.pulsarsecurity.com/preferred-network-list-pnl>

The reason for client scanning is to determine a suitable AP to which the client may need to roam now or in the future. A client can use two scanning methods: active and passive. During an active scan, the client radio transmits a probe request and listens for a probe response from an AP. With a passive scan, the client radio listens on each channel for beacons sent periodically by an AP. A passive scan generally takes more time, since the client must listen and wait for a beacon versus actively probing to find an AP. Another limitation with a passive scan is that if the client does not wait long enough on a channel, then the client may miss an AP beacon.

<https://www.wi-fi.org/knowledge-center/faq/what-are-passive-and-active-scanning>

Below is an example Wi-Fi probe response that includes information of the AP.

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

802.11 Management - Probe Response

- Probe Timestamp: 23996945615 Microseconds [24-31]
- Beacon Interval: 102 Time Units (104 Milliseconds, and 448 Microseconds) [32-33]
- Capability Info: %0001000000000001
- SSID ID=0 SSID Len=4 SSID=OPEN
- Supported Rates**
 - Element ID: 1 Supported Rates [42]
 - Length: 4 [43]
 - Supported Rate: 24.0 Mbps (BSS Basic Rate) [44]
 - Supported Rate: 36.0 Mbps (Not BSS Basic Rate) [45]
 - Supported Rate: 48.0 Mbps (Not BSS Basic Rate) [46]
 - Supported Rate: 54.0 Mbps (Not BSS Basic Rate) [47]
- Country**
 - Element ID: 7 Country [48]
 - Length: 18 [49]
 - Country Code: AU [50-51]
 - Environment: 0x20 Any [52]
 - Starting Channel: 36 [53]
 - Number of Channels: 4 [54]
 - Max Tx Power (dBm): 23 [55]
 - Starting Channel: 52 [56]
 - Number of Channels: 4 [57]
 - Max Tx Power (dBm): 23 [58]
 - Starting Channel: 100 [59]
 - Number of Channels: 5 [60]
 - Max Tx Power (dBm): 30 [61]
 - Starting Channel: 132 [62]
 - Number of Channels: 3 [63]
 - Max Tx Power (dBm): 30 [64]
 - Starting Channel: 149 [65]
 - Number of Channels: 5 [66]
 - Max Tx Power (dBm): 30 [67]
- OBSS Load**
 - Element ID: 11 OBSS Load [68]
 - Length: 5 [69]
 - Station Count: 1 [70-71]
 - Channel Utilization: 0 % [72]
 - Avail Admission Capacity: 26562 [73-74]
- HT Cap= ID=45 HT Cap Len=26

Annotations:

- Information regarding access point (points to SSID and Supported Rates)
- Information regarding access point (points to Country)
- Probe response (points to the entire frame)

<https://mmcciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.

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

[1d] 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	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. As an example, 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. <u>Persistent randomization</u> <u>Android uses the persistent randomization type by default when the MAC randomization feature is enabled. Android generates a persistent randomized MAC address based on the parameters of the network profile including SSID, security type, or FQDN (for Passpoint networks). This MAC address remains the same until factory reset. The MAC address does not get re-randomized if the user forgets and re-adds the Wi-Fi network since the MAC address depends on the parameters of the network profile.</u> <u>Persistent MAC addresses are necessary in cases where networks rely on the persistence of the MAC address to provide useful functionality to the user, for example, to remember a device and allow users to bypass the login screen as expected, or to enable parental controls.</u> <u>For Android 10 and 11, the framework uses persistent randomization for all networks when MAC randomization is enabled.</u> https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior
---	---

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

[android / device / generic / goldfish / refs/tags/android-9.0.0_r34 / . / wifi / WifiConfigStore.xml](#)

blob: bb5645aacde00f44a93c3386c8e42cf140bfe6a5 [file] [log] [blame]

```

1  <?xml version='1.0' encoding='utf-8' standalone='yes' ?>
2  <WifiConfigStoreData>
3      <int name="Version" value="1" />
4      <NetworkList>
5          <Network>
6              <WifiConfiguration>
7                  <string name="ConfigKey">&quot;AndroidWifi&quot;NONE</string>
8                  <string name="SSID">&quot;AndroidWifi&quot;</string>
9                  <null name="BSSID" />
10                 <null name="PreSharedKey" />
11                 <null name="WEPKeys" />
12                 <int name="WEPKeyIndex" value="0" />
13                 <boolean name="HiddenSSID" value="false" />

```

https://android.googlesource.com/device/generic/goldfish/+/refs/tags/android-9.0.0_r34/wifi/WifiConfigStore.xml

In an infrastructure BSS or in an IBSS, STAs receiving Probe Request frames shall respond with a probe response when the SSID in the probe request is the wildcard SSID or matches the specific SSID of the STA or when the specific SSID of the STA is included in the SSID List element. Furthermore, a STA with dot11RadioMeasurementActivated true receiving a probe request with a DSSS Parameter Set element containing a Current Channel field value that is not the same as the value of dot11CurrentChannel shall not respond with a probe response. An AP shall respond to all probe requests meeting the above criteria. In an IBSS a STA that transmitted a Beacon frame since the last TBTT shall respond to group addressed Probe Request frames. A STA in an IBSS shall respond to Probe Request frames sent to the individual address of the STA.

Source: IEEE 802.11-2012.pdf

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

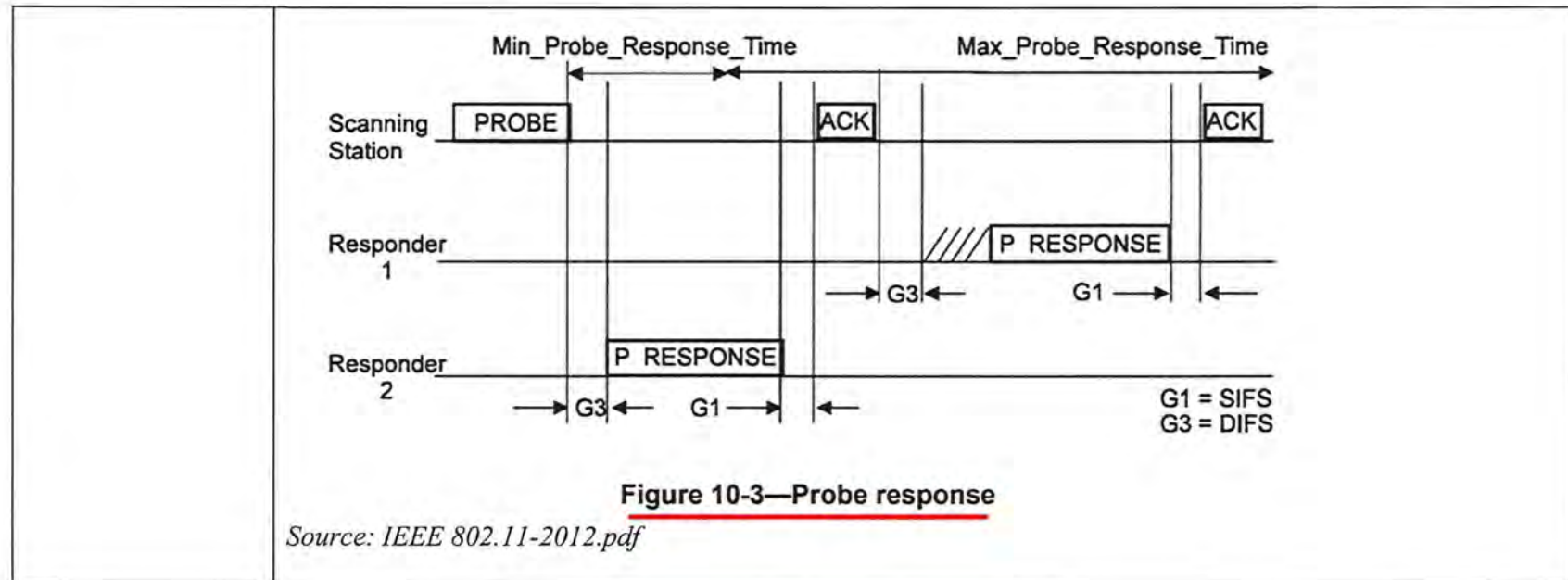


EXHIBIT A-INFRINGEMENT CONTENTIONS FOR U.S. PATENT NO. 10,694,384

Before answering the question, let us first understand what a preferred network list is. The PNL is a historical record of all the network names (SSIDs) that a device has previously connected to, and trusts to automatically connect to again in the future.

User devices trying to connect to a Wi-Fi network watch for access points (APs) broadcasting its availability for a device to connect to its network. Within that information contains the network name, or Service Set Identifier (SSID). Wi-Fi enabled devices trying to connect to a wireless network, and using Active Service Discovery, will then broadcast its interest in connecting to the AP if the network name is in its PNL, which increases the connection speed.

For instance, if you connect to a **Starbucks** Wi-Fi network once, your device will remember and try to automatically connect to any network with the SSID Starbucks. This is true whether you go to the same Starbucks in the future, or a Starbucks 1,000 miles away. All the user device knows is the network name; no additional data is stored. Auto-connecting to wireless networks in PNL saves time and is convenient for the user, but it is a security risk. Therefore, it is important to identify all networks in the PNL and stop connecting automatically to Wi-Fi to stay safe.

<https://blog.pulsarsecurity.com/preferred-network-list-pnl>

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

The screenshot displays a Wi-Fi probe response packet analysis. The following fields are highlighted with red boxes and callouts:

- Supported Rates:** A red box highlights the list of supported rates (24.0, 36.0, 48.0, 54.0 Mbps). A callout points to this box with the text "information regarding access point".
- Country:** A red box highlights the country information (AU, 0x20 Any). A callout points to this box with the text "information regarding access point".
- OBSS Load:** A red box highlights the OBSS Load information (Station Count: 1, Channel Utilization: 0%). A callout points to this box with the text "probe response".

Below the screenshot, a URL is provided:

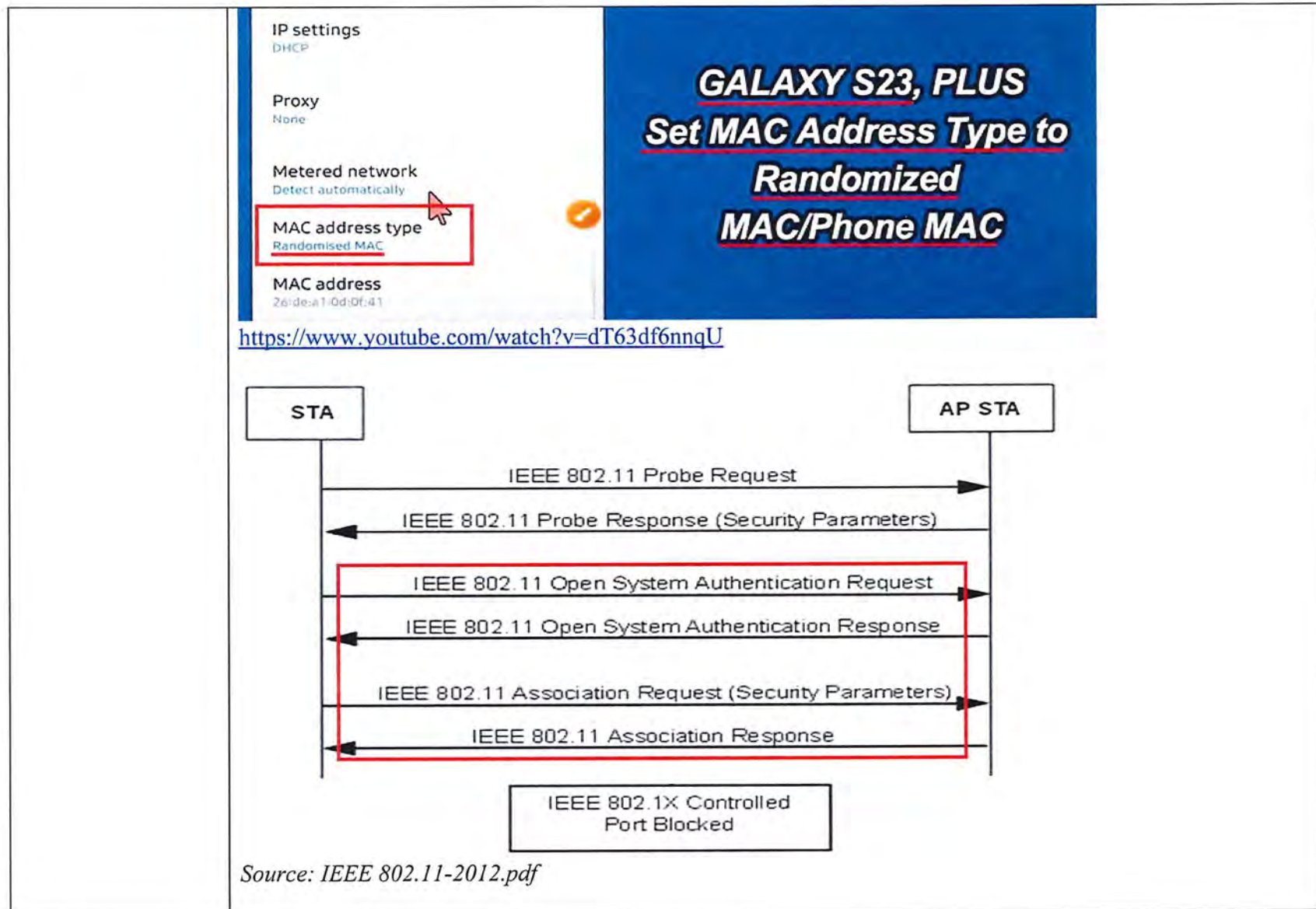
<https://mrnciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.

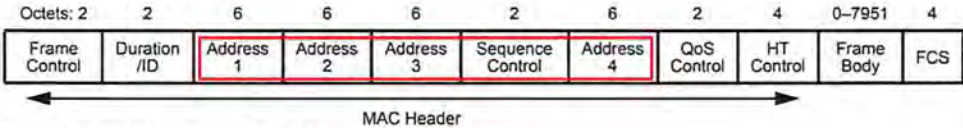
EXHIBIT A-INFRINGEMENT CONTENTIONS FOR U.S. PATENT NO. 10,694,384

[1e] 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.	The Accused Products transmit to the access point determined to be the authenticated access point, a connection request, such as an association message or other message for connecting to the access point. The message is a connection request. The message includes an authentic device identifier for the end device. For example, the message includes a persistent MAC address for connecting to the access point. After receiving the probe response from the access point, as discussed above, the Accused Products confirm the received SSID information from the probe responses with the access point information stored in its memory. Once confirmed that there is an SSID in a probe response from an access point with which the UE was connected previously, the Accused Products initiate a connection using the persistent MAC address for the access point, which is an authentic device identifier for the Accused Product. <u>Persistent randomization</u> <u>Android uses the persistent randomization type by default when the MAC randomization feature is enabled. Android generates a persistent randomized MAC address based on the parameters of the network profile including SSID, security type, or FQDN (for Passpoint networks). This MAC address remains the same until factory reset. The MAC address does not get re-randomized if the user forgets and re-adds the Wi-Fi network since the MAC address depends on the parameters of the network profile.</u> https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior
--	--

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



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.



Source: IEEE 802.11-2012.pdf

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.

Source: IEEE 802.11-2012.pdf

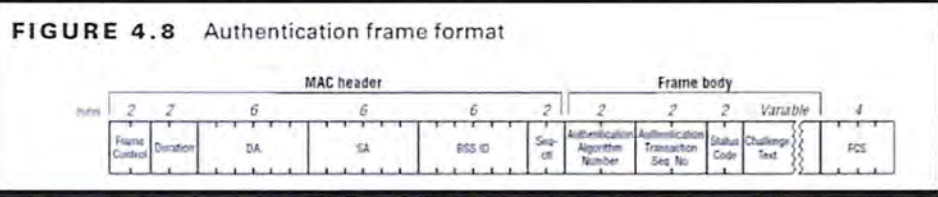
802.11 Mgmt : Authentication Frame

POSTED BY NAYARASI IN CWAP ≈ 10 COMMENTS

Once a client station is discover a SSID (Probe Request/Response or listening to Beacons) it move to Join phase. This exchange comprise of at least 4 frames

- 1. Authentication (Request)
- 2. Authentication (Response)
- 3. Association Request
- 4. Association Response

The frame format of those Authentication frames are as shown below.(from page 136- CWAP Official Study Guide)



<https://mrncciew.com/2014/10/10/802-11-mgmt-authentication-frame/>

The Accused Products may use persistent randomization, in which for the same Wi-Fi network and device combination, the MAC address remains the same. When an Accused Product connects to a Wi-Fi network it was previously connected to, it will use the same MAC address.

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

Persistent randomization

Android uses the persistent randomization type by default when the MAC randomization feature is enabled. Android generates a persistent randomized MAC address based on the parameters of the network profile including SSID, security type, or FQDN (for Passpoint networks). This MAC address remains the same until factory reset. The MAC address does not get re-randomized if the user forgets and re-adds the Wi-Fi network since the MAC address depends on the parameters of the network profile.

Persistent MAC addresses are necessary in cases where networks rely on the persistence of the MAC address to provide useful functionality to the user, for example, to remember a device and allow users to bypass the login screen as expected, or to enable parental controls.

For Android 10 and 11, the framework uses persistent randomization for all networks when MAC randomization is enabled.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

[android](#) / [device](#) / [generic](#) / [goldfish](#) / [refs/tags/android-9.0.0_r34](#) / [_](#) / [wifi](#) / [WifiConfigStore.xml](#)

blob: bb5645aacde0f44a93c3386c8e42cf140bfe6a5 [file] [log] [blame]

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<WifiConfigStoreData>
  <int name="Version" value="1" />
  <NetworkList>
    <Network>
      <WifiConfiguration>
        <string name="ConfigKey">&quot;AndroidWifi&quot;NONE</string>
        <string name="SSID">&quot;AndroidWifi&quot;</string>
        <null name="BSSID" />
        <null name="PreSharedKey" />
        <null name="WEPKeys" />
        <int name="WEPKeyIndex" value="0" />
        <boolean name="HiddenSSID" value="false" />
```

https://android.googlesource.com/device/generic/goldfish/+refs/tags/android-9.0.0_r34/wifi/WifiConfigStore.xml

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

	An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
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.	The Accused Products practice a method wherein the fake MAC address is distinct from an actual original MAC address of a hardware network interface of the end device. The Accused Products generate a fake MAC address that is different from the original MAC address of the hardware by generating a randomized MAC address for use in probe requests. <u>MAC Randomization Behavior</u> □ - <u>The MAC randomization feature allows devices to use a randomized MAC address when connecting to a Wi-Fi network. For implementation instructions, see Implementing MAC Randomization. This page describes the behavior of MAC randomization in Android.</u> <u>MAC addresses are used by devices when connecting to a Wi-Fi network or an access point. Because these MAC addresses are transmitted without encryption, they can be captured and used to potentially track a user's location. Historically, devices use the factory MAC address to associate to a Wi-Fi network. The factory MAC address is globally unique and static, allowing the device to be tracked and individually identified.</u> <u>The MAC randomization feature increases user privacy by using a randomized MAC address when connecting to a Wi-Fi network.</u> <u>MAC addresses are 48 bits long and usually represented by 12 hex digits (6 octets as each octet is 8 bits) such as 00:11:22:AA:BB:CC. The MAC randomization feature randomizes the address by setting the locally administered bit to 1, and the unicast bit to 0. The other 46 bits are randomized.</u> https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior

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

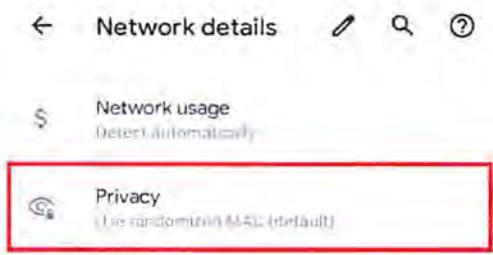
	For devices running Android 10 or higher, the framework uses randomized MAC address by default. Users can enable or disable MAC randomization for individual networks through an option in the Network details screen in Settings, as shown in Figure 1. If a user disables MAC randomization for a network, the framework uses the factory MAC address (globally unique address).  Figure 1. MAC randomization option. https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
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-	The Accused Products practice a method wherein the 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. The Accused Products generate a fake MAC address by generating a randomized MAC address for use in probe requests. This fake MAC address is insufficient to identify the end device. As such, user privacy is increased because the present location of the end-device (i.e. being in a location of communications distance with the access point) is not leaked, as the device MAC address is not identified. That is, the location of the end-user device is not presented to non-authenticated access points.

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

authenticated access points.

Persistent randomization

Android uses the persistent randomization type by default when the MAC randomization feature is enabled. Android generates a persistent randomized MAC address based on the parameters of the network profile including SSID, security type, or FQDN (for Passpoint networks). This MAC address remains the same until factory reset. The MAC address does not get re-randomized if the user forgets and re-adds the Wi-Fi network since the MAC address depends on the parameters of the network profile.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

MAC Randomization Behavior

The MAC randomization feature allows devices to use a randomized MAC address when connecting to a Wi-Fi network. For implementation instructions, see [Implementing MAC Randomization](#). This page describes the behavior of MAC randomization in Android.

MAC addresses are used by devices when connecting to a Wi-Fi network or an access point. Because these MAC addresses are transmitted without encryption, they can be captured and used to potentially track a user's location. Historically, devices use the factory MAC address to associate to a Wi-Fi network. The factory MAC address is globally unique and static, allowing the device to be tracked and individually identified.

The MAC randomization feature increases user privacy by using a randomized MAC address when connecting to a Wi-Fi network.

MAC addresses are 48 bits long and usually represented by 12 hex digits (6 octets as each octet is 8 bits) such as 00:11:22:AA:BB:CC. The MAC randomization feature randomizes the address by setting the *locally administered* bit to 1, and the *unicast* bit to 0. The other 46 bits are randomized.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

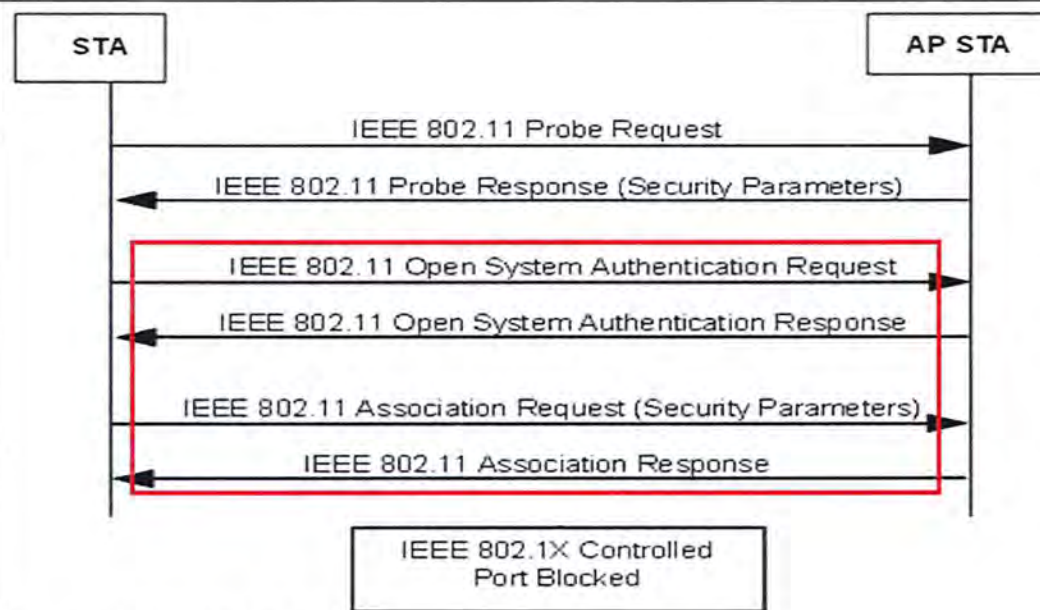
EXHIBIT A-INFRINGEMENT CONTENTIONS FOR U.S. PATENT NO. 10,694,384

	For devices running Android 10 or higher, the framework uses randomized MAC address by default. <u>Users can enable or disable MAC randomization for individual networks through an option in the Network details screen in Settings, as shown in Figure 1. If a user disables MAC randomization for a network, the framework uses the factory MAC address (globally unique address).</u>  Figure 1. MAC randomization option. https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
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.	Generating the fake MAC address includes generating the fake MAC address from one or more characters that are selected randomly. The Accused Products generate a fake MAC address by, for example, randomly setting one or more bits of the MAC address (e.g., setting the locally administered bit to 1, the unicast bit to 0, and then randomizing the remaining 46 bits).

	MAC Randomization Behavior  <u>The MAC randomization feature allows devices to use a randomized MAC address when connecting to a Wi-Fi network. For implementation instructions, see Implementing MAC Randomization. This page describes the behavior of MAC randomization in Android.</u> <u>MAC addresses are used by devices when connecting to a Wi-Fi network or an access point. Because these MAC addresses are transmitted without encryption, they can be captured and used to potentially track a user's location. Historically, devices use the factory MAC address to associate to a Wi-Fi network. The factory MAC address is globally unique and static, allowing the device to be tracked and individually identified.</u> <u>The MAC randomization feature increases user privacy by using a randomized MAC address when connecting to a Wi-Fi network.</u> <u>MAC addresses are 48 bits long and usually represented by 12 hex digits (6 octets as each octet is 8 bits) such as 00:11:22:AA:BB:CC. The MAC randomization feature randomizes the address by setting the <i>locally administered</i> bit to 1, and the <i>unicast</i> bit to 0. The other 46 bits are randomized.</u> https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
6. The method of claim 1, further comprising: receiving, by the end device from the access point, an approval of the connection request; and	The Accused Products receive from the access point, an approval of the connection request and connect to a wireless local area network provided by the access point. For example, as shown below, the Accused Products receive an Authentication Response and/or an Association Response for connecting to the access point. Once this messaging is completed, the Accused Product has joined the network provided by the access point. The network is a wireless local area network (WLAN).

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

connecting, by the end device, to a wireless local area network provided by the access point.



Source: IEEE 802.11-2012.pdf

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

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.

Source: IEEE 802.11-2012.pdf

wireless local area network (WLAN) system: A system that includes the distribution system (DS), access points (APs), and portal entities. It is also the logical location of distribution and integration service functions of an extended service set (ESS). A WLAN system contains one or more APs and zero or more portals in addition to the DS.

Source: IEEE 802.11-2012.pdf

	802.11 Mgmt : Authentication Frame POSTED BY NAYARASI IN CWAP ≈ 10 COMMENTS Once a client station is discover a SSID (Probe Request/Response or listening to Beacons) it move to Join phase. This exchange comprise of at least 4 frames 1. Authentication (Request) 2. Authentication (Response) 3. Association Request 4. Association Response The frame format of those Authentication frames are as shown below.(from page 136- CWAP Official Study Guide) FIGURE 4.8 Authentication frame format https://mrnciew.com/2014/10/10/802-11-mgmt-authentication-frame/ An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
7. The method of claim 6, wherein the access point includes a Wi-Fi	The access point includes a Wi-Fi access point, and the wireless local area network includes a Wi-Fi network. The Accused Products are designed to connect to Wi-Fi access points in order to join a Wi-Fi network.

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

access point, and wherein the wireless local area network includes a Wi-Fi network.	Phone	<u>Galaxy S23</u>	Galaxy S23+	Galaxy S23 Ultra
	<u>Connectivity</u>	5G, <u>Wi-Fi 6E</u> , Bluetooth 5.3, NFC	5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband	5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband
https://www.androidpolice.com/samsung-galaxy-s23/				
Galaxy S23				
				
Wi-Fi 6E				
<u>802.11 a/b/g/n/ac/ax</u>				
https://www.samsung.com/us/smartphones/galaxy-s23/specs/				

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

	• Connectivity: The Galaxy S23 series boasts unparalleled Snapdragon Connect technologies across 5G, Wi-Fi, and Bluetooth®. Featuring the multiple-award-winning Snapdragon X70 5G Modem-RF System with the Qualcomm® 5G AI Processor, the Galaxy S23 series harnesses the power of AI to enable breakthrough 5G coverage, power efficiency, speeds, and latency. These new devices also support 5G+5G/4G Dual-SIM Dual-Active[™], which harnesses the power and flexibility of two 5G SIMs at once. Additionally, all Galaxy S23 series variants feature the Qualcomm® FastConnect™ 6900 and 7800 systems delivering multi-gigabit Wi-Fi speeds, ultra-low latency, and deeply immersive Bluetooth Audio experiences. https://www.qualcomm.com/news/releases/2023/02/qualcomm-and-samsung-partner-to-bring-the-fastest-snapdragon-eve
8. The method of claim 1, further comprising: receiving, by the end device, a list of authenticated access points that includes information regarding one or more access points, 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.	The Accused Products practice a method of receiving a list of authenticated access points that includes information regarding one or more access points, 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. The Accused Products receive a SSID list or preferred network list. The Accused Products support the Wi-Fi standard. According to the standard, a UE (e.g., the accused product) inquires about available Wi-Fi access points using a probe request. The probe request may comprise a SSID list or preferred network list which is a set of SSIDs to which the UE got connected previously. The Accused Products determine that the access point is included in the list when determining that the access point is an authenticated access point.

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

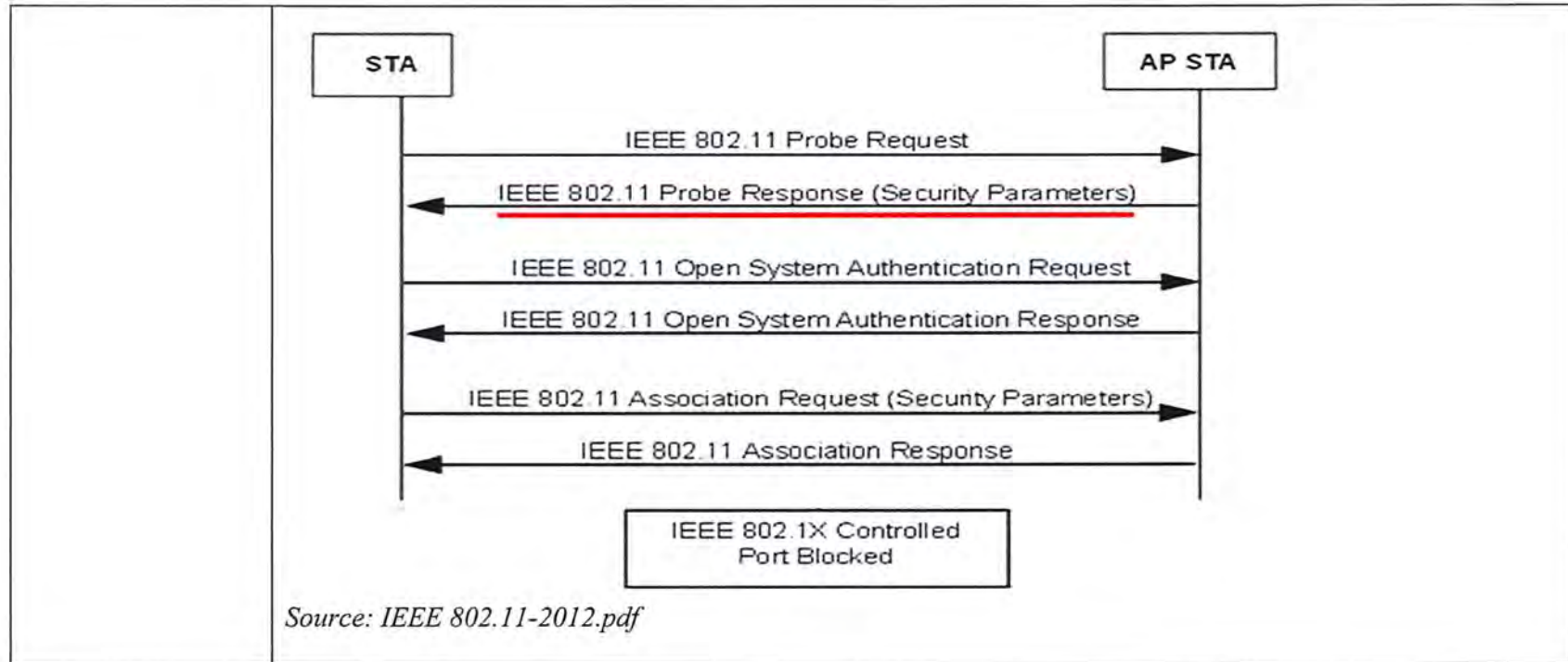


EXHIBIT A-INFRINGEMENT CONTENTIONS FOR U.S. PATENT NO. 10,694,384

	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 <u>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.</u> 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. <i>Source: IEEE 802.11-2012.pdf</i>
--	---

802.11 Mgmt : Authentication Frame

POSTED BY NAYARASI IN CWAP

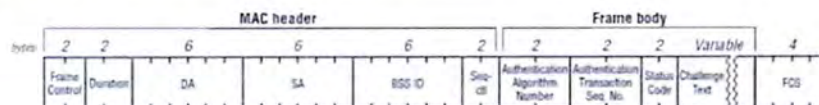
≈ 10 COMMENTS

Once a client station is discover a SSID (Probe Request/Response or listening to Beacons) it move to Join phase. This exchange comprise of at least 4 frames

1. Authentication (Request)
2. Authentication (Response)
3. Association Request
4. Association Response

The frame format of those Authentication frames are as shown below. (from page 136- CWAP Official Study Guide)

FIGURE 4.8 Authentication frame format



<https://mrmcciew.com/2014/10/10/802-11-mgmt-authentication-frame/>

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

	Before answering the question, let us first understand what a preferred network list is. <u>The PNL is a historical record of all the network names (SSIDs) that a device has previously connected to, and trusts to automatically connect to again in the future.</u> User devices trying to connect to a Wi-Fi network watch for access points (APs) broadcasting its availability for a device to connect to its network. Within that information contains the network name, or Service Set Identifier (SSID). Wi-Fi enabled devices trying to connect to a wireless network, and <u>using Active Service Discovery, will then broadcast its interest in connecting to the AP if the network name is in its PNL, which increases the connection speed.</u> For instance, if you connect to a Starbucks Wi-Fi network once, your device will remember and try to <u>automatically connect to any network with the SSID Starbucks.</u> This is true whether you go to the same Starbucks in the future, or a Starbucks 1,000 miles away. All the user device knows is the network name; no additional data is stored. Auto-connecting to wireless networks in PNL saves time and is convenient for the user, but it is a security risk. Therefore, it is important to identify all networks in the PNL and stop connecting automatically to Wi-Fi to stay safe. https://blog.pulsarsecurity.com/preferred-network-list-pnl An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
9. A method performed by an end device, the method comprising:	To the extent the preamble is limiting, the Accused Products practice a method performed by an end device. The Accused Products include Android OS 10 or above or Wear OS 3 or above. Each Accused Product includes an SoC and Wi-Fi connection functionality. As a specific example shown below, the Galaxy S23 includes the Android 13 operating system, which includes randomized MAC for Wi-Fi connections. It comprises an SoC, Snapdragon 8 Gen 2, a Wi-Fi chipset, and FastConnect. It connects to a Wi-Fi network using the Wi-Fi chipset.

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

SAMSUNG

Shop Mobile TV & Audio Appliances Computing Displays Accessories SmartThings

Explore Support For Business

Q

🛒

👤

NEW

Galaxy S23

Unlocked | Lavender

Get up to **\$746** instant trade-in credit

Price Before Trade-In

Get up to **\$799.99**

with Samsung P-Sending

\$33.34/mo for 24 mos

Continue

Learn about Galaxy S23 key features

Save an extra \$100.00 with Samsung Offers Program membership



Galaxy S23 Ultra

Galaxy S23 | S23+

Device

Galaxy S23

\$799.99

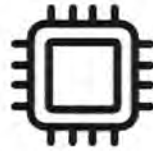
Galaxy S23+

\$799.99

Connectivity

<https://www.samsung.com/us/smartphones/galaxy-s23/buy/galaxy-s23-128gb-unlocked-sm-s911ulixaa/>

Galaxy S23



Super fast processing

Snapdragon® 8 Gen 2

Octa-Core

<https://www.samsung.com/us/smartphones/galaxy-s23/specs/>

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

Phone	<u>Galaxy S23</u>	Galaxy S23+	Galaxy S23 Ultra
Chipset	Snapdragon 8 Gen 2 for Galaxy	Snapdragon 8 Gen 2 for Galaxy	Snapdragon 8 Gen 2 for Galaxy
RAM & Storage	8+128GB, 8+256GB (UFS 3.1)	8+256GB, 8+512GB (UFS 4.0)	8+256GB, 12+512GB, 12GB+1TB (UFS 4.0)
Display	6.1" FHD+ Dynamic AMOLED 2x, 120Hz Adaptive Refresh Rate, 425ppi, 1,750nit (outdoor peak)	6.6" FHD+ Dynamic AMOLED 2x, 120Hz Adaptive Refresh Rate, 393ppi, 1,750nit (outdoor peak)	6.8" QHD+ Dynamic AMOLED 2x, 120Hz Adaptive Refresh Rate, 500ppi, 1,750nit (outdoor peak)
<u>Software</u>	<u>Android 13 / One UI 5.1</u>	Android 13 / One UI 5.1	Android 13 / One UI 5.1

<https://www.androidpolice.com/samsung-galaxy-s23/>



<https://www.youtube.com/watch?v=BadWvxWe8y8>

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

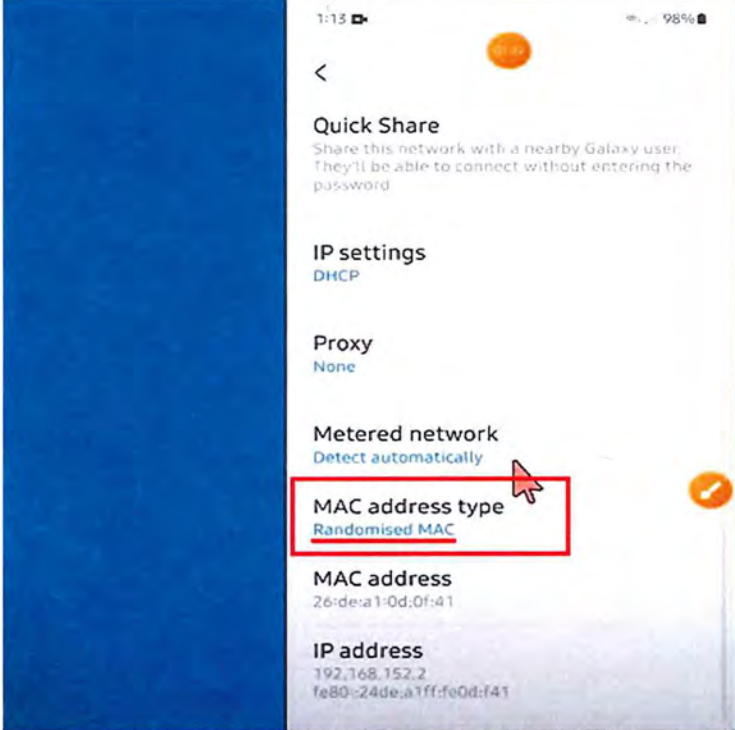
	 The screenshot shows the 'Quick Share' settings on a Galaxy S23 Plus. The 'MAC address type' is set to 'Randomised MAC', which is highlighted with a red box and a red arrow. Other settings visible include 'IP settings' (DHCP), 'Proxy' (None), 'Metered network' (Detect automatically), 'MAC address' (26:de:a1:0d:0f:41), and 'IP address' (192.168.152.2). <u>GALAXY S23, PLUS</u> <u>Set MAC Address Type to</u> <u>Randomized</u> <u>MAC/Phone MAC</u> https://www.youtube.com/watch?v=dT63df6nnqU
--	---

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



Samsung Galaxy S23 / Galaxy S23 Ultra - View MAC Address

<https://www.youtube.com/watch?v=AaMm2HHwbI0>

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

	Featuring the Snapdragon X70 5G Modem RF System, <u>Snapdragon 8 Gen 2</u> is the world's first and only mobile platform with a dedicated 5G AI processor. Plus, gaming, streaming, and communication from home soar via Wi-Fi 7 (the industry's lowest latency offering), all brought to you by the <u>Qualcomm® FastConnect™ 7800 Mobile Connectivity System</u>. • 5G Dual-SIM Dual-Active (DSDA) enables the simultaneous use of two 5G+5G or 5G+4G SIM cards for ultimate user flexibility • Blazing Wi-Fi speeds of up to 5.8 Gbps—more than double Wi-Fi 6 • World's first commercial Wi-Fi 7 SoC, with advanced High Band Simultaneous Multi-Link https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/Snapdragon-8-Gen-2-Product-Brief.pdf • <u>The Samsung Galaxy S23 series features Qualcomm Technologies' leading connectivity solutions</u>, including the Snapdragon® X70 Modem-RF System, the world's fastest and smartest 5G modem-RF system, and <u>Qualcomm® FastConnect™ for high-speed and ultra-low latency Wi-Fi</u>, and the latest Bluetooth audio enhancements. https://www.qualcomm.com/news/releases/2023/02/qualcomm-and-samsung-partner-to-bring-the-fastest-snapdragon-eve MAC Randomization is implemented in devices running the Android OS since at least Android OS 10 as well as Wear OS 3.0.
--	---

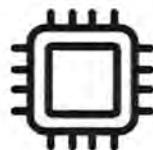
EXHIBIT A-INFRINGEMENT CONTENTIONS FOR U.S. PATENT NO. 10,694,384

	In Android 10, MAC randomization is enabled by default for client mode, SoftAp, and Wi-Fi Direct. MAC randomization prevents listeners from using MAC addresses to build a history of device activity, thus increasing user privacy. Additionally, MAC addresses are randomized as part of Wi-Fi Aware and Wi-Fi RTT operations. For more information, see MAC Randomization Behavior. https://source.android.com/docs/core/connect/wifi-mac-randomization Wear OS, including Wear OS 3.0, is based on Android. See https://developer.android.com/training/wearables/wear-v-mobile#:~:text=Wear%20OS%20is%20based%20on,design%20a%20Wear%20OS%20app. Devices operating on Wear OS 3.0 implement MAC randomization. See https://www.reddit.com/r/GalaxyWatch/comments/pcmkj1/galaxy_watch_4_wifi_mac_address/
[9a] obtaining, by the end device, an authenticated access point list that includes information regarding one or more access points;	The Accused Products obtain an authenticated access point list that includes information regarding one or more access points. For example, the memory stores a list of previously-connected access points, using information received from access points, along with their respective persistent MAC address. In connecting to a Wi-Fi access point, the CPU of the UE receives authenticated access point information stored in its memory. Once confirmed that there is an SSID in a probe response from an access point with which the UE was connected previously, the UE (e.g., the Accused Product) initiates an authentication process with stored pre-shared key information and a previously used authenticated MAC address (e.g., the persistent MAC address used for prior connections with the access point).

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

	android / device / generic / goldfish / refs/tags/android-9.0.0_r34 / wifi / WifiConfigStore.xml <pre>blob: bb5645aacde0f44a93c3386c8e42cf140bfe6a5 [file] [log] [blame]</pre> <pre><?xml version='1.0' encoding='utf-8' standalone='yes' ?> <WifiConfigStoreData> <int name="Version" value="1" /> <NetworkList> <Network> <WifiConfiguration> <string name="ConfigKey">&quot;AndroidWifi&quot;NONE</string> <string name="SSID">&quot;AndroidWifi&quot;</string> <null name="BSSID" /> <null name="PreSharedKey" /> <null name="WEPKeys" /> <int name="WEPKeyIndex" value="0" /> <boolean name="HiddenSSID" value="false" /></pre> https://android.googlesource.com/device/generic/goldfish/+refs/tags/android-9.0.0_r34/wifi/WifiConfigStore.xml An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
[9b] 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;	The Accused Products generate 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. For example, the Accused Products generate a randomized MAC address. As shown below, an example of the Accused Products comprise an SoC, Snapdragon 8 Gen 2. It also includes the Android OS 10 or higher (e.g., Android 13 operating system) and has randomized MAC for Wi-Fi connections. The operating system is used to generate a randomized MAC address to be used for when scanning or searching for access points, such as for Wi-Fi probe requests. The operating system runs on a CPU of the SoC (e.g., the Kryo CPU) of the Accused Product.

Galaxy S23



Super fast processing

Snapdragon® 8 Gen 2

Octa-Core

<https://www.samsung.com/us/smartphones/galaxy-s23/specs/>

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

	Phone	<u>Galaxy S23</u>	Galaxy S23+	Galaxy S23 Ultra
	Chipset	Snapdragon 8 Gen 2 for Galaxy	Snapdragon 8 Gen 2 for Galaxy	Snapdragon 8 Gen 2 for Galaxy
	RAM & Storage	8+128GB, 8+256GB (UFS 3.1)	8+256GB, 8+512GB (UFS 4.0)	8+256GB, 12+512GB, 12GB+1TB (UFS 4.0)
	Display	6.1" FHD+ Dynamic AMOLED 2x, 120Hz Adaptive Refresh Rate, 425ppi, 1,750nit (outdoor peak)	6.6" FHD+ Dynamic AMOLED 2x, 120Hz Adaptive Refresh Rate, 393ppi, 1,750nit (outdoor peak)	6.8" QHD+ Dynamic AMOLED 2x, 120Hz Adaptive Refresh Rate, 500ppi, 1,750nit (outdoor peak)
	<u>Software</u>	<u>Android 13 / One UI 5.1</u>	Android 13 / One UI 5.1	Android 13 / One UI 5.1
	https://www.androidpolice.com/samsung-galaxy-s23/			
				
	CPU Kryo CPU • 64-bit Architecture • 1 Prime core, up to 3.36 GHz² • Arm Cortex-X3 technology • 4 Performance cores, up to 2.8 GHz • 3 Efficiency cores, up to 2.0 GHz			

<https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/Snapdragon-8-Gen-2-Product-Brief.pdf>

Phone	<u>Galaxy S23</u>	Galaxy S23+	Galaxy S23 Ultra
<u>Connectivity</u>	5G, <u>Wi-Fi 6E</u> , Bluetooth 5.3, NFC	5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband	5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband

<https://www.androidpolice.com/samsung-galaxy-s23/>

Galaxy S23



Wi-Fi 6E

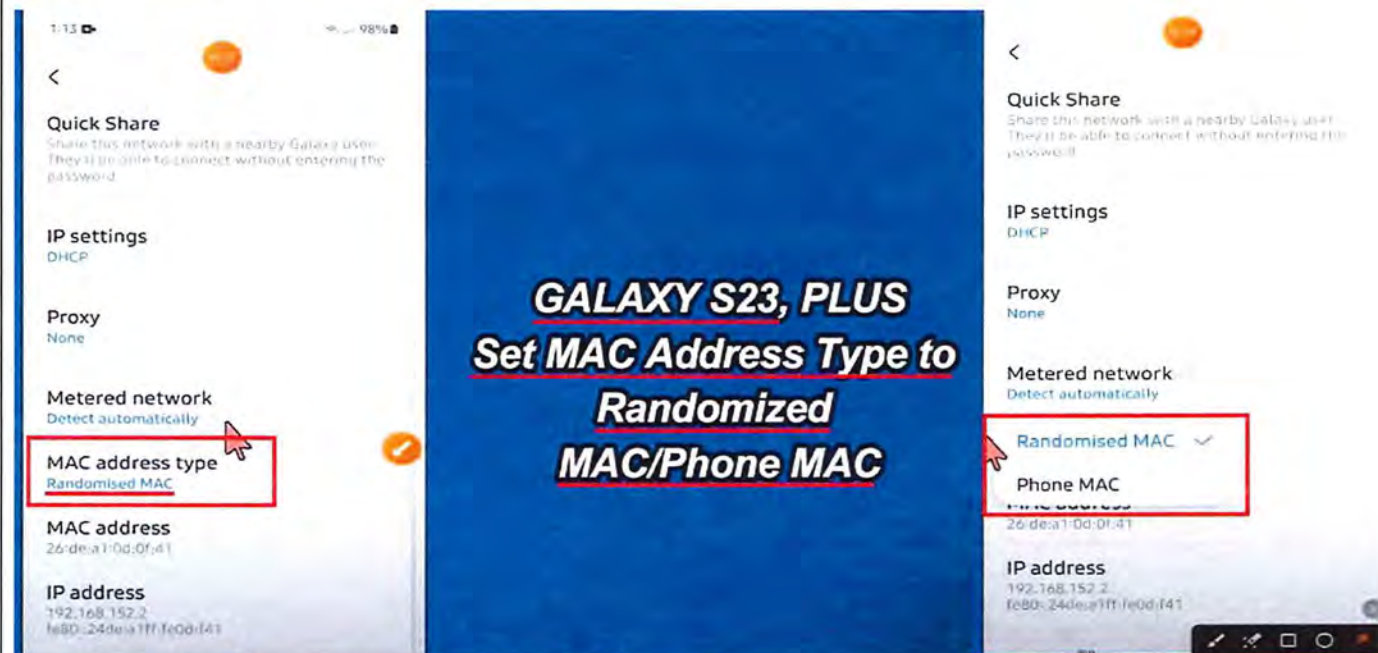
802.11 a/b/g/n/ac/ax

<https://www.samsung.com/us/smartphones/galaxy-s23/specs/>

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

- **Connectivity:** The Galaxy S23 series boasts unparalleled Snapdragon Connect technologies across 5G, Wi-Fi, and Bluetooth®. Featuring the multiple-award-winning Snapdragon X70 5G Modem-RF System with the Qualcomm® 5G AI Processor, the Galaxy S23 series harnesses the power of AI to enable breakthrough 5G coverage, power efficiency, speeds, and latency. These new devices also support 5G+5G/4G Dual-SIM Dual-Active³, which harnesses the power and flexibility of two 5G SIMs at once. Additionally, all Galaxy S23 series variants feature the Qualcomm® FastConnect™ 6900 and 7800 systems delivering multi-gigabit Wi-Fi speeds, ultra-low latency, and deeply immersive Bluetooth Audio experiences.

<https://www.qualcomm.com/news/releases/2023/02/qualcomm-and-samsung-partner-to-bring-the-fastest-snapdragon-eve>



<https://www.youtube.com/watch?v=dT63df6nnqU>

The Accused Products support the Wi-Fi standard. According to the standard, the Accused Products (each a UE) inquire about available Wi-Fi access points using a probe request that includes a MAC address. For a probe request the Accused Products use a randomized MAC address, which is a fake MAC address.

MAC Randomization Behavior

The MAC randomization feature allows devices to use a randomized MAC address when connecting to a Wi-Fi network. For implementation instructions, see [Implementing MAC Randomization](#). This page describes the behavior of MAC randomization in Android.

MAC addresses are used by devices when connecting to a Wi-Fi network or an access point. Because these MAC addresses are transmitted without encryption, they can be captured and used to potentially track a user's location. Historically, devices use the factory MAC address to associate to a Wi-Fi network. The factory MAC address is globally unique and static, allowing the device to be tracked and individually identified.

The MAC randomization feature increases user privacy by using a randomized MAC address when connecting to a Wi-Fi network.

MAC addresses are 48 bits long and usually represented by 12 hex digits (6 octets as each octet is 8 bits) such as 00:11:22:AA:BB:CC. The MAC randomization feature randomizes the address by setting the locally administered bit to 1, and the unicast bit to 0. The other 46 bits are randomized.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

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

	For devices running Android 10 or higher, the framework uses randomized MAC address by default. <u>Users can enable or disable MAC randomization for individual networks through an option in the Network details screen in Settings, as shown in Figure 1. If a user disables MAC randomization for a network, the framework uses the factory MAC address (globally unique address).</u>  Figure 1. MAC randomization option. https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
[9c] transmitting, by the end device to at least one access point, a probe request that includes the generated MAC address;	The Accused Products receive from the access point, a probe response that includes information regarding the access point. As an example, a probe response from a Wi-Fi access point includes the SSID (wireless network name), supported data rates, encryption types, capabilities, etc. of the access point; 2. APs receiving the probe request check to see if the mobile station has at least one common supported data rate. If they have compatible data rates, a probe response is sent advertising the SSID (wireless network name), supported data rates, encryption types if required, and other 802.11 capabilities of the AP. https://documentation.meraki.com/MR/Wi-Fi Basics and Best Practices/802.11 Association Process Explained The Accused Products support the Wi-Fi standard. The Accused Products receive probe responses from multiple available access points. As an example, an access point responds with the probe response when the SSID in the probe request is the wildcard SSID or matches the specific SSID of the access point or when the specific SSID

of the access point is included in the SSID List element. As a further example, an access point responds to a probe request when it supports data rates or other requirements of the Accused Products.

Persistent randomization

Android uses the persistent randomization type by default when the MAC randomization feature is enabled. Android generates a persistent randomized MAC address based on the parameters of the network profile including SSID, security type, or FQDN (for Passpoint networks). This MAC address remains the same until factory reset. The MAC address does not get re-randomized if the user forgets and re-adds the Wi-Fi network since the MAC address depends on the parameters of the network profile.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

MAC Randomization Behavior

The MAC randomization feature allows devices to use a randomized MAC address when connecting to a Wi-Fi network. For implementation instructions, see [Implementing MAC Randomization](#). This page describes the behavior of MAC randomization in Android.

MAC addresses are used by devices when connecting to a Wi-Fi network or an access point. Because these MAC addresses are transmitted without encryption, they can be captured and used to potentially track a user's location. Historically, devices use the factory MAC address to associate to a Wi-Fi network. The factory MAC address is globally unique and static, allowing the device to be tracked and individually identified.

The MAC randomization feature increases user privacy by using a randomized MAC address when connecting to a Wi-Fi network.

MAC addresses are 48 bits long and usually represented by 12 hex digits (6 octets as each octet is 8 bits) such as 00:11:22:AA:BB:CC. The MAC randomization feature randomizes the address by setting the locally administered bit to 1, and the unicast bit to 0. The other 46 bits are randomized.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

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

For devices running Android 10 or higher, the framework uses randomized MAC address by default. Users can enable or disable MAC randomization for individual networks through an option in the **Network details** screen in **Settings**, as shown in Figure 1. If a user disables MAC randomization for a network, the framework uses the factory MAC address (globally unique address).

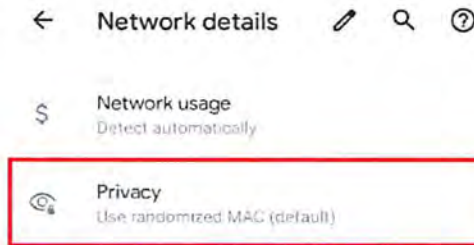


Figure 1. MAC randomization option.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

MAC Randomization Behavior

The MAC randomization feature allows devices to use a randomized MAC address when connecting to a Wi-Fi network. For implementation instructions, see [Implementing MAC Randomization](#). This page describes the behavior of MAC randomization in Android.

MAC addresses are used by devices when connecting to a Wi-Fi network or an access point. Because these MAC addresses are transmitted without encryption, they can be captured and used to potentially track a user's location. Historically, devices use the factory MAC address to associate to a Wi-Fi network. The factory MAC address is globally unique and static, allowing the device to be tracked and individually identified.

The MAC randomization feature increases user privacy by using a randomized MAC address when connecting to a Wi-Fi network.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

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

IP settings
DHCP

Proxy
None

Metered network
Detect automatically

MAC address type
Randomised MAC

MAC address
26:de:a1:0d:0f:41

GALAXY S23, PLUS
Set MAC Address Type to
Randomized
MAC/Phone MAC

<https://www.youtube.com/watch?v=dT63df6nnqU>

STA

AP STA

IEEE 802.11 Probe Request

IEEE 802.11 Probe Response (Security Parameters)

IEEE 802.11 Open System Authentication Request

IEEE 802.11 Open System Authentication Response

IEEE 802.11 Association Request (Security Parameters)

IEEE 802.11 Association Response

IEEE 802.11X Controlled Port Blocked

Source: IEEE 802.11-2012.pdf

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

Information regarding the access point is included in the probe response, as shown below.

Table 8-27—Probe Response frame body

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability	
4	SSID	If dot11MeshActivated is true, the SSID element is the wildcard value as described in § 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.
9	IBSS Parameter Set	The IBSS Parameter Set element is present only within Probe Response frames generated by STAs in an IBSS.
10	Country	The Country element is present if dot11MultiDomainCapabilityActivated is true or dot11SpectrumManagementRequired is true or dot11RadioMeasurementActivated is true.
11	FH Parameters	The FH Parameters element, as specified in § 4.2.11, is optionally present if dot11MultiDomainCapabilityActivated is true.
12	FH Pattern Table	The FH Pattern Table element, as specified in § 4.2.12, is optionally present if dot11MultiDomainCapabilityActivated is true.
13	Power Constraint	The Power Constraint element is present if dot11SpectrumManagementRequired is true and is optionally present if dot11RadioMeasurementActivated is true.
14	Channel Switch Announcement	The Channel Switch Announcement element is optionally present if dot11SpectrumManagementRequired is true.
15	Quiet	The Quiet element is optionally present if dot11SpectrumManagementRequired is true or if dot11RadioMeasurementActivated is true.
16	IBSS DFS	The IBSS DFS element is present if dot11SpectrumManagementRequired is true in an IBSS.
17	TPC Report	The TPC Report element is present if dot11SpectrumManagementRequired is true or dot11RadioMeasurementActivated is true.
18	ERP	The ERP element is present within Probe Response frames generated by STAs using ERPs and is optionally present otherwise.
19	Extended Supported Rates	The Extended Supported Rates element is present if there are more than eight supported rates, and it is optionally present otherwise.
20	RSN	The RSN is present only if dot11RSNAActivated is true.
21	BSS Load	The BSS Load element is present if dot11QoSOptionImplemented and dot11QBSSLoadImplemented are both true.
22	EDCA Parameter Set	The EDCA Parameter Set element is present if dot11QoSOptionImplemented is true and dot11MeshActivated is

<https://mrncciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

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

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.
26	AP Channel Report	If dot11RMChannelReportActivated is true, one AP Channel Report element is optionally present for each operating class that has at least 1 channel to report.
27	BSS Average Access Delay	The BSS Average Access Delay element is optionally present if dot11RMBSSAverageAccessDelayActivated is true and the value of the AP Average Access Delay field is not equal to 255 (measurement not available).
28	Antenna	The Antenna element is optionally present if dot11RMAntennaInformationActivated is true and the value of the Antenna ID field is not equal to 0 (unknown antenna).
29	BSS Available Admission Capacity	The BSS Available Admission Capacity element is optionally present if dot11RMBSSAvailableAdmissionCapacityActivated is true with the following exceptions: 1) when Available Admission Capacity Bitmask equals 0 (Available Admission Capacity List contains no entries), or 2) when the BSS Load element is present and the Available Capacity Bitmask equals 256 (Available Admission Capacity List contains only the AC_VO entry).
30	BSS AC Access Delay	The BSS AC Access Delay element is optionally present if dot11RMBSSAverageAccessDelayActivated is true and at least one field of the element is not equal to 255 (measurement not available).
31	Mobility Domain	The MDE is present if dot11FastBSSTransitionActivated is true.
32	DSE registered location	The DSE Registered Location element is present if dot11LCDSERequired is true.
33	Extended Channel Switch Announcement	The Extended Channel Switch Announcement element is optionally present if dot11ExtendedChannelSwitchActivated is true.
34	Supported Operating Classes	The Supported Operating Classes element is present if dot11ExtendedChannelSwitchActivated is true.
35	HT Capabilities	The HT Capabilities element is present when dot11HighThroughputOptionImplemented attribute is true.
36	HT Operation	The HT Operation element is included by an AP and a mesh STA when dot11HighThroughputOptionImplemented attribute is true.
37	20-40 BSS Coexistence	The 20-40 BSS Coexistence element is optionally present when the dot112040BSSCoexistenceManagementSupport attribute is true.
38	Overlapping BSS Scan Parameters	The Overlapping BSS Scan Parameters element is optionally present if the dot11FortyMHzOptionImplemented attribute is true.
39	Extended Capabilities	The Extended Capabilities element is optionally present if any of the fields in this element are nonzero.

<https://mrnciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

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

40	QoS Traffic Capability	The QoS Traffic Capability element is optionally present if dot11MgmtOptionACStationCountActivated is true
41	Channel Usage	The Channel Usage element is present if the Channel Usage element is present in the Probe Request frame and dot11MgmtOptionChannelUsageActivated is true
42	Time Advertisement	The Time Advertisement element is present if dot11MgmtOptionUTCSTSOOffsetActivated is true.
43	Time Zone	The Time Zone element is present if dot11MgmtOptionUTCSTSOOffsetActivated is true.
44	Interworking	The Interworking element is present if dot11InterworkingServiceActivated is true
45	Advertisement Protocol	Advertisement Protocol element is present if dot11InterworkingServiceActivated is true and at least one dot11GASAdvertisementID MIB attribute exists
46	Roaming Consortium	The Roaming Consortium element is present if dot11InterworkingServiceActivated is true and the dot11RoamingConsortiumTable has at least one entry
47	Emergency Alert Identifier	One or more Emergency Alert Identifier elements are present if dot11EASActivated is true and there are one or more EAS message(s) active in the network
48	Mesh ID	The Mesh ID element is present if dot11MeshActivated is true.
49	Mesh Configuration	The Mesh Configuration element is present if dot11MeshActivated is true
50	Mesh Awake Window	The Mesh Awake Window element is optionally present if dot11MeshActivated is true
51	Beacon Timing	The Beacon Timing element is optionally present if both dot11MeshActivated and dot11MBCAActivated are true
52	MCCAOP Advertisement Overview	The MCCAOP Advertisement Overview element is optionally present if both dot11MeshActivated and dot11MCCAActivated are true
53	MCCAOP Advertisement	One or more MCCAOP Advertisement elements are optionally present if both dot11MeshActivated and dot11MCCAActivated are true.
54	Mesh Channel Switch Parameters	The Mesh Channel Switch Parameters element is present if dot11MeshActivated is true and either Channel Switch Announcement element or Extended Channel Switch Announcement element is present
Last-1	Vendor Specific	One or more vendor-specific elements are optionally present. These elements follow all other elements, except the Requested elements
Last-n	Requested elements	Elements requested by the Request element of the Probe Request frame are present if dot11MultiDomainCapabilityActivated is true See 10.1.4.3.2.

<https://mmcciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

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

4.3.13.15 SSID list

The SSID List element enables the non-AP STA to request information on a list of SSIDs. This is intended to reduce the number of Probe Request frames sent by the non-AP STA.

Source: IEEE 802.11-2012.pdf

In an infrastructure BSS or in an IBSS, STAs receiving Probe Request frames shall respond with a probe response when the SSID in the probe request is the wildcard SSID or matches the specific SSID of the STA or when the specific SSID of the STA is included in the SSID List element. Furthermore, a STA with dot11RadioMeasurementActivated true receiving a probe request with a DSSS Parameter Set element containing a Current Channel field value that is not the same as the value of dot11CurrentChannel shall not respond with a probe response. An AP shall respond to all probe requests meeting the above criteria. In an IBSS a STA that transmitted a Beacon frame since the last TBTT shall respond to group addressed Probe Request frames. A STA in an IBSS shall respond to Probe Request frames sent to the individual address of the STA.

Source: IEEE 802.11-2012.pdf

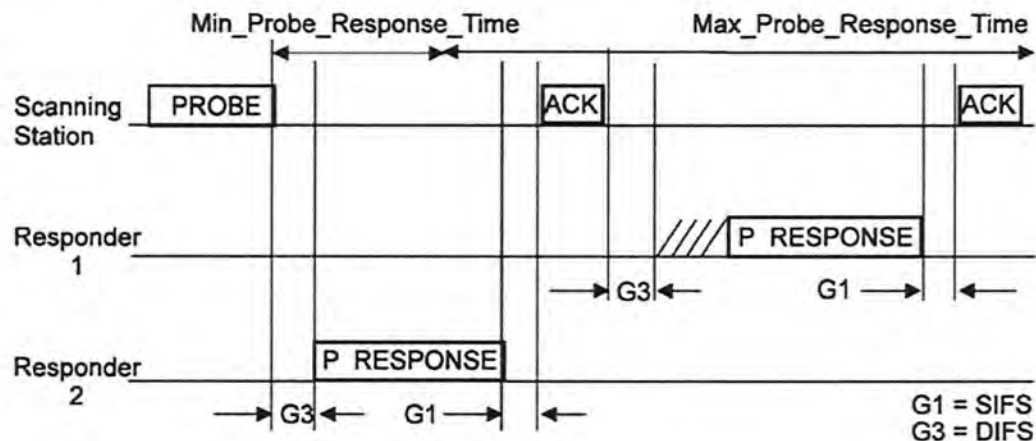


Figure 10-3—Probe response

Source: IEEE 802.11-2012.pdf

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

Before answering the question, let us first understand what a preferred network list is. The PNL is a historical record of all the network names (SSIDs) that a device has previously connected to, and trusts to automatically connect to again in the future.

User devices trying to connect to a Wi-Fi network watch for access points (APs) broadcasting its availability for a device to connect to its network. Within that information contains the network name, or Service Set Identifier (SSID). Wi-Fi enabled devices trying to connect to a wireless network, and using Active Service Discovery, will then broadcast its interest in connecting to the AP if the network name is in its PNL, which increases the connection speed.

For instance, if you connect to a Starbucks Wi-Fi network once, your device will remember and try to automatically connect to any network with the SSID Starbucks. This is true whether you go to the same Starbucks in the future, or a Starbucks 1,000 miles away. All the user device knows is the network name; no additional data is stored. Auto-connecting to wireless networks in PNL saves time and is convenient for the user, but it is a security risk. Therefore, it is important to identify all networks in the PNL and stop connecting automatically to Wi-Fi to stay safe.

<https://blog.pulsarsecurity.com/preferred-network-list-pnl>

The reason for client scanning is to determine a suitable AP to which the client may need to roam now or in the future. A client can use two scanning methods: active and passive. During an active scan, the client radio transmits a probe request and listens for a probe response from an AP. With a passive scan, the client radio listens on each channel for beacons sent periodically by an AP. A passive scan generally takes more time, since the client must listen and wait for a beacon versus actively probing to find an AP. Another limitation with a passive scan is that if the client does not wait long enough on a channel, then the client may miss an AP beacon.

<https://www.wi-fi.org/knowledge-center/faq/what-are-passive-and-active-scanning>

Below is an example of a Wi-Fi probe response that includes information of the access point.

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

802.11 Management - Probe Response

- Probe Timestamp: 23996945615 Microseconds [24-31]
- Beacon Interval: 102 Time Units (104 Milliseconds, and 448 Microseconds) [32-33]
- Capability Info: 0001000000000001
- SSID ID=0 SSID Len=4 SSID=OPEN
- Supported Rates
 - Element ID: 1 Supported Rates [41]
 - Length: 4 [43]
 - Supported Rate: 24.0 Mbps (BSS Basic Rate) [44]
 - Supported Rate: 36.0 Mbps (Not BSS Basic Rate) [45]
 - Supported Rate: 48.0 Mbps (Not BSS Basic Rate) [46]
 - Supported Rate: 54.0 Mbps (Not BSS Basic Rate) [47]
- Country
 - Element ID: 7 Country [48]
 - Length: 18 [49]
 - Country Code: AU [50-51]
 - Environment: 0x20 Any [52]
 - Starting Channel: 36 [53]
 - Number of Channels: 4 [54]
 - Max Tx Power (dBm): 23 [55]
 - Starting Channel: 52 [56]
 - Number of Channels: 4 [57]
 - Max Tx Power (dBm): 23 [58]
 - Starting Channel: 100 [59]
 - Number of Channels: 5 [60]
 - Max Tx Power (dBm): 30 [61]
 - Starting Channel: 132 [62]
 - Number of Channels: 3 [63]
 - Max Tx Power (dBm): 30 [64]
 - Starting Channel: 149 [65]
 - Number of Channels: 5 [66]
 - Max Tx Power (dBm): 30 [67]
- QSS Load
 - Element ID: 11 QSS Load [68]
 - Length: 5 [69]
 - Station Count: 1 [70-71]
 - Channel Utilization: 0 % [72]
 - Avail Admission Capacity: 26562 [73-74]
- HT Cap= ID=45 HT Cap Len=26

<https://mrnciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.

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

[9d] 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;	The Accused Products receive from the access point (e.g., a Wi-Fi access point), a probe response that includes information regarding the access point (e.g., information such as SSID, supported data rates, etc.). A Wi-Fi probe response includes the SSID (wireless network name), supported data rates, etc. of the access point: 2. APs receiving the probe request check to see if the mobile station has at least one common supported data rate. If they have compatible data rates, a probe response is sent advertising the SSID (wireless network name), supported data rates, encryption types if required, and other 802.11 capabilities of the AP. https://documentation.meraki.com/MR/Wi-Fi Basics and Best Practices/802.11 Association Process Explained The Accused Products support the Wi-Fi standard. The Accused Products receive the probe responses from multiple available access points. An access point responds with the probe response only when the SSID in the probe request is the wildcard SSID or matches the specific SSID of the access point or when the specific SSID of the access point is included in the SSID List element. <u>Persistent randomization</u> <u>Android uses the persistent randomization type by default when the MAC randomization feature is enabled. Android generates a persistent randomized MAC address based on the parameters of the network profile including SSID, security type, or FQDN (for Passpoint networks). This MAC address remains the same until factory reset. The MAC address does not get re-randomized if the user forgets and re-adds the Wi-Fi network since the MAC addressed depends on the parameters of the network profile.</u> https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior
---	--

MAC Randomization Behavior -

The MAC randomization feature allows devices to use a randomized MAC address when connecting to a Wi-Fi network. For implementation instructions, see [Implementing MAC Randomization](#). This page describes the behavior of MAC randomization in Android.

MAC addresses are used by devices when connecting to a Wi-Fi network or an access point. Because these MAC addresses are transmitted without encryption, they can be captured and used to potentially track a user's location. Historically, devices use the factory MAC address to associate to a Wi-Fi network. The factory MAC address is globally unique and static, allowing the device to be tracked and individually identified.

The MAC randomization feature increases user privacy by using a randomized MAC address when connecting to a Wi-Fi network.

MAC addresses are 48 bits long and usually represented by 12 hex digits (6 octets as each octet is 8 bits) such as 00:11:22:AA:BB:CC. The MAC randomization feature randomizes the address by setting the locally administered bit to 1, and the unicast bit to 0. The other 46 bits are randomized.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

For devices running Android 10 or higher, the framework uses randomized MAC address by default. Users can enable or disable MAC randomization for individual networks through an option in the **Network details** screen in **Settings**, as shown in Figure 1. If a user disables MAC randomization for a network, the framework uses the factory MAC address (globally unique address).

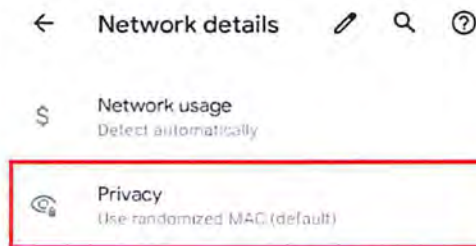


Figure 1. MAC randomization option.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

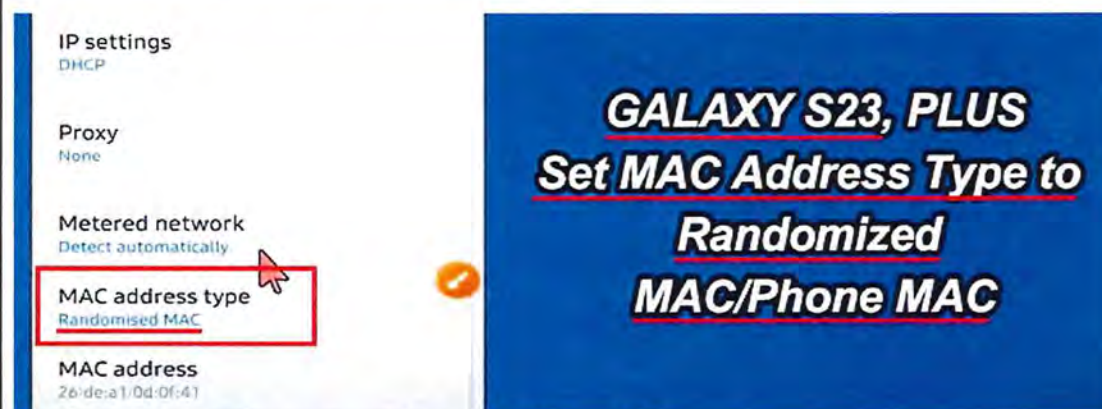
MAC Randomization Behavior

The MAC randomization feature allows devices to use a randomized MAC address when connecting to a Wi-Fi network. For implementation instructions, see [Implementing MAC Randomization](#). This page describes the behavior of MAC randomization in Android.

MAC addresses are used by devices when connecting to a Wi-Fi network or an access point. Because these MAC addresses are transmitted without encryption, they can be captured and used to potentially track a user's location. Historically, devices use the factory MAC address to associate to a Wi-Fi network. The factory MAC address is globally unique and static, allowing the device to be tracked and individually identified.

The MAC randomization feature increases user privacy by using a randomized MAC address when connecting to a Wi-Fi network.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>



<https://www.youtube.com/watch?v=dT63df6nnqU>

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

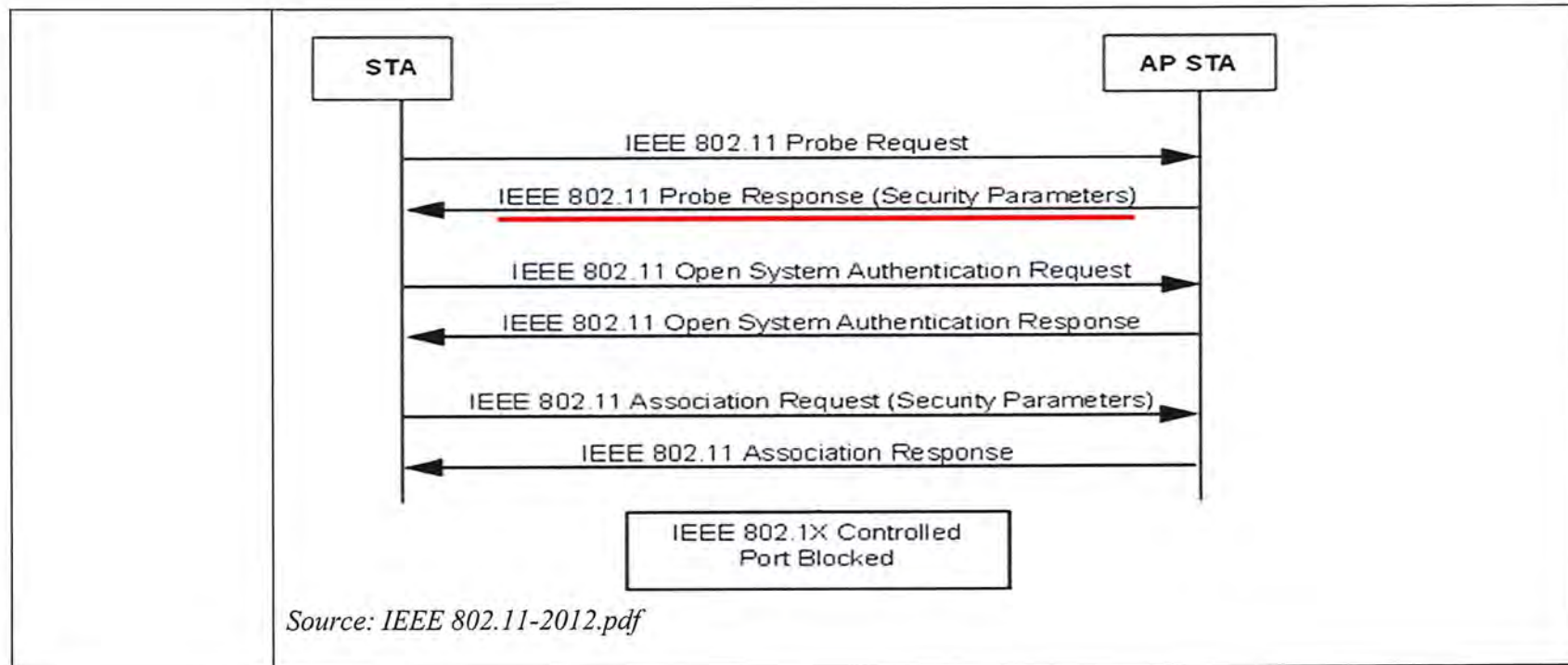


EXHIBIT A-INFRINGEMENT CONTENTIONS FOR U.S. PATENT NO. 10,694,384

Table 8-27—Probe Response frame body		
Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability	
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.
9	IBSS Parameter Set	The IBSS Parameter Set element is present only within Probe Response frames generated by STAs in an IBSS.
10	Country	The Country element is present if dot11MultiDomainCapabilityActivated is true or dot11SpectrumManagementRequired is true or dot11RadioMeasurementActivated is true.
11	FH Parameters	The FH Parameters element, as specified in 8.4.2.11, is optionally present if dot11MultiDomainCapabilityActivated is true.
12	FH Pattern Table	The FH Pattern Table element, as specified in 8.4.2.12, is optionally present if dot11MultiDomainCapabilityActivated is true.
13	Power Constraint	The Power Constraint element is present if dot11SpectrumManagementRequired is true and is optionally present if dot11RadioMeasurementActivated is true.
14	Channel Switch Announcement	The Channel Switch Announcement element is optionally present if dot11SpectrumManagementRequired is true.
15	Quiet	The Quiet element is optionally present if dot11SpectrumManagementRequired is true or if dot11RadioMeasurementActivated is true.
16	IBSS DFS	The IBSS DFS element is present if dot11SpectrumManagementRequired is true in an IBSS.
17	TPC Report	The TPC Report element is present if dot11SpectrumManagementRequired is true or dot11RadioMeasurementActivated is true.
18	ERP	The ERP element is present within Probe Response frames generated by STAs using ERPs and is optionally present otherwise.
19	Extended Supported Rates	The Extended Supported Rates element is present if there are more than eight supported rates, and it is optionally present otherwise.
20	RSN	The RSNE is present only if dot11RSNAActivated is true.
21	BSS Load	The BSS Load element is present if dot11QoSOptionImplemented and dot11QBSSLoadImplemented are both true.
22	EDCA Parameter Set	The EDCA Parameter Set element is present if dot11QoSOptionImplemented is true and dot11MeshActivated is

<https://mrnciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

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

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.
26	AP Channel Report	If dot11RMChannelReportActivated is true, one AP Channel Report element is optionally present for each operating class that has at least 1 channel to report.
27	BSS Average Access Delay	The BSS Average Access Delay element is optionally present if dot11RMBSSAverageAccessDelayActivated is true and the value of the AP Average Access Delay field is not equal to 255 (measurement not available).
28	Antenna	The Antenna element is optionally present if dot11RMAntennaInformationActivated is true and the value of the Antenna ID field is not equal to 0 (unknown antenna).
29	BSS Available Admission Capacity	The BSS Available Admission Capacity element is optionally present if dot11RMBSSAvailableAdmissionCapacityActivated is true with the following exceptions: 1) when Available Admission Capacity Bitmap equals 0 (Available Admission Capacity List contains no entries), or 2) when the BSS Load element is present and the Available Capacity Bitmap equals 256 (Available Admission Capacity List contains only the AC_VO entry).
30	BSS AC Access Delay	The BSS AC Access Delay element is optionally present if dot11RMBSSAverageAccessDelayActivated is true and at least one field of the element is not equal to 255 (measurement not available).
31	Mobility Domain	The MDE is present if dot11FastBSSTransitionActivated is true.
32	DSE registered location	The DSE Registered Location element is present if dot11LCIDSERequired is true.
33	Extended Channel Switch Announcement	The Extended Channel Switch Announcement element is optionally present if dot11ExtendedChannelSwitchActivated is true.
34	Supported Operating Classes	The Supported Operating Classes element is present if dot11ExtendedChannelSwitchActivated is true.
35	HT Capabilities	The HT Capabilities element is present when dot11HighThroughputOptionImplemented attribute is true.
36	HT Operation	The HT Operation element is included by an AP and a mesh STA when dot11HighThroughputOptionImplemented attribute is true.
37	20-40 BSS Coexistence	The 20-40 BSS Coexistence element is optionally present when the dot112040BSSCoexistenceManagementSupport attribute is true.
38	Overlapping BSS Scan Parameters	The Overlapping BSS Scan Parameters element is optionally present if the dot11FortyMHzOptionImplemented attribute is true.
39	Extended Capabilities	The Extended Capabilities element is optionally present if any of the fields in this element are nonzero.

<https://mrnciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

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

40	QoS Traffic Capability	The QoS Traffic Capability element is optionally present if dot11MgmtOptionACStationCountActivated is true
41	Channel Usage	The Channel Usage element is present if the Channel Usage element is present in the Probe Request frame and dot11MgmtOptionChannelUsageActivated is true
42	Time Advertisement	The Time Advertisement element is present if dot11MgmtOptionUTCTSOOffsetActivated is true.
43	Time Zone	The Time Zone element is present if dot11MgmtOptionUTCTSOOffsetActivated is true.
44	Interworking	The Interworking element is present if dot11InterworkingServiceActivated is true
45	Advertisement Protocol	Advertisement Protocol element is present if dot11InterworkingServiceActivated is true and at least one dot11GASAdvertisementID MIB attribute exists
46	Roaming Consortium	The Roaming Consortium element is present if dot11InterworkingServiceActivated is true and the dot11RoamingConsortiumTable has at least one entry.
47	Emergency Alert Identifier	One or more Emergency Alert Identifier elements are present if dot11EASActivated is true and there are one or more EAS message(s) active in the network
48	Mesh ID	The Mesh ID element is present if dot11MeshActivated is true.
49	Mesh Configuration	The Mesh Configuration element is present if dot11MeshActivated is true
50	Mesh Awake Window	The Mesh Awake Window element is optionally present if dot11MeshActivated is true
51	Beacon Tuning	The Beacon Tuning element is optionally present if both dot11MeshActivated and dot11MBCAActivated are true
52	MCCAOP Advertisement Overview	The MCCAOP Advertisement Overview element is optionally present if both dot11MeshActivated and dot11MCCAActivated are true
53	MCCAOP Advertisement	One or more MCCAOP Advertisement elements are optionally present if both dot11MeshActivated and dot11MCCAActivated are true
54	Mesh Channel Switch Parameters	The Mesh Channel Switch Parameters element is present if dot11MeshActivated is true and either Channel Switch Announcement element or Extended Channel Switch Announcement element is present.
Last-1	Vendor Specific	One or more vendor-specific elements are optionally present. These elements follow all other elements, except the Requested elements
Last-n	Requested elements	Elements requested by the Request element of the Probe Request frame are present if dot11MultiDomainCapabilityActivated is true. See 10.1.4.3.2.

<https://mrnciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

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

4.3.13.15 SSID list

The SSID List element enables the non-AP STA to request information on a list of SSIDs. This is intended to reduce the number of Probe Request frames sent by the non-AP STA.

Source: IEEE 802.11-2012.pdf

In an infrastructure BSS or in an IBSS, STAs receiving Probe Request frames shall respond with a probe response when the SSID in the probe request is the wildcard SSID or matches the specific SSID of the STA or when the specific SSID of the STA is included in the SSID List element. Furthermore, a STA with dot11RadioMeasurementActivated true receiving a probe request with a DSSS Parameter Set element containing a Current Channel field value that is not the same as the value of dot11CurrentChannel shall not respond with a probe response. An AP shall respond to all probe requests meeting the above criteria. In an IBSS a STA that transmitted a Beacon frame since the last TBTT shall respond to group addressed Probe Request frames. A STA in an IBSS shall respond to Probe Request frames sent to the individual address of the STA.

Source: IEEE 802.11-2012.pdf

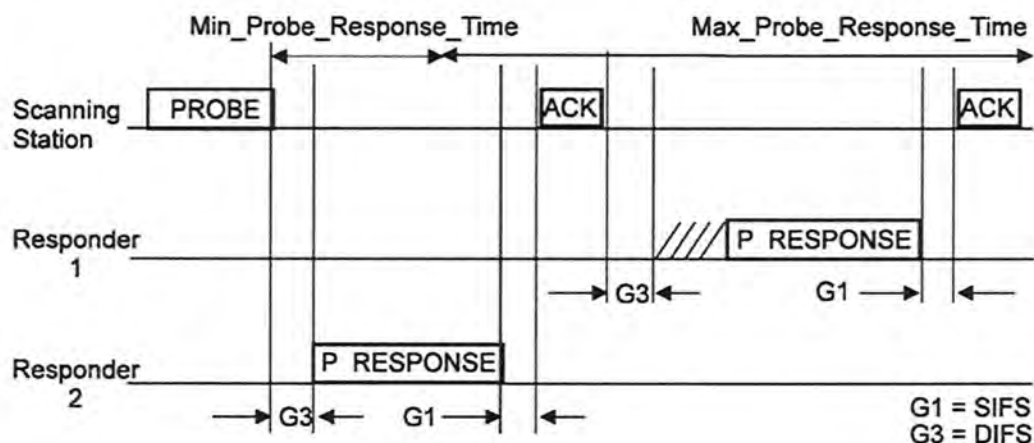


Figure 10-3—Probe response

Source: IEEE 802.11-2012.pdf

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

Before answering the question, let us first understand what a preferred network list is. The PNL is a historical record of all the network names (SSIDs) that a device has previously connected to, and trusts to automatically connect to again in the future.

User devices trying to connect to a Wi-Fi network watch for access points (APs) broadcasting its availability for a device to connect to its network. Within that information contains the network name, or Service Set Identifier (SSID). Wi-Fi enabled devices trying to connect to a wireless network, and using Active Service Discovery, will then broadcast its interest in connecting to the AP if the network name is in its PNL, which increases the connection speed.

For instance, if you connect to a Starbucks Wi-Fi network once, your device will remember and try to automatically connect to any network with the SSID Starbucks. This is true whether you go to the same Starbucks in the future, or a Starbucks 1,000 miles away. All the user device knows is the network name; no additional data is stored. Auto-connecting to wireless networks in PNL saves time and is convenient for the user, but it is a security risk. Therefore, it is important to identify all networks in the PNL and stop connecting automatically to Wi-Fi to stay safe.

<https://blog.pulsarsecurity.com/preferred-network-list-pnl>

The reason for client scanning is to determine a suitable AP to which the client may need to roam now or in the future. A client can use two scanning methods: active and passive. During an active scan, the client radio transmits a probe request and listens for a probe response from an AP. With a passive scan, the client radio listens on each channel for beacons sent periodically by an AP. A passive scan generally takes more time, since the client must listen and wait for a beacon versus actively probing to find an AP. Another limitation with a passive scan is that if the client does not wait long enough on a channel, then the client may miss an AP beacon.

<https://www.wi-fi.org/knowledge-center/faq/what-are-passive-and-active-scanning>

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

802.11 Management - Probe Response

- Probe Timestamp: 23996945615 Microseconds [24-31]
- Beacon Interval: 102 Time Units (104 Milliseconds, and 448 Microseconds) [32-33]
- Capability Info: %0001000000000001
- SSID ID=0 SSID Len=4 SSID=OPEN
- Supported Rates**
 - Element ID: 1 Supported Rates [42]
 - Length: 4 [43]
 - Supported Rate: 24.0 Mbps (BSS Basic Rate) [44]
 - Supported Rate: 36.0 Mbps (Not BSS Basic Rate) [45]
 - Supported Rate: 48.0 Mbps (Not BSS Basic Rate) [46]
 - Supported Rate: 54.0 Mbps (Not BSS Basic Rate) [47]
- Country**
 - Element ID: 7 Country [48]
 - Length: 18 [49]
 - Country Code: AU [50-51]
 - Environment: 0x20 Any [52]
 - Starting Channel: 36 [53]
 - Number of Channels: 4 [54]
 - Max Tx Power (dBm): 23 [55]
 - Starting Channel: 52 [56]
 - Number of Channels: 4 [57]
 - Max Tx Power (dBm): 23 [58]
 - Starting Channel: 100 [59]
 - Number of Channels: 5 [60]
 - Max Tx Power (dBm): 30 [61]
 - Starting Channel: 132 [62]
 - Number of Channels: 3 [63]
 - Max Tx Power (dBm): 30 [64]
 - Starting Channel: 149 [65]
 - Number of Channels: 5 [66]
 - Max Tx Power (dBm): 30 [67]
- QBSS Load**
 - Element ID: 11 QBSS Load [68]
 - Length: 5 [69]
 - Station Count: 1 [70-71]
 - Channel Utilization: 0 % [72]
 - Avail Admission Capacity: 26562 [73-74]
- HT Cap= ID=45 HT Cap Len=26

<https://mrnciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.

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

[9e] 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,	The Accused Products perform a method of determining that the access point (e.g., a Wi-Fi access point) is an authenticated access point (e.g., a previously connected Wi-Fi access point) based, at least in part, on the information in the probe response being indicative that the access point (e.g., a Wi-Fi access point) is an authenticated access point. As an example, 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. As shown, 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. <u>Persistent randomization</u> <u>Android uses the persistent randomization type by default when the MAC randomization feature is enabled. Android generates a persistent randomized MAC address based on the parameters of the network profile including SSID, security type, or FQDN (for Passpoint networks). This MAC address remains the same until factory reset. The MAC address does not get re-randomized if the user forgets and re-adds the Wi-Fi network since the MAC addressed depends on the parameters of the network profile.</u> <u>Persistent MAC addresses are necessary in cases where networks rely on the persistence of the MAC address to provide useful functionality to the user, for example, to remember a device and allow users to bypass the login screen as expected, or to enable parental controls.</u> <u>For Android 10 and 11, the framework uses persistent randomization for all networks when MAC randomization is enabled.</u> https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior
--	--

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

[android / device / generic / goldfish / refs/tags/android-9.0.0_r34 / _ / wifi / WifiConfigStore.xml](#)

blob: bb5645aacde0f44a93c3386c8e42cf140bfe6a5 [file] [log] [blame]

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<WifiConfigStoreData>
  <int name="Version" value="1" />
  <NetworkList>
    <Network>
      <WifiConfiguration>
        <string name="ConfigKey">&quot;AndroidWifi&quot;NONE</string>
        <string name="SSID">&quot;AndroidWifi&quot;</string>
        <null name="BSSID" />
        <null name="PreSharedKey" />
        <null name="WEPKeys" />
        <int name="WEPKeyIndex" value="0" />
        <boolean name="HiddenSSID" value="false" />
```

https://android.googlesource.com/device/generic/goldfish/+refs/tags/android-9.0.0_r34/wifi/WifiConfigStore.xml

In an infrastructure BSS or in an IBSS, STAs receiving Probe Request frames shall respond with a probe response when the SSID in the probe request is the wildcard SSID or matches the specific SSID of the STA or when the specific SSID of the STA is included in the SSID List element. Furthermore, a STA with dot11RadioMeasurementActivated true receiving a probe request with a DSSS Parameter Set element containing a Current Channel field value that is not the same as the value of dot11CurrentChannel shall not respond with a probe response. An AP shall respond to all probe requests meeting the above criteria. In an IBSS a STA that transmitted a Beacon frame since the last TBTT shall respond to group addressed Probe Request frames. A STA in an IBSS shall respond to Probe Request frames sent to the individual address of the STA.

Source: IEEE 802.11-2012.pdf

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

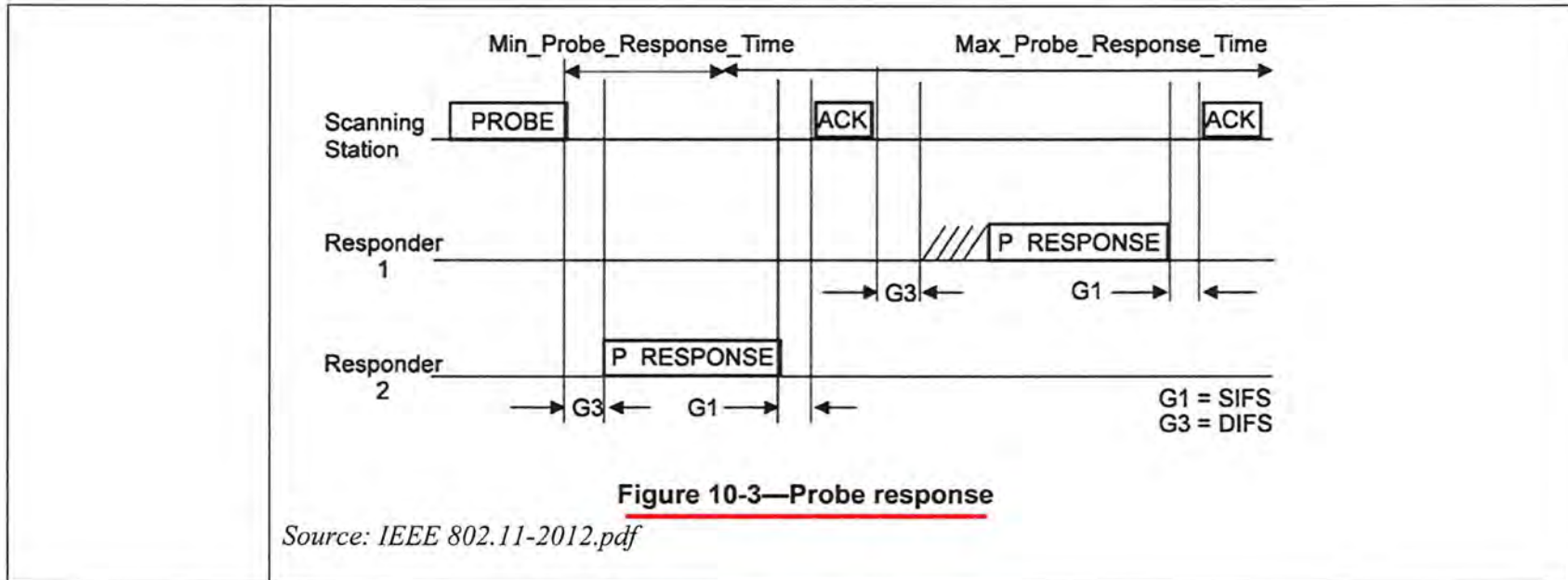


EXHIBIT A-INFRINGEMENT CONTENTIONS FOR U.S. PATENT NO. 10,694,384

Before answering the question, let us first understand what a preferred network list is. The PNL is a historical record of all the network names (SSIDs) that a device has previously connected to, and trusts to automatically connect to again in the future.

User devices trying to connect to a Wi-Fi network watch for access points (APs) broadcasting its availability for a device to connect to its network. Within that information contains the network name, or Service Set Identifier (SSID). Wi-Fi enabled devices trying to connect to a wireless network, and using Active Service Discovery, will then broadcast its interest in connecting to the AP if the network name is in its PNL, which increases the connection speed.

For instance, if you connect to a **Starbucks** Wi-Fi network once, your device will remember and try to automatically connect to any network with the SSID Starbucks. This is true whether you go to the same Starbucks in the future, or a Starbucks 1,000 miles away. All the user device knows is the network name; no additional data is stored. Auto-connecting to wireless networks in PNL saves time and is convenient for the user, but it is a security risk. Therefore, it is important to identify all networks in the PNL and stop connecting automatically to Wi-Fi to stay safe.

<https://blog.pulsarsecurity.com/preferred-network-list-pnl>

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

The screenshot displays a Wi-Fi packet analysis tool showing a '802.11 Management - Probe Response' packet. The packet structure is as follows:

- Probe Timestamp:** 23996945615 Microseconds [24-31]
- Beacon Interval:** 102 Time Units (104 Milliseconds, and 448 Microseconds) [32-33]
- Capability Info:** %0001000000000001
- SSID ID=0 SSID Len=4 SSID=OPEN** (Annotated with a red box and a callout: "information regarding access point")
- Supported Rates** (Annotated with a red box and a callout: "information regarding access point")
 - Element ID: 1 Supported Rates [42]
 - Length: 4 [43]
 - Supported Rate: 24.0 Mbps (BSS Basic Rate) [44]
 - Supported Rate: 36.0 Mbps (Not BSS Basic Rate) [45]
 - Supported Rate: 48.0 Mbps (Not BSS Basic Rate) [46]
 - Supported Rate: 54.0 Mbps (Not BSS Basic Rate) [47]
- Country** (Annotated with a red box and a callout: "information regarding access point")
 - Element ID: 7 Country [48]
 - Length: 18 [49]
 - Country Code: AU [50-51]
 - Environment: 0x20 Any [52]
 - Starting Channel: 36 [53]
 - Number of Channels: 4 [54]
 - Max Tx Power (dBm): 23 [55]
 - Starting Channel: 52 [56]
 - Number of Channels: 4 [57]
 - Max Tx Power (dBm): 23 [58]
 - Starting Channel: 100 [59]
 - Number of Channels: 5 [60]
 - Max Tx Power (dBm): 30 [61]
 - Starting Channel: 132 [62]
 - Number of Channels: 3 [63]
 - Max Tx Power (dBm): 30 [64]
 - Starting Channel: 149 [65]
 - Number of Channels: 5 [66]
 - Max Tx Power (dBm): 30 [67]
- OBSS Load** (Annotated with a red box)
 - Element ID: 11 OBSS Load [68]
 - Length: 5 [69]
 - Station Count: 1 [70-71]
 - Channel Utilization: 0 % [72]
 - Avail Admission Capacity: 26562 [73-74]
- HT Cap= ID=45 HT Cap Len=26**

The entire packet structure is enclosed in a large red box, with a callout pointing to it labeled "probe response".

<https://mrnciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.

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

[9f] 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	The Accused Products determine that the access point (e.g., a Wi-Fi access point) is an authenticated access point (e.g., a previously connected Wi-Fi access point) is based, at least in part, on the information in the probe response being indicative that the access point is an authenticated access point by determining that the information regarding the at least one access point is included in the authenticated access point list. The Accused Products confirm the received access point identifying information (e.g., the SSID information) from the probe responses with the access point information stored in its memory. If the received information correlates to the access point list, then the access point was previously connected and thus an authenticated access point. Once confirmed that there is an SSID in a probe response from an access point with which the UE was connected previously, the UE (e.g., the Accused Product) initiates an authentication process with stored pre-shared key information and a previously used authenticated MAC address (e.g., the persistent MAC address used for prior connections with the access point). As shown, the Accused Products maintain a list of previously-connected access points and a persistent MAC address for each access point. The list of previously-connected access points is matched to the access point's SSID received in the probe response. <u>Persistent randomization</u> <u>Android uses the persistent randomization type by default when the MAC randomization feature is enabled. Android generates a persistent randomized MAC address based on the parameters of the network profile including SSID, security type, or FQDN (for Passpoint networks). This MAC address remains the same until factory reset. The MAC address does not get re-randomized if the user forgets and re-adds the Wi-Fi network since the MAC addressed depends on the parameters of the network profile.</u> <u>Persistent MAC addresses are necessary in cases where networks rely on the persistence of the MAC address to provide useful functionality to the user, for example, to remember a device and allow users to bypass the login screen as expected, or to enable parental controls.</u> <u>For Android 10 and 11, the framework uses persistent randomization for all networks when MAC randomization is enabled.</u> https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior
--	--

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

[android](#) / [device](#) / [generic](#) / [goldfish](#) / [refs/tags/android-9.0.0_r34](#) / [wifi](#) / [WifiConfigStore.xml](#)

blob: bb5645aacde00f44a93c3386c8e42cf140bfe6a5 [file] [log] [blame]

```

1  <?xml version='1.0' encoding='utf-8' standalone='yes' ?>
2  <WifiConfigStoreData>
3      <int name="Version" value="1" />
4      <NetworkList>
5          <Network>
6              <WifiConfiguration>
7                  <string name="ConfigKey">&quot;AndroidWifi&quot;NONE</string>
8                  <string name="SSID">&quot;AndroidWifi&quot;</string>
9                  <null name="BSSID" />
10                 <null name="PreSharedKey" />
11                 <null name="WEPKeys" />
12                 <int name="WEPKeyIndex" value="0" />
13                 <boolean name="HiddenSSID" value="false" />

```

https://android.googlesource.com/device/generic/goldfish/+refs/tags/android-9.0.0_r34/wifi/WifiConfigStore.xml

In an infrastructure BSS or in an IBSS, STAs receiving Probe Request frames shall respond with a probe response when the SSID in the probe request is the wildcard SSID or matches the specific SSID of the STA or when the specific SSID of the STA is included in the SSID List element. Furthermore, a STA with dot11RadioMeasurementActivated true receiving a probe request with a DSSS Parameter Set element containing a Current Channel field value that is not the same as the value of dot11CurrentChannel shall not respond with a probe response. An AP shall respond to all probe requests meeting the above criteria. In an IBSS a STA that transmitted a Beacon frame since the last TBTT shall respond to group addressed Probe Request frames. A STA in an IBSS shall respond to Probe Request frames sent to the individual address of the STA.

Source: IEEE 802.11-2012.pdf

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

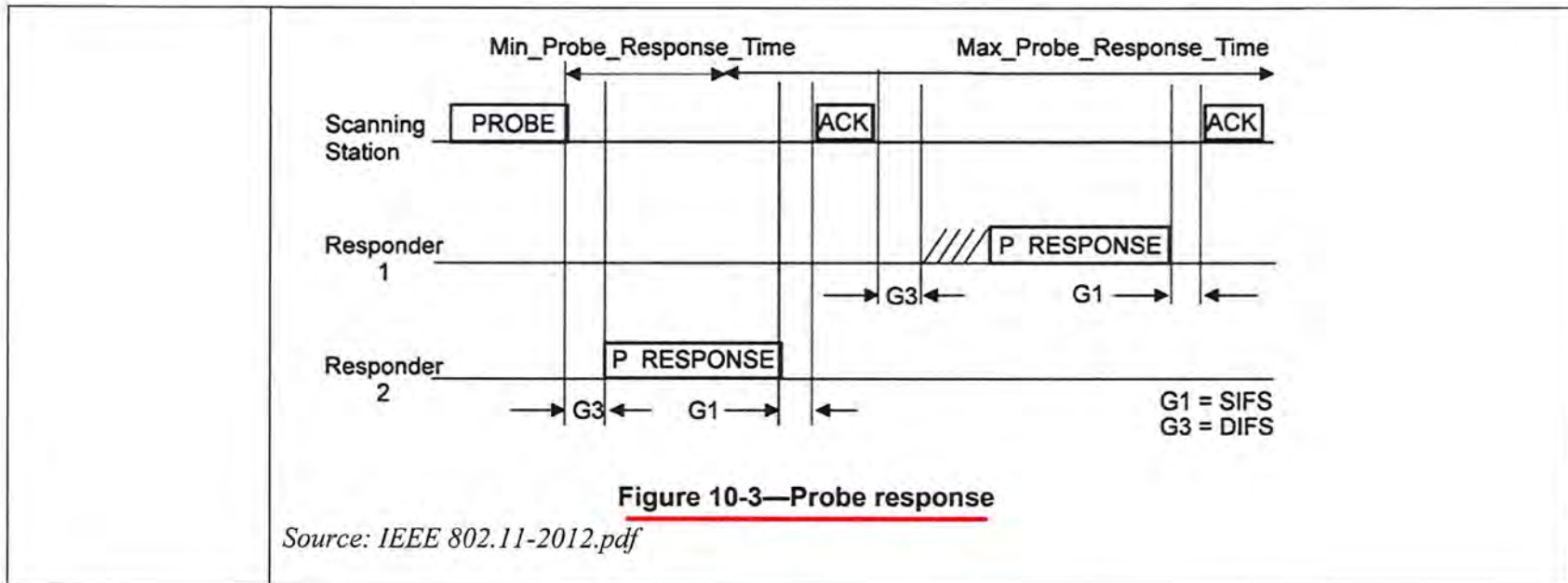


EXHIBIT A-INFRINGEMENT CONTENTIONS FOR U.S. PATENT NO. 10,694,384

Before answering the question, let us first understand what a preferred network list is. The PNL is a historical record of all the network names (SSIDs) that a device has previously connected to, and trusts to automatically connect to again in the future.

User devices trying to connect to a Wi-Fi network watch for access points (APs) broadcasting its availability for a device to connect to its network. Within that information contains the network name, or Service Set Identifier (SSID). Wi-Fi enabled devices trying to connect to a wireless network, and using Active Service Discovery, will then broadcast its interest in connecting to the AP if the network name is in its PNL, which increases the connection speed.

For instance, if you connect to a **Starbucks** Wi-Fi network once, your device will remember and try to automatically connect to any network with the SSID Starbucks. This is true whether you go to the same Starbucks in the future, or a Starbucks 1,000 miles away. All the user device knows is the network name; no additional data is stored. Auto-connecting to wireless networks in PNL saves time and is convenient for the user, but it is a security risk. Therefore, it is important to identify all networks in the PNL and stop connecting automatically to Wi-Fi to stay safe.

<https://blog.pulsarsecurity.com/preferred-network-list-pnl>

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

The screenshot displays a Wi-Fi probe response packet analysis. Red boxes and arrows highlight specific fields and their relevance to the infringement contentions.

- Probe Response Header:**
 - Probe Timestamp: 23996945615 Microseconds [24-31]
 - Beacon Interval: 102 Time Units (104 Milliseconds, and 448 Microseconds) [32-33]
 - Capability Info: 0001000000000001
 - SSID ID=0 SSID Len=4 SSID=OPEN
- Supported Rates:**
 - Element ID: 1 Supported Rates [42]
 - Length: 4 [43]
 - Supported Rate: 24.0 Mbps (BSS Basic Rate) [44]
 - Supported Rate: 36.0 Mbps (Not BSS Basic Rate) [45]
 - Supported Rate: 48.0 Mbps (Not BSS Basic Rate) [46]
 - Supported Rate: 54.0 Mbps (Not BSS Basic Rate) [47]
- Country:**
 - Element ID: 7 Country [48]
 - Length: 18 [49]
 - Country Code: AU [50-51]
 - Environment: 0x20 Any [52]
 - Starting Channel: 36 [53]
 - Number of Channels: 4 [54]
 - Max Tx Power (dBm): 23 [55]
 - Starting Channel: 52 [56]
 - Number of Channels: 4 [57]
 - Max Tx Power (dBm): 23 [58]
 - Starting Channel: 100 [59]
 - Number of Channels: 5 [60]
 - Max Tx Power (dBm): 30 [61]
 - Starting Channel: 132 [62]
 - Number of Channels: 3 [63]
 - Max Tx Power (dBm): 30 [64]
 - Starting Channel: 149 [65]
 - Number of Channels: 5 [66]
 - Max Tx Power (dBm): 30 [67]
- QSS Load:**
 - Element ID: 11 QSS Load [68]
 - Length: 5 [69]
 - Station Count: 1 [70-71]
 - Channel Utilization: 0 % [72]
 - Avail Admission Capacity: 26562 [73-74]
- HT Cap:**
 - HT Cap ID=45 HT Cap Len=26

Red annotations include:

- A box around the SSID ID=0 SSID Len=4 SSID=OPEN field with an arrow pointing to it labeled "information regarding access point".
- A box around the Supported Rates field with an arrow pointing to it labeled "information regarding access point".
- A box around the Country field with an arrow pointing to it labeled "information regarding access point".
- A box around the QSS Load field with an arrow pointing to it labeled "probe response".

<https://mrncciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.

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

[9g] 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.	The Accused Products transmit to the access point determined to be the authenticated access point, a connection request, such as an association message or other message for connecting to the access point. The message includes an authentic device identifier for the end device. For example, the message includes a persistent MAC address for connecting to the access point. After receiving the probe response from the access point, as discussed above, the Accused Products confirm the received SSID information from the probe responses with the access point information stored in its memory. Once confirmed that there is an SSID in a probe response from an access point with which the UE was connected previously, the Accused Products initiate a connection using the persistent MAC address for the access point, which is an authentic device identifier for the Accused Product. <u>Persistent randomization</u> <u>Android uses the persistent randomization type by default when the MAC randomization feature is enabled. Android generates a persistent randomized MAC address based on the parameters of the network profile including SSID, security type, or FQDN (for Passpoint networks). This MAC address remains the same until factory reset. The MAC address does not get re-randomized if the user forgets and re-adds the Wi-Fi network since the MAC address depends on the parameters of the network profile.</u> https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior
--	--

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

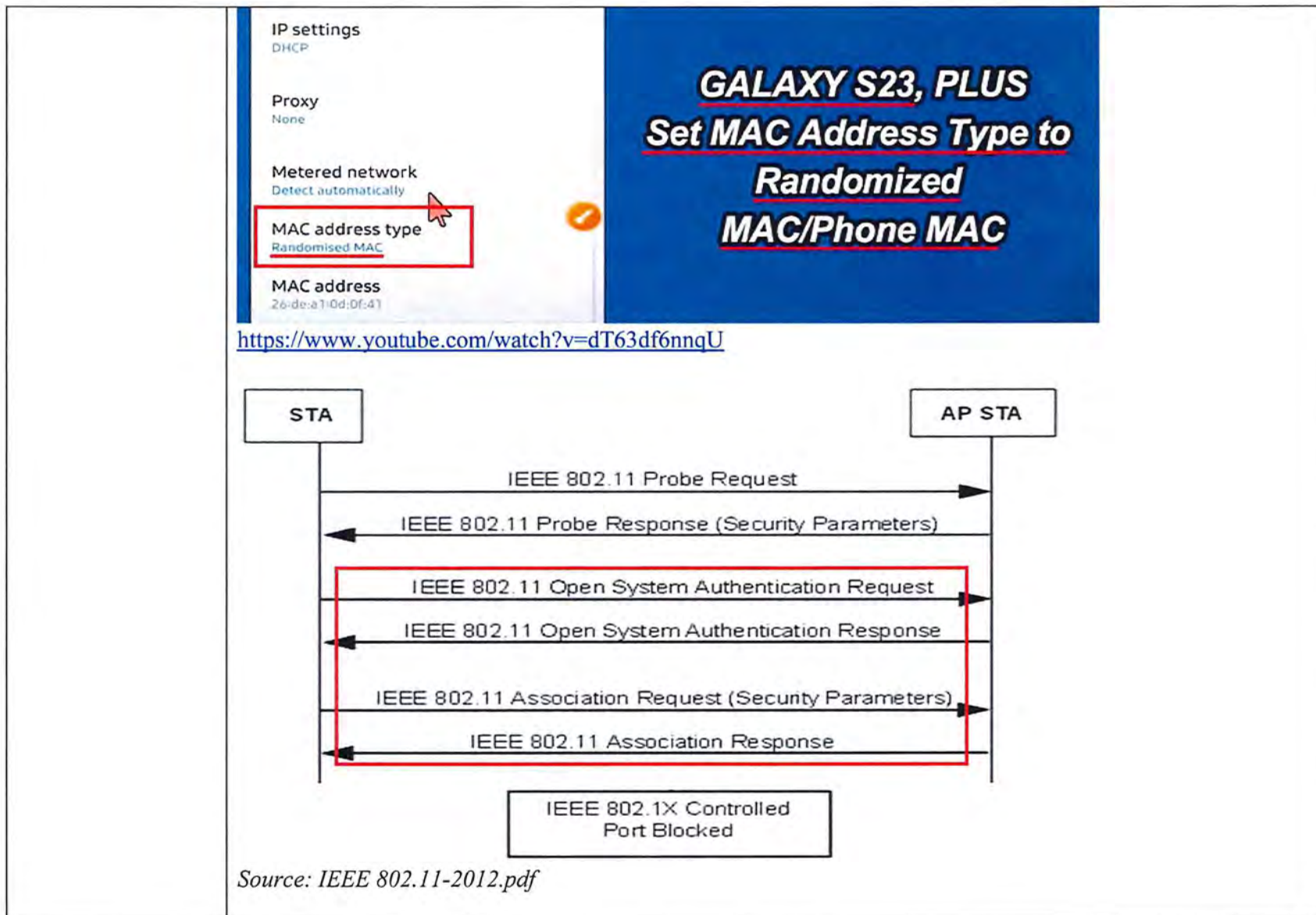
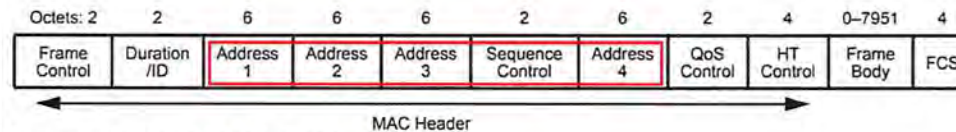


EXHIBIT A-INFRINGEMENT CONTENTIONS FOR U.S. PATENT NO. 10,694,384

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.



Source: IEEE 802.11-2012.pdf

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.

Source: IEEE 802.11-2012.pdf

802.11 Mgmt : Authentication Frame

POSTED BY NAYARASI IN CWAP

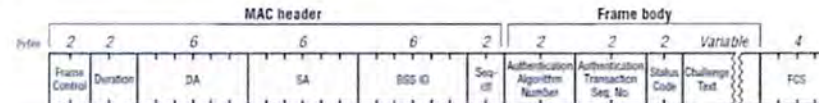
≈ 10 COMMENTS

Once a client station is discover a SSID (Probe Request/Response or listening to Beacons) it move to Join phase. This exchange comprise of at least 4 frames

1. Authentication (Request)
2. Authentication (Response)
3. Association Request
4. Association Response

The frame format of those Authentication frames are as shown below. (from page 136- CWAP Official Study Guide)

FIGURE 4.8 Authentication frame format



<https://mmcciew.com/2014/10/10/802-11-mgmt-authentication-frame/>

As shown, the Accused Products may use persistent randomization, in which for the same Wi-Fi network and device combination, the MAC address remains the same. When an Accused Product connects to a Wi-Fi network it was previously connected to, it will use the same MAC address.

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

Persistent randomization

Android uses the persistent randomization type by default when the MAC randomization feature is enabled. Android generates a persistent randomized MAC address based on the parameters of the network profile including SSID, security type, or FQDN (for Passpoint networks). This MAC address remains the same until factory reset. The MAC address does **not** get re-randomized if the user forgets and re-adds the Wi-Fi network since the MAC address depends on the parameters of the network profile.

Persistent MAC addresses are necessary in cases where networks rely on the persistence of the MAC address to provide useful functionality to the user, for example, to remember a device and allow users to bypass the login screen as expected, or to enable parental controls.

For Android 10 and 11, the framework uses persistent randomization for all networks when MAC randomization is enabled.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

[android / device / generic / goldfish / refs/tags/android-9.0.0_r34 / _ / wifi / WifiConfigStore.xml](#)

blob: bb5645aacde0f44a93c3386c8e42cf140bfe6a5 [file] [log] [blame]

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<WifiConfigStoreData>
  <int name="Version" value="1" />
  <NetworkList>
    <Network>
      <WifiConfiguration>
        <string name="ConfigKey">&quot;AndroidWifi&quot;NONE</string>
        <string name="SSID">&quot;AndroidWifi&quot;</string>
        <null name="BSSID" />
        <null name="PreSharedKey" />
        <null name="WEPKeys" />
        <int name="WEPKeyIndex" value="0" />
        <boolean name="HiddenSSID" value="false" />
```

https://android.googlesource.com/device/goldfish/+refs/tags/android-9.0.0_r34/wifi/WifiConfigStore.xml

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

	An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
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.	The Accused Products practice a method wherein the fake MAC address is distinct from an actual original MAC address of a hardware network interface of the end device. The Accused Products generate a fake MAC address by generating a randomized MAC address for use in probe requests. This fake MAC address is insufficient to identify the end device. As such, user privacy is increased because the present location of the end-device (i.e. being in a location of communication distance with the access point) is not leaked, as the device MAC address is not identified. That is, the location of the end-user device is not presented to non-authenticated access points. <u>Persistent randomization</u> <u>Android uses the persistent randomization type by default when the MAC randomization feature is enabled. Android generates a persistent randomized MAC address based on the parameters of the network profile including SSID, security type, or FQDN (for Passpoint networks).</u> This MAC address remains the same until factory reset. The MAC address does not get re-randomized if the user forgets and re-adds the Wi-Fi network since the MAC addressed depends on the parameters of the network profile. https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior

MAC Randomization Behavior

The MAC randomization feature allows devices to use a randomized MAC address when connecting to a Wi-Fi network. For implementation instructions, see [Implementing MAC Randomization](#). This page describes the behavior of MAC randomization in Android.

MAC addresses are used by devices when connecting to a Wi-Fi network or an access point. Because these MAC addresses are transmitted without encryption, they can be captured and used to potentially track a user's location. Historically, devices use the factory MAC address to associate to a Wi-Fi network. The factory MAC address is globally unique and static, allowing the device to be tracked and individually identified.

The MAC randomization feature increases user privacy by using a randomized MAC address when connecting to a Wi-Fi network.

MAC addresses are 48 bits long and usually represented by 12 hex digits (6 octets as each octet is 8 bits) such as 00:11:22:AA:BB:CC. The MAC randomization feature randomizes the address by setting the *locally administered* bit to 1, and the *unicast* bit to 0. The other 46 bits are randomized.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

For devices running Android 10 or higher, the framework uses randomized MAC address by default. Users can enable or disable MAC randomization for individual networks through an option in the **Network details** screen in **Settings**, as shown in Figure 1. If a user disables MAC randomization for a network, the framework uses the factory MAC address (globally unique address).

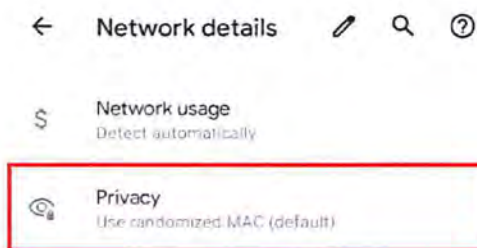


Figure 1. MAC randomization option.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

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

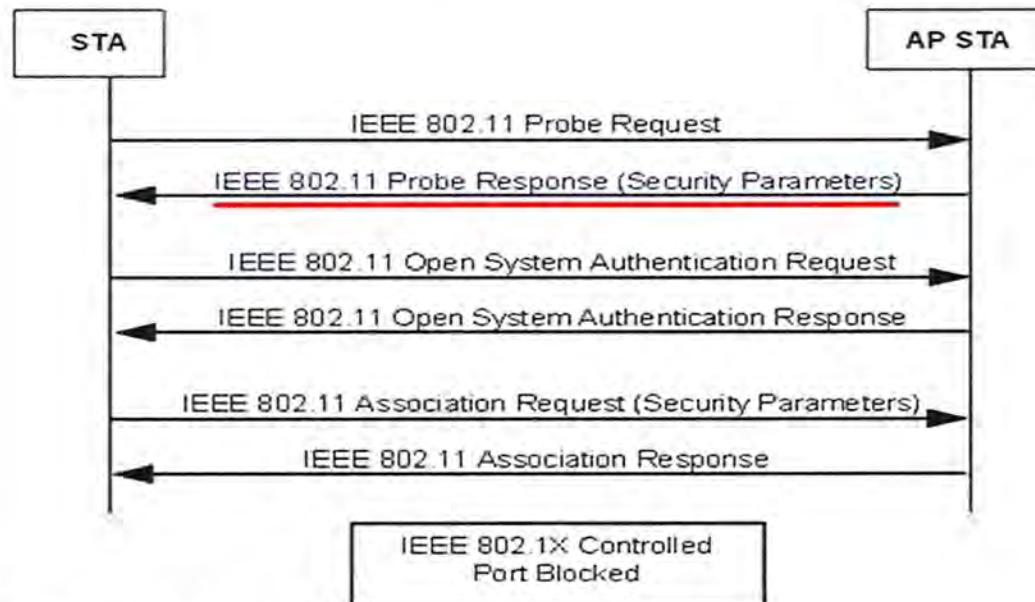
	<u>An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.</u>
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.	The Accused Products practice a method wherein generating the fake MAC address includes generating the MAC address from one or more characters that are selected randomly. The Accused Products generate a fake MAC address by, for example, randomly setting one or more bits of the MAC address (e.g., setting the locally administered bit to 1, the unicast bit to 0, and then randomizing the remaining 46 bits). <u>MAC Randomization Behavior</u>  <u>The MAC randomization feature allows devices to use a randomized MAC address when connecting to a Wi-Fi network. For implementation instructions, see Implementing MAC Randomization. This page describes the behavior of MAC randomization in Android.</u> <u>MAC addresses are used by devices when connecting to a Wi-Fi network or an access point. Because these MAC addresses are transmitted without encryption, they can be captured and used to potentially track a user's location. Historically, devices use the factory MAC address to associate to a Wi-Fi network. The factory MAC address is globally unique and static, allowing the device to be tracked and individually identified.</u> <u>The MAC randomization feature increases user privacy by using a randomized MAC address when connecting to a Wi-Fi network.</u> <u>MAC addresses are 48 bits long and usually represented by 12 hex digits (6 octets as each octet is 8 bits) such as 00:11:22:AA:BB:CC. The MAC randomization feature randomizes the address by setting the locally administered bit to 1, and the unicast bit to 0. The other 46 bits are randomized.</u> https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.

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

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.

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.

The Accused Products support the Wi-Fi standard. The Accused Products receive the probe responses from multiple available access points. An access point responds with the probe response only when the SSID in the probe request is the wildcard SSID or matches the specific SSID of the access point or when the specific SSID of the access point is included in the SSID List element.



Source: IEEE 802.11-2012.pdf

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

Table 8-27—Probe Response frame body

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability	
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.
9	IBSS Parameter Set	The IBSS Parameter Set element is present only within Probe Response frames generated by STAs in an IBSS.
10	Country	The Country element is present if dot11MultiDomainCapabilityActivated is true or dot11SpectrumManagementRequired is true or dot11RadioMeasurementActivated is true.
11	FH Parameters	The FH Parameters element, as specified in 8.4.2.11, is optionally present if dot11MultiDomainCapabilityActivated is true.
12	FH Pattern Table	The FH Pattern Table element, as specified in 8.4.2.12, is optionally present if dot11MultiDomainCapabilityActivated is true.
13	Power Constraint	The Power Constraint element is present if dot11SpectrumManagementRequired is true and is optionally present if dot11RadioMeasurementActivated is true.
14	Channel Switch Announcement	The Channel Switch Announcement element is optionally present if dot11SpectrumManagementRequired is true.
15	Quiet	The Quiet element is optionally present if dot11SpectrumManagementRequired is true or if dot11RadioMeasurementActivated is true.
16	IBSS DFS	The IBSS DFS element is present if dot11SpectrumManagementRequired is true in an IBSS.
17	TPC Report	The TPC Report element is present if dot11SpectrumManagementRequired is true or dot11RadioMeasurementActivated is true.
18	ERP	The ERP element is present within Probe Response frames generated by STAs using ERPs and is optionally present otherwise.
19	Extended Supported Rates	The Extended Supported Rates element is present if there are more than eight supported rates, and it is optionally present otherwise.
20	RSN	The RSNE is present only if dot11RSNAActivated is true.
21	BSS Load	The BSS Load element is present if dot11QoSOptionImplemented and dot11QBSSLoadImplemented are both true.
22	EDCA Parameter Set	The EDCA Parameter Set element is present if dot11QoSOptionImplemented is true and dot11MeshActivated is.

<https://mrncciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

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

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
26	AP Channel Report	If dot11RMChannelReportActivated is true, one AP Channel Report element is optionally present for each operating class that has at least 1 channel to report.
27	BSS Average Access Delay	The BSS Average Access Delay element is optionally present if dot11RMBSSAverageAccessDelayActivated is true and the value of the AP Average Access Delay field is not equal to 255 (measurement not available).
28	Antenna	The Antenna element is optionally present if dot11RMAntennaInformationActivated is true and the value of the Antenna ID field is not equal to 0 (unknown antenna).
29	BSS Available Admission Capacity	The BSS Available Admission Capacity element is optionally present if dot11RMBSSAvailableAdmissionCapacityActivated is true with the following exceptions: 1) when Available Admission Capacity Bitmap equals 0 (Available Admission Capacity List contains no entries), or 2) when the BSS Load element is present and the Available Capacity Bitmap equals 256 (Available Admission Capacity List contains only the AC_VO entry).
30	BSS AC Access Delay	The BSS AC Access Delay element is optionally present if dot11RMBSSAverageAccessDelayActivated is true and at least one field of the element is not equal to 255 (measurement not available).
31	Mobility Domain	The MDE is present if dot11FastBSSTransitionActivated is true.
32	DSE registered location	The DSE Registered Location element is present if dot11LCIDSERequired is true.
33	Extended Channel Switch Announcement	The Extended Channel Switch Announcement element is optionally present if dot11ExtendedChannelSwitchActivated is true.
34	Supported Operating Classes	The Supported Operating Classes element is present if dot11ExtendedChannelSwitchActivated is true.
35	HT Capabilities	The HT Capabilities element is present when dot11HighThroughputOptionImplemented attribute is true.
36	HT Operation	The HT Operation element is included by an AP and a mesh STA when dot11HighThroughputOptionImplemented attribute is true.
37	20-40 BSS Coexistence	The 20-40 BSS Coexistence element is optionally present when the dot112040BSSCoexistenceManagementSupport attribute is true.
38	Overlapping BSS Scan Parameters	The Overlapping BSS Scan Parameters element is optionally present if the dot11FortyMHzOptionImplemented attribute is true.
39	Extended Capabilities	The Extended Capabilities element is optionally present if any of the fields in this element are nonzero.

<https://mrnciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

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

40	QoS Traffic Capability	The QoS Traffic Capability element is optionally present if dot11MgmtOptionACStationCountActivated is true.
41	Channel Usage	The Channel Usage element is present if the Channel Usage element is present in the Probe Request frame and dot11MgmtOptionChannelUsageActivated is true.
42	Time Advertisement	The Time Advertisement element is present if dot11MgmtOptionUTCSTSOOffsetActivated is true.
43	Time Zone	The Time Zone element is present if dot11MgmtOptionUTCSTSOOffsetActivated is true.
44	Interworking	The Interworking element is present if dot11InterworkingServiceActivated is true.
45	Advertisement Protocol	Advertisement Protocol element is present if dot11InterworkingServiceActivated is true and at least one dot11GASAdvertisementID MIB attribute exists.
46	Roaming Consortium	The Roaming Consortium element is present if dot11InterworkingServiceActivated is true and the dot11RoamingConsortiumTable has at least one entry.
47	Emergency Alert Identifier	One or more Emergency Alert Identifier elements are present if dot11EASActivated is true and there are one or more EAS message(s) active in the network.
48	Mesh ID	The Mesh ID element is present if dot11MeshActivated is true.
49	Mesh Configuration	The Mesh Configuration element is present if dot11MeshActivated is true.
50	Mesh Awake Window	The Mesh Awake Window element is optionally present if dot11MeshActivated is true.
51	Beacon Timing	The Beacon Timing element is optionally present if both dot11MeshActivated and dot11MBCAAActivated are true.
52	MCCAOP Advertisement Overview	The MCCAOP Advertisement Overview element is optionally present if both dot11MeshActivated and dot11MCCAActivated are true.
53	MCCAOP Advertisement	One or more MCCAOP Advertisement elements are optionally present if both dot11MeshActivated and dot11MCCAActivated are true.
54	Mesh Channel Switch Parameters	The Mesh Channel Switch Parameters element is present if dot11MeshActivated is true and either Channel Switch Announcement element or Extended Channel Switch Announcement element is present.
Last-1	Vendor Specific	One or more vendor-specific elements are optionally present. These elements follow all other elements, except the Requested elements.
Last-n	Requested elements	Elements requested by the Request element of the Probe Request frame are present if dot11MultiDomainCapabilityActivated is true. See 10.1.4.3.2.

<https://mrncciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

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

4.3.13.15 SSID list

The SSID List element enables the non-AP STA to request information on a list of SSIDs. This is intended to reduce the number of Probe Request frames sent by the non-AP STA.

Source: IEEE 802.11-2012.pdf

In an infrastructure BSS or in an IBSS, STAs receiving Probe Request frames shall respond with a probe response when the SSID in the probe request is the wildcard SSID or matches the specific SSID of the STA or when the specific SSID of the STA is included in the SSID List element. Furthermore, a STA with dot11RadioMeasurementActivated true receiving a probe request with a DSSS Parameter Set element containing a Current Channel field value that is not the same as the value of dot11CurrentChannel shall not respond with a probe response. An AP shall respond to all probe requests meeting the above criteria. In an IBSS a STA that transmitted a Beacon frame since the last TBTT shall respond to group addressed Probe Request frames. A STA in an IBSS shall respond to Probe Request frames sent to the individual address of the STA.

Source: IEEE 802.11-2012.pdf

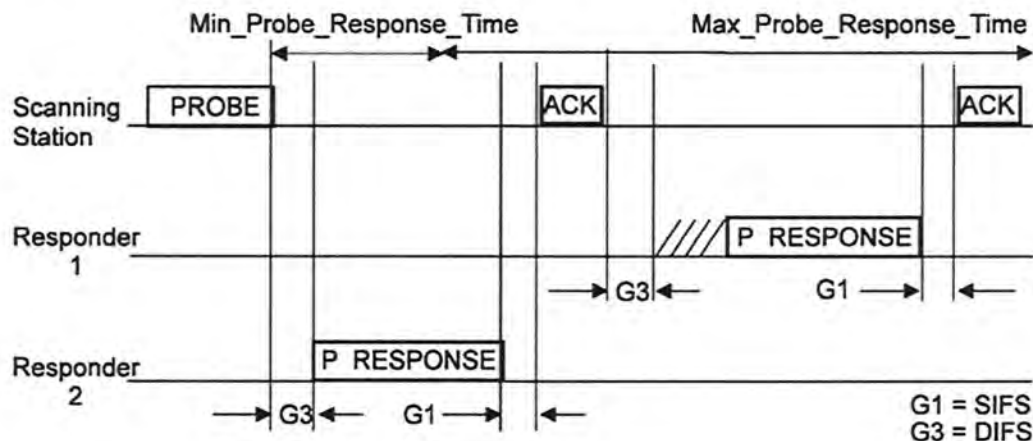


Figure 10-3—Probe response

Source: IEEE 802.11-2012.pdf

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

Before answering the question, let us first understand what a preferred network list is. The PNL is a historical record of all the network names (SSIDs) that a device has previously connected to, and trusts to automatically connect to again in the future.

User devices trying to connect to a Wi-Fi network watch for access points (APs) broadcasting its availability for a device to connect to its network. Within that information contains the network name, or Service Set Identifier (SSID). Wi-Fi enabled devices trying to connect to a wireless network, and using Active Service Discovery, will then broadcast its interest in connecting to the AP if the network name is in its PNL, which increases the connection speed.

For instance, if you connect to a Starbucks Wi-Fi network once, your device will remember and try to automatically connect to any network with the SSID Starbucks. This is true whether you go to the same Starbucks in the future, or a Starbucks 1,000 miles away. All the user device knows is the network name; no additional data is stored. Auto-connecting to wireless networks in PNL saves time and is convenient for the user, but it is a security risk. Therefore, it is important to identify all networks in the PNL and stop connecting automatically to Wi-Fi to stay safe.

<https://blog.pulsarsecurity.com/preferred-network-list-pnl>

The reason for client scanning is to determine a suitable AP to which the client may need to roam now or in the future. A client can use two scanning methods: active and passive. During an active scan, the client radio transmits a probe request and listens for a probe response from an AP. With a passive scan, the client radio listens on each channel for beacons sent periodically by an AP. A passive scan generally takes more time, since the client must listen and wait for a beacon versus actively probing to find an AP. Another limitation with a passive scan is that if the client does not wait long enough on a channel, then the client may miss an AP beacon.

<https://www.wi-fi.org/knowledge-center/faq/what-are-passive-and-active-scanning>

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

The screenshot displays a Wi-Fi management frame (Probe Response) with the following fields and values:

- 802.11 Management - Probe Response**
 - Probe Timestamp: 23996945615 Microseconds [24-31]
 - Beacon Interval: 102 Time Units (104 Milliseconds, and 448 Microseconds) [32-33]
 - Capability Info: 0001000000000001
 - SSID ID=0 SSID Len=4 SSID=OPEN
 - Supported Rates**
 - Element ID: 1 Supported Rates [42]
 - Length: 4 [43]
 - Supported Rate: 24.0 Mbps (BSS Basic Rate) [44]
 - Supported Rate: 36.0 Mbps (Not BSS Basic Rate) [45]
 - Supported Rate: 48.0 Mbps (Not BSS Basic Rate) [46]
 - Supported Rate: 54.0 Mbps (Not BSS Basic Rate) [47]
 - Country**
 - Element ID: 7 Country [48]
 - Length: 18 [49]
 - Country Code: AU [50-51]
 - Environment: 0x20 Any [52]
 - Starting Channel: 36 [53]
 - Number of Channels: 4 [54]
 - Max Tx Power (dBm): 23 [55]
 - Starting Channel: 52 [56]
 - Number of Channels: 4 [57]
 - Max Tx Power (dBm): 23 [58]
 - Starting Channel: 100 [59]
 - Number of Channels: 5 [60]
 - Max Tx Power (dBm): 30 [61]
 - Starting Channel: 132 [62]
 - Number of Channels: 3 [63]
 - Max Tx Power (dBm): 30 [64]
 - Starting Channel: 149 [65]
 - Number of Channels: 5 [66]
 - Max Tx Power (dBm): 30 [67]
 - QoS Load**
 - Element ID: 11 QoS Load [68]
 - Length: 5 [69]
 - Station Count: 1 [70-71]
 - Channel Utilization: 0 % [72]
 - Avail Admission Capacity: 26562 [73-74]
 - HT Cap= ID=45 HT Cap Len=26

Callouts in the image:

- information regarding access point**: Points to the SSID and Supported Rates fields.
- information regarding access point**: Points to the Country field.
- probe response**: Points to the entire packet structure.

<https://mrncciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.

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

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.	The Accused Products practice a method 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. As an example, 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. As shown, 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. <u>Persistent randomization</u> <u>Android uses the persistent randomization type by default</u> when the MAC randomization feature is enabled. Android generates a <u>persistent randomized MAC address based on the parameters of the network profile including SSID, security type, or FQDN (for Passpoint networks)</u>. This MAC address remains the same until factory reset. The MAC address does not get re-randomized if the user forgets and re-adds the Wi-Fi network since the <u>MAC address depends on the parameters of the network profile</u>. <u>Persistent MAC addresses are necessary in cases where networks rely on the persistence of the MAC address to provide useful functionality to the user</u>, for example, to remember a device and allow users to bypass the login screen as expected, or to enable parental controls. <u>For Android 10 and 11, the framework uses persistent randomization for all networks when MAC randomization is enabled.</u> https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior
---	--

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

[android / device / generic / goldfish / refs/tags/android-9.0.0_r34 / . / wifi / WifiConfigStore.xml](#)

blob: bb5645aacde00f44a93c3386c8e42cf140bfe6a5 [\[file\]](#) [\[log\]](#) [\[blame\]](#)

```
1 <?xml version='1.0' encoding='utf-8' standalone='yes' ?>
2 <WifiConfigStoreData>
3   <int name="Version" value="1" />
4   <NetworkList>
5     <Network>
6       <WifiConfiguration>
7         <string name="ConfigKey">&quot;AndroidWifi&quot;NONE</string>
8         <string name="SSID">&quot;AndroidWifi&quot;</string>
9         <null name="BSSID" />
10        <null name="PreSharedKey" />
11        <null name="WEPKeys" />
12        <int name="WEPKeyIndex" value="0" />
13        <boolean name="HiddenSSID" value="false" />
```

https://android.googlesource.com/device/generic/goldfish/+refs/tags/android-9.0.0_r34/wifi/WifiConfigStore.xml

In an infrastructure BSS or in an IBSS, STAs receiving Probe Request frames shall respond with a probe response when the SSID in the probe request is the wildcard SSID or matches the specific SSID of the STA or when the specific SSID of the STA is included in the SSID List element. Furthermore, a STA with dot11RadioMeasurementActivated true receiving a probe request with a DSSS Parameter Set element containing a Current Channel field value that is not the same as the value of dot11CurrentChannel shall not respond with a probe response. An AP shall respond to all probe requests meeting the above criteria. In an IBSS a STA that transmitted a Beacon frame since the last TBTT shall respond to group addressed Probe Request frames. A STA in an IBSS shall respond to Probe Request frames sent to the individual address of the STA.

Source: IEEE 802.11-2012.pdf

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

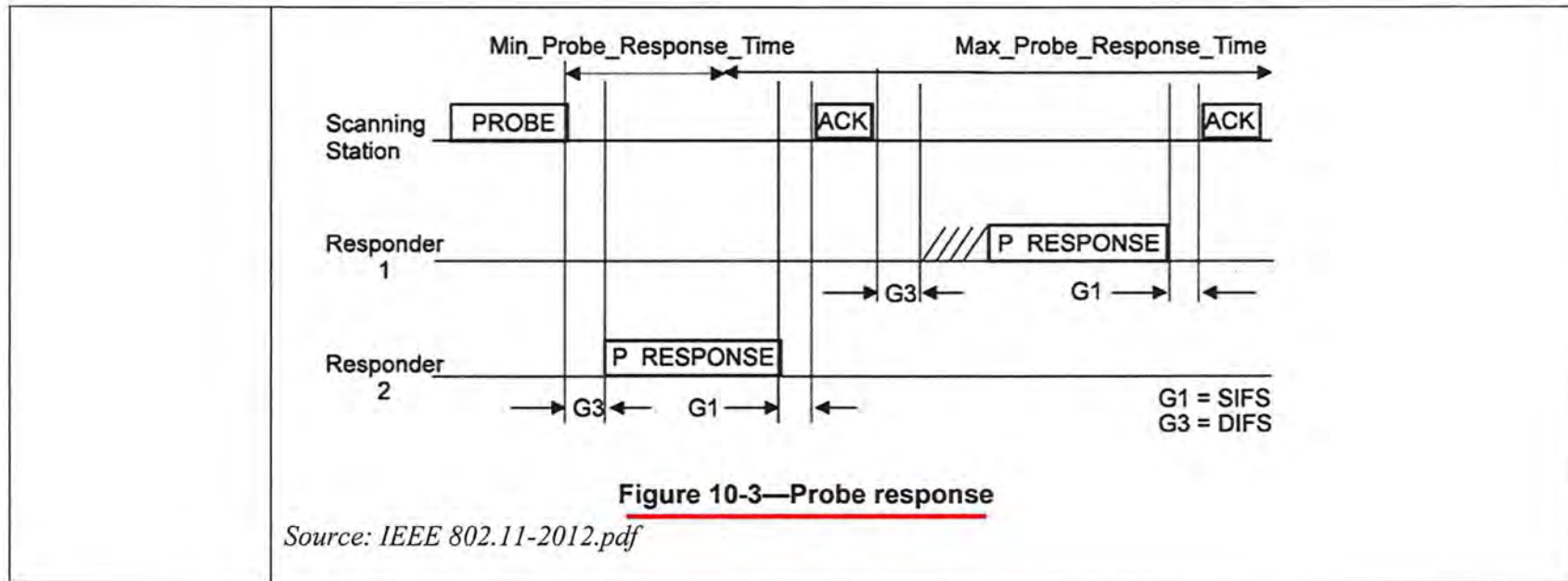


EXHIBIT A-INFRINGEMENT CONTENTIONS FOR U.S. PATENT NO. 10,694,384

Before answering the question, let us first understand what a preferred network list is. The PNL is a historical record of all the network names (SSIDs) that a device has previously connected to, and trusts to automatically connect to again in the future.

User devices trying to connect to a Wi-Fi network watch for access points (APs) broadcasting its availability for a device to connect to its network. Within that information contains the network name, or Service Set Identifier (SSID). Wi-Fi enabled devices trying to connect to a wireless network, and using Active Service Discovery, will then broadcast its interest in connecting to the AP if the network name is in its PNL, which increases the connection speed.

For instance, if you connect to a **Starbucks** Wi-Fi network once, your device will remember and try to automatically connect to any network with the SSID Starbucks. This is true whether you go to the same Starbucks in the future, or a Starbucks 1,000 miles away. All the user device knows is the network name; no additional data is stored. Auto-connecting to wireless networks in PNL saves time and is convenient for the user, but it is a security risk. Therefore, it is important to identify all networks in the PNL and stop connecting automatically to Wi-Fi to stay safe.

<https://blog.pulsarsecurity.com/preferred-network-list-pnl>

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

802.11 Management - Probe Response

- Probe Timestamp: 23996945615 Microseconds [24-31]
- Beacon Interval: 102 Time Units (104 Milliseconds, and 448 Microseconds) [32-35]
- Capability Info: %0001000000000001
- SSID ID=0 SSID Len=4 SSID=OPEN
- Supported Rates
 - Element ID: 1 Supported Rates [42]
 - Length: 4 [43]
 - Supported Rate: 24.0 Mbps (BSS Basic Rate) [44]
 - Supported Rate: 36.0 Mbps (Not BSS Basic Rate) [45]
 - Supported Rate: 48.0 Mbps (Not BSS Basic Rate) [46]
 - Supported Rate: 54.0 Mbps (Not BSS Basic Rate) [47]
- Country
 - Element ID: 7 Country [48]
 - Length: 18 [49]
 - Country Code: AU [50-51]
 - Environment: 0x20 Any [52]
 - Starting Channel: 36 [53]
 - Number of Channels: 4 [54]
 - Max Tx Power (dBm): 23 [55]
 - Starting Channel: 52 [56]
 - Number of Channels: 4 [57]
 - Max Tx Power (dBm): 23 [58]
 - Starting Channel: 100 [59]
 - Number of Channels: 5 [60]
 - Max Tx Power (dBm): 30 [61]
 - Starting Channel: 132 [62]
 - Number of Channels: 3 [63]
 - Max Tx Power (dBm): 30 [64]
 - Starting Channel: 149 [65]
 - Number of Channels: 5 [66]
 - Max Tx Power (dBm): 30 [67]
- OBSS Load
 - Element ID: 11 OBSS Load [68]
 - Length: 5 [69]
 - Station Count: 1 [70-71]
 - Channel Utilization: 0 % [72]
 - Avail Admission Capacity: 26562 [73-74]
- HT Cap= ID=45 HT Cap Len=26

<https://mrncciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.

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

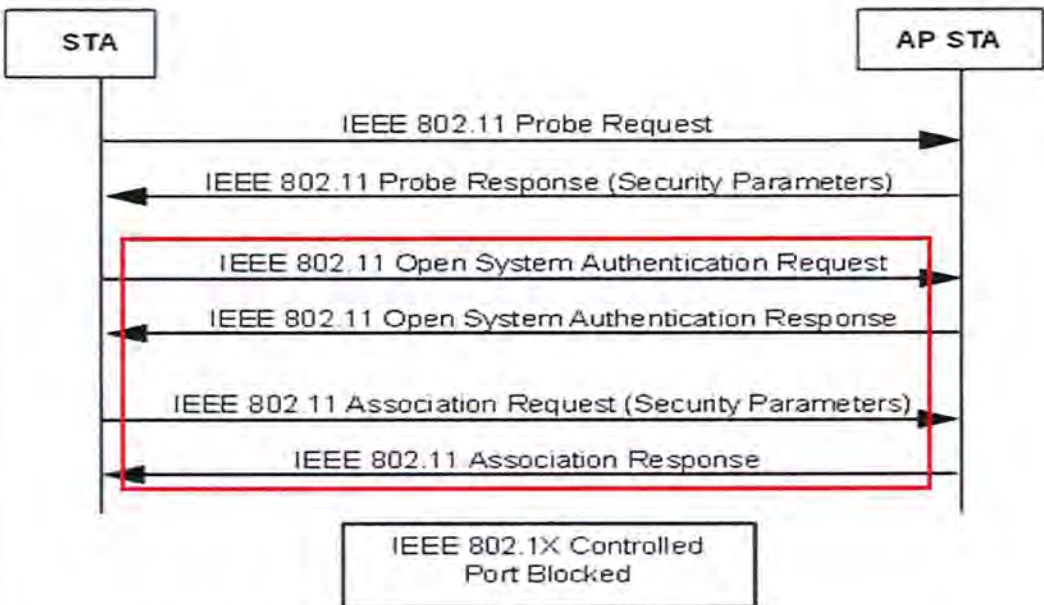
14. The method of claim 9, further comprising: receiving, by the end device from the at least one access point, an approval of the connection request; transmitting, by the end device to the at least one access point after receiving the approval of the connection request, an association request; receiving, 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	The Accused Products practice a method of 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. As an example, the Accused Products receive an open system authentication response from an access point. The Accused Products then transmit an association request. Then the Accused Products receive an association response from the access point, at which point the Accused Product is connected to a network via the access point in accordance with the association response.  <pre> sequenceDiagram participant STA participant AP_STA as AP STA STA->>AP_STA: IEEE 802.11 Probe Request AP_STA-->STA: IEEE 802.11 Probe Response (Security Parameters) STA->>AP_STA: IEEE 802.11 Open System Authentication Request AP_STA-->STA: IEEE 802.11 Open System Authentication Response STA->>AP_STA: IEEE 802.11 Association Request (Security Parameters) AP_STA-->STA: IEEE 802.11 Association Response </pre> Source: IEEE 802.11-2012.pdf
---	--

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

point in accordance with the association response.

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.

Source: IEEE 802.11-2012.pdf

802.11 Mgmt : Authentication Frame

POSTED BY NAYARASI IN CWAP

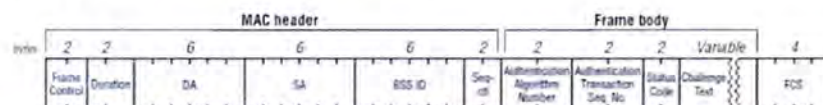
≈ 10 COMMENTS

Once a client station is discover a SSID (Probe Request/Response or listening to Beacons) it move to Join phase. This exchange comprise of at least 4 frames

1. Authentication (Request)
2. Authentication (Response)
3. Association Request
4. Association Response

The frame format of those Authentication frames are as shown below.(from page 136- CWAP Official Study Guide)

FIGURE 4.8 Authentication frame format



<https://mrnciew.com/2014/10/10/802-11-mgmt-authentication-frame/>

An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.

15. The method of claim 14, wherein the at least one access point

The at least one access point includes a Wi-Fi access point, and the communication network includes a Wi-Fi network that is accessible through the Wi-Fi access point.

The Accused Products are designed to connect to Wi-Fi access points in order to join a Wi-Fi network.

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

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.

Phone	<u>Galaxy S23</u>	Galaxy S23+	Galaxy S23 Ultra
<u>Connectivity</u>	5G, <u>Wi-Fi 6E</u> , Bluetooth 5.3, NFC	5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband	5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband

<https://www.androidpolice.com/samsung-galaxy-s23/>

Galaxy S23



Wi-Fi 6E

802.11 a/b/g/n/ac/ax

<https://www.samsung.com/us/smartphones/galaxy-s23/specs/>

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

	• Connectivity: The Galaxy S23 series boasts unparalleled Snapdragon Connect technologies across 5G, Wi-Fi, and Bluetooth®. Featuring the multiple-award-winning Snapdragon X70 5G Modem-RF System with the Qualcomm® 5G AI Processor, the Galaxy S23 series harnesses the power of AI to enable breakthrough 5G coverage, power efficiency, speeds, and latency. These new devices also support 5G+5G/4G Dual-SIM Dual-Active³, which harnesses the power and flexibility of two 5G SIMs at once. Additionally, all Galaxy S23 series variants feature the Qualcomm® FastConnect™ 6900 and 7800 systems delivering multi-gigabit Wi-Fi speeds, ultra-low latency, and deeply immersive Bluetooth Audio experiences. https://www.qualcomm.com/news/releases/2023/02/qualcomm-and-samsung-partner-to-bring-the-fastest-snapdragon-eve
17. An end device, comprising:	To the extent the preamble is limiting, the Accused Products comprise an end device. The Accused Products include Android OS 10 or above or Wear OS 3 or above. Each Accused Product includes an SoC and Wi-Fi connection functionality. As a specific example shown below, the Galaxy S23 includes the Android 13 operating system, which includes randomized MAC for Wi-Fi connections. It comprises an SoC, Snapdragon 8 Gen 2, a Wi-Fi chipset, and FastConnect. It connects to a Wi-Fi network using the Wi-Fi chipset.

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

SAMSUNG

Shop Mobile TV & Audio Appliances Computing Displays Accessories SmartThings

Explore Support For Business

Q

🛒

👤

NEW

Galaxy S23

Unlocked | Lavender

2,400,000 (approx. MSRP) ★★★★★ 4.5 (2072) [Write a Review](#)

[Learn about Galaxy S23 key features](#)

Pricing before trade-in

Get up to **\$415** instant trade-in credit

Total

\$799.99

with Samsung Financing

\$33.34/mo for 24 mos

[Continue](#)

[Save an extra \\$100.00 with Samsung Offers Program membership](#)

Galaxy S23 Ultra

Galaxy S23 | S23+

Device

Galaxy S23

\$799.99

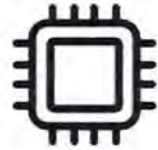
Galaxy S23+

\$999.99

Connectivity

<https://www.samsung.com/us/smartphones/galaxy-s23/buy/galaxy-s23-128gb-unlocked-sm-s911ulixaa/>

Galaxy S23



Super fast processing

Snapdragon® 8 Gen 2

Octa-Core

<https://www.samsung.com/us/smartphones/galaxy-s23/specs/>

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

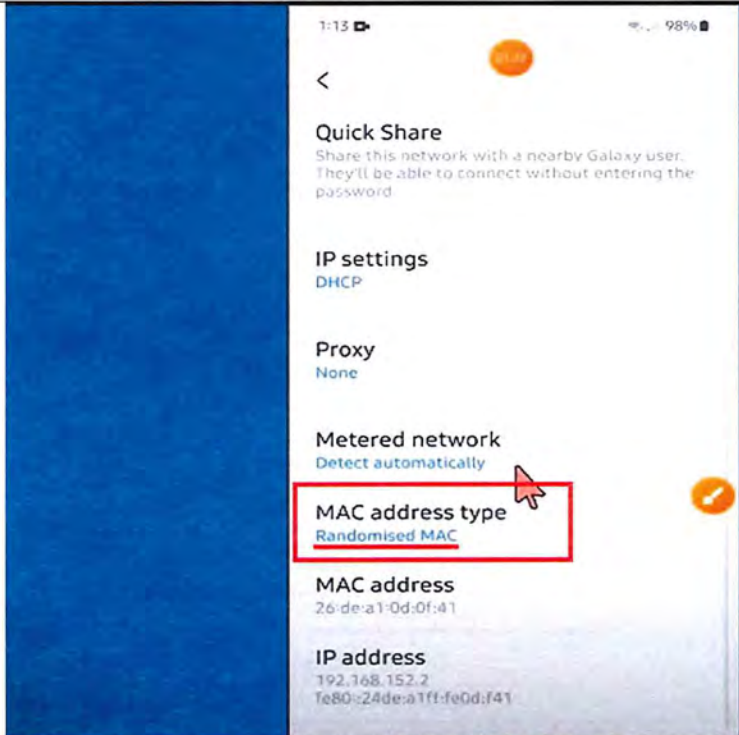
Phone	<u>Galaxy S23</u>	Galaxy S23+	Galaxy S23 Ultra
Chipset	Snapdragon 8 Gen 2 for Galaxy	Snapdragon 8 Gen 2 for Galaxy	Snapdragon 8 Gen 2 for Galaxy
RAM & Storage	8+128GB, 8+256GB (UFS 3.1)	8+256GB, 8+512GB (UFS 4.0)	8+256GB, 12+512GB, 12GB+1TB (UFS 4.0)
Display	6.1" FHD+ Dynamic AMOLED 2x, 120Hz Adaptive Refresh Rate, 425ppi, 1,750nit (outdoor peak)	6.6" FHD+ Dynamic AMOLED 2x, 120Hz Adaptive Refresh Rate, 393ppi, 1,750nit (outdoor peak)	6.8" QHD+ Dynamic AMOLED 2x, 120Hz Adaptive Refresh Rate, 500ppi, 1,750nit (outdoor peak)
<u>Software</u>	<u>Android 13 / One UI 5.1</u>	Android 13 / One UI 5.1	Android 13 / One UI 5.1

<https://www.androidpolice.com/samsung-galaxy-s23/>



<https://www.youtube.com/watch?v=BadWvxWe8y8>

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



The screenshot shows the 'Quick Share' settings on a Samsung Galaxy S23 Plus. The 'MAC address type' is set to 'Randomised MAC', which is highlighted by a red rectangular box. A mouse cursor is pointing at the 'Randomised MAC' option. The 'MAC address' is listed as '26:de:a1:0d:0f:41' and the 'IP address' is '192.168.152.2'.

GALAXY S23, PLUS
Set MAC Address Type to
Randomized
MAC/Phone MAC

<https://www.youtube.com/watch?v=dT63df6nnqU>

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



<https://www.youtube.com/watch?v=AaMm2HHwbI0>

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

Featuring the Snapdragon X70 5G Modem RF System, Snapdragon 8 Gen 2 is the world's first and only mobile platform with a dedicated 5G AI processor. Plus, gaming, streaming, and communication from home soar via Wi-Fi 7 (the industry's lowest latency offering), all brought to you by the Qualcomm® FastConnect™ 7800 Mobile Connectivity System.

- 5G Dual-SIM Dual-Active (DSDA) enables the simultaneous use of two 5G+5G or 5G+4G SIM cards for ultimate user flexibility
- Blazing Wi-Fi speeds of up to 5.8 Gbps—more than double Wi-Fi 6
- World's first commercial Wi-Fi 7 SoC, with advanced High Band Simultaneous Multi-Link

<https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/Snapdragon-8-Gen-2-Product-Brief.pdf>

- The Samsung Galaxy S23 series features Qualcomm Technologies' leading connectivity solutions, including the Snapdragon® X70 Modem-RF System, the world's fastest and smartest 5G modem-RF system, and Qualcomm® FastConnect™ for high-speed and ultra-low latency Wi-Fi, and the latest Bluetooth audio enhancements.

<https://www.qualcomm.com/news/releases/2023/02/qualcomm-and-samsung-partner-to-bring-the-fastest-snapdragon-eve>

MAC Randomization is implemented in devices running the Android OS since at least Android OS 10 as well as Wear OS 3.0.

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

	In Android 10, MAC randomization is enabled by default for client mode, SoftAp, and Wi-Fi Direct. MAC randomization prevents listeners from using MAC addresses to build a history of device activity, thus increasing user privacy. Additionally, MAC addresses are randomized as part of Wi-Fi Aware and Wi-Fi RTT operations. For more information, see MAC Randomization Behavior. https://source.android.com/docs/core/connect/wifi-mac-randomization Wear OS, including Wear OS 3.0, is based on Android. See https://developer.android.com/training/wearables/wear-v-mobile#:~:text=Wear%20OS%20is%20based%20on,design%20a%20Wear%20OS%20app. Devices operating on Wear OS 3.0 implement MAC randomization. See https://www.reddit.com/r/GalaxyWatch/comments/pcmkl1/galaxy_watch_4_wifi_mac_address/
[17a] a hardware network interface associated with an actual media access control (MAC) address;	The Accused Products include a hardware network interface associated with an actual media access control (MAC) address. As shown below, the Accused Products include, for example, a hardware network interface for connecting including a chipset (e.g., Snapdragon 8 Gen 2 chipset including a Wi-Fi SOC called FastConnect), as shown in the example below, which is used to connect to Wi-Fi networks. The Accused Products also include an operating system (Android 10 or higher or Wear OS 3 and higher) that runs on a CPU. In the example below, the Galaxy S23 includes the Android 13 operating system that runs on the Kryo CPU of the SoC of the Accused Product. https://www.samsung.com/us/smartphones/galaxy-s23/specs/

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

Phone	<u>Galaxy S23</u>	Galaxy S23+	Galaxy S23 Ultra
Chipset	Snapdragon 8 Gen 2 for Galaxy	Snapdragon 8 Gen 2 for Galaxy	Snapdragon 8 Gen 2 for Galaxy
RAM & Storage	8+128GB, 8+256GB (UFS 3.1)	8+256GB, 8+512GB (UFS 4.0)	8+256GB, 12+512GB, 12GB+1TB (UFS 4.0)
Display	6.1" FHD+ Dynamic AMOLED 2x, 120Hz Adaptive Refresh Rate, 425ppi, 1,750nit (outdoor peak)	6.6" FHD+ Dynamic AMOLED 2x, 120Hz Adaptive Refresh Rate, 393ppi, 1,750nit (outdoor peak)	6.8" QHD+ Dynamic AMOLED 2x, 120Hz Adaptive Refresh Rate, 500ppi, 1,750nit (outdoor peak)
Software	<u>Android 13 / One UI 5.1</u>	Android 13 / One UI 5.1	Android 13 / One UI 5.1

<https://www.androidpolice.com/samsung-galaxy-s23/>



CPU

Kryo CPU

- 64-bit Architecture
- 1 Prime core, up to 3.36 GHz²
 - Arm Cortex-X3 technology
- 4 Performance cores, up to 2.8 GHz
- 3 Efficiency cores, up to 2.0 GHz

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

<https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/Snapdragon-8-Gen-2-Product-Brief.pdf>

Phone	<u>Galaxy S23</u>	Galaxy S23+	Galaxy S23 Ultra
<u>Connectivity</u>	5G, <u>Wi-Fi 6E</u> , Bluetooth 5.3, NFC	5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband	5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband

<https://www.androidpolice.com/samsung-galaxy-s23/>

<https://www.samsung.com/us/smartphones/galaxy-s23/specs/>

- **Connectivity:** The Galaxy S23 series boasts unparalleled Snapdragon Connect technologies across 5G, Wi-Fi, and Bluetooth®. Featuring the multiple-award-winning Snapdragon X70 5G Modem-RF System with the Qualcomm® 5G AI Processor, the Galaxy S23 series harnesses the power of AI to enable breakthrough 5G coverage, power efficiency, speeds, and latency. These new devices also support 5G+5G/4G Dual-SIM Dual-Active³, which harnesses the power and flexibility of two 5G SIMs at once. Additionally, all Galaxy S23 series variants feature the Qualcomm® FastConnect™ 6900 and 7800 systems delivering multi-gigabit Wi-Fi speeds, ultra-low latency, and deeply immersive Bluetooth Audio experiences.

<https://www.qualcomm.com/news/releases/2023/02/qualcomm-and-samsung-partner-to-bring-the-fastest-snapdragon-eve>

Qualcomm® FastConnect™ 7800 Mobile Connectivity System



Leading Wi-Fi 7 and Dual Bluetooth come together in this powerful and versatile connectivity system

FastConnect is an advanced 14nm Wi-Fi and Bluetooth® Connectivity system delivering fast global speeds and ultra-low sustained latency. Unlock extreme performance for mobile, compute, and XR experiences.

<https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/images/products/by-technology/wi-fi/Qualcomm-FastConnect-7800-Overview-Infographic.png>

The Accused Products support the Wi-Fi standard. As part of that standard, a device's hardware network interface is associated with an actual MAC address. As an example, the hardware network interface is associated with a factory-set MAC address that is globally unique and static, allowing the device to be individually identified:

MAC Randomization Behavior

The MAC randomization feature allows devices to use a randomized MAC address when connecting to a Wi-Fi network. For implementation instructions, see [Implementing MAC Randomization](#). This page describes the behavior of MAC randomization in Android.

MAC addresses are used by devices when connecting to a Wi-Fi network or an access point. Because these MAC addresses are transmitted without encryption, they can be captured and used to potentially track a user's location. Historically, devices use the factory MAC address to associate to a Wi-Fi network. The factory MAC address is globally unique and static, allowing the device to be tracked and individually identified.

The MAC randomization feature increases user privacy by using a randomized MAC address when connecting to a Wi-Fi network.

MAC addresses are 48 bits long and usually represented by 12 hex digits (6 octets as each octet is 8 bits) such as 00:11:22:AA:BB:CC. The MAC randomization feature randomizes the address by setting the *locally administered* bit to 1, and the *unicast* bit to 0. The other 46 bits are randomized.

For devices running Android 10 or higher, the framework uses randomized MAC address by default. Users can enable or disable MAC randomization for individual networks through an option in the **Network details** screen in **Settings**, as shown in Figure 1. If a user disables MAC randomization for a network, the framework uses the factory MAC address (globally unique address).

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

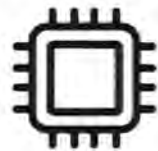
EXHIBIT A-INFRINGEMENT CONTENTIONS FOR U.S. PATENT NO. 10,694,384

[17b] 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;

The Accused Products have 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.

The Accused Products have a processor such as an SoC (e.g., a Snapdragon 8 Gen 2 in the example below). They also include, an operating system (Android 10 or higher or Wear OS 3 or higher) and have randomized MAC for Wi-Fi connections. The operating system generates a randomized MAC address to be used when searching or scanning for a Wi-Fi access point. The operating system runs on the CPU of the Accused Products (e.g., the Kryo CPU of the SoC in the example below).

Galaxy S23



Super fast processing

Snapdragon® 8 Gen 2

Octa-Core

<https://www.samsung.com/us/smartphones/galaxy-s23/specs/>

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

Phone	<u>Galaxy S23</u>	Galaxy S23+	Galaxy S23 Ultra
Chipset	Snapdragon 8 Gen 2 for Galaxy	Snapdragon 8 Gen 2 for Galaxy	Snapdragon 8 Gen 2 for Galaxy
RAM & Storage	8+128GB, 8+256GB (UFS 3.1)	8+256GB, 8+512GB (UFS 4.0)	8+256GB, 12+512GB, 12GB+1TB (UFS 4.0)
Display	6.1" FHD+ Dynamic AMOLED 2x, 120Hz Adaptive Refresh Rate, 425ppi, 1,750nit (outdoor peak)	6.6" FHD+ Dynamic AMOLED 2x, 120Hz Adaptive Refresh Rate, 393ppi, 1,750nit (outdoor peak)	6.8" QHD+ Dynamic AMOLED 2x, 120Hz Adaptive Refresh Rate, 500ppi, 1,750nit (outdoor peak)
Software	<u>Android 13 / One UI 5.1</u>	Android 13 / One UI 5.1	Android 13 / One UI 5.1

<https://www.androidpolice.com/samsung-galaxy-s23/>



CPU

Kryo CPU

- 64-bit Architecture
- 1 Prime core, up to 3.36 GHz²
 - Arm Cortex-X3 technology
- 4 Performance cores, up to 2.8 GHz
- 3 Efficiency cores, up to 2.0 GHz

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

<https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/Snapdragon-8-Gen-2-Product-Brief.pdf>

Phone	<u>Galaxy S23</u>	Galaxy S23+	Galaxy S23 Ultra
<u>Connectivity</u>	5G, <u>Wi-Fi 6E</u> , Bluetooth 5.3, NFC	5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband	5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband

<https://www.androidpolice.com/samsung-galaxy-s23/>

Galaxy S23



Wi-Fi 6E

802.11 a/b/g/n/ac/ax

<https://www.samsung.com/us/smartphones/galaxy-s23/specs/>

- **Connectivity:** The Galaxy S23 series boasts unparalleled Snapdragon Connect technologies across 5G, Wi-Fi, and Bluetooth®. Featuring the multiple-award-winning Snapdragon X70 5G Modem-RF System with the Qualcomm® 5G AI Processor, the Galaxy S23 series harnesses the power of AI to enable breakthrough 5G coverage, power efficiency, speeds, and latency. These new devices also support 5G+5G/4G Dual-SIM Dual-Active³, which harnesses the power and flexibility of two 5G SIMs at once. Additionally, all Galaxy S23 series variants feature the Qualcomm® FastConnect™ 6900 and 7800 systems delivering multi-gigabit Wi-Fi speeds, ultra-low latency, and deeply immersive Bluetooth Audio experiences.

<https://www.qualcomm.com/news/releases/2023/02/qualcomm-and-samsung-partner-to-bring-the-fastest-snapdragon-eve>

Qualcomm® FastConnect™ 7800 Mobile Connectivity System



Leading Wi-Fi 7 and Dual Bluetooth come together in this powerful and versatile connectivity system

FastConnect is an advanced 14nm Wi-Fi and Bluetooth® Connectivity system delivering fast global speeds and ultra-low sustained latency. Unlock extreme performance for mobile, compute, and XR experiences.

<https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/images/products/by-technology/wi-fi/Qualcomm-FastConnect-7800-Overview-Infographic.png>

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

1:13 98%

<

Quick Share

Share this network with a nearby Galaxy user. They'll be able to connect without entering the password.

IP settings

DHCP

Proxy

None

Metered network

Detect automatically

MAC address type

Randomised MAC

MAC address

26-de:a1:00:0f:41

IP address

192.168.152.2

fe80::24de:a1ff:fe0d:f41

GALAXY S23, PLUS

Set MAC Address Type to

Randomized

MAC/Phone MAC

<

Quick Share

Share this network with a nearby Galaxy user. They'll be able to connect without entering the password.

IP settings

DHCP

Proxy

None

Metered network

Detect automatically

Randomised MAC ✓

Phone MAC

26-de:a1:00:0f:41

IP address

192.168.152.2

fe80::24de:a1ff:fe0d:f41

<https://www.youtube.com/watch?v=dT63df6nnqU>

The Accused Products support the Wi-Fi standard. According to the standard, the Accused Products (each a UE) inquire about available Wi-Fi access points using a probe request that includes a MAC address. For a probe request the Accused Products use a randomized MAC address, which is a fake MAC address.

MAC Randomization Behavior -

The MAC randomization feature allows devices to use a randomized MAC address when connecting to a Wi-Fi network. For implementation instructions, see [Implementing MAC Randomization](#). This page describes the behavior of MAC randomization in Android.

MAC addresses are used by devices when connecting to a Wi-Fi network or an access point. Because these MAC addresses are transmitted without encryption, they can be captured and used to potentially track a user's location. Historically, devices use the factory MAC address to associate to a Wi-Fi network. The factory MAC address is globally unique and static, allowing the device to be tracked and individually identified.

The MAC randomization feature increases user privacy by using a randomized MAC address when connecting to a Wi-Fi network.

MAC addresses are 48 bits long and usually represented by 12 hex digits (6 octets as each octet is 8 bits) such as 00:11:22:AA:BB:CC. The MAC randomization feature randomizes the address by setting the *locally administered* bit to 1, and the *unicast* bit to 0. The other 46 bits are randomized.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

For devices running Android 10 or higher, the framework uses randomized MAC address by default. Users can enable or disable MAC randomization for individual networks through an option in the **Network details** screen in **Settings**, as shown in Figure 1. If a user disables MAC randomization for a network, the framework uses the factory MAC address (globally unique address).

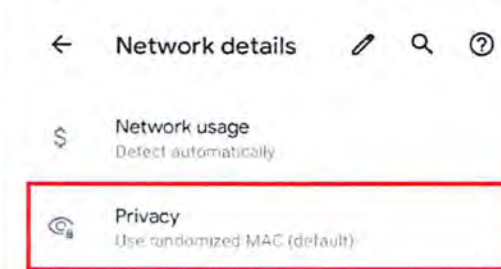
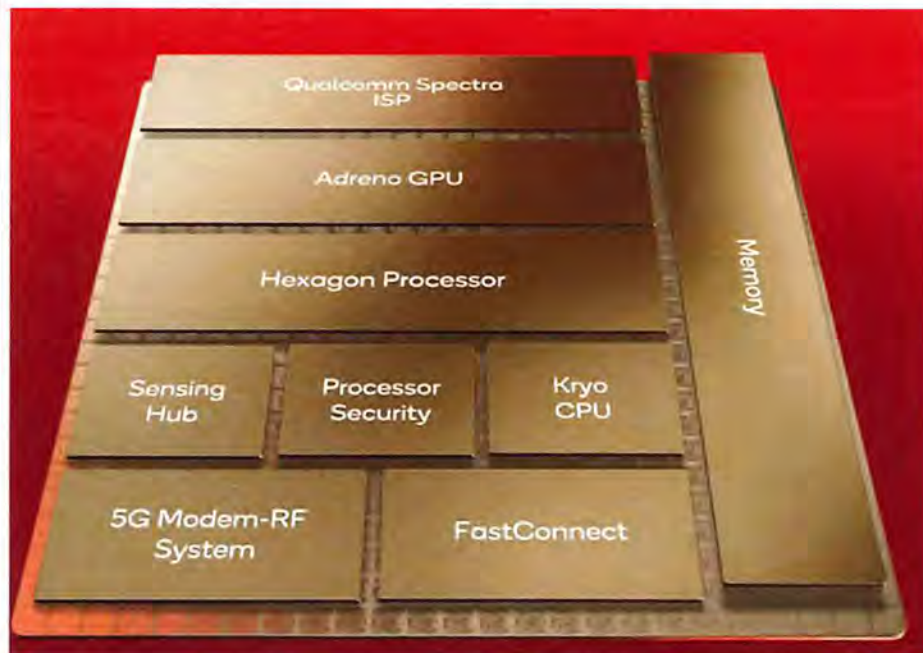


Figure 1. MAC randomization option.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

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

The CPU is a part of the Snapdragon SOC and coupled to the FastConnect network interface.



<https://www.qualcomm.com/news/onq/2022/11/new-snapdragon-8-gen-2-8-extraordinary-mobile-experiences-unveiled>

An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.

[17c] a transmitter coupled to the processor and operable to transmit to an access point, a probe request that

The Accused Products have a transmitter coupled to the processor and operable to transmit to an access point, a probe request that includes the generated MAC address.

The Accused Products support the Wi-Fi standard. According to the standard, the Accused Products (each a UE) send probe requests to access points to inquire about available Wi-Fi access points using a probe request. The

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

includes the generated MAC address; and	probe request comprises a sender address field (e.g., device identifier). The UE utilizes a random MAC address as the sender address in a probe request. The Accused Products transmit probe requests to identify available access points, and thus include a transmitter: The reason for client scanning is to determine a suitable AP to which the client may need to roam now or in the future. A client can use two scanning methods: active and passive. <u>During an active scan, the client radio transmits a probe request and listens for a probe response from an AP.</u> With a passive scan, the client radio listens on each channel for beacons sent periodically by an AP. A passive scan generally takes more time, since the client must listen and wait for a beacon versus actively probing to find an AP. Another limitation with a passive scan is that if the client does not wait long enough on a channel, then the client may miss an AP beacon. https://www.wi-fi.org/knowledge-center/faq/what-are-passive-and-active-scanning
---	---

CWAP 802.11- Probe Request/Response

POSTED BY NAYARASI IN CWAP

≈ 27 COMMENTS

Discovering the network by scanning all possible channels & listening to beacons is not considered to be very efficient (*passive scanning*). To enhance this discovery process, stations often use what is called *active scanning*.

In Active scanning, stations still go through each channel in turn, but instead of passively listening to the signals on that frequency, station send a *Probe Request* management frame asking what network is available on that channel.

Probe Request are sent to the broadcast DA address (*ff:ff:ff:ff:ff:ff*). Once a Probe sent, STA starts a ProbeTimer countdown & wait for answers. At the end of the timer, STA process the answer it has received. If no answers received, STA moves to next channel & repeats the discovery process.

STA sending Probe Request may specify the SSID they looking (called *directed probe request*). Then only IBSS STA or AP support that SSID will answer. *The SSID value can also be set to 0* (ie *SSID field is present, but empty*). This is called *Wildcard SSID* or *Null Probe Request*.

<https://mrnciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

A Wi-Fi probe request includes a MAC address:

Probe requests are packets broadcasted in plain text by Wi-Fi mobile devices to discover 802.11 Access Points (APs) in their proximity [1]. These unencrypted messages contain information about their sources (i.e., MAC address and supported data rate and supported connection to an AP). The operation of capturing data on a

<https://www.sciencedirect.com/science/article/abs/pii/S1389128622000196>

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

The Wi-Fi probe request of the Accused Products includes a randomized MAC address, which is a fake MAC address.

MAC Randomization Behavior

The MAC randomization feature allows devices to use a randomized MAC address when connecting to a Wi-Fi network. For implementation instructions, see [Implementing MAC Randomization](#). This page describes the behavior of MAC randomization in Android.

MAC addresses are used by devices when connecting to a Wi-Fi network or an access point. Because these MAC addresses are transmitted without encryption, they can be captured and used to potentially track a user's location. Historically, devices use the *factory MAC address* to associate to a Wi-Fi network. The factory MAC address is globally unique and static, allowing the device to be tracked and individually identified.

The MAC randomization feature increases user privacy by using a randomized MAC address when connecting to a Wi-Fi network.

MAC addresses are 48 bits long and usually represented by 12 hex digits (6 octets as each octet is 8 bits) such as 00:11:22:AA:BB:CC. The MAC randomization feature randomizes the address by setting the *locally administered* bit to 1, and the *unicast* bit to 0. The other 46 bits are randomized.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

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

For devices running Android 10 or higher, the framework uses randomized MAC address by default. Users can enable or disable MAC randomization for individual networks through an option in the **Network details** screen in **Settings**, as shown in Figure 1. If a user disables MAC randomization for a network, the framework uses the factory MAC address (globally unique address).

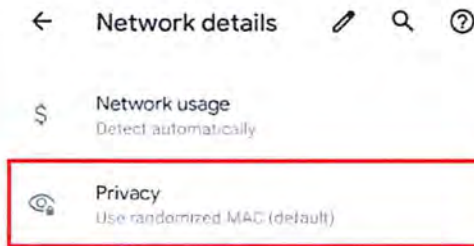
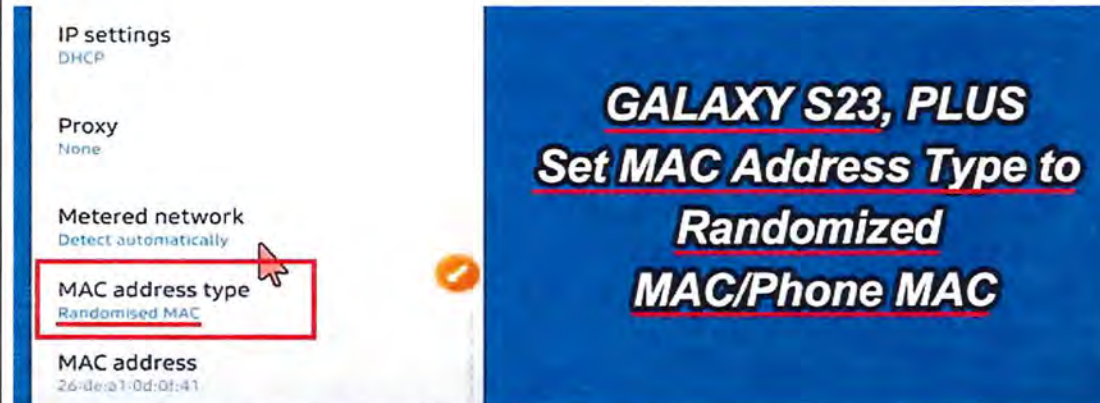


Figure 1. MAC randomization option.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>



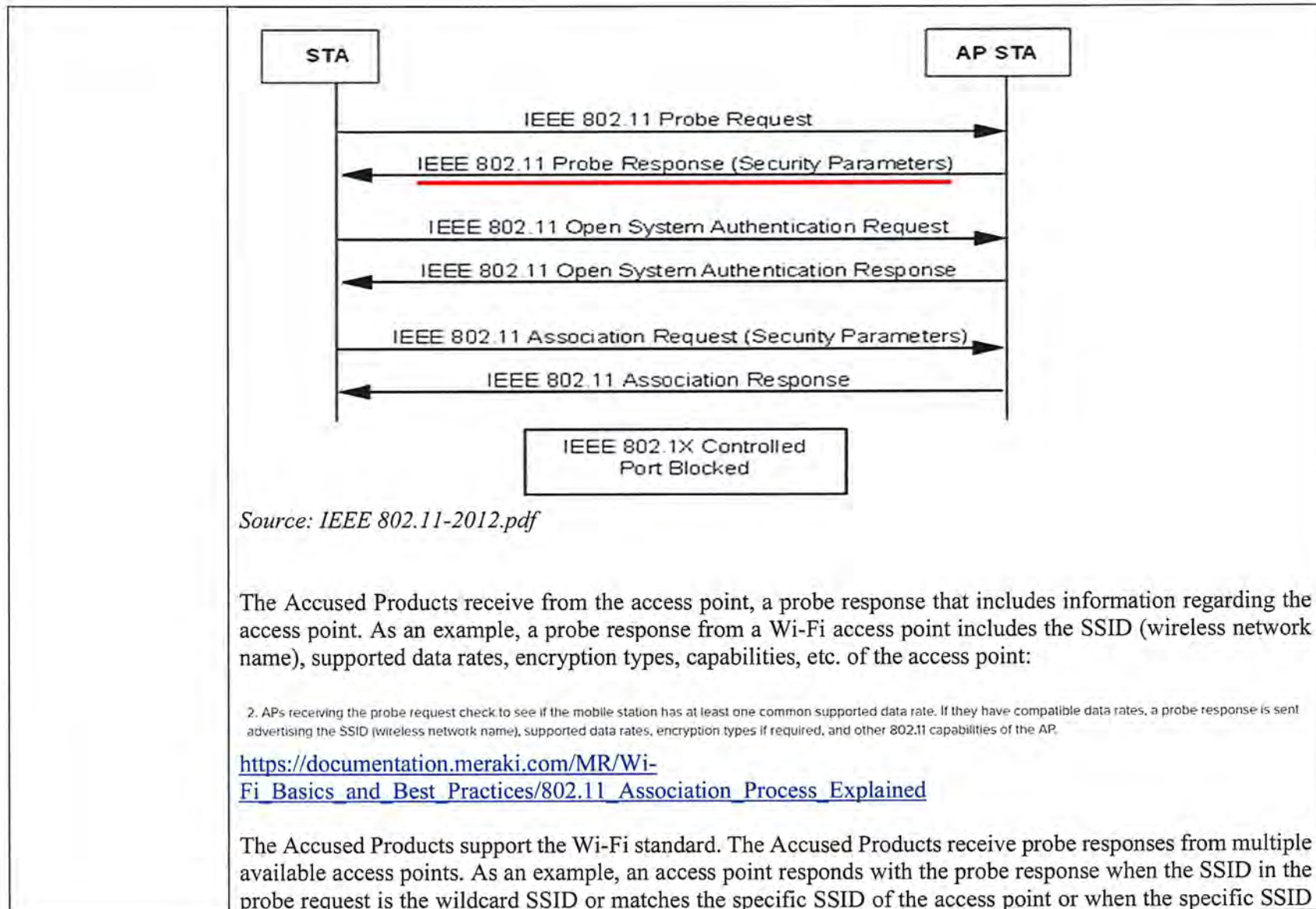
<https://www.youtube.com/watch?v=dT63df6nnqU>

An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.

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

[17d] a receiver coupled to the processor and operable to receive, from the access point, a probe response that includes information regarding the access point,	The Accused Products include a receiver coupled to the processor and operable to receive, from the access point, a probe response that includes information regarding the access point. The Accused Products receive probe responses for access points and thus necessarily include a receiver for receiving the response. The receiver is connected to the processor, as received information is processed by the processor. • Connectivity: The Galaxy S23 series boasts unparalleled Snapdragon Connect technologies across 5G, Wi-Fi, and Bluetooth®. Featuring the multiple-award-winning Snapdragon X70 5G Modem-RF System with the Qualcomm® 5G AI Processor, the Galaxy S23 series harnesses the power of AI to enable breakthrough 5G coverage, power efficiency, speeds, and latency. These new devices also support 5G+5G/4G Dual-SIM Dual-Active³, which harnesses the power and flexibility of two 5G SIMs at once. Additionally, all Galaxy S23 series variants feature the Qualcomm® FastConnect™ 6900 and 7800 systems delivering multi-gigabit Wi-Fi speeds, ultra-low latency, and deeply immersive Bluetooth Audio experiences. https://www.qualcomm.com/news/releases/2023/02/qualcomm-and-samsung-partner-to-bring-the-fastest-snapdragon-eve
---	---

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



of the access point is included in the SSID List element. As a further example, an access point responds to a probe request when it supports data rates or other requirements of the Accused Products.

Persistent randomization

Android uses the persistent randomization type by default when the MAC randomization feature is enabled. Android generates a persistent randomized MAC address based on the parameters of the network profile including SSID, security type, or FQDN (for Passpoint networks). This MAC address remains the same until factory reset. The MAC address does not get re-randomized if the user forgets and re-adds the Wi-Fi network since the MAC address depends on the parameters of the network profile.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

MAC Randomization Behavior

The MAC randomization feature allows devices to use a randomized MAC address when connecting to a Wi-Fi network. For implementation instructions, see [Implementing MAC Randomization](#). This page describes the behavior of MAC randomization in Android.

MAC addresses are used by devices when connecting to a Wi-Fi network or an access point. Because these MAC addresses are transmitted without encryption, they can be captured and used to potentially track a user's location. Historically, devices use the factory MAC address to associate to a Wi-Fi network. The factory MAC address is globally unique and static, allowing the device to be tracked and individually identified.

The MAC randomization feature increases user privacy by using a randomized MAC address when connecting to a Wi-Fi network.

MAC addresses are 48 bits long and usually represented by 12 hex digits (6 octets as each octet is 8 bits) such as 00:11:22:AA:BB:CC. The MAC randomization feature randomizes the address by setting the locally administered bit to 1, and the unicast bit to 0. The other 46 bits are randomized.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

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

For devices running Android 10 or higher, the framework uses randomized MAC address by default. Users can enable or disable MAC randomization for individual networks through an option in the **Network details** screen in **Settings**, as shown in Figure 1. If a user disables MAC randomization for a network, the framework uses the factory MAC address (globally unique address).

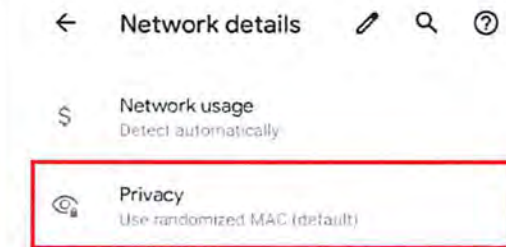


Figure 1. MAC randomization option.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

MAC Randomization Behavior

The MAC randomization feature allows devices to use a randomized MAC address when connecting to a Wi-Fi network. For implementation instructions, see [Implementing MAC Randomization](#). This page describes the behavior of MAC randomization in Android.

MAC addresses are used by devices when connecting to a Wi-Fi network or an access point. Because these MAC addresses are transmitted without encryption, they can be captured and used to potentially track a user's location. Historically, devices use the factory MAC address to associate to a Wi-Fi network. The factory MAC address is globally unique and static, allowing the device to be tracked and individually identified.

The MAC randomization feature increases user privacy by using a randomized MAC address when connecting to a Wi-Fi network.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

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

IP settings
DHCP

Proxy
None

Metered network
Detect automatically

MAC address type
Randomised MAC

MAC address
26:de:a1:0d:0f:41

GALAXY S23, PLUS
Set MAC Address Type to
Randomized
MAC/Phone MAC

<https://www.youtube.com/watch?v=dT63df6nnqU>

STA

AP STA

IEEE 802.11 Probe Request

IEEE 802.11 Probe Response (Security Parameters)

IEEE 802.11 Open System Authentication Request

IEEE 802.11 Open System Authentication Response

IEEE 802.11 Association Request (Security Parameters)

IEEE 802.11 Association Response

IEEE 802.1X Controlled Port Blocked

Source: IEEE 802.11-2012.pdf

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

Information regarding the access point is included in the probe response, as shown below.

Table 8-27—Probe Response frame body

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability	
4	SSID	If <code>dot11MeshActivated</code> 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.
9	IBSS Parameter Set	The IBSS Parameter Set element is present only within Probe Response frames generated by STAs in an IBSS.
10	Country	The Country element is present if <code>dot11MeshDomainCapabilityActivated</code> is true or <code>dot11SpectrumManagementRequired</code> is true or <code>dot11RadioMeasurementActivated</code> is true.
11	FH Parameters	The FH Parameters element, as specified in 8.4.2.11, is optionally present if <code>dot11MeshDomainCapabilityActivated</code> is true.
12	FH Pattern Table	The FH Pattern Table element, as specified in 8.4.2.12, is optionally present if <code>dot11MeshDomainCapabilityActivated</code> is true.
13	Power Constraint	The Power Constraint element is present if <code>dot11SpectrumManagementRequired</code> is true and is optionally present if <code>dot11RadioMeasurementActivated</code> is true.
14	Channel Switch Announcement	The Channel Switch Announcement element is optionally present if <code>dot11SpectrumManagementRequired</code> is true.
15	Quiet	The Quiet element is optionally present if <code>dot11SpectrumManagementRequired</code> is true or if <code>dot11RadioMeasurementActivated</code> is true.
16	IBSS DFS	The IBSS DFS element is present if <code>dot11SpectrumManagementRequired</code> is true in an IBSS.
17	TPC Report	The TPC Report element is present if <code>dot11SpectrumManagementRequired</code> is true or <code>dot11RadioMeasurementActivated</code> is true.
18	ERP	The ERP element is present within Probe Response frames generated by STAs using ERPs and is optionally present otherwise.
19	Extended Supported Rates	The Extended Supported Rates element is present if there are more than eight supported rates, and it is optionally present otherwise.
20	RSN	The RSN is present only if <code>dot11RSNAActivated</code> is true.
21	BSS Load	The BSS Load element is present if <code>dot11QoSOptionImplemented</code> and <code>dot11QBSSLoadImplemented</code> are both true.
22	EDCA Parameter Set	The EDCA Parameter Set element is present if <code>dot11QoSOptionImplemented</code> is true and <code>dot11MeshActivated</code> is

<https://mrnciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

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

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.
26	AP Channel Report	If dot11RMAFChannelReportActivated is true, one AP Channel Report element is optionally present for each operating class that has at least 1 channel to report.
27	BSS Average Access Delay	The BSS Average Access Delay element is optionally present if dot11RMBSSAverageAccessDelayActivated is true and the value of the AP Average Access Delay field is not equal to 255 (measurement not available).
28	Antenna	The Antenna element is optionally present if dot11RMAntennaInformationActivated is true and the value of the Antenna ID field is not equal to 0 (unknown antenna).
29	BSS Available Admission Capacity	The BSS Available Admission Capacity element is optionally present if dot11RMBSSAvailableAdmissionCapacityActivated is true with the following exceptions: 1) when Available Admission Capacity Bitmap equals 0 (Available Admission Capacity List contains no entries), or 2) when the BSS Load element is present and the Available Capacity Bitmap equals 256 (Available Admission Capacity List contains only the AC_VO entry).
30	BSS AC Access Delay	The BSS AC Access Delay element is optionally present if dot11RMBSSAverageAccessDelayActivated is true and at least one field of the element is not equal to 255 (measurement not available).
31	Mobility Domain	The MDE is present if dot11FastBSSTransitionActivated is true.
32	DSE registered location	The DSE Registered Location element is present if dot11LCIDSERequired is true.
33	Extended Channel Switch Announcement	The Extended Channel Switch Announcement element is optionally present if dot11ExtendedChannelSwitchActivated is true.
34	Supported Operating Classes	The Supported Operating Classes element is present if dot11ExtendedChannelSwitchActivated is true.
35	HT Capabilities	The HT Capabilities element is present when dot11HighThroughputOptionImplemented attribute is true.
36	HT Operation	The HT Operation element is included by an AP and a mesh STA when dot11HighThroughputOptionImplemented attribute is true.
37	20-40 BSS Coexistence	The 20-40 BSS Coexistence element is optionally present when the dot112040BSSCoexistenceManagementSupport attribute is true.
38	Overlapping BSS Scan Parameters	The Overlapping BSS Scan Parameters element is optionally present if the dot11FortyMHzOptionImplemented attribute is true.
39	Extended Capabilities	The Extended Capabilities element is optionally present if any of the fields in this element are nonzero.

<https://mrnciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

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

40	QoS Traffic Capability	The QoS Traffic Capability element is optionally present if dot11MgmtOptionACStationCountActivated is true.
41	Channel Usage	The Channel Usage element is present if the Channel Usage element is present in the Probe Request frame and dot11MgmtOptionChannelUsageActivated is true.
42	Time Advertisement	The Time Advertisement element is present if dot11MgmtOptionUTCSTSOOffsetActivated is true.
43	Time Zone	The Time Zone element is present if dot11MgmtOptionUTCSTSOOffsetActivated is true.
44	Interworking	The Interworking element is present if dot11InterworkingServiceActivated is true.
45	Advertisement Protocol	Advertisement Protocol element is present if dot11InterworkingServiceActivated is true and at least one dot11GASAdvertisementID MIB attribute exists.
46	Roaming Consortium	The Roaming Consortium element is present if dot11InterworkingServiceActivated is true and the dot11RoamingConsortiumTable has at least one entry.
47	Emergency Alert Identifier	One or more Emergency Alert Identifier elements are present if dot11EASActivated is true and there are one or more EAS message(s) active in the network.
48	Mesh ID	The Mesh ID element is present if dot11MeshActivated is true.
49	Mesh Configuration	The Mesh Configuration element is present if dot11MeshActivated is true.
50	Mesh Awake Window	The Mesh Awake Window element is optionally present if dot11MeshActivated is true.
51	Beacon Timing	The Beacon Timing element is optionally present if both dot11MeshActivated and dot11MBCAActivated are true.
52	MCCAOP Advertisement Overview	The MCCAOP Advertisement Overview element is optionally present if both dot11MeshActivated and dot11MCCAActivated are true.
53	MCCAOP Advertisement	One or more MCCAOP Advertisement elements are optionally present if both dot11MeshActivated and dot11MCCAActivated are true.
54	Mesh Channel Switch Parameters	The Mesh Channel Switch Parameters element is present if dot11MeshActivated is true and either Channel Switch Announcement element or Extended Channel Switch Announcement element is present.
Last-1	Vendor Specific	One or more vendor-specific elements are optionally present. These elements follow all other elements, except the Requested elements.
Last-n	Requested elements	Elements requested by the Request element of the Probe Request frame are present if dot11MultiDomainCapabilityActivated is true. See 10.1.4.3.2.

<https://mmcciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

4.3.13.15 SSID list

The SSID List element enables the non-AP STA to request information on a list of SSIDs. This is intended to reduce the number of Probe Request frames sent by the non-AP STA.

Source: IEEE 802.11-2012.pdf

In an infrastructure BSS or in an IBSS, STAs receiving Probe Request frames shall respond with a probe response when the SSID in the probe request is the wildcard SSID or matches the specific SSID of the STA or when the specific SSID of the STA is included in the SSID List element. Furthermore, a STA with dot11RadioMeasurementActivated true receiving a probe request with a DSSS Parameter Set element containing a Current Channel field value that is not the same as the value of dot11CurrentChannel shall not respond with a probe response. An AP shall respond to all probe requests meeting the above criteria. In an IBSS a STA that transmitted a Beacon frame since the last TBTT shall respond to group addressed Probe Request frames. A STA in an IBSS shall respond to Probe Request frames sent to the individual address of the STA.

Source: IEEE 802.11-2012.pdf

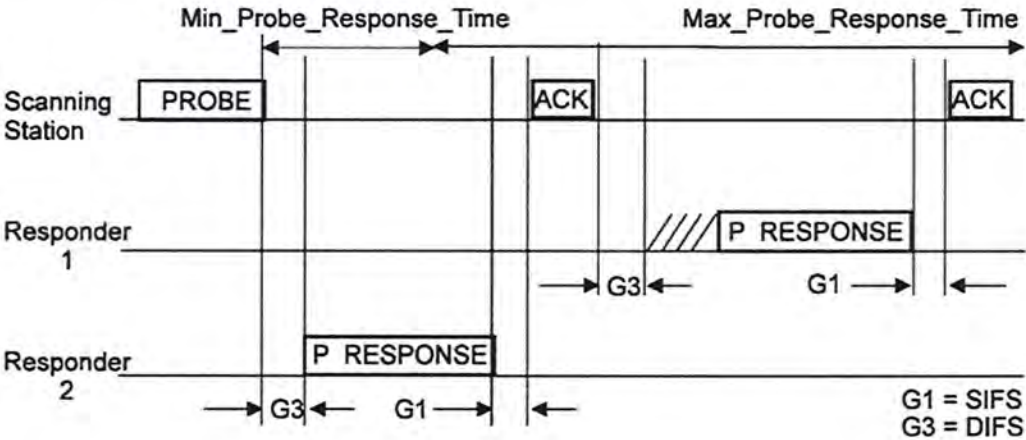


Figure 10-3—Probe response

Source: IEEE 802.11-2012.pdf

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

Before answering the question, let us first understand what a preferred network list is. The PNL is a historical record of all the network names (SSIDs) that a device has previously connected to, and trusts to automatically connect to again in the future.

User devices trying to connect to a Wi-Fi network watch for access points (APs) broadcasting its availability for a device to connect to its network. Within that information contains the network name, or Service Set Identifier (SSID). Wi-Fi enabled devices trying to connect to a wireless network, and using Active Service Discovery, will then broadcast its interest in connecting to the AP if the network name is in its PNL, which increases the connection speed.

For instance, if you connect to a **Starbucks** Wi-Fi network once, your device will remember and try to automatically connect to any network with the SSID Starbucks. This is true whether you go to the same Starbucks in the future, or a Starbucks 1,000 miles away. All the user device knows is the network name; no additional data is stored. Auto-connecting to wireless networks in PNL saves time and is convenient for the user, but it is a security risk. Therefore, it is important to identify all networks in the PNL and stop connecting automatically to Wi-Fi to stay safe.

<https://blog.pulsarsecurity.com/preferred-network-list-pnl>

The reason for client scanning is to determine a suitable AP to which the client may need to roam now or in the future. A client can use two scanning methods: active and passive. During an active scan, the client radio transmits a probe request and listens for a probe response from an AP. With a passive scan, the client radio listens on each channel for beacons sent periodically by an AP. A passive scan generally takes more time, since the client must listen and wait for a beacon versus actively probing to find an AP. Another limitation with a passive scan is that if the client does not wait long enough on a channel, then the client may miss an AP beacon.

<https://www.wi-fi.org/knowledge-center/faq/what-are-passive-and-active-scanning>

Below is an example of a Wi-Fi probe response that includes information of the access point.

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

802.11 Management - Probe Response

- Probe Timestamp: 23996945615 *Microseconds* [24-31]
- Beacon Interval: 102 *Time Units (104 Milliseconds, and 448 Microseconds)* [32-33]
- Capability Info: %0001000000000001
- SSID ID=0 SSID Len=4 SSID=OPEN
- Supported Rates**
 - Element ID: 1 *Supported Rates* [42]
 - Length: 4 [43]
 - Supported Rate: 24.0 *Mbps (BSS Basic Rate)* [44]
 - Supported Rate: 36.0 *Mbps (Not BSS Basic Rate)* [45]
 - Supported Rate: 48.0 *Mbps (Not BSS Basic Rate)* [46]
 - Supported Rate: 54.0 *Mbps (Not BSS Basic Rate)* [47]
- Country**
 - Element ID: 7 *Country* [48]
 - Length: 18 [49]
 - Country Code: AU [50-51]
 - Environment: 0x20 *Any* [52]
 - Starting Channel: 36 [53]
 - Number of Channels: 4 [54]
 - Max Tx Power (dBm): 23 [55]
 - Starting Channel: 52 [56]
 - Number of Channels: 4 [57]
 - Max Tx Power (dBm): 23 [58]
 - Starting Channel: 100 [59]
 - Number of Channels: 5 [60]
 - Max Tx Power (dBm): 30 [61]
 - Starting Channel: 132 [62]
 - Number of Channels: 3 [63]
 - Max Tx Power (dBm): 30 [64]
 - Starting Channel: 149 [65]
 - Number of Channels: 5 [66]
 - Max Tx Power (dBm): 30 [67]
- QoS Load**
 - Element ID: 11 *QoS Load* [68]
 - Length: 5 [69]
 - Station Count: 1 [70-71]
 - Channel Utilization: 0 % [72]
 - Avail Admission Capacity: 26562 [73-74]
- HT Cap= ID=45 HT Cap Len=26

<https://mrnciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.

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

[17e] 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	The processor determines 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. As an example, the processor running the OS 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 initiate 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. <u>Persistent randomization</u> <u>Android uses the persistent randomization type by default when the MAC randomization feature is enabled. Android generates a persistent randomized MAC address based on the parameters of the network profile including SSID, security type, or FQDN (for Passpoint networks). This MAC address remains the same until factory reset. The MAC address does not get re-randomized if the user forgets and re-adds the Wi-Fi network since the MAC addressed depends on the parameters of the network profile.</u> <u>Persistent MAC addresses are necessary in cases where networks rely on the persistence of the MAC address to provide useful functionality to the user, for example, to remember a device and allow users to bypass the login screen as expected, or to enable parental controls.</u> <u>For Android 10 and 11, the framework uses persistent randomization for all networks when MAC randomization is enabled.</u> https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior
---	--

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

[android](#) / [device](#) / [generic](#) / [goldfish](#) / [refs/tags/android-9.0.0_r34](#) / [wifi](#) / [WifiConfigStore.xml](#)

blob: bb5645aacde00f44a93c3386c8e42cf140bfe6a5 [file] [log] [blame]

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<WifiConfigStoreData>
  <int name="Version" value="1" />
  <NetworkList>
    <Network>
      <WifiConfiguration>
        <string name="ConfigKey">&quot;AndroidWifi&quot;NONE</string>
        <string name="SSID">&quot;AndroidWifi&quot;</string>
        <null name="BSSID" />
        <null name="PreSharedKey" />
        <null name="WEPKeys" />
        <int name="WEPKeyIndex" value="0" />
        <boolean name="HiddenSSID" value="false" />
```

https://android.googlesource.com/device/generic/goldfish/+refs/tags/android-9.0.0_r34/wifi/WifiConfigStore.xml

In an infrastructure BSS or in an IBSS, STAs receiving Probe Request frames shall respond with a probe response when the SSID in the probe request is the wildcard SSID or matches the specific SSID of the STA or when the specific SSID of the STA is included in the SSID List element. Furthermore, a STA with dot11RadioMeasurementActivated true receiving a probe request with a DSSS Parameter Set element containing a Current Channel field value that is not the same as the value of dot11CurrentChannel shall not respond with a probe response. An AP shall respond to all probe requests meeting the above criteria. In an IBSS a STA that transmitted a Beacon frame since the last TBTT shall respond to group addressed Probe Request frames. A STA in an IBSS shall respond to Probe Request frames sent to the individual address of the STA.

Source: IEEE 802.11-2012.pdf

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

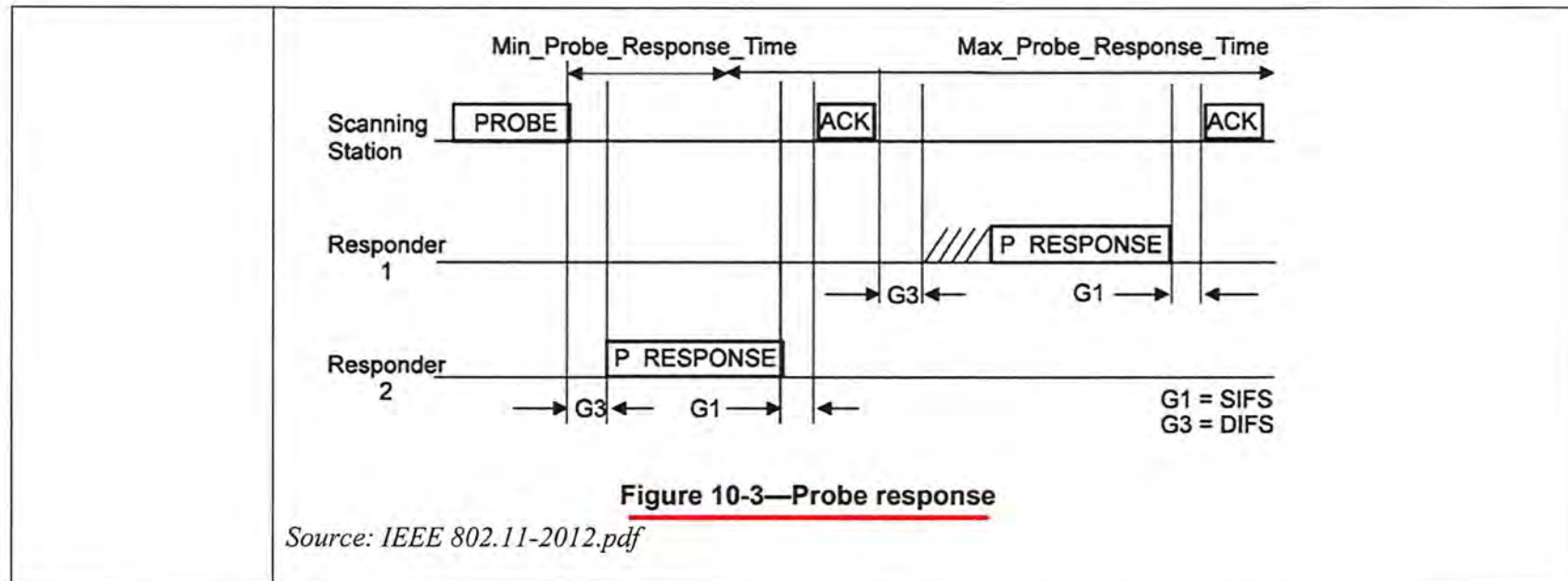


EXHIBIT A-INFRINGEMENT CONTENTIONS FOR U.S. PATENT NO. 10,694,384

Before answering the question, let us first understand what a preferred network list is. The PNL is a historical record of all the network names (SSIDs) that a device has previously connected to, and trusts to automatically connect to again in the future.

User devices trying to connect to a Wi-Fi network watch for access points (APs) broadcasting its availability for a device to connect to its network. Within that information contains the network name, or Service Set Identifier (SSID). Wi-Fi enabled devices trying to connect to a wireless network, and using Active Service Discovery, will then broadcast its interest in connecting to the AP if the network name is in its PNL, which increases the connection speed.

For instance, if you connect to a **Starbucks** Wi-Fi network once, your device will remember and try to automatically connect to any network with the SSID Starbucks. This is true whether you go to the same Starbucks in the future, or a Starbucks 1,000 miles away. All the user device knows is the network name; no additional data is stored. Auto-connecting to wireless networks in PNL saves time and is convenient for the user, but it is a security risk. Therefore, it is important to identify all networks in the PNL and stop connecting automatically to Wi-Fi to stay safe.

<https://blog.pulsarsecurity.com/preferred-network-list-pnl>

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

The screenshot displays a Wi-Fi packet analysis tool showing a '802.11 Management - Probe Response' packet. The packet details are as follows:

- Probe Timestamp:** 23996945615 Microseconds [24-31]
- Beacon Interval:** 102 Time Units (104 Milliseconds, and 448 Microseconds) [32-33]
- Capability Info:** %0001000000000001
- SSID ID=0 SSID Len=4 SSID=OPEN** (Annotated with 'information regarding access point')
- Supported Rates** (Annotated with 'information regarding access point'):
 - Element ID: 1 Supported Rates [42]
 - Length: 4 [43]
 - Supported Rate: 24.0 Mbps (BSS Basic Rate) [44]
 - Supported Rate: 36.0 Mbps (Not BSS Basic Rate) [45]
 - Supported Rate: 48.0 Mbps (Not BSS Basic Rate) [46]
 - Supported Rate: 54.0 Mbps (Not BSS Basic Rate) [47]
- Country** (Annotated with 'information regarding access point'):
 - Element ID: 7 Country [48]
 - Length: 18 [49]
 - Country Code: AU [50-51]
 - Environment: 0x20 Any [52]
 - Starting Channel: 36 [53]
 - Number of Channels: 4 [54]
 - Max Tx Power (dBm): 23 [55]
 - Starting Channel: 52 [56]
 - Number of Channels: 4 [57]
 - Max Tx Power (dBm): 23 [58]
 - Starting Channel: 100 [59]
 - Number of Channels: 5 [60]
 - Max Tx Power (dBm): 30 [61]
 - Starting Channel: 132 [62]
 - Number of Channels: 3 [63]
 - Max Tx Power (dBm): 30 [64]
 - Starting Channel: 149 [65]
 - Number of Channels: 5 [66]
 - Max Tx Power (dBm): 30 [67]
- OBSS Load** (Annotated with 'probe response'):
 - Element ID: 11 OBSS Load [68]
 - Length: 5 [69]
 - Station Count: 1 [70-71]
 - Channel Utilization: 0 % [72]
 - Avail Admission Capacity: 26562 [73-74]
- HT Cap= ID=45 HT Cap Len=26**

<https://mrncciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.

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

[17f] 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.	The hardware network interface (e.g., the Wi-Fi connection interface) of the Accused Products is operable to connect to a wireless local area network in response to a determination that the access point is the authenticated access point (e.g., a previously connected Wi-Fi access point). For example, the Galaxy S23 contains a FastConnect SOC which provides Wi-Fi connectivity: <table border="1" data-bbox="529 470 1648 686"><tr><th>Phone</th><th><u>Galaxy S23</u></th><th>Galaxy S23+</th><th>Galaxy S23 Ultra</th></tr><tr><th><u>Connectivity</u></th><td>5G, <u>Wi-Fi 6E</u>, Bluetooth 5.3, NFC</td><td>5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband</td><td>5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband</td></tr></table> https://www.androidpolice.com/samsung-galaxy-s23/ • Connectivity: The Galaxy S23 series boasts unparalleled Snapdragon Connect technologies across 5G, Wi-Fi, and Bluetooth®. Featuring the multiple-award-winning Snapdragon X70 5G Modem-RF System with the Qualcomm® 5G AI Processor, the Galaxy S23 series harnesses the power of AI to enable breakthrough 5G coverage, power efficiency, speeds, and latency. These new devices also support 5G+5G/4G Dual-SIM Dual-Active³, which harnesses the power and flexibility of two 5G SIMs at once. Additionally, all Galaxy S23 series variants feature the Qualcomm® FastConnect™ 6900 and 7800 systems delivering multi-gigabit Wi-Fi speeds, ultra-low latency, and deeply immersive Bluetooth Audio experiences. https://www.qualcomm.com/news/releases/2023/02/qualcomm-and-samsung-partner-to-bring-the-fastest-snapdragon-eve	Phone	<u>Galaxy S23</u>	Galaxy S23+	Galaxy S23 Ultra	<u>Connectivity</u>	5G, <u>Wi-Fi 6E</u> , Bluetooth 5.3, NFC	5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband	5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband
Phone	<u>Galaxy S23</u>	Galaxy S23+	Galaxy S23 Ultra						
<u>Connectivity</u>	5G, <u>Wi-Fi 6E</u> , Bluetooth 5.3, NFC	5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband	5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband						

Qualcomm® FastConnect™ 7800 Mobile Connectivity System



Leading Wi-Fi 7 and Dual Bluetooth come together in this powerful and versatile connectivity system

FastConnect is an advanced 14nm Wi-Fi and Bluetooth® Connectivity system delivering fast global speeds and ultra-low sustained latency. Unlock extreme performance for mobile, compute, and XR experiences.

<https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/images/products/by-technology/wi-fi/Qualcomm-FastConnect-7800-Overview-Infographic.png>

After receiving the probe response from the access point, as discussed above, the Accused Products confirm the received SSID information from the probe responses with the access point information stored in its memory. Once confirmed that there is an SSID in a probe response from an access point with which the UE was connected previously, the Accused Products initiate a connection using the persistent MAC address for the access point, which is an authentic device identifier for the Accused Product.

Persistent randomization

Android uses the persistent randomization type by default when the MAC randomization feature is enabled. Android generates a persistent randomized MAC address based on the parameters of the network profile including SSID, security type, or FQDN (for Passpoint networks). This MAC address remains the same until factory reset. The MAC address does not get re-randomized if the user forgets and re-adds the Wi-Fi network since the MAC address depends on the parameters of the network profile.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>



<https://www.youtube.com/watch?v=dT63df6nnqU>

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

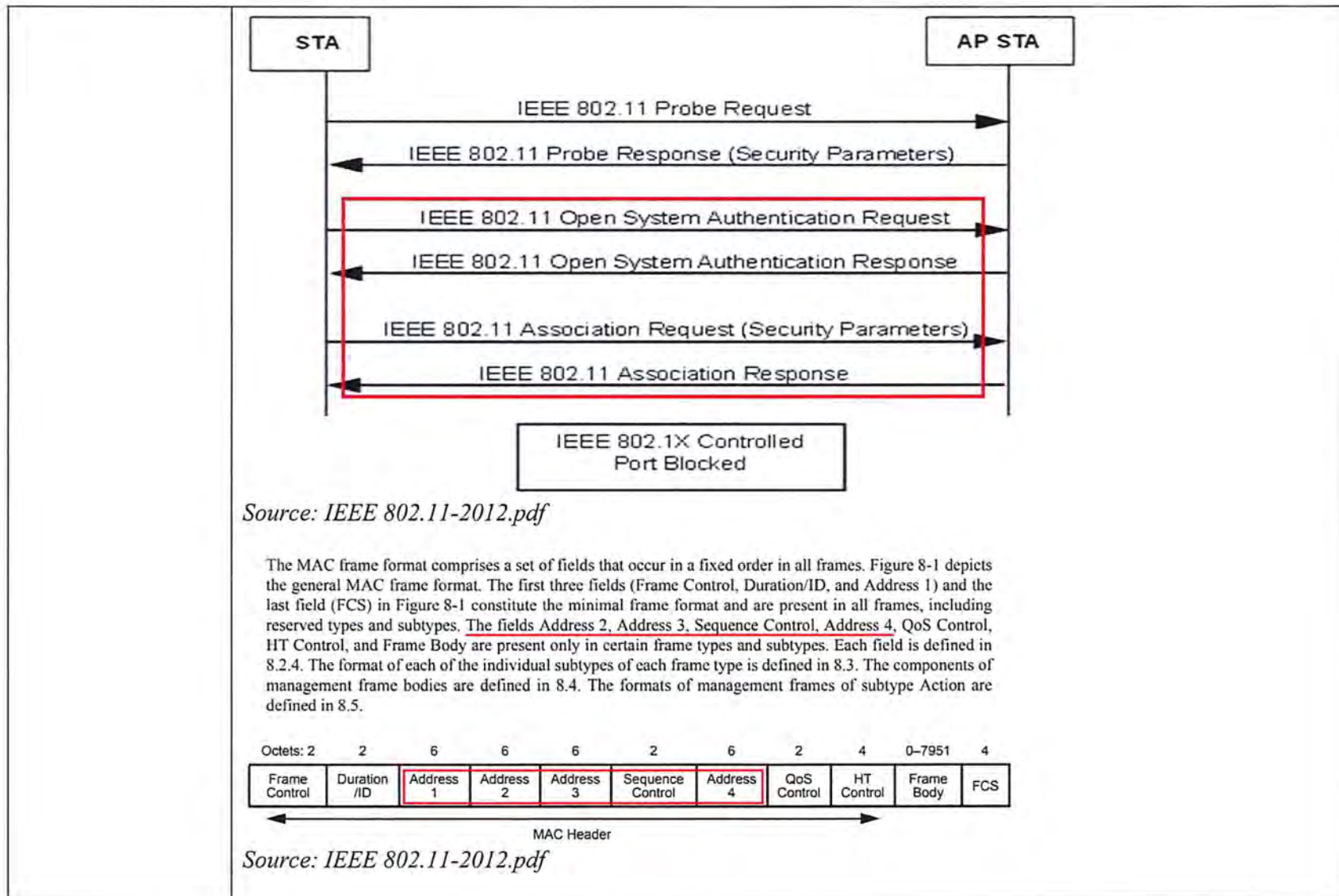


EXHIBIT A-INFRINGEMENT CONTENTIONS FOR U.S. PATENT NO. 10,694,384

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.

Source: IEEE 802.11-2012.pdf

802.11 Mgmt : Authentication Frame

POSTED BY NAYARASI IN CWAP

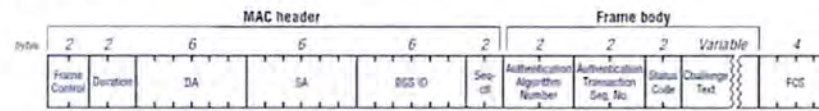
≈ 10 COMMENTS

Once a client station is discover a SSID (Probe Request/Response or listening to Beacons) it move to Join phase. This exchange comprise of at least 4 frames

1. Authentication (Request)
2. Authentication (Response)
3. Association Request
4. Association Response

The frame format of those Authentication frames are as shown below. (from page 136- CWAP Official Study Guide)

FIGURE 4.8 Authentication frame format



<https://mrnciew.com/2014/10/10/802-11-mgmt-authentication-frame/>

As shown, the Accused Products may use persistent randomization, in which for the same Wi-Fi network and device combination, the MAC address remains the same. When an Accused Product connects to a Wi-Fi network it was previously connected to, it will use the same MAC address.

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

Persistent randomization

Android uses the persistent randomization type by default when the MAC randomization feature is enabled. Android generates a persistent randomized MAC address based on the parameters of the network profile including SSID, security type, or FQDN (for Passpoint networks). This MAC address remains the same until factory reset. The MAC address does **not** get re-randomized if the user forgets and re-adds the Wi-Fi network since the MAC address depends on the parameters of the network profile.

Persistent MAC addresses are necessary in cases where networks rely on the persistence of the MAC address to provide useful functionality to the user, for example, to remember a device and allow users to bypass the login screen as expected, or to enable parental controls.

For Android 10 and 11, the framework uses persistent randomization for all networks when MAC randomization is enabled.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

[android / device / generic / goldfish / refs/tags/android-9.0.0_r34 / _ / wifi / WifiConfigStore.xml](#)

blob: bb5645aacde0f44a93c3386c8e42cf140bfe6a5 [file] [log] [blame]

```
1  <?xml version='1.0' encoding='utf-8' standalone='yes' ?>
2  <WifiConfigStoreData>
3      <int name="Version" value="1" />
4      <NetworkList>
5          <Network>
6              <WifiConfiguration>
7                  <string name="ConfigKey">&quot;AndroidWifi&quot;NONE</string>
8                  <string name="SSID">&quot;AndroidWifi&quot;</string>
9                  <null name="BSSID" />
10                 <null name="PreSharedKey" />
11                 <null name="WEPKeys" />
12                 <int name="WEPTxKeyIndex" value="0" />
13                 <boolean name="HiddenSSID" value="false" />
```

https://android.googlesource.com/device/generic/goldfish/+refs/tags/android-9.0.0_r34/wifi/WifiConfigStore.xml

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

	An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.										
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.	The Accused Products connect to access points that include Wi-Fi access points, and the wireless local area network includes a Wi-Fi network. The Accused Products are designed to connect to Wi-Fi access points in order to join a Wi-Fi network. <table border="1"> <thead> <tr> <th>Phone</th><th><u>Galaxy S23</u></th><th>Galaxy S23+</th><th>Galaxy S23 Ultra</th></tr> </thead> <tbody> <tr> <td><u>Connectivity</u></td><td>5G, <u>Wi-Fi 6E</u>, Bluetooth 5.3, NFC</td><td>5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband</td><td>5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband</td></tr> </tbody> </table> https://www.androidpolice.com/samsung-galaxy-s23/			Phone	<u>Galaxy S23</u>	Galaxy S23+	Galaxy S23 Ultra	<u>Connectivity</u>	5G, <u>Wi-Fi 6E</u> , Bluetooth 5.3, NFC	5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband	5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband
Phone	<u>Galaxy S23</u>	Galaxy S23+	Galaxy S23 Ultra								
<u>Connectivity</u>	5G, <u>Wi-Fi 6E</u> , Bluetooth 5.3, NFC	5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband	5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband								

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

	Galaxy S23  Wi-Fi 6E <u>802.11 a/b/g/n/ac/ax</u> https://www.samsung.com/us/smartphones/galaxy-s23/specs/ • Connectivity: The Galaxy S23 series boasts unparalleled Snapdragon Connect technologies across 5G, Wi-Fi, and Bluetooth®. Featuring the multiple-award-winning Snapdragon X70 5G Modem-RF System with the Qualcomm® 5G AI Processor, the Galaxy S23 series harnesses the power of AI to enable breakthrough 5G coverage, power efficiency, speeds, and latency. These new devices also support 5G+5G/4G Dual-SIM Dual-Active³, which harnesses the power and flexibility of two 5G SIMs at once. Additionally, all Galaxy S23 series variants feature the Qualcomm® FastConnect™ 6900 and 7800 systems delivering multi-gigabit Wi-Fi speeds, ultra-low latency, and deeply immersive Bluetooth Audio experiences. https://www.qualcomm.com/news/releases/2023/02/qualcomm-and-samsung-partner-to-bring-the-fastest-snapdragon-eve
19. The end device of claim 17, wherein	The processor is operable to generate the fake MAC address from one or more characters that are selected randomly.

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

the processor is operable to generate the MAC address from one or more characters that are selected randomly.	The processor generates a fake MAC address by, for example, randomly setting one or more bits of the MAC address (e.g., setting the locally administered bit to 1, the unicast bit to 0, and then randomizing the remaining 46 bits). <u>MAC Randomization Behavior</u> □ - <u>The MAC randomization feature allows devices to use a randomized MAC address when connecting to a Wi-Fi network. For implementation instructions, see implementing MAC Randomization. This page describes the behavior of MAC randomization in Android.</u> <u>MAC addresses are used by devices when connecting to a Wi-Fi network or an access point. Because these MAC addresses are transmitted without encryption, they can be captured and used to potentially track a user's location. Historically, devices use the factory MAC address to associate to a Wi-Fi network. The factory MAC address is globally unique and static, allowing the device to be tracked and individually identified.</u> <u>The MAC randomization feature increases user privacy by using a randomized MAC address when connecting to a Wi-Fi network.</u> <u>MAC addresses are 48 bits long and usually represented by 12 hex digits (6 octets as each octet is 8 bits) such as 00:11:22:AA:BB:CC. The MAC randomization feature randomizes the address by setting the locally administered bit to 1, and the unicast bit to 0. The other 46 bits are randomized.</u> https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
20. The end device of claim 17, wherein: the transmitter is further operable to transmit, to the access point in	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. The Accused Products confirm the received access point identifying information (e.g., the SSID information) from the probe responses with the access point information stored in memory. If the received information correlates to the access point list, then the access point was previously connected and thus an authenticated access point. Once confirmed that there is an SSID in a probe response from an access point with which the UE was

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

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,

the receiver is further operable to receive, from the access point, an approval of the connection request, and

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.

connected previously, the transmitter transmits information to initiate a connection with the access point, which includes an authentic device identifier for the end device such as a persistent MAC address.

As shown, the Accused Products maintain a list of previously-connected access points and a persistent MAC address for each access point. The list of previously-connected access points is matched to the access point's SSID received in the probe response.

Persistent randomization

Android uses the persistent randomization type by default when the MAC randomization feature is enabled. Android generates a persistent randomized MAC address based on the parameters of the network profile including SSID, security type, or FQDN (for Passpoint networks). This MAC address remains the same until factory reset. The MAC address does not get re-randomized if the user forgets and re-adds the Wi-Fi network since the MAC address depends on the parameters of the network profile.

Persistent MAC addresses are necessary in cases where networks rely on the persistence of the MAC address to provide useful functionality to the user, for example, to remember a device and allow users to bypass the login screen as expected, or to enable parental controls.

For Android 10 and 11, the framework uses persistent randomization for all networks when MAC randomization is enabled.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

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

[android](#) / [device](#) / [generic](#) / [goldfish](#) / [refs/tags/android-9.0.0_r34](#) / [wifi](#) / [WifiConfigStore.xml](#)

blob: bb5645aacde00f44a93c3386c8e42cf140bfe6a5 [file] [log] [blame]

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<WifiConfigStoreData>
  <int name="Version" value="1" />
  <NetworkList>
    <Network>
      <WifiConfiguration>
        <string name="ConfigKey">&quot;AndroidWifi&quot;NONE</string>
        <string name="SSID">&quot;AndroidWifi&quot;</string>
        <null name="BSSID" />
        <null name="PreSharedKey" />
        <null name="WEPKeys" />
        <int name="WEPKeyIndex" value="0" />
        <boolean name="HiddenSSID" value="false" />
```

https://android.googlesource.com/device/generic/goldfish/+refs/tags/android-9.0.0_r34/wifi/WifiConfigStore.xml

In an infrastructure BSS or in an IBSS, STAs receiving Probe Request frames shall respond with a probe response when the SSID in the probe request is the wildcard SSID or matches the specific SSID of the STA or when the specific SSID of the STA is included in the SSID List element. Furthermore, a STA with dot11RadioMeasurementActivated true receiving a probe request with a DSSS Parameter Set element containing a Current Channel field value that is not the same as the value of dot11CurrentChannel shall not respond with a probe response. An AP shall respond to all probe requests meeting the above criteria. In an IBSS a STA that transmitted a Beacon frame since the last TBTT shall respond to group addressed Probe Request frames. A STA in an IBSS shall respond to Probe Request frames sent to the individual address of the STA.

Source: IEEE 802.11-2012.pdf

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

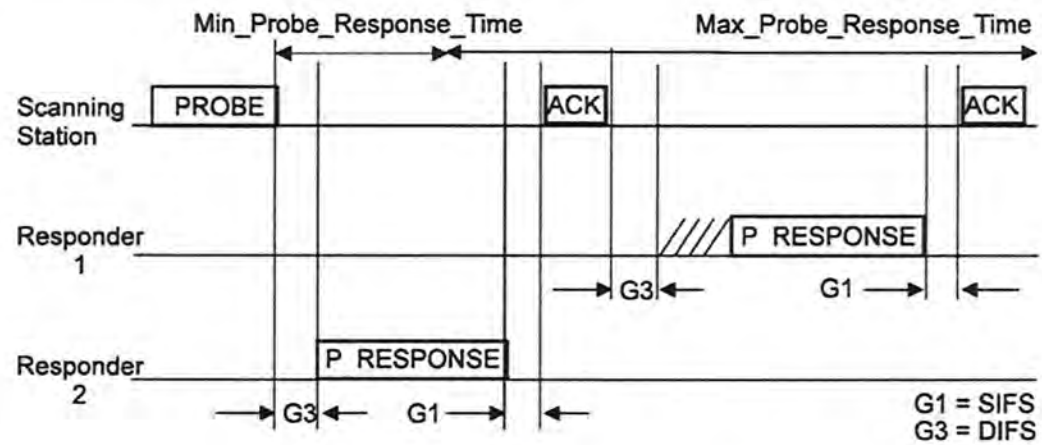


Figure 10-3—Probe response

Source: IEEE 802.11-2012.pdf

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

Before answering the question, let us first understand what a preferred network list is. The PNL is a historical record of all the network names (SSIDs) that a device has previously connected to, and trusts to automatically connect to again in the future.

User devices trying to connect to a Wi-Fi network watch for access points (APs) broadcasting its availability for a device to connect to its network. Within that information contains the network name, or Service Set Identifier (SSID). Wi-Fi enabled devices trying to connect to a wireless network, and using Active Service Discovery, will then broadcast its interest in connecting to the AP if the network name is in its PNL, which increases the connection speed.

For instance, if you connect to a **Starbucks** Wi-Fi network once, your device will remember and try to automatically connect to any network with the SSID Starbucks. This is true whether you go to the same Starbucks in the future, or a Starbucks 1,000 miles away. All the user device knows is the network name; no additional data is stored. Auto-connecting to wireless networks in PNL saves time and is convenient for the user, but it is a security risk. Therefore, it is important to identify all networks in the PNL and stop connecting automatically to Wi-Fi to stay safe.

<https://blog.pulsarsecurity.com/preferred-network-list-pnl>

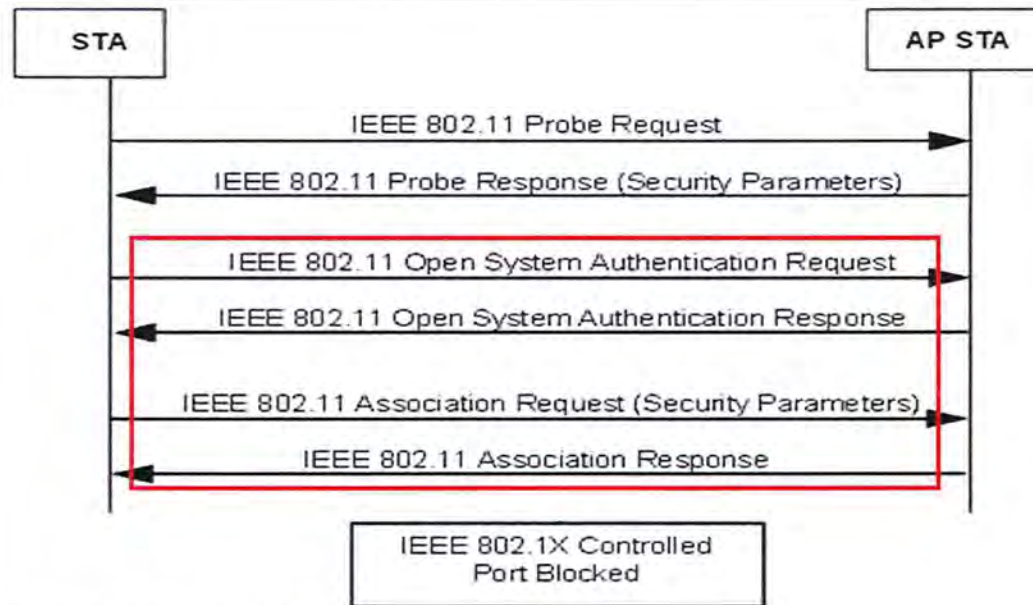
EXHIBIT A-INFRINGEMENT CONTENTIONS FOR U.S. PATENT NO. 10,694,384

802.11 Management - Probe Response

- Probe Timestamp: 23996945615 Microseconds [24-31]
- Beacon Interval: 102 Time Units (104 Milliseconds, and 448 Microseconds) [32-33]
- Capability Info: 0000000000000001
- SSID ID=0 SSID Len=4 SSID=OPEN
- Supported Rates
 - Element ID: 1 Supported Rates [42]
 - Length: 4 [43]
 - Supported Rate: 24.0 Mbps (BSS Basic Rate) [44]
 - Supported Rate: 36.0 Mbps (Not BSS Basic Rate) [45]
 - Supported Rate: 48.0 Mbps (Not BSS Basic Rate) [46]
 - Supported Rate: 54.0 Mbps (Not BSS Basic Rate) [47]
- Country
 - Element ID: 7 Country [48]
 - Length: 18 [49]
 - Country Code: AU [50-51]
 - Environment: 0x20 Any [52]
 - Starting Channel: 36 [53]
 - Number of Channels: 4 [54]
 - Max Tx Power (dBm): 23 [55]
 - Starting Channel: 52 [56]
 - Number of Channels: 4 [57]
 - Max Tx Power (dBm): 23 [58]
 - Starting Channel: 100 [59]
 - Number of Channels: 5 [60]
 - Max Tx Power (dBm): 30 [61]
 - Starting Channel: 132 [62]
 - Number of Channels: 3 [63]
 - Max Tx Power (dBm): 30 [64]
 - Starting Channel: 149 [65]
 - Number of Channels: 5 [66]
 - Max Tx Power (dBm): 30 [67]
- QSSS Load
 - Element ID: 11 QSSS Load [68]
 - Length: 5 [69]
 - Station Count: 1 [70-71]
 - Channel Utilization: 0 % [72]
 - Avail Admission Capacity: 26562 [73-74]
- HT Cap: ID=45 HT Cap Len=26

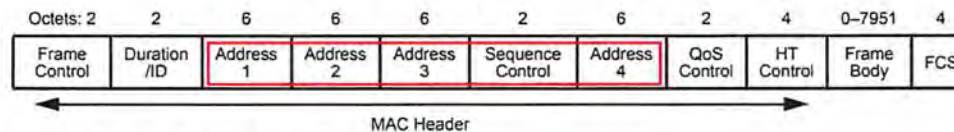
<https://mrncciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

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



Source: IEEE 802.11-2012.pdf

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.



Source: IEEE 802.11-2012.pdf

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

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.

Source: IEEE 802.11-2012.pdf

The receiver is operable to receive, from the access point, an approval of the connection request.

The Accused Products receive an open system authentication response and/or an association response from an access point.

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

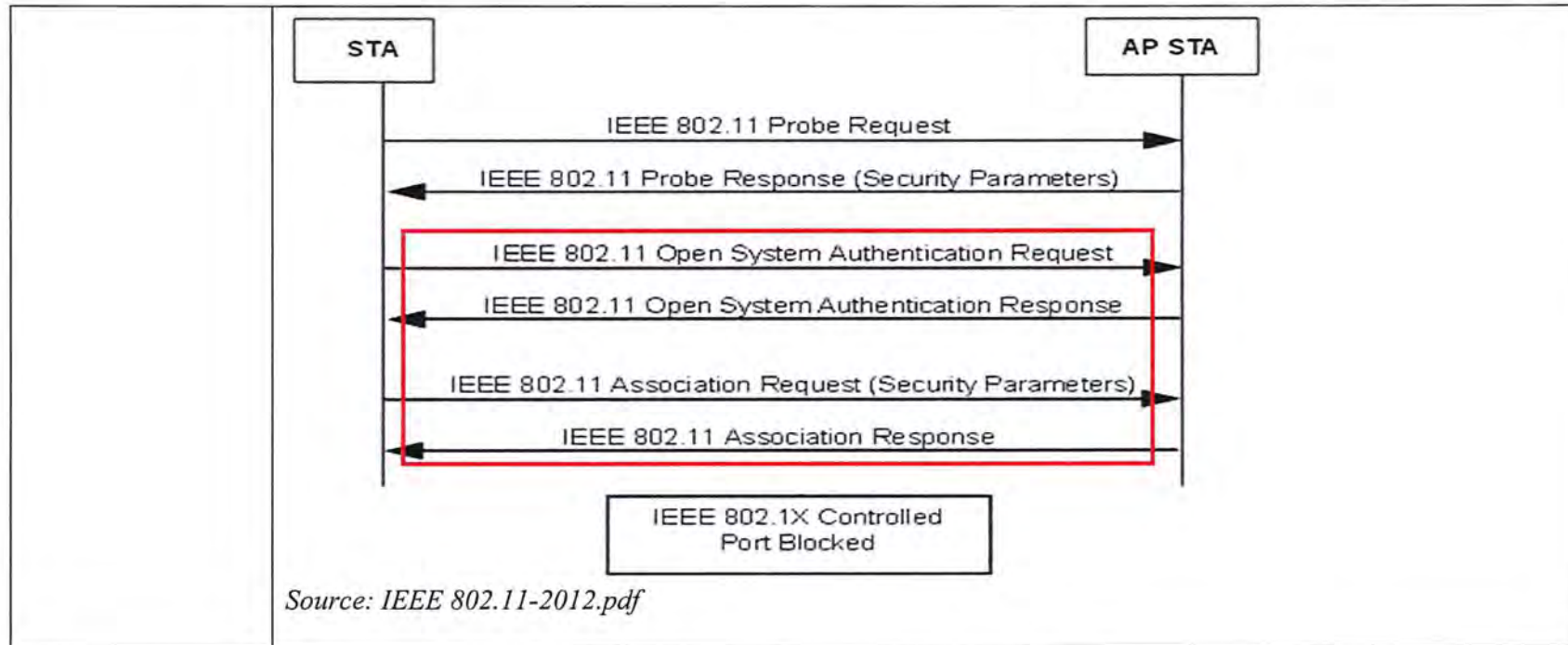


EXHIBIT A-INFRINGEMENT CONTENTIONS FOR U.S. PATENT NO. 10,694,384

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

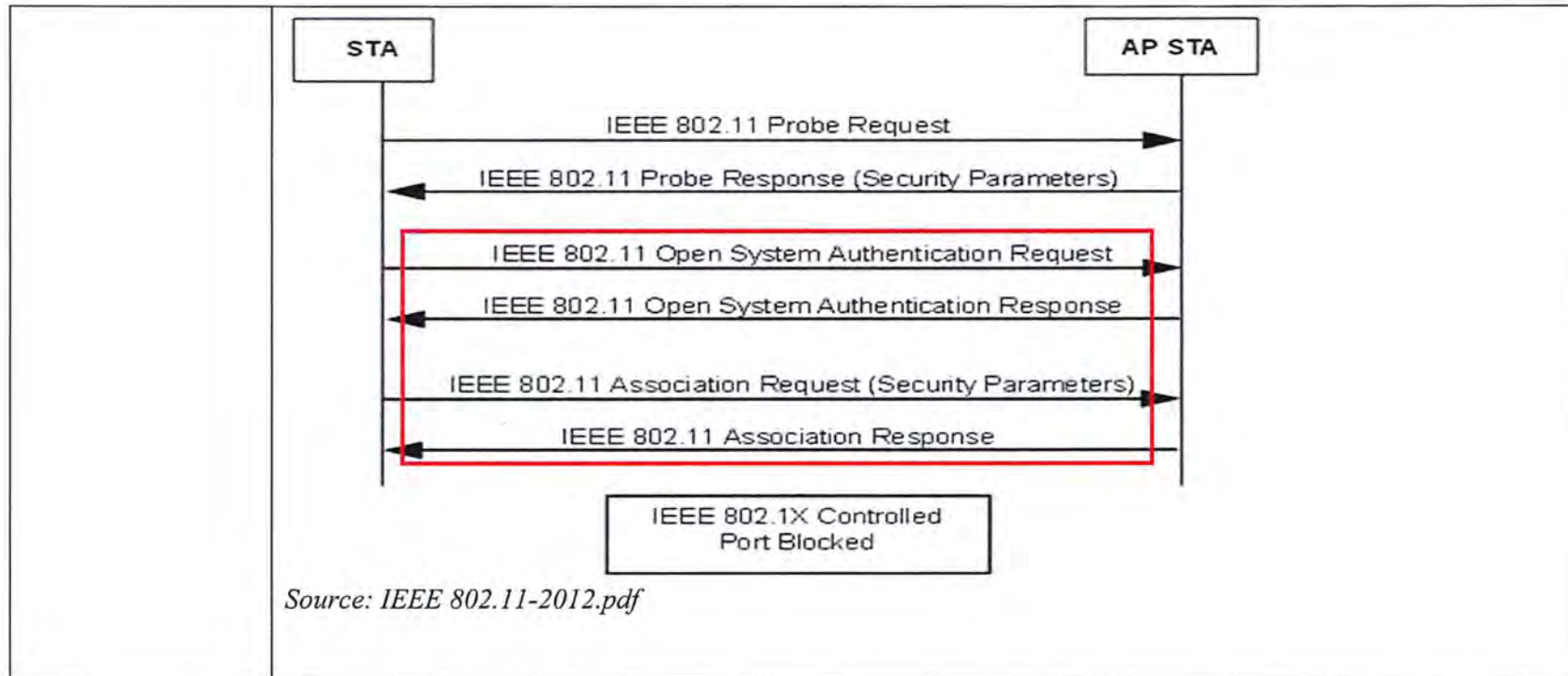
The TA field contains an IEEE MAC individual address that identifies the STA that has transmitted, onto the WM, the MPDU contained in the frame body field. The Individual/Group bit is always transmitted as a 0 in the transmitter address.

Source: IEEE 802.11-2012.pdf

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.

The Accused Products then transmit an association request. The Accused Products then receive an association response from the access point, at which point the Accused Product is connected to a network via the access point in accordance with the association response.

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



802.11 Mgmt : Authentication Frame

POSTED BY NAYARASI IN CWAP

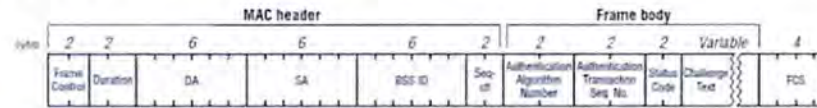
≈ 10 COMMENTS

Once a client station is discover a SSID (Probe Request/Response or listening to Beacons) it move to Join phase. This exchange comprise of at least 4 frames

1. Authentication (Request)
2. Authentication (Response)
3. Association Request
4. Association Response

The frame format of those Authentication frames are as shown below.(from page 136- CWAP Official Study Guide)

FIGURE 4.8 Authentication frame format



<https://mrnciew.com/2014/10/10/802-11-mgmt-authentication-frame/>

An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.

22. The end device of claim 17, further comprising a memory coupled to

The Accused Products have 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.

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

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.	As an example, 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. <u>Persistent randomization</u> <u>Android uses the persistent randomization type by default when the MAC randomization feature is enabled. Android generates a persistent randomized MAC address based on the parameters of the network profile including SSID, security type, or FQDN (for Passpoint networks). This MAC address remains the same until factory reset. The MAC address does not get re-randomized if the user forgets and re-adds the Wi-Fi network since the MAC address depends on the parameters of the network profile.</u> <u>Persistent MAC addresses are necessary in cases where networks rely on the persistence of the MAC address to provide useful functionality to the user, for example, to remember a device and allow users to bypass the login screen as expected, or to enable parental controls.</u> <u>For Android 10 and 11, the framework uses persistent randomization for all networks when MAC randomization is enabled.</u> https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior
---	--

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

[android](#) / [device](#) / [generic](#) / [goldfish](#) / [refs/tags/android-9.0.0_r34](#) / [wifi](#) / [WifiConfigStore.xml](#)

blob: bb5645aacde0f44a93c3386c8e42cf140bfe6a5 [file] [log] [blame]

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<WifiConfigStoreData>
  <int name="Version" value="1" />
  <NetworkList>
    <Network>
      <WifiConfiguration>
        <string name="ConfigKey">&quot;AndroidWifi&quot;NONE</string>
        <string name="SSID">&quot;AndroidWifi&quot;</string>
        <null name="BSSID" />
        <null name="PreSharedKey" />
        <null name="WEPKeys" />
        <int name="WEPKeyIndex" value="0" />
        <boolean name="HiddenSSID" value="false" />
```

https://android.googlesource.com/device/generic/goldfish/+refs/tags/android-9.0.0_r34/wifi/WifiConfigStore.xml

In an infrastructure BSS or in an IBSS, STAs receiving Probe Request frames shall respond with a probe response when the SSID in the probe request is the wildcard SSID or matches the specific SSID of the STA or when the specific SSID of the STA is included in the SSID List element. Furthermore, a STA with dot11RadioMeasurementActivated true receiving a probe request with a DSSS Parameter Set element containing a Current Channel field value that is not the same as the value of dot11CurrentChannel shall not respond with a probe response. An AP shall respond to all probe requests meeting the above criteria. In an IBSS a STA that transmitted a Beacon frame since the last TBTT shall respond to group addressed Probe Request frames. A STA in an IBSS shall respond to Probe Request frames sent to the individual address of the STA.

Source: IEEE 802.11-2012.pdf

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

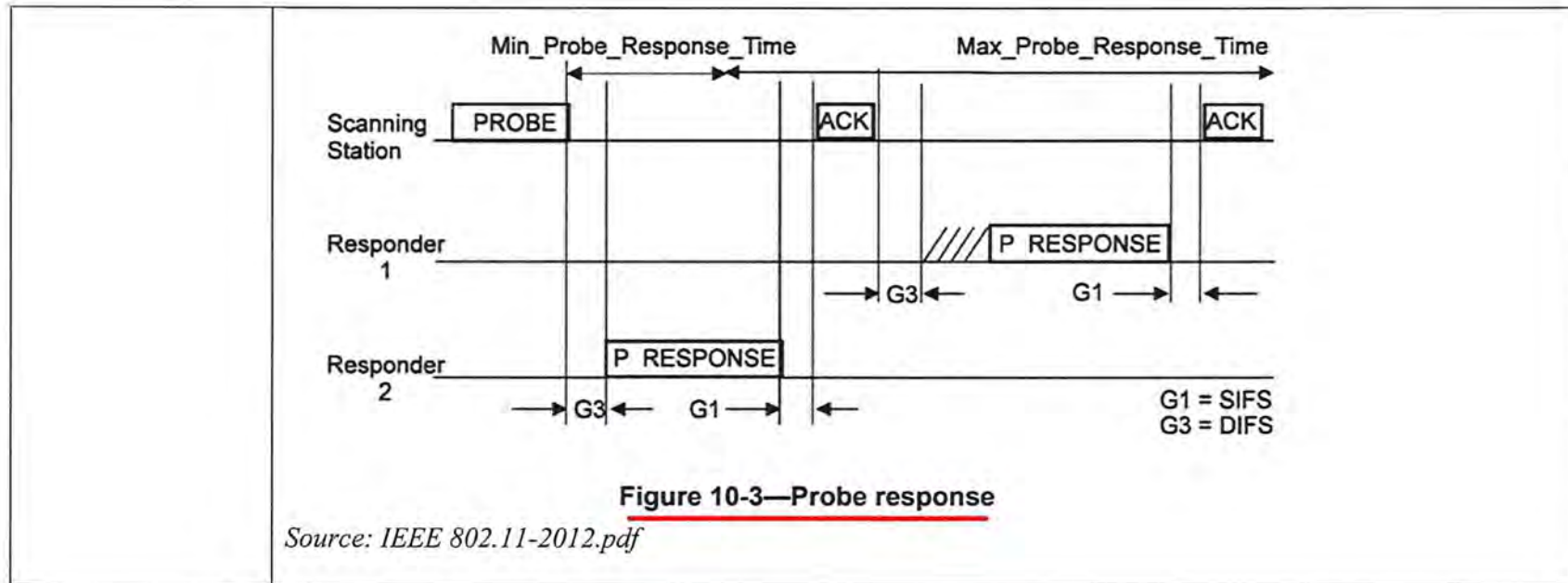


EXHIBIT A-INFRINGEMENT CONTENTIONS FOR U.S. PATENT NO. 10,694,384

Before answering the question, let us first understand what a preferred network list is. The PNL is a historical record of all the network names (SSIDs) that a device has previously connected to, and trusts to automatically connect to again in the future.

User devices trying to connect to a Wi-Fi network watch for access points (APs) broadcasting its availability for a device to connect to its network. Within that information contains the network name, or Service Set Identifier (SSID). Wi-Fi enabled devices trying to connect to a wireless network, and using Active Service Discovery, will then broadcast its interest in connecting to the AP if the network name is in its PNL, which increases the connection speed.

For instance, if you connect to a **Starbucks** Wi-Fi network once, your device will remember and try to automatically connect to any network with the SSID Starbucks. This is true whether you go to the same Starbucks in the future, or a Starbucks 1,000 miles away. All the user device knows is the network name; no additional data is stored. Auto-connecting to wireless networks in PNL saves time and is convenient for the user, but it is a security risk. Therefore, it is important to identify all networks in the PNL and stop connecting automatically to Wi-Fi to stay safe.

<https://blog.pulsarsecurity.com/preferred-network-list-pnl>

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

The screenshot displays a Wi-Fi probe response packet analysis. The packet is identified as '802.11 Management - Probe Response'. Key fields and their values are as follows:

- Probe Timestamp:** 23996945615 Microseconds [24-31]
- Beacon Interval:** 102 Time Units (104 Milliseconds, and 448 Microseconds) [32-33]
- Capability Info:** X0001000000000001
- SSID:** ID=0 SSID Len=4 SSID=OPEN
- Supported Rates:**
 - Element ID: 1 Supported Rates [42]
 - Length: 4 [43]
 - Supported Rate: 24.0 Mbps (BSS Basic Rate) [44]
 - Supported Rate: 36.0 Mbps (Not BSS Basic Rate) [45]
 - Supported Rate: 48.0 Mbps (Not BSS Basic Rate) [46]
 - Supported Rate: 54.0 Mbps (Not BSS Basic Rate) [47]
- Country:**
 - Element ID: 7 Country [48]
 - Length: 18 [49]
 - Country Code: AU [50-51]
 - Environment: 0x20 Any [52]
 - Starting Channel: 36 [53]
 - Number of Channels: 4 [54]
 - Max Tx Power (dBm): 23 [55]
 - Starting Channel: 52 [56]
 - Number of Channels: 4 [57]
 - Max Tx Power (dBm): 23 [58]
 - Starting Channel: 100 [59]
 - Number of Channels: 5 [60]
 - Max Tx Power (dBm): 30 [61]
 - Starting Channel: 132 [62]
 - Number of Channels: 3 [63]
 - Max Tx Power (dBm): 30 [64]
 - Starting Channel: 149 [65]
 - Number of Channels: 5 [66]
 - Max Tx Power (dBm): 30 [67]
- OBSS Load:**
 - Element ID: 11 OBSS Load [68]
 - Length: 5 [69]
 - Station Count: 1 [70-71]
 - Channel Utilization: 0 % [72]
 - Avail Admission Capacity: 26562 [73-74]
- HT Cap:** ID=45 HT Cap Len=26

Red annotations highlight specific information:

- A box around the SSID field is labeled 'information regarding access point'.
- A box around the Supported Rates field is labeled 'information regarding access point'.
- A box around the Country field is labeled 'information regarding access point'.
- A box around the OBSS Load field is labeled 'probe response'.

<https://mrcciew.com/2014/10/27/cwap-802-11-probe-requestresponse/>

An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.

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

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.

Each Accused Product is a cell phone, personal data assistant (PDA), personal media player device, wireless web-watch device, personal headset device, application specific device, or hybrid device.

Each Accused Products is a cell phone, tablet, or smartwatch.

The screenshot displays the Samsung website's product page for the Galaxy S23. At the top, the Samsung logo is enclosed in a red rectangular box. Navigation links such as 'Shop', 'Mobile', 'TV & Audio', 'Appliances', 'Computing', 'Displays', 'Accessories', and 'SmartThings' are visible. The product title 'Galaxy S23' is underlined. Below the title, there are promotional banners and a 'Continue' button. The main image shows two smartphones; the back of the white one is highlighted with a red box. To the right, under the 'Device' heading, 'Galaxy S23' is selected and enclosed in a blue box, with a price of \$799.99. Below it, 'Galaxy S23+' is listed with a price of \$999.99. The 'Connectivity' section is partially visible at the bottom.

<https://www.samsung.com/us/smartphones/galaxy-s23/buy/galaxy-s23-128gb-unlocked-sm-s911ulixaa/>

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

Meet our Galaxy tablets



Galaxy Tab S9 Series
Stunning screens, durability and power.
From \$799.99
[Buy now](#)
[Learn more](#)



Galaxy Tab S9 FE Series
The new standard of tablet essentials.
From \$349.99 ~~\$449.99~~
[Buy now](#)
[Learn more](#)



Galaxy Tab S6 Lite
Reliable power at the right price.
From \$299.99 ~~\$429.99~~
[Buy now](#)
[Learn more](#)



Galaxy Tab A9+
Level up family fun at an incredible value.
From \$219.99 ~~\$269.99~~
[Buy now](#)
[Learn more](#)

<https://www.samsung.com/us/tablets/>



Galaxy Watch6
Start your everyday wellness journey with personalized heart rate zone workouts² and insights for better rest with Advanced Sleep Coaching.^{3,4}
[Learn more](#) [Buy now](#)

<https://www.samsung.com/us/watches/>

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

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.

The Accused Products use information in the probe request that 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.

The Accused Products generate a fake MAC address by generating a randomized MAC address for use in probe requests. This fake MAC address is insufficient to identify the original MAC address of the hardware such that user privacy is increased (e.g., prevents disclosure of present location information.)

Persistent randomization

Android uses the persistent randomization type by default when the MAC randomization feature is enabled. Android generates a persistent randomized MAC address based on the parameters of the network profile including SSID, security type, or FQDN (for Passpoint networks). This MAC address remains the same until factory reset. The MAC address does not get re-randomized if the user forgets and re-adds the Wi-Fi network since the MAC address depends on the parameters of the network profile.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

MAC Randomization Behavior

The MAC randomization feature allows devices to use a randomized MAC address when connecting to a Wi-Fi network. For implementation instructions, see [Implementing MAC Randomization](#). This page describes the behavior of MAC randomization in Android.

MAC addresses are used by devices when connecting to a Wi-Fi network or an access point. Because these MAC addresses are transmitted without encryption, they can be captured and used to potentially track a user's location. Historically, devices use the factory MAC address to associate to a Wi-Fi network. The factory MAC address is globally unique and static, allowing the device to be tracked and individually identified.

The MAC randomization feature increases user privacy by using a randomized MAC address when connecting to a Wi-Fi network.

MAC addresses are 48 bits long and usually represented by 12 hex digits (6 octets as each octet is 8 bits) such as 00:11:22:AA:BB:CC. The MAC randomization feature randomizes the address by setting the locally administered bit to 1, and the unicast bit to 0. The other 46 bits are randomized.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

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

For devices running Android 10 or higher, the framework uses randomized MAC address by default. Users can enable or disable MAC randomization for individual networks through an option in the **Network details** screen in **Settings**, as shown in Figure 1. If a user disables MAC randomization for a network, the framework uses the factory MAC address (globally unique address).

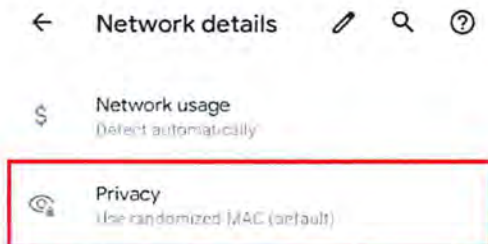


Figure 1. MAC randomization option.

<https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior>

MAC Randomization is implemented in devices running the Android OS since at least Android OS 10 as well as Wear OS 3.0.

In Android 10, MAC randomization is enabled by default for client mode, SoftAp, and Wi-Fi Direct.

MAC randomization prevents listeners from using MAC addresses to build a history of device activity, thus increasing user privacy.

Additionally, MAC addresses are randomized as part of [Wi-Fi Aware](#) and [Wi-Fi RTT](#) operations.

For more information, see [MAC Randomization Behavior](#).

<https://source.android.com/docs/core/connect/wifi-mac-randomization>

Wear OS, including Wear OS 3.0, is based on Android.

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

See <https://developer.android.com/training/wearables/wear-v-mobile#:~:text=Wear%20OS%20is%20based%20on.design%20a%20Wear%20OS%20app>.

Devices operating on Wear OS 3.0 implement MAC randomization.

See https://www.reddit.com/r/GalaxyWatch/comments/pcmki1/galaxy_watch_4_wifi_mac_address/

An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.