IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

SECURE WI-FI LLC, Plaintiff, v. SAMSUNG ELECTRONICS CO. LTD. and SAMSUNG ELECTRONICS AMERICA, INC., Defendants.	Civil Action No.: 2:24-cv-00047 **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Secure Wi-Fi LLC ("Plaintiff" or "Secure Wi-Fi"), through its attorneys, for its Complaint against Samsung Electronics Co. Ltd. ("SEC") and Samsung Electronics America, Inc., ("SEA") (collectively, "Defendants" or "Samsung"), demands a trial by jury and alleges as follows:

INTRODUCTION

1. This Complaint arises from Samsung's unlawful infringement of the following United States Patents owned by Secure Wi-Fi: United States Patent Nos. 10,694,384, 9,961,552, and 9,717,005 (collectively the "Asserted Patents").

THE PARTIES

2. Secure Wi-Fi is a Texas limited liability company with its principal place of business located at 5900 Balcones Drive, Suite 100, Austin, Texas 78731. Secure Wi-Fi is the sole owner by assignment of all right, title and interest in the Asserted Patents, including the right to recover for past, present and future infringement and damages.

3. On information and belief, Defendant Samsung Electronics Co., Ltd. is a foreign corporation organized and existing under the laws of the Republic of Korea. SEC has a principal place of business located at 129 Samsung-ro, Yeongtong-Gu, Suwon-Si, Gyeonggi-Do, 443-742, Republic of Korea. Samsung Electronics Co., Ltd. may be served at least by process under the Hague Convention.

4. On information and belief, Samsung Electronics Co., Ltd.'s DX division is responsible for the design, manufacture, and sale of mobile devices, such as smartphones, and related software, applications, and services that operate on cellular networks around the world and in the United States.

5. On information and belief, Defendant Samsung Electronics America, Inc. is a wholly owned subsidiary corporation of Samsung Electronics Co., Ltd. and is organized and existing under the laws of New York with a principal place of business at 85 Challenger Road, Ridgefield Park, New Jersey 07660 and offices and/or other facilities in Texas at least at 6625 Excellence Way, Plano, Texas 75023 and 12100 Samsung Boulevard, Austin, Texas 78754.

6. Samsung Electronics America, Inc. is registered to do business in Texas and has maintained regular and established places of business with offices and/or other facilities in this District at least at 6625 Excellence Way Plano, Texas 75023 and 1301 E. Lookout Drive, Richardson, Texas 75082. Samsung Electronics America, Inc. may be served through its registered agent for service of process, CT Corporation System, 1999 Bryan St., Suite. 900, Dallas, Texas 75201.

7. On information and belief, Defendant Samsung Electronics America, Inc. oversees domestic sales and distribution of Samsung's consumer electronics products, including the products accused of infringement in this case.

8. Defendants Samsung Electronics Co., Ltd., and Samsung Electronics America, Inc., have acted in concert with respect to the facts alleged herein such that any act of Samsung Electronics Co., Ltd., is attributable to Samsung Electronics America, Inc., and vice versa.

JURISDICTION AND VENUE

9. This action arises under the patent laws of the United States, Title 35 of the United States Code. Subject matter jurisdiction is proper in this Court pursuant to 28 U.S.C. §§ 1331 and 1338(a).

10. This Court has personal jurisdiction over Defendants in this action because each has committed and continues to commit acts within this District giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over each would not offend traditional notions of fair play and substantial justice. Defendants, directly and through subsidiaries or intermediaries, have committed and continue to commit acts of infringement in this District, by among other things, making, using, importing, offering to sell and selling smartphones that include the Android 10 operating system and/or later Android operating system versions that infringe the Asserted Patents. Defendants have not contested personal jurisdiction in this Court in prior actions.

11. On information and belief, Defendants have each derived substantial revenue from infringing acts in the Eastern District of Texas, including from the sale of infringing products.

12. Venue is proper in this District pursuant to at least 28 U.S.C. §1391 and §1400(b). Upon information and belief, SEA has a regular and established place of business in this District, including at 625 Excellence Way, Plano, Texas 75023, and Defendants have committed acts of infringement in this district.

13. Samsung Electronics, Co. Ltd., is not a resident of the United States and may be sued in this District because suits against foreign entities are proper in any judicial district where they are subject to personal jurisdiction.

FIRST COUNT

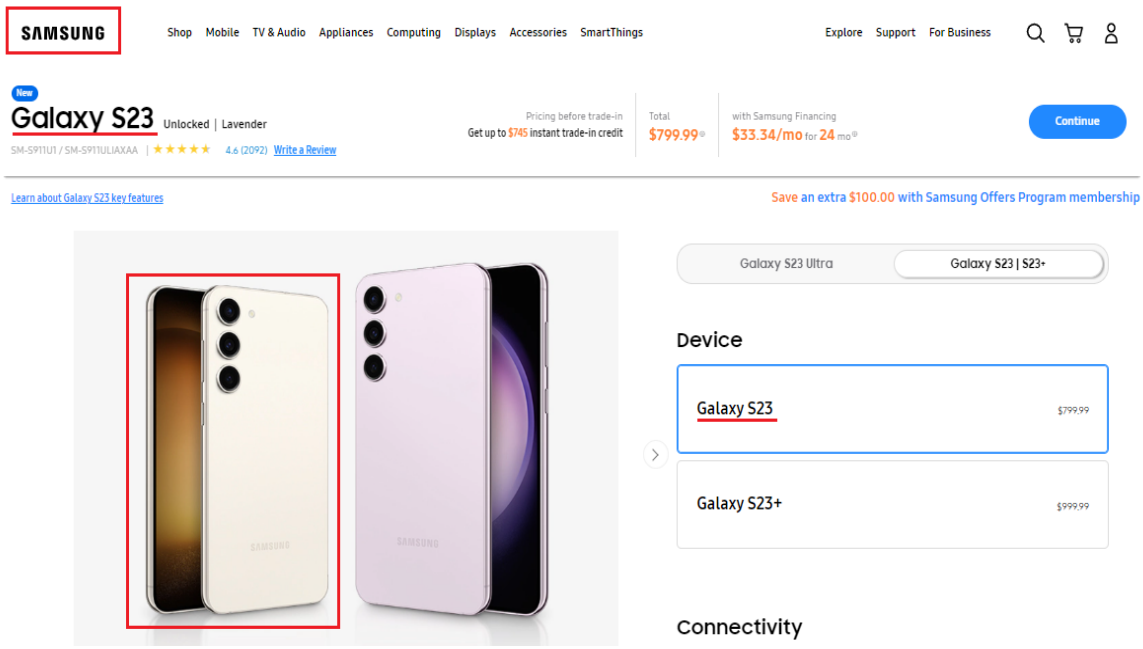
(INFRINGEMENT OF U.S. PATENT NO. 10,694,384)

14. Secure Wi-Fi incorporates by reference the foregoing paragraphs as if fully set forth herein.

15. Secure Wi-Fi owns by assignment, all rights, title and interest, including the right to recover damages for past, present and future infringement, in U.S. Patent No. 10,694,384 titled "Schemes for Connecting to Wireless Network." The '384 patent was duly and legally issued by the United States Patent and Trademark Office on June 23, 2020. A true and correct copy of the '384 Patent is attached as Exhibit A.

16. On information and belief, Defendants have directly infringed and continue to directly infringe one or more claims of the '384 patent, including at least claim 17 of the '384 patent, in the state of Texas, in this judicial district, and elsewhere in the United States by, among other things, making, using, selling, offering for sale, and/or importing into the United States products that embody one or more of the inventions claimed in the '384 patent, including but not limited to the Accused Instrumentalities, including Samsung Galaxy smartphones that include the Android 10 operating system or later versions of the Android operating system as well as all reasonably similar products, in violation of 35 U.S.C. § 271(a). By way of example, the Accused Instrumentalities are an end device, such as the Galaxy S23 smartphone that includes the Android 13 operating system with randomized MAC for Wi-Fi connections.

17. The '384 Accused Instrumentalities satisfy all claim limitations of one or more claims of the '384 patent, including exemplary claim 17. The Accused Instrumentalities are end devices. The Galaxy S23, for example, is an end device having a "Snapdragon 8 Gen 2" chipset. The Galaxy S23 also includes the Android 13 operating system.



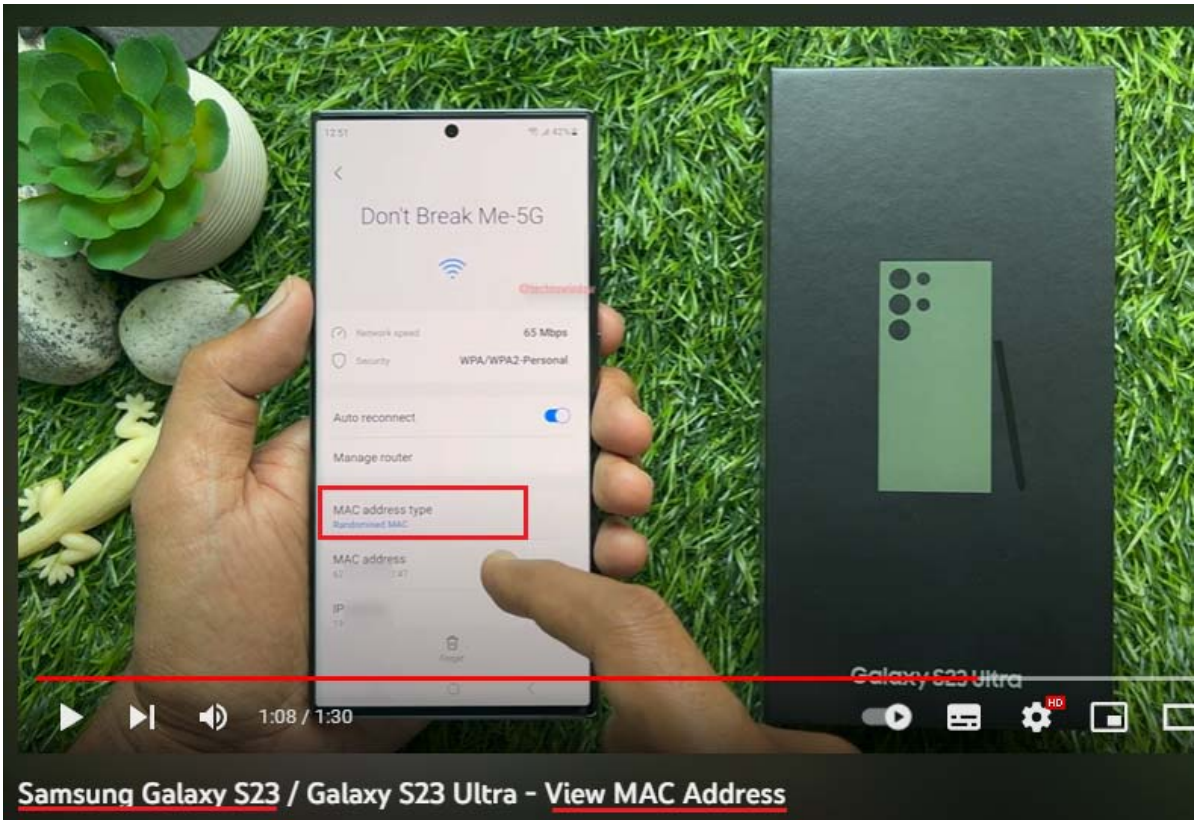
https://www.samsung.com/us/smartphones/galaxy-s23/buy/galaxy-s23-128gb-unlocked-sm-s911uliaxaa/

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

Phone	Galaxy S23	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	Android 13 / One UI 5.1	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



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

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

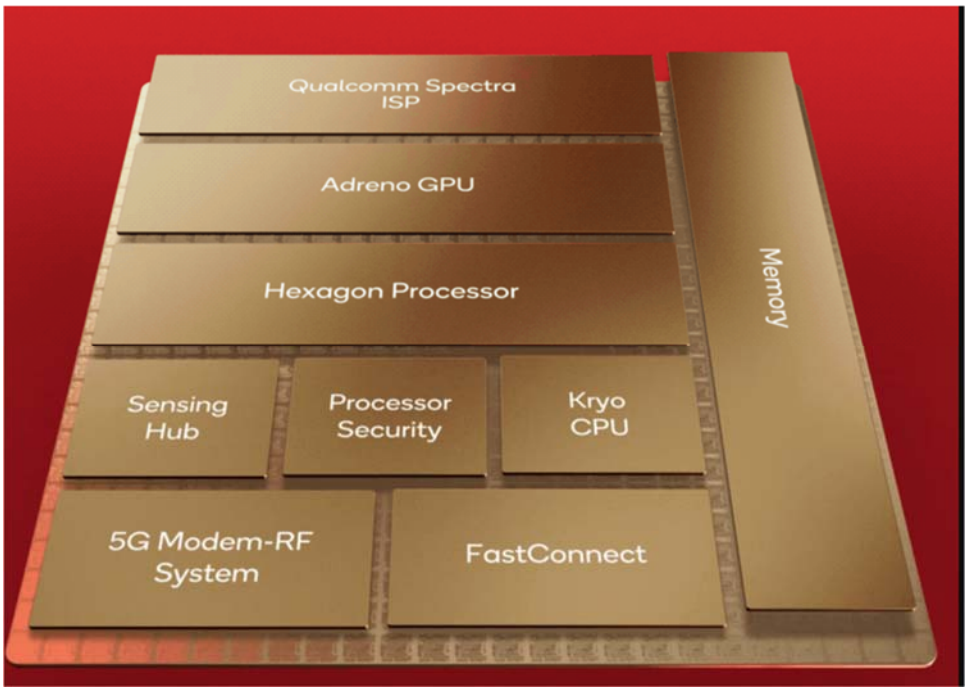
- The Samsung Galaxy S23 series features Qualcomm Technologies' leading connectivity solutions, including the Snapdragon® X70 Modem-RF System, the world's fastest and smartest 5G modem-RF system, and Qualcomm® FastConnect™ for high-speed and ultra-low latency Wi-Fi, and the latest Bluetooth audio enhancements.

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

18. The Accused Instrumentalities have a hardware network interface associated with an actual media control (MAC) address. For example, the Galaxy S23 includes the SnapDragon 8 Gen 2 SOC's Wi-Fi interface called FastConnect. FastConnect is used to connect to Wi-Fi networks.

Phone	Galaxy S23	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	Android 13 / One UI 5.1	Android 13 / One UI 5.1	Android 13 / One UI 5.1

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



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

Phone	Galaxy S23	Galaxy S23+	Galaxy S23 Ultra
Connectivity	5G, Wi-Fi 6E, 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/

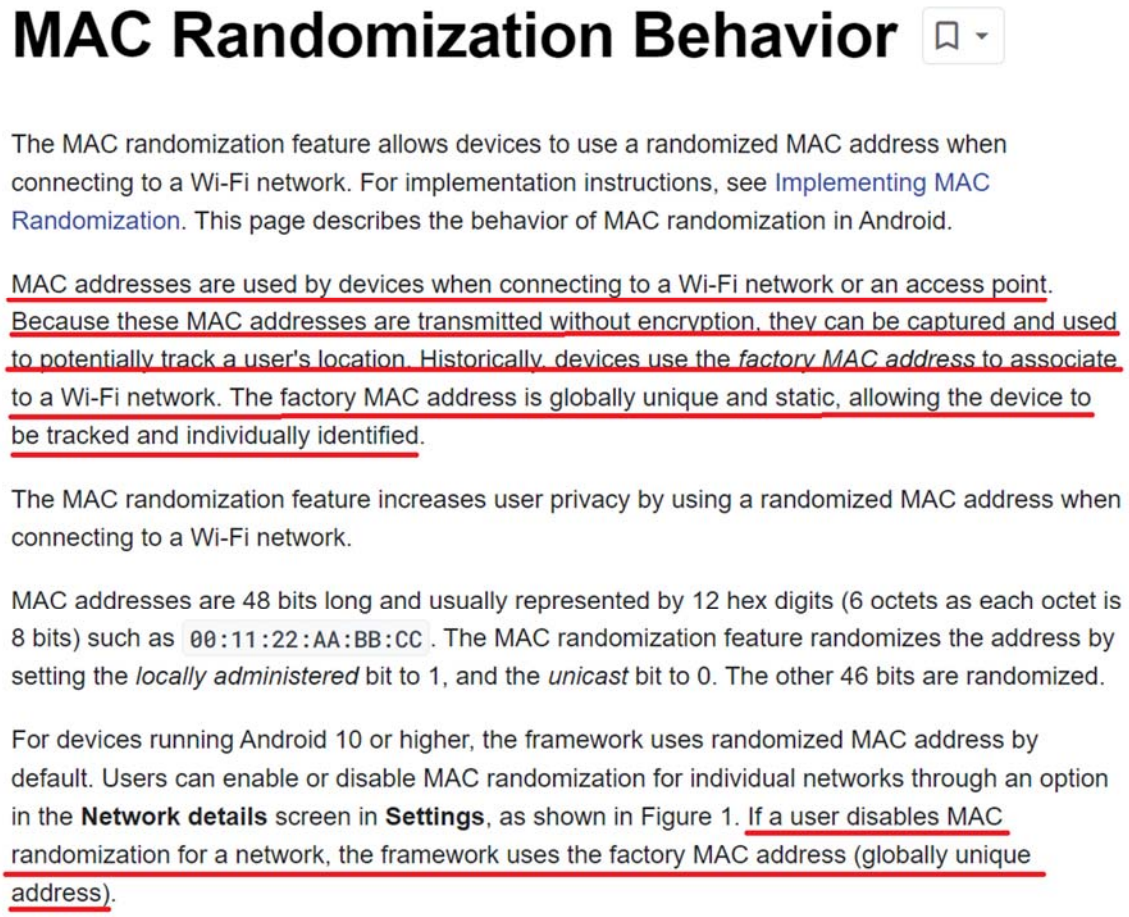
Connectivity: The Galaxy S23 series boasts unparalleled Snapdragon Connect technologies across 5G, Wi-Fi, and Bluetooth®. Featuring the multiple-award-winning Snapdragon X70 5G Modem-RF System with the Qualcomm® 5G AI Processor, the Galaxy S23 series harnesses the power of AI to enable breakthrough 5G coverage, power efficiency, speeds, and latency. These new devices also support 5G+5G/4G Dual-SIM Dual-Active[3], 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.qualcomm.com/content/dam/qcomm-martech/dm-assets/images/products/by-technology/wi-fi/Qualcomm-FastConnect-7800-Overview-Infographic.png

19. The hardware network interface of the Accused Instrumentalities is associated with an actual media control (MAC) address, e.g., a factory-set MAC address. The hardware network

interface of the Accused Instrumentalities is associated with a factory-set MAC address that is globally unique and static, allowing the Accused Instrumentality 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.

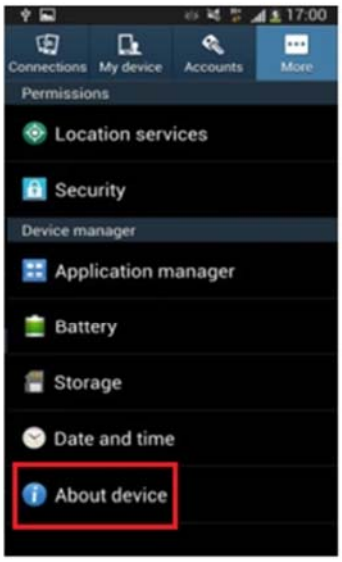
The MAC randomization feature increases user privacy by using a randomized MAC address when connecting to a Wi-Fi network.

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

20. The Accused Instrumentalities include a "Wi-Fi MAC address." The Wi-Fi MAC address is an example of an actual MAC address.



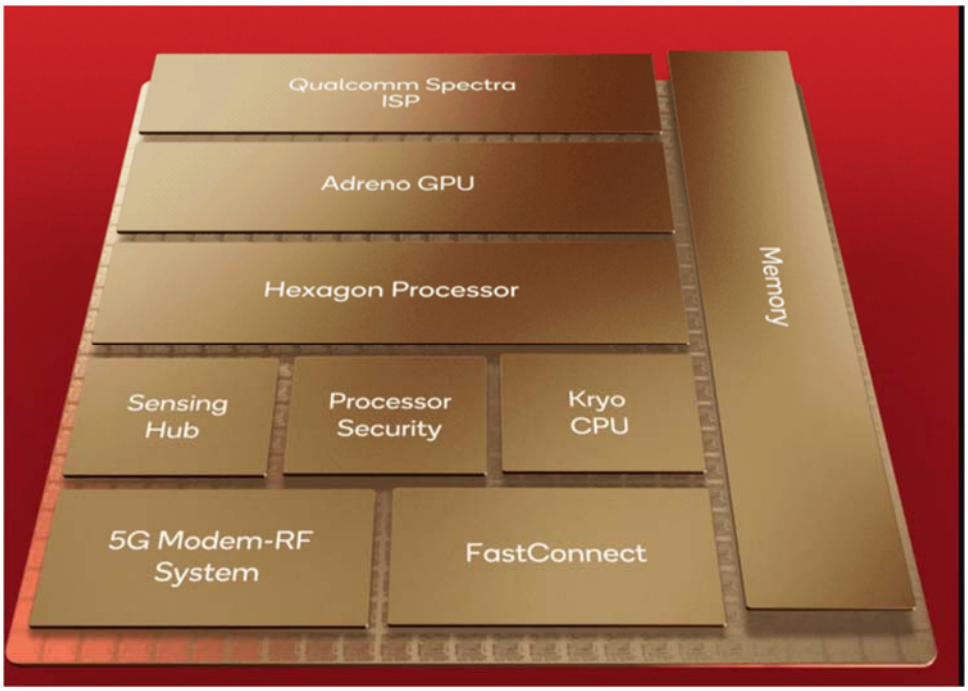
4 Touch Status and then scroll down to read your device's Wi-Fi MAC address.

https://www.samsung.com/hk_en/support/mobile-devices/where-do-i-find-the-wifi-mac-address-in-my-samsung-galaxy-note-10-1-or-8-0/

21. The Accused Instrumentalities include 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. As an example, the Accused Instrumentalities include a processor for executing functionality of the Android operating system to generate a randomized MAC address for the end device that is distinct from the factory-set MAC address. By way of example, the Galaxy 23 includes the Android 13 operating system, portions of which, when executed by a processor, generate randomized MAC addresses for Wi-Fi connections. The processor is coupled to the hardware network interface for, e.g., performing Wi-Fi connections and transmitting information between an access point and the processor.

Phone	Galaxy S23	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	Android 13 / One UI 5.1	Android 13 / One UI 5.1	Android 13 / One UI 5.1

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



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

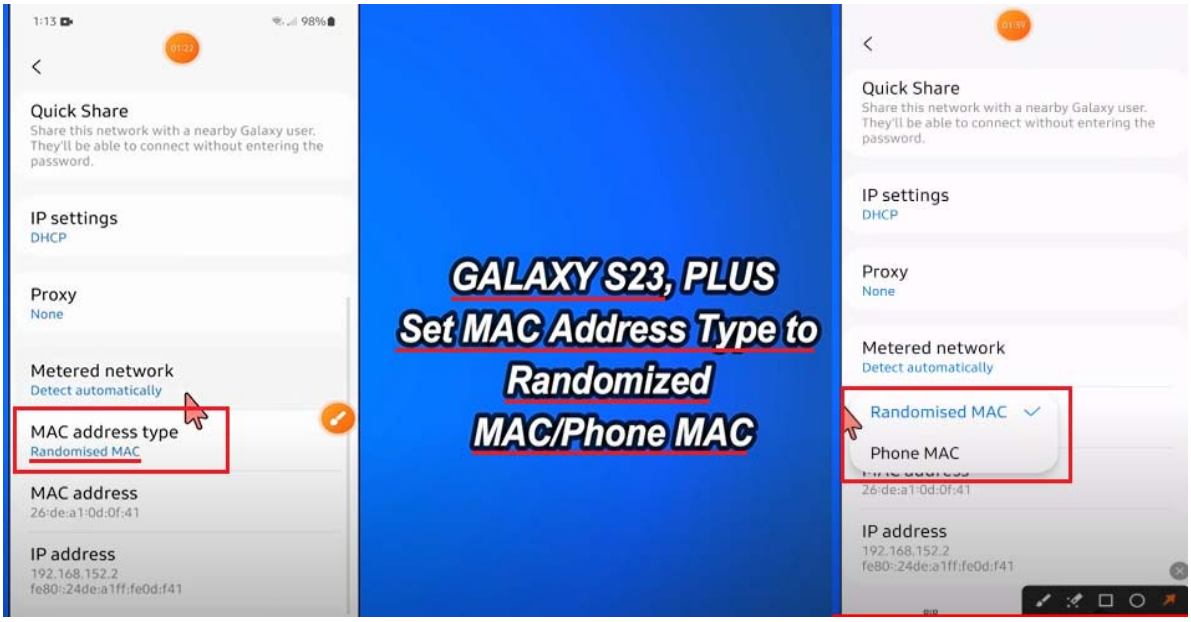
Phone	Galaxy S23	Galaxy S23+	Galaxy S23 Ultra
Connectivity	5G, Wi-Fi 6E, Bluetooth 5.3, NFC	5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband	5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband

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

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[3], 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.qualcomm.com/content/dam/qcomm-martech/dm-assets/images/products/by-technology/wi-fi/Qualcomm-FastConnect-7800-Overview-Infographic.png



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

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 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).

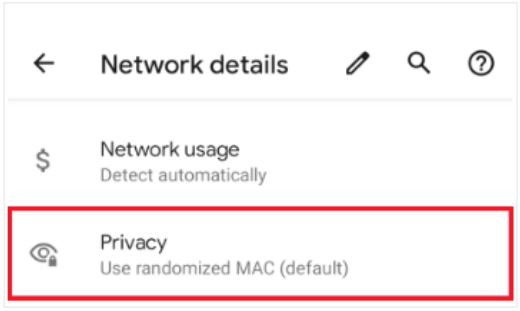


Figure 1. MAC randomization option.

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

22. The Accused Instrumentalities contain a transmitter coupled to the processor that is operable to transmit, by the end device (e.g., the Accused Instrumentality) to an access point (e.g., a Wi-Fi access point), a probe request that includes the generated MAC address (e.g., a randomized MAC address).

23. The Accused Instrumentalities, including the Galaxy S23, are configured to connect to Wi-Fi access points. The Accused Instrumentalities include a transmitter for connecting to Wi-Fi access points.

24. The Accused Instrumentalities support the Wi-Fi standard. According to the standard, a UE (e.g., the Accused Instrumentality) inquires about available Wi-Fi access points using a probe request, which is sent via a transmitter. The probe request comprises a sender address field (e.g., a device identifier). The UE (e.g., the Accused Instrumentality) utilizes a random MAC address as the sender address in a probe request. The Accused Instrumentalities receive probe responses from available access points via the FastConnect network interface. The Accused Instrumentalities select a desired access point for connection based on, for example, the access point capabilities or desired network condition.

25. The Accused Instrumentalities, in accordance with the Wi-Fi standard, transmit probe requests to identify available access points.

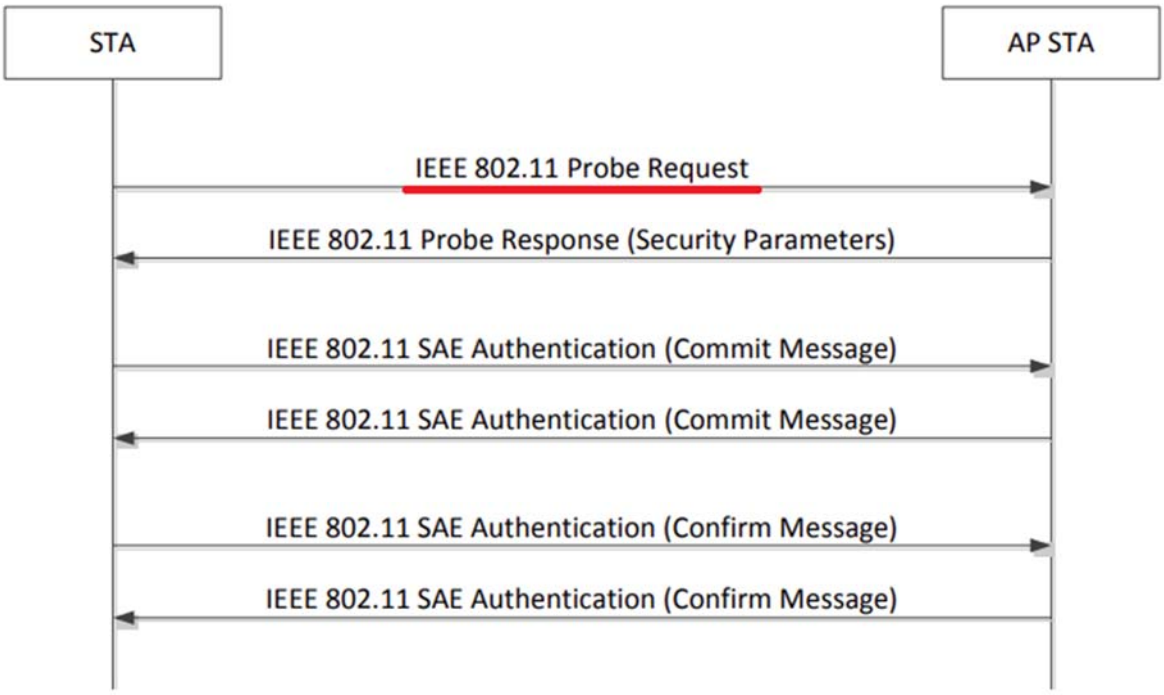
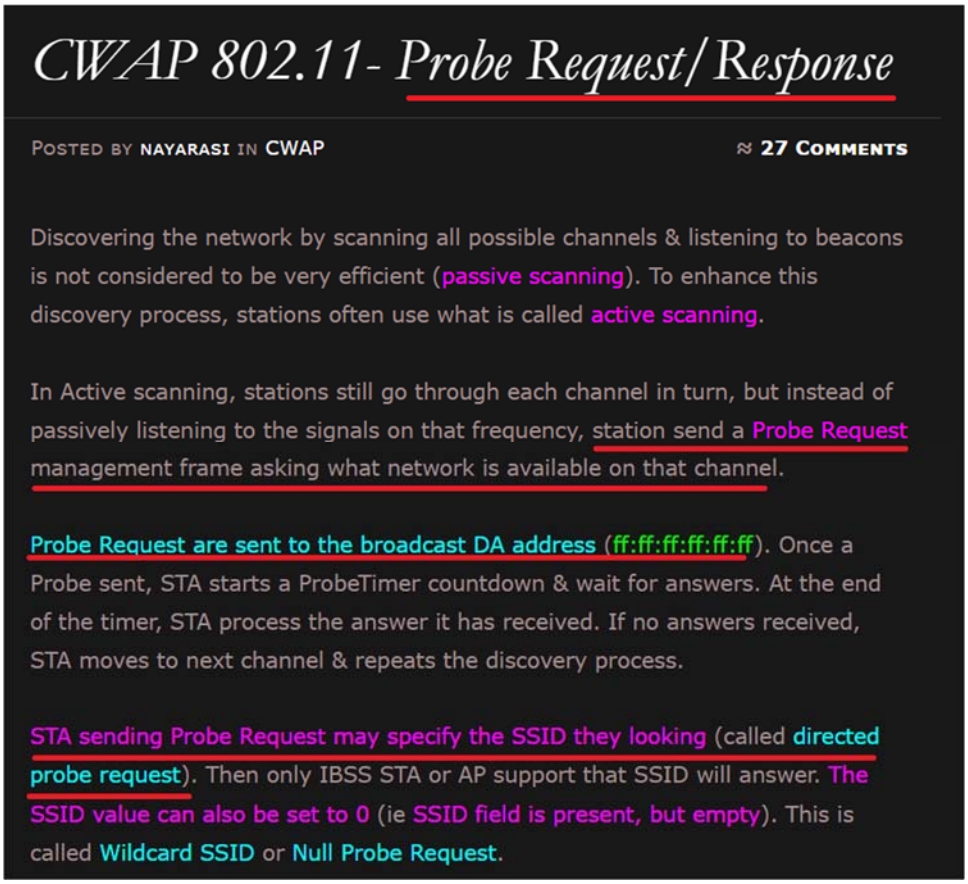


Figure 4-21—Example using SAE Authentication

Source: IEEE 802.11-2012.pdf at p. 87.
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://mrncciew.com/2014/10/27/cwap-802-11-probe-requestresponse/

26. The Accused Instrumentalities transmit a Wi-Fi probe request to an access point, which includes the Accused Instrumentality'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

27. The Wi-Fi probe request transmitted by the Accused Instrumentalities includes the generated 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).

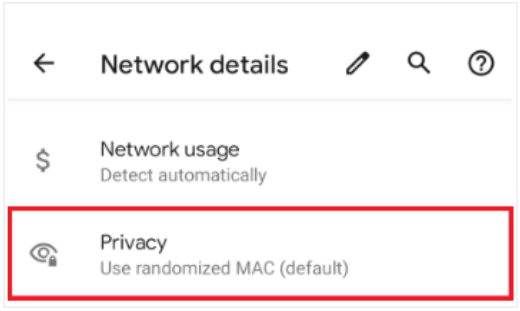


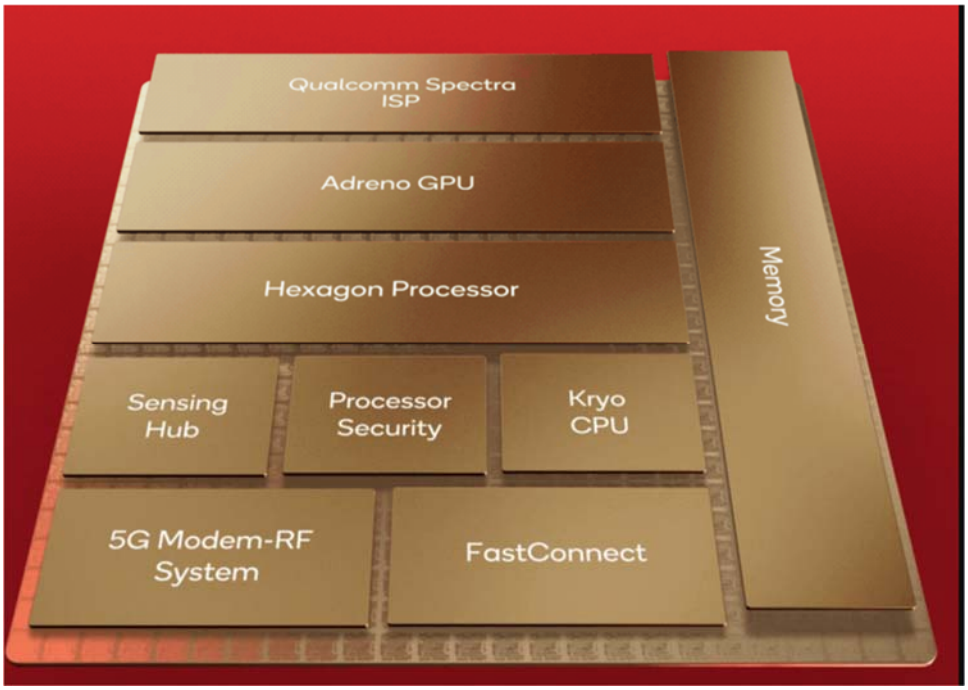
Figure 1. MAC randomization option.

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

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

28. The processor in the Accused Instrumentalities is coupled to the FastConnect network interface which includes the capability to transmit probe requests.

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



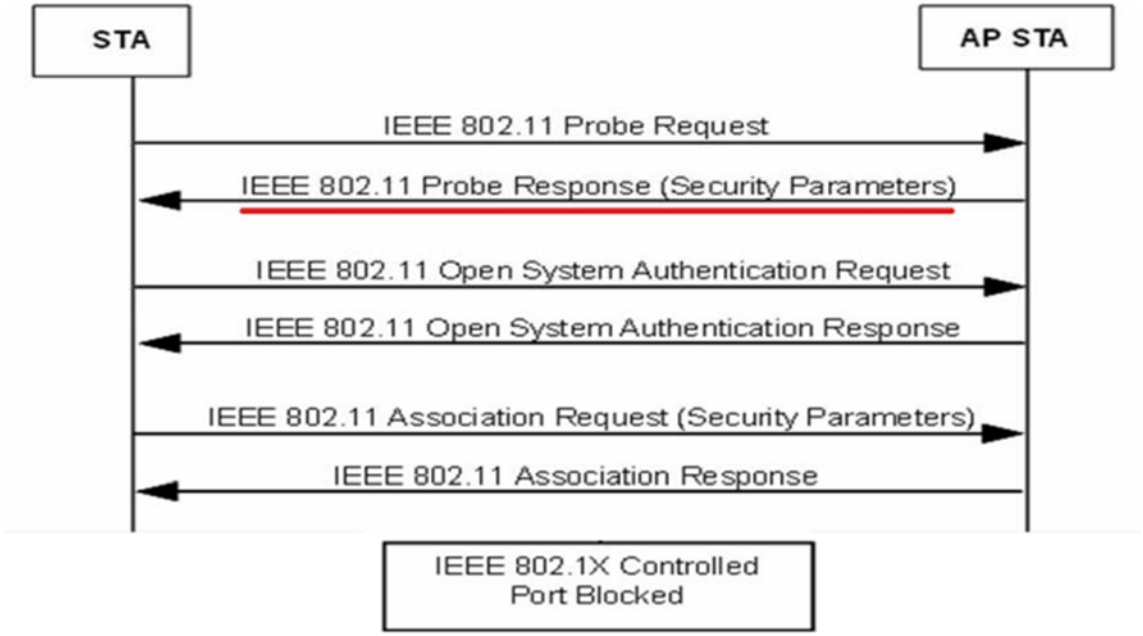
https://www.qualcomm.com/news/onq/2022/11/new-snapdragon-8-gen-2-8-extraordinary-mobile-experiences-unveiled

29. The Accused Instrumentalities contain a receiver coupled to the processor that is operable to 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 or supported data rates).

30. The Accused Instrumentalities support the Wi-Fi standard. The Accused Instrumentalities are configured to receive Wi-Fi probe responses from multiple available access points, e.g., via the FastConnect network interface. By way of example, a receiver of the Accused Instrumentalities is configured to receive a probe response from an access point 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. A Wi-Fi probe response includes, for example, the SSID (wireless network name) and/or supported data rates 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



Source: IEEE 802.11-2012.pdf at p. 84

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 dot11QosOption-Implemented 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/

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

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 dot11MgmtOptionUTCTSFOffsetActivated is true.
43	Time Zone	The Time Zone element is present if dot11MgmtOptionUTCTSFOffsetActivated 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/

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 at p. 59.

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 at p. 979.

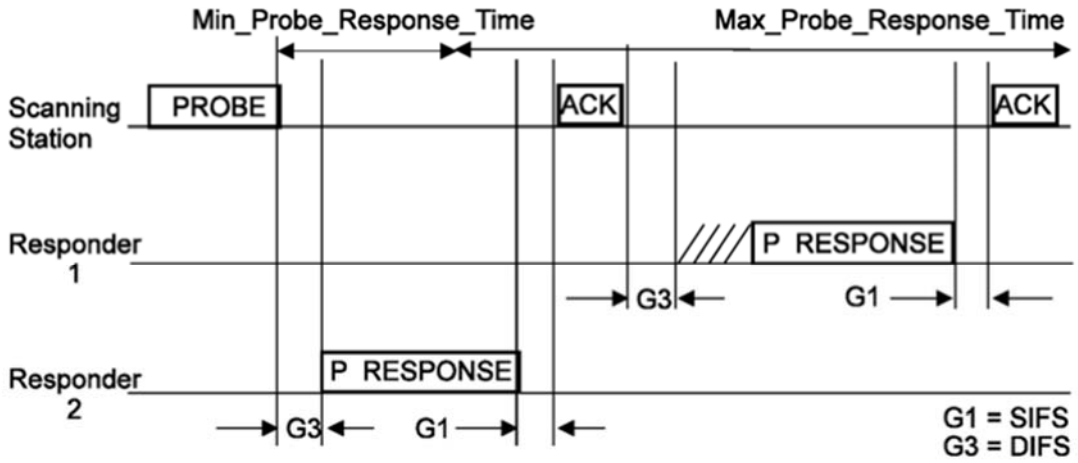
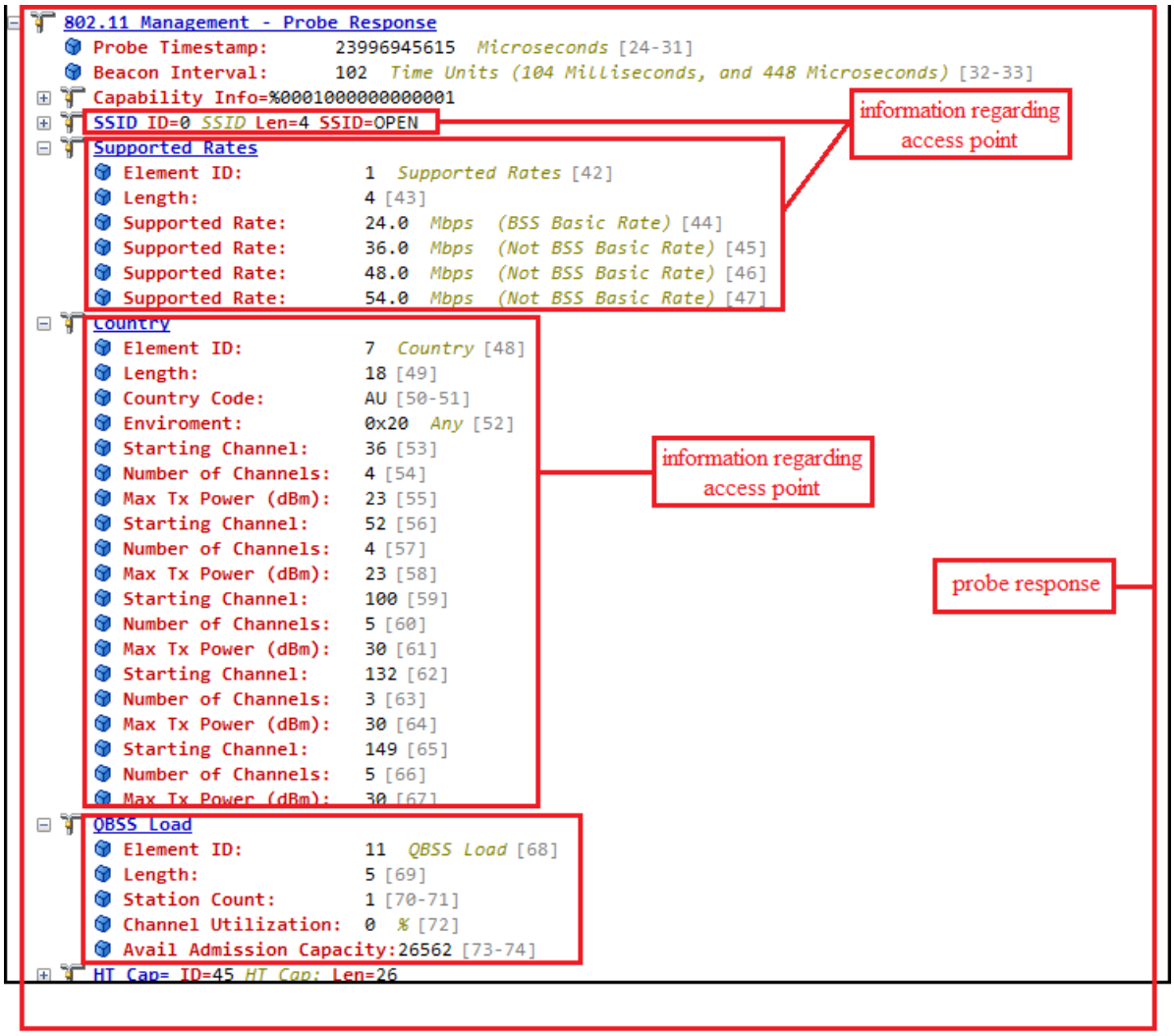


Figure 10-3—Probe response

Source: IEEE 802.11-2012.pdf at p. 980.

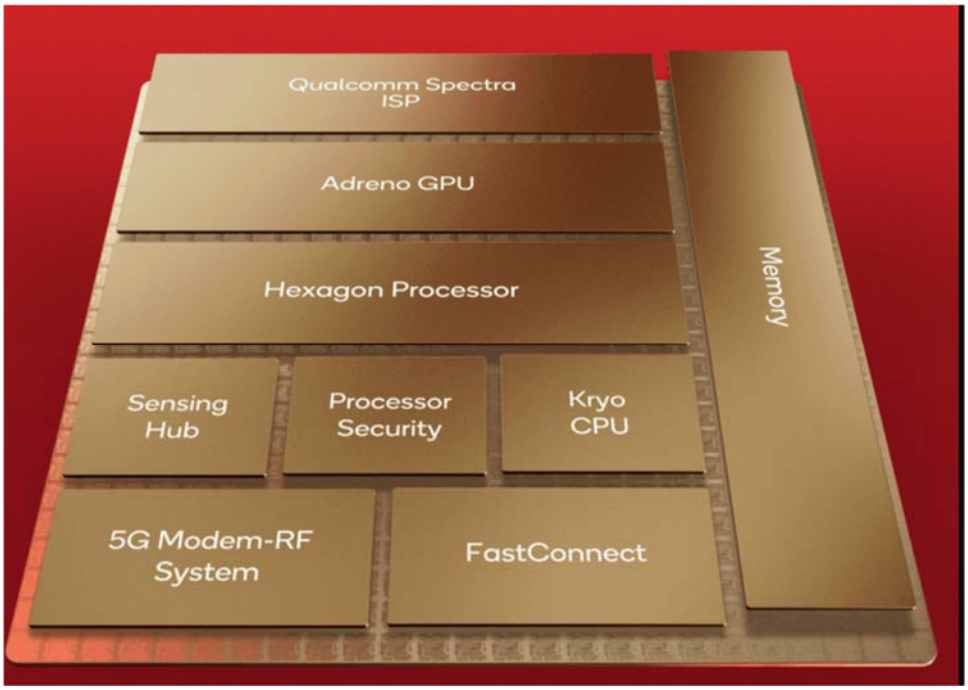
https://blog.pulsarsecurity.com/preferred-network-list-pnl
https://www.wi-fi.org/knowledge-center/faq/what-are-passive-and-active-scanning



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

31. The processor in the Accused Instrumentalities is coupled to the FastConnect network interface which includes the capability to receive probe responses.

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

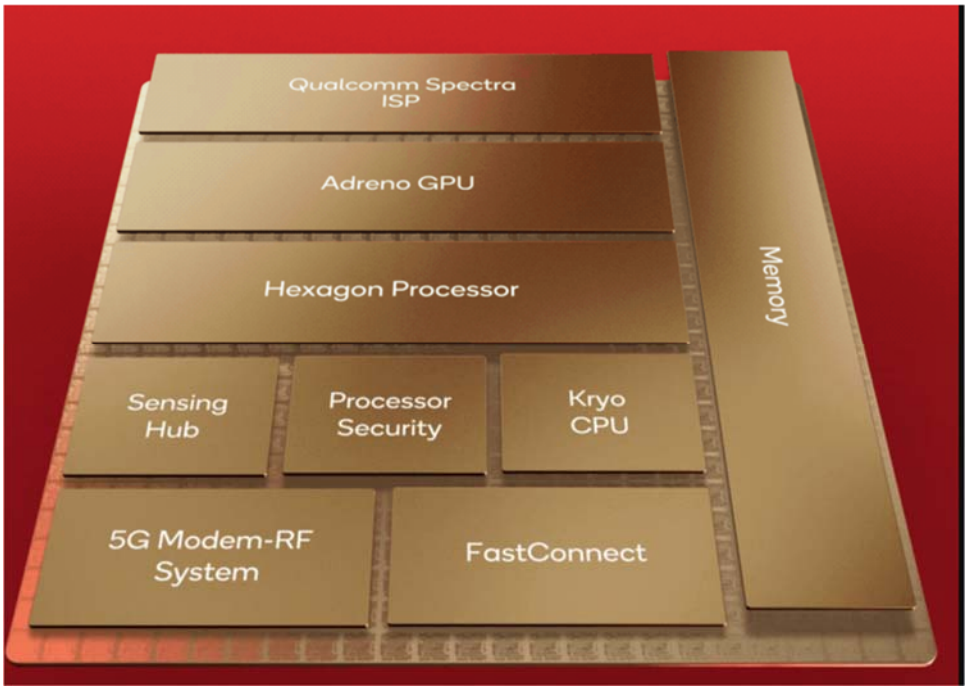


https://www.qualcomm.com/news/onq/2022/11/new-snapdragon-8-gen-2-8-extraordinary-mobile-experiences-unveiled

32. The processor in the Accused Instrumentalities is operable to 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) based, at least in part, on the information (e.g., SSID, supported data rates, etc.) in the probe response being indicative that the access point (e.g., a Wi-Fi access point) was connected with the end device (e.g., the Accused Instrumentality) previous to when the access point received the probe request transmitted by the transmitter of the Accused Instrumentality. The Galaxy S23, for example, contains a processor executing functionality of the Android operating system to perform the determination.

Phone	Galaxy S23	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	Android 13 / One UI 5.1	Android 13 / One UI 5.1	Android 13 / One UI 5.1

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



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

Phone	Galaxy S23	Galaxy S23+	Galaxy S23 Ultra
Connectivity	5G, Wi-Fi 6E, 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/

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[3], 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

33. The processor of the Accused Instrumentalities is configured to confirm the received SSID information from the probe responses with information related to previously-connected access points. Once confirmed that there is a SSID in a probe response from an access point with which the Accused Instrumentality was connected previously, the Accused Instrumentality initiates an authentication process with the stored pre-shared key information and the previously used authenticated MAC address (e.g., the persistent MAC address used for prior connections with the access point). For example, the Accused Instrumentality utilizes persistent randomization, in which for the same Wi-Fi network and device combination, the MAC address remains the same. When an Accused Instrumentality connects to a Wi-Fi network to which it was previously connected, it will use the same MAC address.

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 addressed 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: 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="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

34. The hardware network interface (e.g., the FastConnect hardware network interface and related components) of the Accused Instrumentalities is operable to connect, in response to determining that the access point is the authenticated access point (e.g., a previously connected Wi-Fi access point, as discussed previously), the end device to a wireless local area network provided by the access point (e.g., a Wi-Fi access point) is the authenticated access point.

Phone	Galaxy S23	Galaxy S23+	Galaxy S23 Ultra
Connectivity	5G, Wi-Fi 6E, 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/

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[3], 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.qualcomm.com/content/dam/qcomm-martech/dm-assets/images/products/by-technology/wi-fi/Qualcomm-FastConnect-7800-Overview-Infographic.png

35. The Accused Instrumentalities support the Wi-Fi standard. According to the standard, the Accused Instrumentalities are configured to inquire about available Wi-Fi access points using a probe request. The probe request comprises an SSID list or preferred network list which is a set of SSIDs to which the Accused Instrumentalities were connected previously.

36. The Accused Instrumentalities are configured to receive probe responses from multiple available access points. By way of 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.

37. The Accused Instrumentalities confirm the received SSID information from the probe responses with the access point information stored in their memory. Once confirmed that there is a SSID in a probe response from an access point with which the Accused Instrumentality was connected previously, the Accused Instrumentality initiates an authentication process.

> **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 addressed 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

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.

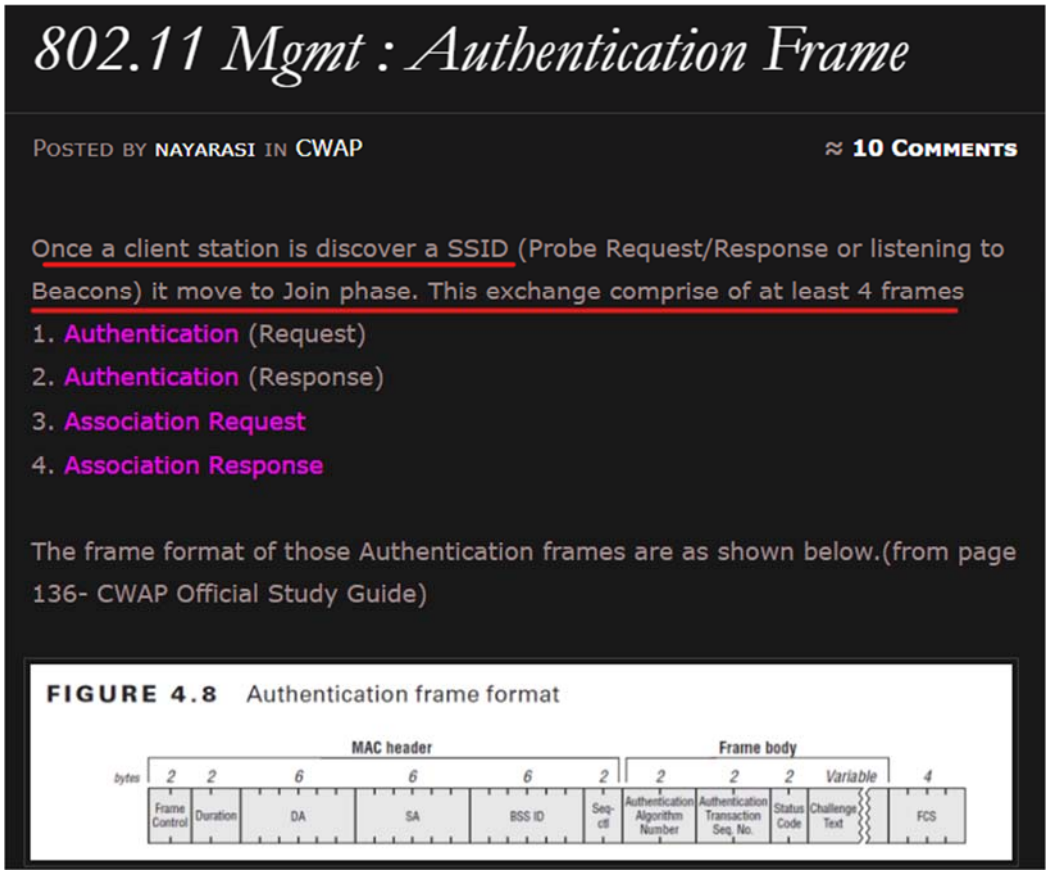
8.2.4.3.7 RA field

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 at p. 388.



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

38. As shown below, the Accused Instrumentalities utilize persistent randomization, in which for the same Wi-Fi network and device combination, the MAC address remains the same. When the Accused Instrumentality connects to a Wi-Fi network to which it was previously connected, it will use the same MAC address.

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 addressed 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: 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="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

39. By making, using, offering for sale, selling and/or importing into the United States the Accused Instrumentalities, Defendants have injured and continue to injure Secure W-Fi and are liable for infringement of the ’384 patent pursuant to 35 U.S.C. § 271(a).

40. In addition, and/or in the alternative to direct infringement, Defendants have also infringed and continue to infringe the claims of the ’384 patent by, among other things, actively inducing others to use the Accused Instrumentalities in violation of 35 U.S.C. § 271(b).

41. Samsung's users, customers, consumers, agents, distributors, and other third parties who use, sell, offer to sell, and/or import the Accused Instrumentalities in accordance with Samsung's instructions infringe the claims of the '384 patent, in violation of 35 U.S.C. § 271(a). Samsung intentionally instructs its customers to infringe through support information such as websites, videos, demonstrations, support information and other published information. For example, Samsung's website instructs and encourages its customers to use, manage and control the infringing components and functionalities of the Accused Instrumentalities. *See*, *e.g.*, https://www.samsung.com/us/smartphones/galaxy-s23/specs/ (advertising the Wi-Fi capabilities of Accused Instrumentalities); https://downloadcenter.samsung.com/content/UM/202302/20230207045923682/SAM_S911_S916_S918_EN_UM_OS13_020223_FINAL.pdf, at 3, 119 (advertising and instructing users to connect perform Wi-Fi connections); *id*. at 121-122 (advertising and instructing Wi-Fi connections); https://www.samsung.com/my/support/mobile-devices/how-to-connect-wi-fi-network-on-my-samsung-device/ ("How to connect to Wi-Fi network on my Samsung Device."); *id*. at 16 (encouraging users to "make full use of [their] device's Android features").

42. The Accused Instrumentalities implement infringing functionality by default when connecting to a Wi-Fi network. *See, e.g.*, https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior. The Accused Instrumentalities are designed and intended to perform MAC randomization for Wi-Fi connections and necessarily infringe the '384 patent in the normal, intended manner without any additional specific action of the end user other than connecting to a Wi-Fi network.

43. Thus, Samsung actively instructs and directs its customers to infringe and actively encourages infringement by its customers. Samsung is thereby liable for infringement of the '384 patent under 35 U.S.C. § 271(b).

44. At a minimum, Samsung has had knowledge of the '384 patent since at least the filing and/or service date of the Complaint in this action. Despite this knowledge, Samsung has continued to engage in activities to encourage and assist its customers, consumers, agents, distributors, and other third parties in the use, sale, offer for sale, and/or importation of the Accused Instrumentalities. Thus, on information and belief, Samsung (1) had actual knowledge of the patent; (2) knowingly induced its customers to infringe the patent; and (3) had specific intent to induce the patent infringement.

45. Additionally, and/or alternatively, Samsung is liable as a contributory infringer of the '384 patent under 35 U.S.C. § 271(c) by having offered to sell, sold and imported and continuing to offer to sell, selling, and importing into the United States the Accused Instrumentalities and reasonably similar products, to be especially made or adapted for use in infringement of the '384 patent. The portions of the Samsung Accused Instrumentalities that enable Wi-Fi connections of the Accused Instrumentalities utilizing MAC randomization constitute a material component for use in practicing the '384 patent and are especially made and are not staple articles of commerce suitable for non-infringing use.

46. Secure Wi-Fi has complied with 35 U.S.C. § 287 because Secure Wi-Fi does not make, offer for sale or sell products that practice the '384 patent during the relevant time period.

47. As a result of Samsung's direct and indirect infringement of the '384 patent, Secure Wi-Fi is entitled to monetary damages (past, present, and future) in an amount adequate to compensate for Samsung's infringement, but in no event less than a reasonable royalty for the use made of the invention by Samsung, together with interest and costs as fixed by the Court.

48. On information and belief, despite having knowledge of the '384 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '384 patent, Samsung has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Samsung's infringing activities relative to the '384 patent have been, and continue to be, willful, wanton, malicious, bad-faith, deliberate, consciously wrongful, and an egregious case of misconduct beyond typical infringement such that Secure Wi-Fi is entitled to enhanced damages under 35 U.S.C. § 284 up to three times the amount found or assessed.

49. Samsung's acts of direct and indirect infringement have caused and continue to cause damage to Secure Wi-Fi. Secure Wi-Fi is entitled to damages in accordance with 35 U.S.C. §§ 271, 281, and 284 sustained as a result of Samsung's wrongful acts in an amount to be proven at trial.

SECOND COUNT

(INFRINGEMENT OF U.S. PATENT NO. 9,961,552)

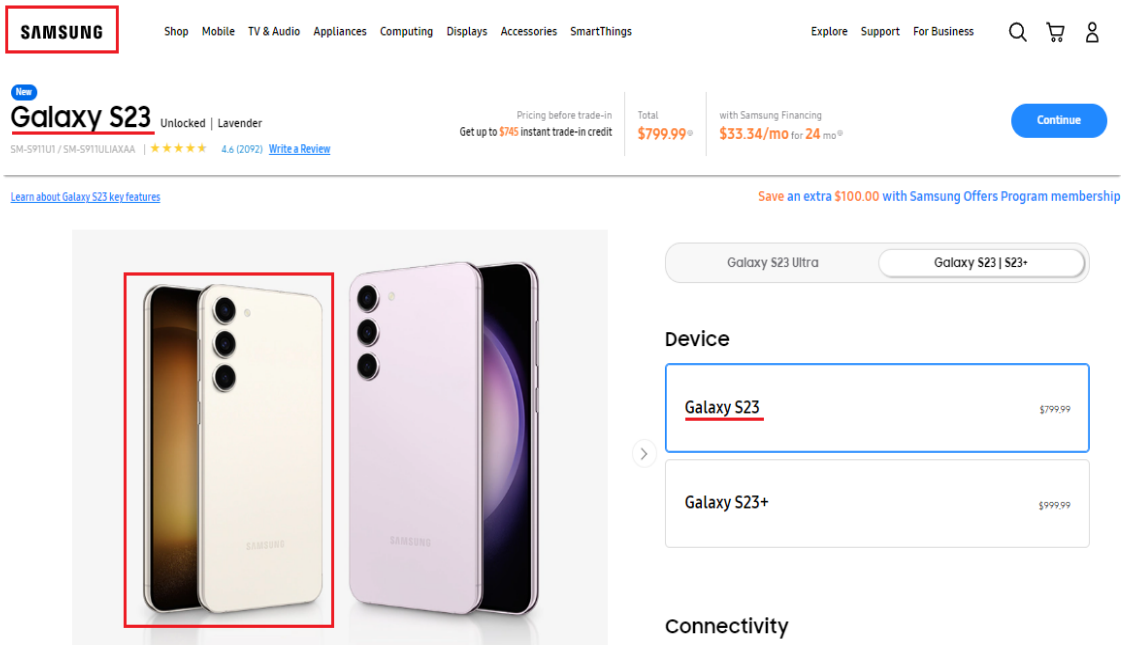
50. Secure Wi-Fi incorporates by reference the foregoing paragraphs as if fully set forth herein.

51. Secure Wi-Fi owns by assignment, all rights, title and interest, including the right to recover damages for past, present and future infringement, in U.S. Patent No. 9,961,552 titled "Schemes for Connecting to Wireless Network." The '552 patent was duly and legally issued by the United States Patent and Trademark Office on May 1, 2018. A true and correct copy of the '552 patent is attached as Exhibit B.

52. On information and belief, Defendants have directly infringed and continue to directly infringe one or more claims of the '552 patent, including at least claim 10 of the '552 patent, in the state of Texas, in this judicial district, and elsewhere in the United States by, among other things, making, using, selling, offering for sale, and/or importing into the United States products that embody

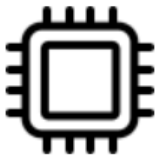
one or more of the inventions claimed in the '552 patent, including Samsung Galaxy smartphones that include the Android 10 operating system or later versions of Android operating system, as well as all reasonably similar products, in violation of 35 U.S.C. § 271(a). By way of example, the Accused Instrumentalities are an end device, such as the Galaxy S23 smartphone that includes the Android 13 operating system with randomized MAC for Wi-Fi connections.

53. The Accused Instrumentalities satisfy all claim limitations of one or more claims of the '552 patent, including exemplary claim 10. The Accused Instrumentalities practice a method performed by a device (e.g., the Accused Instrumentality). As shown below, the Galaxy S23 is a device that includes the Android 13 operating system and utilizes randomized MAC addresses for Wi-Fi connections. The Accused Instrumentalities contain an SoC. For example, the Galaxy S23 includes a Snapdragon 8 Gen 2 chipset..



https://www.samsung.com/us/smartphones/galaxy-s23/buy/galaxy-s23-128gb-unlocked-sm-s911uliaxaa/

Galaxy S23



Super fast processing

Snapdragon® 8 Gen 2

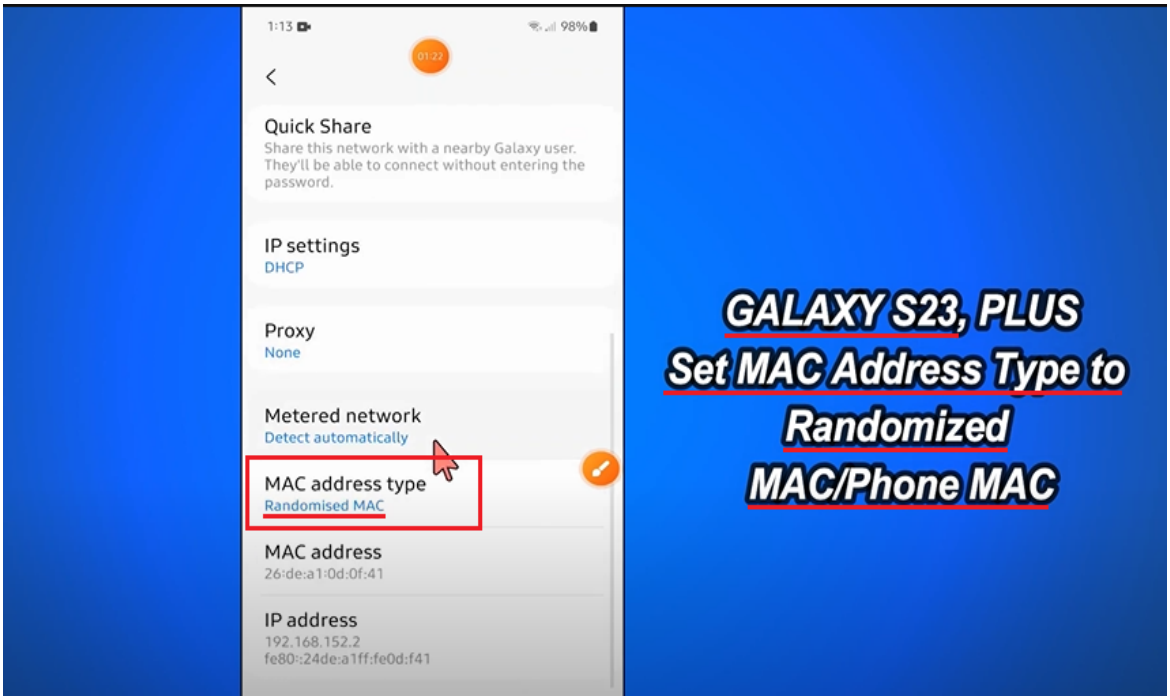
Octa-Core

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

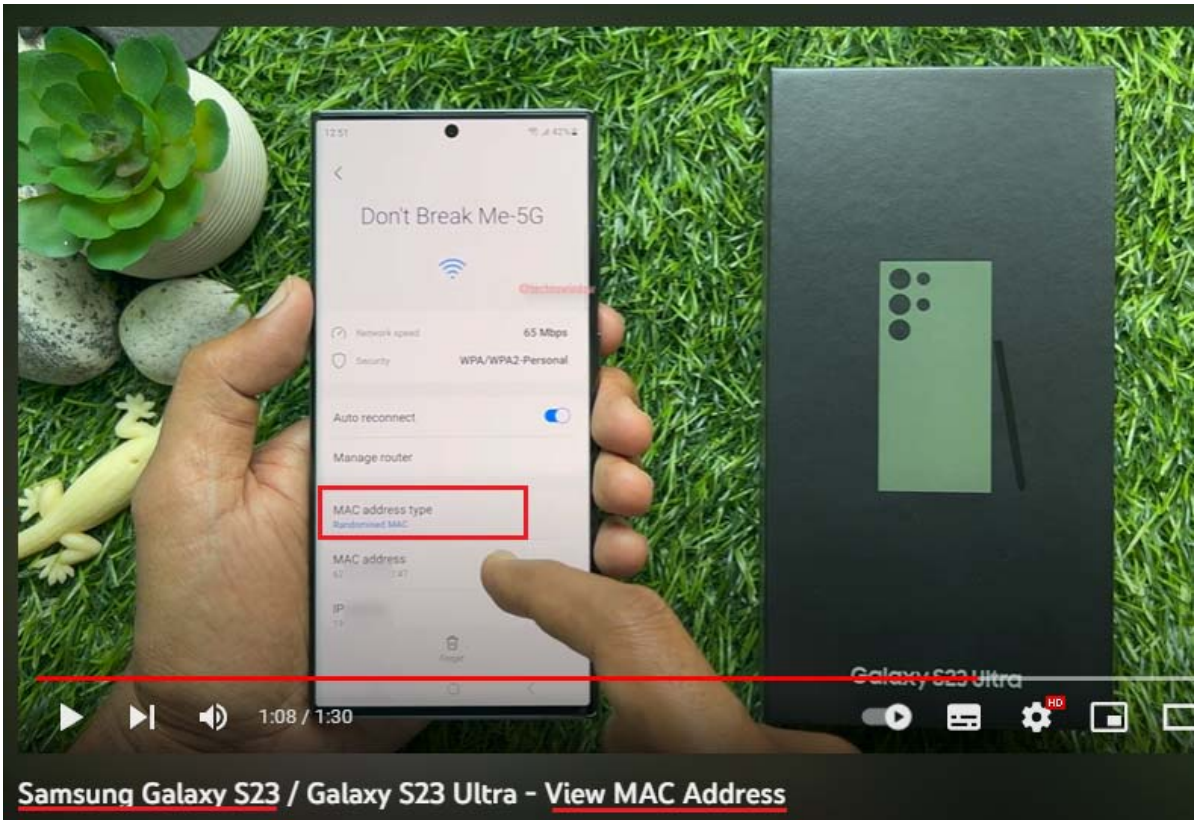
Phone	Galaxy S23	Galaxy S23+	Galaxy S23 Ultra
Chipset	Snapdragon 8 Gen 2 for Galaxy	Snapdragon 8 Gen 2 for Galaxy	Snapdragon 8 Gen 2 for Galaxy
RAM & Storage	8+128GB, 8+256GB (UFS 3.1)	8+256GB, 8+512GB (UFS 4.0)	8+256GB, 12+512GB, 12GB+1TB (UFS 4.0)
Display	6.1" FHD+ Dynamic AMOLED 2x, 120Hz Adaptive 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	Android 13 / One UI 5.1	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



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



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

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

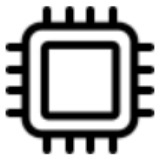
- The Samsung Galaxy S23 series features Qualcomm Technologies' leading connectivity solutions, including the Snapdragon® X70 Modem-RF System, the world's fastest and smartest 5G modem-RF system, and Qualcomm® FastConnect™ for high-speed and ultra-low latency Wi-Fi, and the latest Bluetooth audio enhancements.

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

54. The Accused Instrumentalities receive, from a server (e.g., the components for providing services of the Android Operating system including, e.g., for MAC randomization for Wi-Fi connections), an authenticated access point list (e.g., a list of previously connected access points such as WiFiConfigStore.xml file) that includes information (e.g., SSID, supported data rates, pre-shared keys) regarding one or more access points (e.g., a previously connected access point) that are controlled by the server (e.g., components that provide services of the Android Operating system including, for example, the connection and/or data transmission from access points).

55. The Accused Instrumentalities support the Android operating system, versions 10 or higher. The Galaxy S23 includes the Android 13 operating system. Android operating system versions 10 or higher, including the Android 13 operating system, include functionality for implementing randomized MAC for Wi-Fi connections. The Accused Instrumentalities implement a persistent randomized MAC address to be used with a Wi-Fi network. The operating system also facilitates storing a list of previously connected access point such as, for example, WiFiConfigStore.xml file. The list comprises information pertaining to previously connected access points such as, for example, SSID or pre-shared keys. The server provides an authenticated access point list in connection with performing the MAC randomization functionality of the Android operating system.

Galaxy S23



Super fast processing

Snapdragon® 8 Gen 2

Octa-Core

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

Phone	Galaxy S23	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	Android 13 / One UI 5.1	Android 13 / One UI 5.1	Android 13 / One UI 5.1

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

Phone	Galaxy S23	Galaxy S23+	Galaxy S23 Ultra
Connectivity	5G, Wi-Fi 6E, 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

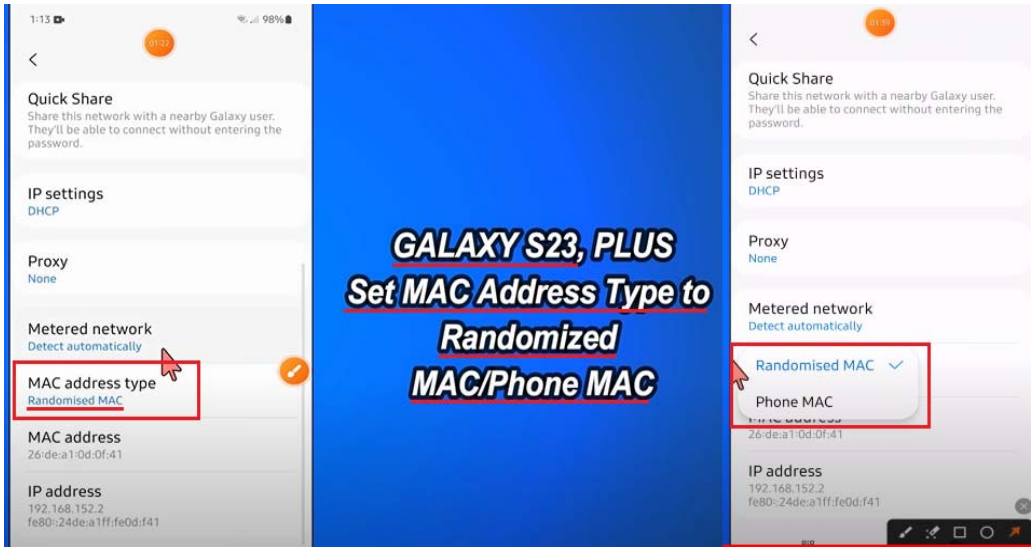
Wi-Fi 6E

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

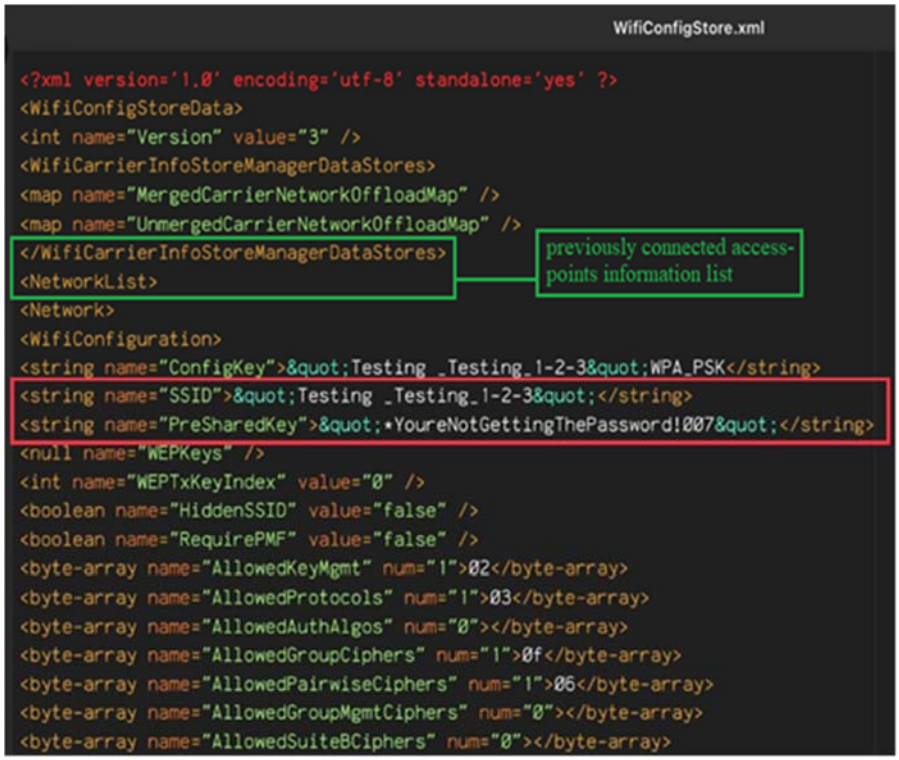
https://www.samsung.com/us/smartphones/galaxy-s23/specs/

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-Active[3], 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



https://twitter.com/josh_hickman1/status/1472553296187514889/photo/1

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="WEPTxKeyIndex" value="0" />
```

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

56. The Accused Instrumentalities receive from the server, a fake device identifier (e.g., a randomized MAC address) for the device (e.g., the Wi-Fi chipset of the Accused Instrumentality), wherein the received fake device identifier (e.g., a randomized MAC address) includes at least one of one or more random numbers or one or more random characters (e.g., Bytes of the MAC address) to falsely identify the device in a probe request frame (e.g., a Wi-Fi probe request).

57. By way of example, the Galaxy S23 includes an SoC, Snapdragon 8 Gen 2. They also include the Android 13 operating system and have randomized MAC for Wi-Fi connections. The server, components for providing the services of the operating system, provides a randomized MAC address to be used for connecting to a Wi-Fi network.

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

Phone	Galaxy S23	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	Android 13 / One UI 5.1	Android 13 / One UI 5.1	Android 13 / One UI 5.1

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

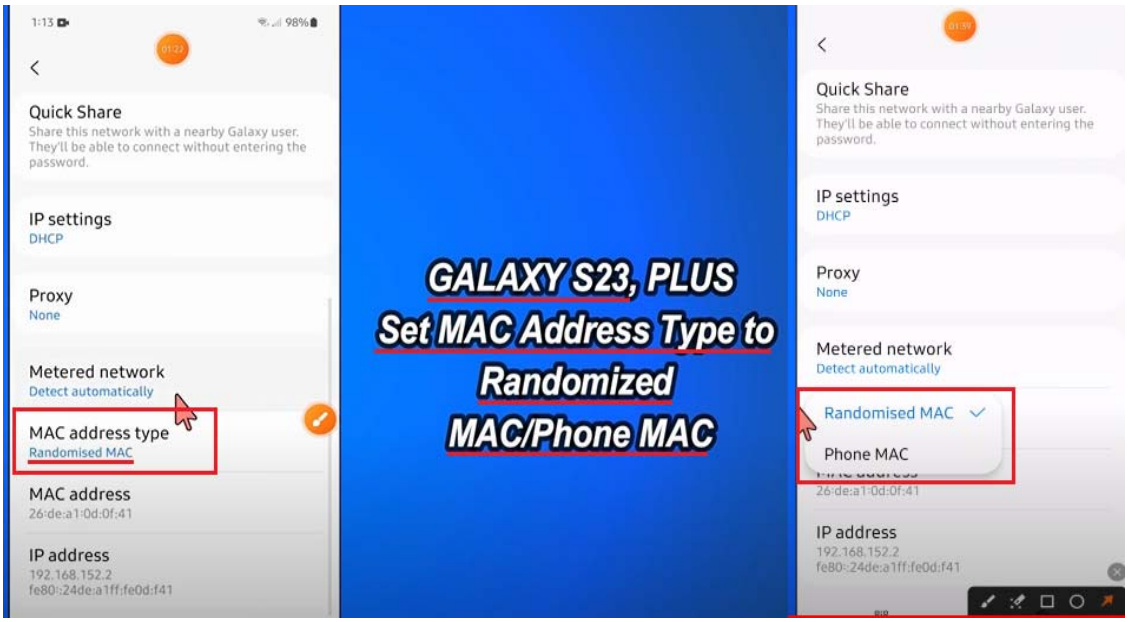
Phone	Galaxy S23	Galaxy S23+	Galaxy S23 Ultra
Connectivity	5G, Wi-Fi 6E, Bluetooth 5.3, NFC	5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband	5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband

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

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-Active[3], 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

58. The Accused Instrumentalities support the Wi-Fi standard. According to the standard, a UE (e.g., the Accused Instrumentality) inquires about available Wi-Fi access points using a probe request. The Accused Instrumentality receives the probe responses from multiple available access

points. It selects a desired access point for connection based on, for example, the access point capabilities or the desired network condition.

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 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).

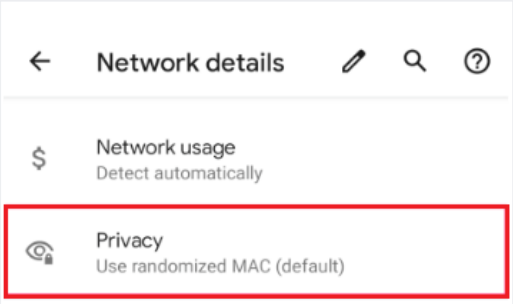
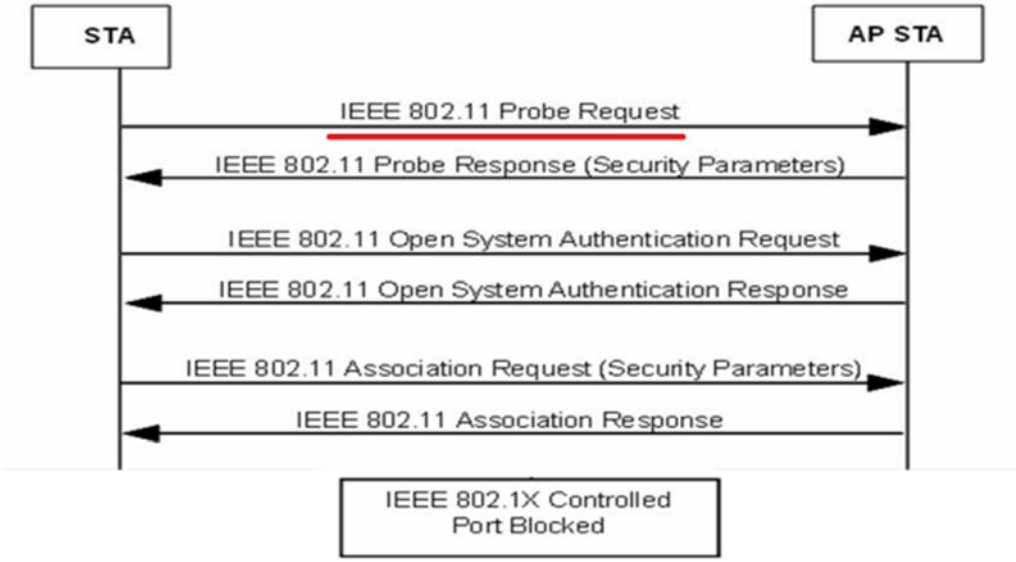


Figure 1. MAC randomization option.

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



Source: IEEE 802.11-2012.pdf at p. 84.

Table 8-26—Probe Request frame body

Order	Information	Notes
1	SSID	If dot11MeshActivated is true, the SSID element is the wildcard value as described in 8.4.2.2.
2	Supported rates	
3	Request information	The Request element is optionally present if dot11MultiDomainCapabilityActivated is true.
4	Extended Supported Rates	The Extended Supported Rates element is present if there are more than eight supported rates, and is optionally present otherwise.
5	DSSS Parameter Set	The DSSS Parameter Set element is present within Probe Request frames generated by STAs using Clause 16, Clause 17, or Clause 19 PHYs if dot11RadioMeasurementActivated is true. The DSSS Parameter Set element is present within Probe Request frames generated by STAs using a Clause 20 PHY in the 2.4 GHz band if dot11RadioMeasurementActivated is true. The DSSS Parameter Set element is optionally present within Probe Request frames generated by STAs using Clause 16, Clause 17, or Clause 19 PHYs if dot11RadioMeasurementActivated is false. The DSSS Parameter Set element is optionally present within Probe Request frames generated by STAs using a Clause 20 PHY in the 2.4 GHz band if dot11RadioMeasurementActivated is false.
6	Supported Operating Classes	The Supported Operating Classes element is present if dot11ExtendedChannelSwitchActivated is true.
7	HT Capabilities	The HT Capabilities element is present when dot11HighThroughputOptionImplemented attribute is true.
8	20/40 BSS Coexistence	The 20/40 BSS Coexistence element is optionally present when the dot112040BSSCoexistenceManagementSupport attribute is true.
9	Extended Capabilities	The Extended Capabilities element is optionally present if any of the fields in this element are nonzero.
10	SSID List	The SSID List element is optionally present if dot11MgmtOptionSSIDListActivated is true.
11	Channel Usage	The Channel Usage element is optionally present if dot11MgmtOptionChannelUsageActivated is true.
12	Interworking	The Interworking element is present if dot11InterworkingServiceActivated is true.
13	Mesh ID	The Mesh ID element is present if dot11MeshActivated is true.
Last	Vendor Specific	One or more vendor-specific elements are optionally present. These elements follow all other elements.

https://mrncciew.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.

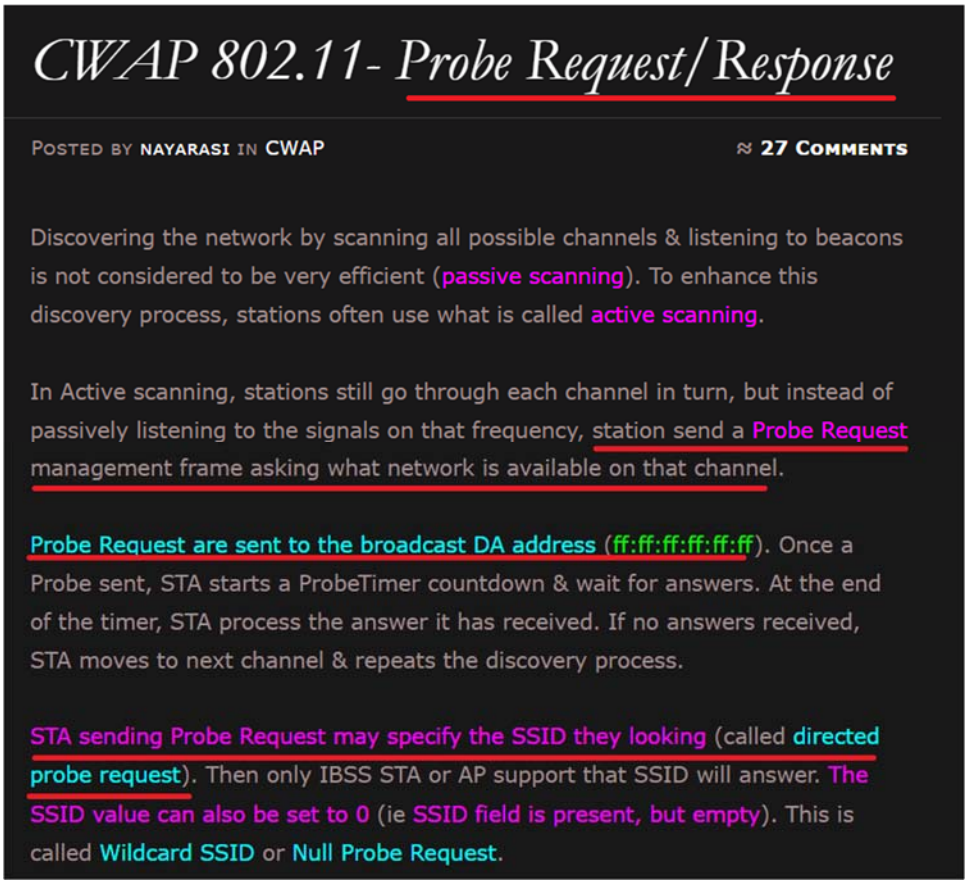
Source: IEEE 802.11-2012.pdf at p. 59.

Upon receipt of the MLME-SCAN.request primitive, a STA shall perform scanning. The SSID parameter indicates the SSID for which to scan. The SSID List parameter indicates one or more SSIDs for which to scan. To become a member of a particular ESS using passive scanning, a STA shall scan for Beacon frames containing that ESS's SSID, returning all Beacon frames matching the desired SSID in the BSSDescriptionSet parameter of the corresponding MLME-SCAN.confirm primitive with the appropriate bits in the Capabilities Information field indicating whether the Beacon frame came from an infrastructure BSS or IBSS. If the value of dot11RMMeasurementPilotActivated is greater than 1, the STA shall additionally scan for Measurement Pilot frames, returning in the BSSDescriptionFromMeasurementPilotSet parameter all Measurement Pilot frames that equal the requested BSSID of the corresponding MLME-SCAN.request primitive and are not already members of the BSSDescriptionSet. To actively scan, the STA shall transmit Probe request frames containing the desired SSID or one or more SSID List elements. When the SSID List element is present in the Probe Request frame, one or more of the SSID elements may include a wildcard SSID (see 8.4.2.2). The exact procedure for determining the SSID or SSID List values in the MLME-SCAN.request

Source: IEEE 802.11-2012.pdf at p. 977.

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



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

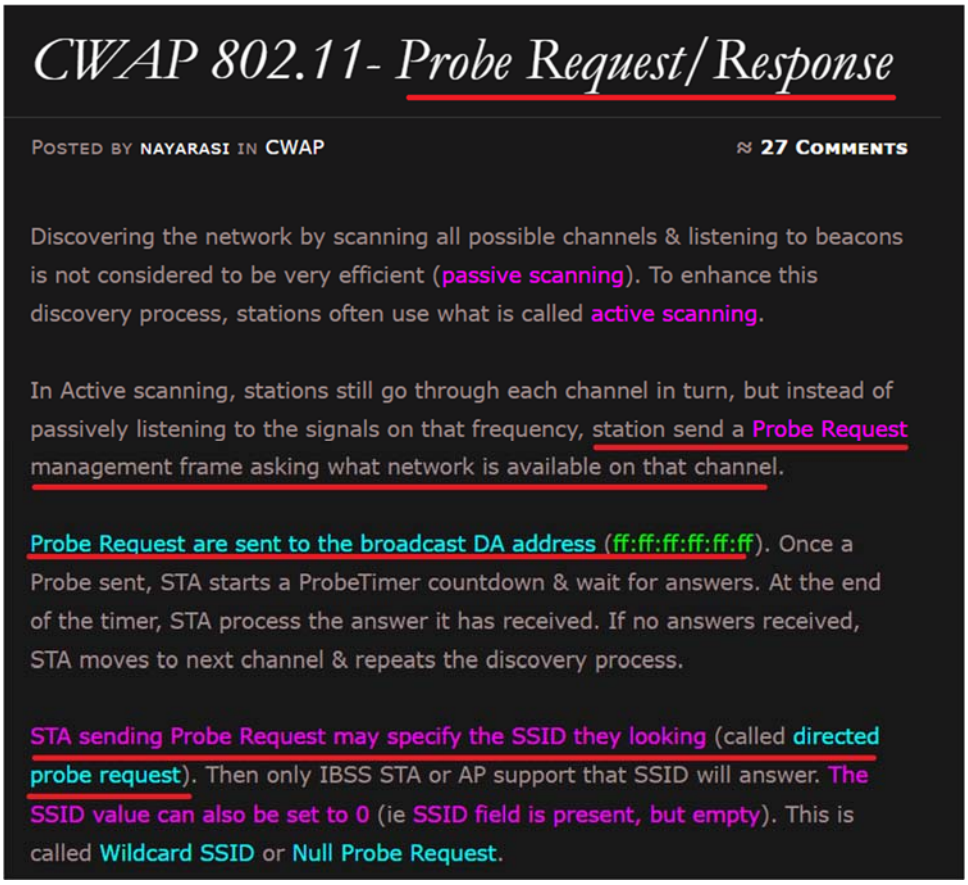
59. The Accused Instrumentalities transmit, to at least one access point (e.g., a Wi-Fi access point), the probe request frame (e.g., a Wi-Fi probe request) that includes the received fake device identifier (e.g., a randomized MAC address).

60. The Accused Instrumentalities support the Wi-Fi standard. According to the standard, a UE (e.g., the Accused Instrumentality) inquires about available Wi-Fi access points using a probe request. The probe request comprises a sender address field (e.g., a device identifier). The Accused Instrumentalities utilize a random MAC address as the sender address in a probe request. The Accused Instrumentality receives probe responses from available access points. The Accused Instrumentality selects a desired access point for connection based on, for example, the access point capabilities or

desired network condition. The Accused Instrumentality transmits probe requests to identify available access points.

> 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



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

61. A Wi-Fi probe request includes the randomized 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

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).

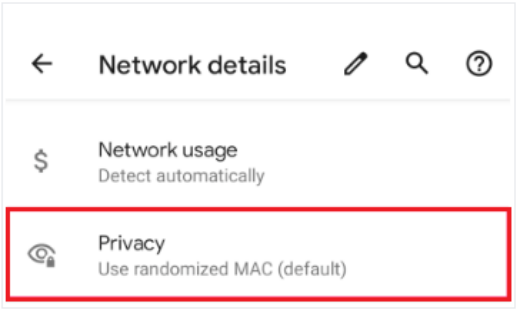


Figure 1. MAC randomization option.

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

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

62. The Accused Instrumentalities receive, from the at least one access point (e.g., a Wi-Fi access point) in response to the transmitting the probe request frame (e.g., a Wi-Fi probe request), a probe response frame (e.g., a Wi-Fi probe response) that includes information (e.g., SSID, supported data rates, etc.) regarding the at least one access point (e.g., a Wi-Fi access point).

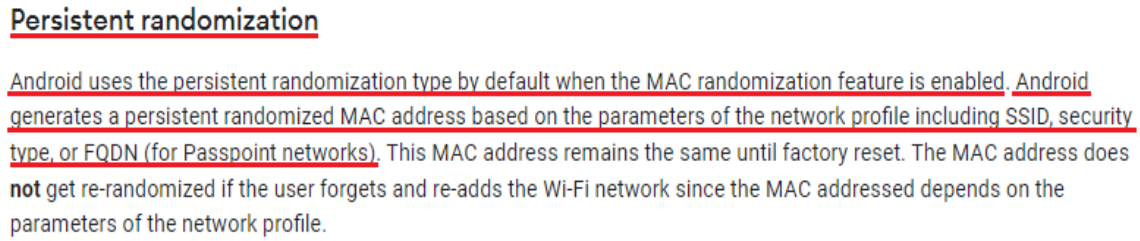
63. A Wi-Fi probe response includes, for example, the SSID (wireless network name). As another example, a Wi-Fi probe response includes supported data rates of the access point.

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

64. The Accused Instrumentalities support the Wi-Fi standard. The Accused Instrumentalities receive probe responses from multiple available access points. An access point responds with a probe response when the SSID in the probe request is the wildcard SSID or matches

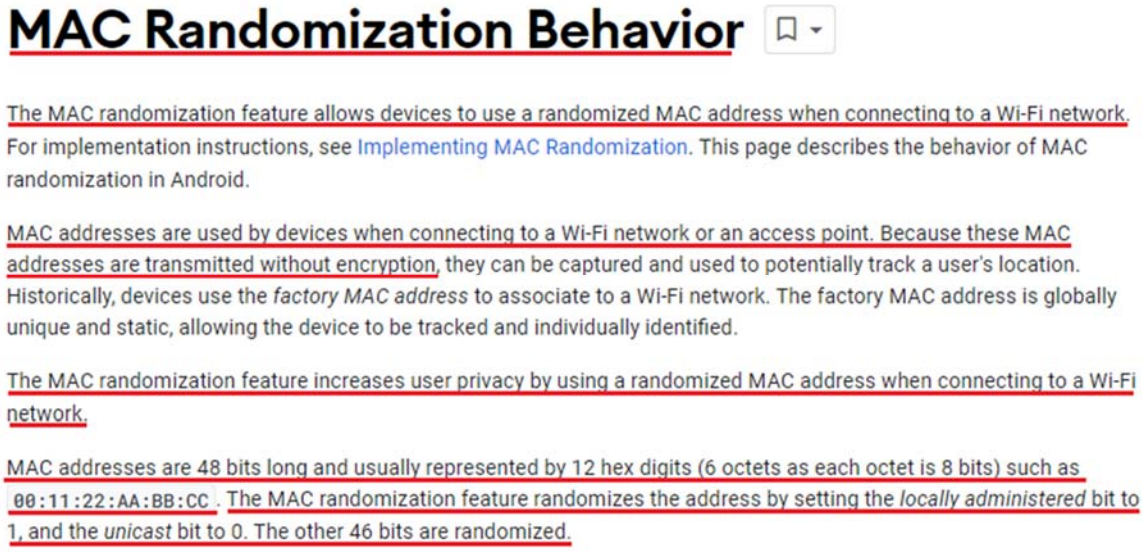
the specific SSID of the access point or when the specific SSID of the access point is included in the SSID list element.



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 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).

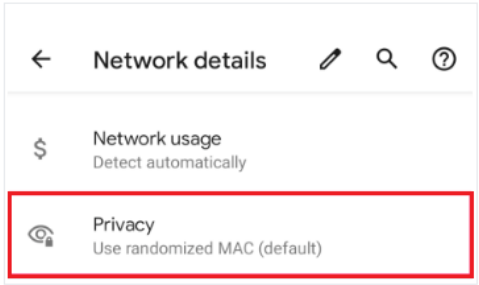


Figure 1. MAC randomization option.

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

MAC Randomization Behavior

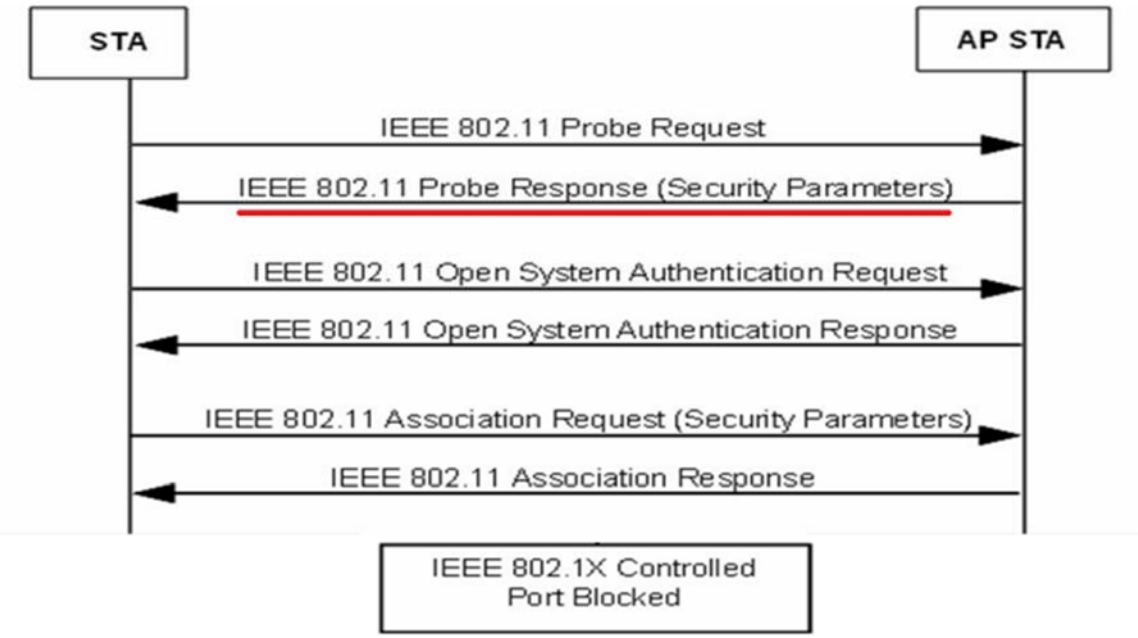
The MAC randomization feature allows devices to use a randomized MAC address when connecting to a Wi-Fi network. For implementation instructions, see Implementing MAC Randomization. This page describes the behavior of MAC randomization in Android.

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



Source: IEEE 802.11-2012.pdf at p. 84.

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 dot11QosOption-Implemented 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/

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 dot11ExendedChannelSwitchActivated 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://mrncciew.com/2014/10/27/cwap-802-11-probe-requestresponse/

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 dot11MgmtOptionUTCTSFOffsetActivated is true.
43	Time Zone	The Time Zone element is present if dot11MgmtOptionUTCTSFOffsetActivated 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/

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 at p. 59.

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 at p. 979.

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.

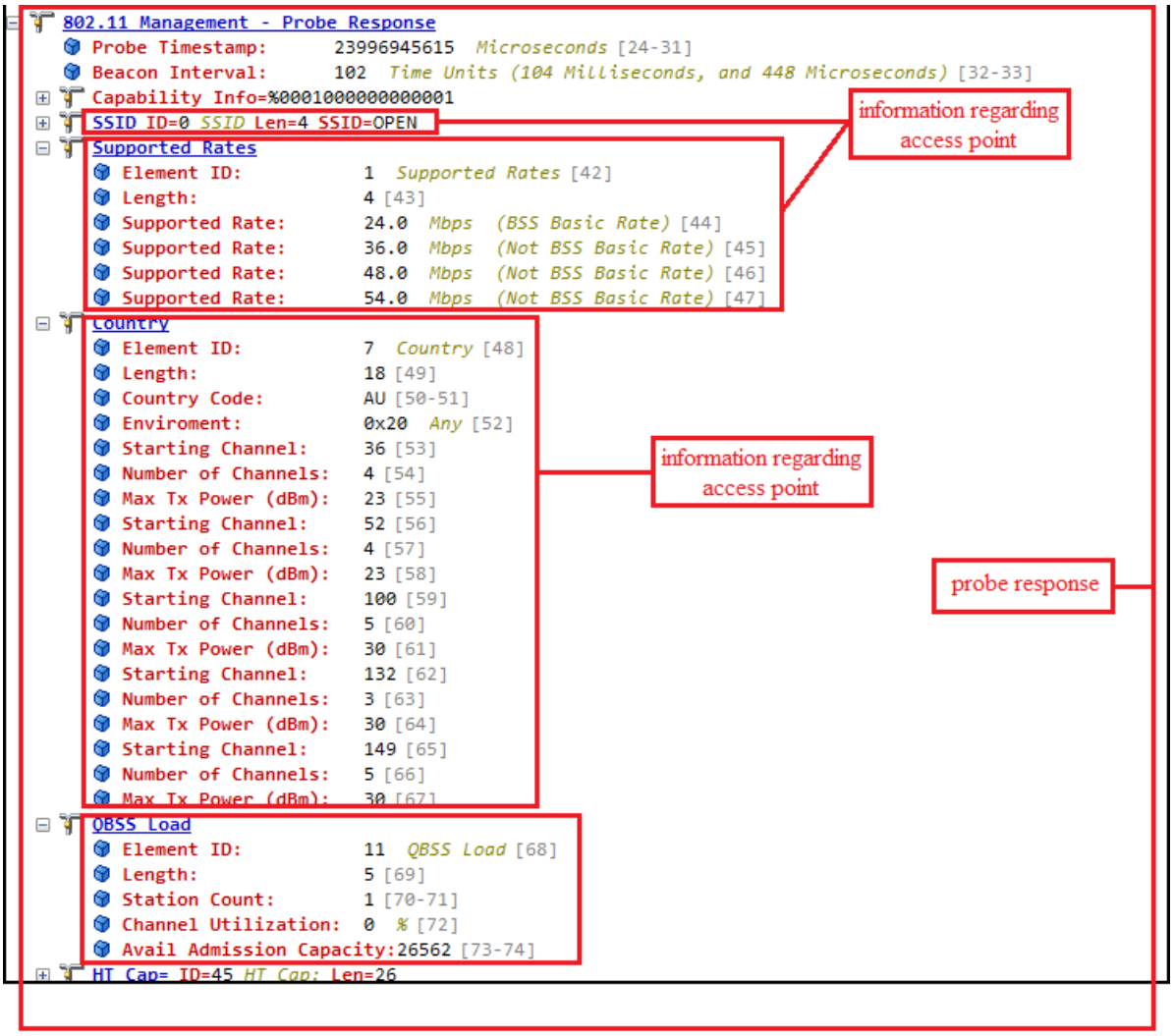
User devices trying to connect to a Wi-Fi network watch for access points (APs) broadcasting its availability for a device to connect to its network. Within that information contains the network name, or Service Set Identifier (SSID). Wi-Fi enabled devices trying to connect to a wireless network, and 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



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

65. The Accused Instrumentalities determine, in response to receiving the probe response frame (e.g., a probe response) and based at least, in part, on the information (e.g., SSID, supported data rates, keys etc.) regarding the at least one access point (e.g., a Wi-Fi access point), whether the at least one access point (e.g., a Wi-Fi access point) is an authenticated access point (e.g., a previously connected access point), wherein the determining whether the at least one access point (e.g., a Wi-Fi access point) is the authenticated access point (e.g., a previously connected access point) includes determining whether the information (e.g., SSID, supported data rates, keys, etc.) regarding the at

least one access point (e.g., a Wi-Fi access point) is included in the authenticated access point list (e.g., a previously connected access point list such as WiFiConfigStore.xml file) that is received from the server (components that provide the Android Operating services including the MAC randomization feature).

66. The Accused Instrumentalities support the Wi-Fi standard. According to the standard, a UE (e.g., the Accused Instrumentality) inquires about available Wi-Fi access points using a probe request. The probe request comprises a SSID list or preferred network list which is a set of SSIDs to which the Accused Instrumentality was connected previously. The Accused Instrumentalities receive the probe responses from multiple available access points. 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.

67. The Accused Instrumentalities support the Android operating system version 10 and higher and include randomized MAC for Wi-Fi connections. By way of example, the Galaxy S23 includes Android operating system version 13. The operating system generates a persistent randomized MAC address to be used with a Wi-Fi network. A list of previously connected access points, e.g., WiFiConfigStore.xml file, is received from the server. The list comprises different information pertaining to previously connected access points such as SSID, pre-shared keys, etc.

68. The Accused Instrumentalities confirm the received SSID information from the probe responses with the access point information of the list. Once confirmed that there is a SSID in a probe response from an access point with which the Accused Instrumentality was connected previously, the Accused Instrumentality initiates an authentication process with stored pre-shared key information and previously used authenticated MAC address, using persistent randomization.

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 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).

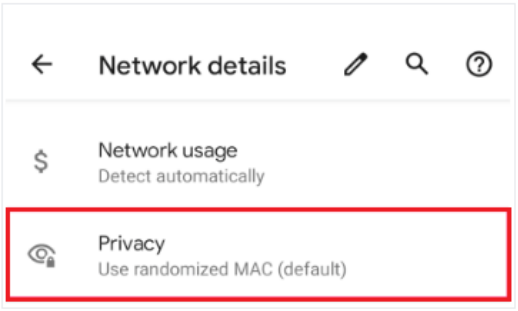


Figure 1. MAC randomization option.

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

MAC Randomization Behavior

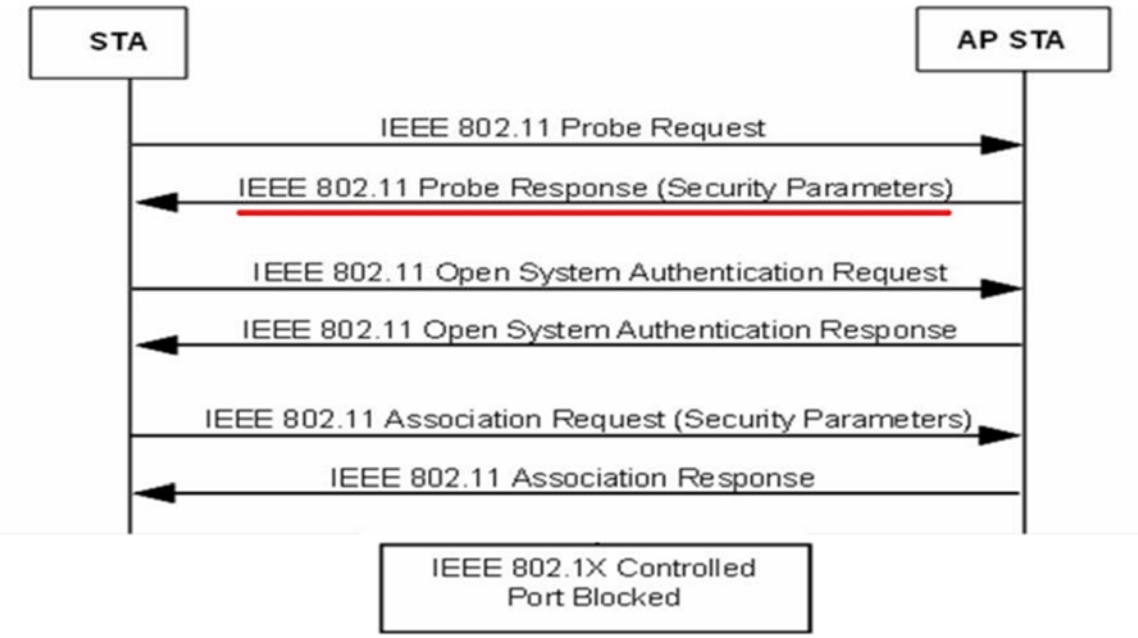
The MAC randomization feature allows devices to use a randomized MAC address when connecting to a Wi-Fi network. For implementation instructions, see Implementing MAC Randomization. This page describes the behavior of MAC randomization in Android.

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



Source: IEEE 802.11-2012.pdf at p.84.

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 dot11QosOption-Implemented 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/

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 dot11ExendedChannelSwitchActivated 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://mrncciew.com/2014/10/27/cwap-802-11-probe-requestresponse/

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 dot11MgmtOptionUTCTSFOffsetActivated is true.
43	Time Zone	The Time Zone element is present if dot11MgmtOptionUTCTSFOffsetActivated 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/

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 at p. 59.

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 at p. 979.

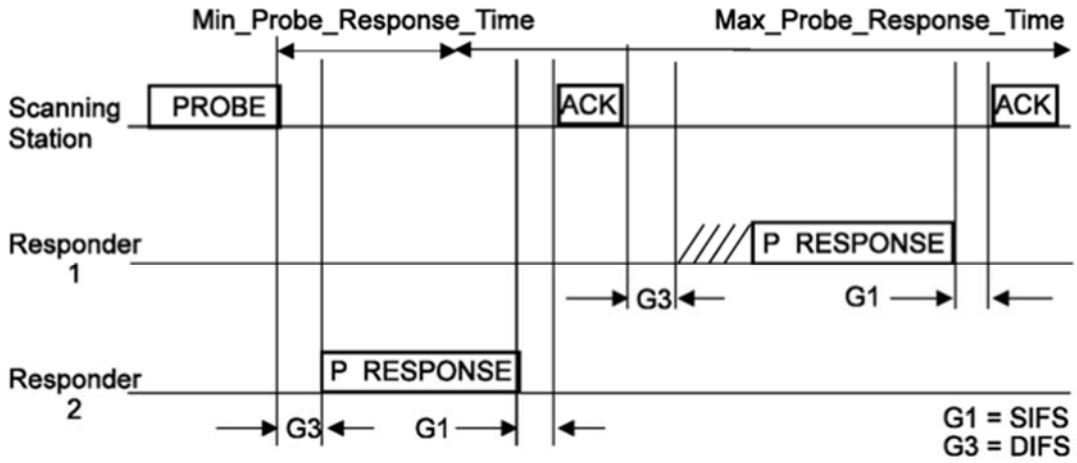


Figure 10-3—Probe response

Source: IEEE 802.11-2012.pdf at p. 980.

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.

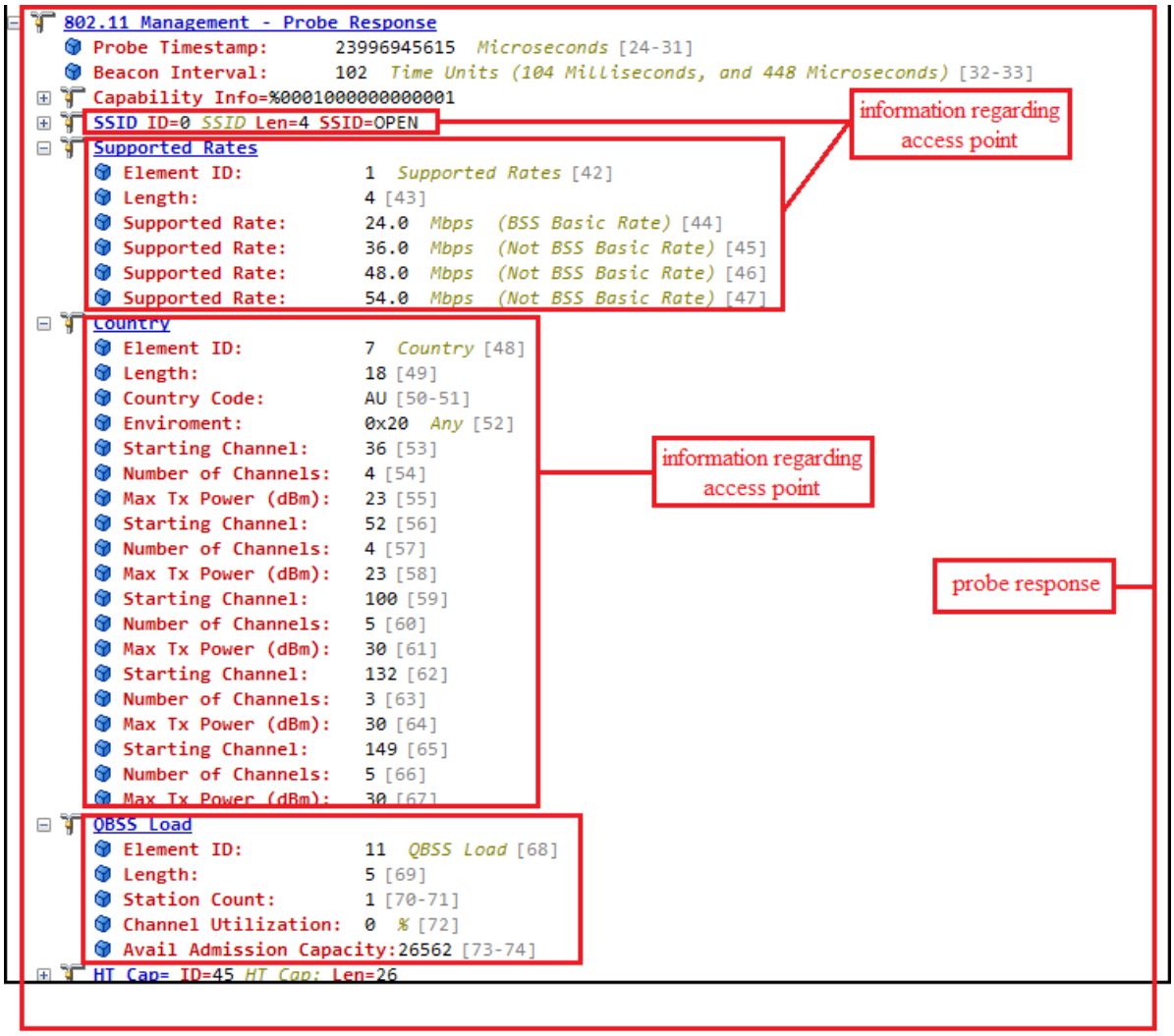
User devices trying to connect to a Wi-Fi network watch for access points (APs) broadcasting its availability for a device to connect to its network. Within that information contains the network name, or Service Set Identifier (SSID). Wi-Fi enabled devices trying to connect to a wireless network, and 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



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

69. The Accused Instrumentalities include functionality for persistent MAC randomization, in which for the same Wi-Fi network and device combination, the MAC address remains the same. When the Accused Instrumentalities connect to a Wi-Fi network to which they were previously connected, they will use the same MAC address.

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 addressed 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.

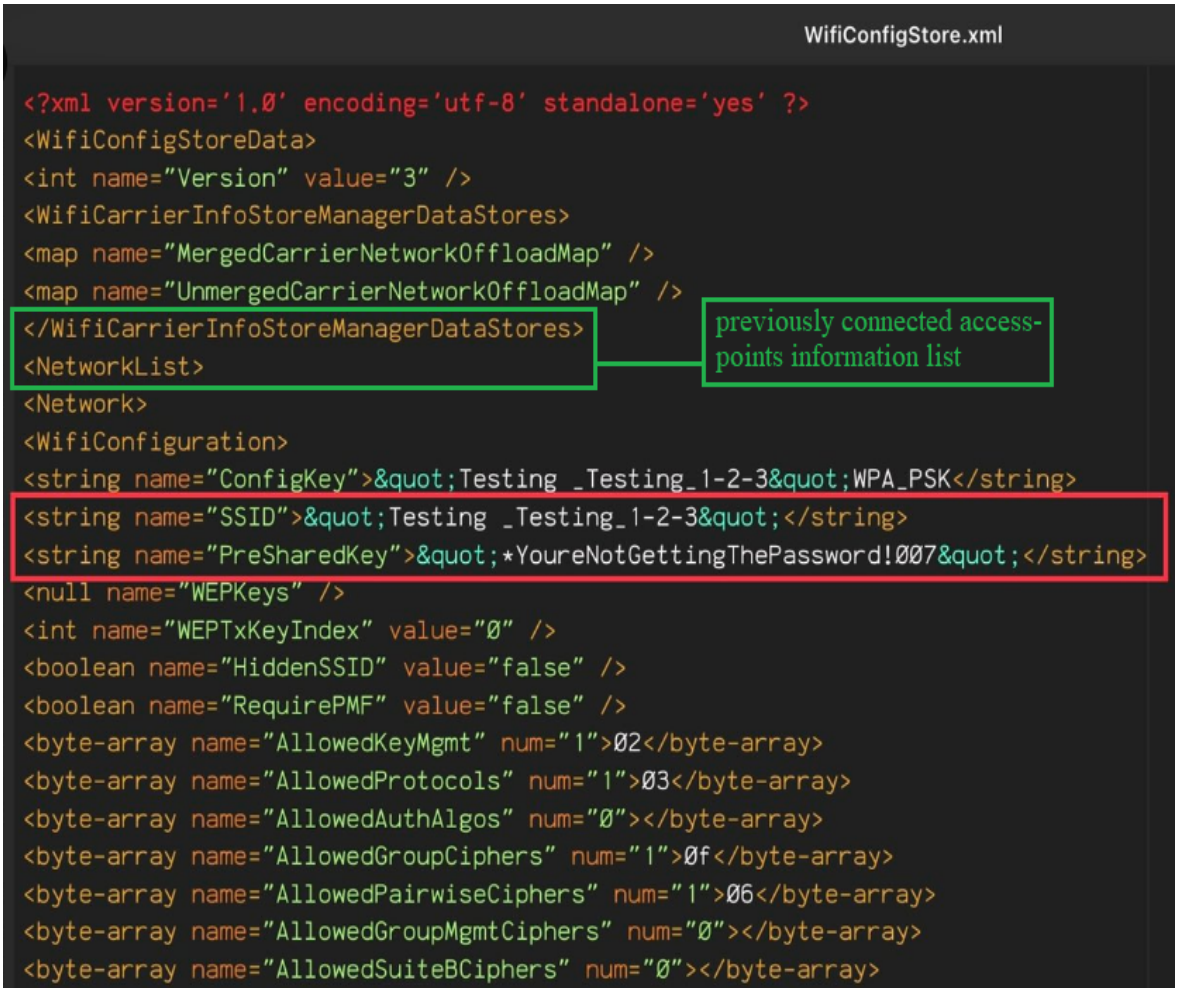
https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior

android / device / generic / goldfish / refs/tags/android-9.0.0_r34 / . / wifi / **WifiConfigStore.xml**

blob: 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="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




```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<WifiConfigStoreData>
<int name="Version" value="3" />
<WifiCarrierInfoStoreManagerDataStores>
<map name="MergedCarrierNetworkOffloadMap" />
<map name="UnmergedCarrierNetworkOffloadMap" />
</WifiCarrierInfoStoreManagerDataStores>
<NetworkList>
<Network>
<WifiConfiguration>
<string name="ConfigKey">&quot;Testing _Testing_1-2-3&quot;WPA_PSK</string>
<string name="SSID">&quot;Testing _Testing_1-2-3&quot;</string>
<string name="PreSharedKey">&quot;*YoureNotGettingThePassword!007&quot;</string>
<null name="WEPKeys" />
<int name="WEPTxKeyIndex" value="0" />
<boolean name="HiddenSSID" value="false" />
<boolean name="RequirePMF" value="false" />
<byte-array name="AllowedKeyMgmt" num="1">02</byte-array>
<byte-array name="AllowedProtocols" num="1">03</byte-array>
<byte-array name="AllowedAuthAlgos" num="0"></byte-array>
<byte-array name="AllowedGroupCiphers" num="1">0f</byte-array>
<byte-array name="AllowedPairwiseCiphers" num="1">06</byte-array>
<byte-array name="AllowedGroupMgmtCiphers" num="0"></byte-array>
<byte-array name="AllowedSuiteBCiphers" num="0"></byte-array>
```

https://twitter.com/josh_hickman1/status/1472553296187514889/photo/1

70. The Accused Instrumentalities transmit, to the at least one access point (e.g., a Wi-Fi access point) in response to a determination that the at least one access point (e.g., a Wi-Fi access point) is the authenticated access point (e.g., a previously authenticated access point), a connection request (e.g., an association request) that includes an authentic device identifier for the device (e.g., a previously authenticated MAC address used by the device for connecting to the access point).

71. The Accused Instrumentalities support the Wi-Fi standard. According to the standard, a UE (e.g., the Accused Instrumentality) inquires about available Wi-Fi access points using a probe

request. The probe request comprises a SSID list or preferred network list which is a set of SSIDs to which the UE connected previously.

72. The Accused Instrumentalities receive the probe responses from multiple available access points. 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.

73. The Accused Instrumentalities confirm the received SSID information from the probe responses with the access point information. Once confirmed that there is a SSID in a probe response from an access point to which the Accused Instrumentality was connected previously, the Accused Instrumentality initiates an authentication process, e.g., with a stored pre-shared key. For example, the Accused Instrumentality sends a connection request using stored key information and the previously used authenticated MAC address.

> **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 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).

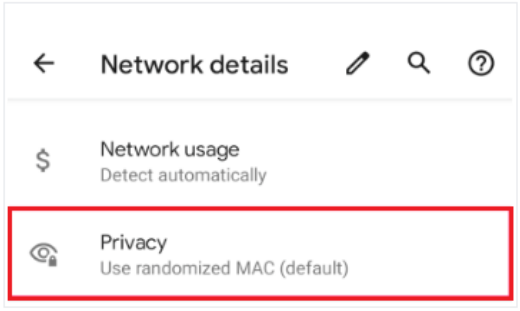


Figure 1. MAC randomization option.

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

MAC Randomization Behavior

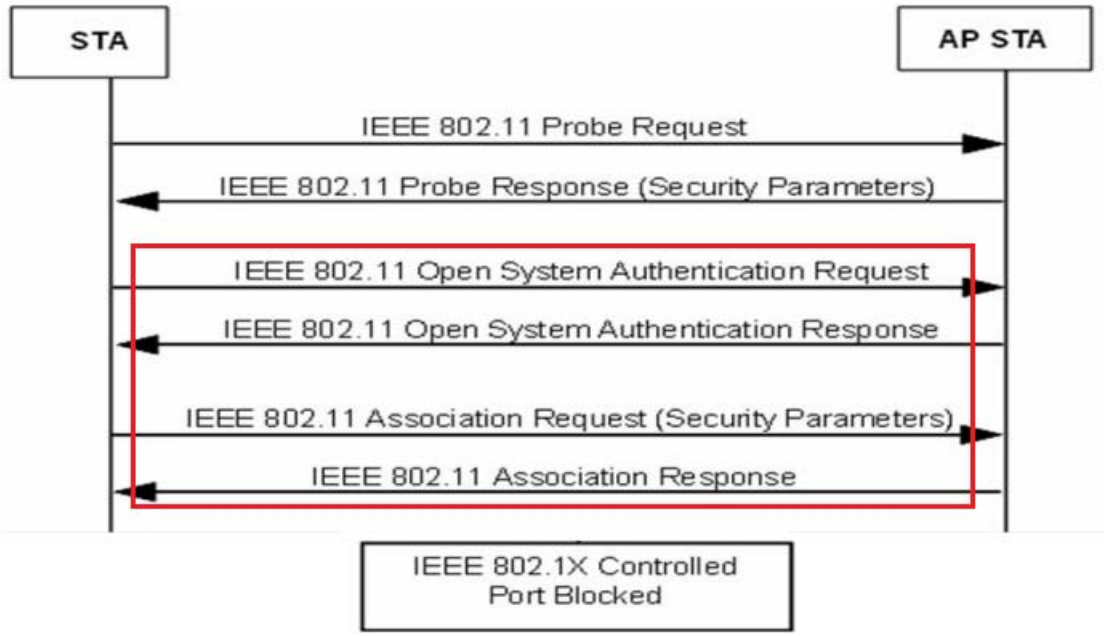
The MAC randomization feature allows devices to use a randomized MAC address when connecting to a Wi-Fi network. For implementation instructions, see Implementing MAC Randomization. This page describes the behavior of MAC randomization in Android.

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.

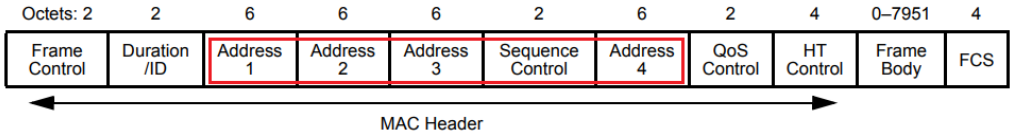
https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior

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



Source: IEEE 802.11-2012.pdf at p. 84.

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 at p. 381.

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 at p. 388.

802.11 Mgmt : Authentication Frame

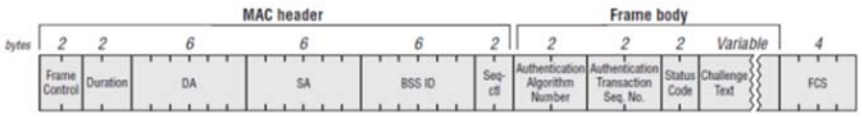
POSTED BY NAYARASI IN CWAP ≈ 10 COMMENTS

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

74. The Accused Instrumentalities include functionality for persistent MAC randomization, in which for the same Wi-Fi network and device combination, the MAC address remains the same. When the Accused Instrumentality connects to a Wi-Fi network to which it was previously connected, it will use the same MAC address.

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 addressed 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.

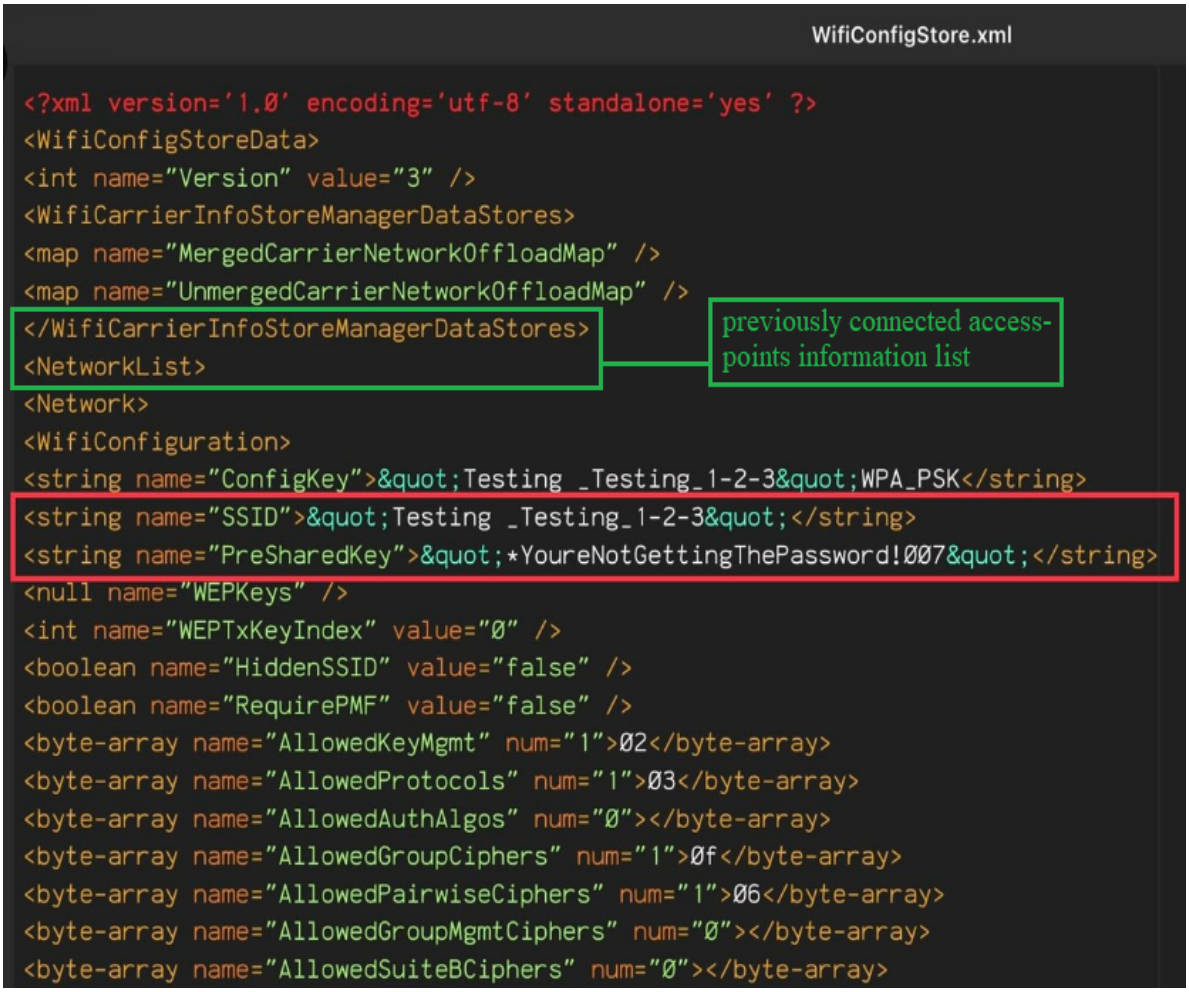
https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior

android / device / generic / goldfish / refs/tags/android-9.0.0_r34 / . / wifi / **WifiConfigStore.xml**

blob: 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="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




```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<WifiConfigStoreData>
<int name="Version" value="3" />
<WifiCarrierInfoStoreManagerDataStores>
<map name="MergedCarrierNetworkOffloadMap" />
<map name="UnmergedCarrierNetworkOffloadMap" />
</WifiCarrierInfoStoreManagerDataStores>
<NetworkList>
<Network>
<WifiConfiguration>
<string name="ConfigKey">&quot;Testing _Testing_1-2-3&quot;WPA_PSK</string>
<string name="SSID">&quot;Testing _Testing_1-2-3&quot;</string>
<string name="PreSharedKey">&quot;*YoureNotGettingThePassword!007&quot;</string>
<null name="WEPKeys" />
<int name="WEPTxKeyIndex" value="0" />
<boolean name="HiddenSSID" value="false" />
<boolean name="RequirePMF" value="false" />
<byte-array name="AllowedKeyMgmt" num="1">02</byte-array>
<byte-array name="AllowedProtocols" num="1">03</byte-array>
<byte-array name="AllowedAuthAlgos" num="0"></byte-array>
<byte-array name="AllowedGroupCiphers" num="1">0f</byte-array>
<byte-array name="AllowedPairwiseCiphers" num="1">06</byte-array>
<byte-array name="AllowedGroupMgmtCiphers" num="0"></byte-array>
<byte-array name="AllowedSuiteBCiphers" num="0"></byte-array>
```

https://twitter.com/josh_hickman1/status/1472553296187514889/photo/1

75. By making, using, offering for sale, selling and/or importing into the United States the Accused Instrumentalities, Samsung has injured and continues to injure Secure Wi-Fi and is liable for infringement of the '552 patent pursuant to 35 U.S.C. § 271(a).

76. In addition, and/or in the alternative to its direct infringement, Defendants have also infringed and continue to infringe the claims of the '552 patent by, among other things, actively inducing others to use the Accused Instrumentalities in violation of 35 U.S.C. § 271(b).

77. Samsung's users, customers, consumers, agents, distributors, and other third parties who use, sell, offer to sell, and/or import the Accused Instrumentalities in accordance with Samsung's

instructions infringe the claims of the '552 patent, in violation of 35 U.S.C. § 271(a). Samsung intentionally instructs its customers to infringe through support information such as websites, videos, demonstrations, support information and other published information. For example, Samsung's website instructs and encourages its customers to use, manage and control the infringing components and functionalities of the Accused Instrumentalities. *See*, *e.g.*, https://www.samsung.com/us/smartphones/galaxy-s23/specs/ (advertising the Wi-Fi capabilities of Accused Instrumentalities); https://downloadcenter.samsung.com/content/UM/202302/20230207045923682/SAM_S911_S916_S918_EN_UM_OS13_020223_FINAL.pdf, at 3, 119 (advertising and instructing users to connect perform Wi-Fi connections); *id*. at 121-122 (advertising and instructing Wi-Fi connections); https://www.samsung.com/my/support/mobile-devices/how-to-connect-wi-fi-network-on-my-samsung-device/ ("How to connect to Wi-Fi network on my Samsung Device."); *id*. at 16 (encouraging users to "make full use of [their] device's Android features").

78. The Accused Instrumentalities implement infringing functionality by default when connecting to a Wi-Fi network. *See, e.g.*, https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior. The Accused Instrumentalities are designed and intended to perform MAC randomization for Wi-Fi connections and necessarily infringe the '552 patent in the normal, intended manner without any additional specific action of the end user other than connecting to a Wi-Fi network.

79. Thus, Samsung actively instructs and directs its customers to infringe and actively encourages infringement by its customers. Samsung is thereby liable for infringement of the '552 patent under 35 U.S.C. § 271(b).

80. At a minimum, Samsung has had knowledge of the '552 patent since at least the filing and/or service date of the Complaint in this action. Despite this knowledge, Samsung has continued to engage in activities to encourage and assist its customers, consumers, agents, distributors, and other third parties in the use, sale, offer for sale, and/or importation of the Accused Instrumentalities. Thus, on information and belief, Samsung (1) had actual knowledge of the patent; (2) knowingly induced its customers to infringe the patent; and (3) had specific intent to induce the patent infringement.

81. Additionally, and/or alternatively, Samsung is liable as a contributory infringer of the '552 patent under 35 U.S.C. § 271(c) by having offered to sell, sold and imported and continuing to offer to sell, selling, and importing into the United States the Accused Instrumentalities and reasonably similar products, to be especially made or adapted for use in infringement of the '552 patent. The portions of the Samsung Accused Instrumentalities that enable Wi-Fi connections of the Accused Instrumentalities utilizing MAC randomization constitute a material component for use in practicing the '552 patent and are especially made and are not staple articles of commerce suitable for non-infringing use.

82. Secure Wi-Fi has complied with 35 U.S.C. § 287 because Secure Wi-Fi does not make, offer for sale or sell products that practice the '552 patent during the relevant time period.

83. As a result of Samsung's direct and indirect infringement of the '552 patent, Secure Wi-Fi is entitled to monetary damages (past, present and future) in an amount adequate to compensate for Samsung's infringement, but in no event less than a reasonable royalty for the use made of the invention by Samsung, together with interest and costs as fixed by the Court.

84. On information and belief, despite having knowledge of the '552 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '552 patent, Samsung has nevertheless continued its infringing conduct and disregarded an objectively high

likelihood of infringement. Samsung's infringing activities relative to the '552 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, and an egregious case of misconduct beyond typical infringement such that Secure Wi-Fi is entitled to enhanced damages under 35 U.S.C. § 284 up to three times the amount found or assessed.

85. Samsung's acts of direct and indirect infringement have caused and continue to cause damage to Secure Wi-Fi. Secure Wi-Fi is entitled to damages in accordance with 35 U.S.C. §§ 271, 281, and 284 sustained as a result of Samsung's wrongful acts in an amount to be proven at trial.

THIRD COUNT

(INFRINGEMENT OF U.S. PATENT NO. 9,717,005)

86. Secure Wi-Fi incorporates by reference the foregoing paragraphs as if fully set forth herein.

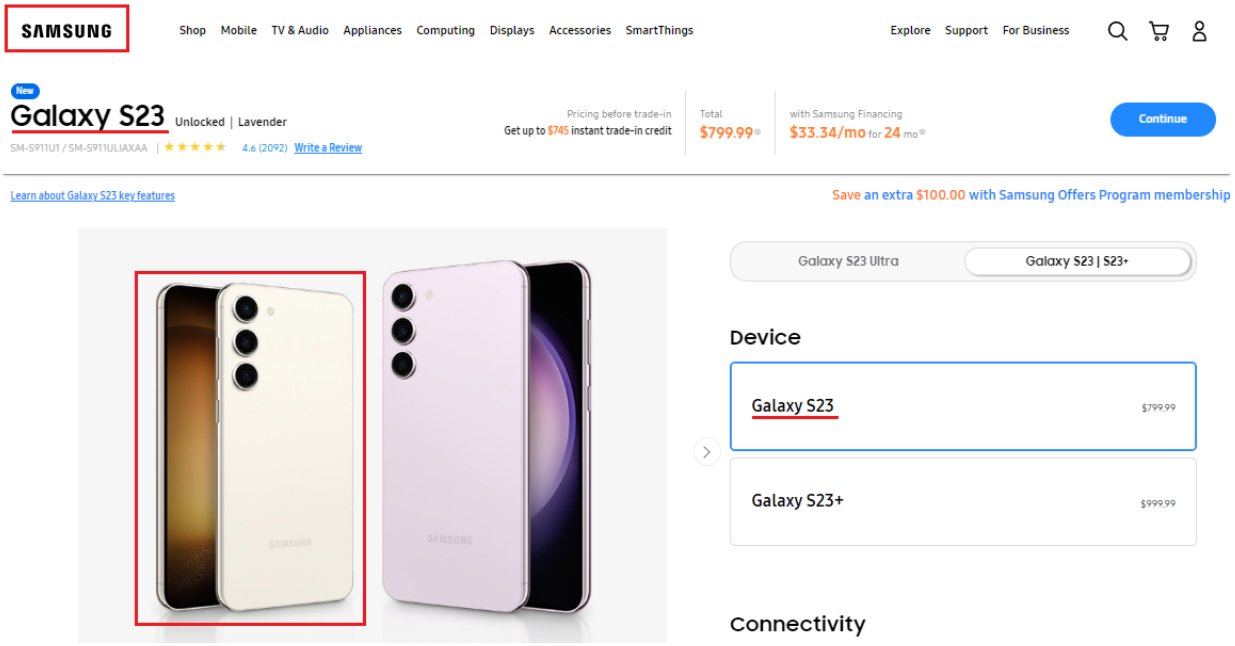
87. Secure Wi-Fi owns by assignment, all rights, title and interest, including the right to recover damages for past, present and future infringement, in U.S. Patent No. 9,717,005 titled "Schemes for Connecting to Wireless Network." The '005 patent was duly and legally issued by the United States Patent and Trademark Office on July 25, 2017. A true and correct copy of the '005 Patent is attached as Exhibit C.

88. On information and belief, Defendants have directly infringed and continue to directly infringe one or more claims of the '005 patent, including at least claim 1 of the '005 patent, in the state of Texas, in this judicial district, and elsewhere in the United States by, among other things, making, using, selling, offering for sale, and/or importing into the United States products that embody one or more of the inventions claimed in the '005 patent, including but not limited to the Accused Instrumentalities, including Samsung Galaxy smartphones that include the Android 10 operating system or later versions of the Android operating system as well as all reasonably similar products,

in violation of 35 U.S.C. § 271(a). By way of example, the Accused Instrumentalities are an end device, such as the Galaxy S23 smartphone that includes the Android 13 operating system with randomized MAC for Wi-Fi connections.

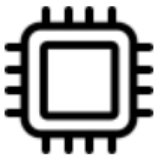
89. The Accused Instrumentalities satisfy all claim limitations of one or more claims of the '005 patent, including exemplary claim 1. The Accused Instrumentalities practice a method performed under control of an end device (e.g., under the control of the Accused Instrumentality).

90. By way of example, the Galaxy S23 includes the Android 13 operating system and has randomized MAC addresses for Wi-Fi connections. The Accused Instrumentalities contain a SoC, Snapdragon 8 Gen 2 chipset.



https://www.samsung.com/us/smartphones/galaxy-s23/buy/galaxy-s23-128gb-unlocked-sm-s911uliaxaa/

Galaxy S23



Super fast processing

Snapdragon® 8 Gen 2

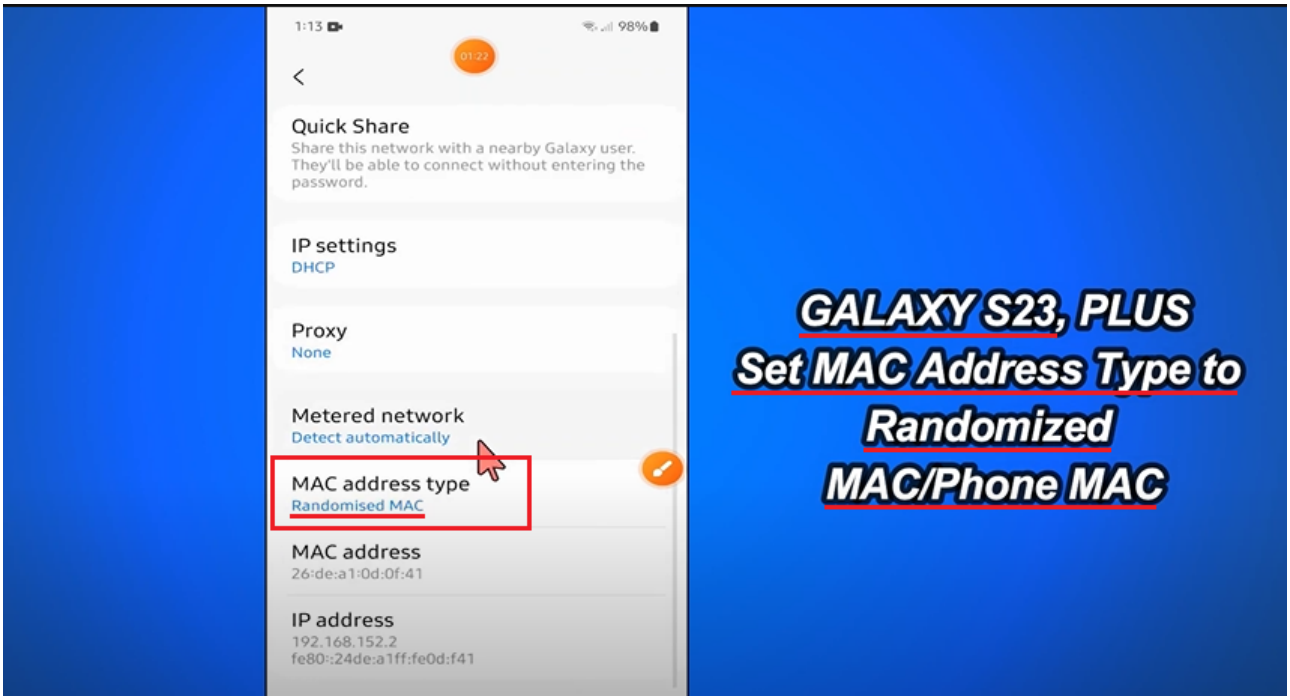
Octa-Core

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

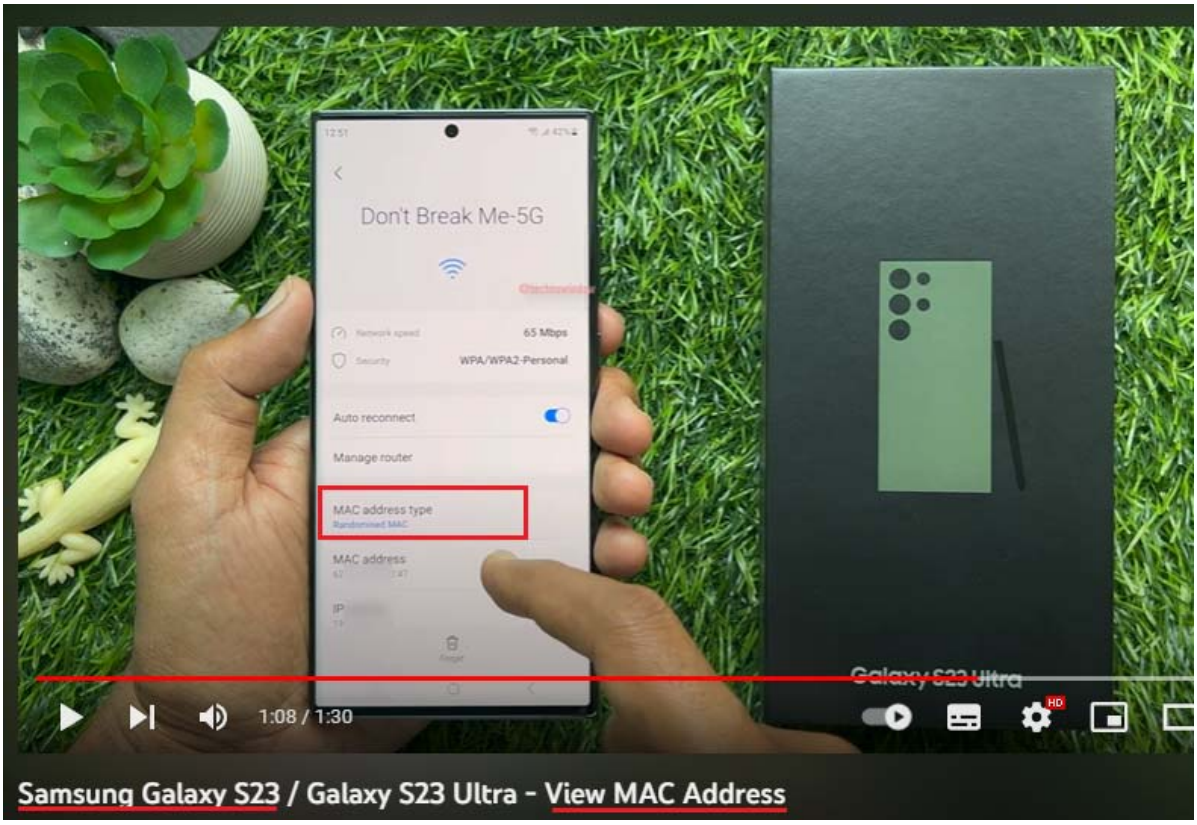
Phone	Galaxy S23	Galaxy S23+	Galaxy S23 Ultra
Chipset	Snapdragon 8 Gen 2 for Galaxy	Snapdragon 8 Gen 2 for Galaxy	Snapdragon 8 Gen 2 for Galaxy
RAM & Storage	8+128GB, 8+256GB (UFS 3.1)	8+256GB, 8+512GB (UFS 4.0)	8+256GB, 12+512GB, 12GB+1TB (UFS 4.0)
Display	6.1" FHD+ Dynamic AMOLED 2x, 120Hz Adaptive 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	Android 13 / One UI 5.1	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



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



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

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

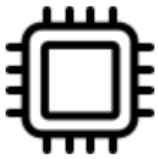
https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/Snapdragon-8-Gen-2-Product-Brief.pdf

- 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

91. The Accused Instrumentalities receive a fake device identifier (e.g., a randomized MAC address) from a mobile operating server (e.g., components for providing services of the Android operating system, including MAC randomization). The Accused Instrumentalities include the Android operating system version 10 or later and include functionality for using randomized MAC addresses for Wi-Fi connections. By way of example, the Galaxy S23 includes the Android 13 operating system. The operating system provides a persistent randomized MAC address to be used with a Wi-Fi network, which is received to perform Wi-Fi connections.

Galaxy S23



Super fast processing

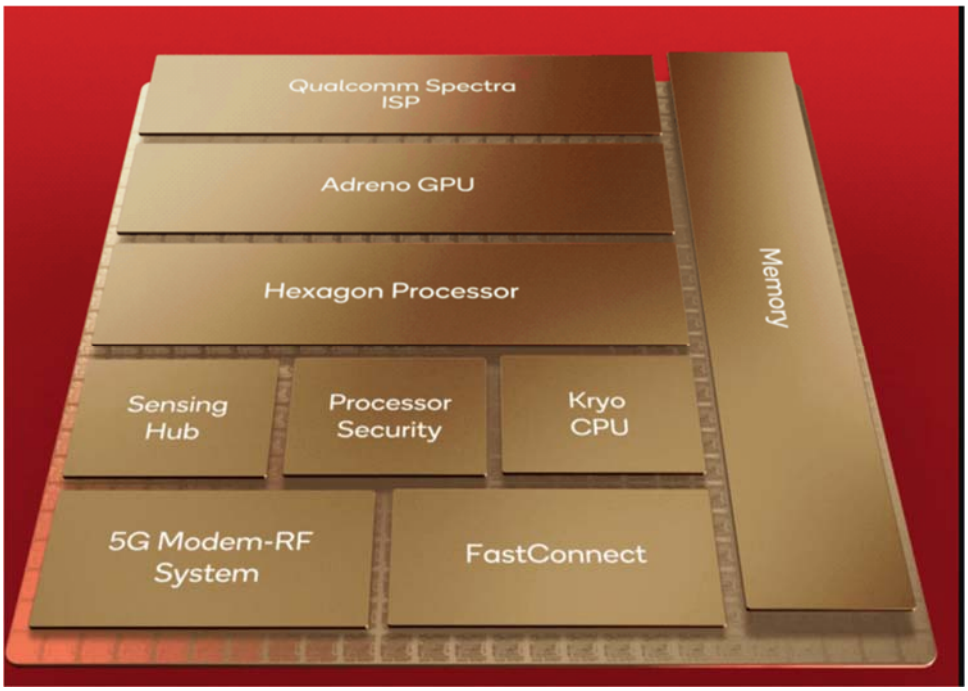
Snapdragon® 8 Gen 2

Octa-Core

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

Phone	Galaxy S23	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	Android 13 / One UI 5.1	Android 13 / One UI 5.1	Android 13 / One UI 5.1

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



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

Phone	Galaxy S23	Galaxy S23+	Galaxy S23 Ultra
Connectivity	5G, Wi-Fi 6E, 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

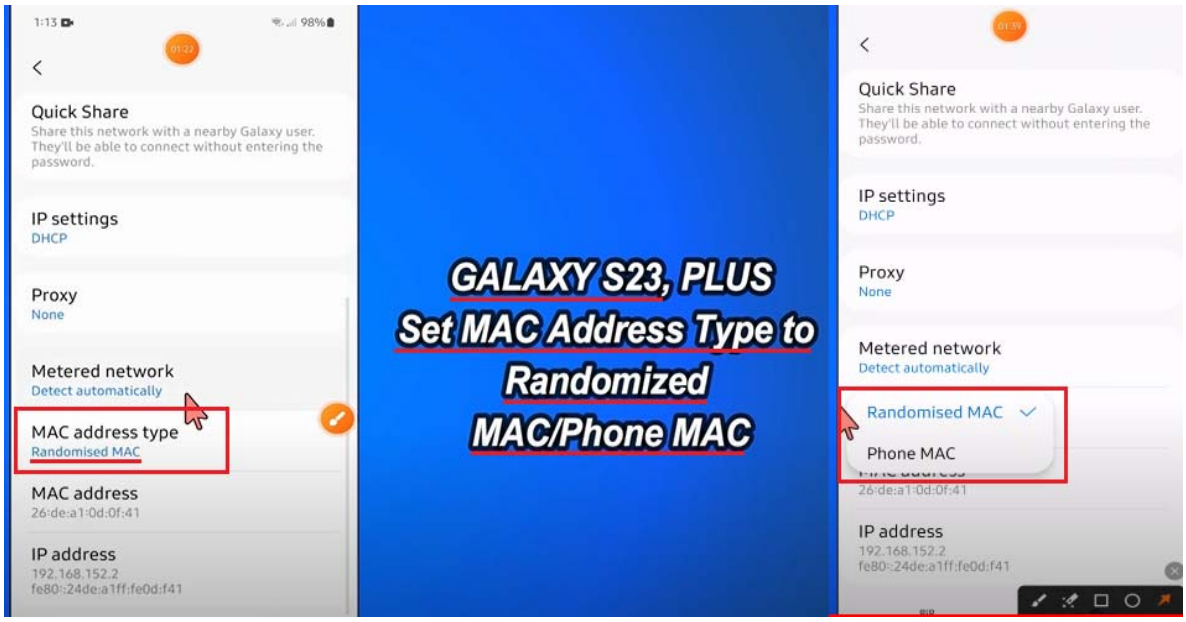
Wi-Fi 6E

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-Active[3], 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

92. The Accused Instrumentalities transmit, to an access point, a probe request frame that includes the fake device identifier for the end device. The Accused Instrumentalities support the Wi-Fi standard. According to the standard, a UE (e.g., the Accused Instrumentality) inquires about available Wi-Fi access points using a probe request. The Accused Instrumentalities include the fake device identifiers in the probe request. The Accused Instrumentality receives the probe responses from multiple available access points. It selects a desired access point for connection based on, for example, the access point capabilities or the desired network condition.

> **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 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).

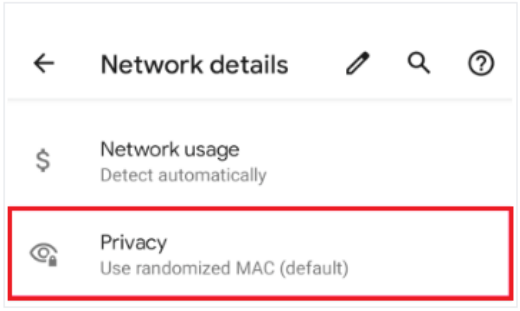


Figure 1. MAC randomization option.

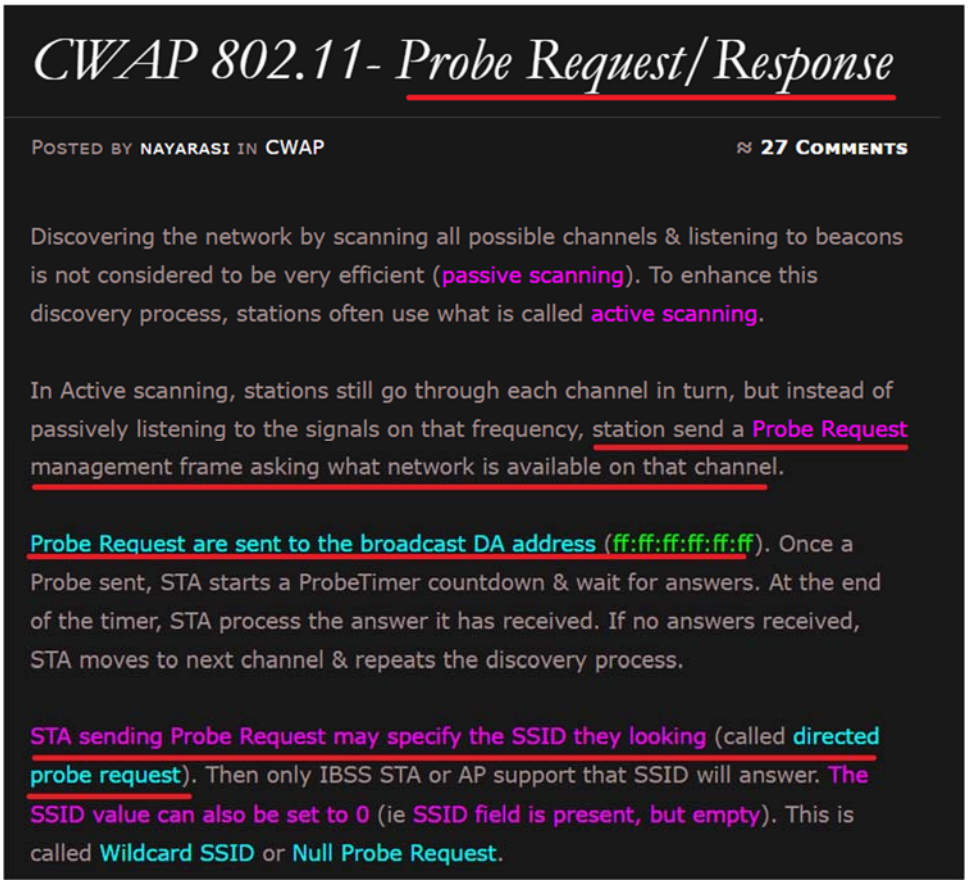
https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior

93. The probe request comprises a sender address field (e.g., a device identifier). The UE (e.g., the Accused Instrumentality) utilizes a random MAC address as the sender address in a probe request. The Accused Instrumentality receives probe responses from available access points. It selects a desired access point for connection based on, for example, the access point capabilities or desired network condition.

94. The Accused Instrumentalities transmit probe requests to identify available access points.

> 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



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

95. A Wi-Fi probe request includes the Accused Instrumentality'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

96. The Wi-Fi probe request of the Accused Instrumentalities includes 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).

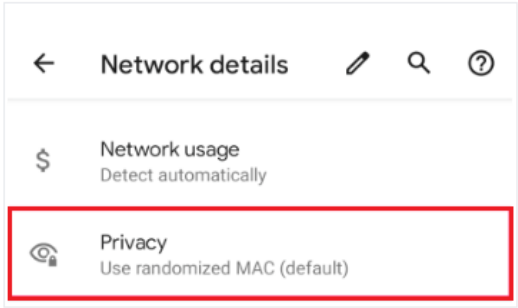


Figure 1. MAC randomization option.

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

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

97. The Accused Instrumentalities receive from the access point (e.g., a Wi-Fi access point), a probe response frame (e.g., a Wi-Fi probe response) that includes information (e.g., SSID, supported data rates, etc.) regarding the access point (e.g., a Wi-Fi access point). A Wi-Fi probe response includes, for example, the SSID (wireless network name) or supported data rates 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

98. The Accused instrumentalities support the Wi-Fi standard. The Accused Instrumentalities receive the probe responses from multiple available access points. 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.

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 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).

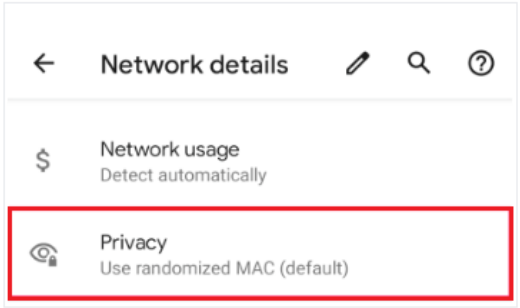


Figure 1. MAC randomization option.

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

MAC Randomization Behavior

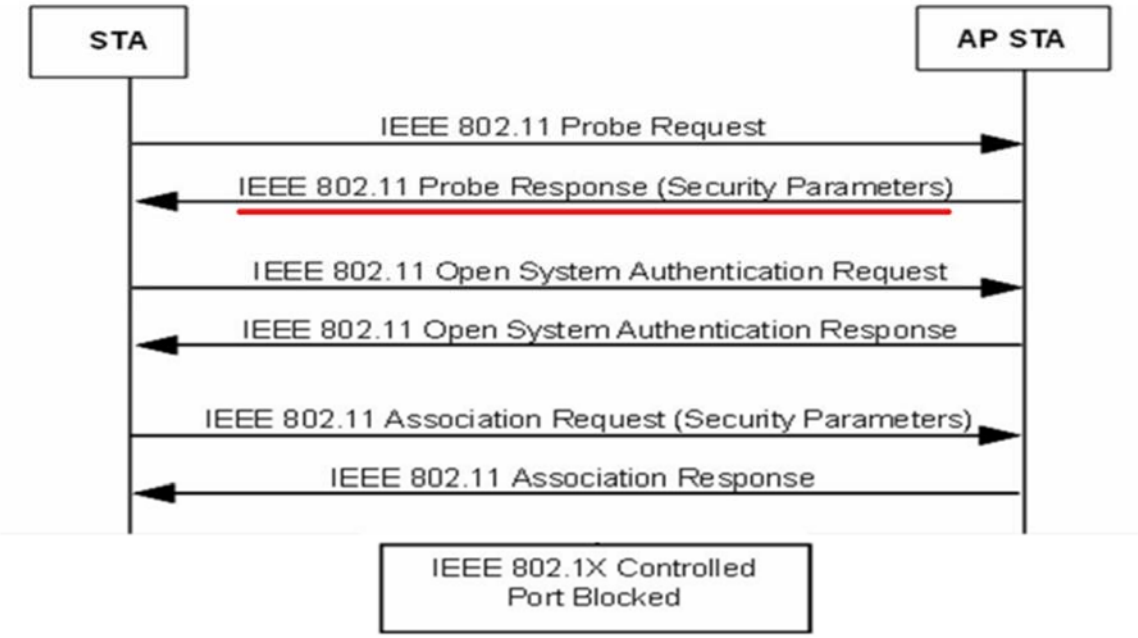
The MAC randomization feature allows devices to use a randomized MAC address when connecting to a Wi-Fi network. For implementation instructions, see Implementing MAC Randomization. This page describes the behavior of MAC randomization in Android.

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



Source: IEEE 802.11-2012.pdf at p. 84.

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 dot11QosOption-Implemented 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/

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 dot11ExendedChannelSwitchActivated 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://mrncciew.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 at p. 59.

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 at p. 979.

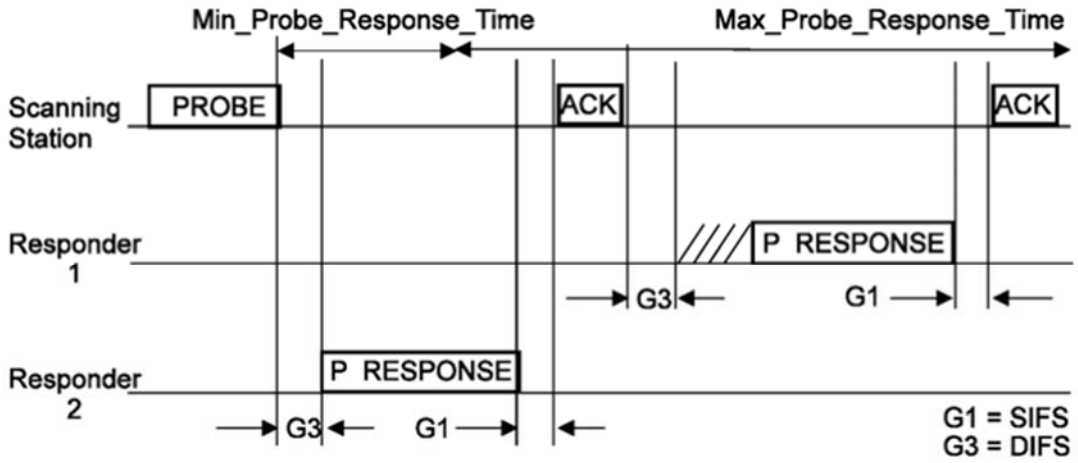


Figure 10-3—Probe response

Source: IEEE 802.11-2012.pdf at p. 980.

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.

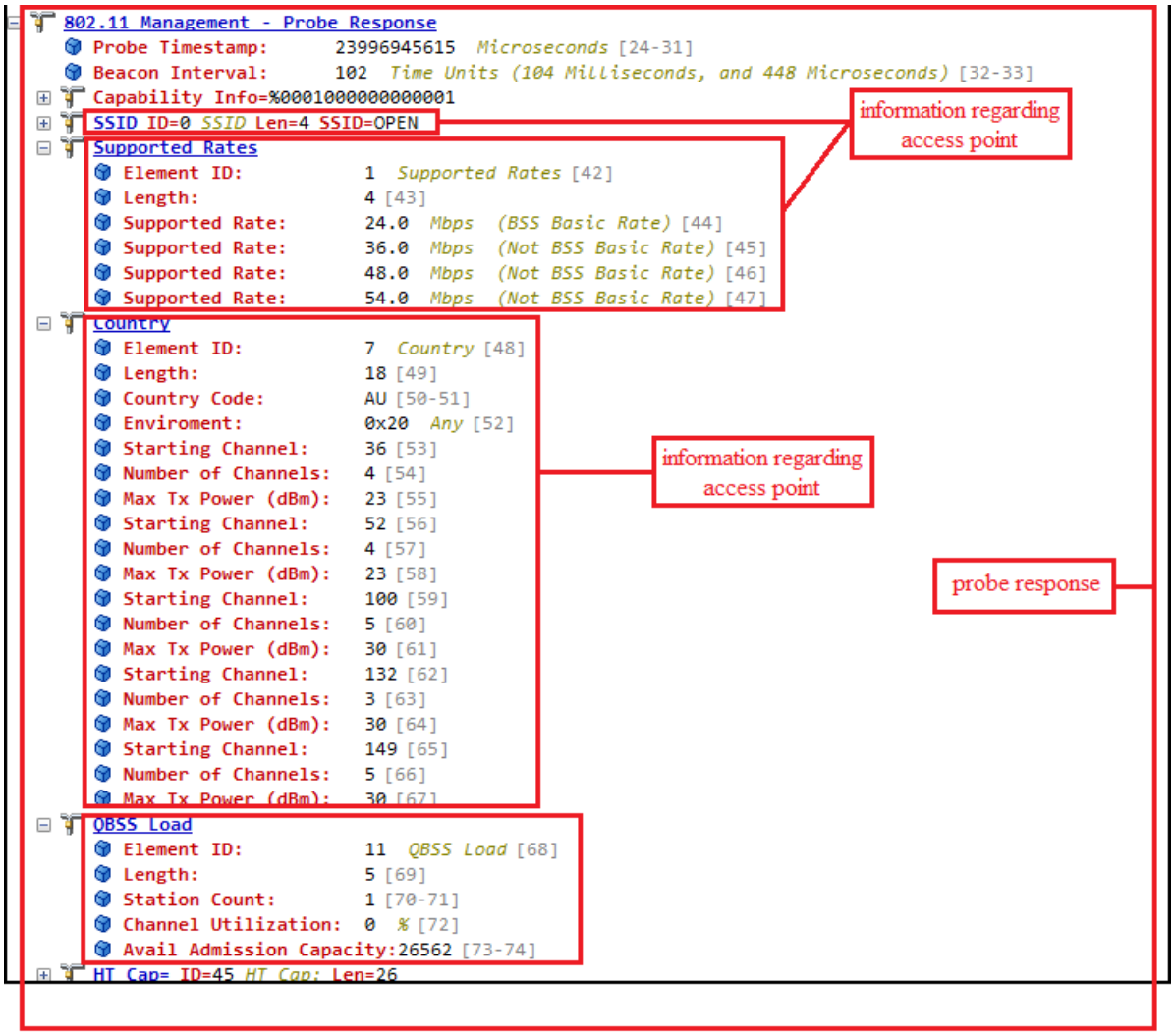
User devices trying to connect to a Wi-Fi network watch for access points (APs) broadcasting its availability for a device to connect to its network. Within that information contains the network name, or Service Set Identifier (SSID). Wi-Fi enabled devices trying to connect to a wireless network, and 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



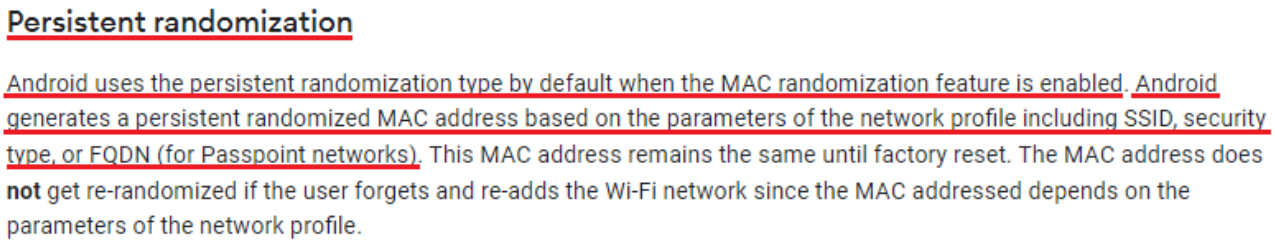
https://mrncciew.com/2014/10/27/cwap-802-11-probe-requestresponse/

99. The Accused Instrumentalities determine that the access point (e.g., a Wi-Fi access point) is an authenticated access point based at least in part on the information (e.g., SSID, supported data rates, etc.) in the probe response frame (e.g., a probe response).

100. The Accused Instrumentalities support the Wi-Fi standard. According to the standard, a UE (e.g., the Accused Instrumentality) inquires about available Wi-Fi access points using a probe request. The probe request comprises a SSID list or preferred network list which is a set of SSIDs to which the Accused Instrumentality was connected previously.

101. The Accused Instrumentalities receive the probe responses from multiple available access points. 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.

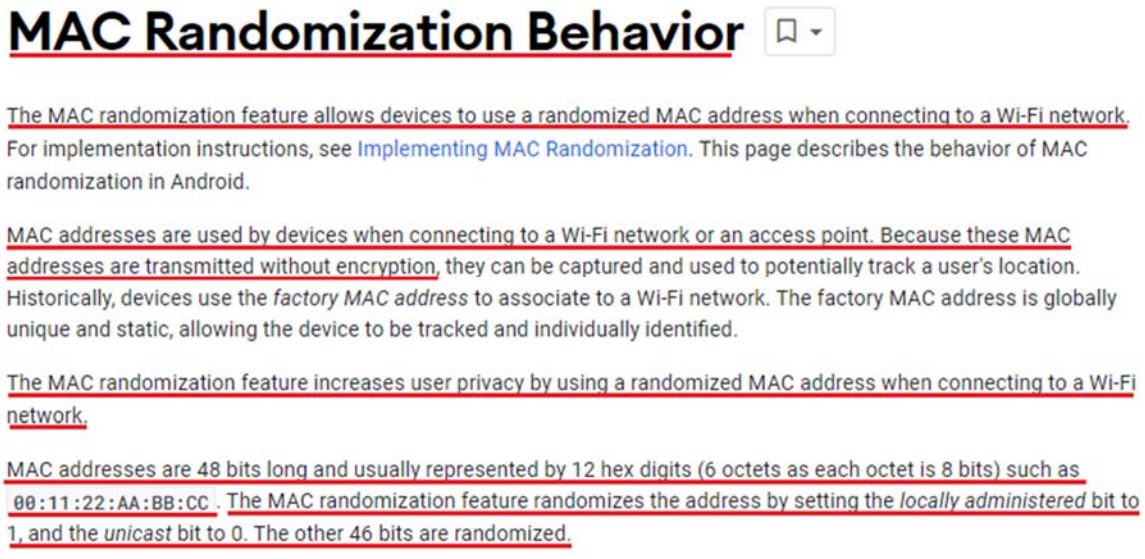
102. The Accused Instrumentalities confirm the received SSID information from the probe responses with access point information stored in their memory. Once confirmed that there is a SSID in a probe response from an access point with which the Accused Instrumentality was connected previously, the Accused Instrumentality initiates the authentication process with stored pre-shared key information and previously used authenticated MAC address, using persistent randomization.



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 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).

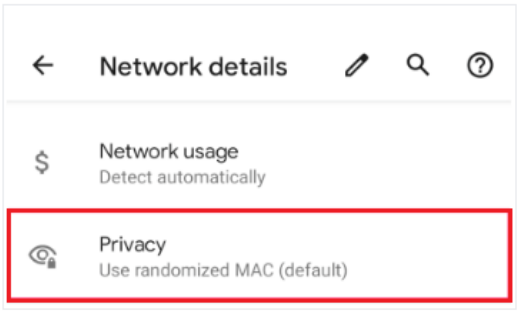


Figure 1. MAC randomization option.

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

MAC Randomization Behavior

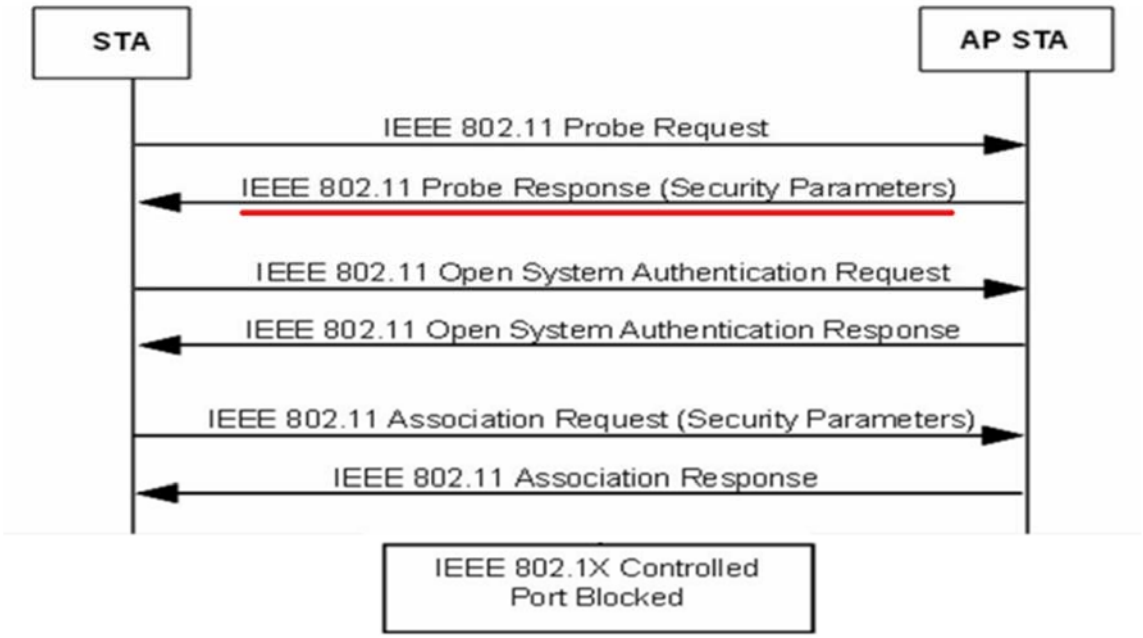
The MAC randomization feature allows devices to use a randomized MAC address when connecting to a Wi-Fi network. For implementation instructions, see Implementing MAC Randomization. This page describes the behavior of MAC randomization in Android.

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



Source: IEEE 802.11-2012.pdf at p. 84.

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 dot11QosOption-Implemented 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/

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

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 dot11MgmtOptionUTCTSFOffsetActivated is true.
43	Time Zone	The Time Zone element is present if dot11MgmtOptionUTCTSFOffsetActivated 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/

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 at p. 59.

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 at p. 979.

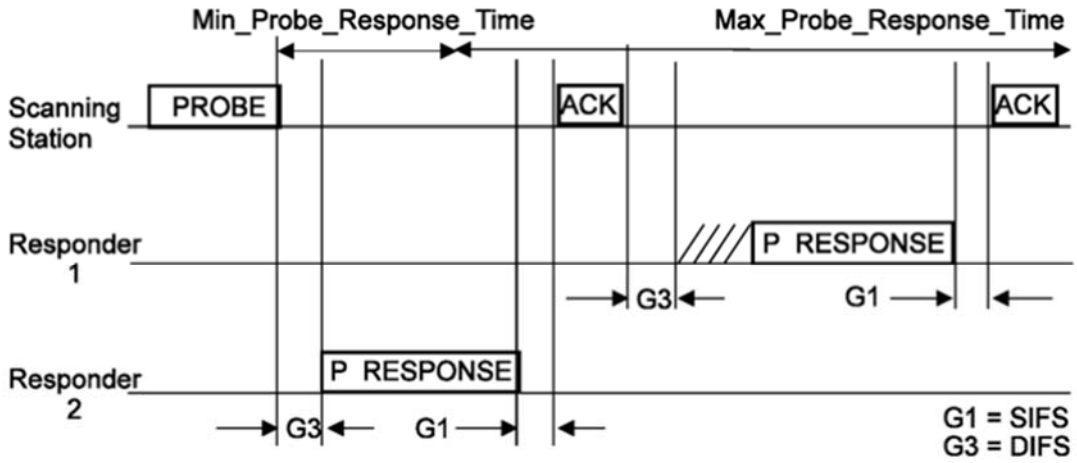


Figure 10-3—Probe response

Source: IEEE 802.11-2012.pdf at p. 980.

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.

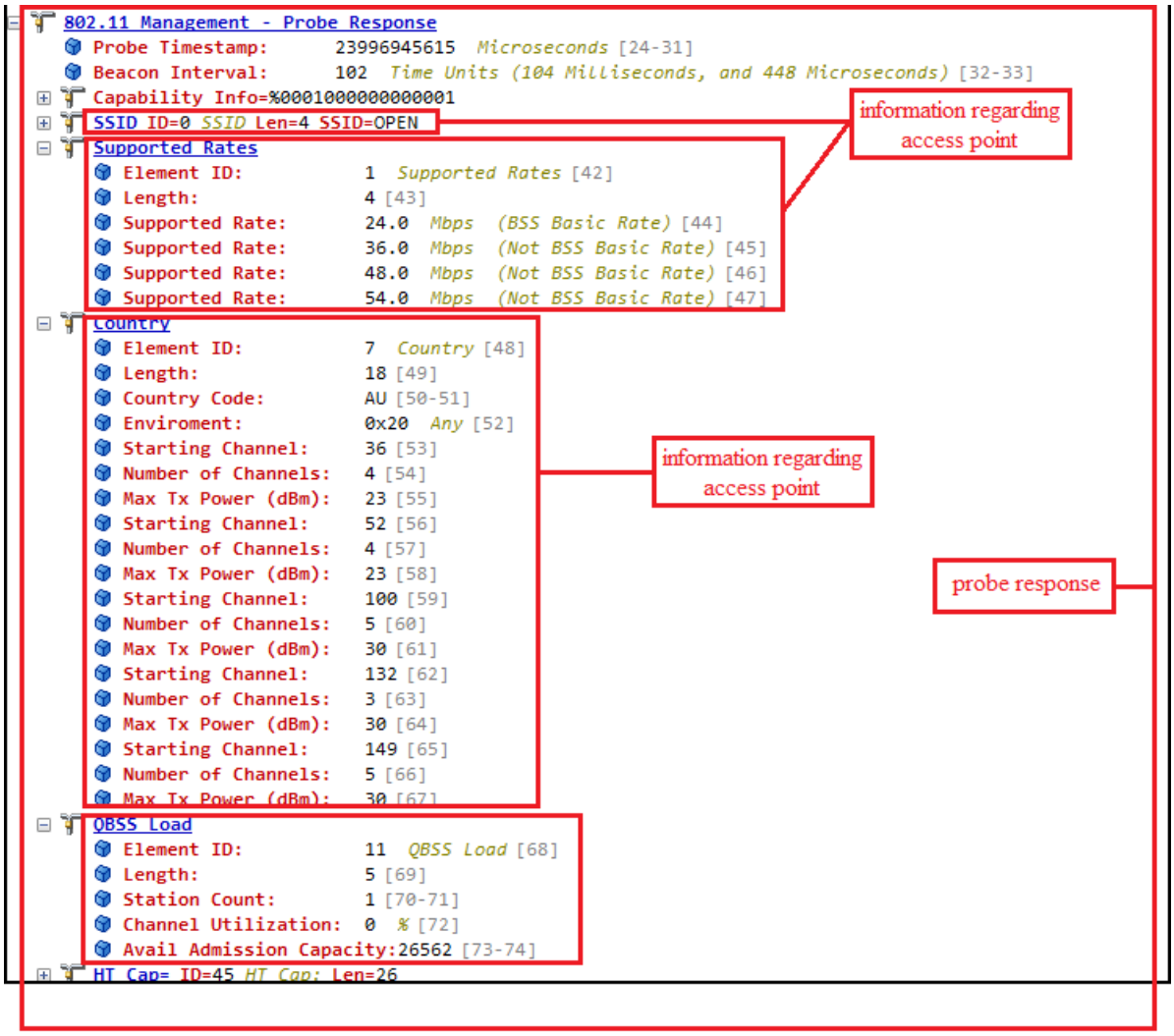
User devices trying to connect to a Wi-Fi network watch for access points (APs) broadcasting its availability for a device to connect to its network. Within that information contains the network name, or Service Set Identifier (SSID). Wi-Fi enabled devices trying to connect to a wireless network, and 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



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

103. The Accused Instrumentalities disclose persistent randomization, in which for the same Wi-Fi network and device combination, the MAC address remains the same. When the Accused Instrumentality connects to a Wi-Fi network to which it was previously connected, it will use the same MAC address.

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 addressed 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: 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">&amp;quot;AndroidWifi&amp;quot;NONE</string>
8                  <string name="SSID">&amp;quot;AndroidWifi&amp;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

104. The Accused Instrumentalities determine that an access point (e.g., a Wi-Fi access point) is authenticated such that the access point is controlled by the mobile operating server and the access point was connected with the end device (e.g., the the Accused Instrumentality) previous to when the access point received the transmitted probe request frame (e.g., a probe request).

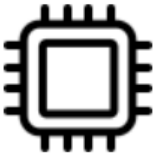
105. The Accused Instrumentalities support the Wi-Fi standard. According to the standard, a UE (e.g., the Accused Instrumentality) inquires about available Wi-Fi access points using a probe

request. The probe request comprises a SSID list or preferred network list which is a set of SSIDs to which the UE (e.g., the Accused Instrumentality) was connected previously.

106. The Accused Instrumentalities 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.

107. The Accused Instrumentalities confirm the received SSID information from the probe responses with the access point information stored in memory. Once confirmed that there is a SSID in a probe response from an access point with which the Accused Instrumentality was connected previously, the Accused Instrumentality initiates the authentication process with stored pre-shared key information and previously used authenticated MAC address, using persistent randomization. The connection of the Accused Instrumentality with the access point is controlled by the mobile operating server, as it controls what, if any, information is provided by the access point, including a probe response.

Galaxy S23



Super fast processing

Snapdragon® 8 Gen 2

Octa-Core

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

Phone	Galaxy S23	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	Android 13 / One UI 5.1	Android 13 / One UI 5.1	Android 13 / One UI 5.1

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

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 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).

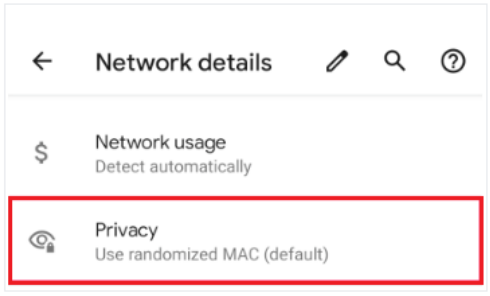


Figure 1. MAC randomization option.

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

MAC Randomization Behavior

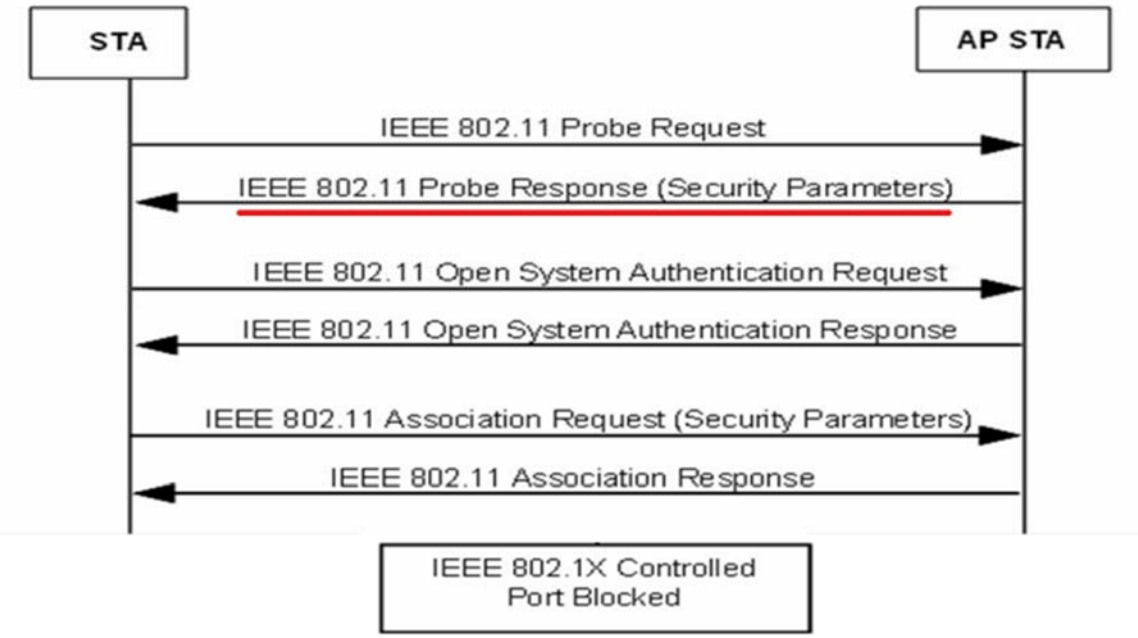
The MAC randomization feature allows devices to use a randomized MAC address when connecting to a Wi-Fi network. For implementation instructions, see Implementing MAC Randomization. This page describes the behavior of MAC randomization in Android.

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



Source: IEEE 802.11-2012.pdf at p. 84.

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 dot11QosOption-Implemented 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/

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 dot11ExendedChannelSwitchActivated 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://mrncciew.com/2014/10/27/cwap-802-11-probe-requestresponse/

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 dot11MgmtOptionUTCTSFOffsetActivated is true.
43	Time Zone	The Time Zone element is present if dot11MgmtOptionUTCTSFOffsetActivated 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/

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 at p. 59.

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 at p. 979.

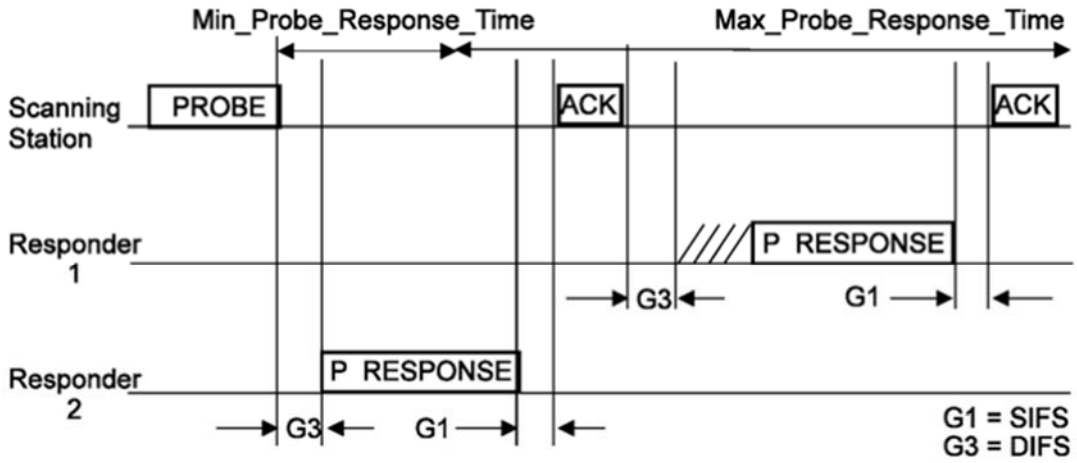


Figure 10-3—Probe response

Source: IEEE 802.11-2012.pdf at p. 980.

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.

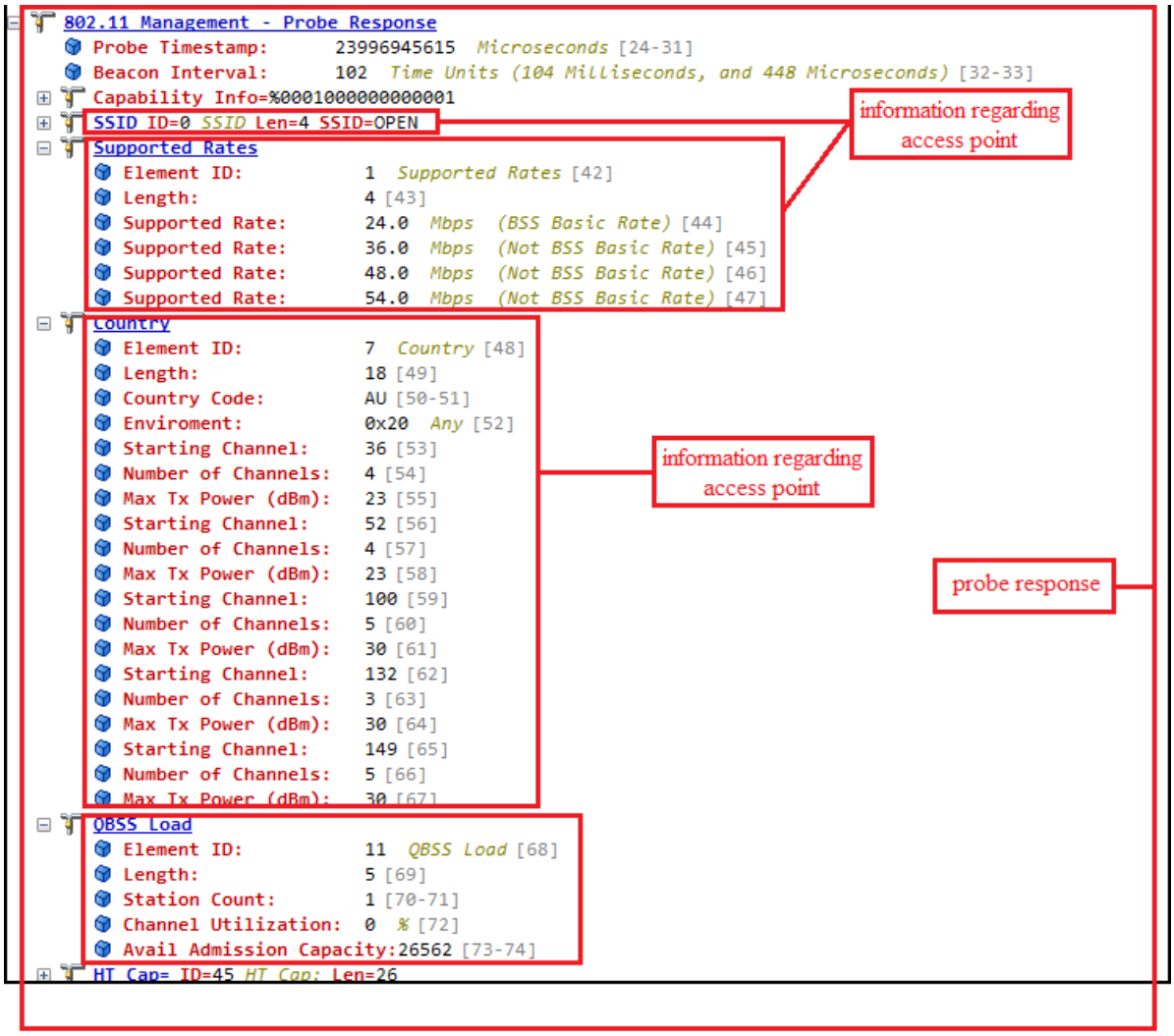
User devices trying to connect to a Wi-Fi network watch for access points (APs) broadcasting its availability for a device to connect to its network. Within that information contains the network name, or Service Set Identifier (SSID). Wi-Fi enabled devices trying to connect to a wireless network, and 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



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

108. The Accused Instrumentalities include functionality for persistent randomization, in which for the same Wi-Fi network and device combination, the MAC address remains the same. When the Accused Instrumentality connects to a Wi-Fi network to which it was previously connected, it will use the same MAC address.

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 addressed 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: 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">&amp;quot;AndroidWifi&amp;quot;NONE</string>
8                  <string name="SSID">&amp;quot;AndroidWifi&amp;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" />
```

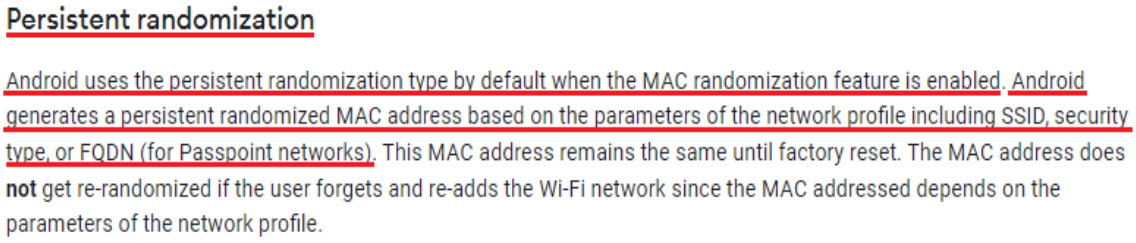
https://android.googlesource.com/device/generic/goldfish/+/refs/tags/android-9.0.0_r34/wifi/WifiConfigStore.xml

109. The Accused instrumentalities transmit to the access point (e.g., a Wi-Fi access point) determined to be the authenticated access point (e.g., a previously connected Wi-Fi access point), a connection request (e.g., an association request) that includes an authentic device identifier (e.g., a previously authenticated MAC address) for the end device (e.g., the Wi-Fi chipset of the Accused Instrumentality).

110. The Accused Instrumentalities support the Wi-Fi standard. According to the standard, a UE (e.g., the Accused Instrumentality) inquires about available Wi-Fi access points using a probe request. The probe request comprises a SSID list or preferred network list which is a set of SSIDs to which the UE (e.g., the Accused Instrumentality) was connected previously.

111. The Accused Instrumentalities receive the probe responses from multiple available access points. 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.

112. The Accused Instrumentalities confirm the received SSID information from the probe responses with the access point information stored in memory. Once confirmed that there is a SSID in a probe response from an access point with which the Accused Instrumentality was connected previously, the Accused Instrumentality initiates the authentication process with a stored pre-shared key. The Accused Instrumentality sends further authentication and association messages using stored key information and previously used authenticated MAC address, using persistent randomization.



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 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).

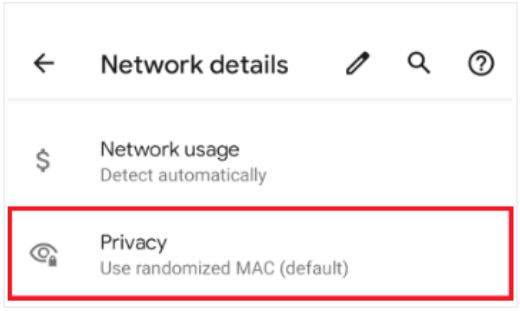


Figure 1. MAC randomization option.

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

MAC Randomization Behavior

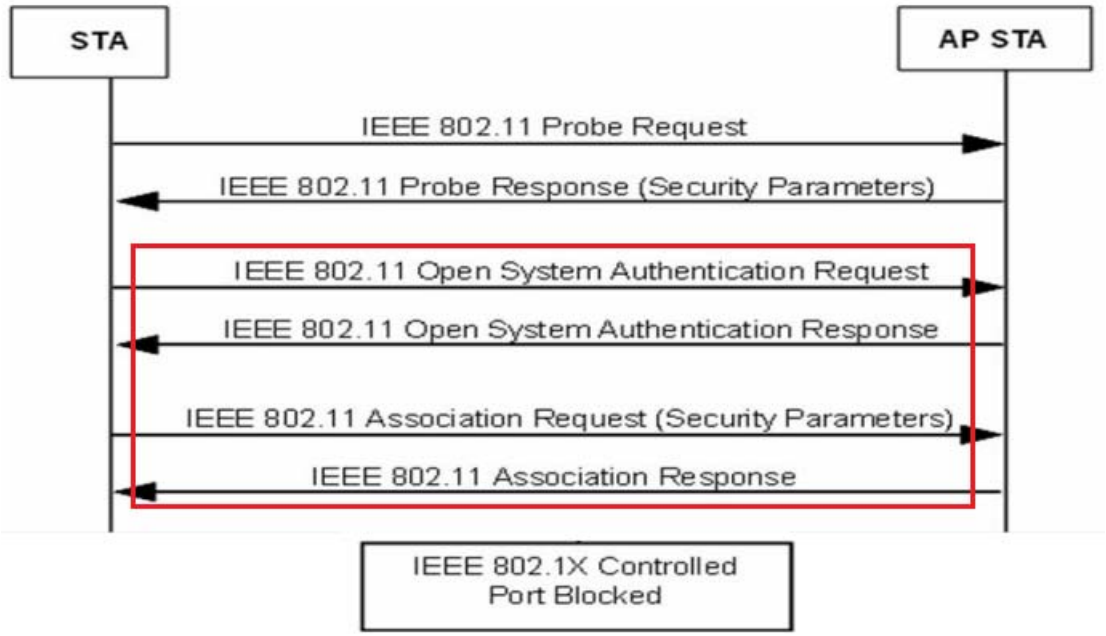
The MAC randomization feature allows devices to use a randomized MAC address when connecting to a Wi-Fi network. For implementation instructions, see Implementing MAC Randomization. This page describes the behavior of MAC randomization in Android.

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.

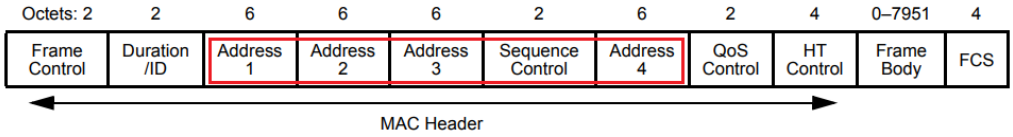
https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior

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



Source: IEEE 802.11-2012.pdf at p. 84.

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 at p. 381.

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 at p. 388.

802.11 Mgmt : Authentication Frame

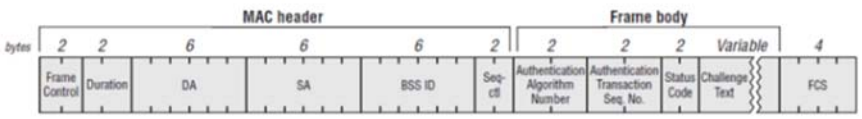
POSTED BY NAYARASI IN CWAP ≈ 10 COMMENTS

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

113. The Accused Instrumentalities include functionality for persistent randomization, in which for the same Wi-Fi network and device combination, the MAC address remains the same. When the Accused Instrumentality connects to a Wi-Fi network to which it was previously connected, it will use the same MAC address.

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 addressed 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: 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="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

114. By making, using, offering for sale, selling and/or importing into the United States the Accused Instrumentalities, Samsung has injured and continues to injure Secure Wi-Fi and is liable for infringement of the '005 patent pursuant to 35 U.S.C. § 271(a).

115. In addition, and/or in the alternative to direct infringement, Defendants have also infringed and continue to infringe the claims of the '005 patent by, among other things, actively inducing others to use the Accused Instrumentalities in violation of 35 U.S.C. § 271(b).

116. Samsung's users, customers, consumers, agents, distributors, and other third parties who use, sell, offer to sell, and/or import the Accused Instrumentalities in accordance with Samsung's instructions infringe the claims of the '005 patent, in violation of 35 U.S.C. § 271(a). Samsung intentionally instructs its customers to infringe through support information such as websites, videos, demonstrations, support information and other published information. For example, Samsung's website instructs and encourages its customers to use, manage and control the infringing components and functionalities of the Accused Instrumentalities. *See*, *e.g.*, https://www.samsung.com/us/smartphones/galaxy-s23/specs/ (advertising the Wi-Fi capabilities of Accused Instrumentalities); https://downloadcenter.samsung.com/content/UM/202302/20230207045923682/SAM_S911_S916_S918_EN_UM_OS13_020223_FINAL.pdf, at 3, 119 (advertising and instructing users to connect perform Wi-Fi connections); *id*. at 121-122 (advertising and instructing Wi-Fi connections); https://www.samsung.com/my/support/mobile-devices/how-to-connect-wi-fi-network-on-my-samsung-device/ ("How to connect to Wi-Fi network on my Samsung Device."); *id*. at 16 (encouraging users to "make full use of [their] device's Android features").

117. The Accused Instrumentalities implement infringing functionality by default when connecting to a Wi-Fi network. *See, e.g.*, https://source.android.com/docs/core/connect/wifi-mac-

randomization-behavior. The Accused Instrumentalities are designed and intended to perform MAC randomization for Wi-Fi connections and necessarily infringe the '005 patent in the normal, intended manner without any additional specific action of the end user other than connecting to a Wi-Fi network.

118. Thus, Samsung actively instructs and directs its customers to infringe and actively encourages infringement by its customers. Samsung is thereby liable for infringement of the '005 patent under 35 U.S.C. § 271(b).

119. At a minimum, Samsung has had knowledge of the '005 patent since at least March 26, 2018, when it affirmatively discussed and quoted U.S. Patent Publication No. 2014/0140331 in connection with the prosecution of U.S. Application No. 14/664,289. By March 26, 2018, the '005 patent had issued. Samsung analyzed and discussed U.S. Application No. 14/664,289 after the '005 patent issued. Samsung thus had knowledge of the '005 patent at least as early as March 26, 2018. Samsung has also had knowledge of the '005 patent since at least the filing and/or service date of the Complaint in this action. Despite this knowledge, Samsung has continued to engage in activities to encourage and assist its customers, consumers, agents, distributors, and other third parties in the use, sale, offer for sale, and/or importation of the Accused Instrumentalities. Thus, on information and belief, Samsung (1) had actual knowledge of the patent; (2) knowingly induced its customers to infringe the patent; and (3) had specific intent to induce the patent infringement.

120. Additionally, and/or alternatively, Samsung is liable as a contributory infringer of the '005 patent under 35 U.S.C. § 271(c) by having offered to sell, sold and imported and continuing to offer to sell, selling, and importing into the United States the Accused Instrumentalities and reasonably similar products, to be especially made or adapted for use in infringement of the '005 patent. The portions of the Samsung Accused Instrumentalities that enable Wi-Fi connections of the

Accused Instrumentalities utilizing MAC randomization constitute a material component for use in practicing the '005 patent and are especially made and are not staple articles of commerce suitable for non-infringing use.

121. Secure Wi-Fi has complied with 35 U.S.C. § 287 because Secure Wi-Fi does not make, offer for sale or sell products that practice the '005 patent during the relevant time period.

122. As a result of Samsung's direct and indirect infringement of the '005 patent, Secure Wi-Fi is entitled to monetary damages (past, present and future) in an amount adequate to compensate for Samsung's infringement, but in no event less than a reasonable royalty for the use made of the invention by Samsung, together with interest and costs as fixed by the Court.

123. On information and belief, despite having knowledge of the '005 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '005 patent, Samsung has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Samsung's infringing activities relative to the '005 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, and an egregious case of misconduct beyond typical infringement such that Secure Wi-Fi is entitled to enhanced damages under 35 U.S.C. § 284 up to three times the amount found or assessed.

124. Samsung's acts of direct and indirect infringement have caused and continue to cause damage to Secure Wi-Fi. Secure Wi-Fi is entitled to damages in accordance with 35 U.S.C. §§ 271, 281, and 284 sustained as a results of Samsung's wrongful acts in an amount to be proven at trial.

PRAYER FOR RELIEF

Secure Wi-Fi respectfully requests that the Court find in favor of Secure Wi-Fi and against Samsung, and the Court grant Secure Wi-Fi the following relief:

A. For judgment that Samsung is liable for infringement of one or more claims of the Asserted Patents, directly and/or indirectly, either literally and/or under the doctrine of equivalents;

B. For judgment that Samsung has willfully infringed one or more claims of the Asserted Patents, directly and/or indirectly, either literally and/or under the doctrine of equivalents;

C. For an accounting of all damages sustained by Secure Wi-Fi as the result of Samsung's acts of infringement, including compensatory damages in an amount according to proof, and in no event less than a reasonable royalty;

D. For a mandatory future royalty payable on each and every future sale by Samsung of a product that is found to infringe one or more of the Asserted Patents and on all future products which are reasonably similar to those products found to infringe;

E. For a judgment and order requiring Samsung to pay Secure Wi-Fi's damages, costs, expenses, and pre- and post-judgment interest for its infringement of the Asserted Patents as provided under 35 U.S.C. § 284;

F. For a judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Secure Wi-Fi its reasonable attorneys' fees; and

G. For such other and further relief in law and in equity as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Secure Wi-Fi hereby demands a trial by jury of this action.

Dated: January 25, 2024

Respectfully submitted,

/s/ Marc Belloli

Marc Belloli (*pro hac vice*)
California Bar No. 244290
mbelloli@bdiplaw.com
M. Elizabeth Day (*admitted in EDTX*)
California Bar No. 177125
eday@bdiplaw.com
Jerry D. Tice II (*admitted in Texas*)
Texas State Bar No. 24093263
jtice@bdiplaw.com
Denise M. De Mory (*admitted in EDTX*)
California Bar No. 168076
ddemory@bdiplaw.com
Aaron R. Hand (*admitted in EDTX*)
California Bar No. 245755
ahand@bdiplaw.com
Gareth DeWalt (*pro hac vice*)
California Bar No. 261479
gdewalt@bdiplaw.com
BUNSOW DE MORY LLP
701 El Camino Real,
Redwood City, CA 94063
Tel: (650) 351-7248
Fax: (415) 426-4744

Deron R. Dacus
Texas Bar No. 00790553
ddacus@dacusfirm.com
THE DACUS FIRM, P.C.
821 ESE Loop 323, Suite 430
Tyler, Texas 75701
(903) 705-1117
(903) 581-2543 (fax)
E-mail: ddacus@dacusfirm.com

Attorneys for Plaintiff
Secure Wi-Fi LLC