EXHIBIT C

EXHIBIT C-INFRINGEMENT CONTENTIONS FOR U.S. PATENT NO. 9,961,552

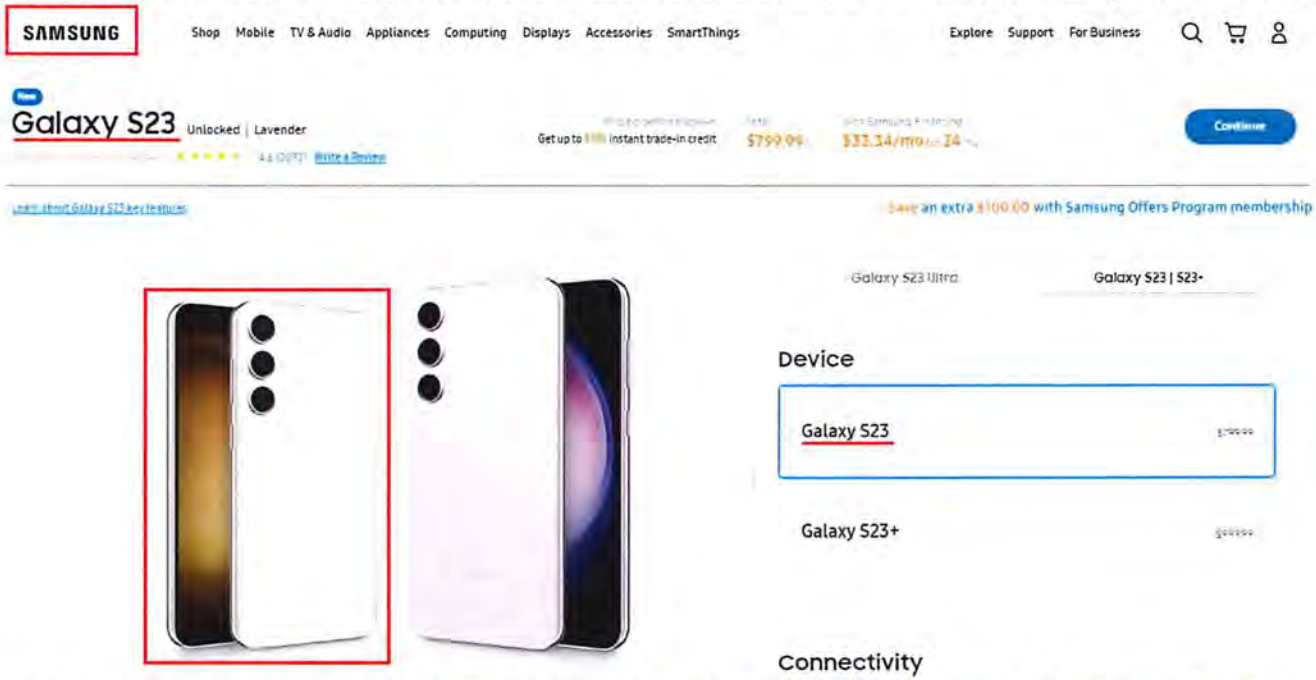
As set forth below, the Accused Products and their referenced structures and functions are designed to and do operate in an infringing manner and perform the claimed systems and methods each and every time an Accused Product is used as intended (i.e., to connect to a Wi-Fi network). The following claim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

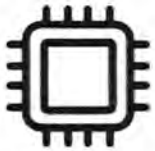
This claim chart specifically addresses infringement of the asserted claims by Samsung's Accused Products using Android OS 10 or above or Wear OS 3 or above. These infringement contentions are illustrative rather than exhaustive. Although the Samsung Accused Products may differ in some respects, for example use of different operating systems, SOCs, mobile platforms, chipsets, and/or connectivity systems, any differences are not relevant with respect to the asserted claims of the '552 patent or Secure Wi-Fi's infringement allegations. On information and belief, the evidence cited in this claim chart is representative of how the other accused products would operate under similar conditions. Excerpts below may be annotated to highlight certain information, aid in readability, or for some other purpose. The annotations are not limiting.

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

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

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

U.S. Patent No. 9,961,552	Samsung Accused Products
10. A method performed by a device, the method comprising	To the extent the preamble is limiting, the Accused Products practice a method performed by a device. The Accused Products include Android OS 10 or above or Wear OS 3 or above. Each Accused Product includes an SoC and Wi-Fi connection functionality. As a specific example shown below, the Galaxy S23 includes the Android 13 operating system, which includes randomized MAC for Wi-Fi connections. It comprises an SoC, Snapdragon 8 Gen 2, a Wi-Fi chipset, and FastConnect. It connects to a Wi-Fi network using the Wi-Fi chipset.  https://www.samsung.com/us/smartphones/galaxy-s23/buy/galaxy-s23-128gb-unlocked-sm-s911uliaxaa/

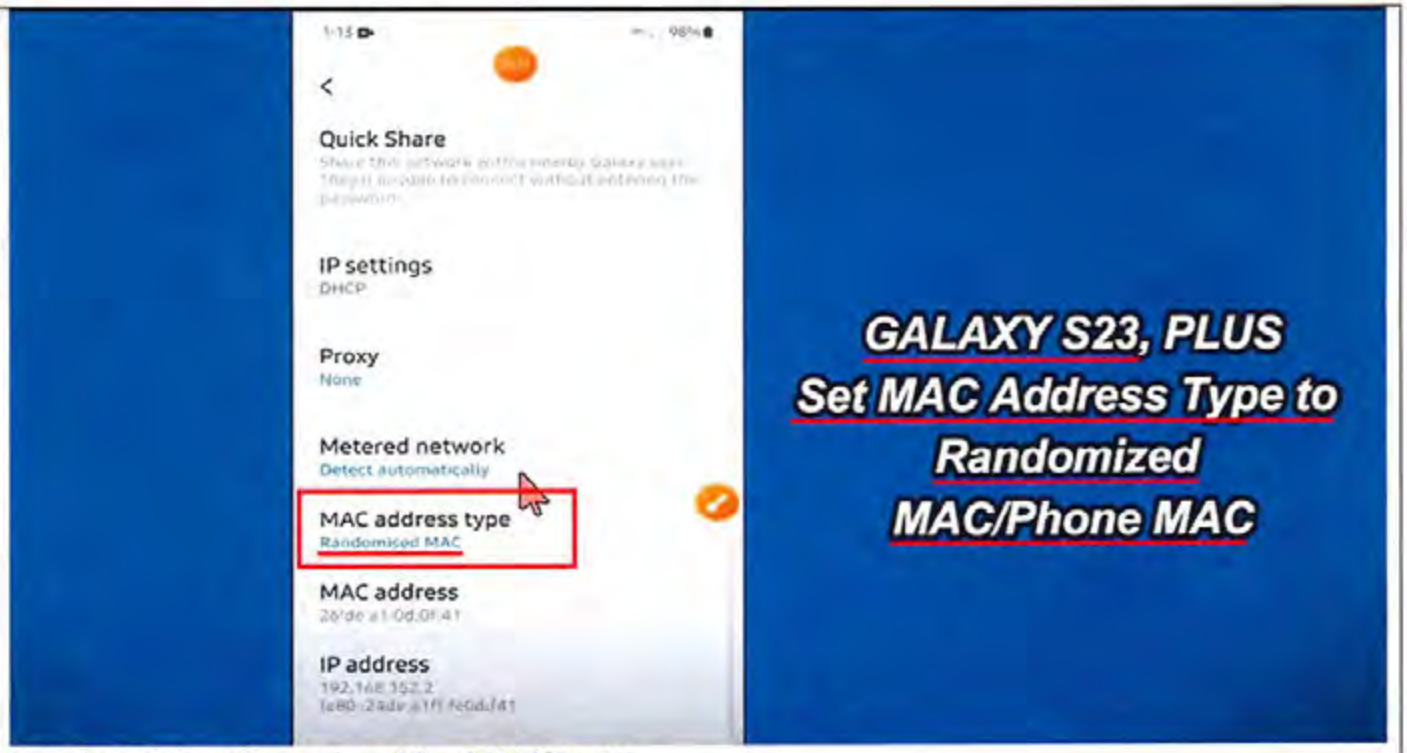
	Galaxy S23  Super fast processing Snapdragon® 8 Gen 2 Octa-Core https://www.samsung.com/us/smartphones/galaxy-s23/specs/

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



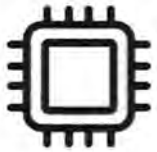
https://www.youtube.com/watch?v=dT63df6nnqU



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

	In Android 10, MAC randomization is enabled by default for client mode, SoftAp, and Wi-Fi Direct. MAC randomization prevents listeners from using MAC addresses to build a history of device activity, thus increasing user privacy. Additionally, MAC addresses are randomized as part of Wi-Fi Aware and Wi-Fi RTT operations. For more information, see MAC Randomization Behavior. https://source.android.com/docs/core/connect/wifi-mac-randomization Wear OS, including Wear OS 3.0, is based on Android. *See* https://developer.android.com/training/wearables/wear-v-mobile#:~:text=Wear%20OS%20is%20based%20on,design%20a%20Wear%20OS%20app. Devices operating on Wear OS 3.0 implement MAC randomization. *See* https://www.reddit.com/r/GalaxyWatch/comments/pcmkj1/galaxy_watch_4_wifi_mac_address/
[10a] receiving, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;	The Accused Products receive, from a server (e.g., the OS and/or a CPU and associated memory for storing and executing the OS and associated data), an authenticated access point list (e.g., previously connected access point list) that includes information (e.g., SSID, supported data rates, pre-shared keys, etc.) regarding one or more access points (e.g., previously connected access point) that are controlled by the server. As shown below, an example of the Accused Products contains an SoC, Snapdragon 8 Gen 2 with a Kryo CPU. Also, it supports Android 13 operating system and has an option for randomized MAC for Wi-Fi connections. The server generates a persistent randomized MAC address to be used with a Wi-Fi network. The server also stores a list of previously connected access points and provides that list to the device in connecting to Wi-Fi access points. The list comprises different information pertaining to previously connected access points such as SSID, pre-shared keys, etc.

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



CPU

Kryo CPU

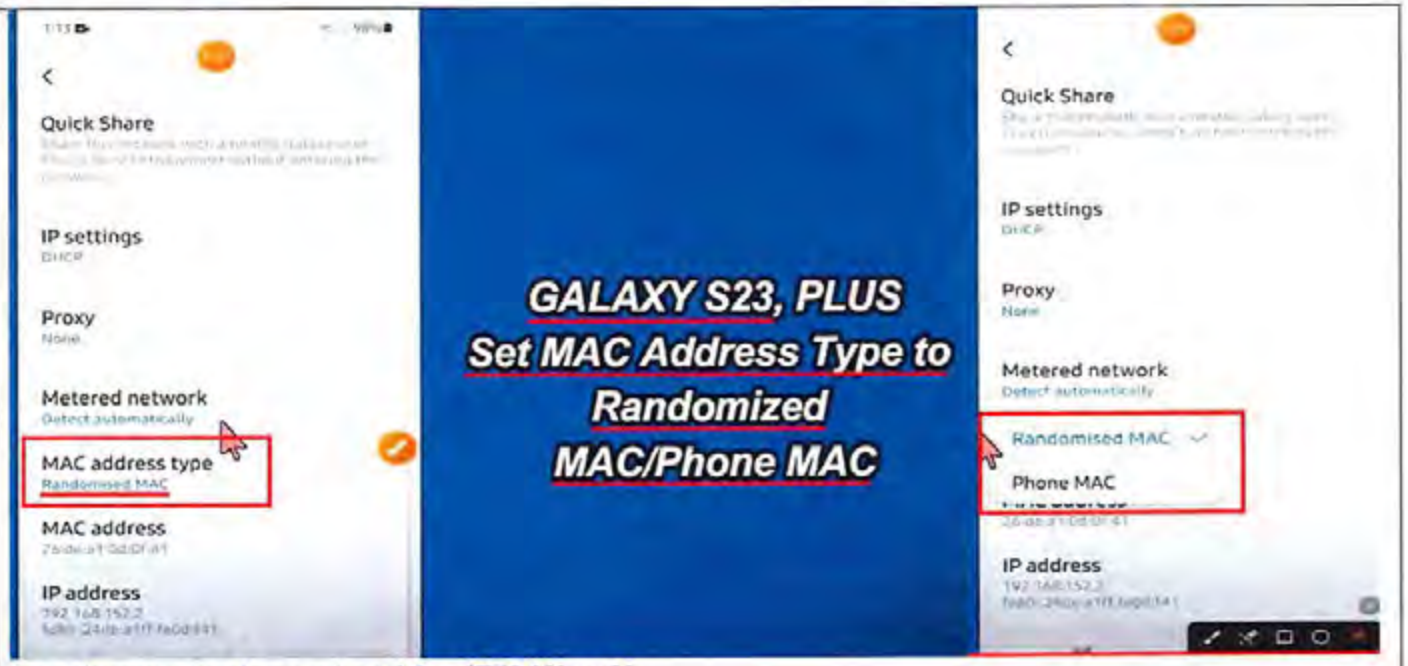
- 64-bit Architecture
- 1 Prime core, up to 3.36 GHz[2]
  - Arm Cortex-X3 technology
- 4 Performance cores, up to 2.8 GHz
- 3 Efficiency cores, up to 2.0 GHz

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

Phone	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

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>
```

previously connected access-points information list

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

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

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]

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

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

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

Source: IEEE 802.11-2012.pdf

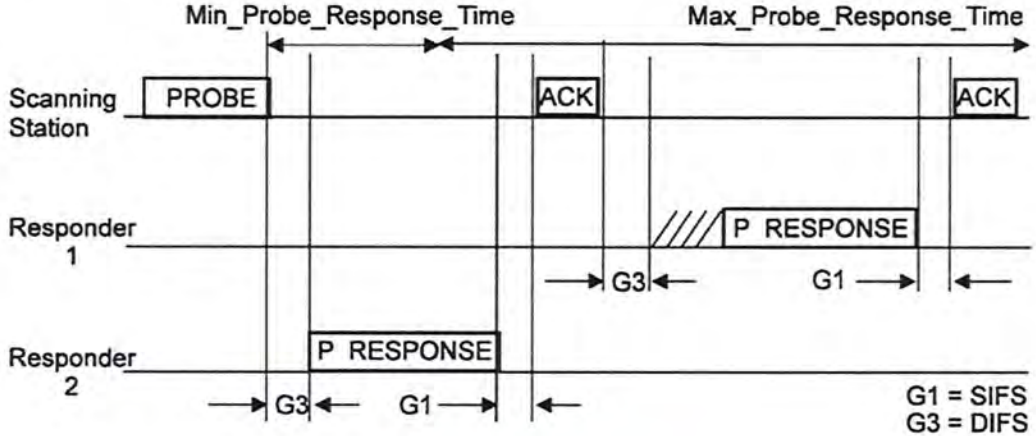
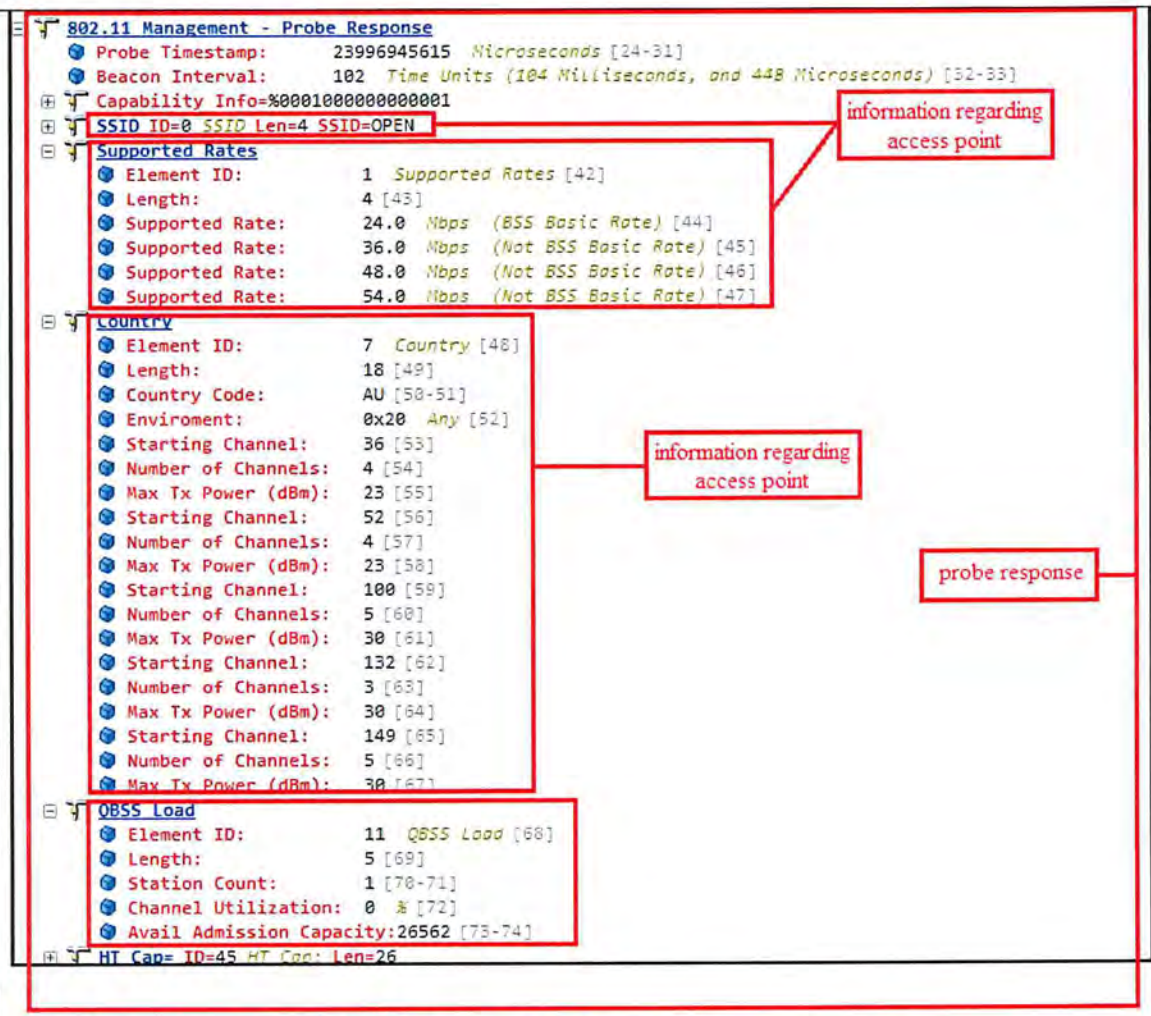


Figure 10-3—Probe response

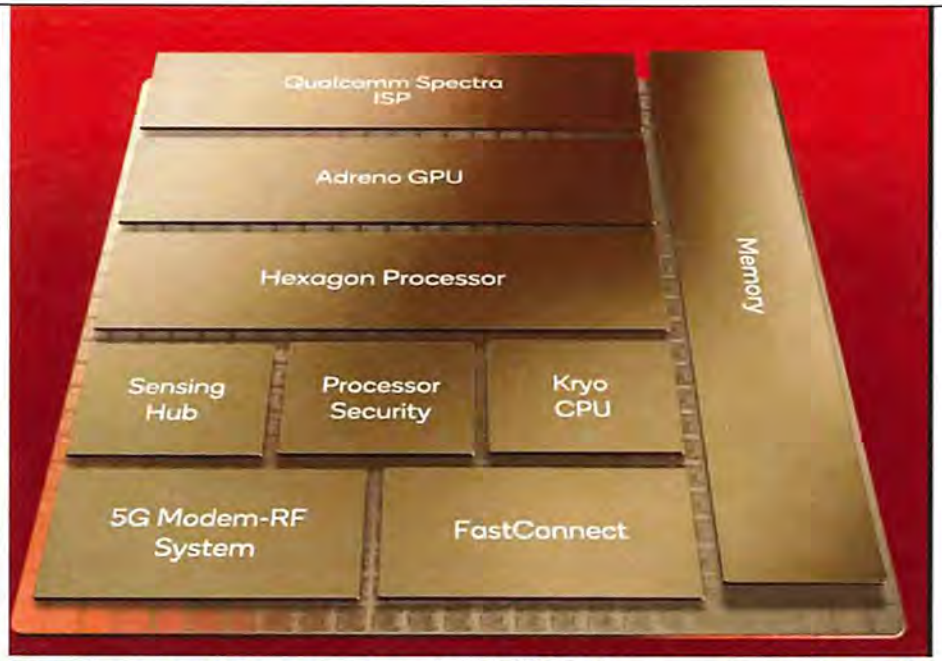
Source: IEEE 802.11-2012.pdf

	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



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

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



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

The access points are controlled by the server. For example, the server, which serves the functionality of the Android operating system, controls connection and/or data transmission of the access points. The Accused Products support the Wi-Fi standard. According to the standard, the Accused Products inquire about available Wi-Fi access points using a probe request, which is generating by the mobile operating server. The probe request comprises identifying information, such as a wildcard SSID or SSID for one or more access points or a preferred network list which is a set of SSIDs to which the UE got connected previously. An access point receiving the probe request must provide a probe response. As a further example, an access point receives and transmits data under control of the mobile operating server.

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

Source: IEEE 802.11-2012.pdf

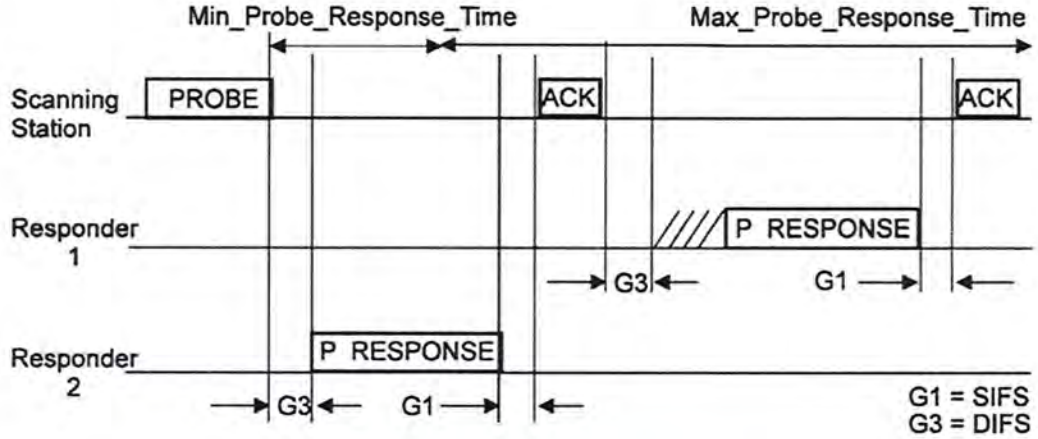
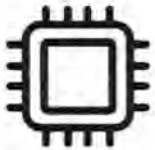


Figure 10-3—Probe response

Source: IEEE 802.11-2012.pdf

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

[10b] receiving, from the server, a fake device identifier for the device, wherein the received fake device identifier includes at least one of one or more random numbers or one or more random characters to falsely identify the device in a probe request frame;	The Accused Products receive from the server, a fake device identifier (e.g., randomized MAC address) for the device, wherein the received fake device identifier includes at least one of one or more random numbers or one or more random characters to falsely identify the device in a probe request frame (e.g., Wi-Fi probe request). The operating system is used to generate a random MAC address for the device. For example, the operating system generates a persistent randomized MAC address to be used with a Wi-Fi network. The operating system runs on a CPU (e.g., the Kryo CPU) of the SoC of the Accused Product. 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/



CPU

Kryo CPU

- 64-bit Architecture
- 1 Prime core, up to 3.36 GHz[2]
  - Arm Cortex-X3 technology
- 4 Performance cores, up to 2.8 GHz
- 3 Efficiency cores, up to 2.0 GHz

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

Phone	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



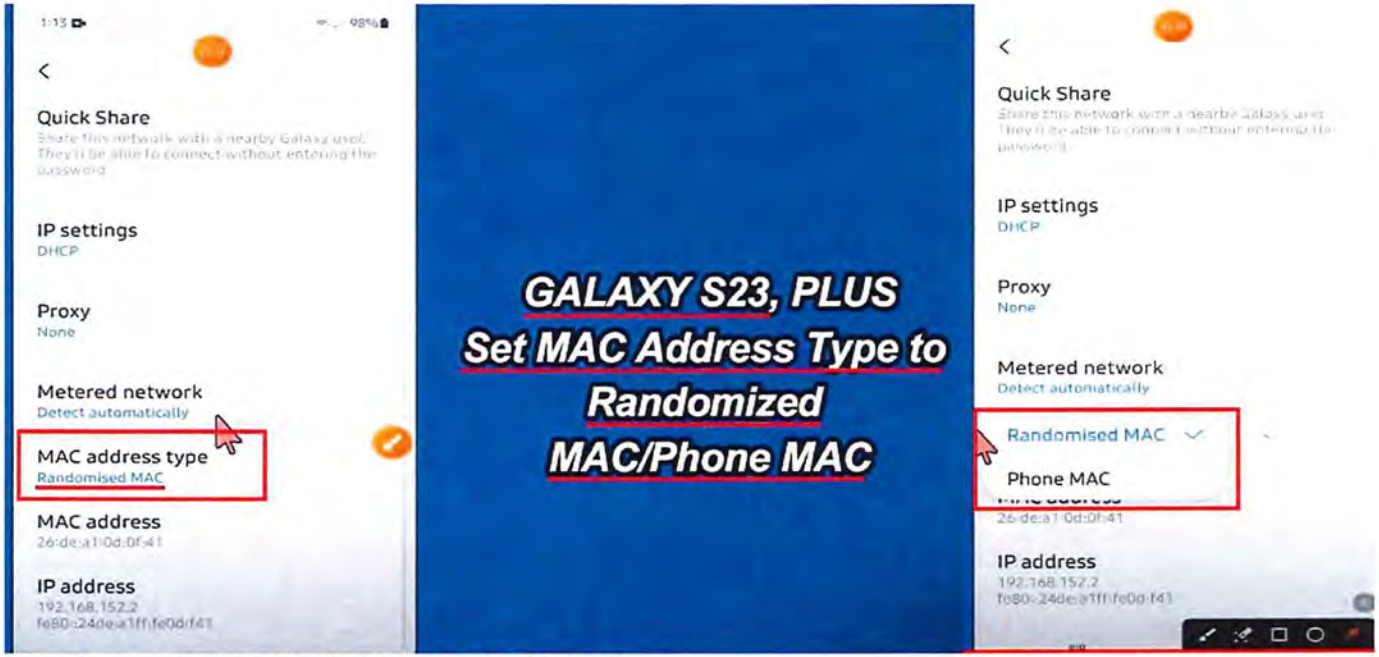
Wi-Fi 6E

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

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

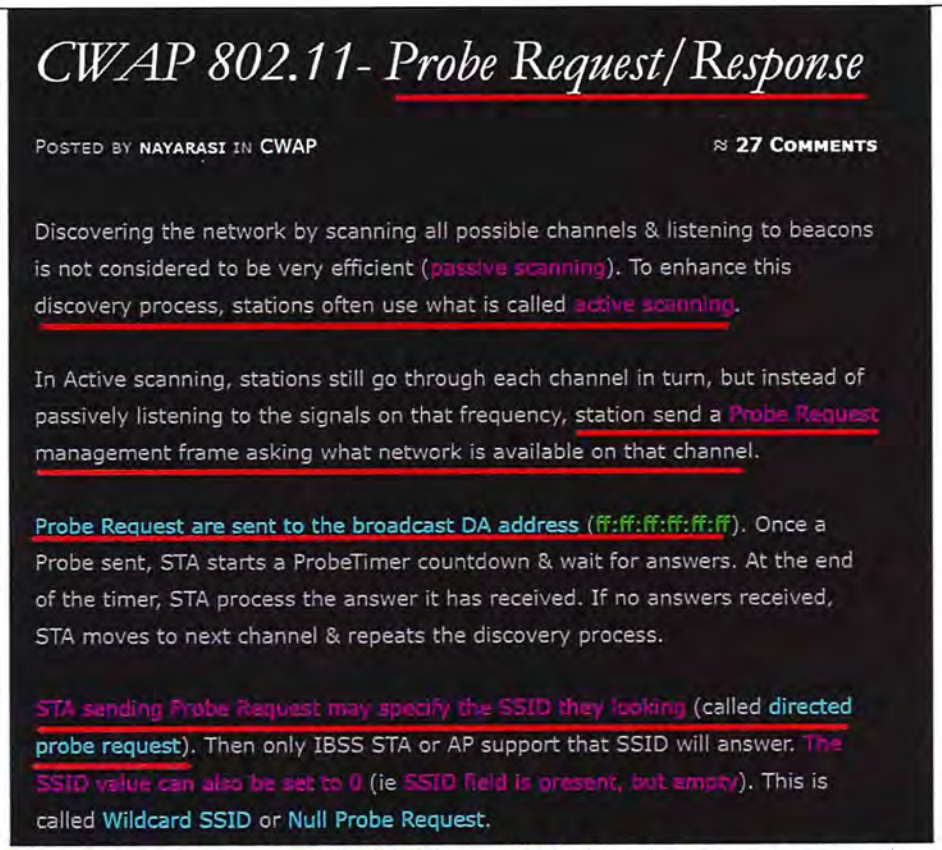
- **Connectivity**: The Galaxy S23 series boasts unparalleled Snapdragon Connect technologies across 5G, Wi-Fi, and Bluetooth®. Featuring the multiple-award-winning Snapdragon X70 5G Modem-RF System with the Qualcomm® 5G AI Processor, the Galaxy S23 series harnesses the power of AI to enable breakthrough 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

	The Accused Products support the Wi-Fi standard. According to the standard, the Accused Products (each a UE) inquire about available Wi-Fi access points using a probe request. The probe request comprises a sender address field (e.g., device identifier). The server generates a random MAC address for use in the probe request. As shown below, the Accused Products utilize probe request frames. 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/

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

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

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

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

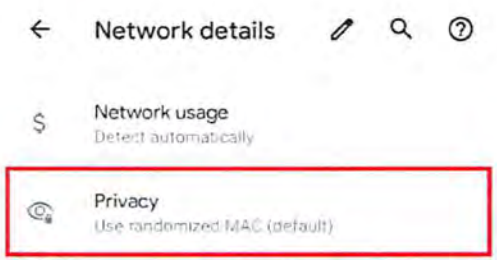


Figure 1. MAC randomization option.

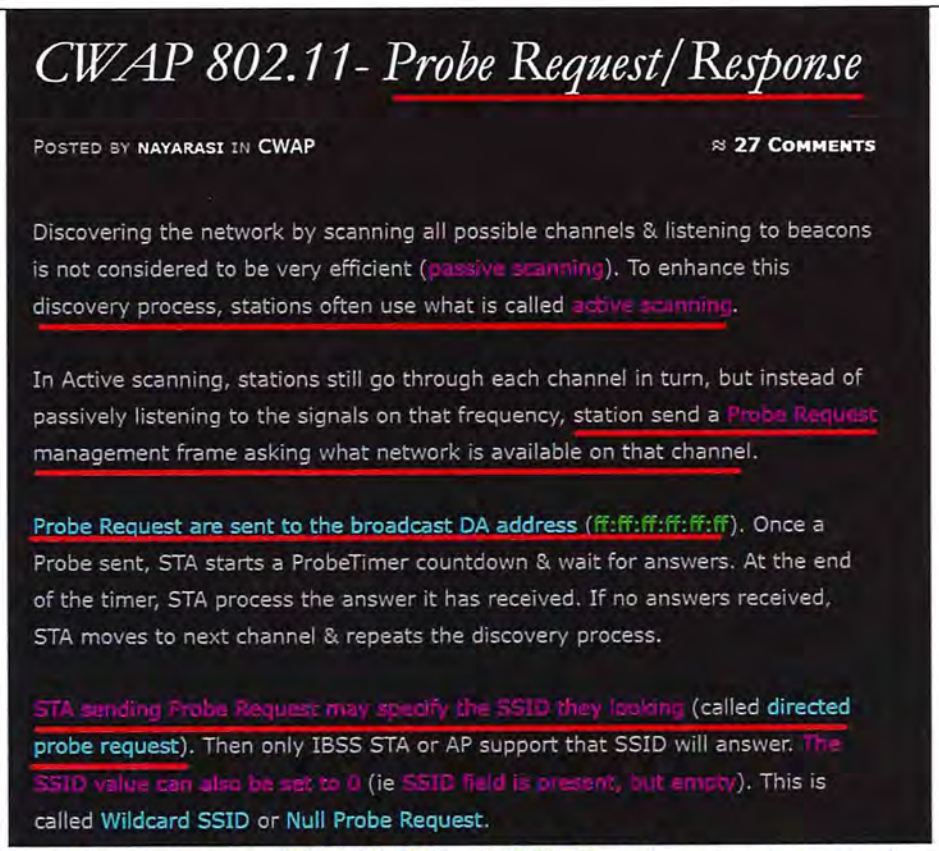
https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior



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

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

[10c] transmitting, to at least one access point, the probe request frame that includes the received fake device identifier;	The Accused Products transmit, to at least one access point (e.g., Wi-Fi access point), the probe request frame (e.g., Wi-Fi probe request) that includes the received fake device identifier (e.g., randomized MAC address). The Accused Products support the Wi-Fi standard. According to the standard, the Accused Products (each a UE) send probe requests to access points to inquire about available Wi-Fi access points using a probe request. The probe request comprises a sender address field (e.g., device identifier). The UE utilizes random a MAC address as the sender address in a probe request. The end user device 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/

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

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

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

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

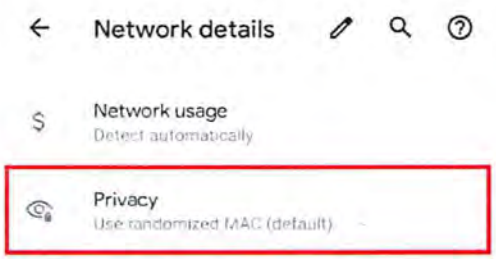


Figure 1. MAC randomization option.

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



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

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

[10d] receiving, from the at least one access point in response to the transmitting the probe request frame, a probe response frame that includes information regarding the at least one access point;	The Accused Products receive from the at least one access point, in response to the transmitting the probe request frame, a probe response frame that includes information regarding the at least access point. As an example, a probe response from a Wi-Fi access point includes the SSID (wireless network name), supported data rates, encryption types, capabilities, etc. of the access point: The Accused Products support the Wi-Fi standard. The Accused Products receive probe responses from multiple available access points. As an example, an access point responds with the probe response when the SSID in the probe request is the wildcard SSID or matches the specific SSID of the access point or when the specific SSID of the access point is included in the SSID List element. As a further example, an access point responds to a probe request when it supports data rates or other requirements of the Accused Products. 2. APs receiving the probe request check to see if the mobile station has at least one common supported data rate. If they have compatible data rates, a probe response is sent advertising the SSID (wireless network name), supported data rates, encryption types if required, and other 802.11 capabilities of the AP. https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/802.11_Association_Process_Explained **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).

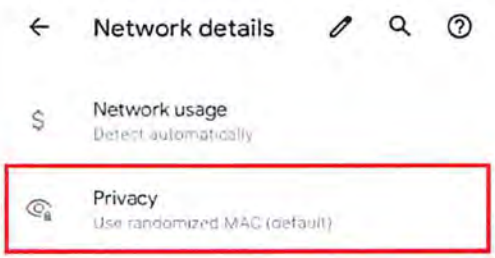


Figure 1. MAC randomization option.

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.

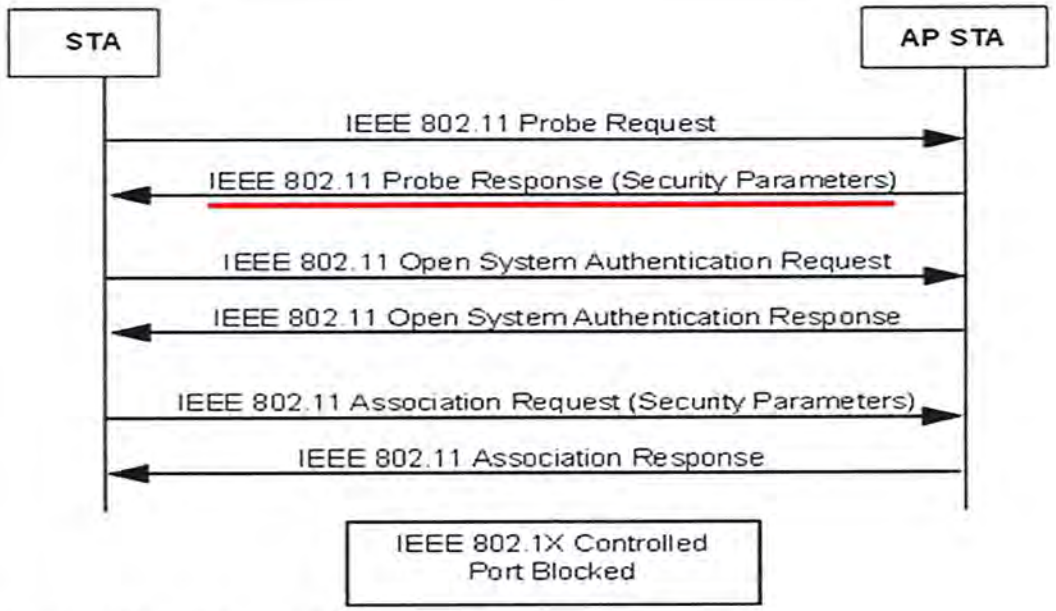
MAC addresses are used by devices when connecting to a Wi-Fi network or an access point. Because these MAC addresses are transmitted without encryption, they can be captured and used to potentially track a user's location. Historically, devices use the *factory MAC address* to associate to a Wi-Fi network.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

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

Table 8-27—Probe Response frame body

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability	
4	SSID	If dot11MeshActivated is true, the SSID element is the wildcard value as described in 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

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

Source: IEEE 802.11-2012.pdf

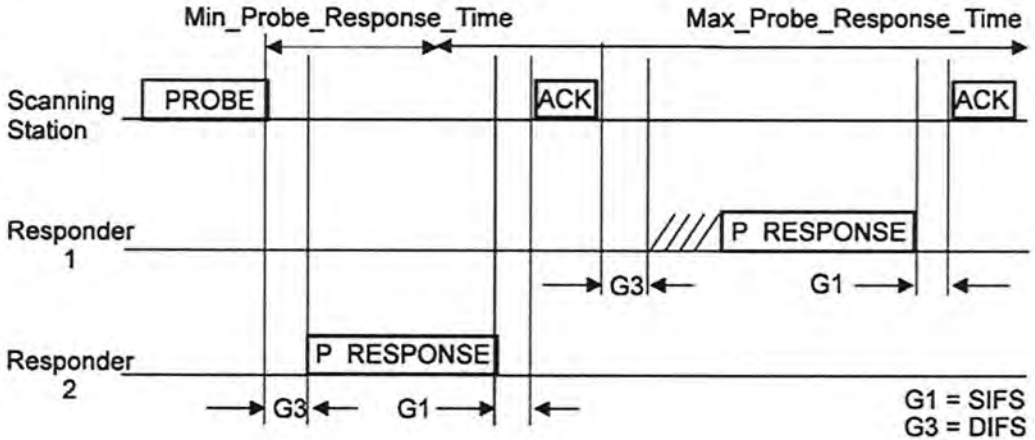
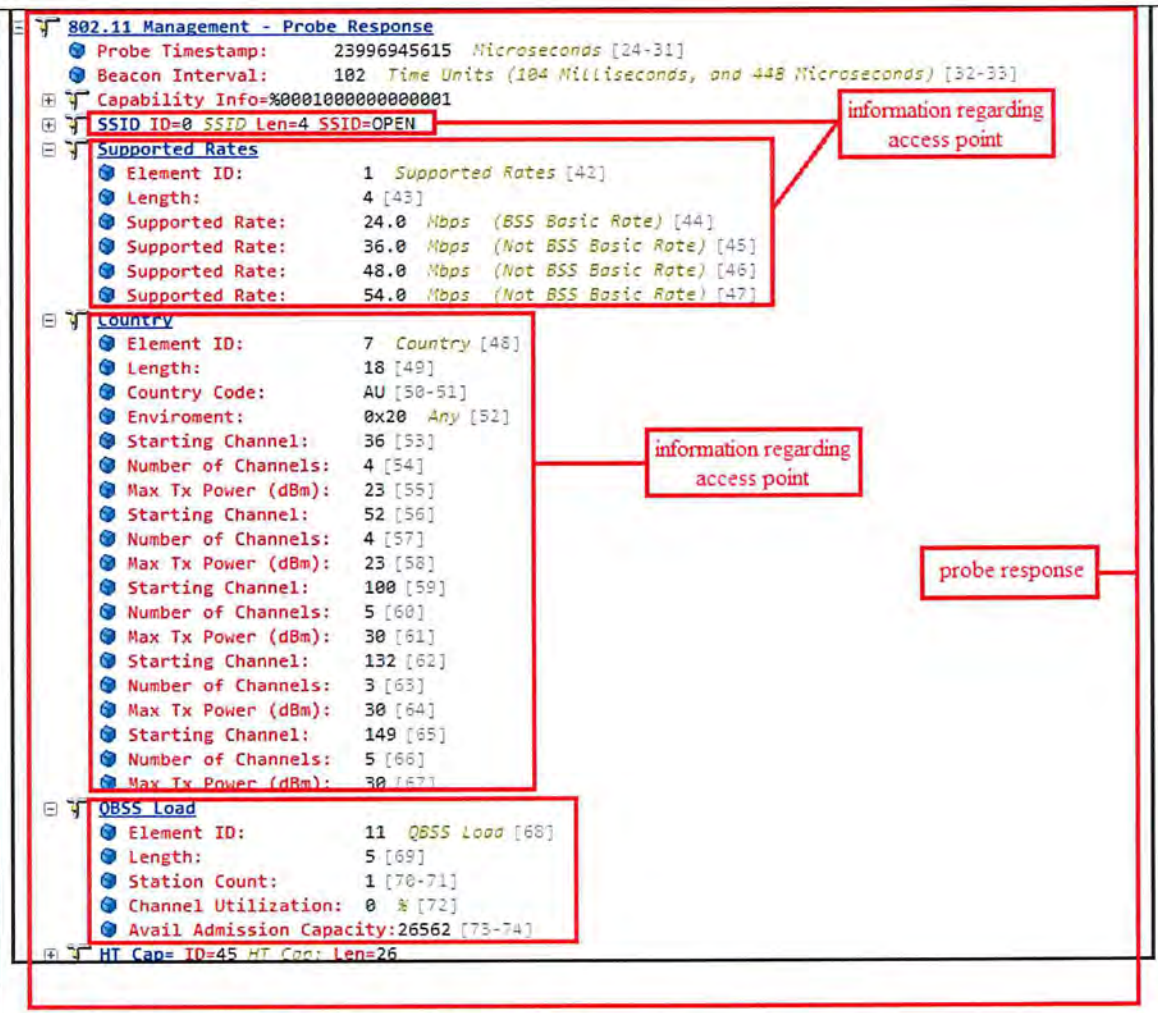


Figure 10-3—Probe response

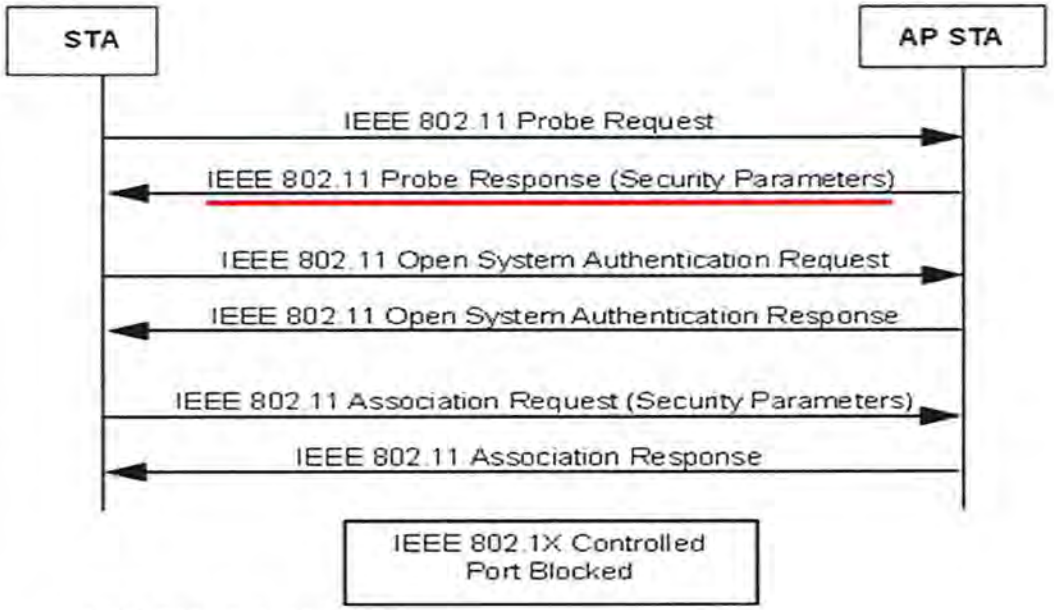
Source: IEEE 802.11-2012.pdf

	Before answering the question, let us first understand what a preferred network list is. The PNL is a historical record of all the network names (SSIDs) that a device has previously connected to, and trusts to automatically connect to again in the future. User devices trying to connect to a Wi-Fi network watch for access points (APs) broadcasting its availability for a device to connect to its network. Within that information contains the network name, or Service Set Identifier (SSID). Wi-Fi enabled devices trying to connect to a wireless network, and using Active Service Discovery, will then broadcast its interest in connecting to the AP if the network name is in its PNL, which increases the connection speed. For instance, if you connect to a **Starbucks** Wi-Fi network once, your device will remember and try to automatically connect to any network with the SSID **Starbucks**. This is true whether you go to the same Starbucks in the future, or a Starbucks 1,000 miles away. All the user device knows is the network name; no additional data is stored. Auto-connecting to wireless networks in PNL saves time and is convenient for the user, but it is a security risk. Therefore, it is important to identify all networks in the PNL and stop connecting automatically to Wi-Fi to stay safe. https://blog.pulsarsecurity.com/preferred-network-list-pnl The reason for client scanning is to determine a suitable AP to which the client may need to roam now or in the future. A client can use two scanning methods: active and passive. During an active scan, the client radio transmits a probe request and listens for a probe response from an AP. With a passive scan, the client radio listens on each channel for beacons sent periodically by an AP. A passive scan generally takes more time, since the client must listen and wait for a beacon versus actively probing to find an AP. Another limitation with a passive scan is that if the client does not wait long enough on a channel, then the client may miss an AP beacon. https://www.wi-fi.org/knowledge-center/faq/what-are-passive-and-active-scanning Below is an example Wi-Fi probe response that includes information of the access point.



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

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

[10e] determining, in response to the receiving the probe response frame and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point, wherein the determining whether the at least one access point is the authenticated access point includes determining whether the information regarding the at least one access point is included in the authenticated access point list that is received from the server; and	The Accused Products determine, in response to the receiving the probe response frame (e.g., probe response) and based at least, in part, on the information (e.g., SSID, supported data rates, key, etc.) regarding the at least one access point (e.g., Wi-Fi access point), whether the at least one access point (e.g., Wi-Fi access point) is an authenticated access point (e.g., previously connected access point), wherein the determining whether the at least one access point (e.g., Wi-Fi access point) is the authenticated access point (e.g., 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., Wi-Fi access point) is included in the authenticated access point list that is received from the server As an example, the Accused Product receives a probe response frame in response to a probe request.  *Source: IEEE 802.11-2012.pdf*

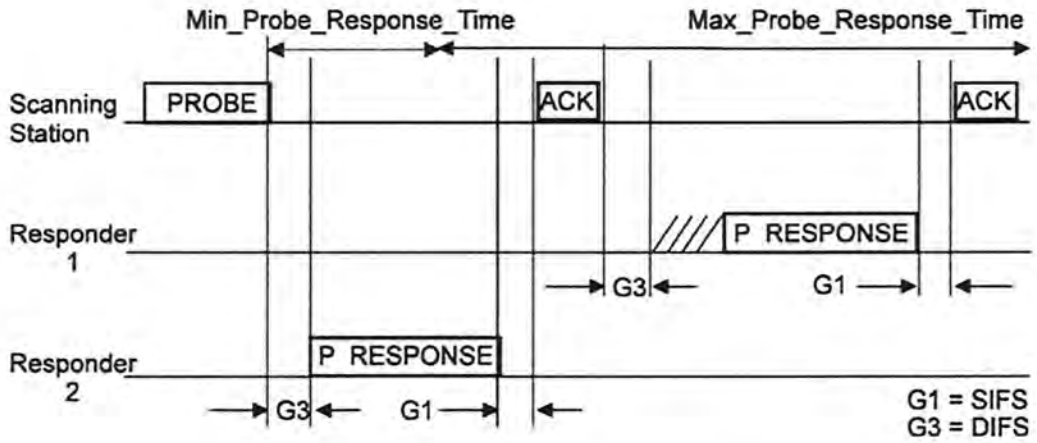


Figure 10-3—Probe response

Source: IEEE 802.11-2012.pdf

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

Table 8-27—Probe Response frame body

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability	
4	SSID	If dot11MeshActivated is true, the SSID element is the wildcard value as described in 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

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

Source: IEEE 802.11-2012.pdf

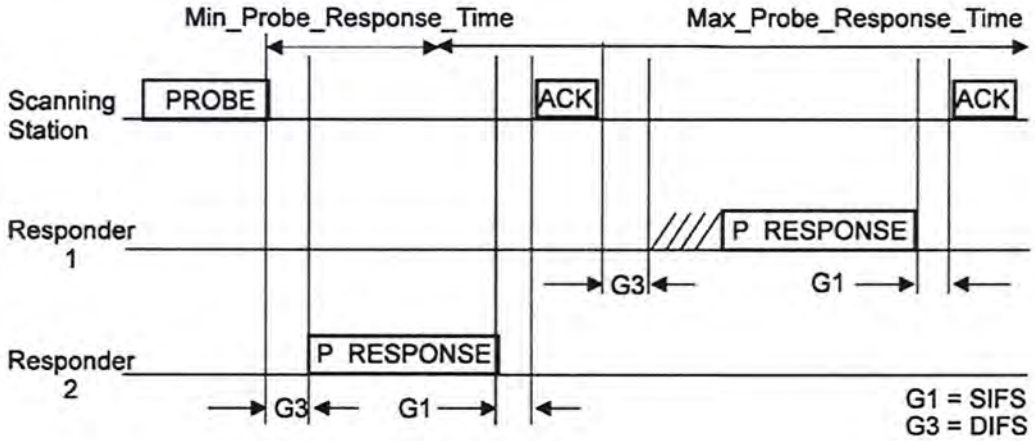
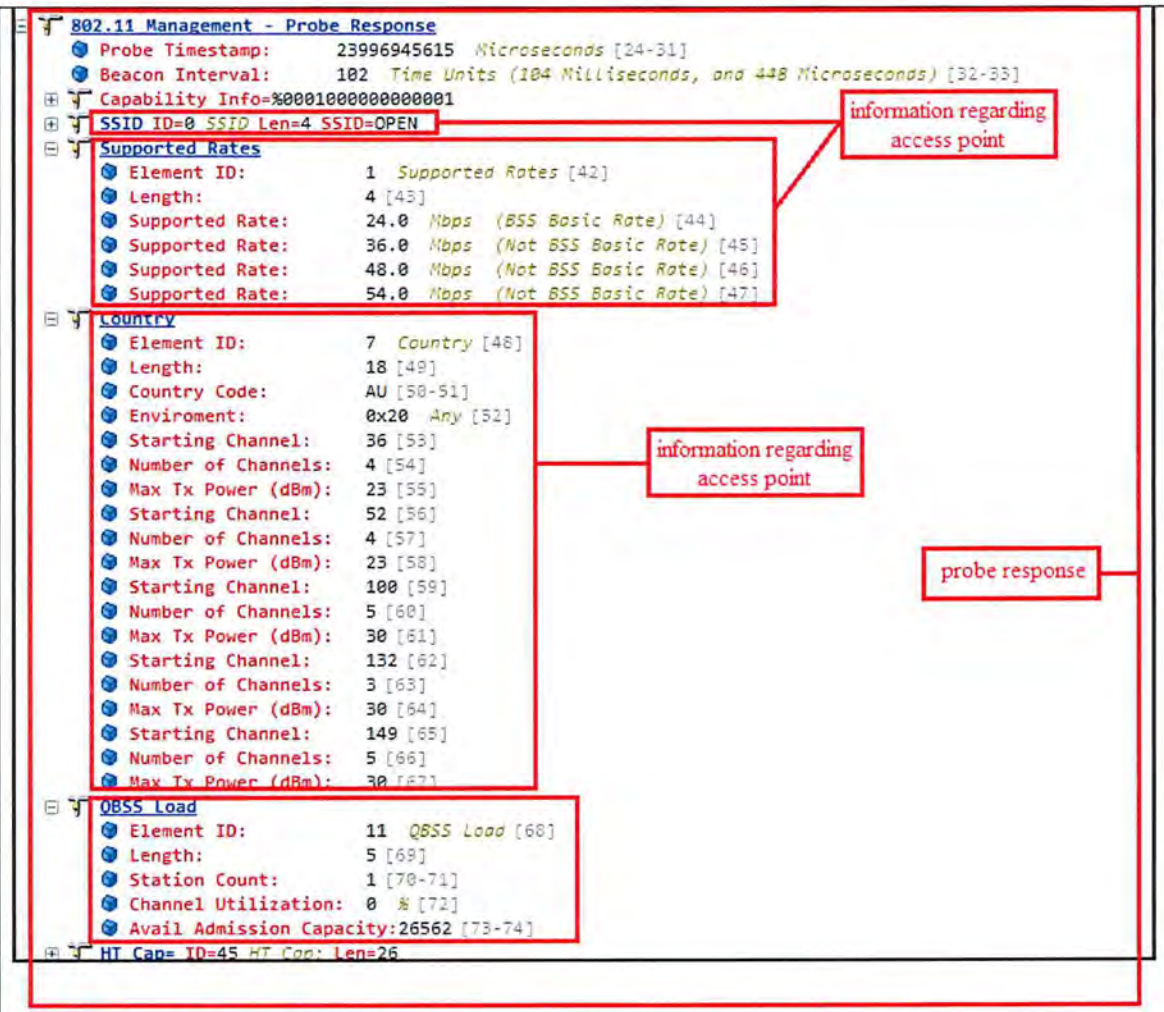


Figure 10-3—Probe response

Source: IEEE 802.11-2012.pdf

	Before answering the question, let us first understand what a preferred network list is. The PNL is a historical record of all the network names (SSIDs) that a device has previously connected to, and trusts to automatically connect to again in the future. User devices trying to connect to a Wi-Fi network watch for access points (APs) broadcasting its availability for a device to connect to its network. Within that information contains the network name, or Service Set Identifier (SSID). Wi-Fi enabled devices trying to connect to a wireless network, and using Active Service Discovery, will then broadcast its interest in connecting to the AP if the network name is in its PNL, which increases the connection speed. For instance, if you connect to a **Starbucks** Wi-Fi network once, your device will remember and try to automatically connect to any network with the SSID **Starbucks**. This is true whether you go to the same Starbucks in the future, or a Starbucks 1,000 miles away. All the user device knows is the network name; no additional data is stored. Auto-connecting to wireless networks in PNL saves time and is convenient for the user, but it is a security risk. Therefore, it is important to identify all networks in the PNL and stop connecting automatically to Wi-Fi to stay safe. https://blog.pulsarsecurity.com/preferred-network-list-pnl The reason for client scanning is to determine a suitable AP to which the client may need to roam now or in the future. A client can use two scanning methods: active and passive. During an active scan, the client radio transmits a probe request and listens for a probe response from an AP. With a passive scan, the client radio listens on each channel for beacons sent periodically by an AP. A passive scan generally takes more time, since the client must listen and wait for a beacon versus actively probing to find an AP. Another limitation with a passive scan is that if the client does not wait long enough on a channel, then the client may miss an AP beacon. https://www.wi-fi.org/knowledge-center/faq/what-are-passive-and-active-scanning Below is an example Wi-Fi probe response that includes information of the access point.



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

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

	the access point using an authenticated device identifier, such as a persistent MAC address that was used for a prior connection with the access point. The Accused Products maintain a list of previously-connected access points which is matched to the access point's SSID received in the probe response. Each previously-connected access point is linked to a persistent MAC address for connecting to that access point. **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]

```
<?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

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

Source: IEEE 802.11-2012.pdf

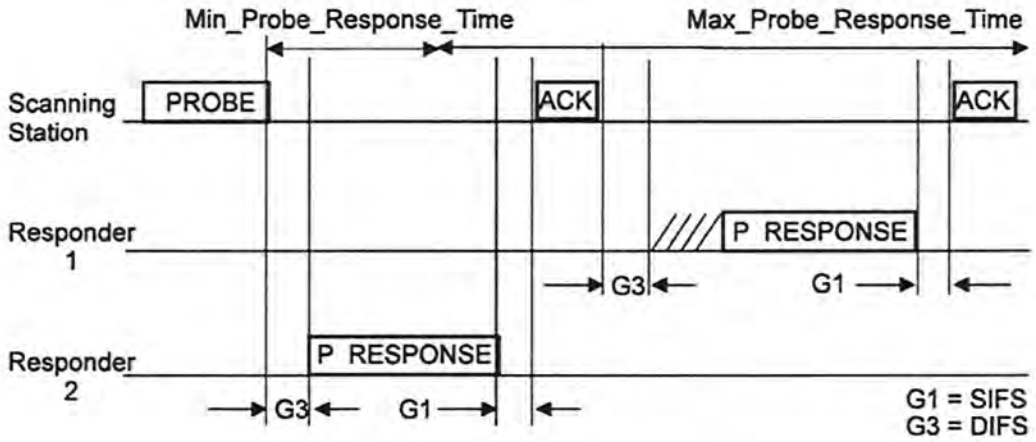
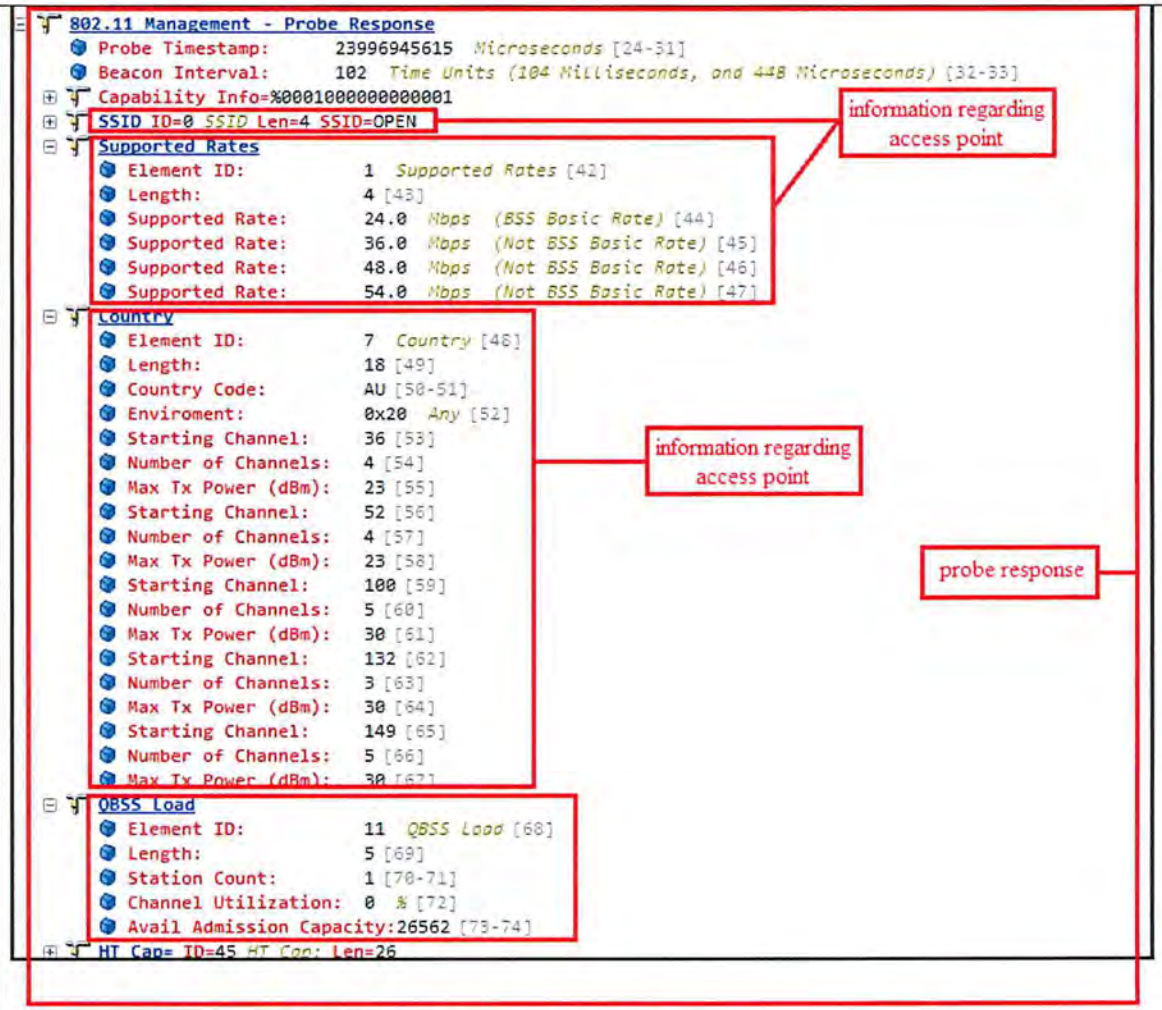


Figure 10-3—Probe response

Source: IEEE 802.11-2012.pdf

	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



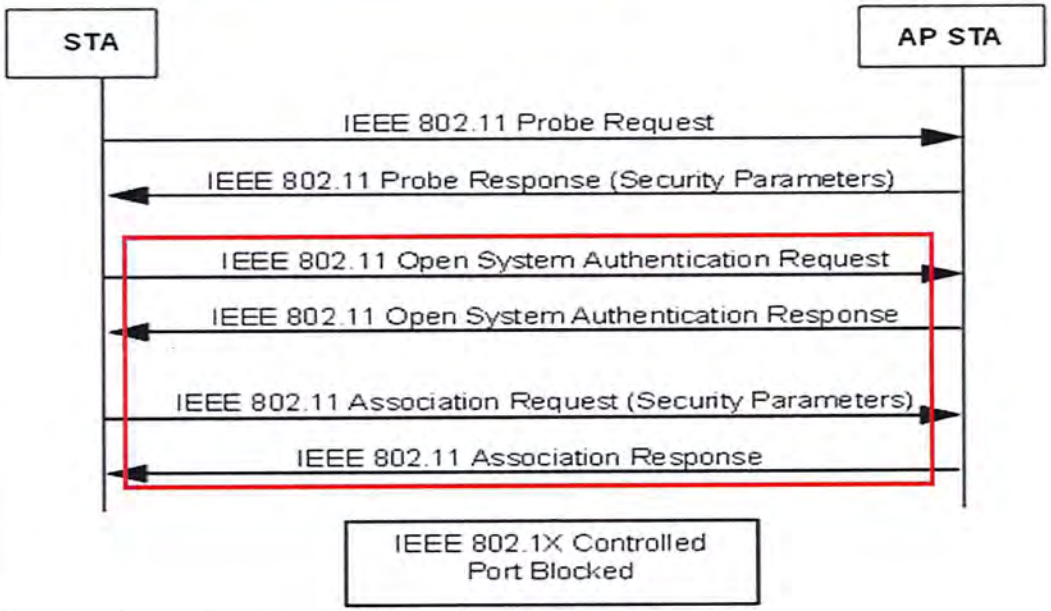
https://mrncciew.com/2014/10/27/cwap-802-11-probe-requestresponse/

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

[10f] transmitting, to the at least one access point in response to a determination that the at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the device.	The Accused Products transmit to the at least one access point in response to a determination that the at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the device. The message includes an authentic device identifier for the end device. For example, the message includes a persistent MAC address for connecting to the access point. After receiving the probe response from the access point, as discussed above, the Accused Products confirm the received SSID information from the probe responses with the access point information stored in memory. Once confirmed that there is an SSID in a probe response from an access point with which the UE was connected previously, the Accused Products initiate a connection using the persistent MAC address for the access point, which is an authentic device identifier for the Accused Product. **Persistent randomization** Android uses the persistent randomization type by default when the MAC randomization feature is enabled. Android generates a persistent randomized MAC address based on the parameters of the network profile including SSID, security type, or FQDN (for Passpoint networks). This MAC address remains the same until factory reset. The MAC address does **not** get re-randomized if the user forgets and re-adds the Wi-Fi network since the MAC addressed depends on the parameters of the network profile. https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior

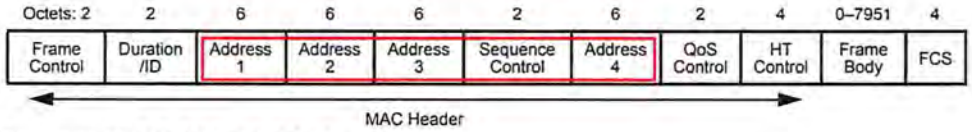


https://www.youtube.com/watch?v=dT63df6nnqU



Source: IEEE 802.11-2012.pdf

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



Source: IEEE 802.11-2012.pdf

8.2.4.3.5 DA field

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

8.2.4.3.6 SA field

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

8.2.4.3.7 RA field

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

8.2.4.3.8 TA field

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

Source: IEEE 802.11-2012.pdf

802.11 Mgmt : Authentication Frame

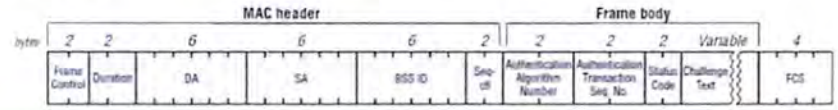
POSTED BY **NAYARASI** IN **CWAP** ≈ **10 COMMENTS**

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

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

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

FIGURE 4.8 Authentication frame format



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

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

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]

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

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

	An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
11. The method of claim 10, wherein the receiving the fake device identifier includes receiving a fake media access control (MAC) address.	Receiving the fake device identifier (as described in relation to claim 10) includes receiving a fake media access control (MAC) address. The server generates a random MAC address, which is a fake MAC address that is different from the original MAC address of the hardware. **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).

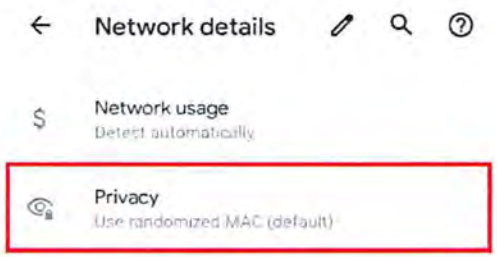


Figure 1. MAC randomization option.

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

	An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
13. The method of claim 10, further comprising: storing the authenticated access point list in a memory.	The Accused Products store the authenticated access point list in a memory. The Accused Products maintain a list of previously-connected access points which is matched to the access point's SSID received in the probe response. Each previously-connected access point is linked to a persistent MAC address for connecting to that access point. **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]

```
<?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" />
                <boolean name="HiddenSSID" value="false" />
```

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

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

Source: IEEE 802.11-2012.pdf

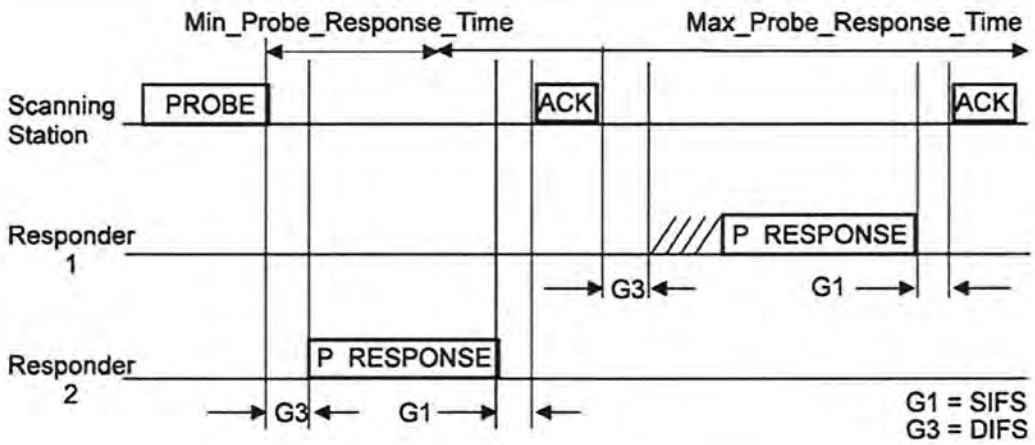
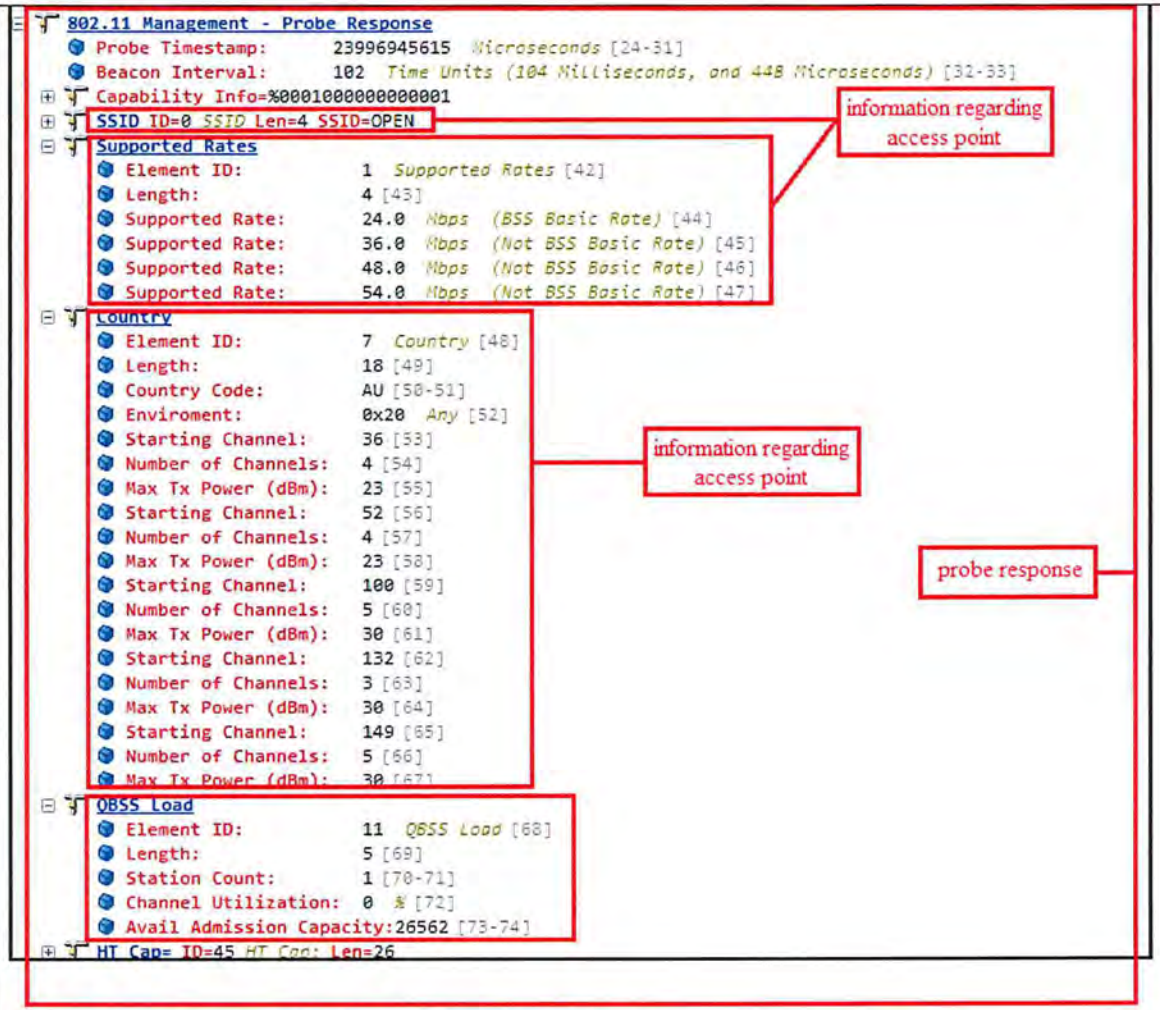


Figure 10-3—Probe response

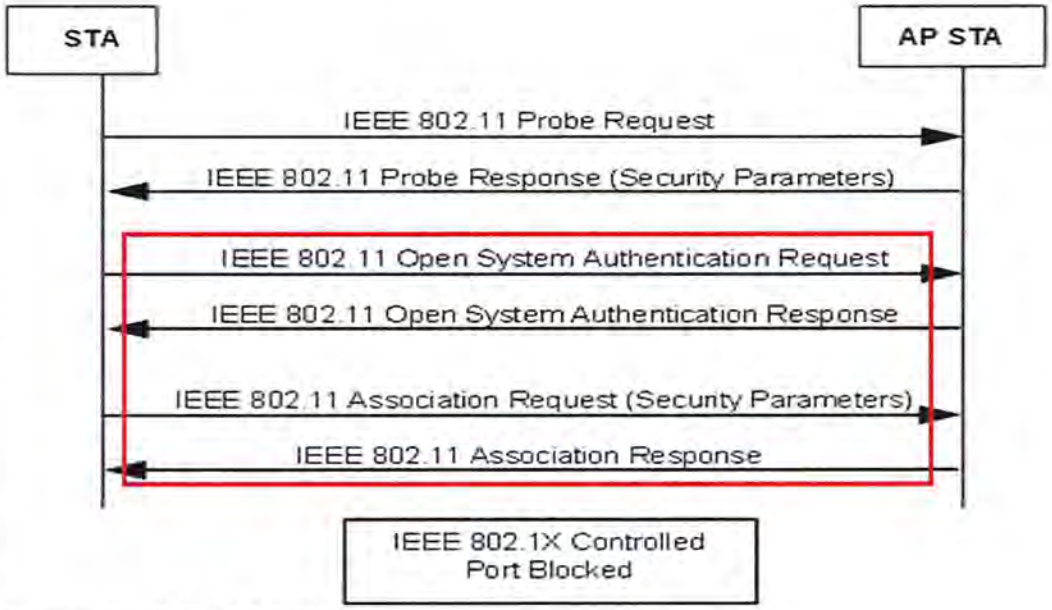
Source: IEEE 802.11-2012.pdf

	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



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

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

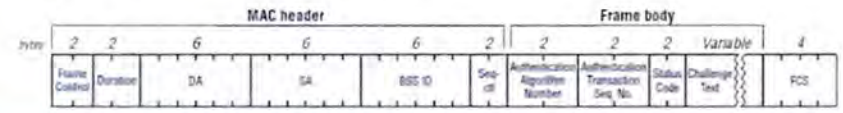
14. The method of claim 10, further comprising: receiving, from the at least one access point, an approval of the connection request; transmitting, to the at least one access point in response to the receiving the approval of the connection request, an association request; receiving, from the at least one access point, an association response to the association request; and connecting to a communication network via the at least one access point in accordance with the association response.	The Accused Products receive, from the at least one access point, an approval of the connection request. The Accused Products support the Wi-Fi standard. According to the standard, a UE (e.g., the Accused Product) inquires about available Wi-Fi access points using a probe request. The probe request comprises a SSID list or preferred network list which is a set of SSID to which the UE got connected previously. As an example, the Accused Products receive an open system authentication response from an access point. The Accused Products then transmit an association request. The Accused Products then receive an association response from the access point, at which point the Accused Product is connected to a network via the access point in accordance with the association response.  *Source: IEEE 802.11-2012.pdf*

	8.2.4.3.5 DA field The DA field contains an IEEE MAC individual or group address that identifies the MAC entity or entities intended as the final recipient(s) of the MSDU (or fragment thereof) or A-MSDU, as defined in 8.3.2.1, contained in the frame body field. **8.2.4.3.6 SA field** The SA field contains an IEEE MAC individual address that identifies the MAC entity from which the transfer of the MSDU (or fragment thereof) or A-MSDU, as defined in 8.3.2.1, contained in the frame body field was initiated. The individual/group bit is always transmitted as a 0 in the source address. **8.2.4.3.7 RA field** The RA field contains an IEEE MAC individual or group address that identifies the intended immediate recipient STA(s), on the WM, for the information contained in the frame body field. **8.2.4.3.8 TA field** The TA field contains an IEEE MAC individual address that identifies the STA that has transmitted, onto the WM, the MPDU contained in the frame body field. The Individual/Group bit is always transmitted as a 0 in the transmitter address. *Source: IEEE 802.11-2012.pdf*

<table>
<tr>
<td></td>
<td>
<h1>802.11 Mgmt : Authentication Frame</h1>
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)

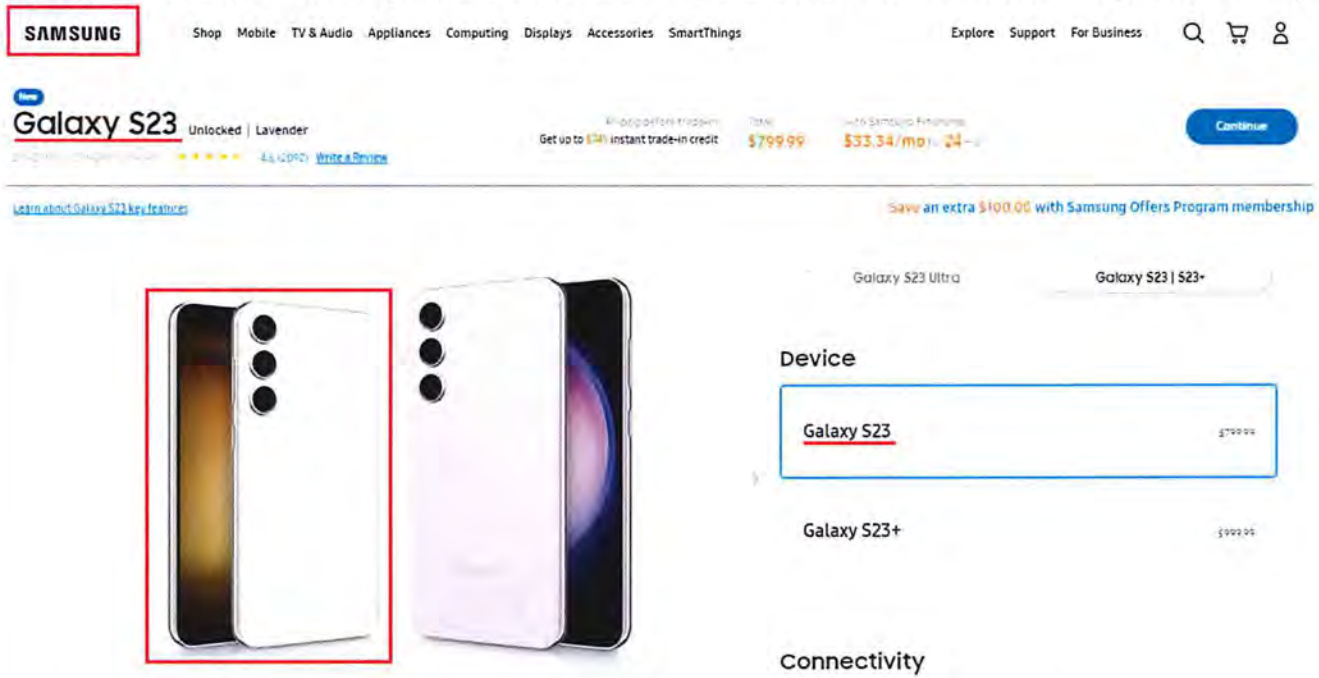
FIGURE 4.8 Authentication frame format


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

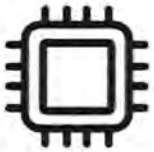
An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
</td>
</tr>
<tr>
<td>15. A method performed by a device, the method comprising:</td>
<td>To the extent the preamble is limiting, the Accused Products practice a method performed by a device.

The Accused Products include Android OS 10 or above or Wear OS 3 or above. Each Accused Product includes an SoC and Wi-Fi connection functionality. As a specific example shown below, the Galaxy S23 includes the</td>
</tr>
</table>

Android 13 operating system, which includes randomized MAC for Wi-Fi connections. It comprises an SoC, Snapdragon 8 Gen 2, a Wi-Fi chipset, and FastConnect. It connects to a Wi-Fi network using the Wi-Fi chipset.



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

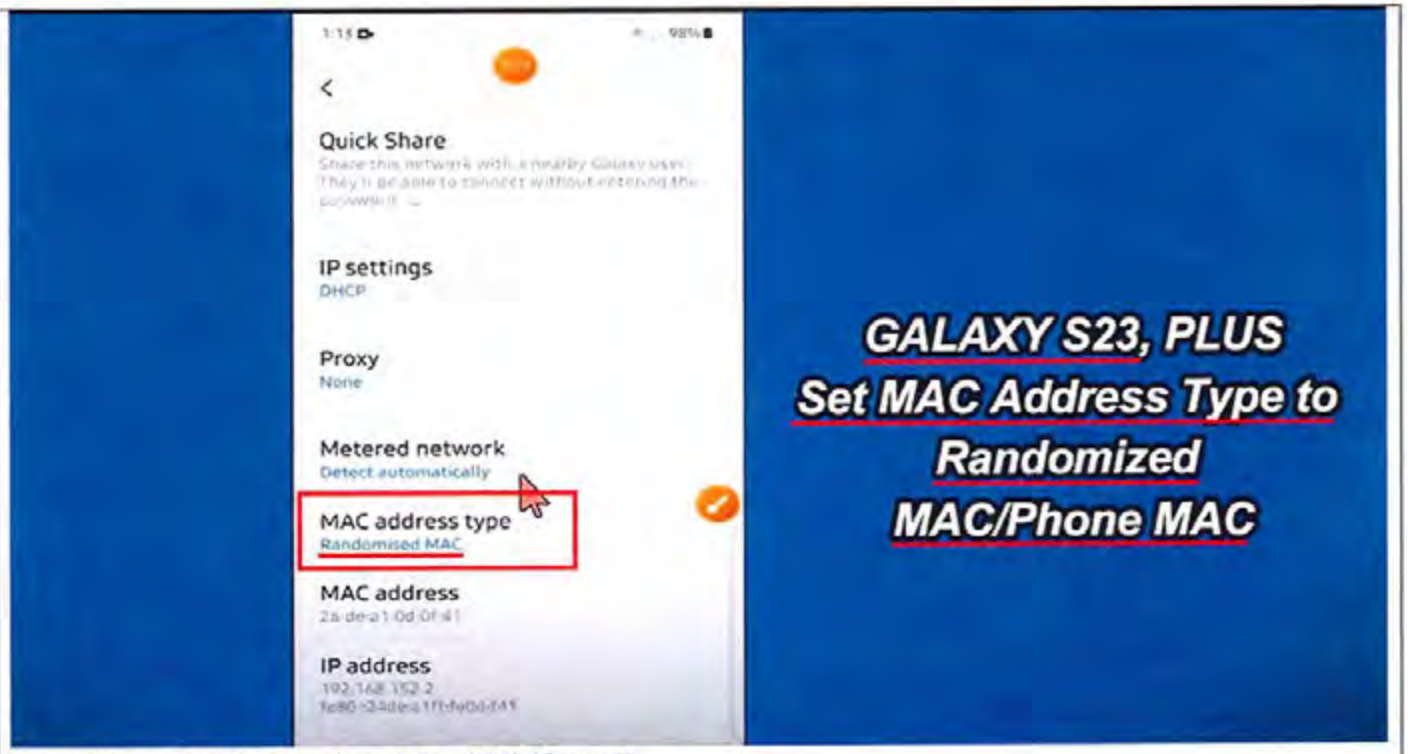
	Galaxy S23  Super fast processing Snapdragon® 8 Gen 2 Octa-Core https://www.samsung.com/us/smartphones/galaxy-s23/specs/

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

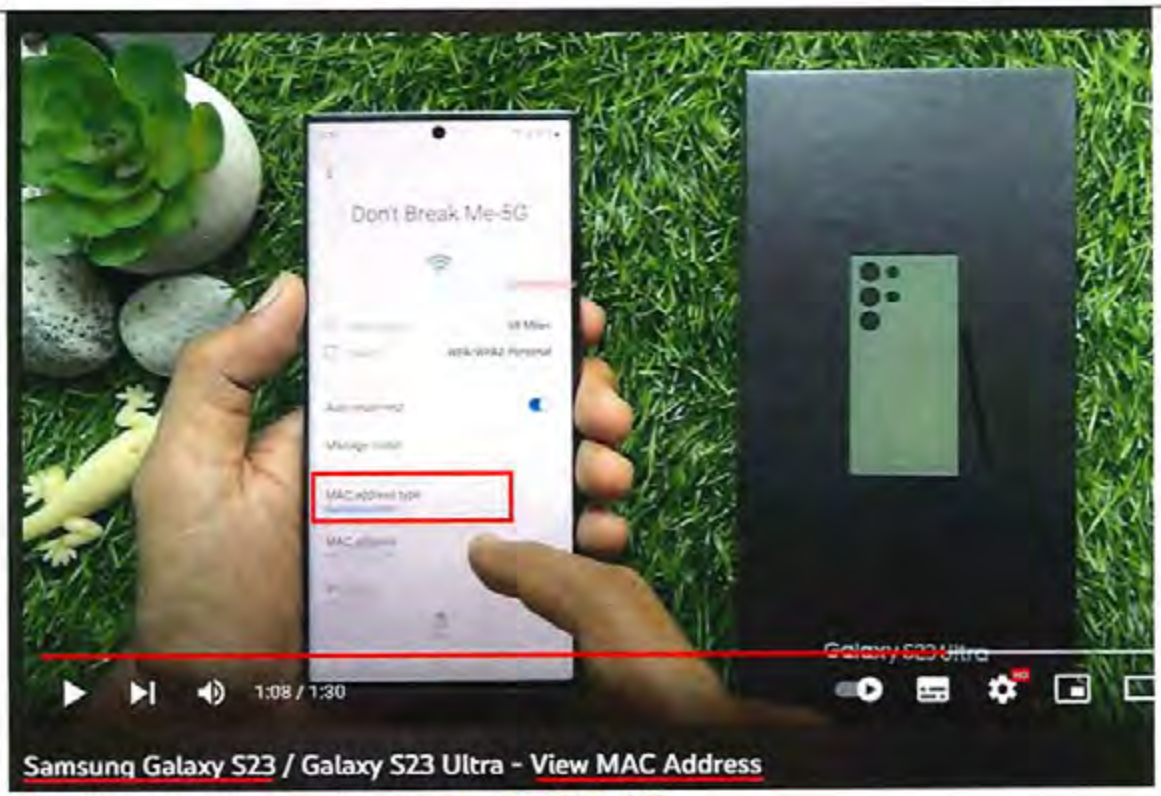
https://www.androidpolice.com/samsung-galaxy-s23/



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



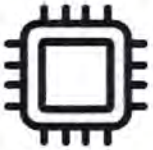
https://www.youtube.com/watch?v=dT63df6nnqU



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

	In Android 10, MAC randomization is enabled by default for client mode, SoftAp, and Wi-Fi Direct. MAC randomization prevents listeners from using MAC addresses to build a history of device activity, thus increasing user privacy. Additionally, MAC addresses are randomized as part of Wi-Fi Aware and Wi-Fi RTT operations. For more information, see MAC Randomization Behavior. https://source.android.com/docs/core/connect/wifi-mac-randomization Wear OS, including Wear OS 3.0, is based on Android. *See* https://developer.android.com/training/wearables/wear-v-mobile#:~:text=Wear%20OS%20is%20based%20on,design%20a%20Wear%20OS%20app. Devices operating on Wear OS 3.0 implement MAC randomization. *See* https://www.reddit.com/r/GalaxyWatch/comments/pcmkj1/galaxy_watch_4_wifi_mac_address/
[15a] receiving, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;	The Accused Products receive, from a server (e.g., the OS and/or a CPU and associated memory for storing and executing the OS and associated data), an authenticated access point list (e.g., previously connected access point list) that includes information (e.g., SSID, supported data rates, pre-shared keys, etc.) regarding one or more access points (e.g., previously connected access point) that are controlled by the server. As shown below, an example of the Accused Products contains an SoC, Snapdragon 8 Gen 2 with a Kryo CPU. Also, it supports Android 13 operating system and has an option for randomized MAC for Wi-Fi connections. The server generates a persistent randomized MAC address to be used with a Wi-Fi network. The server also stores a list of previously connected access points and provides that list to the device in connecting to Wi-Fi access points. The list comprises different information pertaining to previously connected access points such as SSID, pre-shared keys, etc.

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



CPU

Kryo CPU

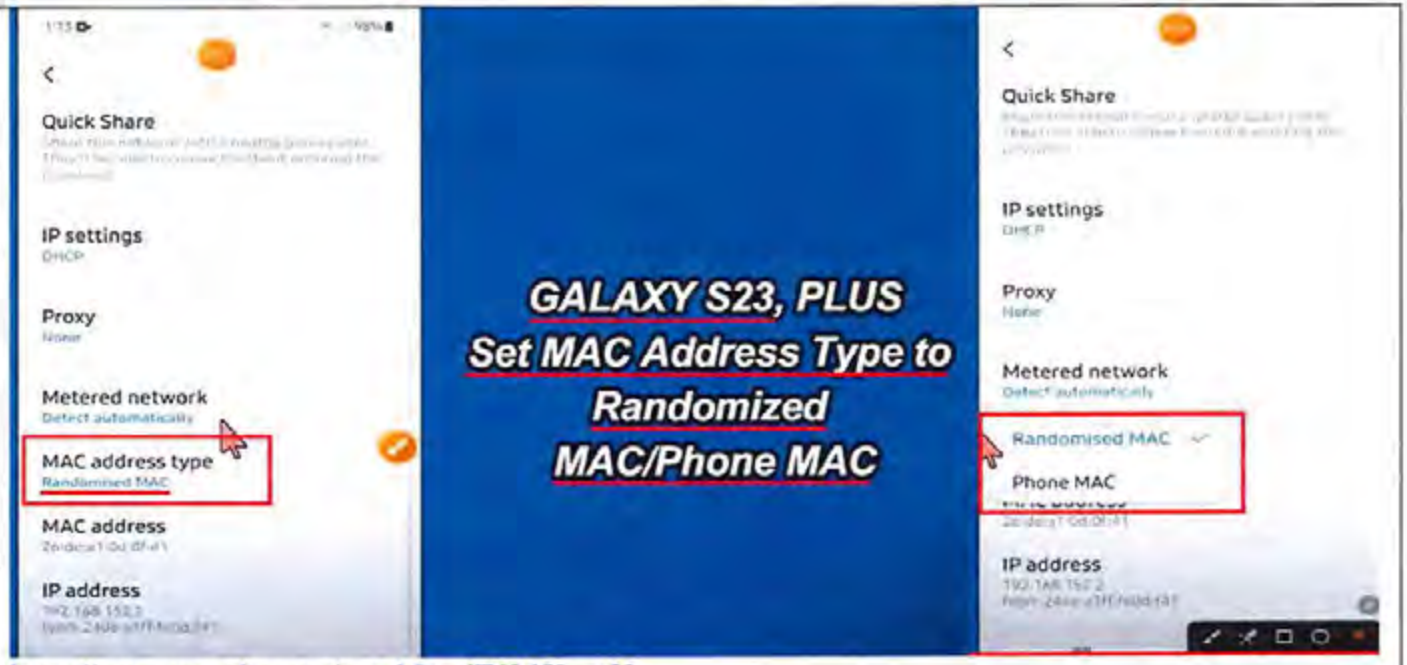
- 64-bit Architecture
- 1 Prime core, up to 3.36 GHz[2]
  - Arm Cortex-X3 technology
- 4 Performance cores, up to 2.8 GHz
- 3 Efficiency cores, up to 2.0 GHz

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

Phone	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

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>
```

previously connected access-points information list

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" />
                <boolean name="HiddenSSID" value="false" />
```

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

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

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]

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

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

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

Source: IEEE 802.11-2012.pdf

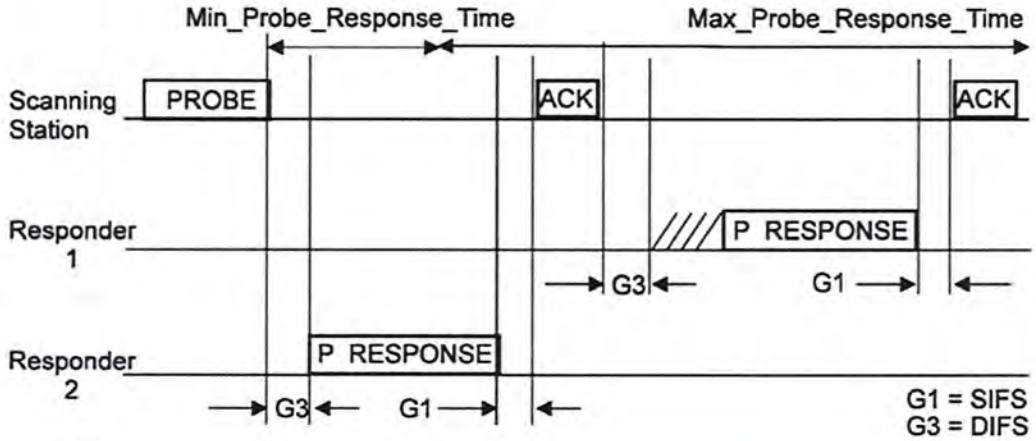
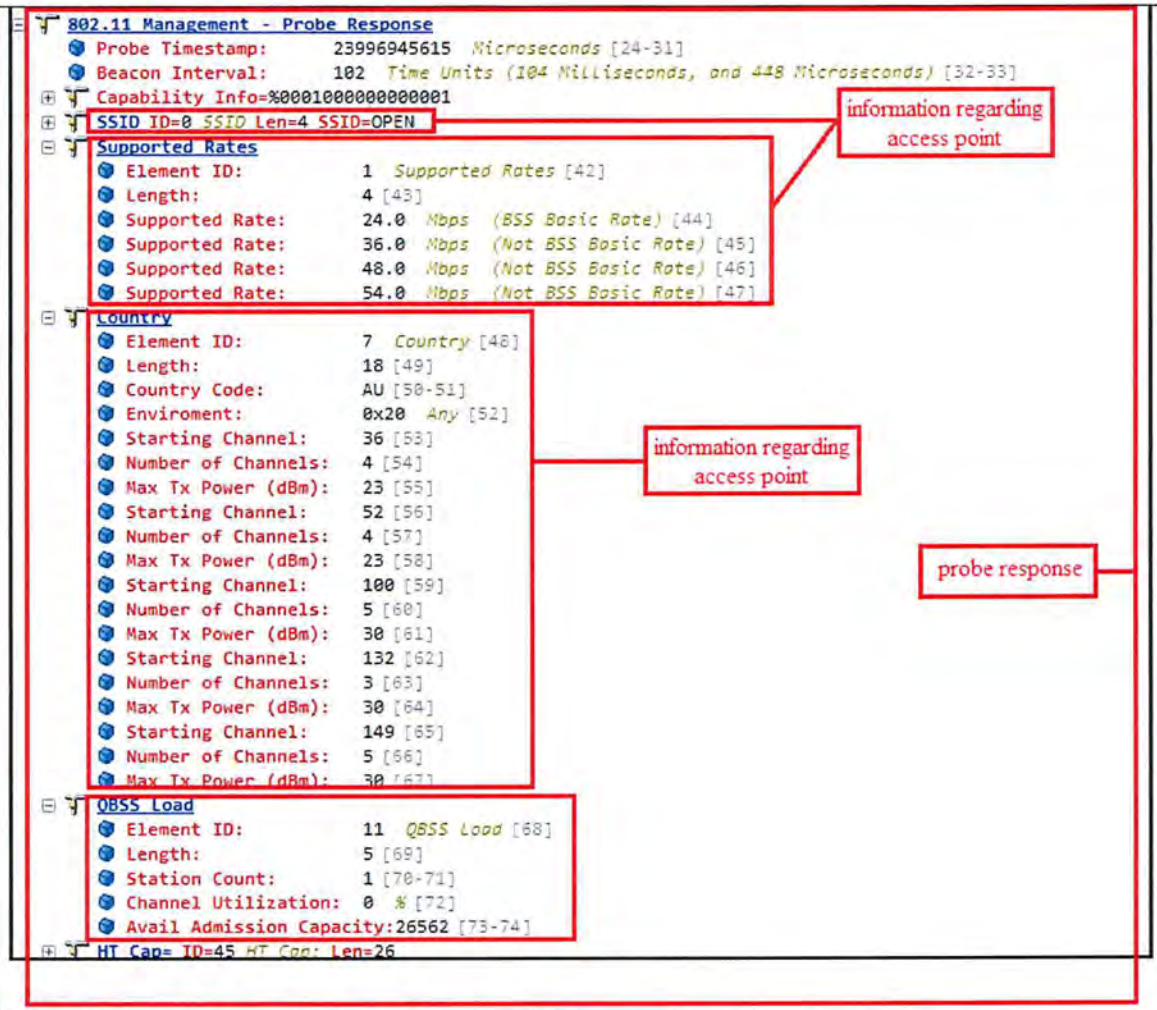


Figure 10-3—Probe response

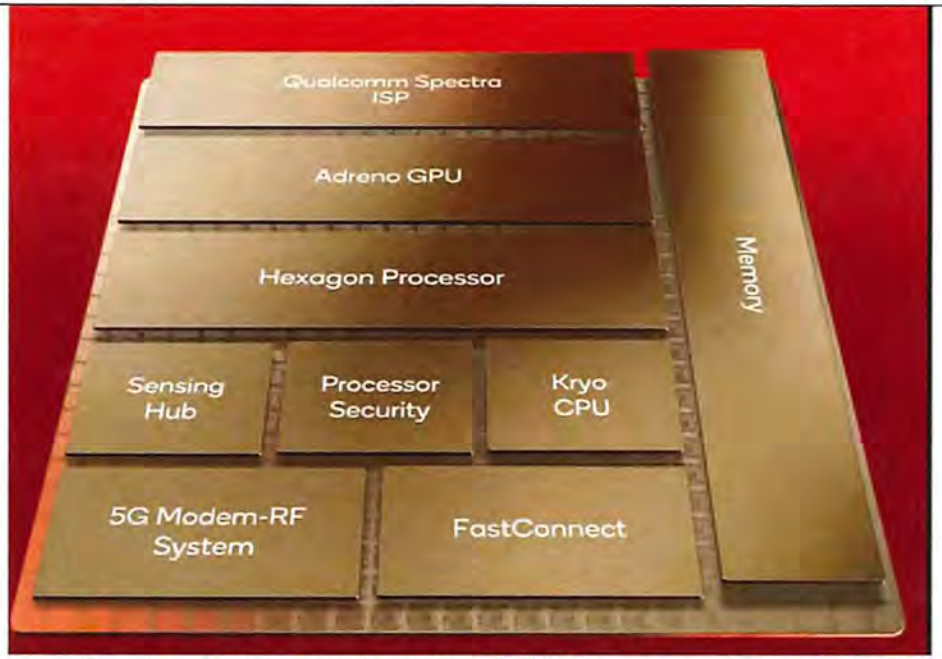
Source: IEEE 802.11-2012.pdf

	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



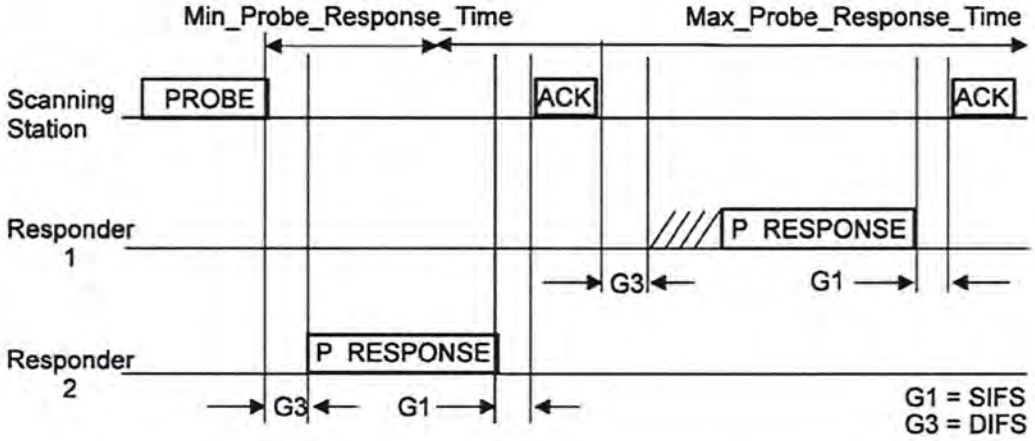
https://mrncciew.com/2014/10/27/cwap-802-11-probe-requestresponse/

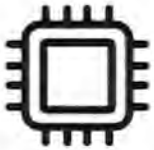
The CPU is a part of the SnapDragon SOC and coupled to the FastConnect network interface.



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

The access points are controlled by the server. For example, the server, which serves the functionality of the Android operating system, controls connection and/or data transmission of the access points. The Accused Products support the Wi-Fi standard. According to the standard, the Accused Products inquire about available Wi-Fi access points using a probe request, which is generating by the mobile operating server. The probe request comprises identifying information, such as a wildcard SSID or SSID for one or more access points or a preferred network list which is a set of SSIDs to which the UE got connected previously. An access point receiving the probe request must provide a probe response. As a further example, an access point receives and transmits data under control of the mobile operating server.

	In an infrastructure BSS or in an IBSS, STAs receiving Probe Request frames shall respond with a probe response when the SSID in the probe request is the wildcard SSID or matches the specific SSID of the STA or when the specific SSID of the STA is included in the SSID List element. Furthermore, a STA with dot11RadioMeasurementActivated true receiving a probe request with a DSSS Parameter Set element containing a Current Channel field value that is not the same as the value of dot11CurrentChannel shall not respond with a probe response. An AP shall respond to all probe requests meeting the above criteria. In an IBSS a STA that transmitted a Beacon frame since the last TBTT shall respond to group addressed Probe Request frames. A STA in an IBSS shall respond to Probe Request frames sent to the individual address of the STA. *Source: IEEE 802.11-2012.pdf*  **Figure 10-3—Probe response** *Source: IEEE 802.11-2012.pdf* An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
[15b] generating a fake device	The Accused Products generate a fake device identifier for the device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters.

identifier for the device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters;	As shown below, an example of the Accused Products contains an SoC, Snapdragon 8 Gen 2. It also includes the Android OS 10 or higher (e.g., Android 13 operating system) and has randomized MAC for Wi-Fi connections. The operating system is used to generate a randomized MAC address to be used for when scanning or searching for access points, such as for Wi-Fi probe requests. The operating system runs on a CPU of the SoC (e.g., the Kryo CPU) of the accused product. Galaxy S23  Super fast processing Snapdragon® 8 Gen 2 Octa-Core https://www.samsung.com/us/smartphones/galaxy-s23/specs/

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/



CPU

Kryo CPU

- 64-bit Architecture
- 1 Prime core, up to 3.36 GHz[2]
  - Arm Cortex-X3 technology
- 4 Performance cores, up to 2.8 GHz
- 3 Efficiency cores, up to 2.0 GHz

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

Phone	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/

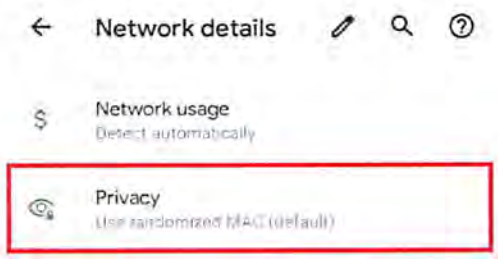
- **Connectivity**: The Galaxy S23 series boasts unparalleled Snapdragon Connect technologies across 5G, Wi-Fi, and Bluetooth®. Featuring the multiple-award-winning Snapdragon X70 5G Modem-RF System with the Qualcomm® 5G AI Processor, the Galaxy S23 series harnesses the power of AI to enable breakthrough 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

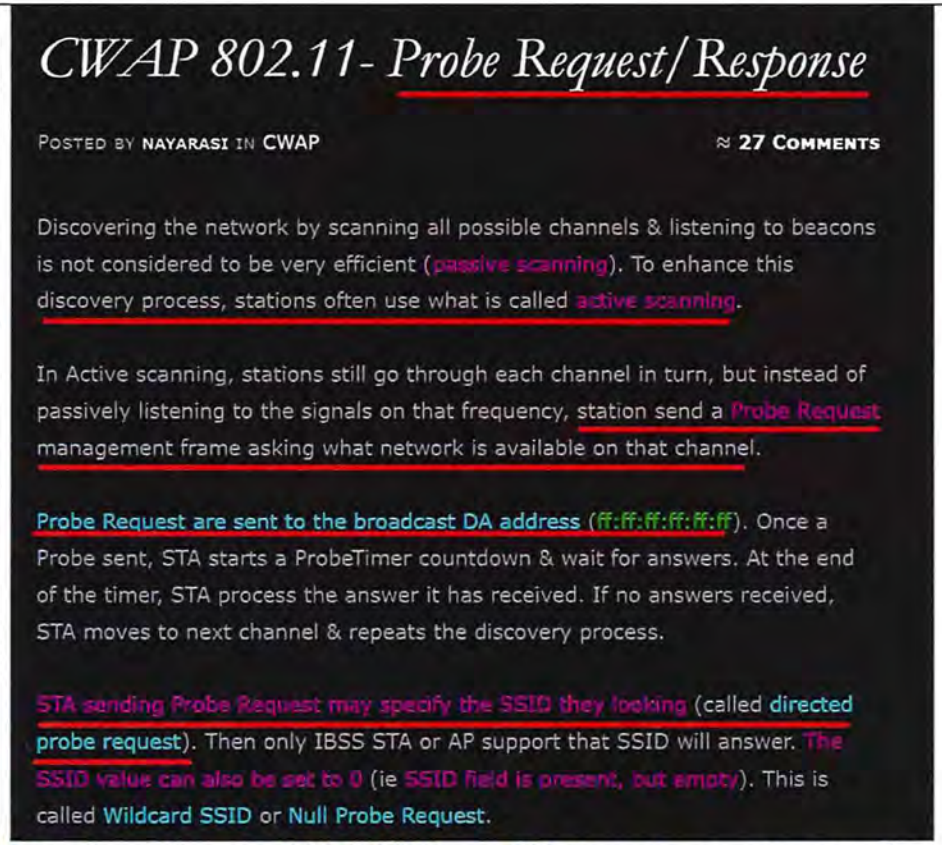


https://www.youtube.com/watch?v=dT63df6nnqU

	The Accused Products support the Wi-Fi standard. According to the standard, the Accused Products (each a UE) inquire about available Wi-Fi access points using a probe request that includes a MAC address. For a probe request the Accused Products use a randomized MAC address, which is a fake device identifier. **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 An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
[15c] transmitting, to at least one access point, a probe request frame that includes the fake device identifier;	The Accused Products transmit, to at least one access point, a probe request frame that includes the fake device identifier. The Accused Products support the Wi-Fi standard. According to the standard, the Accused Products (each a UE) send probe requests to access points to inquire about available Wi-Fi access points using a probe request. The probe request comprises a sender address field (e.g., device identifier). The Accused Products utilize a random MAC address as the sender address in a probe request. The end user device transmits probe requests to identify available access points:

	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/

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

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

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

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

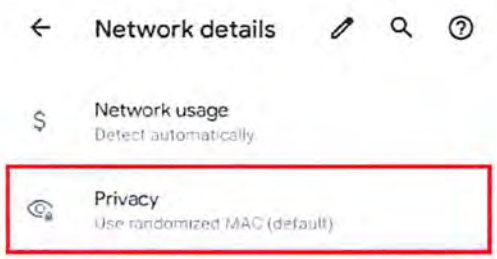


Figure 1. MAC randomization option.

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



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

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

[15d] receiving, from the at least one access point in response to the transmitting the probe request frame, a probe response frame that includes information regarding the at least one access point;	The Accused Products receive from the at least one access point in response to the transmitting the probe request frame, a probe response frame that includes information regarding the at least one access point. As an example, a probe response from a Wi-Fi access point includes the SSID (wireless network name), supported data rates, encryption types, capabilities, etc. of the access point: The Accused Products support the Wi-Fi standard. The Accused Products receive probe responses from multiple available access points. As an example, an access point responds with the probe response when the SSID in the probe request is the wildcard SSID or matches the specific SSID of the access point or when the specific SSID of the access point is included in the SSID List element. As a further example, an access point responds to a probe request when it supports data rates or other requirements of the Accused Products. 2. APs receiving the probe request check to see if the mobile station has at least one common supported data rate. If they have compatible data rates, a probe response is sent advertising the SSID (wireless network name), supported data rates, encryption types if required, and other 802.11 capabilities of the AP. https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/802.11_Association_Process_Explained **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).

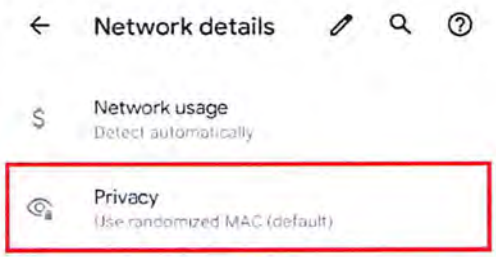


Figure 1. MAC randomization option.

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.

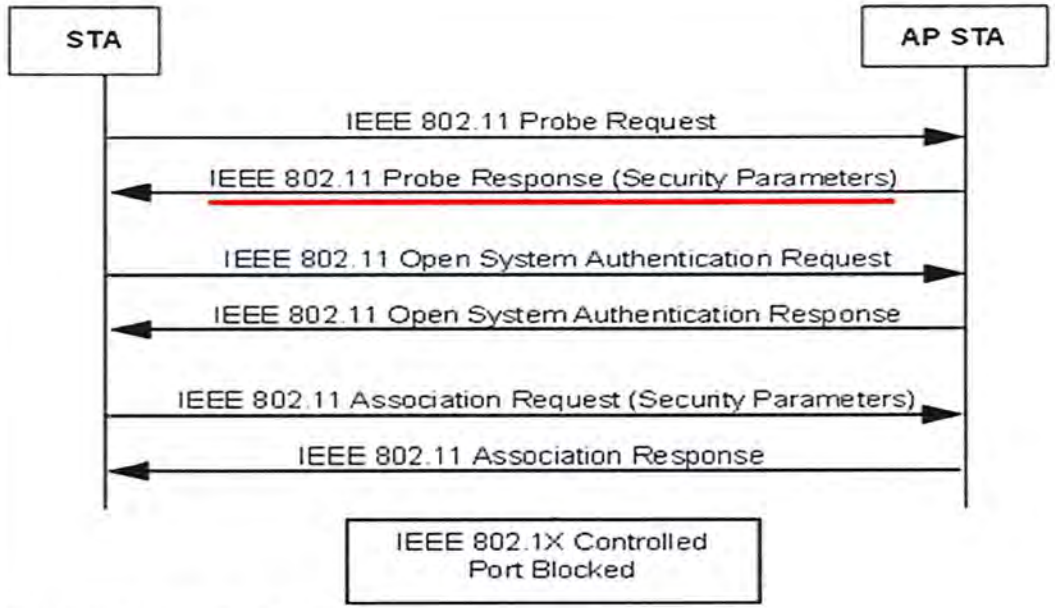
MAC addresses are used by devices when connecting to a Wi-Fi network or an access point. Because these MAC addresses are transmitted without encryption, they can be captured and used to potentially track a user's location. Historically, devices use the *factory MAC address* to associate to a Wi-Fi network.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

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

Table 8-27—Probe Response frame body

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability	
4	SSID	If dot11MeshActivated is true, the SSID element is the wildcard value as described in 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

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

Source: IEEE 802.11-2012.pdf

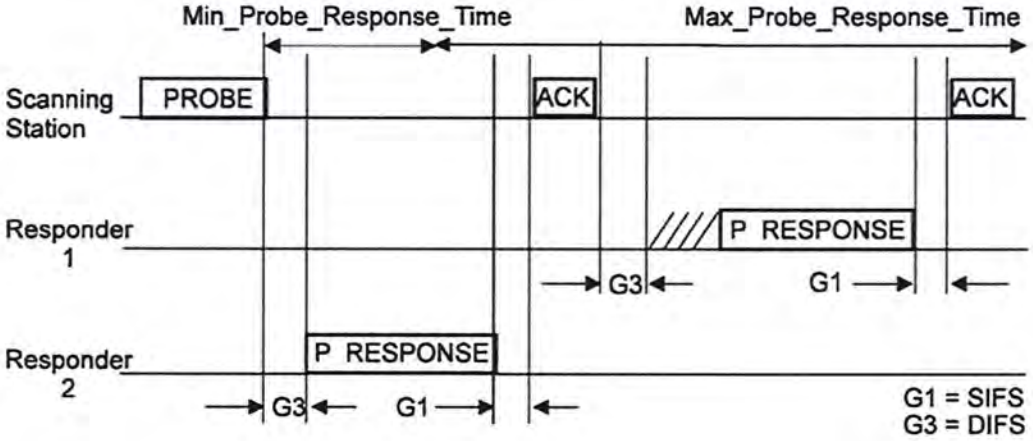
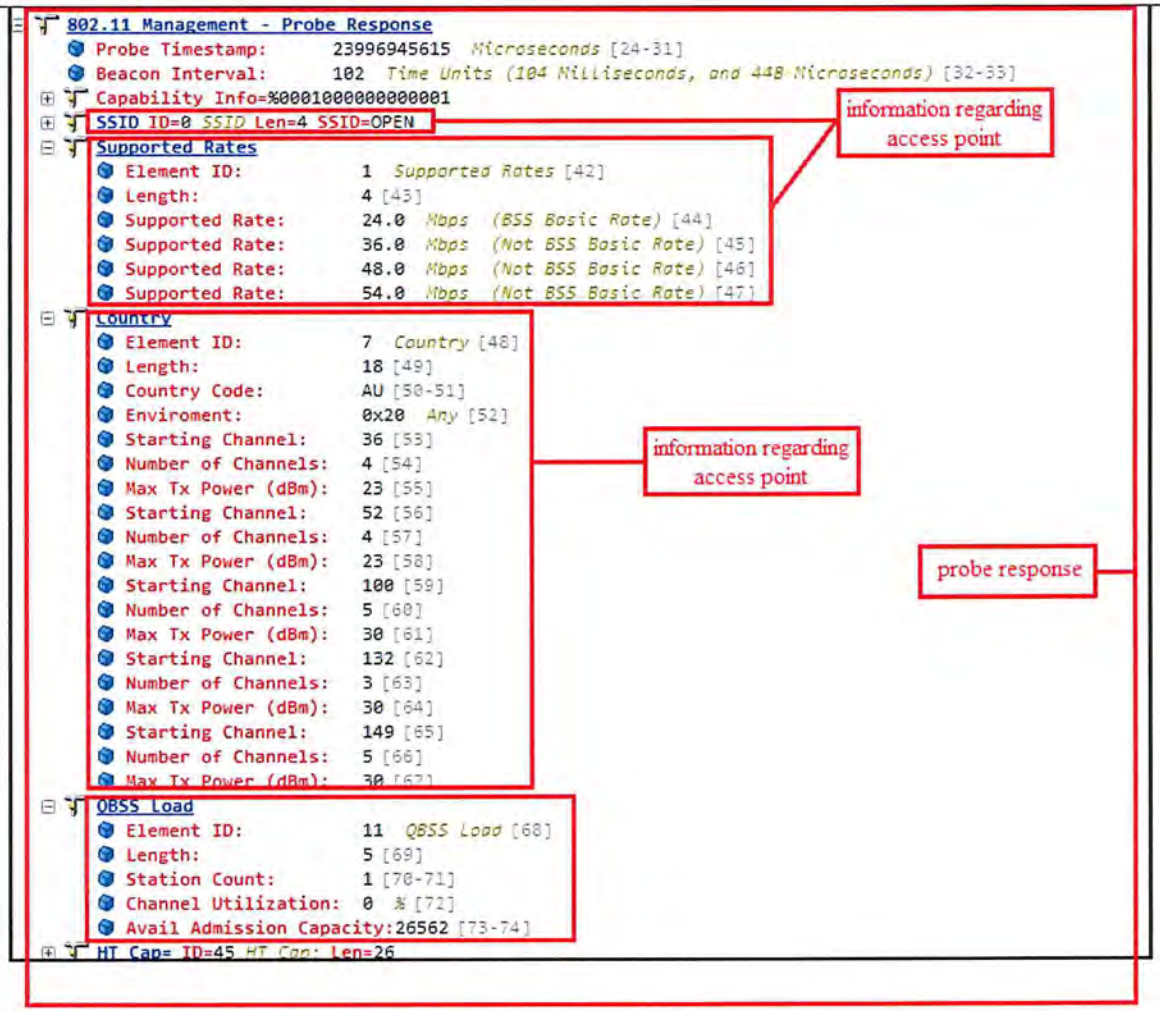


Figure 10-3—Probe response

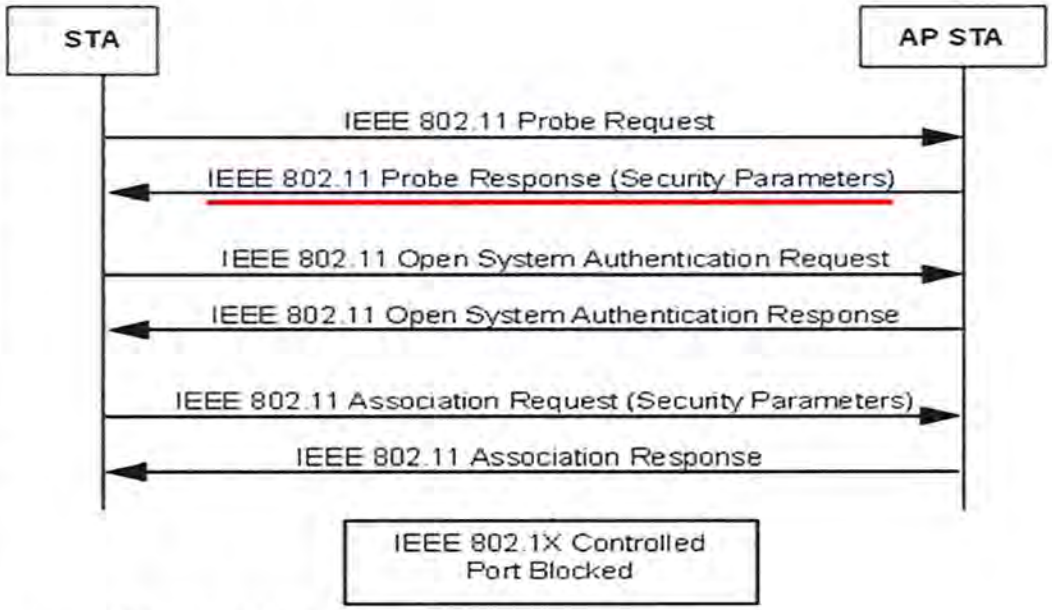
Source: IEEE 802.11-2012.pdf

	Before answering the question, let us first understand what a preferred network list is. The PNL is a historical record of all the network names (SSIDs) that a device has previously connected to, and trusts to automatically connect to again in the future. User devices trying to connect to a Wi-Fi network watch for access points (APs) broadcasting its availability for a device to connect to its network. Within that information contains the network name, or Service Set Identifier (SSID). Wi-Fi enabled devices trying to connect to a wireless network, and using Active Service Discovery, will then broadcast its interest in connecting to the AP if the network name is in its PNL, which increases the connection speed. For instance, if you connect to a **Starbucks** Wi-Fi network once, your device will remember and try to automatically connect to any network with the SSID **Starbucks**. This is true whether you go to the same Starbucks in the future, or a Starbucks 1,000 miles away. All the user device knows is the network name; no additional data is stored. Auto-connecting to wireless networks in PNL saves time and is convenient for the user, but it is a security risk. Therefore, it is important to identify all networks in the PNL and stop connecting automatically to Wi-Fi to stay safe. https://blog.pulsarsecurity.com/preferred-network-list-pnl The reason for client scanning is to determine a suitable AP to which the client may need to roam now or in the future. A client can use two scanning methods: active and passive. During an active scan, the client radio transmits a probe request and listens for a probe response from an AP. With a passive scan, the client radio listens on each channel for beacons sent periodically by an AP. A passive scan generally takes more time, since the client must listen and wait for a beacon versus actively probing to find an AP. Another limitation with a passive scan is that if the client does not wait long enough on a channel, then the client may miss an AP beacon. https://www.wi-fi.org/knowledge-center/faq/what-are-passive-and-active-scanning Below is an example Wi-Fi probe response that includes information of the access point.



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

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

[15e] determining, in response to the receiving the probe response frame and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point, wherein the determining whether the at least one access point is the authenticated access point includes determining whether the information regarding the at least one access point is included in the authenticated access point list that is received from the server, and wherein the determining whether the information regarding the at least	The Accused Products determine in response to receiving the probe response frame and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point, wherein the determining whether the at least one access point is the authenticated access point includes determining whether the information regarding the at least one access point is included in the authenticated access point list that is received from the server, and wherein the determining whether the information regarding the at least one access point is included in the authenticated access point list includes determining whether the at least one access point is under control of the server As an example, the Accused Product receives a probe response frame in response to a probe request.  *Source: IEEE 802.11-2012.pdf*

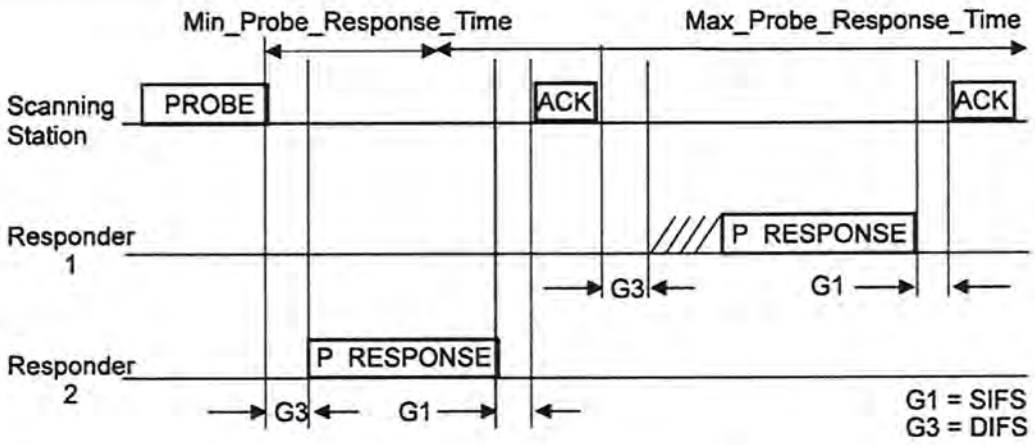
one access point is included in the authenticated access point list includes determining whether the at least one access point is under control of the server; and	 **Figure 10-3—Probe response** *Source: IEEE 802.11-2012.pdf* Information regarding the access point is included in the probe response, as shown below.

Table 8-27—Probe Response frame body

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability	
4	SSID	If dot11MeshActivated is true, the SSID element is the wildcard value as described in 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

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

Source: IEEE 802.11-2012.pdf

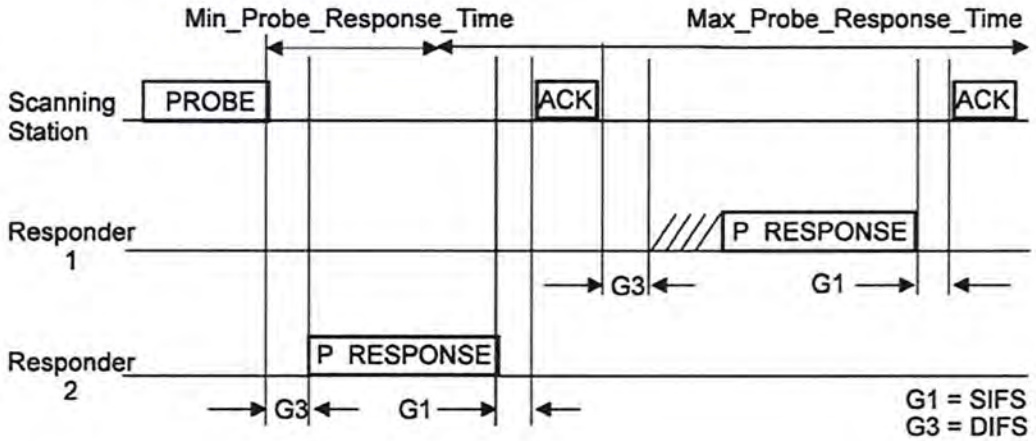
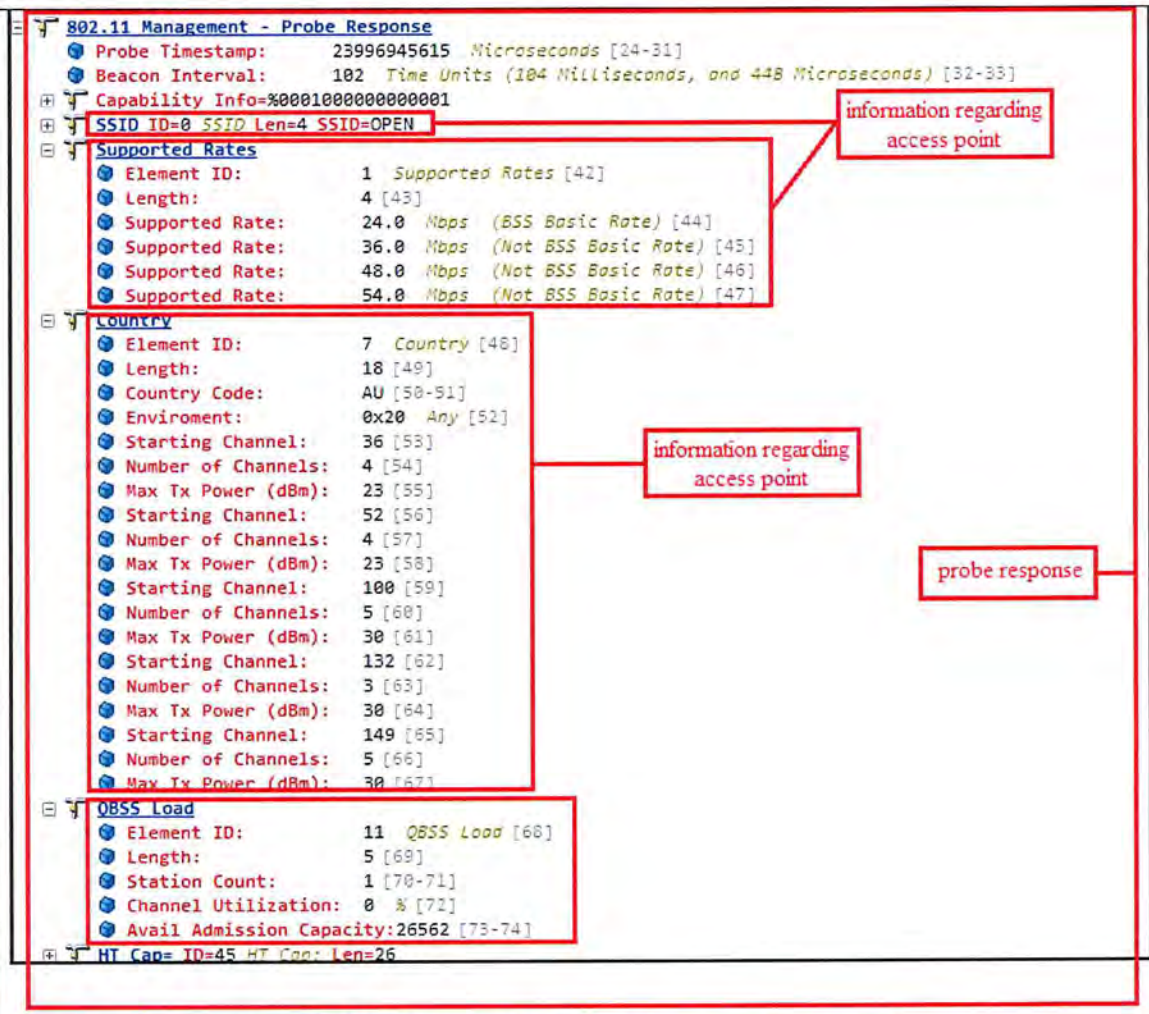


Figure 10-3—Probe response

Source: IEEE 802.11-2012.pdf

	Before answering the question, let us first understand what a preferred network list is. The PNL is a historical record of all the network names (SSIDs) that a device has previously connected to, and trusts to automatically connect to again in the future. User devices trying to connect to a Wi-Fi network watch for access points (APs) broadcasting its availability for a device to connect to its network. Within that information contains the network name, or Service Set Identifier (SSID). Wi-Fi enabled devices trying to connect to a wireless network, and using Active Service Discovery, will then broadcast its interest in connecting to the AP if the network name is in its PNL, which increases the connection speed. For instance, if you connect to a **Starbucks** Wi-Fi network once, your device will remember and try to automatically connect to any network with the SSID **Starbucks**. This is true whether you go to the same Starbucks in the future, or a Starbucks 1,000 miles away. All the user device knows is the network name; no additional data is stored. Auto-connecting to wireless networks in PNL saves time and is convenient for the user, but it is a security risk. Therefore, it is important to identify all networks in the PNL and stop connecting automatically to Wi-Fi to stay safe. https://blog.pulsarsecurity.com/preferred-network-list-pnl The reason for client scanning is to determine a suitable AP to which the client may need to roam now or in the future. A client can use two scanning methods: active and passive. During an active scan, the client radio transmits a probe request and listens for a probe response from an AP. With a passive scan, the client radio listens on each channel for beacons sent periodically by an AP. A passive scan generally takes more time, since the client must listen and wait for a beacon versus actively probing to find an AP. Another limitation with a passive scan is that if the client does not wait long enough on a channel, then the client may miss an AP beacon. https://www.wi-fi.org/knowledge-center/faq/what-are-passive-and-active-scanning Below is an example Wi-Fi probe response that includes information of the access point.



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

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

	access point using an authenticated device identifier, such as a persistent MAC address that was used for a prior connection with the access point. The Accused Products determine that the access point is an authenticated access point by determining that it is in the access point list, indicating it was connected previously. As shown, the Accused Products maintain a list of previously-connected access points which is matched to the access point's SSID received in the probe response. Each previously-connected access point is linked to a persistent MAC address for connecting to that access point. **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]

```
<?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" />
                <boolean name="HiddenSSID" value="false" />
```

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

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

Source: IEEE 802.11-2012.pdf

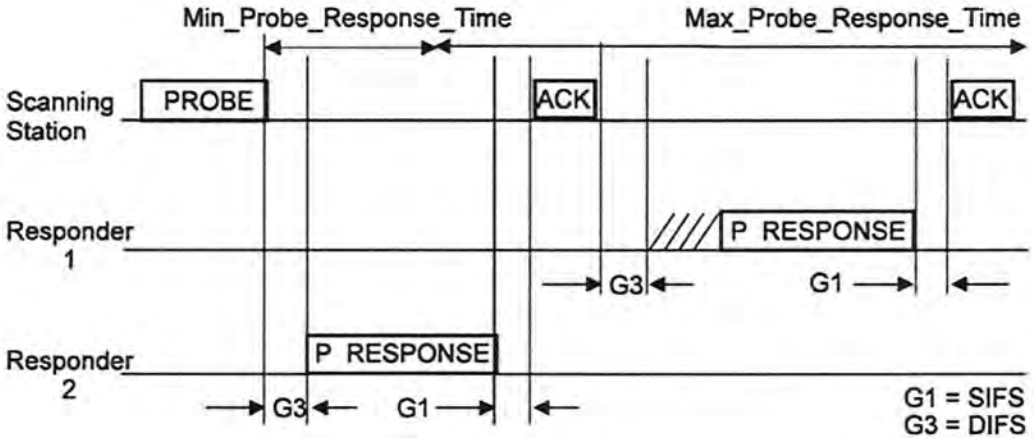
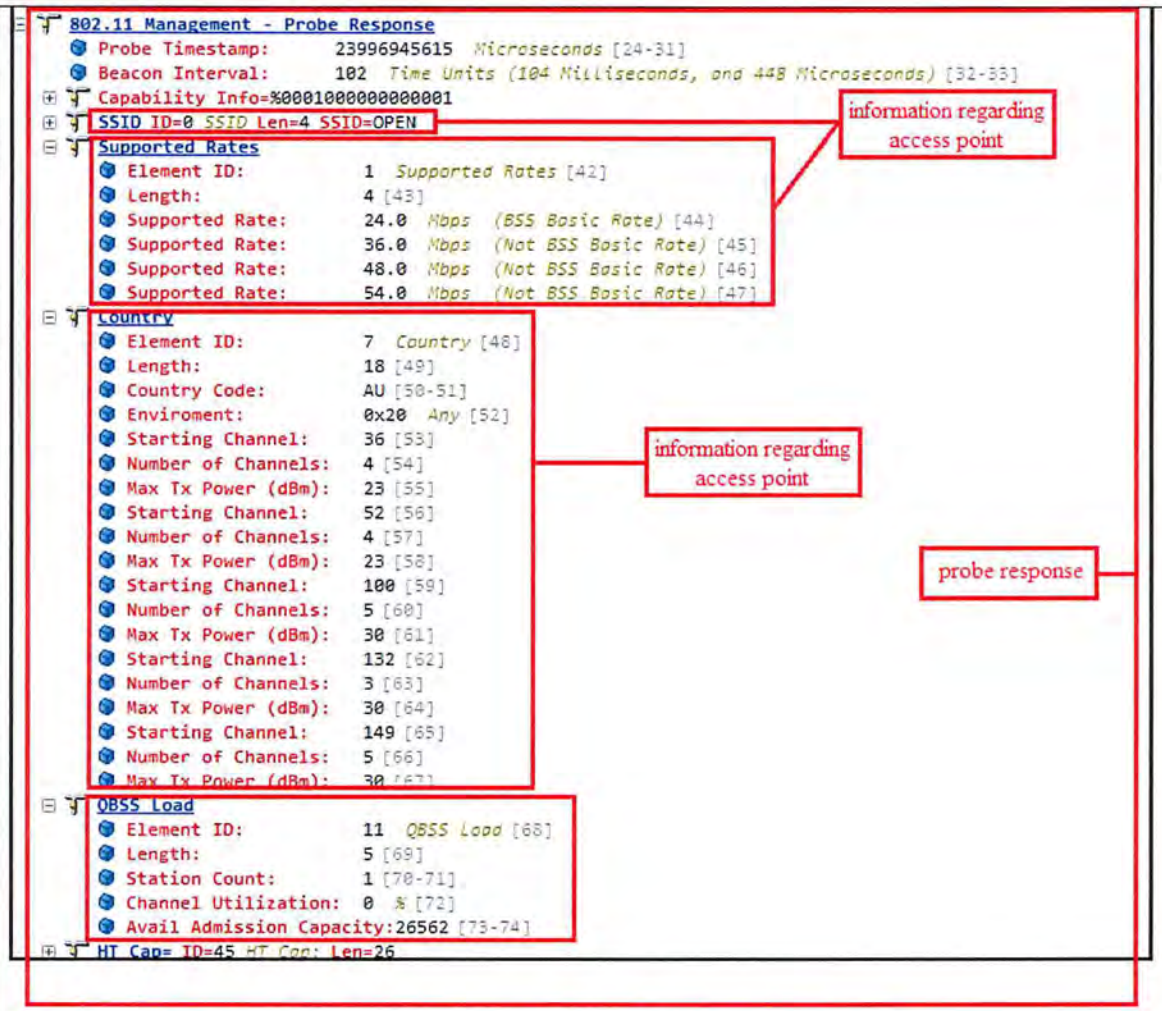


Figure 10-3—Probe response

Source: IEEE 802.11-2012.pdf

	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



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

The Accused Products also determine using information in the probe response that the access points are controlled by the server. For example, the server, which serves the functionality of the Android operating system, controls connection and/or data transmission of the access points. The Accused Products support the Wi-Fi

standard. According to the standard, the Accused Products inquire about available Wi-Fi access points using a probe request, which is generating by the mobile operating server. The probe request comprises identifying information, such as a wildcard SSID or SSID for one or more access points or a preferred network list which is a set of SSIDs to which the UE got connected previously. An access point receiving the probe request must provide a probe response. As a further example, an access point receives and transmits data under control of the mobile operating server.

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

Source: IEEE 802.11-2012.pdf

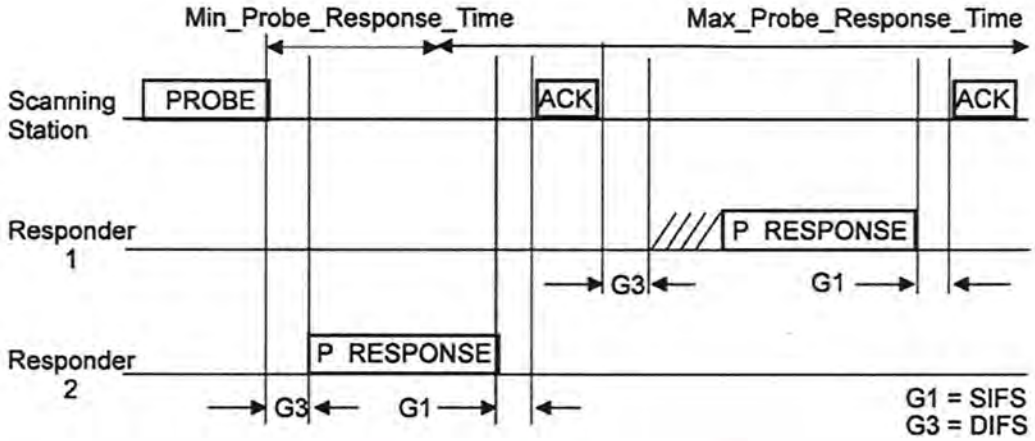
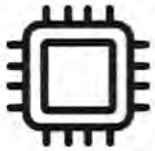


Figure 10-3—Probe response

	Source: IEEE 802.11-2012.pdf The server runs on a CPU of the SoC (e.g., the Kryo CPU) of the accused product. And is used to manage connections with an access point to control those access points to receive and transmit data. 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/



CPU

Kryo CPU

- 64-bit Architecture
- 1 Prime core, up to 3.36 GHz[2]
  - Arm Cortex-X3 technology
- 4 Performance cores, up to 2.8 GHz
- 3 Efficiency cores, up to 2.0 GHz

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

Phone	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



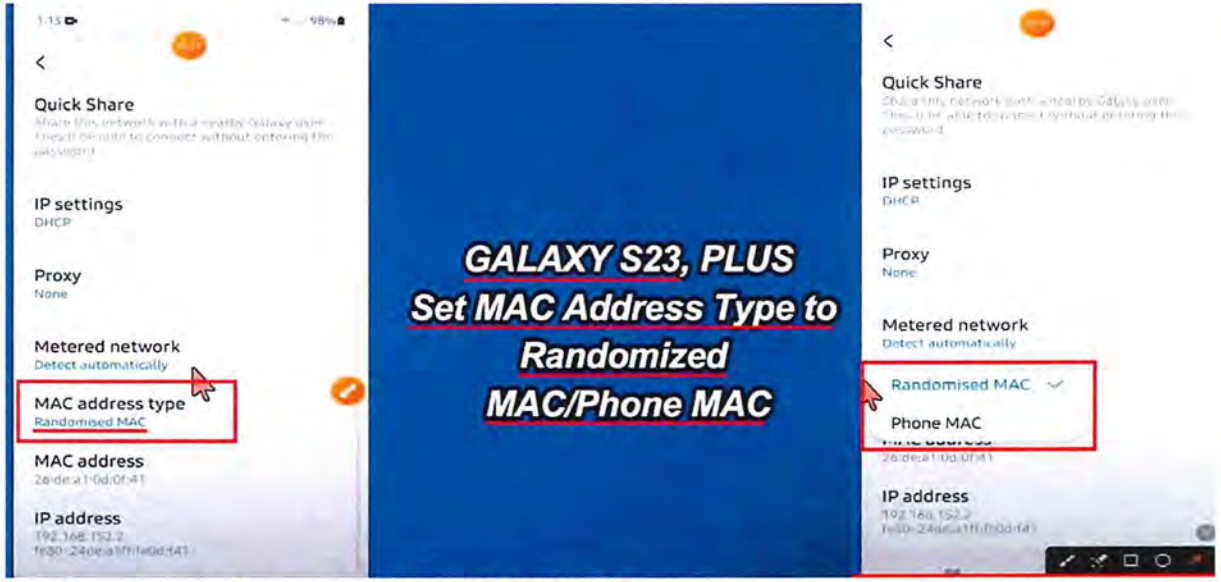
Wi-Fi 6E

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

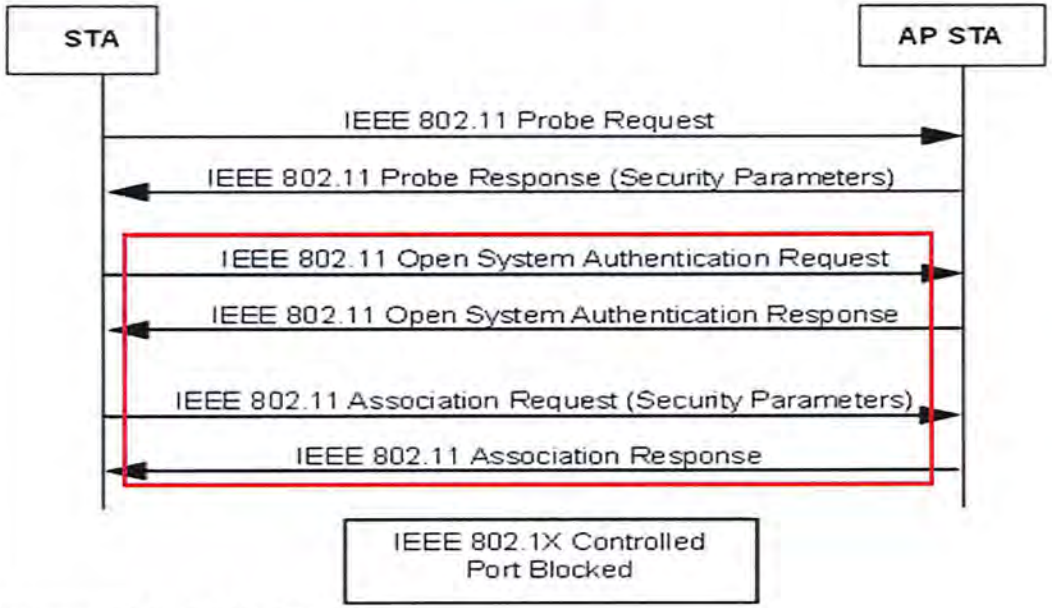


https://www.youtube.com/watch?v=dT63df6nnqU

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

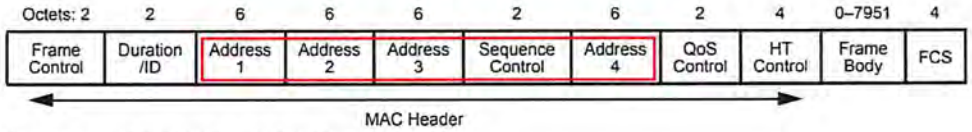
[15f] transmitting, to the at least one access point in response to a determination that the at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the device.	The Accused Products transmit, to the at least one access point in response to a determination that the at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the device. After receiving the probe response from the access point, as discussed above, the Accused Products confirm the received SSID and other information from the probe responses with the access point information stored in memory. Once confirmed that there is an SSID in a probe response from an access point with which the Accused Product was connected previously, the Accused Products initiate a connection using the persistent MAC address for the access point, which is an authentic device identifier for the Accused Product. **Persistent randomization** Android uses the persistent randomization type by default when the MAC randomization feature is enabled. Android generates a persistent randomized MAC address based on the parameters of the network profile including SSID, security type, or FQDN (for Passpoint networks). This MAC address remains the same until factory reset. The MAC address does **not** get re-randomized if the user forgets and re-adds the Wi-Fi network since the MAC 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



Source: IEEE 802.11-2012.pdf

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



Source: IEEE 802.11-2012.pdf

	8.2.4.3.5 DA field The DA field contains an IEEE MAC individual or group address that identifies the MAC entity or entities intended as the final recipient(s) of the MSDU (or fragment thereof) or A-MSDU, as defined in 8.3.2.1, contained in the frame body field. **8.2.4.3.6 SA field** The SA field contains an IEEE MAC individual address that identifies the MAC entity from which the transfer of the MSDU (or fragment thereof) or A-MSDU, as defined in 8.3.2.1, contained in the frame body field was initiated. The individual/group bit is always transmitted as a 0 in the source address. **8.2.4.3.7 RA field** The RA field contains an IEEE MAC individual or group address that identifies the intended immediate recipient STA(s), on the WM, for the information contained in the frame body field. **8.2.4.3.8 TA field** The TA field contains an IEEE MAC individual address that identifies the STA that has transmitted, onto the WM, the MPDU contained in the frame body field. The Individual/Group bit is always transmitted as a 0 in the transmitter address. *Source: IEEE 802.11-2012.pdf*

802.11 Mgmt : Authentication Frame

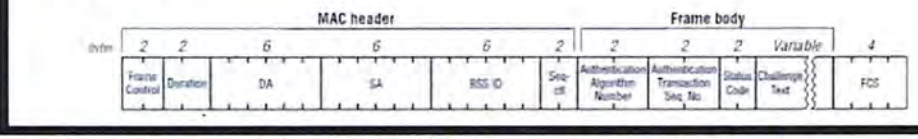
POSTED BY **NAYARASI** IN **CWAP** ≈ **10 COMMENTS**

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

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

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

FIGURE 4.8 Authentication frame format



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

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

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]

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

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

	An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
16. The method of claim 15, wherein the generating the fake device identifier includes generating a fake media access control (MAC) address.	Generating the fake device identifier includes generating a fake media access control (MAC) address. The Accused Products generate a fake MAC address that is different from the original MAC address of the hardware by generating a randomized MAC address for use in probe requests. **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 An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
17. The method of claim 15, wherein the information regarding the at least one access point includes at least one of a media access control (MAC) address of the at least one access	The information regarding the at least one access point includes at least one of a media access control (MAC) address of the at least one access point or a service set identifier (SSID) of the at least one access point. The Accused Products support the Wi-Fi standard. The Accused Products receive the probe responses from multiple available access points. An access point responds with the probe response only when the SSID in the probe request is the wildcard SSID or matches the specific SSID of the access point or when the specific SSID of the access point is included in the SSID List element. As a further example, an access point responds to a probe request when it supports data rates or other requirements of the Accused Products.

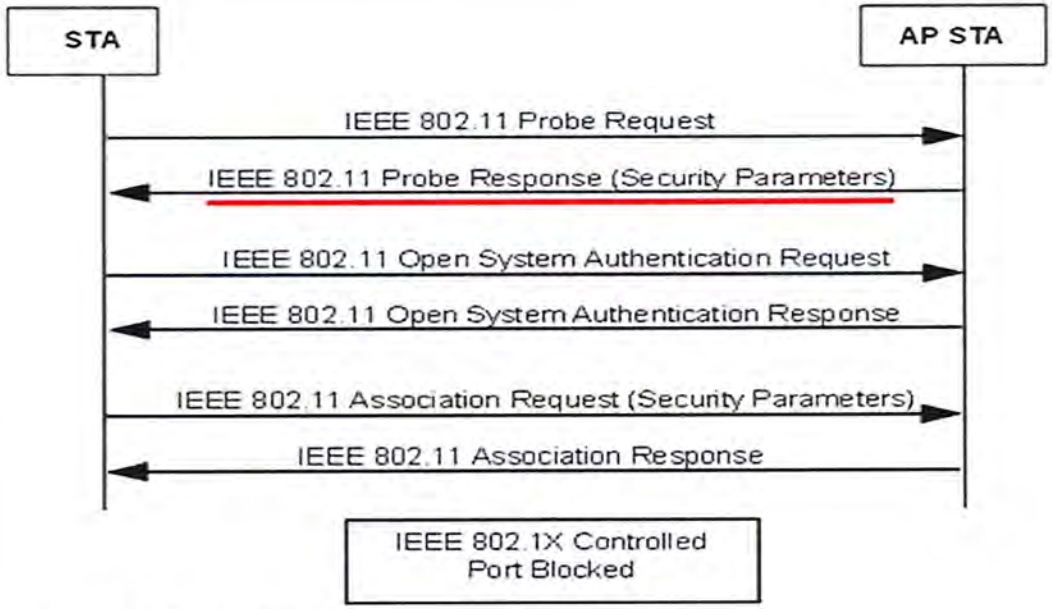
point or a service set identifier (SSID) of the at least one access point.	 *Source: IEEE 802.11-2012.pdf*

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

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

Source: IEEE 802.11-2012.pdf

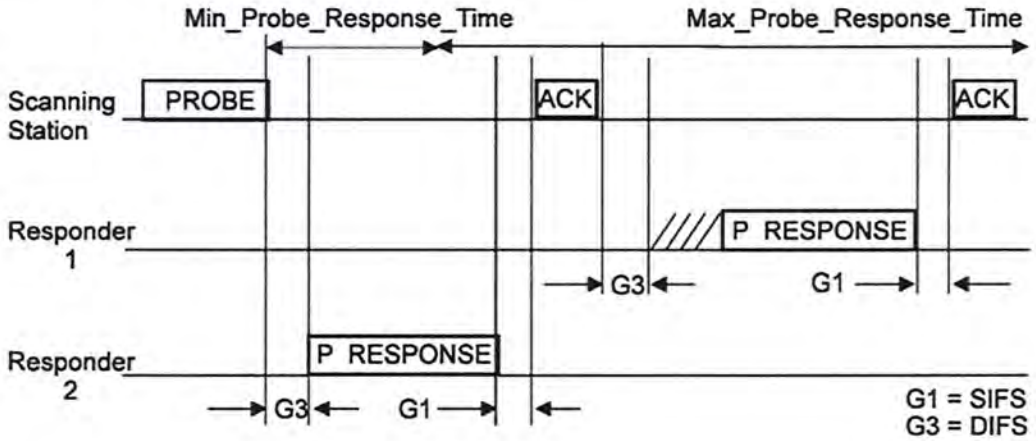
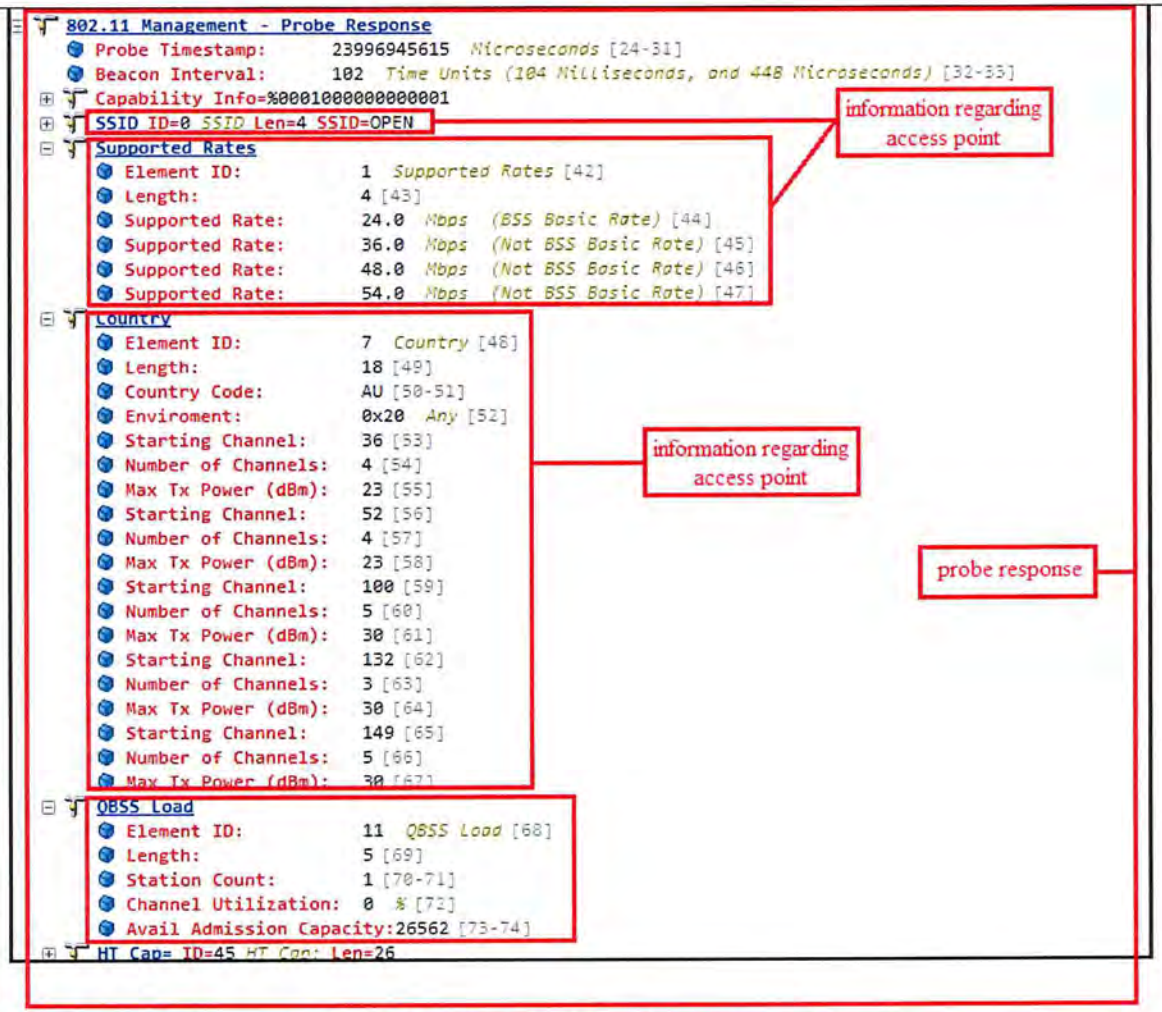


Figure 10-3—Probe response

Source: IEEE 802.11-2012.pdf

	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/

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

18. The method of claim 15, wherein the determining whether the at least one access point is the authenticated access point further includes determining whether the at least one access point was previously connected with the device.	The Accused Products practice a method wherein the determining whether the at least one access point is the authenticated access point further includes determining whether the at least one access point was previously connected with the device. As an example, the Accused Product confirms the received SSID information and/or other information from probe responses with access point information stored in its memory. Once confirmed that there is a probe response from an access point with which the Accused Product was connected previously, the Accused Product initiates a connection to the access point using an authenticated device identifier, such as a persistent MAC address that was used for a prior connection with the access point. As shown, the Accused Products maintain a list of previously-connected access points which is matched to the access point's SSID received in the probe response. Each previously-connected access point is linked to a persistent MAC address for connecting to that access point. **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]

```
<?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" />
                <boolean name="HiddenSSID" value="false" />
```

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

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

Source: IEEE 802.11-2012.pdf

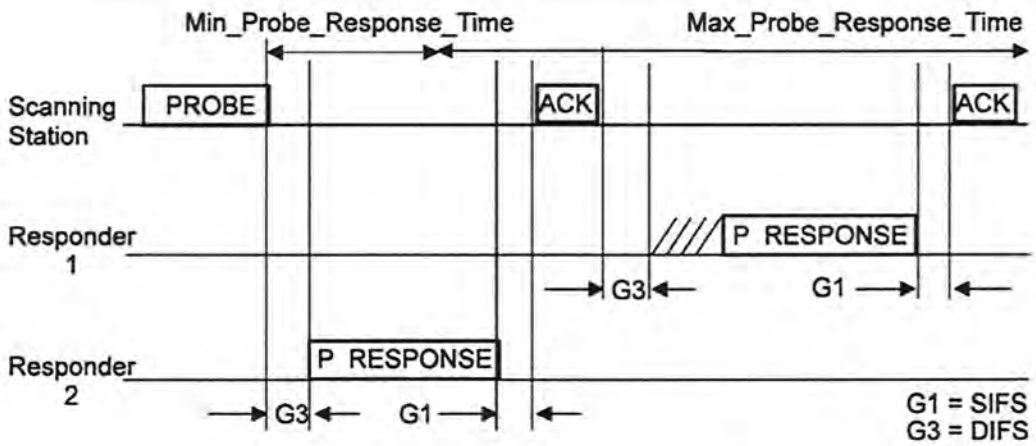
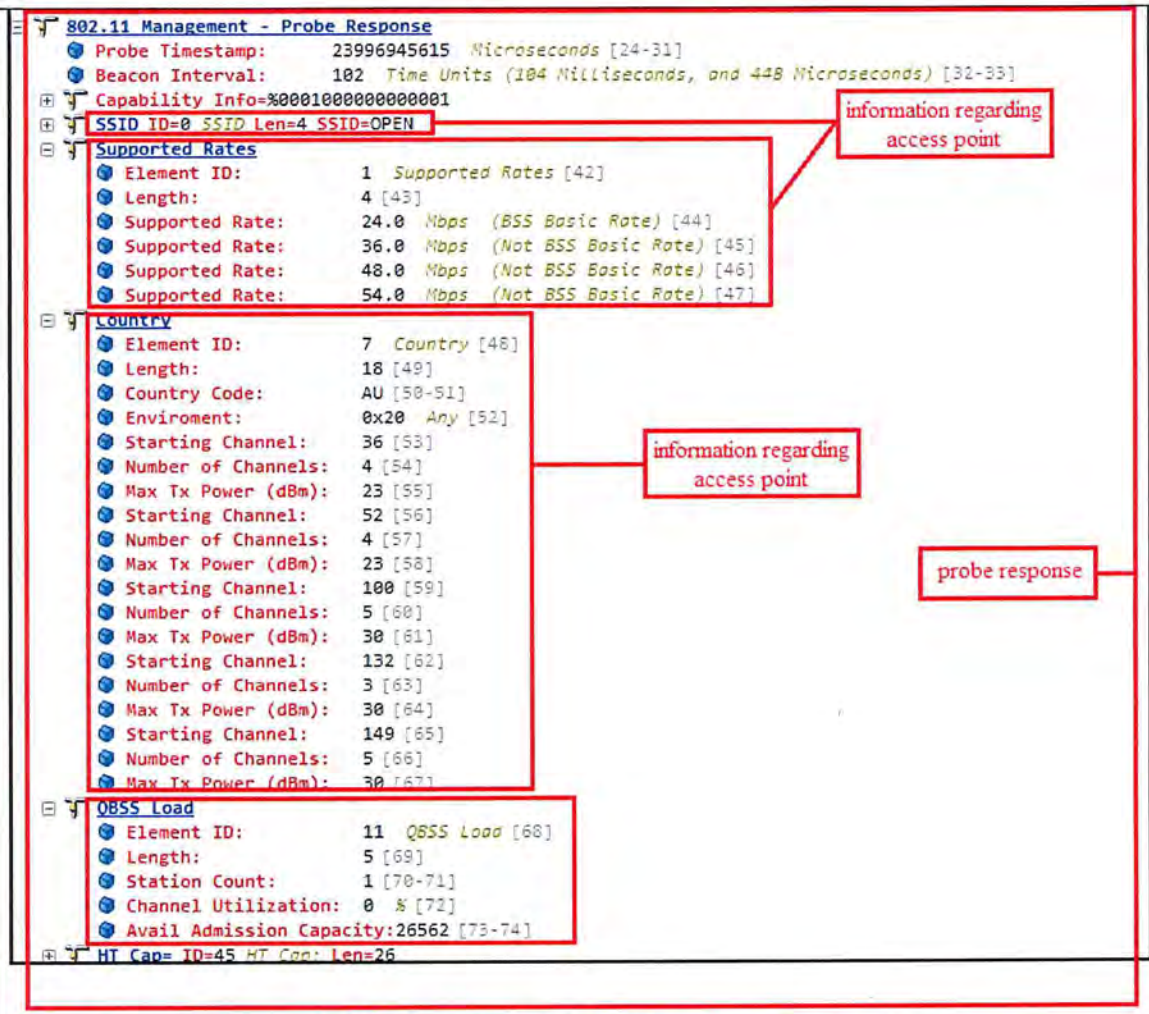


Figure 10-3—Probe response

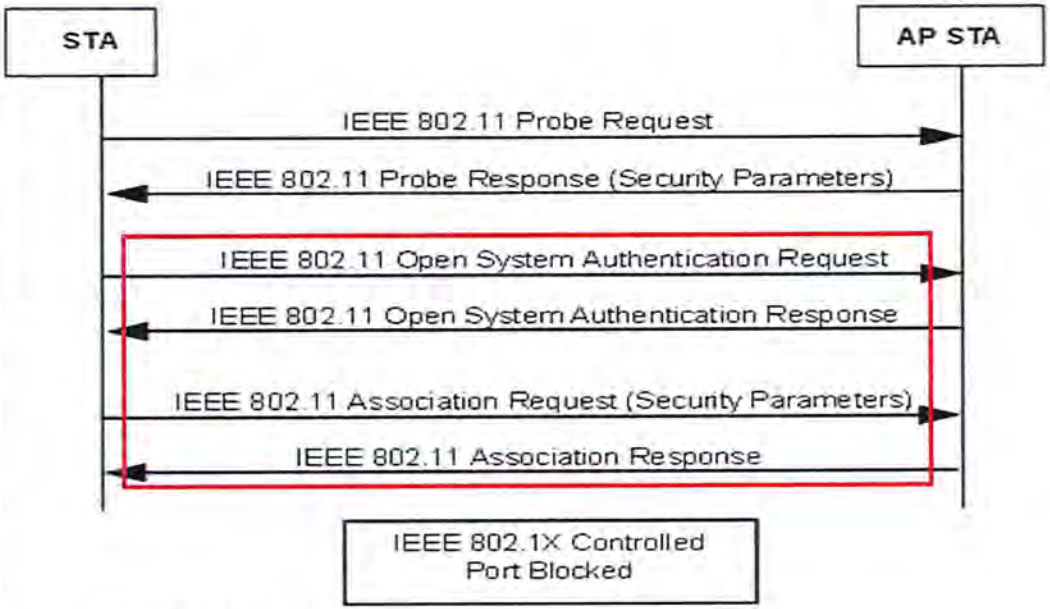
Source: IEEE 802.11-2012.pdf

	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

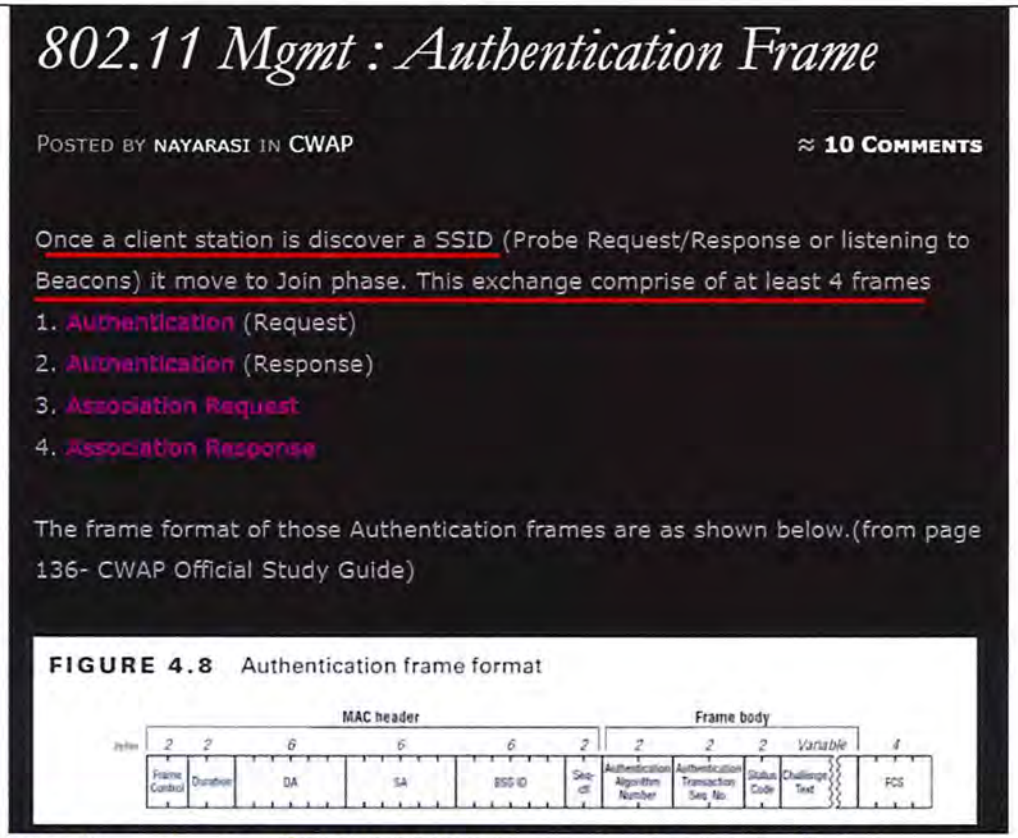


https://mrncciew.com/2014/10/27/cwap-802-11-probe-requestresponse/

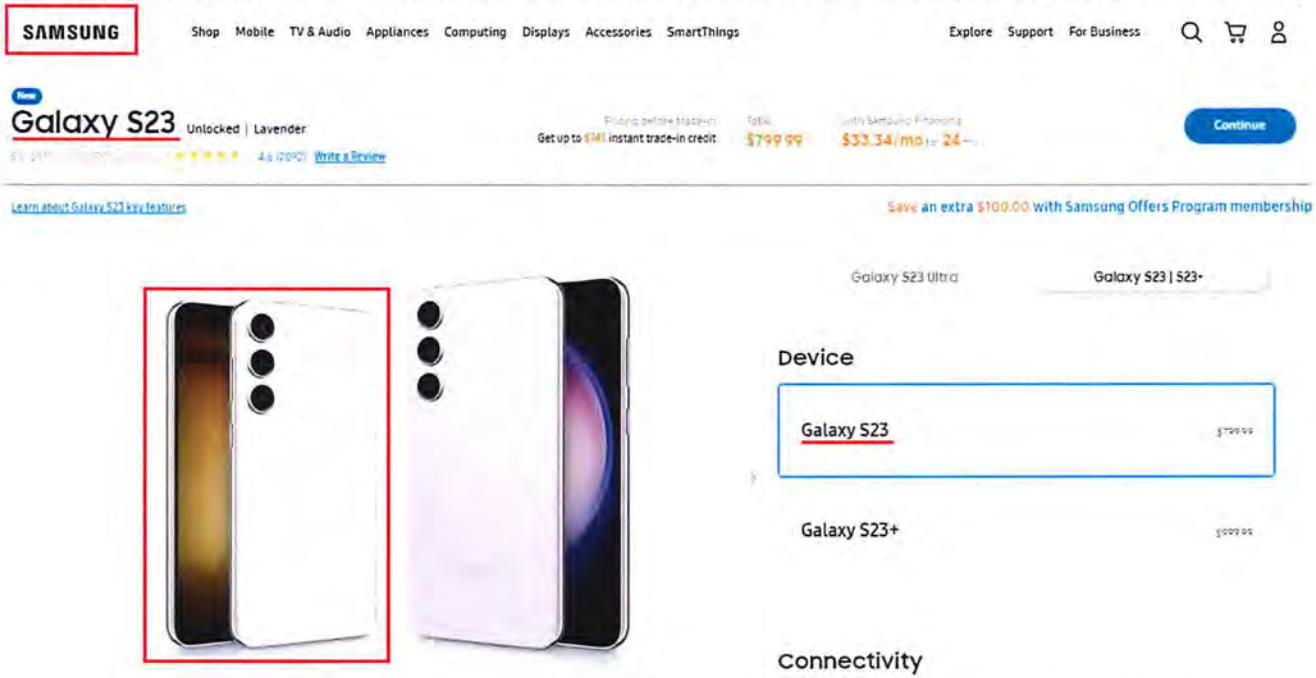
An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.

20. The method of claim 15, further comprising: receiving, from the at least one access point, an approval of the connection request; transmitting, to the at least one access point in response to the receiving the approval of the connection request, an association request; receiving, from the at least one access point, an association response to the association request; and connecting to a communication network via the at least one access point in accordance	The Accused Products receive, from the at least one access point, an approval of the connection request, transmit, to the at least one access point in response to the receiving the approval of the connection request, an association request, receive, from the at least one access point, an association response to the association request, and connect to a communication network via the at least one access point in accordance with the association response. As an example, the Accused Products receive an open system authentication response from an access point. The Accused Products then transmit an association request. The Accused Products then receive an association response from the access point, at which point the Accused Product is connected to a network via the access point in accordance with the association response.  *Source: IEEE 802.11-2012.pdf*

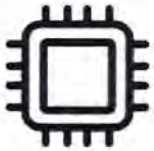
with the association response.	**8.2.4.3.5 DA field** The DA field contains an IEEE MAC individual or group address that identifies the MAC entity or entities intended as the final recipient(s) of the MSDU (or fragment thereof) or A-MSDU, as defined in 8.3.2.1, contained in the frame body field. **8.2.4.3.6 SA field** The SA field contains an IEEE MAC individual address that identifies the MAC entity from which the transfer of the MSDU (or fragment thereof) or A-MSDU, as defined in 8.3.2.1, contained in the frame body field was initiated. The individual/group bit is always transmitted as a 0 in the source address. **8.2.4.3.7 RA field** The RA field contains an IEEE MAC individual or group address that identifies the intended immediate recipient STA(s), on the WM, for the information contained in the frame body field. **8.2.4.3.8 TA field** The TA field contains an IEEE MAC individual address that identifies the STA that has transmitted, onto the WM, the MPDU contained in the frame body field. The Individual/Group bit is always transmitted as a 0 in the transmitter address. *Source: IEEE 802.11-2012.pdf*

	 https://mrncciew.com/2014/10/10/802-11-mgmt-authentication-frame/ An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
21. A method performed by a device, the method comprising:	To the extent the preamble is limiting, the Accused Products practice a method performed by a device. The Accused Products include Android OS 10 or above or Wear OS 3 or above. Each Accused Product includes an SoC and Wi-Fi connection functionality. As a specific example shown below, the Galaxy S23 includes the

Android 13 operating system, which includes randomized MAC for Wi-Fi connections. It comprises an SoC, Snapdragon 8 Gen 2, a Wi-Fi chipset, and FastConnect. It connects to a Wi-Fi network using the Wi-Fi chipset.



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

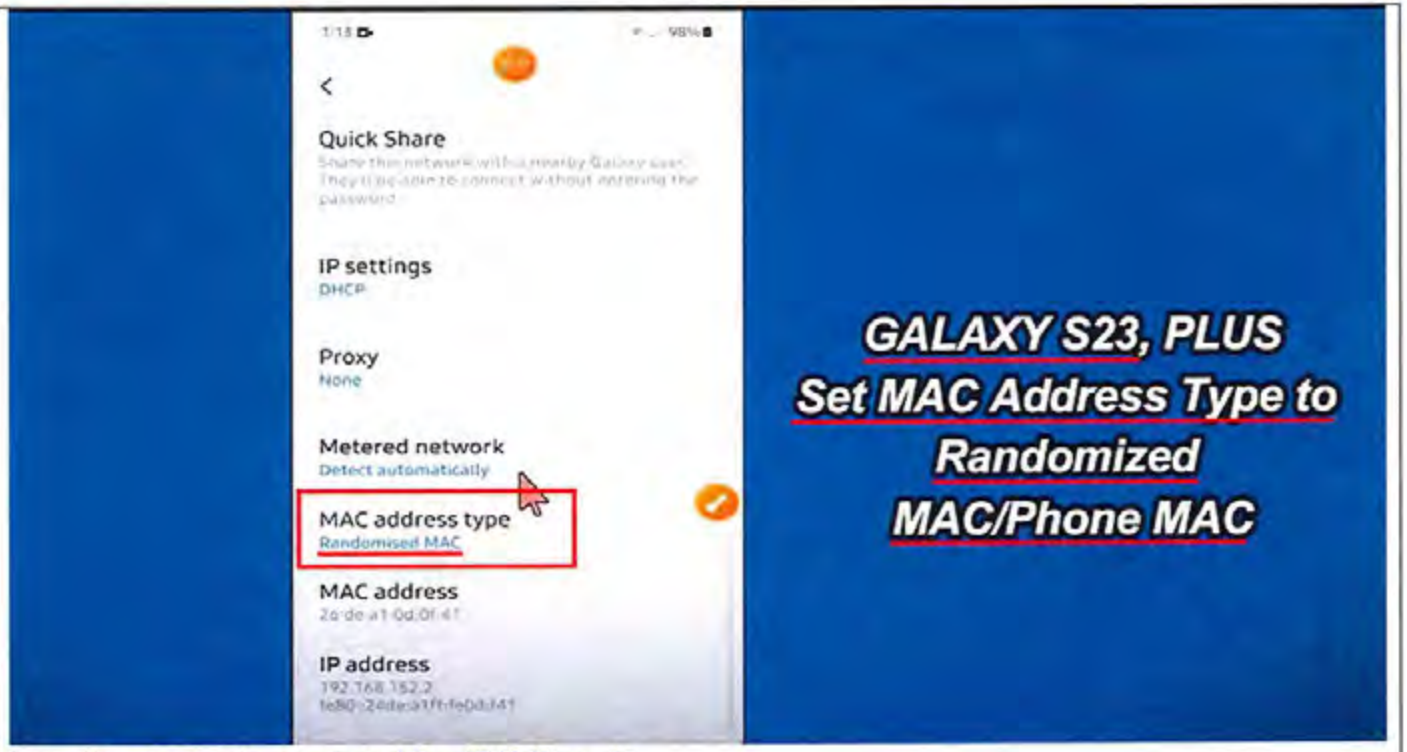
	Galaxy S23  Super fast processing Snapdragon® 8 Gen 2 Octa-Core https://www.samsung.com/us/smartphones/galaxy-s23/specs/

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

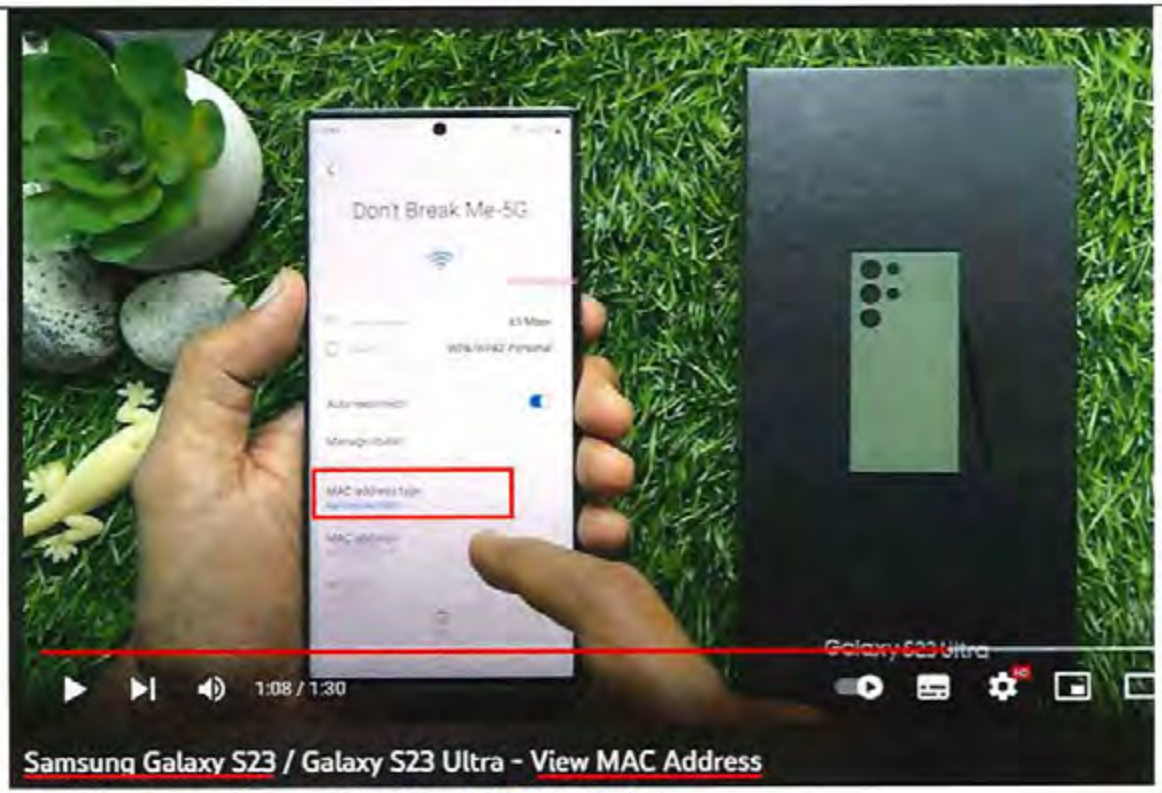
https://www.androidpolice.com/samsung-galaxy-s23/



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



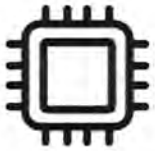
https://www.youtube.com/watch?v=dT63df6nnqU



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

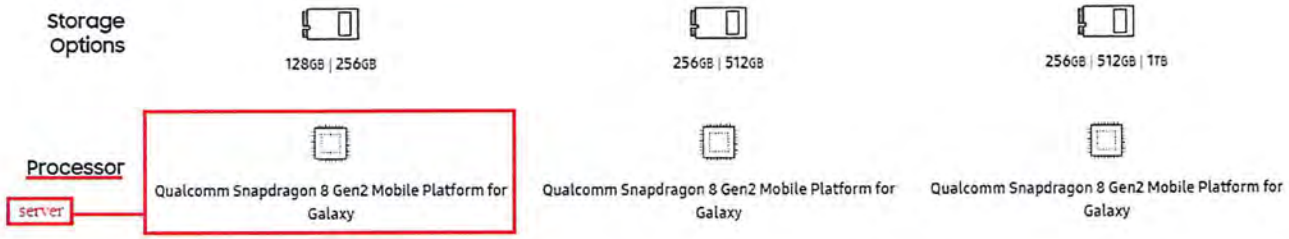
	Featuring the Snapdragon X70 5G Modem RF System, Snapdragon 8 Gen 2 is the world's first and only mobile platform with a dedicated 5G AI processor. Plus, gaming, streaming, and communication from home soar via Wi-Fi 7 (the industry's lowest latency offering), all brought to you by the Qualcomm® FastConnect™ 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 MAC Randomization is implemented in devices running the Android OS since at least Android OS 10 as well as Wear OS 3.0.

	In Android 10, MAC randomization is enabled by default for client mode, SoftAp, and Wi-Fi Direct. MAC randomization prevents listeners from using MAC addresses to build a history of device activity, thus increasing user privacy. Additionally, MAC addresses are randomized as part of Wi-Fi Aware and Wi-Fi RTT operations. For more information, see MAC Randomization Behavior. https://source.android.com/docs/core/connect/wifi-mac-randomization Wear OS, including Wear OS 3.0, is based on Android. *See* https://developer.android.com/training/wearables/wear-v-mobile#:~:text=Wear%20OS%20is%20based%20on,design%20a%20Wear%20OS%20app. Devices operating on Wear OS 3.0 implement MAC randomization. *See* https://www.reddit.com/r/GalaxyWatch/comments/pcmkj1/galaxy_watch_4_wifi_mac_address/
[21a] receiving, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;	The Accused Products receive, from a server (e.g., the OS and/or a CPU and associated memory for storing and executing the OS and associated data), an authenticated access point list (e.g., previously connected access point list) that includes information (e.g., SSID, supported data rates, pre-shared keys, etc.) regarding one or more access points (e.g., previously connected access point) that are controlled by the server. As shown below, an example of the Accused Products contains an SoC, Snapdragon 8 Gen 2 with a Kryo CPU. Also, it supports Android 13 operating system and has an option for randomized MAC for Wi-Fi connections. The server generates a persistent randomized MAC address to be used with a Wi-Fi network. The server also stores a list of previously connected access points and provides that list to the device in connecting to Wi-Fi access points. The list comprises different information pertaining to previously connected access points such as SSID, pre-shared keys, etc.

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



CPU

Kryo CPU

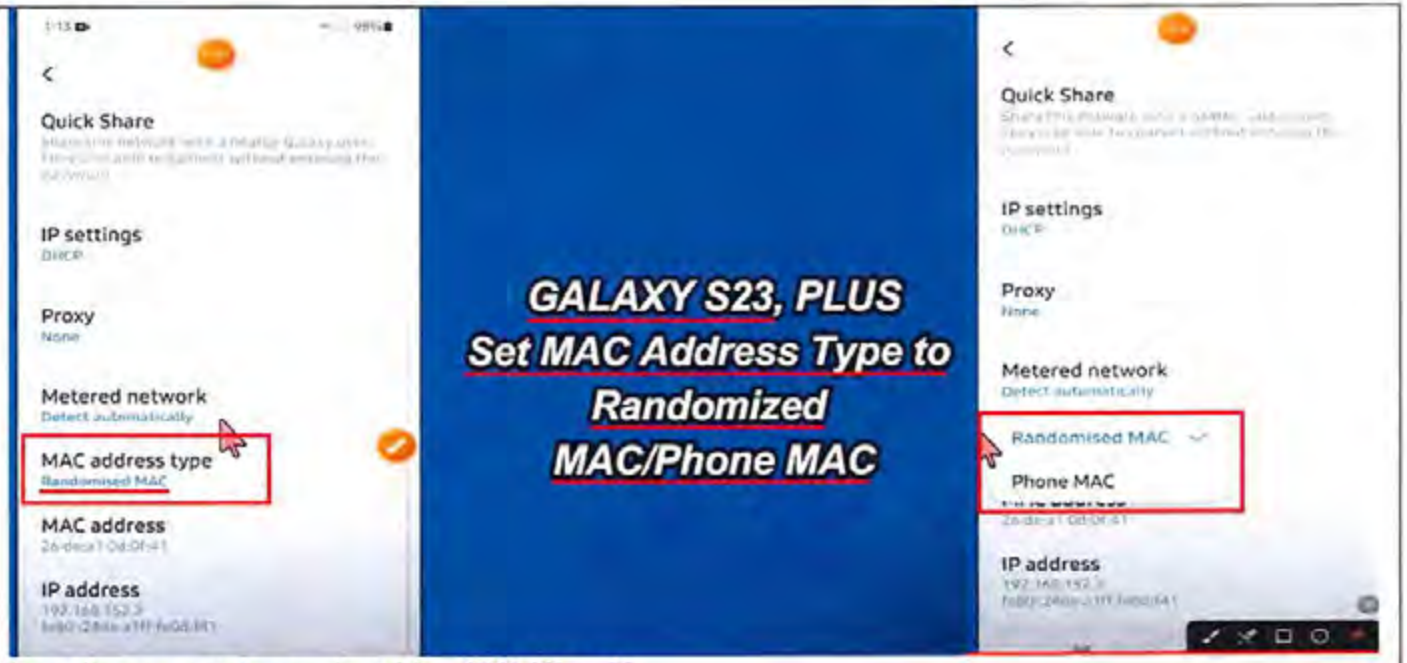
- 64-bit Architecture
- 1 Prime core, up to 3.36 GHz[2]
  - Arm Cortex-X3 technology
- 4 Performance cores, up to 2.8 GHz
- 3 Efficiency cores, up to 2.0 GHz

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

Phone	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

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>
```

previously connected access-points information list

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

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

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]

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

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

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

Source: IEEE 802.11-2012.pdf

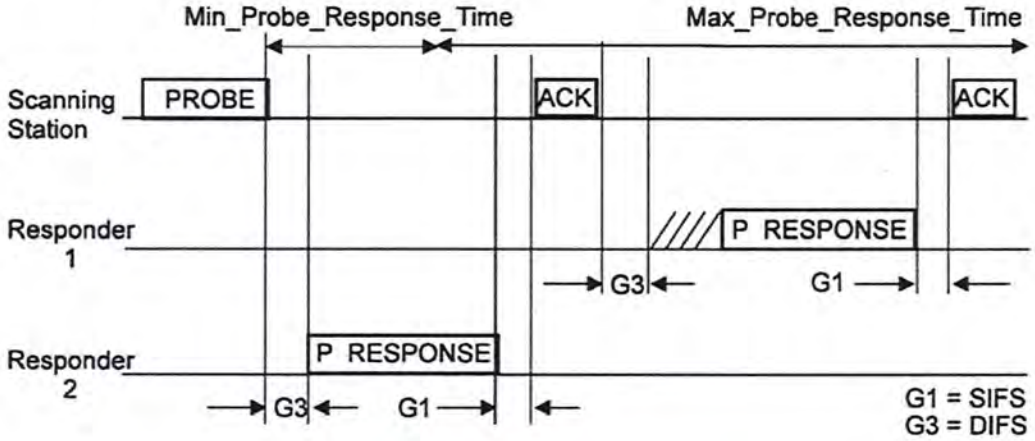
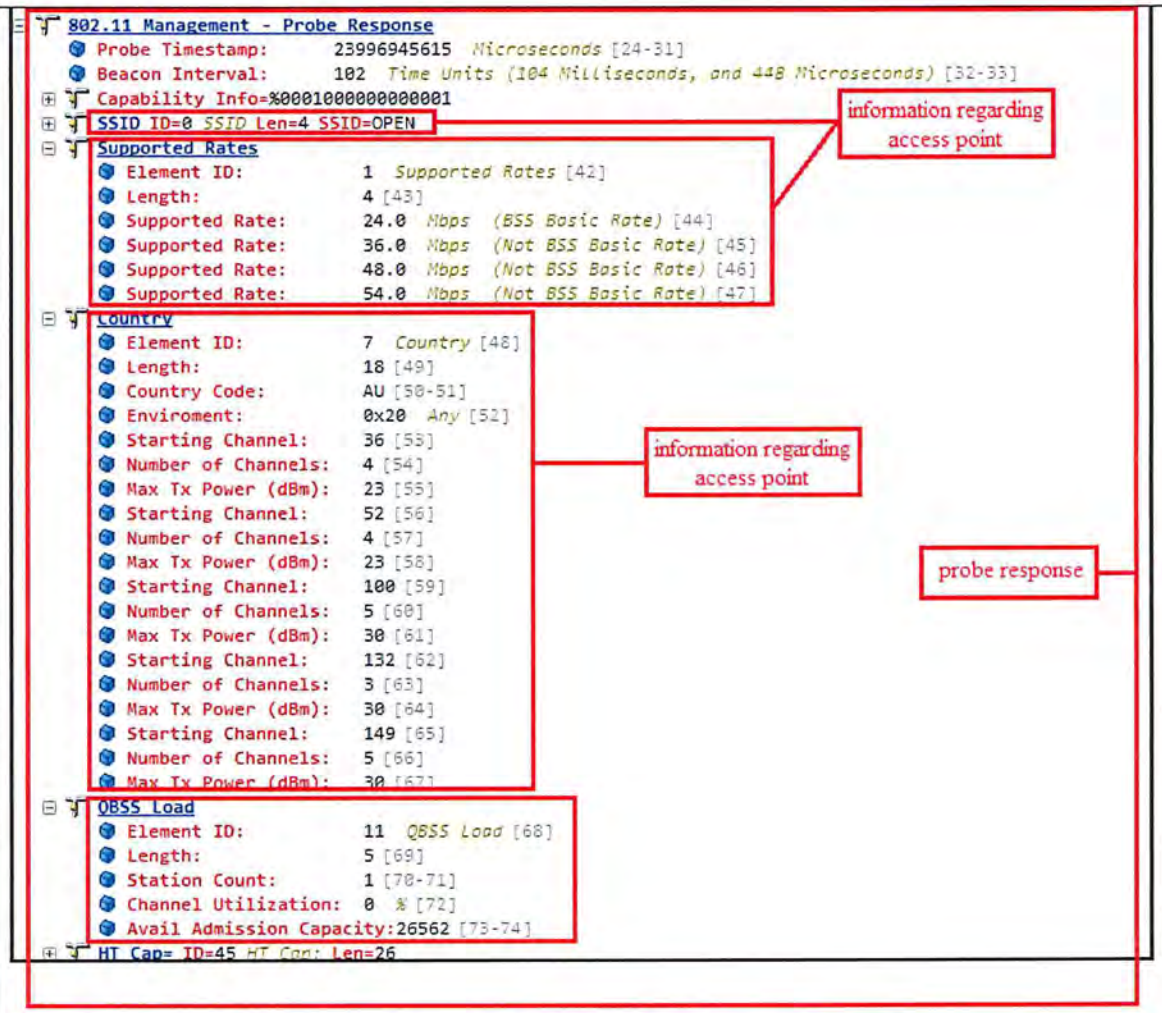


Figure 10-3—Probe response

Source: IEEE 802.11-2012.pdf

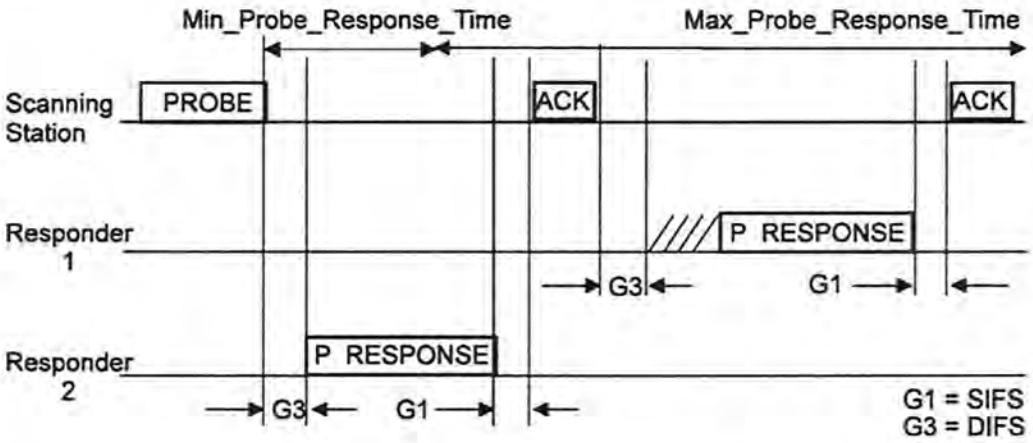
	Before answering the question, let us first understand what a preferred network list is. The PNL is a historical record of all the network names (SSIDs) that a device has previously connected to, and trusts to automatically connect to again in the future. User devices trying to connect to a Wi-Fi network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

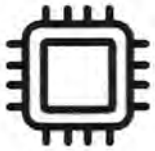


https://mrncciew.com/2014/10/27/cwap-802-11-probe-requestresponse/

The access points are controlled by the server. For example, the server, which serves the functionality of the Android operating system, controls connection and/or data transmission of the access points. The Accused

	Products support the Wi-Fi standard. According to the standard, the Accused Products inquire about available Wi-Fi access points using a probe request, which is generated by the mobile operating server. The probe request comprises identifying information, such as a wildcard SSID or SSID for one or more access points, or a preferred network list which is a set of SSIDs to which the UE got connected previously. An access point receiving the probe request must provide a probe response. As a further example, an access point receives and transmits data under control of the mobile operating server. In an infrastructure BSS or in an IBSS, STAs receiving Probe Request frames shall respond with a probe response when the SSID in the probe request is the wildcard SSID or matches the specific SSID of the STA or when the specific SSID of the STA is included in the SSID List element. Furthermore, a STA with dot11RadioMeasurementActivated true receiving a probe request with a DSSS Parameter Set element containing a Current Channel field value that is not the same as the value of dot11CurrentChannel shall not respond with a probe response. An AP shall respond to all probe requests meeting the above criteria. In an IBSS a STA that transmitted a Beacon frame since the last TBTT shall respond to group addressed Probe Request frames. A STA in an IBSS shall respond to Probe Request frames sent to the individual address of the STA. *Source: IEEE 802.11-2012.pdf*

	 **Figure 10-3—Probe response** *Source: IEEE 802.11-2012.pdf* An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
[21b] generating a collection that includes at least one of one or more random numbers or one or more random characters to provide a fake device identifier for the device to falsely identify the device in a probe request frame;	The Accused Products generate a collection that includes at least one of one or more random numbers or one or more random characters to provide a fake device identifier (e.g. randomized MAC address) for the device to falsely identify the device in a probe request (e.g., Wi-Fi probe request). The operating system is used to generate a random MAC address for the device. For example, the operating system generates a persistent randomized MAC address to be used with a Wi-Fi network. The operating system runs on a CPU (e.g., the Kryo CPU) of the SoC of the accused product.

	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/



CPU

Kryo CPU

- 64-bit Architecture
- 1 Prime core, up to 3.36 GHz[2]
  - Arm Cortex-X3 technology
- 4 Performance cores, up to 2.8 GHz
- 3 Efficiency cores, up to 2.0 GHz

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

Phone	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



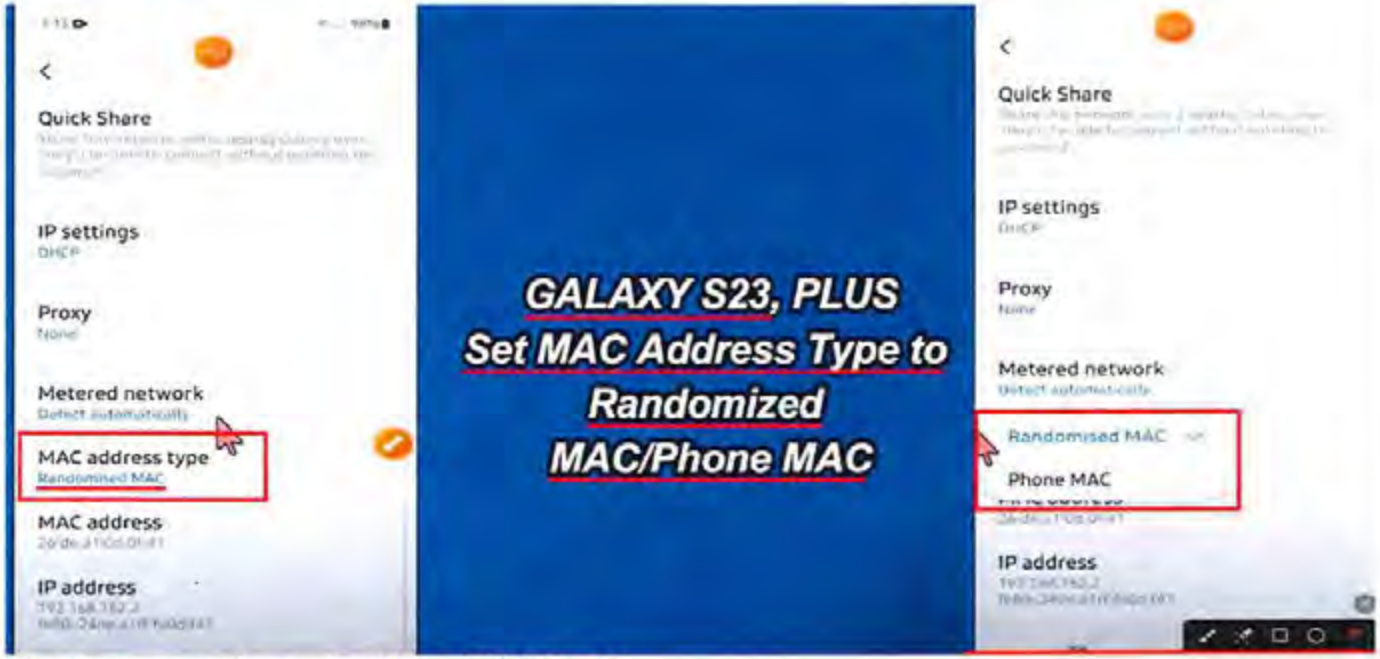
Wi-Fi 6E

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

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

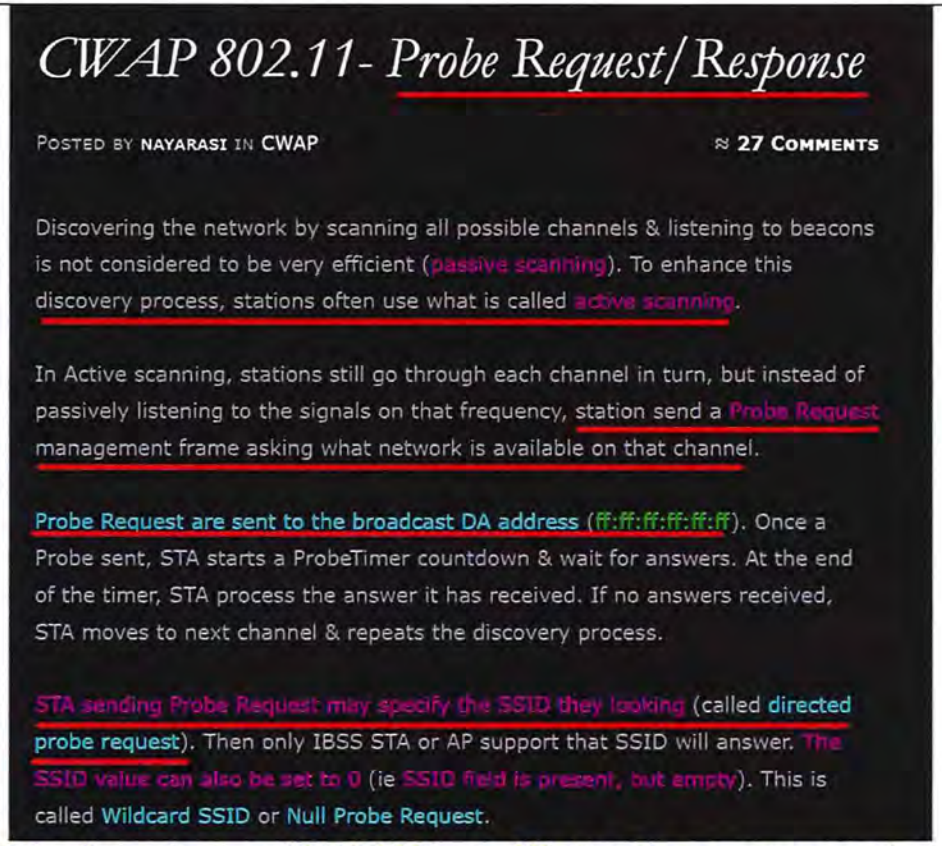
- **Connectivity**: The Galaxy S23 series boasts unparalleled Snapdragon Connect technologies across 5G, Wi-Fi, and Bluetooth®. Featuring the multiple-award-winning Snapdragon X70 5G Modem-RF System with the Qualcomm® 5G AI Processor, the Galaxy S23 series harnesses the power of AI to enable breakthrough 5G coverage, power efficiency, speeds, and latency. These new devices also support 5G+5G/4G Dual-SIM Dual-Active[2], which harnesses the power and flexibility of two 5G SIMs at once. Additionally, all Galaxy S23 series variants feature the Qualcomm® FastConnect™ 6900 and 7800 systems delivering multi-gigabit Wi-Fi speeds, ultra-low latency, and deeply immersive Bluetooth Audio experiences.

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



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

	The Accused Products support the Wi-Fi standard. According to the standard, the Accused Products (each a UE) inquire about available Wi-Fi access points using a probe request. The probe request comprises a sender address field (e.g., device identifier). The server generates a random MAC address for use in the probe request. As shown below, the Accused Products utilize probe request frames. 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/

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

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

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

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

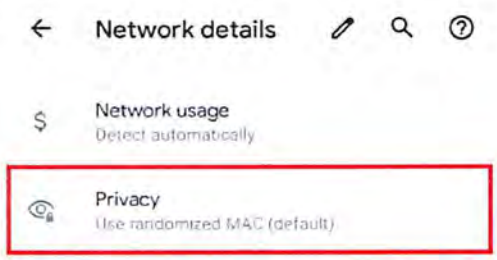


Figure 1. MAC randomization option.

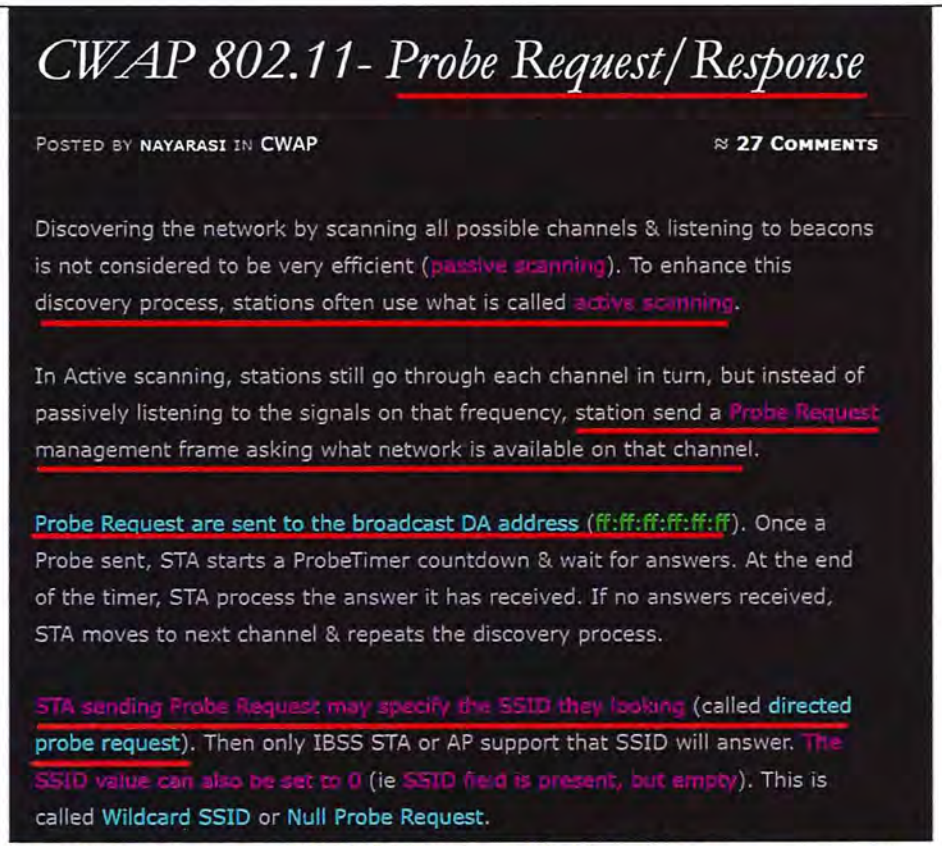
https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior



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

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

[21c] transmitting, in a search for at least one available access point around the device, the probe request frame that includes the fake device identifier;	The Accused Products transmit, in a search for at least one available access point around the device, the probe request frame that includes the fake device identifier. The Accused Products support the Wi-Fi standard. According to the standard, the Accused Products (each a UE) send probe requests to discover access points around the device to inquire about available Wi-Fi access points using a probe request. The probe request comprises a sender address field (e.g., device identifier). The UE utilizes a random MAC address (e.g. fake device identifier) as the sender address in a probe request. The end user device transmits probe requests to scan for 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/

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

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

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

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

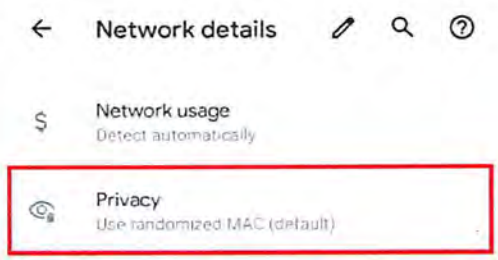


Figure 1. MAC randomization option.

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



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

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

[21d] receiving, from at least one access point around the device in response to the transmitting the probe request frame, a probe response frame that includes information regarding the at least one access point;	The Accused Products receive from at least one access point around the device in response to the transmitting the probe request frame, a probe response frame that includes information regarding the at least one access point. As an example, a probe response from a Wi-Fi access point around the device includes the SSID (wireless network name), supported data rates, encryption types, capabilities, etc. of the access point: The Accused Products support the Wi-Fi standard. The Accused Products receive probe responses from multiple available access points. As an example, an access point responds with the probe response when the SSID in the probe request is the wildcard SSID or matches the specific SSID of the access point or when the specific SSID of the access point is included in the SSID List element. As a further example, an access point responds to a probe request when it supports data rates or other requirements of the Accused Products. 2. APs receiving the probe request check to see if the mobile station has at least one common supported data rate. If they have compatible data rates, a probe response is sent advertising the SSID (wireless network name), supported data rates, encryption types if required, and other 802.11 capabilities of the AP. https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/802.11_Association_Process_Explained **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).

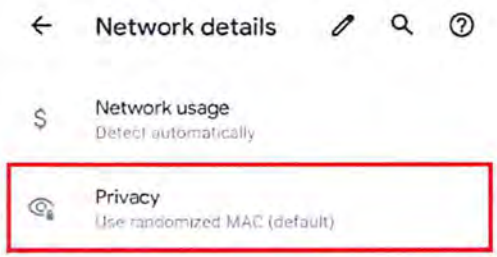


Figure 1. MAC randomization option.

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.

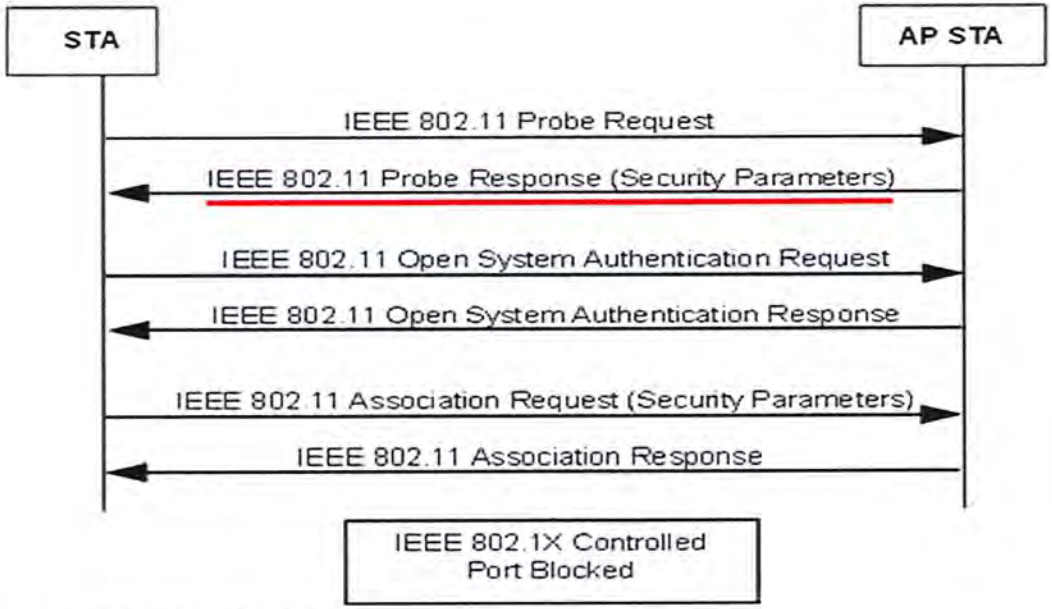
MAC addresses are used by devices when connecting to a Wi-Fi network or an access point. Because these MAC addresses are transmitted without encryption, they can be captured and used to potentially track a user's location. Historically, devices use the *factory MAC address* to associate to a Wi-Fi network.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

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

Table 8-27—Probe Response frame body

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability	
4	SSID	If dot11MeshActivated is true, the SSID element is the wildcard value as described in 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

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

Source: IEEE 802.11-2012.pdf

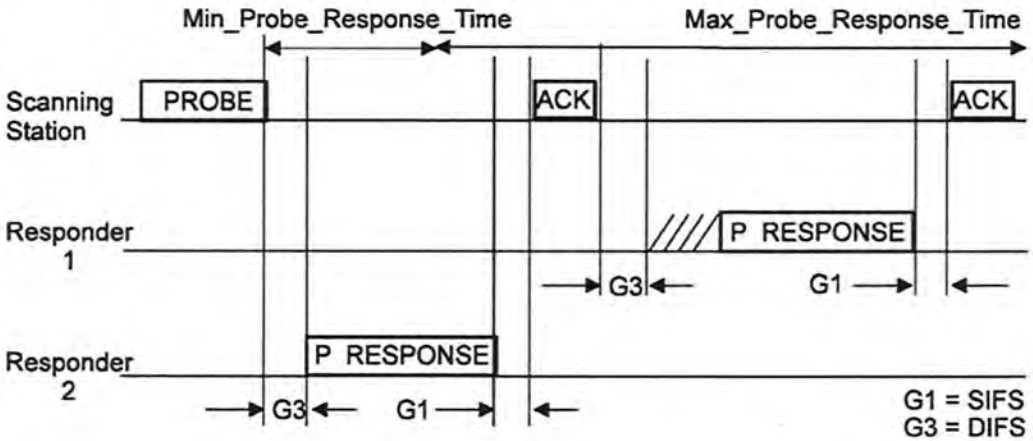
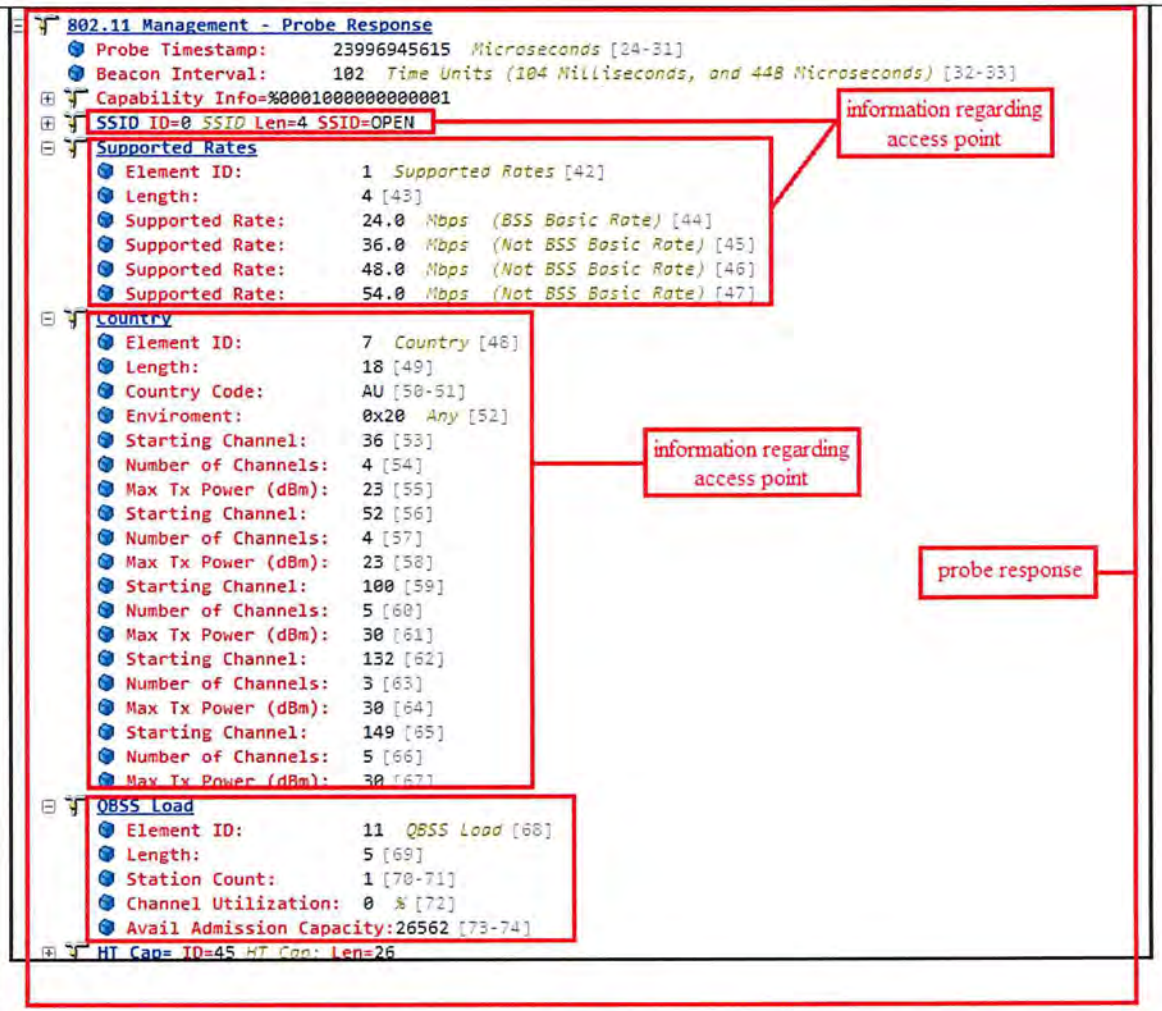


Figure 10-3—Probe response

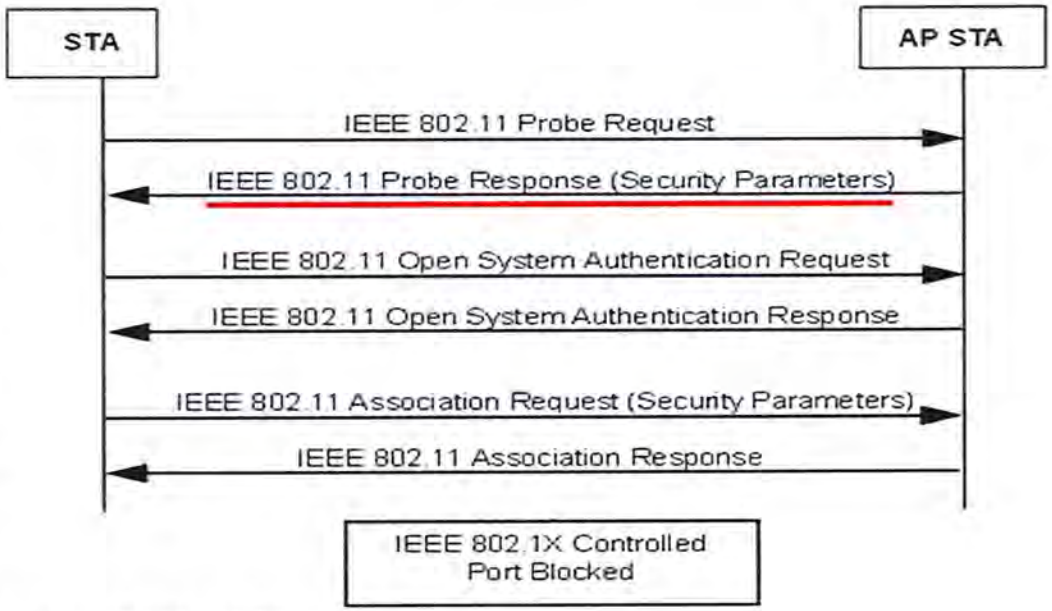
Source: IEEE 802.11-2012.pdf

	Before answering the question, let us first understand what a preferred network list is. The PNL is a historical record of all the network names (SSIDs) that a device has previously connected to, and trusts to automatically connect to again in the future. User devices trying to connect to a Wi-Fi network watch for access points (APs) broadcasting its availability for a device to connect to its network. Within that information contains the network name, or Service Set Identifier (SSID). Wi-Fi enabled devices trying to connect to a wireless network, and using Active Service Discovery, will then broadcast its interest in connecting to the AP if the network name is in its PNL, which increases the connection speed. For instance, if you connect to a **Starbucks** Wi-Fi network once, your device will remember and try to automatically connect to any network with the SSID **Starbucks**. This is true whether you go to the same Starbucks in the future, or a Starbucks 1,000 miles away. All the user device knows is the network name; no additional data is stored. Auto-connecting to wireless networks in PNL saves time and is convenient for the user, but it is a security risk. Therefore, it is important to identify all networks in the PNL and stop connecting automatically to Wi-Fi to stay safe. https://blog.pulsarsecurity.com/preferred-network-list-pnl The reason for client scanning is to determine a suitable AP to which the client may need to roam now or in the future. A client can use two scanning methods: active and passive. During an active scan, the client radio transmits a probe request and listens for a probe response from an AP. With a passive scan, the client radio listens on each channel for beacons sent periodically by an AP. A passive scan generally takes more time, since the client must listen and wait for a beacon versus actively probing to find an AP. Another limitation with a passive scan is that if the client does not wait long enough on a channel, then the client may miss an AP beacon. https://www.wi-fi.org/knowledge-center/faq/what-are-passive-and-active-scanning Below is an example Wi-Fi probe response that includes information of the access point.



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

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

[21e] determining, in response to the receiving the probe response frame and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point, wherein the determining whether the at least one access point is the authenticated access point includes determining whether the information regarding the at least one access point is included in the authenticated access point list, and wherein the determining whether the information regarding the at least one access point is included in the authenticated access	The Accused Products determine in response to receiving the probe response frame and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point, wherein the determining whether the at least one access point is the authenticated access point includes determining whether the information regarding the at least one access point is included in the authenticated access point list, and wherein the determining whether the information regarding the at least one access point is included in the authenticated access point list includes determining whether the at least one access point is under control of the server. As an example, the Accused Product receives a probe response frame in response to a probe request.  *Source: IEEE 802.11-2012.pdf*

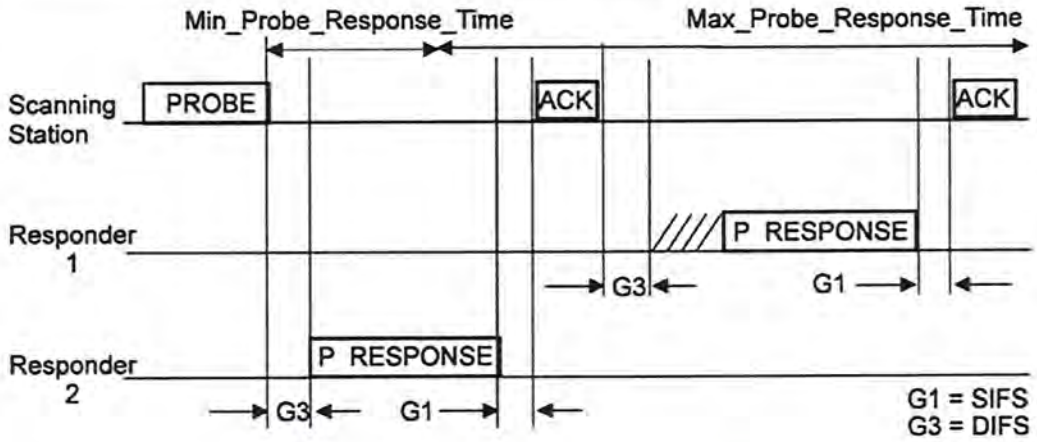
point list includes determining whether the at least one access point is under control of the server; and	 **Figure 10-3—Probe response** *Source: IEEE 802.11-2012.pdf* Information regarding the access point is included in the probe response, as shown below.

Table 8-27—Probe Response frame body

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability	
4	SSID	If dot11MeshActivated is true, the SSID element is the wildcard value as described in 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

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

Source: IEEE 802.11-2012.pdf

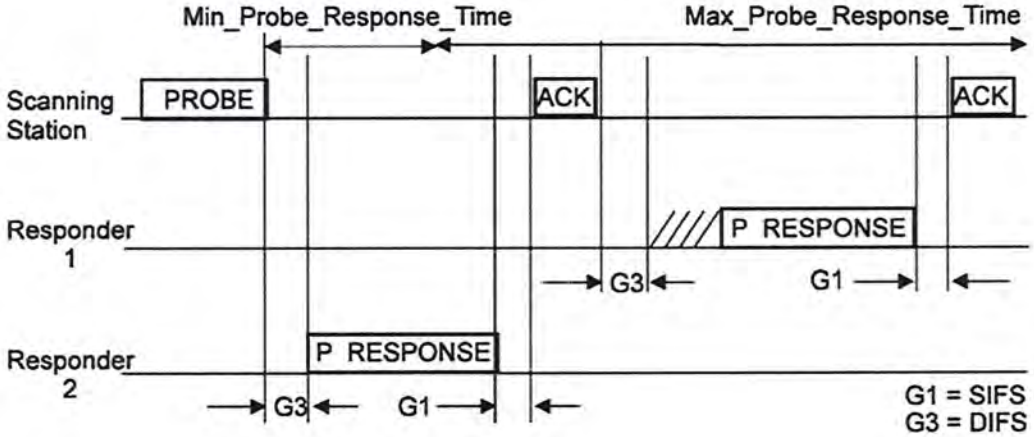
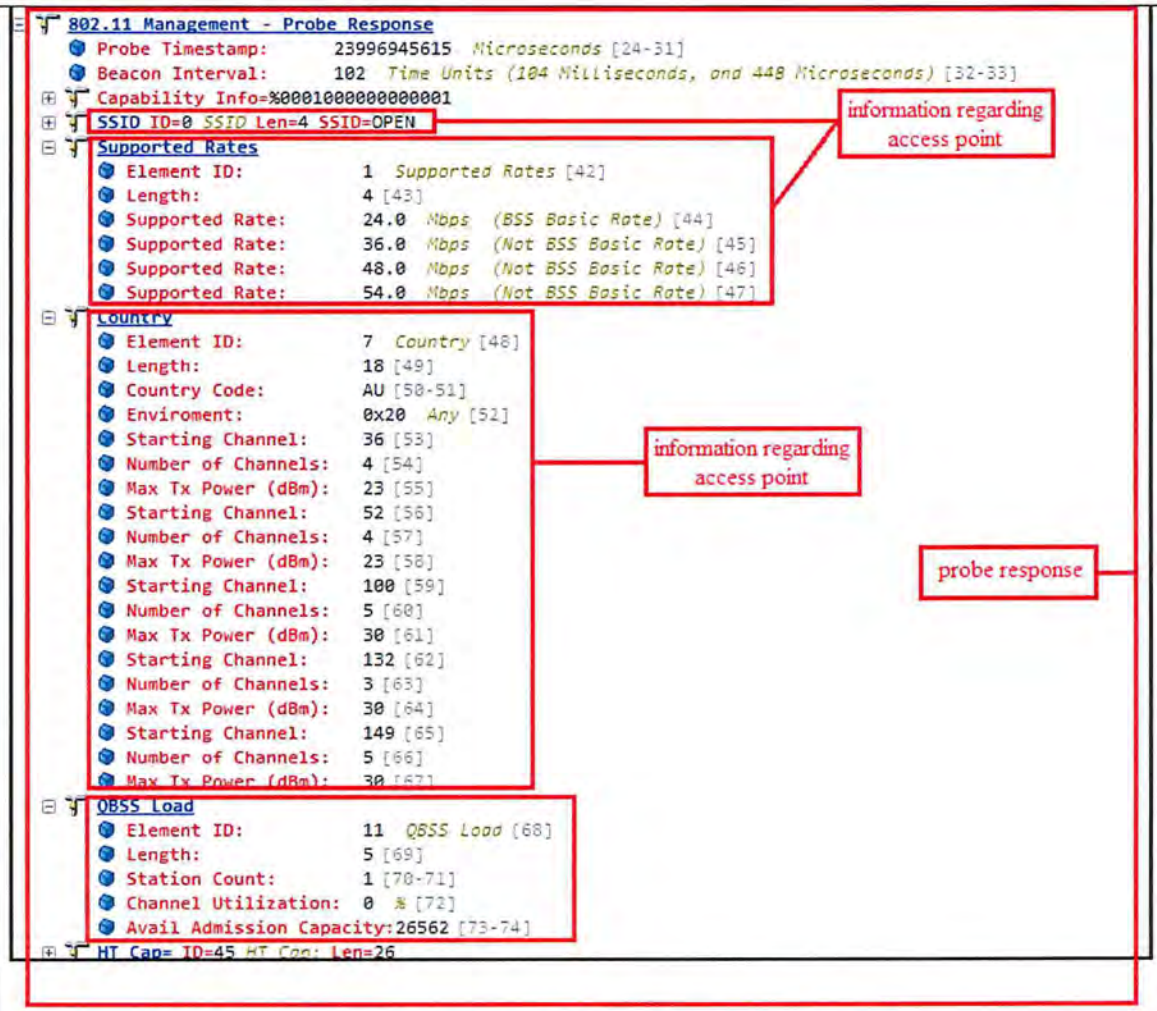


Figure 10-3—Probe response

Source: IEEE 802.11-2012.pdf

	Before answering the question, let us first understand what a preferred network list is. The PNL is a historical record of all the network names (SSIDs) that a device has previously connected to, and trusts to automatically connect to again in the future. User devices trying to connect to a Wi-Fi network watch for access points (APs) broadcasting its availability for a device to connect to its network. Within that information contains the network name, or Service Set Identifier (SSID). Wi-Fi enabled devices trying to connect to a wireless network, and using Active Service Discovery, will then broadcast its interest in connecting to the AP if the network name is in its PNL, which increases the connection speed. For instance, if you connect to a **Starbucks** Wi-Fi network once, your device will remember and try to automatically connect to any network with the SSID **Starbucks**. This is true whether you go to the same Starbucks in the future, or a Starbucks 1,000 miles away. All the user device knows is the network name; no additional data is stored. Auto-connecting to wireless networks in PNL saves time and is convenient for the user, but it is a security risk. Therefore, it is important to identify all networks in the PNL and stop connecting automatically to Wi-Fi to stay safe. https://blog.pulsarsecurity.com/preferred-network-list-pnl The reason for client scanning is to determine a suitable AP to which the client may need to roam now or in the future. A client can use two scanning methods: active and passive. During an active scan, the client radio transmits a probe request and listens for a probe response from an AP. With a passive scan, the client radio listens on each channel for beacons sent periodically by an AP. A passive scan generally takes more time, since the client must listen and wait for a beacon versus actively probing to find an AP. Another limitation with a passive scan is that if the client does not wait long enough on a channel, then the client may miss an AP beacon. https://www.wi-fi.org/knowledge-center/faq/what-are-passive-and-active-scanning Below is an example Wi-Fi probe response that includes information of the access point.



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

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

	access point using an authenticated device identifier, such as a persistent MAC address that was used for a prior connection with the access point. The Accused Products determine that the access point is an authenticated access point by determining that it is in the access point list, indicating it was connected previously. The Accused Products maintain a list of previously-connected access points which is matched to the access point's SSID received in the probe response. Each previously-connected access point is linked to a persistent MAC address for connecting to that access point. **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]

```
<?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" />
                <boolean name="HiddenSSID" value="false" />
```

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

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

Source: IEEE 802.11-2012.pdf

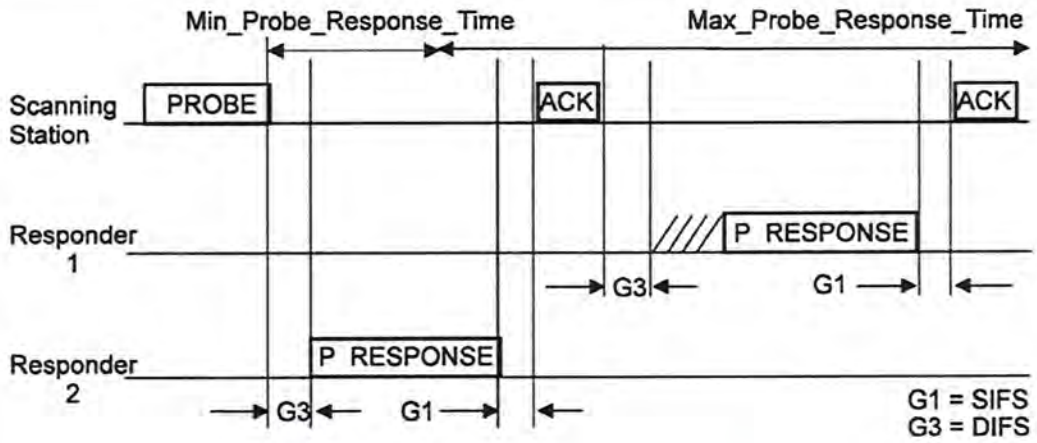
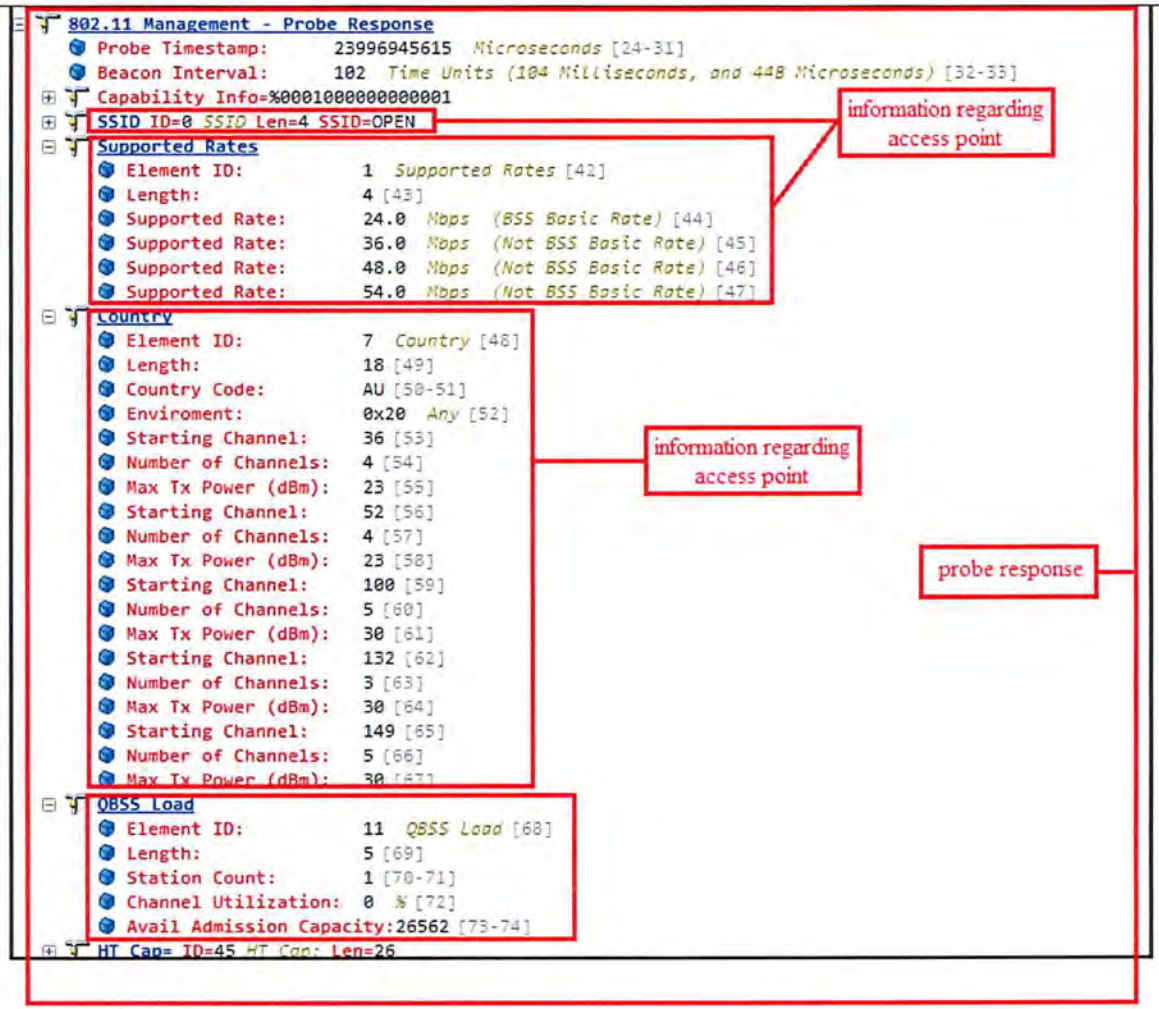


Figure 10-3—Probe response

Source: IEEE 802.11-2012.pdf

	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



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

The Accused Products also determine using information in the probe response that the access points are controlled by the server. For example, the server, which serves the functionality of the Android operating system, controls connection and/or data transmission of the access points. The Accused Products support the Wi-Fi

standard. According to the standard, the Accused Products inquire about available Wi-Fi access points using a probe request, which is generated by the mobile operating server. The probe request comprises identifying information, such as a wildcard SSID or SSID for one or more access points or a preferred network list which is a set of SSIDs to which the UE got connected previously. An access point receiving the probe request must provide a probe response. As a further example, an access point receives and transmits data under control the mobile operating server.

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

Source: IEEE 802.11-2012.pdf

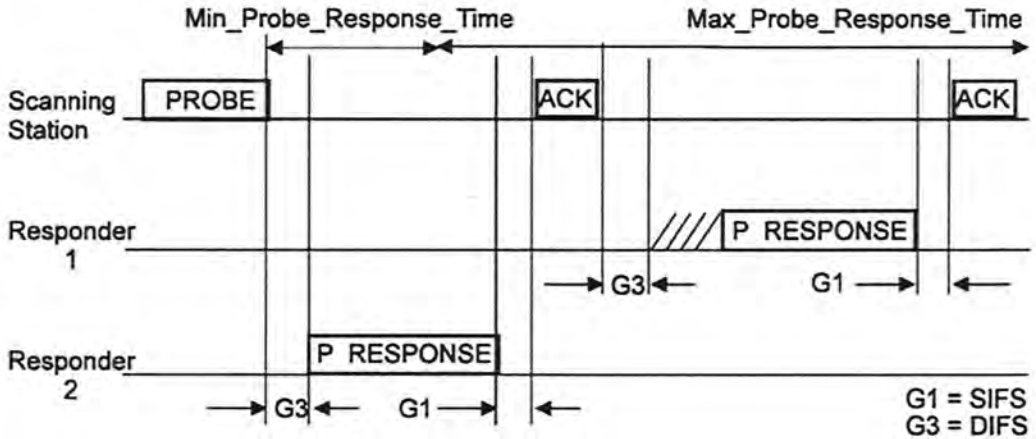
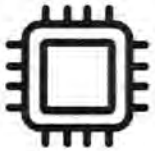


Figure 10-3—Probe response

Source: IEEE 802.11-2012.pdf

The server runs on a CPU of the SoC (e.g., the Kryo CPU) of the Accused Product and is used to manage connections with an access point to control those access points to receive and transmit data.

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/



CPU

Kryo CPU

- 64-bit Architecture
- 1 Prime core, up to 3.36 GHz[2]
  - Arm Cortex-X3 technology
- 4 Performance cores, up to 2.8 GHz
- 3 Efficiency cores, up to 2.0 GHz

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

Phone	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



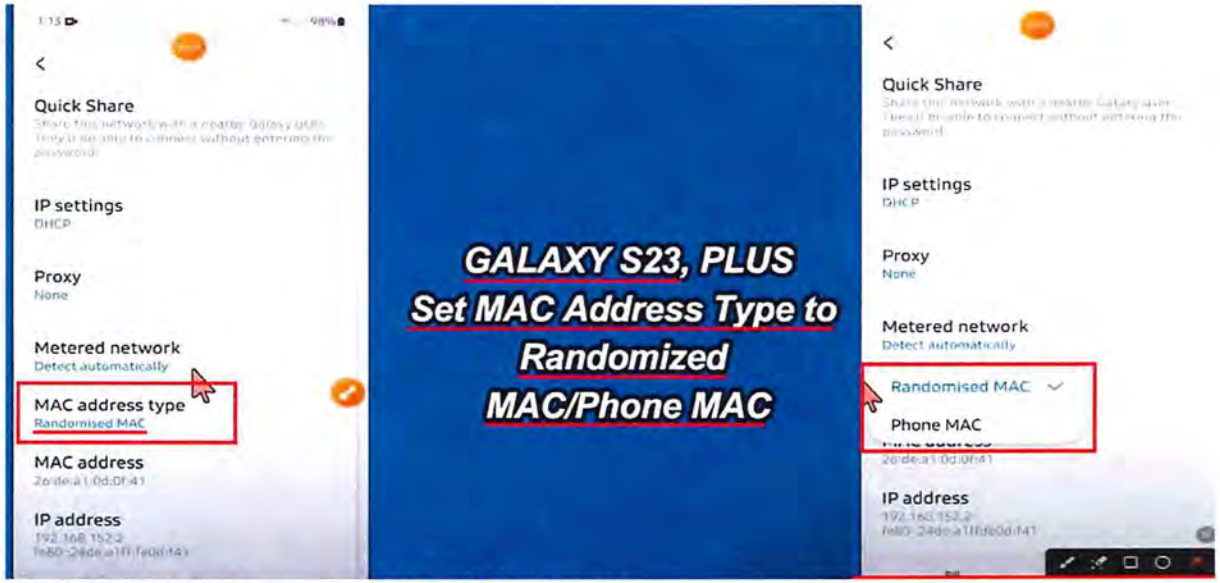
Wi-Fi 6E

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

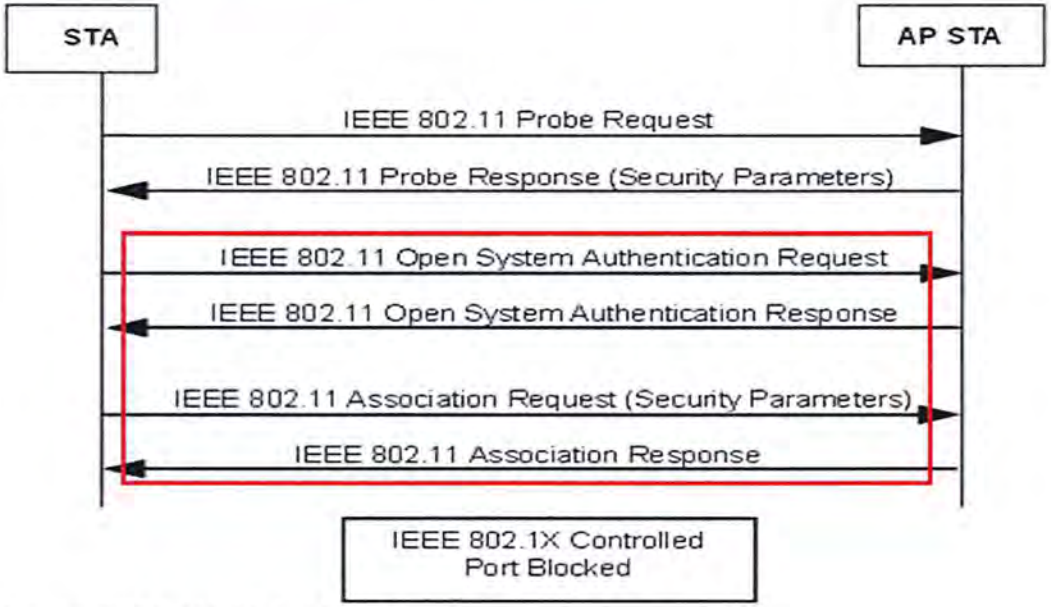


https://www.youtube.com/watch?v=dT63df6nnqU

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

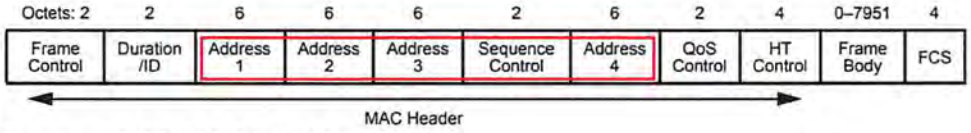
[21f] transmitting, to the at least one access point in response to a determination that the at least one access point is the authenticated access point, a connection request that includes an authentic device identifier for the device.	The Accused Products transmit, to the at least one access point (e.g., Wi-Fi access point) in response to a determination that the at least one access point is the authenticated access point , a connection request (e.g., association and/or authentication request) that includes an authentic device identifier (e.g., a persistent MAC address) for the device. After receiving the probe response from the access point, as discussed above, the Accused Products confirm the received SSID information from the probe responses with the access point information stored in memory. Once confirmed that, the Accused Products initiate a connection using the persistent MAC address for the access point, which is an authentic device identifier for the Accused Product. **Persistent randomization** Android uses the persistent randomization type by default when the MAC randomization feature is enabled. Android generates a persistent randomized MAC address based on the parameters of the network profile including SSID, security type, or FQDN (for Passpoint networks). This MAC address remains the same until factory reset. The MAC address does **not** get re-randomized if the user forgets and re-adds the Wi-Fi network since the MAC 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



Source: IEEE 802.11-2012.pdf

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



Source: IEEE 802.11-2012.pdf

8.2.4.3.5 DA field

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

8.2.4.3.6 SA field

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

8.2.4.3.7 RA field

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

8.2.4.3.8 TA field

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

Source: IEEE 802.11-2012.pdf

802.11 Mgmt : Authentication Frame

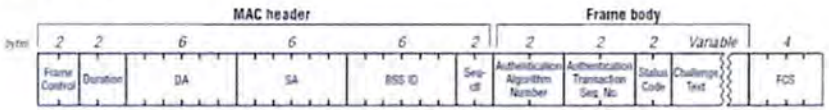
POSTED BY **NAYARASI** IN **CWAP** ≈ **10 COMMENTS**

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

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

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

FIGURE 4.8 Authentication frame format



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

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

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]

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

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

	An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
22. The method of claim 21, wherein: the generating the collection that includes the at least one of one or more random numbers or one or more random characters comprises configuring the collection as a fake media access control (MAC) address, and the fake device identifier includes the fake media access control (MAC) address.	The Accused Products practice a method of generating the collection that includes the at least one of one or more random numbers or one or more random characters which comprises configuring the collection as a fake media access control (MAC) address and that the fake device identifier includes a fake media access control (MAC) address. The Accused Products generate a random MAC address that is different from the original MAC address of the hardware by generating a randomized MAC address for use in probe requests. The generated random MAC address is a fake MAC address. The fake device identifier includes the random 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).

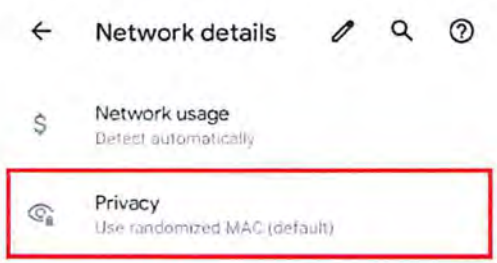
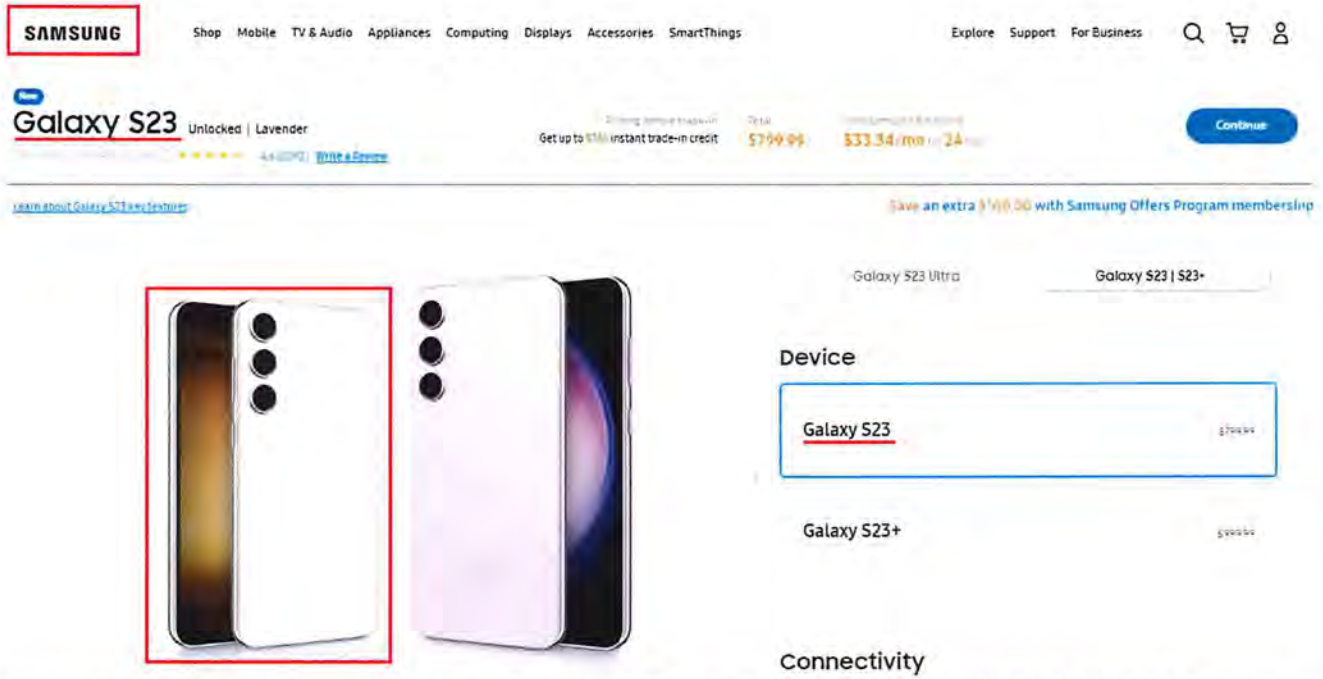
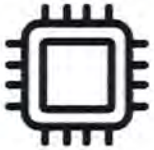


Figure 1. MAC randomization option.

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

	An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
24. A system, comprising: a processor;	To the extent the preamble is limiting, the Accused Products are systems with a processor. The Accused Products include Android OS 10 or above or Wear OS 3 or above. The operating system runs on a CPU of the SoC (e.g., the Kryo CPU) of the Accused Product. Each Accused Product includes an SoC and Wi-Fi connection functionality. As a specific example shown below, the Galaxy S23 includes the Android 13 operating system, which includes randomized MAC for Wi-Fi connections. It contains an SoC, Snapdragon 8 Gen 2, a Wi-Fi chipset, and FastConnect. It connects to a Wi-Fi network using the Wi-Fi chipset.  https://www.samsung.com/us/smartphones/galaxy-s23/buy/galaxy-s23-128gb-unlocked-sm-s911uliaxaa/

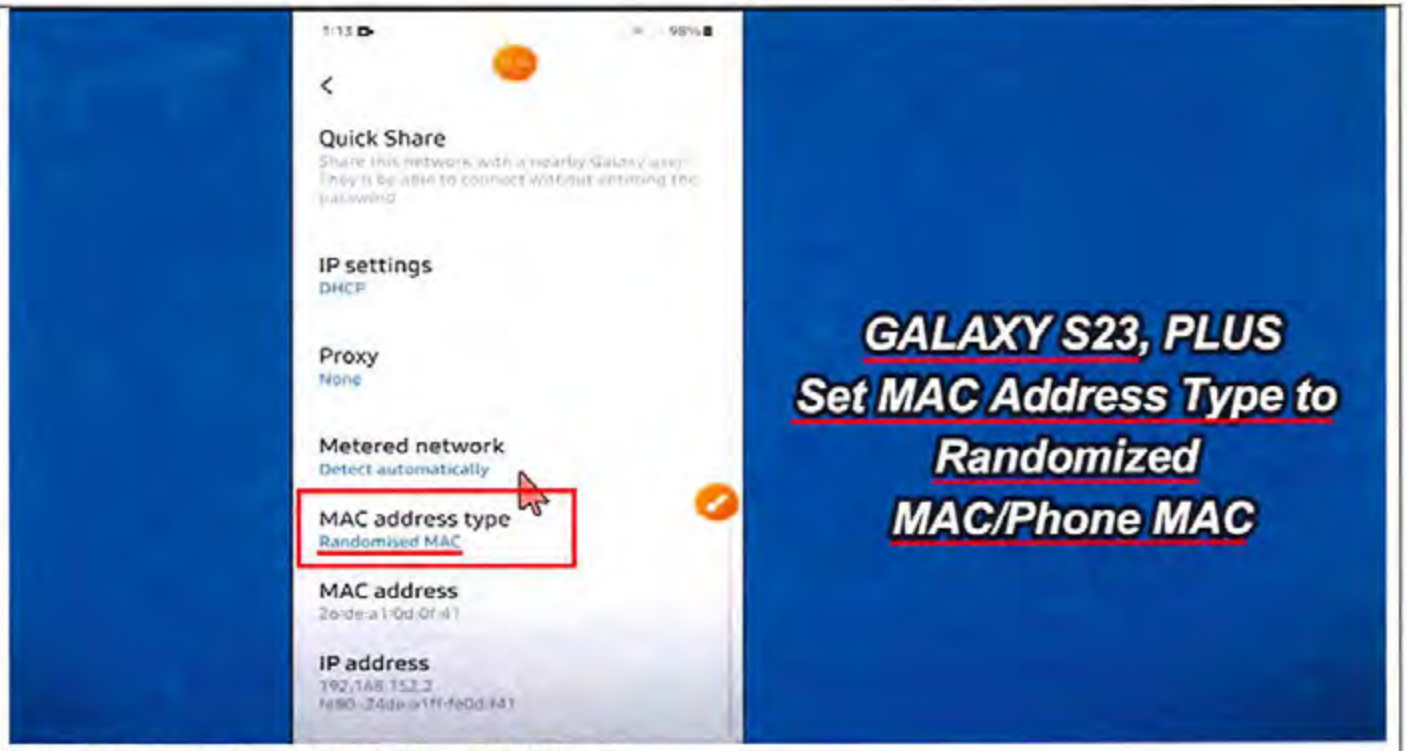
	Galaxy S23  Super fast processing Snapdragon® 8 Gen 2 Octa-Core https://www.samsung.com/us/smartphones/galaxy-s23/specs/

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

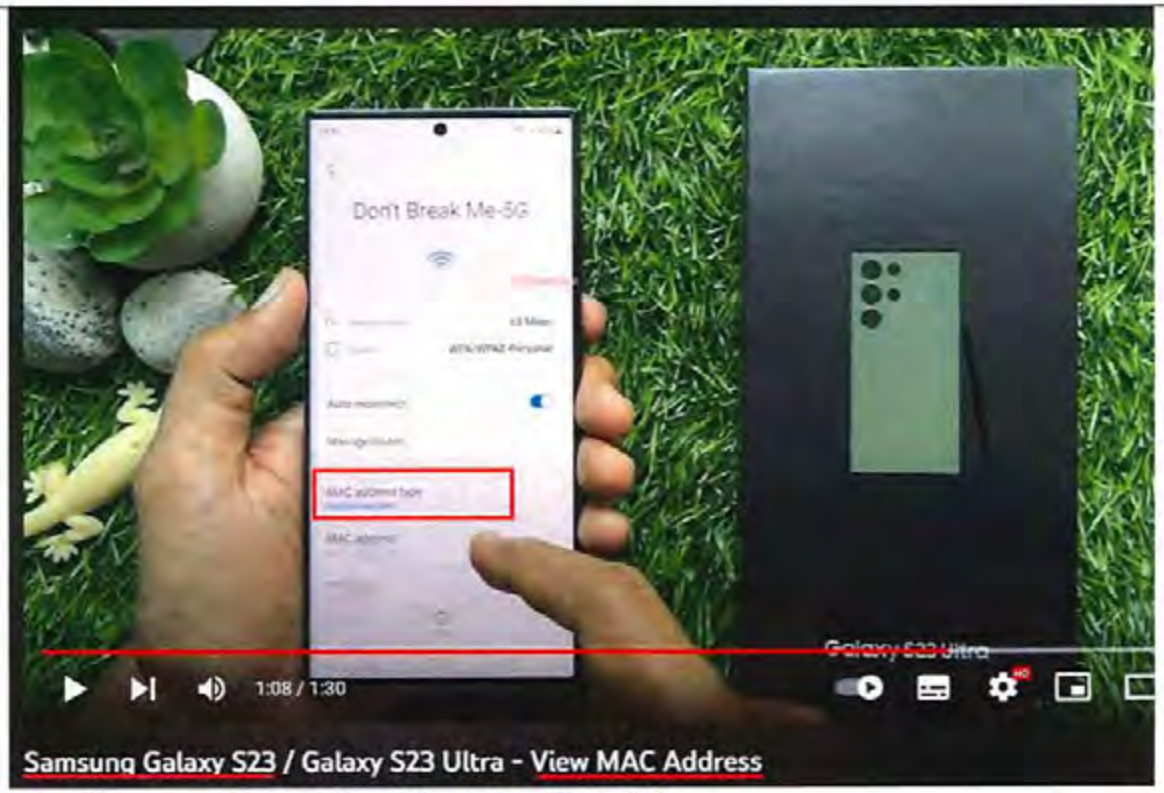
https://www.androidpolice.com/samsung-galaxy-s23/



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



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

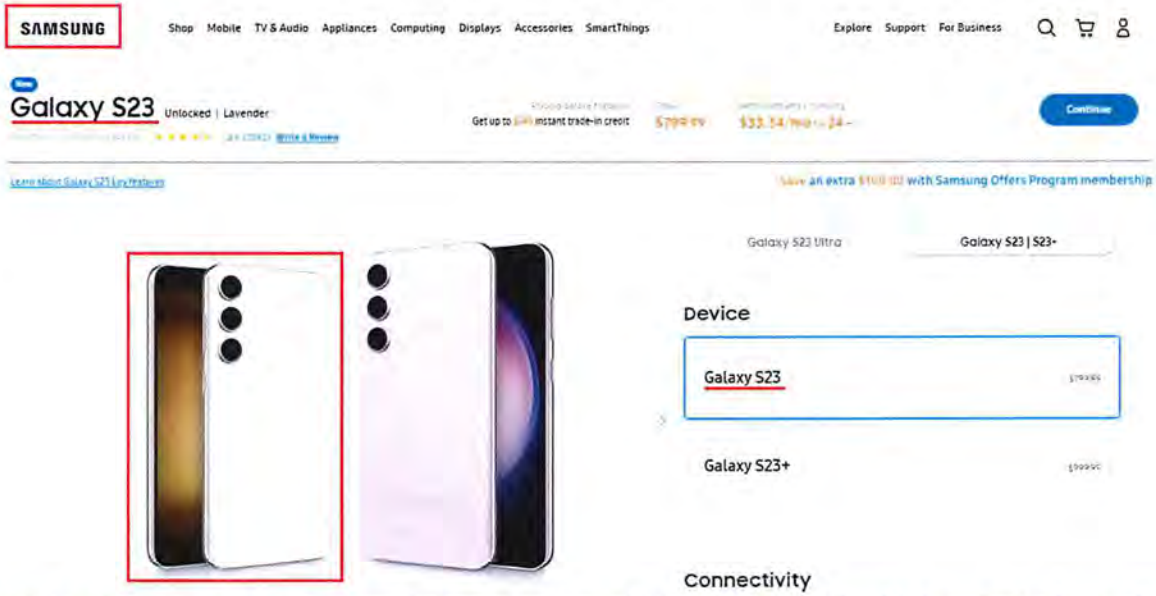
MAC Randomization is implemented in devices running the Android OS since at least Android OS 10 as well as Wear OS 3.0.

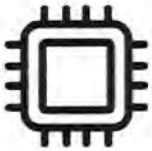
In Android 10, MAC randomization is enabled by default for client mode, SoftAp, and Wi-Fi Direct.

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

Additionally, MAC addresses are randomized as part of Wi-Fi Aware and Wi-Fi RTT operations.

For more information, see MAC Randomization Behavior.

	https://source.android.com/docs/core/connect/wifi-mac-randomization Wear OS, including Wear OS 3.0, is based on Android. *See* https://developer.android.com/training/wearables/wear-v-mobile#:~:text=Wear%20OS%20is%20based%20on,design%20a%20Wear%20OS%20app. Devices operating on Wear OS 3.0 implement MAC randomization. *See* https://www.reddit.com/r/GalaxyWatch/comments/pcmkj1/galaxy_watch_4_wifi_mac_address/
[24a] at least one communication interface;	The Accused Products contain at least one communication interface (e.g. the interface of the Accused Product that communicates with Wi-Fi access points). As shown below, an example of the Accused Products contains an SoC, Snapdragon 8 Gen 2, a Wi-Fi chipset, and FastConnect. It connects to a Wi-Fi network using the Wi-Fi chipset.  https://www.samsung.com/us/smartphones/galaxy-s23/buy/galaxy-s23-128gb-unlocked-sm-s911uliaxaa/

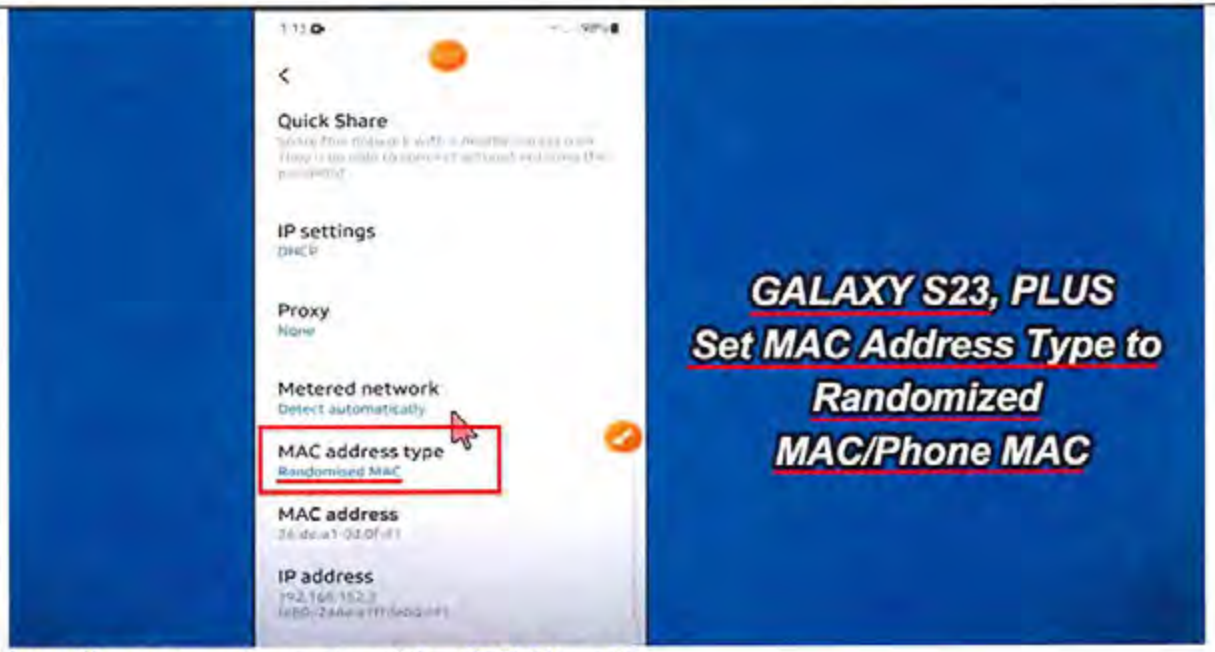
	Galaxy S23  Super fast processing Snapdragon® 8 Gen 2 Octa-Core https://www.samsung.com/us/smartphones/galaxy-s23/specs/

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

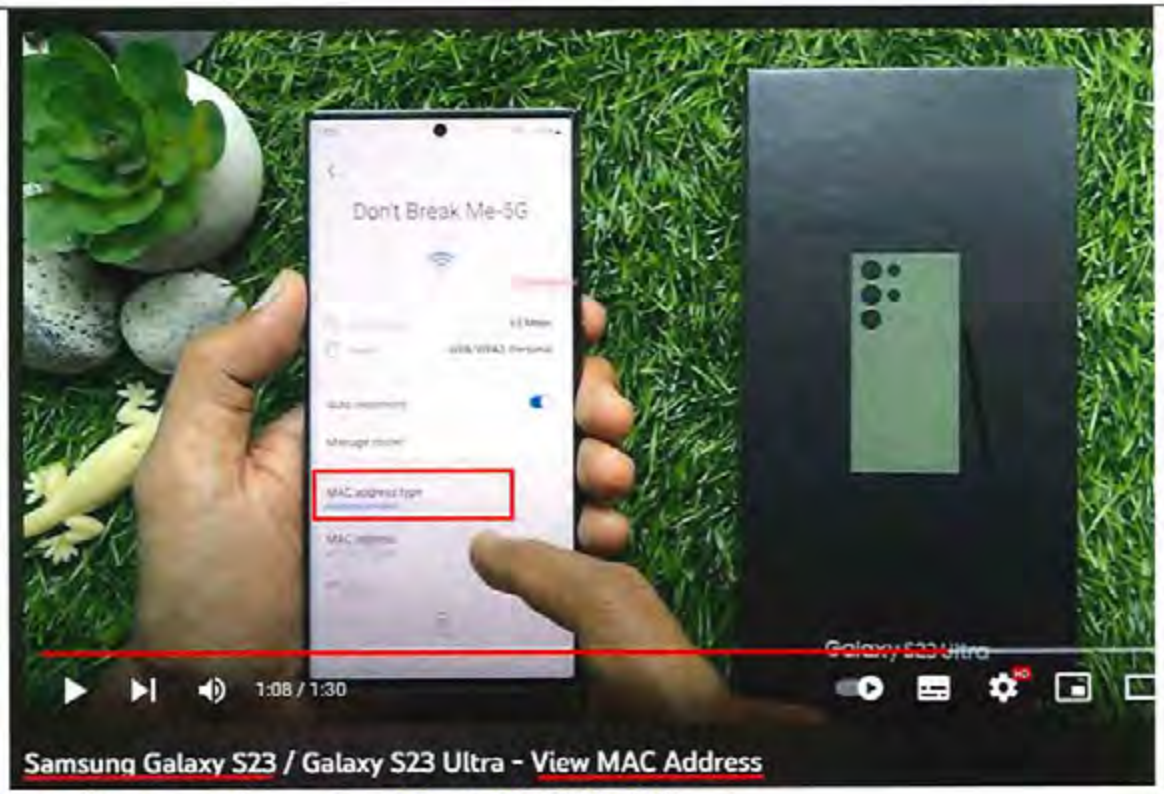
https://www.androidpolice.com/samsung-galaxy-s23/



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

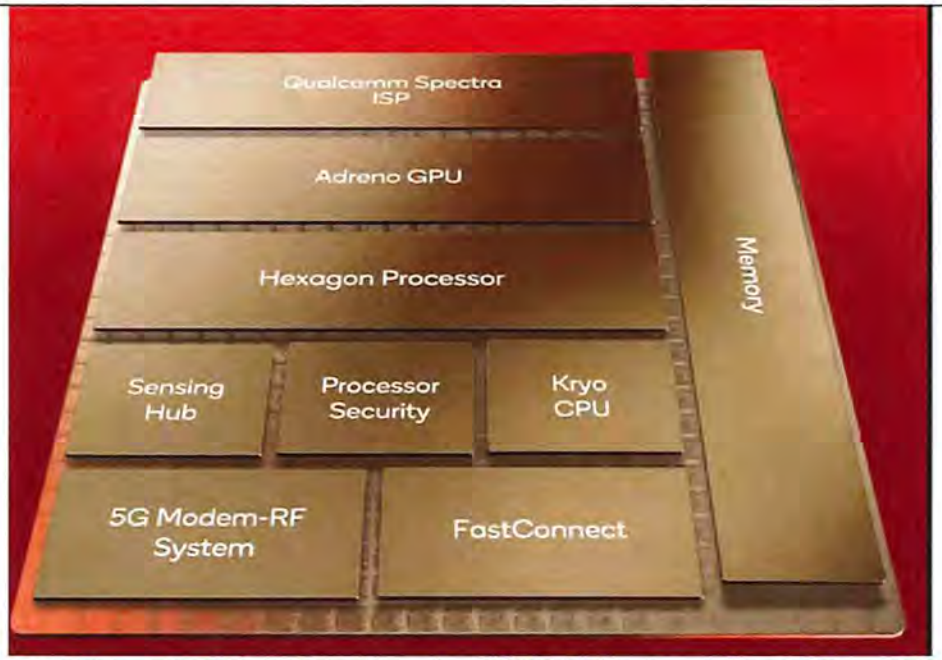


https://www.youtube.com/watch?v=dT63df6nnqU

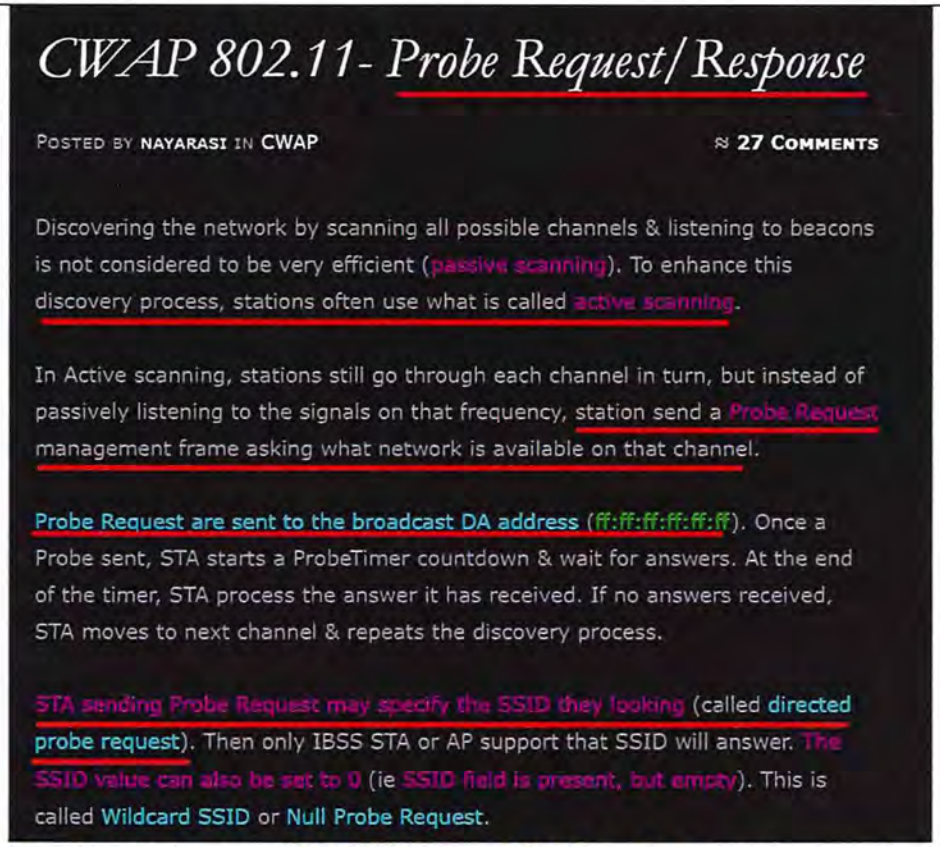


https://www.youtube.com/watch?v=AaMm2HHwbI0

	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

	 https://www.qualcomm.com/news/onq/2022/11/new-snapdragon-8-gen-2-8-extraordinary-mobile-experiences-unveiled An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
[24b] a transmitter to transmit, to at least one access point via the at least one communication interface, a probe request frame that includes a fake device identifier for	The Accused Products contain a transmitter to transmit, to at least one access point (e.g. Wi-Fi access point) via the at least one communication interface, a probe request frame that includes a fake device identifier for a device e.g. randomized MAC address, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters. The Accused Products support the Wi-Fi standard. According to the standard, the Accused Products (each a UE) transmit probe requests, via a transmitter, to access points to inquire about available Wi-Fi access points using a

a device, wherein the fake device identifier includes at least one of one or more random numbers or one or more random characters;	probe request. The probe request comprises a sender address field for a device identifier. The UE utilizes a random MAC address as the sender address in a probe request. The end user device 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/

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

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

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

	The Wi-Fi probe request of the Accused Products includes a randomized MAC address, which is a fake MAC address. The random MAC address includes at least one of one or more random numbers or one or more random characters. **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).

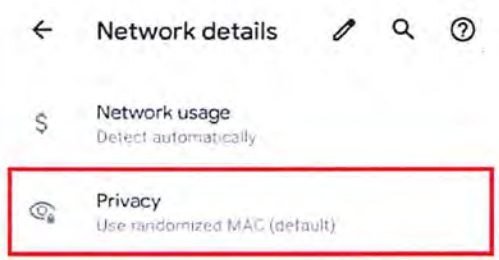


Figure 1. MAC randomization option.

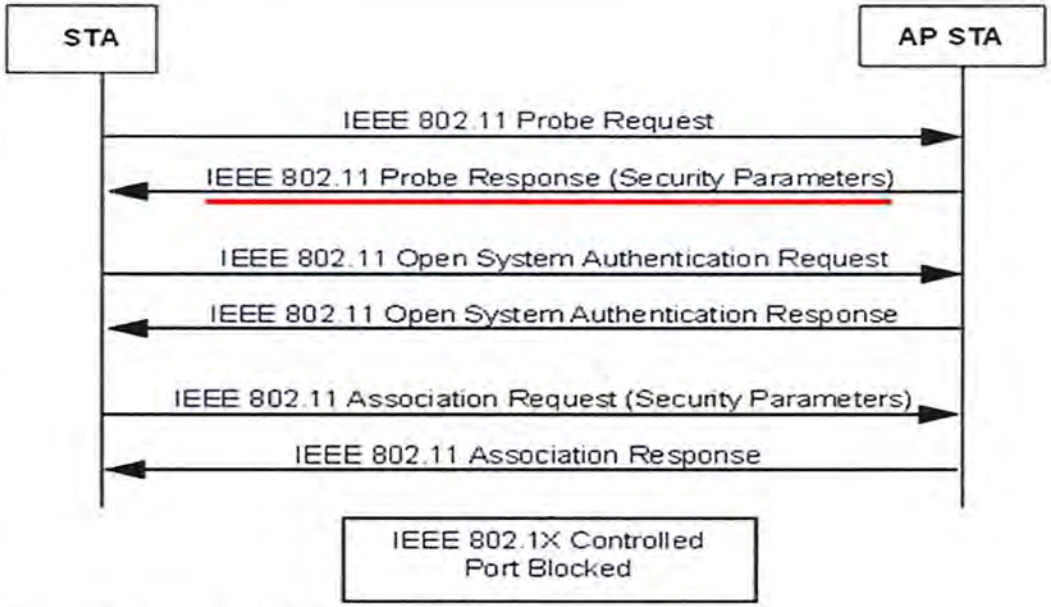
https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior



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

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

[24c] a receiver to: receive, from the at least one access point via the at least one communication interface, a probe response frame that includes information regarding the at least one access point; and	The Accused Products include a receiver that receives, from the at least one access point via the at least one communication interface, a probe response frame that includes information regarding the at least one access point. The Accused Products receive probe responses for access points and thus necessarily include a receiver for receiving the response via the at least one communication interface. • **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



Source: IEEE 802.11-2012.pdf

The Accused Products receive from the access point, a probe response that includes information regarding the access point. As an example, a probe response from a Wi-Fi access point includes the SSID (wireless network name), supported data rates, encryption types, capabilities, etc. of the access point:

2. APs receiving the probe request check to see if the mobile station has at least one common supported data rate. If they have compatible data rates, a probe response is sent advertising the SSID (wireless network name), supported data rates, encryption types if required, and other 802.11 capabilities of the AP.

https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/802.11_Association_Process_Explained

The Accused Products support the Wi-Fi standard. The Accused Products receive probe responses from multiple available access points. As an example, an access point responds with the probe response when the SSID in the probe request is the wildcard SSID or matches the specific SSID of the access point or when the specific SSID

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

Persistent randomization

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

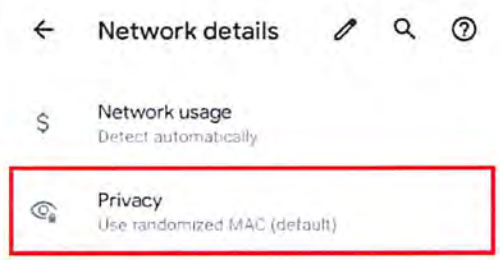


Figure 1. MAC randomization option.

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.

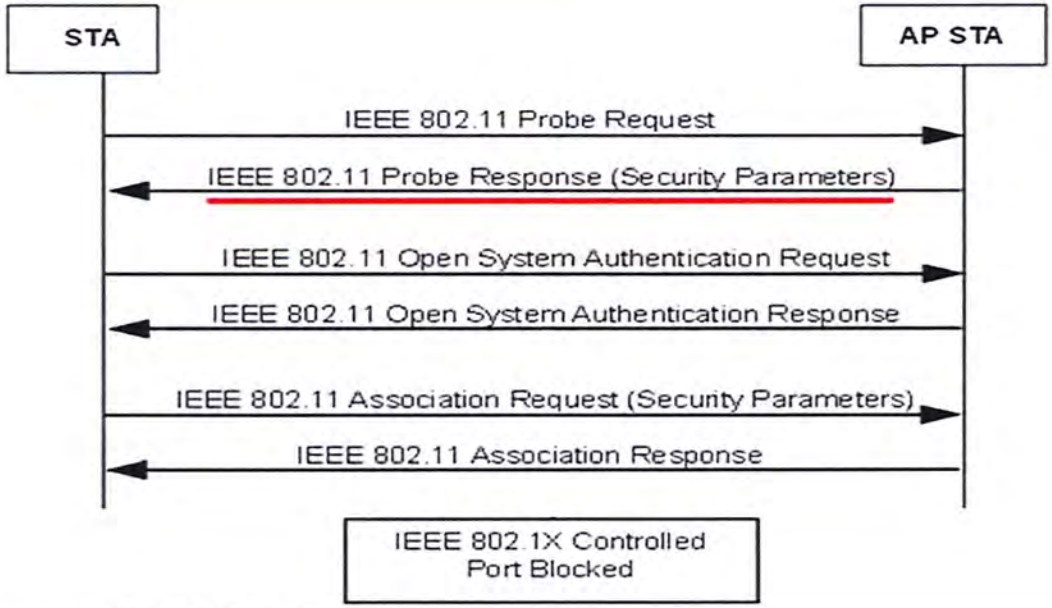
MAC addresses are used by devices when connecting to a Wi-Fi network or an access point. Because these MAC addresses are transmitted without encryption, they can be captured and used to potentially track a user's location. Historically, devices use the *factory MAC address* to associate to a Wi-Fi network.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

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

Table 8-27—Probe Response frame body

Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability	
4	SSID	If dot11MeshActivated is true, the SSID element is the wildcard value as described in 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

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

Source: IEEE 802.11-2012.pdf

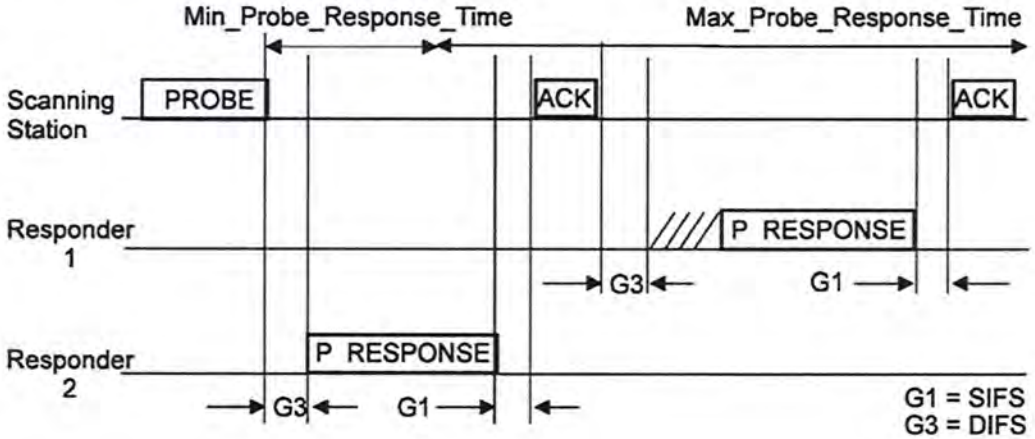


Figure 10-3—Probe response

Source: IEEE 802.11-2012.pdf

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

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

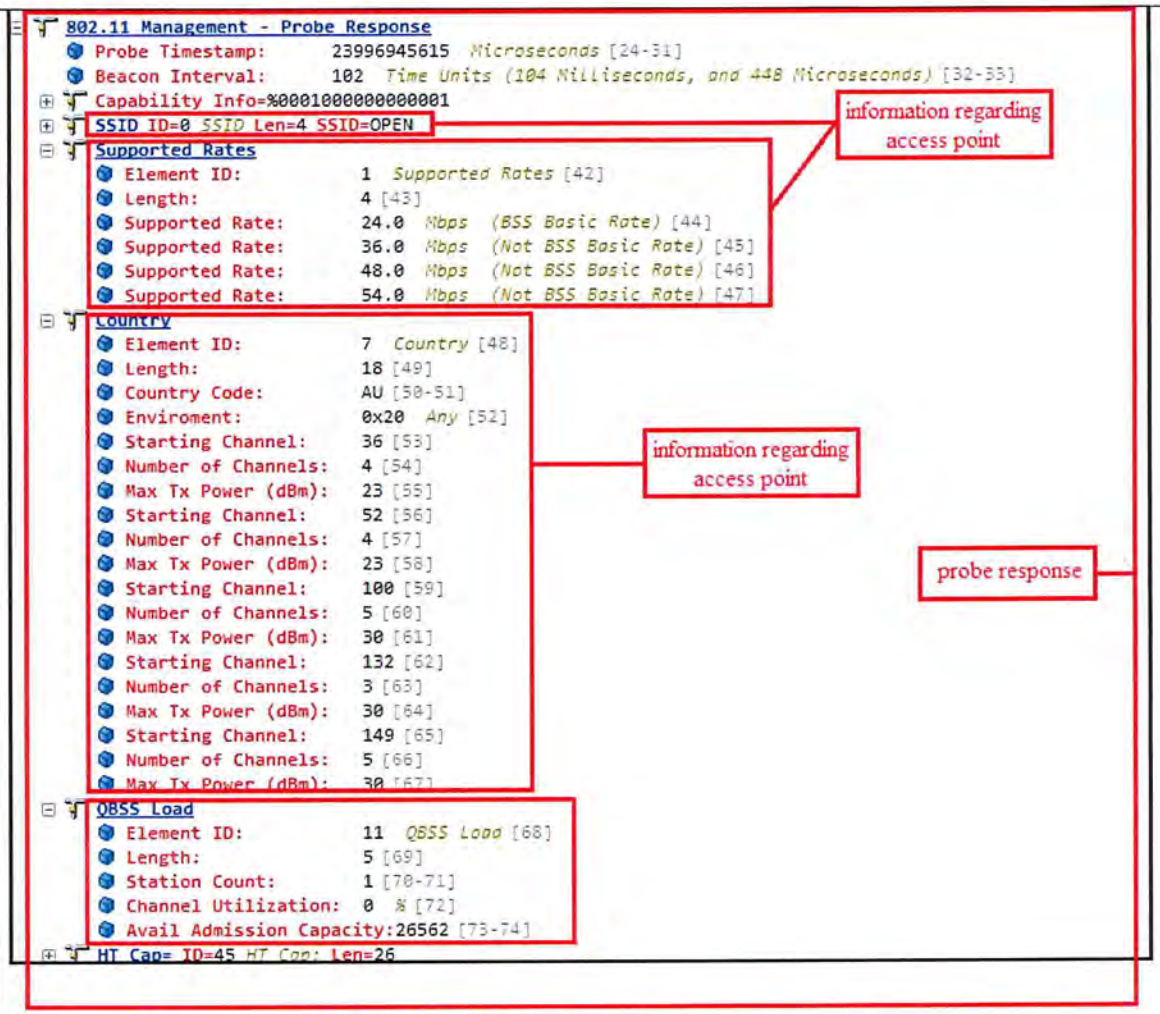
For instance, if you connect to a **Starbucks** Wi-Fi network once, your device will remember and try to automatically connect to any network with the SSID **Starbucks**. This is true whether you go to the same Starbucks in the future, or a Starbucks 1,000 miles away. All the user device knows is the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

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

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

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

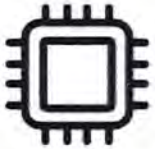
Below is an example Wi-Fi probe response that includes information of the access point.



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

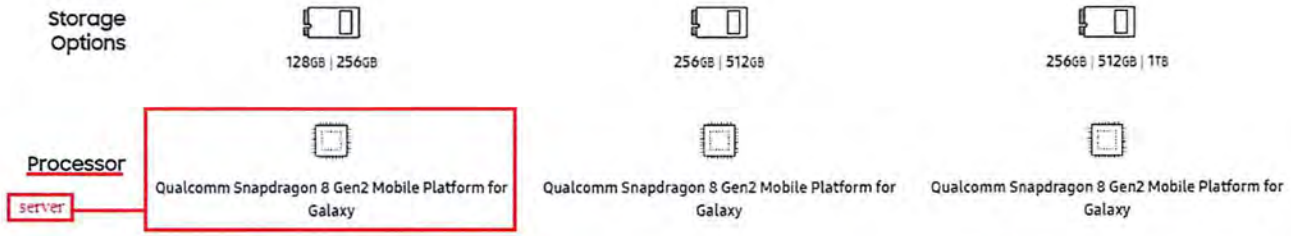
An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.

[24d] receive, from a server, an authenticated access point list that includes information regarding one or more access points that are controlled by the server;	The Accused Products receive, from a server (e.g., the OS and/or a CPU and associated memory for storing and executing the OS and associated data), an authenticated access point list (e.g., previously connected access point list) that includes information (e.g., SSID, supported data rates, pre-shared keys, etc.) regarding one or more access points (e.g., previously connected access point) that are controlled by the server. As shown below, an example of the Accused Products contains an SoC, Snapdragon 8 Gen 2 with a Kryo CPU. Also, it supports Android 13 operating system and has an option for randomized MAC for Wi-Fi connections. The server generates a persistent randomized MAC address to be used with a Wi-Fi network. The server also stores a list of previously connected access points and provides that list to the device in connecting to Wi-Fi access points. The list comprises different information pertaining to previously connected access points such as SSID, pre-shared keys, etc.

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



CPU

Kryo CPU

- 64-bit Architecture
- 1 Prime core, up to 3.36 GHz[2]
  - Arm Cortex-X3 technology
- 4 Performance cores, up to 2.8 GHz
- 3 Efficiency cores, up to 2.0 GHz

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

Phone	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



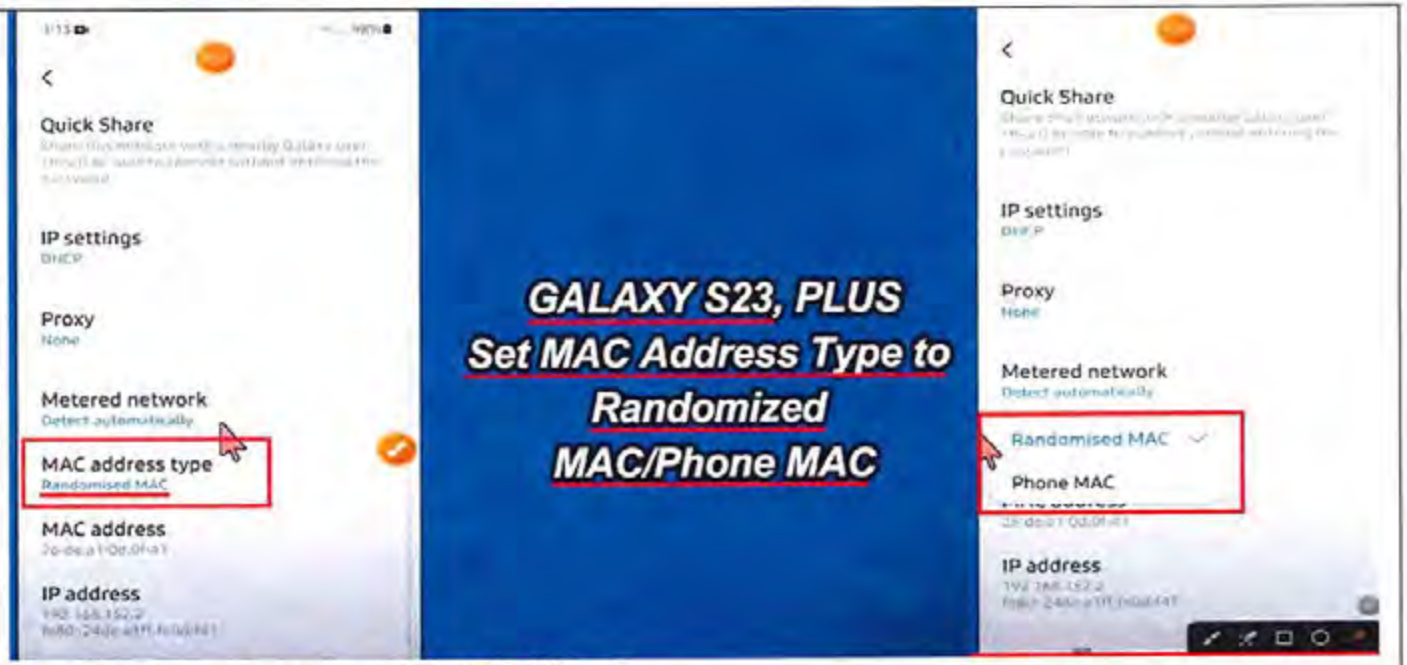
Wi-Fi 6E

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

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>
```

previously connected access-points information list

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

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

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]

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

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

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

Source: IEEE 802.11-2012.pdf

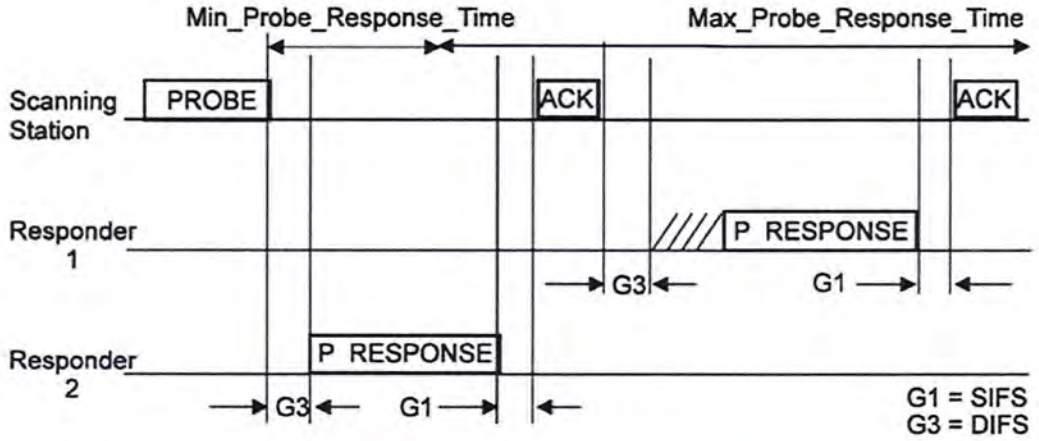
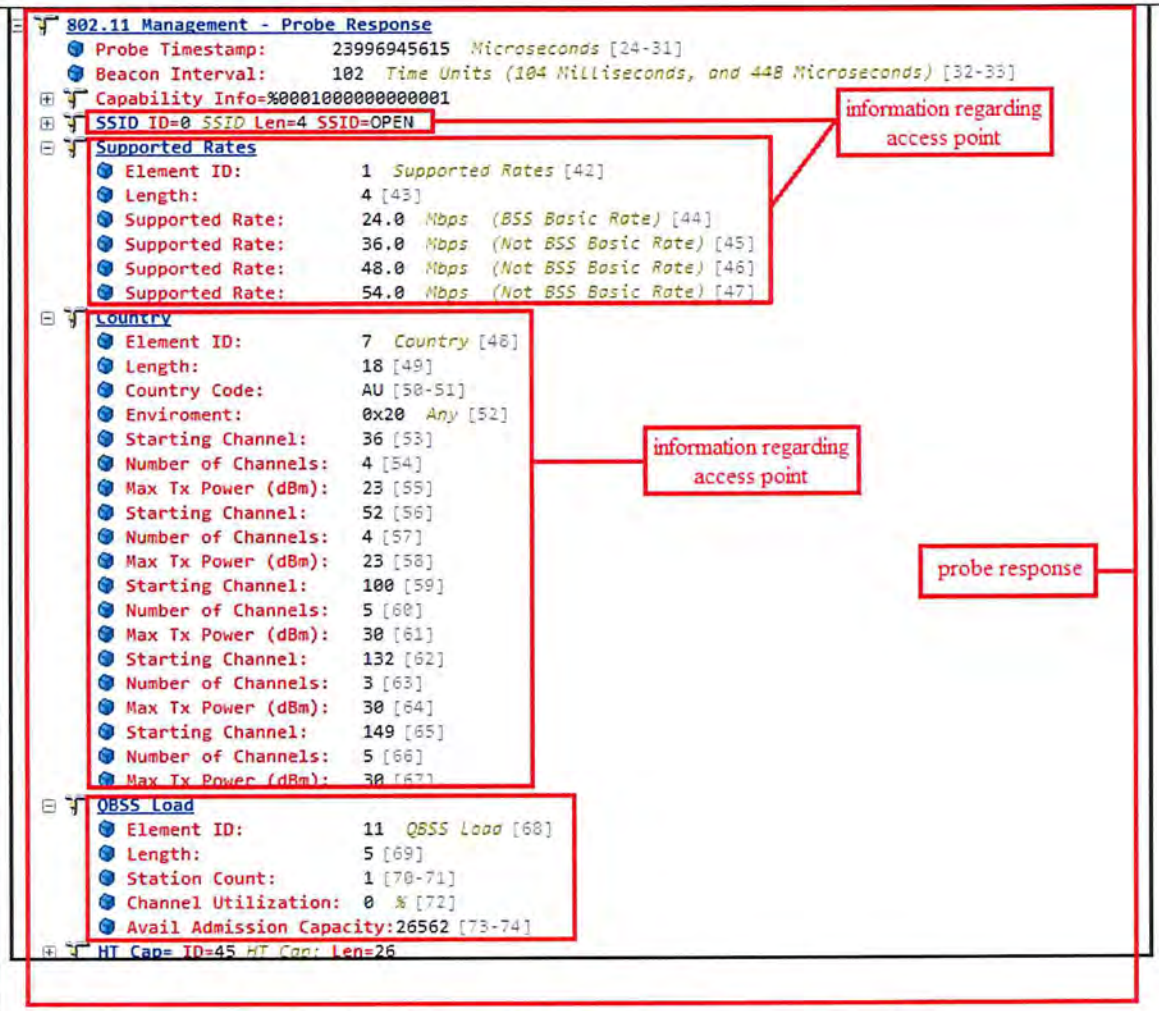


Figure 10-3—Probe response

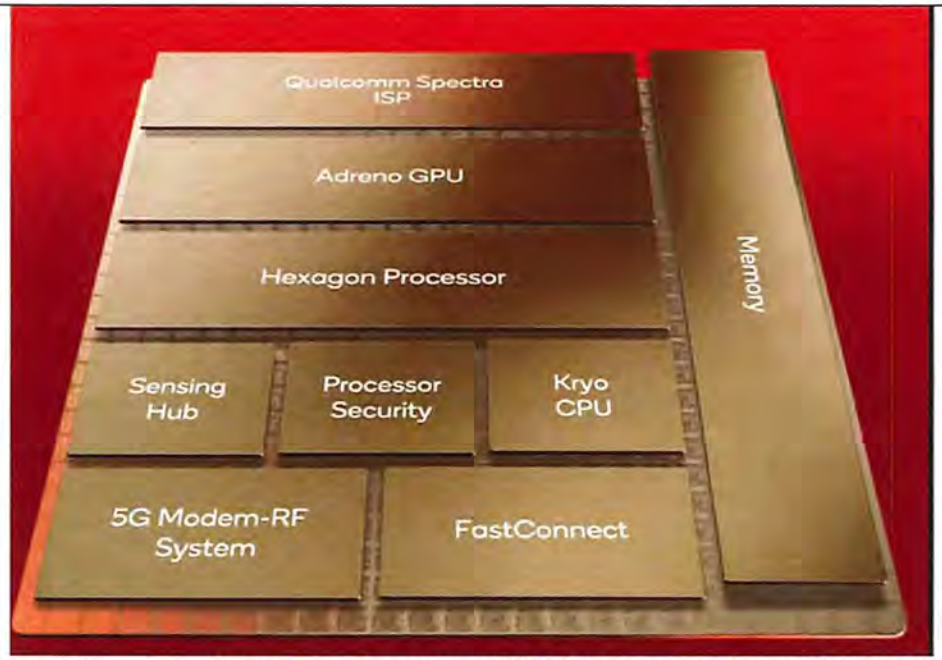
Source: IEEE 802.11-2012.pdf

	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



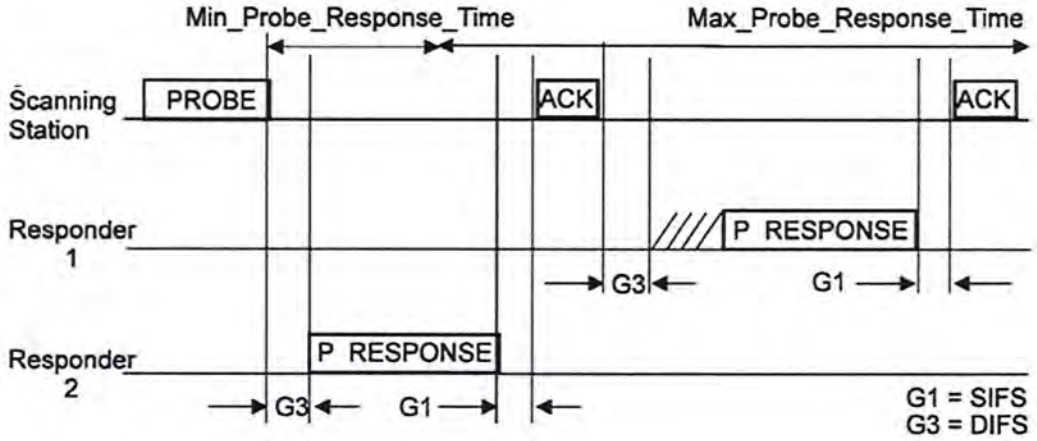
https://mrncciew.com/2014/10/27/cwap-802-11-probe-requestresponse/

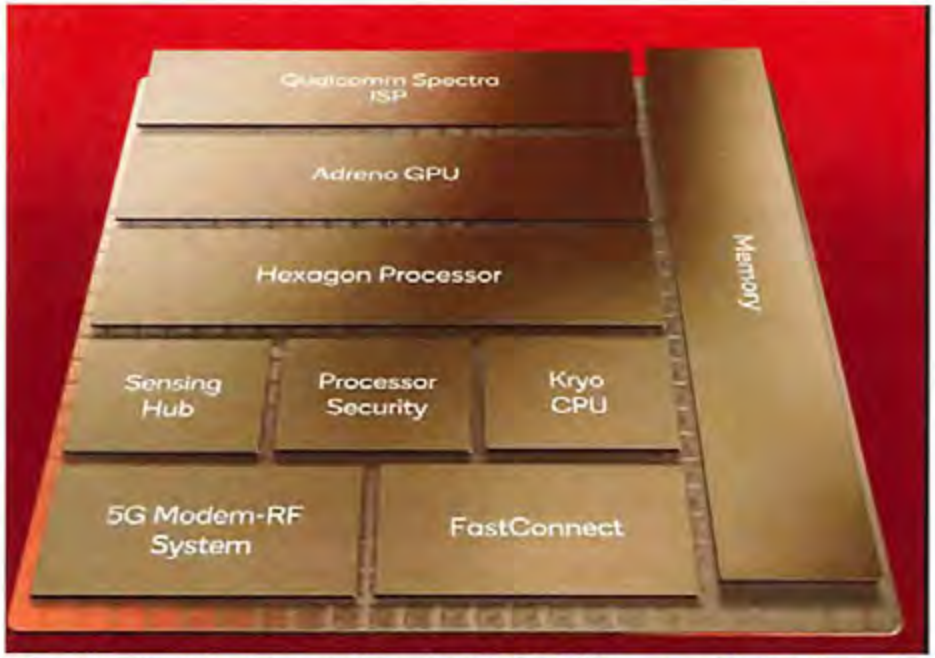
The CPU is a part of the SnapDragon SOC and coupled to the FastConnect network interface.



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

The access points are controlled by the server. For example, the server, which serves the functionality of the Android operating system, controls connection and/or data transmission of the access points. The Accused Products support the Wi-Fi standard. According to the standard, the Accused Products inquire about available Wi-Fi access points using a probe request, which is generating by the mobile operating server. The probe request comprises identifying information, such as a wildcard SSID or SSID for one or more access points or a preferred network list which is a set of SSIDs to which the UE got connected previously. An access point receiving the probe request must provide a probe response. As a further example, an access point receives and transmits data under control of the mobile operating server.

	In an infrastructure BSS or in an IBSS, STAs receiving Probe Request frames shall respond with a probe response when the SSID in the probe request is the wildcard SSID or matches the specific SSID of the STA or when the specific SSID of the STA is included in the SSID List element. Furthermore, a STA with dot11RadioMeasurementActivated true receiving a probe request with a DSSS Parameter Set element containing a Current Channel field value that is not the same as the value of dot11CurrentChannel shall not respond with a probe response. An AP shall respond to all probe requests meeting the above criteria. In an IBSS a STA that transmitted a Beacon frame since the last TBTT shall respond to group addressed Probe Request frames. A STA in an IBSS shall respond to Probe Request frames sent to the individual address of the STA. *Source: IEEE 802.11-2012.pdf*  **Figure 10-3—Probe response** *Source: IEEE 802.11-2012.pdf* An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
[24e] a memory to store the information	The Accused Products have a memory (e.g., memory of the SoC and/or storage) to store information regarding the at least one access point, and the authenticated access point list.

regarding the at least one access point, and the authenticated access point list; and	 https://www.qualcomm.com/news/onq/2022/11/new-snapdragon-8-gen-2-8-extraordinary-mobile-experiences-unveiled

Storage

-	-	128GB
256GB	256GB	256GB
512GB	512GB	-
1TB	-	-

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

As an example, the Accused Product confirms the received SSID information and/or other information from probe responses with access point information stored in its memory. Once confirmed that there is a probe response from an access point with which the Accused Product was connected previously, the Accused Product initiates a connection to the access point using an authenticated device identifier, such as a persistent MAC address that was used for a prior connection with the access point.

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

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]

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

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

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

Source: IEEE 802.11-2012.pdf

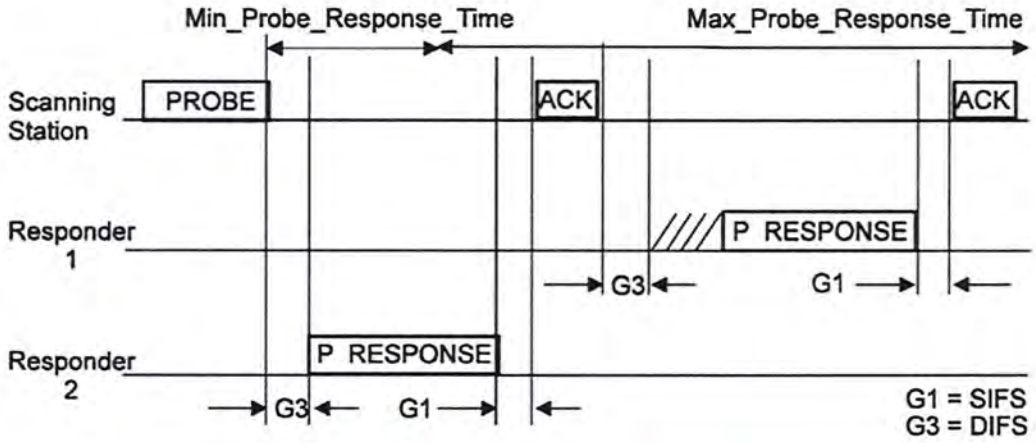
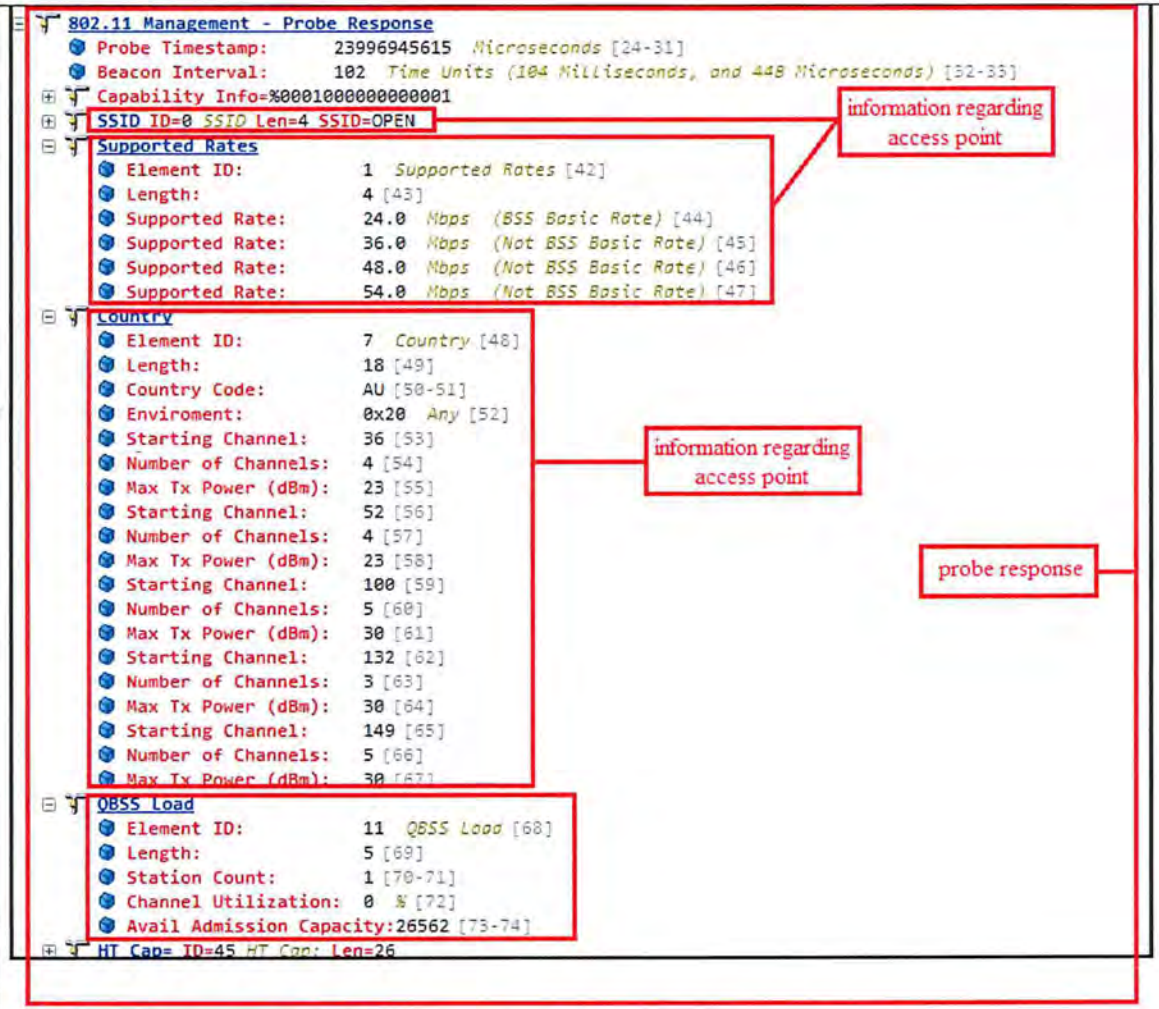


Figure 10-3—Probe response

Source: IEEE 802.11-2012.pdf

	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



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

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

[24f] a determination unit to determine, under control of the processor and based at least, in part, on the information regarding the at least one access point, whether the at least one access point is an authenticated access point and is under control of the server, wherein to determine whether the at least one access point is the authenticated access point and is under control of the server, the determination unit determines whether the information regarding the at least one access point is included in the authenticated access point list	The Accused Products include a determination unit (e.g., the portion of the OS that performs the determination) that determines, under control of the processor (e.g., executing the OS), in response to the receiving the probe response frame (e.g., probe response) and based at least, in part, on the information (e.g., SSID, supported data rates, key, etc.) regarding the at least one access point (e.g., Wi-Fi access point), whether the at least one access point (e.g., Wi-Fi access point) is an authenticated access point. As an example, the operating system and connectivity software of the Accused Product confirms the received SSID information and/or other information from probe responses using access point information stored in its memory. Once confirmed that there is a probe response from an access point with which the Accused Product was connected previously, the Accused Product initiate a connection to the access point using an authenticated device identifier, such as a persistent MAC address that was used for a prior connection with the access point. As shown, the Accused Products maintain a list of previously-connected access points which is matched to the access point's SSID received in the probe response. Each previously-connected access point is linked to a persistent MAC address for connecting to that access point. **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]

```
<?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" />
                <boolean name="HiddenSSID" value="false" />
```

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

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

Source: IEEE 802.11-2012.pdf

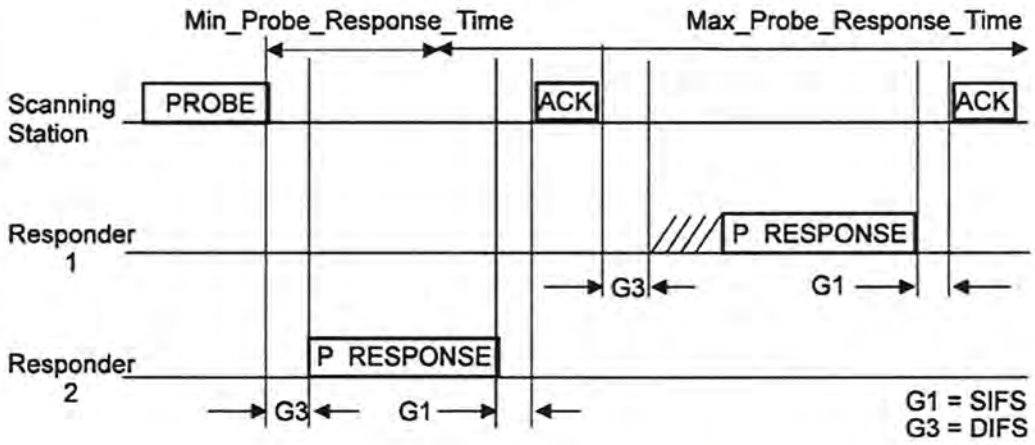


Figure 10-3—Probe response

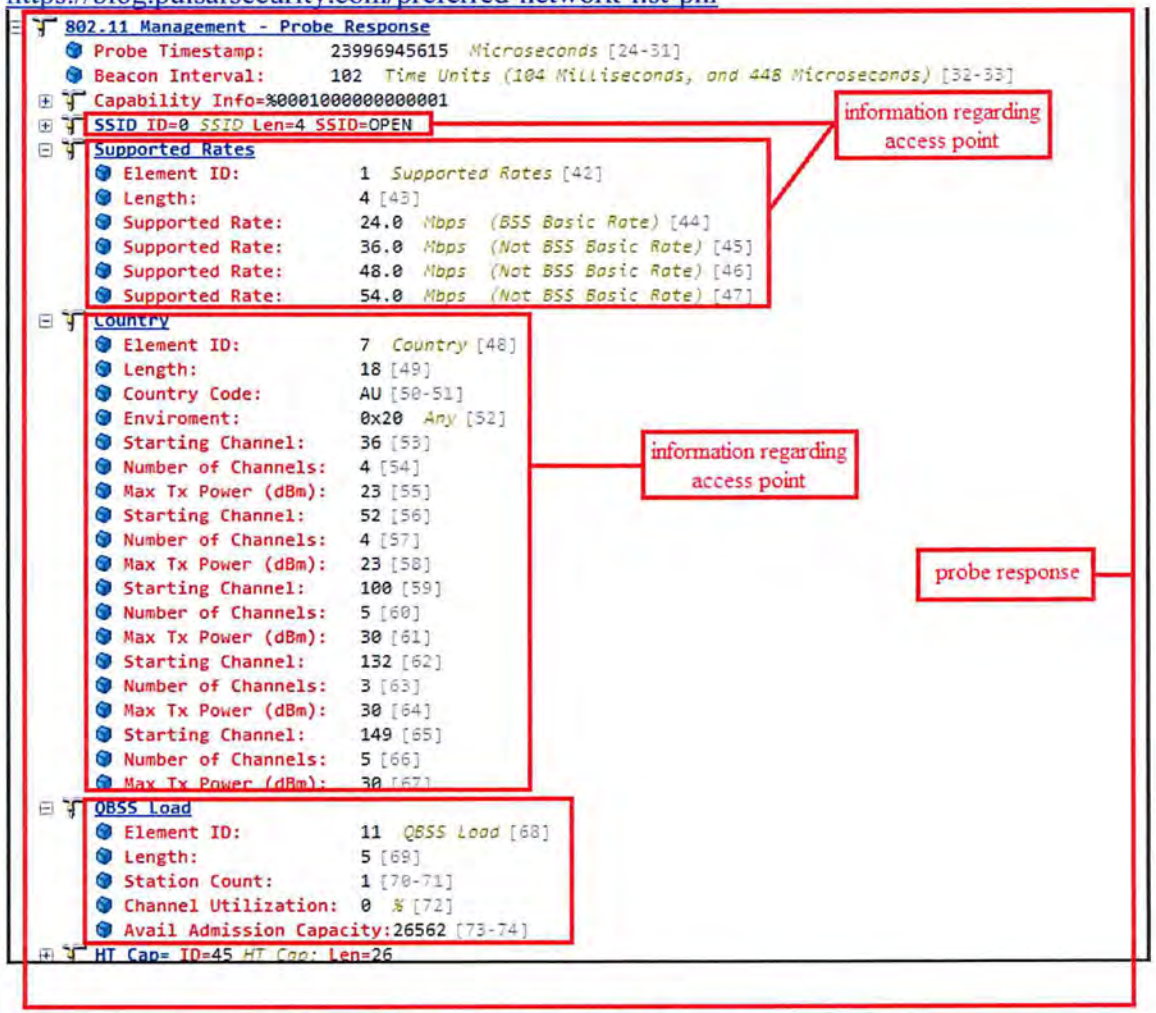
Source: IEEE 802.11-2012.pdf

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.

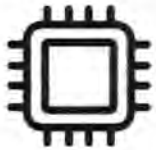
User devices trying to connect to a Wi-Fi network watch for access points (APs) broadcasting its availability for a device to connect to its network. Within that information contains the network name, or Service Set Identifier (SSID). Wi-Fi enabled devices trying to connect to a wireless network, and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



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

	The information in the probe response frame indicates that the access point is controlled by the mobile operating server. For example, the mobile operating server (e.g., the OS and/or a CPU and associated memory for storing and executing the OS and associated data), which serves the functionality of the Android operating system, controls connection and/or data transmission of the access point. The operating system runs on a CPU of the SoC (e.g., the Kryo CPU) of the Accused Product and is used to manage connections with an access point to control those access points to receive and transmit data. 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/



CPU

Kryo CPU

- 64-bit Architecture
- 1 Prime core, up to 3.36 GHz[2]
  - Arm Cortex-X3 technology
- 4 Performance cores, up to 2.8 GHz
- 3 Efficiency cores, up to 2.0 GHz

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

Phone	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



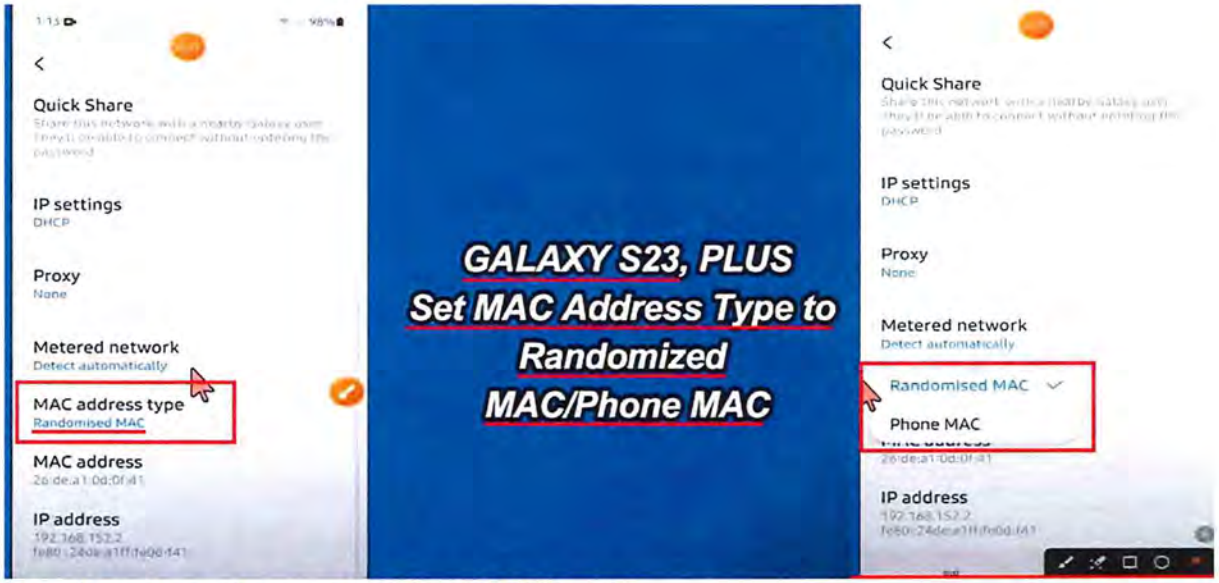
Wi-Fi 6E

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

	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* An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
[24g] wherein the transmitter further transmits to the at least one access point, a connection request that includes an authentic device identifier for the device, in response to a determination by the determination unit that the at least one access point is the authenticated access point and is under control of the server.	The transmitter transmits, to the at least one access point (e.g., Wi-Fi access point) in response to a determination that the at least one access point (e.g., Wi-Fi access point) is the authenticated access point, a connection request (e.g., association and/or authentication request) that includes an authentic device identifier (e.g., persistent MAC address) for the device. The transmitter transmits the connection request in response to a determination by the determination unit that the at least one access point is the authenticated access point and is under control of the server, as discussed above. After receiving the probe response from the access point, as discussed above, the Accused Products confirm the received SSID information from the probe responses with the access point information stored in memory. Once confirmed that there is an SSID in a probe response from an access point with which the Accused Product was connected previously, the Accused Products initiate a connection using the persistent MAC address for the access point, which is an authentic device identifier for the Accused Product.

Persistent randomization

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

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

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

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

Source: IEEE 802.11-2012.pdf

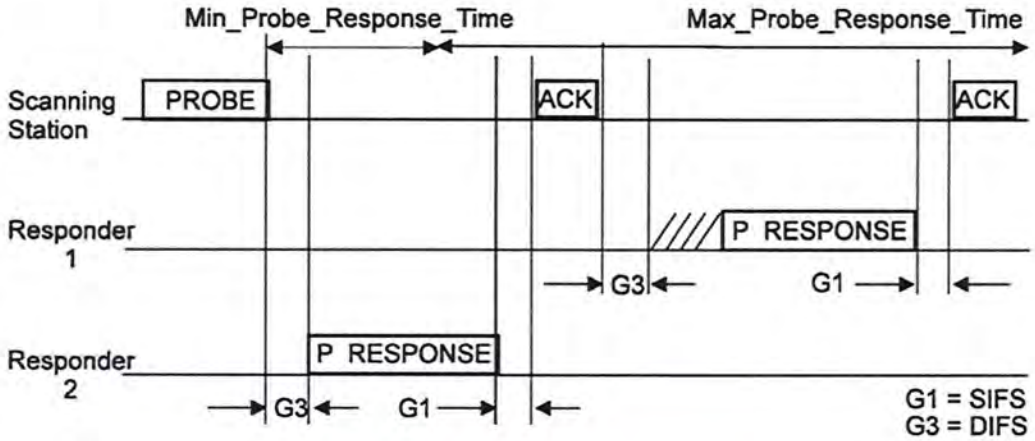
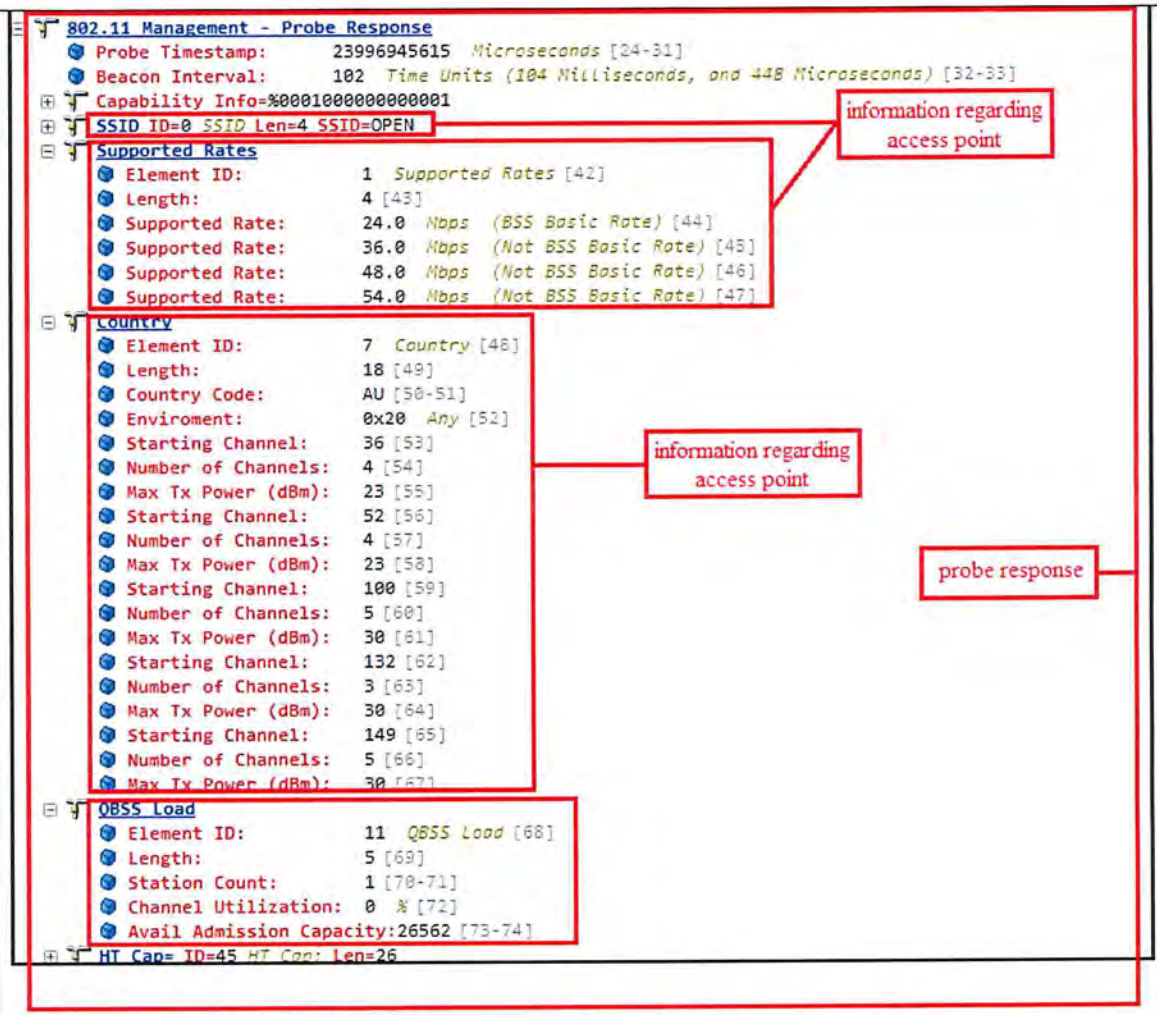


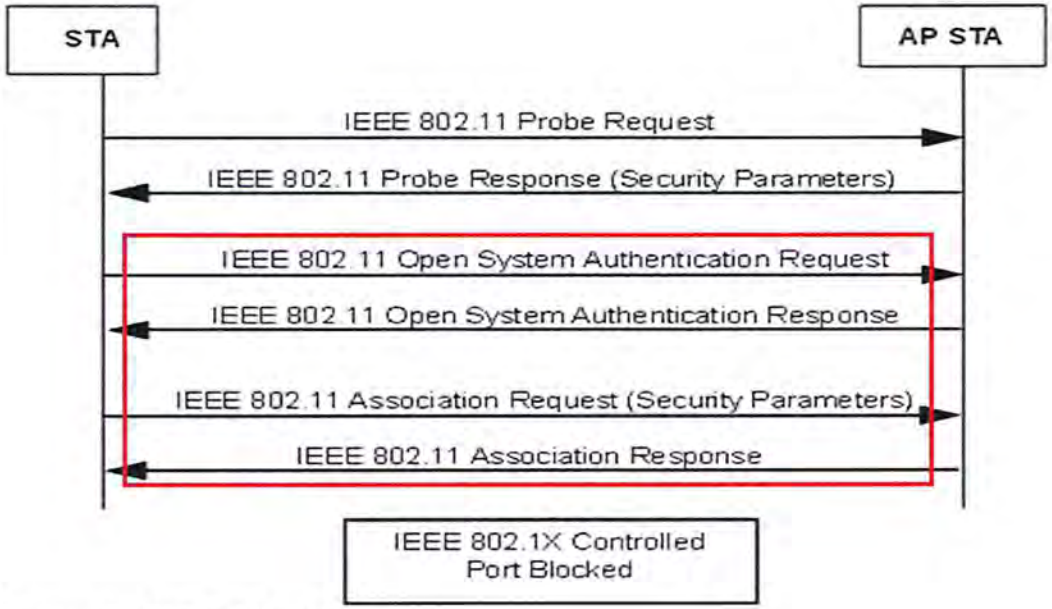
Figure 10-3—Probe response

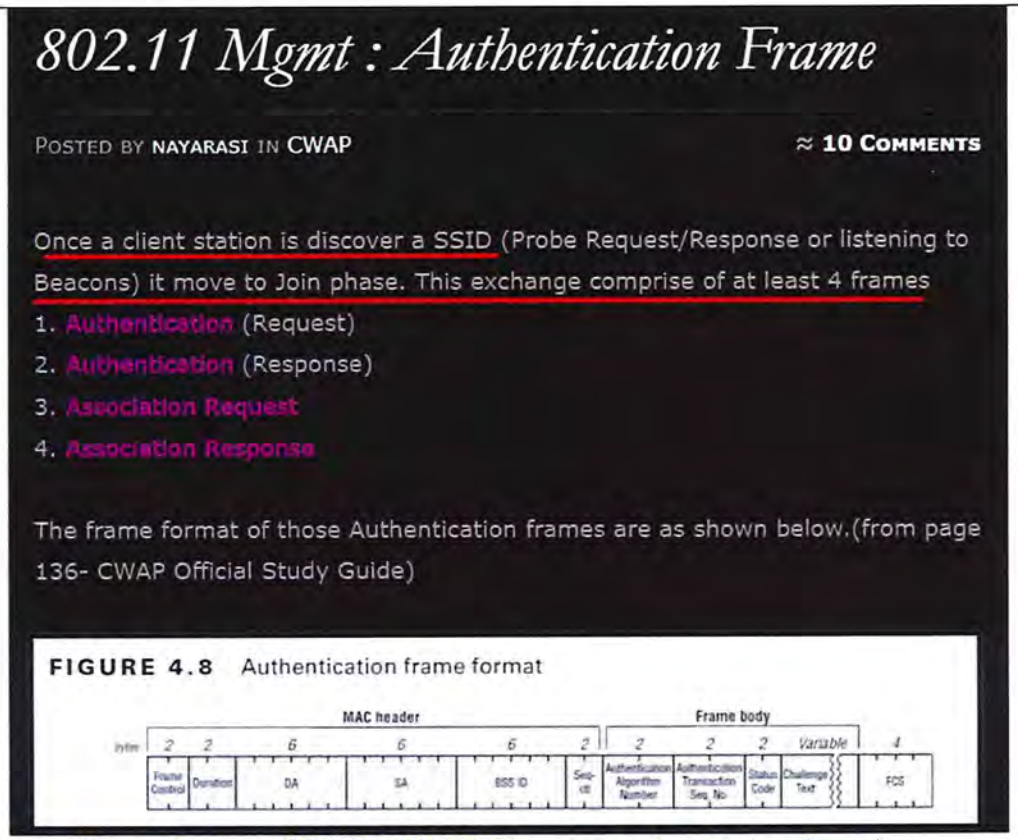
Source: IEEE 802.11-2012.pdf

	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



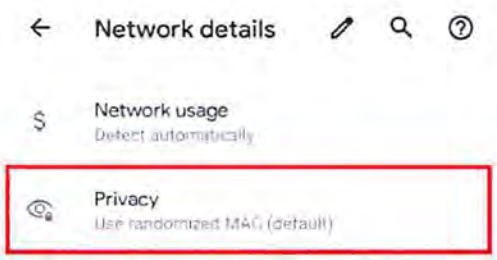
https://mrncciew.com/2014/10/27/cwap-802-11-probe-requestresponse/

	The Accused Products transmit an association and/or authentication request using the previously used persistent MAC address. The Accused Products then receive an association response from the access point, at which point the Accused Product is connected to a network via the access point in accordance with the association response.  *Source: IEEE 802.11-2012.pdf*

	 https://mrncciew.com/2014/10/10/802-11-mgmt-authentication-frame/ An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.
25. The system of claim 24, wherein the fake device identifier includes a fake media access	The fake device identifier includes a fake media access control (MAC) address.

control (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

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

 
Figure 1. MAC randomization option.
https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior

An analysis of source code may be necessary to fully and accurately describe the functionality of the Accused Products with respect to this limitation and, accordingly, Plaintiff reserves the right to supplement these infringement contentions once such information is made available to Plaintiff.</td></tr>
<tr><td>28. The system of claim 24, wherein the at least one access point includes a Wi-Fi access point, and wherein the at least one communication interface is configured for communication with a Wi-Fi network.</td><td>The at least one access point includes a Wi-Fi access point and the at least one communication interface is configured for communication with a Wi-Fi network.

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

<table>
<tr><th>Phone</th><th>Galaxy S23</th><th>Galaxy S23+</th><th>Galaxy S23 Ultra</th></tr>
<tr><td>Connectivity</td><td>5G, Wi-Fi 6E, Bluetooth 5.3, NFC</td><td>5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband</td><td>5G, Wi-Fi 6E, Bluetooth 5.3, NFC, ultra-wideband</td></tr>
</table>
https://www.androidpolice.com/samsung-galaxy-s23/</td></tr>
</table>

	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