Cisco DNA Center Q&A for Randomized MAC Addresses

Revised: August 20, 2021

MAC Randomization

Assigning random MAC addresses to mobile endpoint devices is nothing new, but how we use MAC randomization has changed over time. In the beginning, devices utilized MAC randomization to probe for known wireless networks. In probe request frames, devices hid real MAC addresses by randomizing the MAC address to provide some privacy. Over time, devices began using random MAC addresses to associate to wireless networks. Currently, this randomization causes issues for network elements that rely on MAC addresses to uniquely identify the endpoint device or the user behind the endpoint device. MAC randomization is implemented differently in devices because each hardware vendor uses unique algorithms in the implementation process. The following sections (Microsoft Windows 10 to Apple iOS 14) provide information about how mobile operating systems incorporate MAC randomization.

Microsoft Windows 10

The following bullets provide some key details about MAC randomization and Microsoft Windows 10:

- Randomization can be set up globally for all wireless connections or per network profile, also known as a service set identifier (SSID).
- Randomization is disabled by default because of factory presets.
- On the network profile, you can configure Windows 10 to generate a different random MAC address every day.
- After a random MAC address is used for a given network profile, that address is retained as long as you don't delete the network profile.
- If you delete the network profile, a different random MAC address is generated the next time you connect to the network.
- For more information about MAC randomization and configuration in Microsoft Windows 10, click here.

Google Android 10/11

The following bullets provide some key details about MAC randomization and Google Android 10/11:

- Randomization can be set up per network profile, also known as an SSID.
- Randomization is enabled by default for client mode, SoftAp, and Wi-Fi Direct because of factory presets.
- After a random MAC address is used for a given network profile, the device keeps using the same random MAC address even after you delete and recreate the network profile.
- For more information about MAC randomization and configuration in Google Android 10/11, click here.

Apple iOS 14, iPadOS 14, watchOS7

The following bullets provide some key details about MAC randomization and Apple iOS 14, iPadOS 14, and watchOS7:

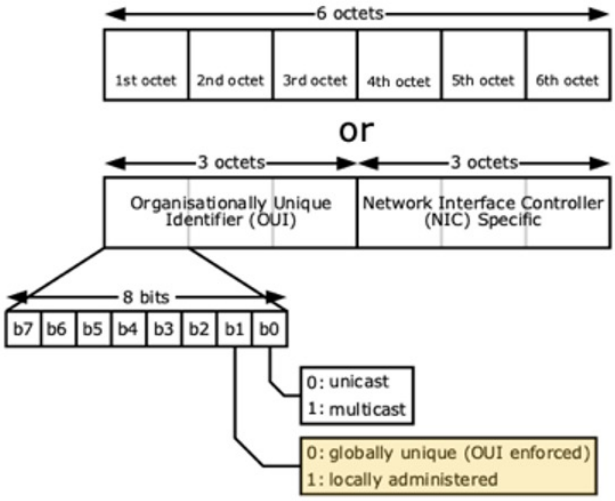
- Randomization can be set up per network profile, also known as an SSID.
- Randomization is enabled by default because of factory presets.

- For earlier iOS versions, MAC randomization is enabled for existing SSIDs when you update to iOS 14.
- After a random MAC address is used for a given network profile, the device keeps using the same random MAC address even after you delete and recreate the network profile.
- For more information about MAC randomization and configuration in Apple iOS 14, iPadOS 14, and watchOS7, click here.

MAC Randomization Behavior

This generation of MAC randomization follows rules set by the IEEE. The following diagram provides the foundational groundwork to understand the IEEE's rules. In Figure 1, you can see the 48-bit structure of a MAC address. Furthermore, the diagram shows how the b0 bit identifies whether the MAC address is unicast or multicast and how the b1 bit identifies if the MAC address is globally or locally administered. For a MAC address to be considered a random MAC address, the MAC address must be locally administered (the b1 bit set as 1) and be a unicast address (the b0 bit set as 0).

Figure 1: Structural Elements of a MAC Address



By Inductiveload, modified/corrected by Kju - SVG drawing based on PNG uploaded by User:Vtraveller. This can be found on Wikipedia here., CC BY-SA 2.5, https://commons.wikimedia.org/w/index.php?curid=1852032

Figure 1 displays the structural elements of a MAC address. Components include octets, bits, the OUI, and the NIC. The b1 bit determines if the MAC address is globallly or locally administered, and the b0 bit determines if the MAC address is a unicast or multicast address.

According to the IEEE, to qualify as a random MAC address, the first octet (in hexadecimal notation) must end with a 2, 6, A, or E. For example, in 32:8c:27:26:72:34 the 2 in the first octet reveals this is a random MAC address.

The following bullets provide clarifying information about MAC randomization's impact on client devices:

- For an end user device, the MAC address per SSID is maintained. The first time the client device joins the SSID, a new random MAC address is generated. If the client rejoins the same SSID, the client receives the same MAC address that it had previously.
- If the client device clears the SSID by forgetting the network and then rejoins the same SSID, the client receives the same MAC address.
- A client device can have a maximum MAC address equal to the number of SSIDs in the network.

- Duplication of MAC addresses is possible.
- Two different clients can have the same MAC address. This behavior is handled on the device side, but on rare occasion it is possible to have duplicate MAC addresses.

General Considerations on Bridged Networks

In bridged networks (Layer 2), we know that for a given VLAN the MAC address is used as a unique identifier, and this same MAC address can exist in different VLANs. Because the Layer 2 network cannot operate with MAC address duplication, the network devices and controllers must manage the duplication.

In a typical network, the control nodes may delegate the responsibility of MAC address duplication detection to First Hop Security (FHS) features. This reactive measure serves to detect and stop the access of the MAC address attacker.

The Layer 2 network treats the random MAC address duplication with this same reactive measure.

To illustrate how the Layer 2 network treats random MAC address duplication behavior and impact, read the following cases:

1. When enabling or disabling the random MAC address on the client, the SSID is the same and the client changes the MAC address (universal<>random).

   This case is treated as if the old client leaves the network and the new client joins. The old client goes through normal aging or no probing response detection and deletion. The new client goes through the normal onboarding process.

2. In a mobility event, the SSID is the same as the client moves networks.

   This case is managed as normal mobility.

3. When there is a duplication of random addresses, a random MAC address duplication may occur. The following bullets explain what may be duplicated:

   - The same SSID on the same VLAN, or different SSIDs mapping to the same VLAN
   - The same wireless LAN controller, or a different wireless LAN controller
   - The same node, or a different access node

Impact on Cisco Switches

This behavior is noted on wireless clients, so the impact analysis is focused on wireless clients. For wired clients, the duplication of MAC addresses is managed by the Switch Integrated Security Features (SISF), a component of Cisco FHS.

Client Onboarding

The wireless infrastructure identifies the wireless client based on the MAC address and treats it as a unique identifier. If the MAC address changes, the client is considered a new client.

The client goes through an authorization/authentication phase followed by IP address acquisition and then neighbor discovery, before finally being able to communicate across the network.

Authentication/Authorization

The client joins the network via access points (APs), and the APs communicate with the controller before granting access to the client. Random or universal addresses go through the same process.

Q&A

What is the impact on authorizing a client with a random MAC address?

Each unique MAC address is managed as a different client, so there is no impact.

Is the duplication of MAC addresses possible?

On rare occasions, you might see duplicate MAC addresses.

What happens if MAC address duplication occurs?

If MAC address duplication occurs in the same controller or network access node, the client is treated as if it left the network and is rejoining. If the MAC address duplication occurs in a different controller or network access node, the client is treated as a mobility event. The controller currently does not manage MAC address duplication.

IP Address Procurement

Clients can have a DHCP server-assigned IP address, a static IP address, or an autoconfigured IP address. These IP addreses are impacted by MAC randomization:

- For DHCP server-assigned and autoconfigured IP addresses, the IP address changes if the MAC address changes. This change is managed as if they are different clients. Therefore, neighbor discovery occurs after the IP address is assigned.
- For static IP addresses, if the MAC address changes but the same IP address is used for the network interface, traffic is impacted until the neighbor discovery cache is refreshed.

Q&A

How does MAC randomization impact the DHCP pool?

Each unique MAC address is managed as a different client. If the SSIDs use different DHCP pools, there is no impact. If the SSIDs use the same DHCP pool, there is a temporary impact until the lease of the IP address assigned to the old MAC address expires.

How does MAC randomization impact autoconfigured addresses?

The new MAC address is managed as a different client. The impact occurs on switches as the forwarding related tables caching the old IP address remain until they are deleted by aging mechanisms.

How does MAC randomization impact clients with a static IP address?

If the client changes the MAC address but keeps using the same IP address, traffic interruption is expected until the Address Resolution Protocol (ARP) cache is refreshed.

Neighbor Discovery

For networking devices to communicate at Layer 3, the devices in the network use a Neighbor Discovery Protocol (NDP), such as ARP, to discover the next hop to the destination MAC address.

Q&A

How does MAC randomization impact NDP and ARP?

Because the MAC address changes, the neighboring devices must refresh the ARP and NDP cache after the MAC address change. Otherwise, the traffic that depends on this information is disrupted.

Impact on Cisco DNA Center

Assurance

Wireless Clients 360

- Assurance identifies the wireless client based on the MAC address and treats it as a unique identifier. If the MAC address changes, the client is considered a new client. The different MAC address-based client history is not merged for the same user device. The user device must search for the individual MAC address to obtain the details and metrics.
- In Assurance, the concurrent client count is calculated based on the latest telemetry data. At a 5-minute interval, if a client that is enabled with a random MAC address joins a different SSID, a duplicate client is created for the other SSID and the client count increases. In the next 5-minute interval, the client count is corrected based on the new telemetry data.
- The Event Viewer and metrics are limited to the MAC address.

Q&A

What is MAC randomization's impact on the unique client count or the overall client count?

The historical client count increases based on the number of SSIDs that the client joins in the network.

Is the duplication of MAC addresses possible?

On rare occasions, you might see duplicate MAC addresses.

My Client 360 window has gaps, but I don't see the client drop out?

If the device joins a different SSID and changes the MAC address, the data isn’t plotted in correspondence to the current MAC address. If the same device rejoins the same SSID and retrieves the old MAC address, the data is plotted. Therefore, the gap is expected. You can see the data by navigating to the **Client 360** window for the other MAC address.

How does MAC randomization impact Cisco DNA Center if the network has duplicate MAC addresses?

Cisco DNA Center displays unexpected behavior and inaccurate metrics.

What is the impact on the Event Viewer?

If the client changes the SSID, the Event Viewer cannot capture the event of another MAC address. To view the event history, you can navigate to the respective client based on the MAC address.

Is it possible to view all events and other metrics in one place?

You must navigate to the respective MAC address to see the specific events and the other key performance indicators.

Application Experience

The overall Application Experience is not impacted by MAC randomization, but the client-based and user-based application metrics are limited to the MAC address.

Q&A

How does MAC randomization impact Application Experience?

In the Overall Application Experience trend window, client usage is separated based on the device's number of MAC addresses.

Is it possible to see the aggregated usage or throughput metrics for a single user device?

There is no direct way to see the aggregated usage or throughput metrics information. However, if all the MAC addresses of the user are known, it is possible to obtain and add the individual application metrics of each MAC address.

Health Score

MAC randomization has no impact on the Health Score.

Q&A

Does MAC randomization have any impact on the client health score?

There is no impact on the client health score. If the client joins the network with a different MAC address, the user is treated as a new client, and the health score is calculated for that user session.

Global Search

If clients enabled with MAC randomization join mulitple SSIDs, you might see more client devices when you do a global search for a user or device name.

Q&A

Why do I see many device entries when I search for a particular device hostname?

If a device enables MAC randomization and that device joins multiple SSIDs, Cisco DNA Center collects more than one unique client entry. The search results display all the client entries based on the MAC address.

Are there any issues with user search?

User search is not impacted by MAC randomization. The search continues to display all the associated device entries. If the client joins different SSIDs, you will see more devices.

Intelligent Capture

The client capture is scheduled based on the MAC address. If the client changes the MAC address, the event is treated as a client disconnect and the packet capture stops.

Q&A

Does MAC randomization have any impact on client capture for my existing schedule?

If the client capture is scheduled before the client upgrades to iOS 14, the MAC ID is absolute. You must delete the existing schedule and recreate a new one with the current MAC address.

If the client changes the SSID, does this impact the client capture?

Yes, the client capture stops after the client switches to a different SSID.

Does MAC randomization have any impact on the scale or number of devices that can be scheduled for client capture?

Cisco DNA Center limits 16 MAC addresses for partial capture and 1 MAC address for full capture. If the client joins multiple SSIDs, there are multiple MAC addresses for the same device. For a single user, you might have to schedule more than one client capture, which limits you from scheduling more captures for different users at the same time.

AI Network Analytics

The following bullets show MAC randomization's impact on AI Network Analytics: the Network Heatmap, site comparison, and AI Issues generation.

- For the Network Heatmap, the client count is a higher number based on the MAC address.
- For site comparison, there is no impact.
- For the AI Issues generation, it is aggregated at the SSID level. Otherwise, there is no impact.

Wi-Fi 6

If clients move between different SSIDs, the client capability count increases for up to 5 minutes. For the next 5-minute interval, the count is corrected based on updated telemetry data obtained from the wireless LAN controller.

Q&A

Does MAC randomization have any impact on Wi-Fi 6 historical metrics?

Based on the unique client MAC address count in Cisco DNA Center, the historical client count might show increased values based on the number of SSIDs that the client joins in the network.

Rogue Clients

Based on MAC randomization, the number of rogue clients depends on the device's number of MAC addresses. Otherwise, there is no impact on intrusion detection, and MAC address collision and signatures are unaffected.

Q&A

Does the rogue detect the correct attack MAC address if MAC randomization is enabled?

The attack MAC address is the random MAC address, not the physical one.

Maps and Cisco DNA Spaces

Duplicate clients on maps are shown when the client joins on a different SSID.

Device Classification

The Organizationally Unique Identifier (OUI) field is not shown, and the device type workstation and OS might be inaccurate.

Cisco DNA Center Client Issues

Global issues may trigger faster because even if the same client fails multiple times across SSID, it is detected as multiple clients failing. Issues that depend on different SSIDs may be delayed.

Q&A

Are there any examples of a global issue that is affected because of MAC randomization?

Client issues, such as authentication failures, DHCP failures, or wireless LAN controller-related failures (that is, with a scope WLC, DHCP server, AAA server), may trigger global issues faster. These failures occur because even if the same client fails multiple times across the SSID, it is detected as multiple clients failing.

Is there any issue that can be delayed in Cisco DNA Center because of MAC randomization?

The “Dual Band capable client prefers 2.4 GHz over 5 GHz” issue relies on the nearest 5-GHz probe data from other APs. This issue may be slower to detect because the client probing on a different SSID is not counted. Cisco DNA Center detects it as a new client.

General Q&A

Q&A

Is there any impact on Apple Analytics?

Apple Analytics is retrieved from wireless LAN controllers, so Cisco DNA Center has no impact on Apple Analytics.

If the IP address lease time is high and the old session is not expired, is a duplicate client shown?

If the VLAN is the same, the DHCP server runs out of IP addresses if a high lease time is set. If the VLAN is different, the behavior is the same as it is today.

Does this limit my number of sessions on the device?

If a MAC-to-user mapping limit is added, it might impact the number of client sessions.

Scale

Q&A

Does MAC randomization impact the number of clients that Cisco DNA Center monitors?

The historical client count might increase if clients use random MAC addresses. In the worst case, the client count might increase to the actual number of clients multiplied by the number of available SSIDs. This increase is only possible if all clients are using random MAC addresses and join all the SSIDs available in 14 days, which might exceed the published scale limits based on the customer scale and use case.

Does MAC randomization have a scale impact on Intelligent Capture?

There is no direct impact, but Cisco DNA Center limits 16 MAC addresses for partial capture and 1 MAC for full capture. If the client joins multiple SSIDs, there are multiple MAC addresses for the same device. For a single user, you might have to schedule more than one client capture, which limits you from scheduling more captures for different users at the same time.

SD-Access Provisioning

MAC randomization has no impact on SD-Access provisioning.

Workaround

One workaround is to disable the MAC randomization feature on the client.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.