purple

MAC Randomization Guide

Overview of MAC Randomization Changes in iOS 18 and macOS 15

September 2024

Background

MAC address randomization was introduced over a decade ago to enhance user privacy by masking device identities on WiFi networks. With iOS 18 and macOS 15, Apple has implemented new MAC address randomization features. These include regularly rotating MAC addresses, which are now enabled by default for 'less secure' WiFi network types: any open network, or networks running older security protocols. This change aims to bolster privacy but presents challenges for WiFi network operators relying on MAC addresses for device identification and management.

Key Changes in iOS 18 and macOS 15

1. **Rotating Private MAC Addresses:** iOS 18 and macOS 15 introduces rotating MAC addresses for connections to WiFi networks with no or weak security (e.g., open networks or public hotspots). These addresses change every 14 days, potentially disrupting network services if the network is using the MAC as a static device identifier.
2. **Fixed Private MAC Addresses:** Used by default for secure WiFi networks (networks using secure passwords/keys, e.g., WPA2/WPA3 or 802.1X based), where MAC addresses remain static. Users retain the option to manually adjust MAC address settings for each WiFi network.
3. **User Control and Implications:** Users can now control MAC address settings on a per-network basis, potentially affecting WiFi networks that rely on MAC addresses for security measures or parental controls.

Impact Analysis by Sector

- **Residential:** Minimal to no impact, mostly affecting homes with unsecured or outdated Wi-Fi protocols. Service providers may require updated security settings or routers.

- **Hospitality:** Impact due to reliance on MAC addresses for guest authentication. WiFi networks may need updates to handle multiple MAC addresses for single devices, where access is limited to a specific number of devices, and guests may have to log in more frequently.

- **Public & Municipal Networks:** Increased friction for users as MAC addresses rotate, causing frequent re-authentication. MAC-based analytics will become less accurate over time (e.g. repeat users).

- **Enterprise:** Challenges in device classification and troubleshooting. Enterprises may need to adopt new strategies for network monitoring and security policy enforcement.

- **Education:** Potential complications in managing authentication logs and user data. Schools and universities may need to shift from MAC-based systems to policy-based alternatives.

- **Transportation:** Similar to public networks, with low-frequency travelers likely needing to re-authenticate each time they use the network.Hospitality: Significant impact due to reliance on MAC addresses for guest authentication. Networks may need updates to handle multiple MAC addresses for single devices.

Impact Analysis by Sector

- **Healthcare:** Critical for Guest Wi-Fi and secure networks. Must shift from MAC-based tracking to other forms of device identification to ensure compliance with privacy laws and uninterrupted service.

- **Stadiums:** Public and guest Wi-Fi in large venues will see frequent user re-authentication, affecting user experience. Networks should consider moving to authentication methods like Passpoint or app-based credentials.

- **Retail:** Customer-facing Wi-Fi services and in-store analytics will be affected by changing MAC addresses, leading to inaccurate foot traffic and customer behavior data. Adjust analytics tools and consider alternative device identification methods.

- **Airports:** Frequent travelers may need to re-authenticate more often due to rotating MAC addresses. Use of loyalty apps and Passpoint can help maintain a seamless user experience.

Future Outlook

The trend toward more frequent MAC address randomization is expected to continue, potentially leading to daily or per-session changes. WiFi network operators should prepare by moving away from reliance on MAC addresses as unique device identifiers and adopting alternative methods for device management and authentication.

Conclusion

While the changes in iOS 18 and macOS 15 primarily enhance user privacy, they pose varying levels of challenges for WiFi network operators. The overall impact on end-users is expected to be minimal, but WiFi network operators must adapt to mitigate disruptions and prepare for more frequent changes in the future.

To view our latest webinar and other IOS information click here.
To learn about Purple's SecurePass solution to the recent changes click here.

Mac Randomization Guide

Want to find out more?
Speak to an expert here

purple