

# Impact of Dual Wi-Fi Acceleration on Enterprise Networks

---

First Published: 2023-10-06

## Impact of Dual Wi-Fi Acceleration on Enterprise Networks

### Introduction to Dual Wi-Fi Acceleration

Some mobile vendors have recently launched a new feature called Dual-Band Wi-Fi on Android smartphones. This feature enables users to simultaneously connect to two distinct Wi-Fi networks operating on different frequency bands, such as 2.4 GHz and 5 GHz.

This functionality is also known as:

- Dual Wi-Fi Acceleration
- Dual Wi-Fi Simultaneous
- Dual-Band Wi-Fi

The significance of this feature is that it will have repercussions on all the Cisco networking products providing Wi-Fi solutions, in terms of scale, security, licenses, and assurance.

This white paper provides details about the feature, its endpoint behavior, and its impact on different networking products.

The key aspects of this feature are:

- A Wi-Fi network operating at 2.4 GHz and another at 5 GHz can coexist without any interference because they operate on different frequency bands. These two networks can independently transmit and receive data simultaneously, without affecting each other.
- The SSIDs can have the same name or two different names.
- The SSIDs can be on the same access point or router, for example a dual-band router at home, or two different devices.



---

**Note** A similar feature called Dual Channel Network Acceleration shares similarities with this feature in scenarios where devices connect to a Wi-Fi network and a GSM or LTE network simultaneously. The Dual Channel Network Acceleration feature is available on multiple Android phone models for many years now and is popular.

---

For the apps on an Android phone to utilize multiple network connections simultaneously, they need to be developed such that they support the Dual Wi-Fi Acceleration feature. Enabling this feature displays a list of

installed apps that are compatible and can take advantage of the technology. Popular apps that are currently compatible are YouTube, Amazon Prime Video, Netflix, WhatsApp, Instagram, and Facebook.

The most significant benefit for end-users is the additional bandwidth available to apps that support this feature. For instance, simultaneously downloading one video while watching another would be quicker using this feature, compared to when this feature is not accessible (assuming the upstream internet connection has ample bandwidth available).

The Wi-Fi 7 standard will support multi-link operation (MLO) as an aggregation of multiple bands or channels. With MLO, multi-link devices (MLDs) can associate and simultaneously exchange data traffic on 2.4-GHz, 5-GHz, and 6-GHz bands with common unicast encryption keys across links, whereas preexisting Wi-Fi technologies do not allow devices to exchange data via multiple bands at the same time with common layers above L2.

## Feature Details

### Chipsets, Vendors

The following chipsets from Qualcomm support the Dual Wi-Fi Acceleration feature:

- Snapdragon 8 Gen1 and 2
- Snapdragon 8+ Gen1
- Snapdragon 870
- Snapdragon 888 Octa-core

The following Android mobile vendors have models that support the feature:

- Realme
- OnePlus
- Oppo
- Vivo
- Xiaomi



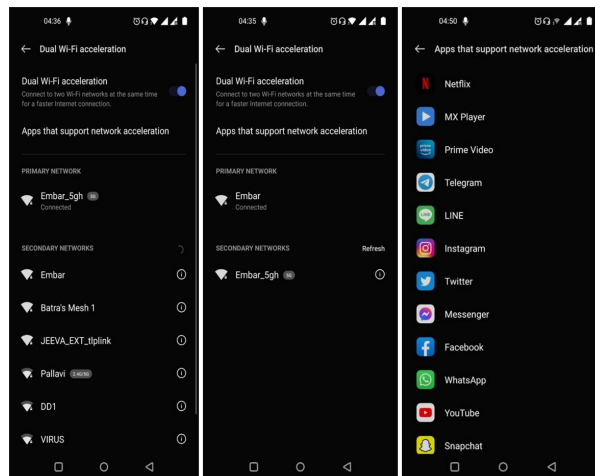
---

**Note** It is possible that additional chipsets and vendors could support this feature in the future.

---

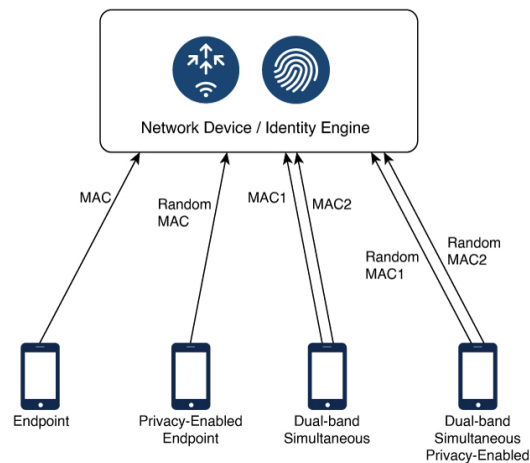
### OnePlus 9RT – Sample Screenshots

The following screenshots on a OnePlus 9RT device show how the Dual Wi-Fi Acceleration feature can be configured. It also shows the typical list of apps that support the acceleration.



## Device Onboarding

The devices enabled with the Dual Wi-Fi Acceleration feature make two separate connections on a network by using two different MAC addresses and two different IP addresses.



Since this feature is supported by specific Qualcomm chipsets, it appears as two separate endpoints to network devices and orchestrators. This paper examines the effects of using this feature and its impact on various Cisco networking products and solutions.

## Observations

All the tests that were performed for this study were conducted using the following devices (except for MAC address correlation, where more devices were tested). Observations are based on this study:

- OnePlus 11 5G
- OnePlus 11r 5G
- Realme GT 5G

## Basic Connectivity

The following are the observations regarding the Wi-Fi connectivity of the device using dual Wi-Fi bands:

- The device establishes two different connections on the network on two different channels (2.4 GHz and 5 GHz).
- The device acquires two different IP addresses and establishes a connection using two different MAC addresses and works on two different network stacks.
- Secondary connectivity cannot be established until primary connectivity is established.
- If the primary MAC address is blocked on the access point or the router, the device cannot connect to the network using the secondary MAC address.
- If the secondary MAC address is blocked, there is no impact on the primary connection.

## MAC Address Correlation

The following table captures the built-in MAC addresses allocated for the two-network stacks for some sample devices.

| Mobile            | Primary MAC Address | Secondary MAC Address | Chipset                     |
|-------------------|---------------------|-----------------------|-----------------------------|
| OnePlus 9R        | AC:D6:18:77:78:07   | 00:0A:F5:89:89:FD     | Snapdragon 870              |
| OnePlus 10 Pro 5G | 48:74:12:95:72:15   | 48:74:12:18:72:15     | Snapdragon 8 Gen1           |
| OnePlus 10T 5G    | 30:BB:7D:4B:62:B3   | 30:BB:7D:D1:62:B3     | Snapdragon 8+ Gen1          |
| OnePlus 11 5G     | 30:BB:7D:D5:39:3D   | 30:6B:7D:56:39:3D     | Snapdragon 8 Gen2           |
| OnePlus 11 5G     | 30:BB:7D:D5:3E:43   | 30:BB:7D:56:3E:43     | Snapdragon 8 Gen2           |
| OnePlus 11r 5G    | 30:BB:7D:DE:4A:A5   | 30:BB:7D:65:4A:A5     | Snapdragon 8+ Gen1          |
| Xiaomi 12 Pro 5G  | 50:DA:D6:8F:DB:FE   | 50:DA:D6:11:DB:FE     | Snapdragon 8 Gen1           |
| Realme GT 2       | CA:DF:39:65:75:31   | C4:DF:39:E5:75:31     | Snapdragon 888<br>Octa-core |

- For all devices, except an old model (OnePlus 9R), the organizationally unique identifier (OUI) and last 2 bytes are the same for primary and secondary MAC addresses, and only differ in the fourth octet.
- The primary and secondary MAC addresses remain fixed regardless of the band (2.4 GHz or 5 GHz) that is selected.
- Primary interface is used to scan all the SSIDs, and there is no wildcard scan using the secondary interface.

## DHCP Correlation

The following are the observations related to the DHCP interaction of mobile devices:

- The device sends the same Hostname (Option 12) and Vendor Class Identifier (Option 60) for both the interfaces.

- No correlation was discovered for the client hardware identifier because it is the same as the MAC address of the interface. This is irrespective of random MAC selection.

## 802.1X Behavior

The secondary interface does not list the SSIDs that have 802.1X configured. We can make a 802.1X connection only by using the primary interface.

## Repercussions

An important finding of the study is that the devices are unable to utilize 802.1X authentication for the secondary interface. While this may not be a significant problem for enterprise networks that use 802.1X authentication, it could become an issue if vendors begin supporting 802.1X on both interfaces, leading to various potential consequences.

Wi-Fi providers, such as airports and cafes are likely to face the immediate consequences listed below.

## Scale Issue

In a network that has been designed based on a certain number of mobile devices or endpoints, enabling this feature could result in each device establishing two connections, potentially doubling the anticipated load. As a result, most networking equipment and controllers are likely to be impacted:

- Access points, controllers, switches, routers
- Cisco ISE servers
- DHCP servers
- Some areas of Cisco DNA Center (for example, Cisco Assurance, Cisco AI Endpoint Analytics)

## Lack of Unified View for Clients

When devices make two simultaneous connections, they appear as two separate endpoints on the network side. Unless a mechanism is found to identify that those two connections belong to the same device, the network treats each as a separate device. This leads to lack of unified view for the devices, and administrators cannot control it effectively. The following products could be affected:

- Cisco DNA Center: Client 360 view
- Cisco ISE: Endpoint view

## License Exhaustion

Sometimes, the licensing of products is based on the number of endpoints on a network, and the devices using the Dual Wi-Fi Acceleration feature might start using up twice the number of entitlements. Cisco ISE is one such product.

## Rapid Threat Response

Products such as Cisco AI Endpoint Analytics and Cisco ISE can be used to automatically (or manually) quarantine malicious endpoints on the network based on threat or anomaly detections. If a device makes two connections and a threat is detected on only one of those, only that MAC address gets quarantined, and the second connection can continue to operate on the network. Ideally, network administrators would like to quarantine the whole device.

## Quota Management

If bandwidth quotas are configured on the network, it is possible that these will get bypassed when a device uses two simultaneous connections, unless the network controller has a way to determine that these two connections belong to the same device.

## Possible Workarounds

While the future enterprise networking Cisco products will have methods to mitigate these repercussions, there are some workarounds that could be employed in the interim.

- Advise users with BYoD devices to turn off the dual Wi-Fi acceleration feature.
- Enhance MDM agent to turn off the feature when the device connects to the enterprise network.
- Be on the look out for MAC addresses with a matching pattern as described above to identify the same endpoints.
- Do not allow insecure SSIDs.

## Conclusion

The Dual Wi-Fi Acceleration feature is exciting for end-users because it enables them to use the available bandwidth more efficiently, especially in scenarios where upstream internet bandwidth is higher than that of a single Wi-Fi band. It is typically targeted for special use cases such as gaming and streaming. It might not be an immediate concern for enterprise networks, mainly because it does not support 802.1X authentication. However, it would be a concern for providers that operate PSK or WebAuth-based networks and could become a concern for enterprises if mobile vendors start supporting 802.1X for dual Wi-Fi acceleration.

Networking or controller vendors need to invest in solutions that determine the uniqueness of devices across both network connections, so that administrators get better visibility into devices and can manage the network more effectively.

## References

- <https://www.oneplus.in/11>
- <https://www.realme.com/in/support/kw/doc/2054463?queryId=d40fde36eaf49c68cb3092500805aab&articleIndex=3>
- <https://www.dignited.com/49852/oppo-vivo-dual-wifi-technology/>

---

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)

© 2023 Cisco Systems, Inc. All rights reserved.