# Wi-Fi Alliance Agile Multiband

## Introduction to Wi-Fi Alliance Agile Multiband

The Wi-Fi Alliance Agile Multiband (MBO) feature enables better use of Wi-Fi network resources. This feature is built on the fundamental premise that both Wi-Fi networks and client devices have information that can enable better roaming decisions and improve the overall performance of Wi-Fi networks and user experience.

**Note** This feature applies to MBO certified clients only.

This feature certifies the interoperability of a bundle of features that are defined by the IEEE standard amendments 802.11k, 802.11v, and 802.11u, as well as the Wi-Fi-Alliance defined specifications. These technologies are used to exchange access points (AP), band, and channel preferences, link quality, and status information between AP and client device.

MBO focuses on the following:

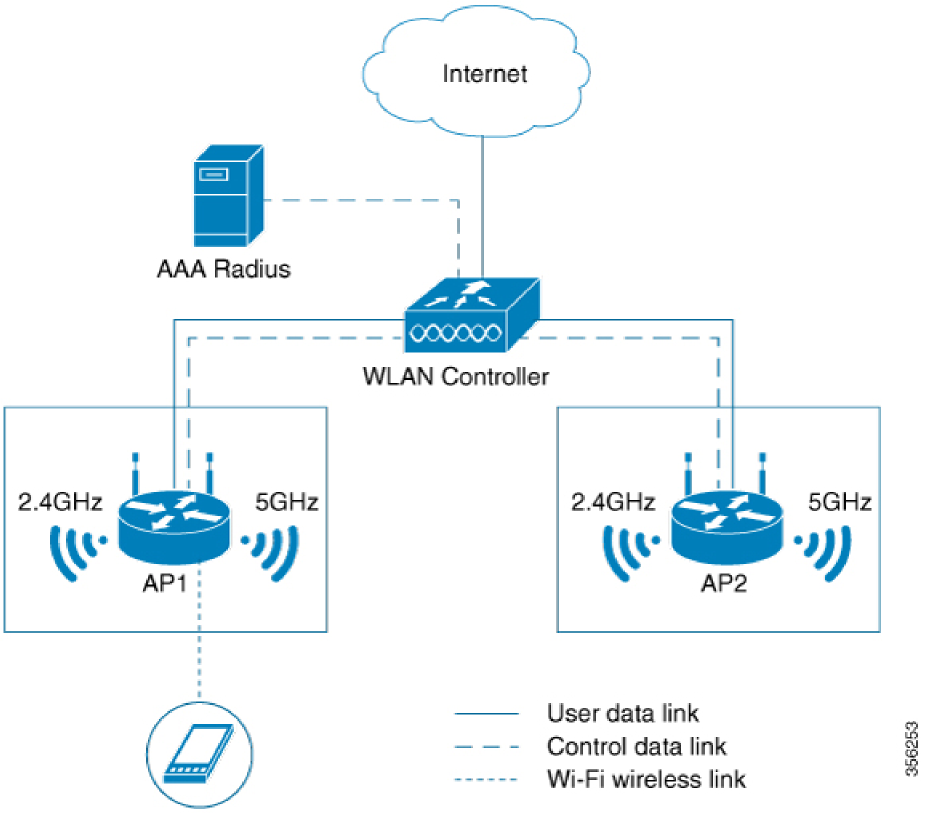
- Interactions between the wireless clients and APs
- Exchange of AP and client knowledge about the wireless medium (such as RF neighbors)
- Allow clients to work with APs and take intelligent decisions on the connection and improve the quality of service.

### Wi-Fi Alliance Agile Multiband Topology

Multiple components form a Wi-Fi Agile Multiband wireless infrastructure network, which may vary based on the wireless network deployment.

The following figure depicts the system topology for connecting Wi-Fi Agile Multiband devices.

*Figure 1: Wi-Fi Agile Multiband Wireless Infrastructure Network*



The following components form a Wi-Fi Agile Multiband wireless infrastructure network:

- Access Point (AP): A Wi-Fi Agile Multiband wireless infrastructure network contains one or more Wi-Fi Agile Multiband APs.
- WLAN Controller: A Wi-Fi Agile Multiband wireless infrastructure network contains zero or more WLAN controllers that provide centralized management and other features to the interconnected APs.
- Client Station (STA): A Wi-Fi Agile Multiband wireless infrastructure network contains zero or more STAs. These client STAs are single WLAN capable only.
- RADIUS Server: A Wi-Fi Agile Multiband wireless infrastructure network contains zero or more RADIUS Servers that provide Authentication, Authorization, and Accounting (AAA) services.

## Supported MBO Components

### MBO AP Capability

A new information element is added to the Beacon, Probe Response, Association Response and Re Association Response Frames for 802.11ax APs to inform clients about MBO support.

**Note** The new information element indicates that Cisco APs are not cellular data aware.

When an SSID is configured on an AP, the MBO AP capability is enabled.

#### 802.11k/v/r Support

One of the prerequisites for MBO is that APs need to support 802.11k/v/r standard-based technologies. Each of the technologies has their own requirements, such as:

- 802.11k – For 802.11k, send the preferred list of AP neighbors to the client upon request and send a beacon request to a client when AP requires a beacon report from the client.
- 802.11v – For 802.11v, steer the client to a less congested AP (not in a MBO client's non-prefer/non-operable channel list that is sent during the association request and/or WNM notification request) using BSS transition.
- 802.11r – The 802.11r MBO-related capabilities are not supported.

#### 802.11u ANQP or GAS Support

For MBO, the 802.11ax APs must have 802.11u ANQP or GAS support.

The following are the prerequisites:

- ANQP responds to the ANQP request for a neighbor report ANQP-element.
- Before authentication, Layer 2 transport needs to be available in the network between a mobile device and server for an advertisement protocol frame.

#### MBO Beacon Request

Whenever an AP sends a beacon request to the client, the MBO-compliant client responds with a beacon report.

#### MBO Associate Disallowed IE

Cisco APs include an **Associate Disallowed IE** in their Beacon/Probe response/(Re) association response when they cannot accommodate any new client.

# Limitations of MBO

All non-802.11ax access points are not supported.

# Configuring MBO on a WLAN

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 2** | **wlan** *wlan-name wlan-id ssid*<br>**Example:** | Configures a WLAN and enters the WLAN configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config)# wlan wlan-demo 1 ssid-demo` | **Note** If you use WPA2 WLAN while configuring MBO for WLAN, you need to enable PMF in your configuration. |
| **Step 3** | **mbo**<br>**Example:**<br>`Device(config-wlan)# mbo` | Configures MBO support on WLAN.<br>**Note** Use the **no mbo** command to disable MBO configuration. |
| **Step 4** | **end**<br>**Example:**<br>`Device(config-wlan)# end` | Returns to privileged EXEC mode.<br>Alternatively, you can also press **Ctrl-Z** to exit global configuration mode. |

# Verifying MBO Configuration

To view the MBO configuration, use the following command:

```
Device# show wlan id 1
WLAN Profile Name     : wlan-demo
================================================
Identifier                                     : 1
Description                                    :
Network Name (SSID)                            : ssid-demo
Status                                         : Disabled
Broadcast SSID                                 : Enabled
802.11ax parameters
    OFDMA Downlink                             : Enabled
    OFDMA Uplink                               : Enabled
    MU-MIMO Downlink                           : Enabled
    MU-MIMO Uplink                             : Enabled
    BSS Color                                  : Enabled
    Partial BSS Color                          : Enabled
    BSS Color Code                             : 0
    BSS Target Wake Up Time                    : Enabled
    BSS Target Wake Up Time Broadcast Support  : Enabled
mDNS Gateway Status                            : Bridge
WIFI Alliance Agile Multiband      : Enabled
```

To view the non-operational or non-preferred channels, use the following command:

```
Device# show wireless client mac-address 3413.e8b5.f252 detail
Client MAC Address : 3413.e8b5.f252
Client IPv4 Address : 192.165.1.53
Client IPv6 Addresses : fe80::98bb:ea89:f016:3332
Client Username: N/A
AP MAC Address : 00ee.ab18.d920
AP Name: ssap-pp
AP slot : 1
Client State : Associated
Policy Profile : prof
Flex Profile : N/A
Wireless LAN Id: 1
WLAN Profile Name: mbo_1
```

```
Wireless LAN Network Name (SSID): mbo_1
BSSID : 00ee.ab18.d92f
Connected For : 25 seconds
Protocol : 802.11ax - 5 GHz
Channel : 36
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Session Timeout : 1800 sec (Remaining time: 1779 sec)
Session Warning Time : Timer not running
Input Policy Name  : None
Input Policy State : None
Input Policy Source : None
Output Policy Name  : None
Output Policy State : None
Output Policy Source : None
WMM Support : Enabled
U-APSD Support : Enabled
  U-APSD value : 0
  APSD ACs    : BK, BE, VI, VO
Fastlane Support : Disabled
Client Active State : Active
Power Save : OFF
Current Rate : 1.5
Supported Rates : 9.0,18.0,36.0,48.0,54.0
Mobility:
  Move Count                  : 0
  Mobility Role               : Local
  Mobility Roam Type          : None
  Mobility Complete Timestamp : 05/15/2019 16:03:34 IST
Client Join Time:
  Join Time Of Client : 05/15/2019 16:03:34 IST
Policy Manager State: Run
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 26 seconds
Policy Type : N/A
Encryption Cipher : None
User Personal Network    : Disabled
Encrypted Traffic Analytics : No
Protected Management Frame - 802.11w : No
EAP Type : Not Applicable
VLAN : default
Multicast VLAN : 0
WFD capable : No
Managed WFD capable : No
Cross Connection capable : No
Support Concurrent Operation : No
Session Manager:
  Point of Attachment : capwap_90400001
  IIF ID             : 0x90400001
  Authorized         : TRUE
  Session timeout    : 1800
  Common Session ID: 000000000000000BB92939C5
  Acct Session ID  : 0x00000000
  Last Tried Aaa Server Details:
  Server IP :
  Auth Method Status List
  Method : None
  Local Policies:
  Service Template : wlan_svc_prof_local (priority 254)
  VLAN             : 165
  Absolute-Timer   : 1800
  Server Policies:
  Resultant Policies:
    VLAN Name         : VLAN0165
    VLAN             : 165
    Absolute-Timer   : 1800
  DNS Snooped IPv4 Addresses : None
  DNS Snooped IPv6 Addresses : None
  Client Capabilities
    CF Pollable : Not implemented
    CF Poll Request : Not implemented
    Short Preamble : Not implemented
    PBCC : Not implemented
    Channel Agility : Not implemented
    Listen Interval : 0
  Fast BSS Transition Details :
    Reassociation Timeout : 0
  11v BSS Transition : Implemented
  11v DMS Capable : No
  QoS Map Capable : Yes
  Non-Preferred Channels : 40
  Non-Operable Channels : 56
  FlexConnect Data Switching : N/A
  FlexConnect Dhcp Status : N/A
  FlexConnect Authentication : N/A
  FlexConnect Central Association : N/A
  Client Statistics:
    Number of Bytes Received : 0
    Number of Bytes Sent : 0
    Number of Packets Received : 0
    Number of Packets Sent : 0
    Number of Policy Errors : 0
    Radio Signal Strength Indicator : -34 dBm
    Signal to Noise Ratio : 56 dB
  Fabric status : Disabled
  Client Scan Reports
  Assisted Roaming Neighbor List
  Nearby AP Statistics:
  EoGRE : No/Simple client
```