Wi-Fi Accessory Configuration Specification

Release R2

Developer

Contents

1. Introduction

1.1. Objective

This specification details requirements and recommendations for Wi-Fi Accessory Configuration accessories and related features.

This specification is an extension of the *Accessory Interface Specification*, therefore all requirements in that specification must be met. Chapters in this specification supersede chapters found in the *Accessory Interface Specification*.

Any conflicts between the *Accessory Interface Specification* and this specification must be resolved in favor of this specification.

1.2. Requirements, recommendations, and permissions

This specification contains statements that are incorporated by reference into legal agreements between Apple and its Licensees. The use of the words *must, must not, required, shall, shall not, should, should not, recommended, not recommended, may, optional,* and *deprecated* in a statement have the following meanings:

- *Must, shall*, or *required* means the statement is an absolute requirement.
- *Must not, shall not,* or *prohibited* means the statement is an absolute prohibition.
- *Should* or *recommended* means the full implications must be understood before choosing a different course.
- *Should not* or *not recommended* means the full implications must be understood before choosing this course.
- *May* or *optional* means the statement is truly optional, and its presence or absence cannot be assumed.
- *Deprecated* means the statement is provided for historical purposes only and is equivalent to "must not."

The absence of requirements, recommendations, or permissions for a specific accessory design in this specification must not be interpreted as implied approval of that design. Licensee is strongly encouraged to ask Apple for feedback on accessory designs that are not explicitly mentioned in this specification.

1.3. Terminology

1.3.1 Device

Device and *iOS device* refer to an iPhone, iPad, or iPod running iOS.

Where appropriate, specific Apple product and operating system references will also be used.

1.3.2 Accessory

Accessory refers to any product that connects to a *device* via the interfaces described in this specification.

2. Wi-Fi Accessory Configuration

2.1 Overview

Apple's Wi-Fi Accessory Configuration feature is designed to allow consumers to easily set up their wireless accessories with the network credentials already stored on their device.

With a Wi-Fi Accessory Configuration-enabled accessory, users can:

- Wirelessly discover their configurable accessory.
- Give their accessory a descriptive name.
- Pass network credentials to the accessory so it may join an infrastructure network.
- Discover applications compatible with the accessory.

2.2 Wi-Fi Accessory Configuration Requirements

The following requirements apply to all accessories that support this feature.

The Wi-Fi Accessory Configuration feature is available on devices running iOS 7.0 or later, tvOS 10.2 or later, or macOS 12.5.1 Monterey or later with AirPort Utility 6.3.9 or later. Wi-Fi Accessory Configuration requires a Wi-Fi network that supports 802.11b/g, 802.11n, or 802.11ac. Wi-Fi Accessory Configuration accessories must include an 802.11b/g, 802.11n, or 802.11ac radio module and a status indicator to indicate when the accessory is in Wi-Fi Accessory Configuration mode. Apple recommends that this status indicator only be used for indicating when the accessory is in Wi-Fi Accessory Configuration mode, and not be used for any other purpose. The accessory must support the ability for the user to manually enter Wi-Fi Accessory Configuration mode as well as perform a factory reset of the accessory. All user-specific information must be erased when performing a factory reset. This includes, but is not limited to:

- Passwords and authentication tokens (e.g. music service provider credentials, etc.).
- Medical data.
- Financial records.
- Personally identifiable information.

The accessory must be able to act as both a software Access Point (AP) and as a station (STA) device. Apple recommends that the accessory not use proprietary wireless technologies in the product that overlap with the international Wi-Fi spectrum.

2.2.1 Wi-Fi Accessory Configuration Accessory Behavioral Requirements

All Wi-Fi Accessory Configuration accessories must meet the following behavioral requirements:

- The accessory must automatically enter Wi-Fi Accessory Configuration mode when it is in a non-configured state.
- The accessory must exit Wi-Fi Accessory Configuration mode when it has been idle for more than 15 minutes.
- The accessory may offer a mechanism for exiting Wi-Fi Accessory Configuration mode in response to a direct user action.
- The software Access Point (AP) must use a unique SSID when entering Wi-Fi Accessory Configuration mode.
- The accessory must enter a non-configured state when the accessory's network credentials have been reset to factory setting.
- Configured accessories must not enter Wi-Fi Accessory Configuration mode automatically upon disconnecting from a network.
- Accessories should support alternative methods of configuration for devices that do not support the Wi-Fi Accessory Configuration feature.

Accessories that implement Wi-Fi Accessory Configuration functionality will not show up on the device as an Access Point (AP). Specifically, these accessories will not be able to offer AP-based features to the device. These features may include web interface-based features (such as firmware upgrade).

If the accessory wishes to offer support to iOS and macOS for these features while not connected to an infrastructure network, it should provide a mechanism for exiting Wi-Fi Accessory Configuration mode and entering a AP mode.

2.2.2 Wi-Fi Accessory Configuration Network Requirements

All Wi-Fi Accessory Configuration accessories must support a wireless network connection and Bonjour, Apple's service discovery protocol. Accessories must also support changing the Bonjour name to a user defined value. The default name of all accessories must be unique out of the box.

When in Software AP mode, the accessory must have a DHCP server as well as an HTTP server that supports persistent connections, i.e. multiple HTTP requests sent through the came TCP connection. When in STA mode, the accessory must support link-local IPv4 addressing as specified in RFC 3927.

2.2.3 Wi-Fi Accessory Configuration Implementation Requirements

All Wi-Fi Accessory Configuration accessories must meet all applicable requirements in this specification and must incorporate the Apple Authentication Coprocessor, see *Apple Authentication 3.0 Coprocessor* in the *Accessory Interface Specification*.

2.2.4 Wi-Fi Certification Requirements

Wi-Fi Accessory Configuration accessories must complete the following certification requirements:

- Wi-Fi CERTIFIED™ (http://www.wi-fi.org/certification)
- MFi certification (https://mfi.apple.com/)

Note: Pre-existing MFi certification on an accessory is not sufficient for Wi-Fi Accessory Configuration accessory certification.

2.3 Wi-Fi Accessory Configuration Setup Experience

The configuration process allows a device to send configuration information and network credentials to the accessory. This may include joining a Wi-Fi network, specifying a friendly name for the accessory, etc. The general flow of operation is:

1. Device discovers accessories. Wi-Fi scans are conducted to find non-configured accessories broadcasting the Apple information element (IE) in the accessory's software access point Wi-Fi beacon frames.
2. Device joins accessory's temporary software access point network.
3. Device searches for accessory via Bonjour. The device browses for `_mfi-config._tcp` and matches the accessory by its Device ID. The Device ID in the Bonjour TXT record is the same one advertised as part of the Device IE.
4. Device resolves via Bonjour and connects via TCP to accessory. This performs normal Bonjour PTR -> SRV -> A/AAAA resolving then connects via TCP.
5. Device authenticates accessory. For MFi-certified accessories, this performs MFi-SAP using the Apple Authentication Coprocessor.
6. Device builds config TLVs, encrypts it, and sends it in an HTTP request to accessory at /config. The TLV contains the information needed by the accessory to configure itself. See Table 2-1.
7. Accessory receives, validates, and saves config request. The accessory must not immediately apply the new configuration. Applying it at this point may interrupt its connection to the controller. The accessory must send its response, disable the sending side of its socket to signal it is done sending, then wait until it receives a FIN from the device (i.e. socket receive returns 0).
8. Device receives accessory response and waits for the accessory to close its connection. The controller must disable the sending side of its socket to signal it has received the response then waits until it receives a FIN from the accessory (i.e. socket receive returns 0).
9. Accessory waits for controller to disconnect then deregisters its Bonjour service and increments its config seed ID.
10. Accessory applies configuration and joins new Wi-Fi network. The accessory must wait until it has fully joined the new Wi-Fi network before continuing to the next step.
11. Accessory re-registers with Bonjour with the new config seed. It is important to only advertise the new configuration seed after the configuration has completed and the accessory has joined the new network. Otherwise, the controller may find a stale instance of the service and prematurely assume success.

12. Device re-joins its original Wi-Fi network.
13. Device searches for accessory via Bonjour. The controller browses for `_mfi-config._tcp` and matches the accessory by its Device ID (same one saved off from the earlier step).
14. Device sends an HTTP request to /configured on the accessory to indicate configuration is complete.
15. Device reports success (or failure) to user.
16. Device prompts user to discover an application for the configured accessory if available.

Table 2-1 Configuration TLVs

Name	ID	Type	Description
bundleSeedID	0x01	String	Unique 10 character string assigned by Apple to an app via the Provisioning Portal (e.g. 24D4XFAF43).
firmwareRevision	0x02	String	Firmware revision of the accessory.
hardwareRevision	0x03	String	Hardware revision of the accessory.
language	0x04	String	BCP-47 language to configure the accessory for. See http://www.iana.org/assignments/language-subtag-registry.
manufacturer	0x05	String	Manufacturer of the accessory (e.g. Apple).
mfiProtocol	0x06	String	Reverse-DNS string describing supported MFi accessory protocols (e.g. com.acme.gadget) for accompanying applications. Note: there may be more than one of this item if multiple protocols are supported.
model	0x07	String	Model name of the accessory (e.g. Accessory1,1).
name	0x08	String	Name that accessory should use to advertise itself to the user.
playPassword	0x09	String	Password used to start an AirPlay stream to the accessory.
serialNumber	0x0A	String	Serial number of the accessory.
wifiPSK	0x0B	Data	Wi-Fi PSK for joining a WPA-protected Wi-Fi network. If it is between 8 and 63 bytes each being 32-126 decimal, inclusive then it is a pre-hashed password. Otherwise, it is expected to be a pre-hashed, 256-bit pre-shared key.
wifiSSID	0x0C	String	Wi-Fi SSID (network name) for the accessory to join. This should be UTF-8.

2.4 Bonjour

The Bonjour service type for Wi-Fi Accessory Configuration is `_mfi-config._tcp`. The name of the Bonjour service is the user-visible name of the accessory (e.g. "Basement Thermostat"). The name may contain any Unicode character and is encoded using UTF-8. It has a maximum length of 63 bytes (which may be fewer than 63 characters as a single Unicode character may require multiple bytes). Additional data needed for discovery-time metadata is advertised via a TXT record. This contains fields for feature detection, versions, etc.

Table 2-2 `_mfi-config._tcp` TXT record keys

Key	Description
deviceid	Globally unique ID for the accessory (e.g. the primary MAC address, such as 00:11:22:33:44:55).
features	Feature flag bits (e.g. 0x3 for bits 0 and 1). See Table 2-3.
flags	Status flags (e.g. 0x04 for bit 3). See Table 2-4.
protovers	Protocol version string <major>.<minor> (e.g. 1.0). Missing means 1.0.
seed	Configuration seed number. This is 0-255 and updates each time the software configuration changes.
srcvers	Source version number. Populated directly by the source code. Valid version numbers are 1.14, 1.20 and 1.22.

Table 2-3 MFi Configuration Feature Flags

Value	Bit	Description
0x00000001	0	App associated with the accessory.
0x00000004	2	Accessory supports TLV-based configuration.

Table 2-4 MFi Configuration Status Flag

Value	Bit	Description
0x01	0	Problem has been detected.
0x02	1	Accessory is not configured.

2.5 Apple Device Information Element (IE)

2.5.1 General Usage

This IE must be included in the following 802.11 management frames:

- Probe response frames.
- Beacon frames, if applicable.

2.5.2 Structure

This section defines a vendor-specific 802.11 IE using the OUI 00-A0-40 (registered to Apple Inc.). The payload portion of the IE is composed of sub-IEs defined by this document.

Table 2-5 Apple Device IE overall structure

Name	Size	Value	Description
Element ID	1	0xDD	Vendor-specific element ID as specified in Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11 - 2007.
Length	1	Variable	Number of bytes in IE (excludes element ID and length bytes).
OUI	3	0x00 0xA0 0x40	Apple Inc. OUI reserved for this IE.
Sub-type	1	0x00	Sub-type of the 00-A0-40 Apple Inc. OUI.
Elements:	Variable	Variable	Sub IE elements defined by this specification.

Table 2-6 Apple Device IE element structure

Name	Size	Description
Element ID	1	Vendor specific element ID as specified in Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11 - 2007.
Length	1	Number of bytes in the element payload (excludes element ID and length bytes).
Payload	Variable	Payload defined by the element ID.

2.5.3 Payload

Table 2-7 Apple Device IE elements

Element ID	Name	Format	Description
0x00	Flags	n:bits	Flags about the accessory: b0-b7, b8-b15, etc. See Table 2-8. Each flag is a bit. Bit numbering starts from the leftmost bit of the first byte and uses the minimum number of bytes needed to encode the bits. For example: If only bit 1 is set, it would be 0x40. If bit 1 (0x40) and bit 7 (0x01) are set, it would be 0x41. If bit 1 (0x40), bit 7 (0x01), and bit 10 (0x0020) are set, it would be 0x41, 0x20. If only bit 10 (0x0020), it would be 0x00, 0x20.
0x01	Name	UTF-8	Friendly name of the accessory. This should only be provided if the user configured a custom name or the firmware of the accessory has reason to believe it can provide a name that is better than the default name the client software will provide for it based on the model. Due to localization issues, it often better to only provide this element if the user has configured a name.
0x02	Manufacturer	UTF-8	Machine-parsable manufacturer of the accessory (e.g. "Manufacturer").
0x03	Model	UTF-8	Machine-parsable model of the accessory (e.g. "AB1234").
0x04	OUI	3 bytes	OUI of the accessory including this IE. (e.g. 0x00 0xA0 0x40)
0x05			Reserved.
0x06	Bluetooth MAC	6 bytes	MAC address of the Bluetooth radio, if applicable.
0x07	Device ID	6 bytes	Globally unique ID for the accessory (e.g. the primary MAC address, such as 00:11:22:33:44:55). This should be the primary MAC address of the device. If the device has multiple MAC addresses, one must be chosen as the primary MAC address such that it never changes (e.g. does not depend on the network interface currently active). The main purpose of this element is to allow devices to discover the accessory via Wi-Fi scans and then later associate it with an IP-based discovery method, such as Bonjour (where the Device ID is expected to be reported via the TXT record).
0x08-0xFF			Reserved.
0xDD	Vendor-specific	n bytes	Same format as a normal vendor-specific IE element.

Table 2-8 Flags

Value	Bit	Description
0x80	0	Supports AirPlay.
0x40	1	Accessory is not configured.
0x20	2	Supports MFi Configuration v1.
0x10	3	Reserved.
0x08	4	Reserved.
0x04	5	Reserved.
0x02	6	Supports WPS.
0x01	7	WPS is active on the accessory.
0x0080	8	Supports AirPrint.
0x0040	9	Reserved.
0x0020	10	Reserved.
0x0010	1	Provides Internet access (e.g. cellular connectivity is supported, provisioned, and enabled).
0x0008	12	Reserved.
0x0004	13	Reserved.
0x0002	14	Supports 2.4 GHz Wi-Fi networks.
0x0001	15	Supports 5 GHz Wi-Fi networks.
0x000080	16	Reserved.
0x000040	17	Reserved. Legacy support for HomeKit Accessory Protocol v1.
0x000008	20	Reserved. Legacy support for HomeKit Wi-Fi Accessory Configuration.
0x000004	21	Uses an Apple Authentication Coprocessor 2.0C or Apple Authentication 3.0 Coprocessor.
0x000002	22	Reserved. Legacy HomeKit software token based authentication.
0x000001	23	Reserved.

2.6 Accessory Compliance Test Plan

The purpose of this test plan is to specify the testing that vendors must perform to verify that their products conform to the Wi-Fi Accessory Configuration specification provided by Apple Inc. Wi-Fi Accessory Association Verification Tests describes tests that must be run and successfully completed for all Wi-Fi Accessory Configuration enabled products.

Table 2-9 Terms And Definitions

Term	Definition
IE	Information Element.
AP	Access Point.
AU	AirPort Utility.
STA	Non-AP 802.11 station.
BSSID	Basic Service Set Identifier.
SSID	Service Set Identifier.
MAC	Media Access Control.
BSS	Basic Service Set.
ESS	Extended Service Set.
DS	Distribution System.
DUT	Device Under Test.
URL	Uniform Resource Locator.
PHY	Physical Layer (802.11a, b, g, n).
OOB	Out of the Box.

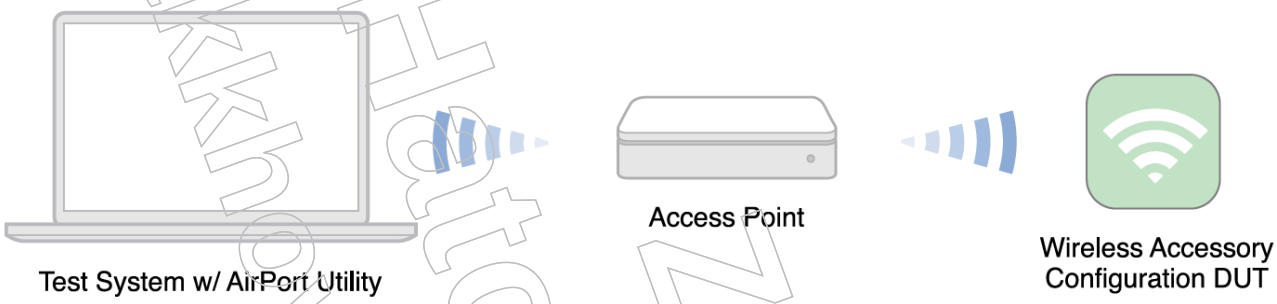
Wi-Fi Accessory Configuration enabled DUTs will be tested on any and all wireless network interfaces that allow for Wi-Fi Accessory Configuration.

The following are minimum requirements to complete the test suites that are included in this test plan.

- MacBook Pro running macOS 12.5.1 Monterey or later
- One of the following:
  - Apple AirPort Extreme 802.11n (5th Generation) Base Station running 7.9.1 or later
  - Apple AirPort Express 802.11n (3rd Generation) Base Station running 7.8.1 or later
  - Apple AirPort Utility 6.3.9 or later
  - Wi-Fi access point with Multicast DNS (eg. TP-Link)

The following test beds are designed and specified for each test case in this test plan. The minimum requirement for every test bed is a macOS computer running the latest version of AirPort Utility (Test System) and a simultaneous dual band Apple Base Station running the latest firmware (Access Point).

Figure 2-1 Test bed



The following test cases must be completed successfully to ensure compliance with the Wi-Fi Accessory Configuration specification and interoperability with Apple Base Station product lines. While it is possible to implement Wi-Fi Accessory Configuration without an Apple Base Station, all tests will be done with an Apple Base Station (AirPort Extreme or Time Capsule) product because certain features of the Base Station are required to complete all of the testing.

Network connectivity is a requirement for Wi-Fi Accessory Configuration. Each DUT must, at minimum, support 802.11g. All supported PHYs must be tested.

2.6.1 Wi-Fi Accessory Association Verification Tests

Wi-Fi Accessory Configuration enabled DUTs have two options of how to be configured based on whether there is an interface that allows for the SSID and security modes to be configured. Only run the test that applies to your DUT. The following tests assume the accessory has had no configuration done to the DUT and is still in its factory default state.

2.6.1.1 Wi-Fi Accessory Configuration Mode Automatic Shutoff

For the Test Environment, see Figure 2-1

1. Power on the DUT.
2. Wait for DUT to complete booting.
3. The DUT should begin beaconing 802.11 beacons including the Device IE indicating it is non-configured and advertising as an 802.11 network with an SSID that is descriptive of the DUT. At minimum the indication of the manufacturer should be present, with no security enabled.
4. The product mode indicator must show that the accessory is in WAC mode or else FAIL.
5. The DUT must show up in the AirPort Utility under "Other Wi-Fi Devices" as a "New Wi-Fi Device" indicating it is a non-configured accessory or else FAIL.
6. Do not interact with the DUT for at least 15 minutes.
7. The DUT should come out of WAC mode and stop beaconing the Device IE indicating it is non-configured.
8. The product mode indicator must show that the accessory is not in WAC mode or else FAIL.
9. Power down the DUT.
10. Power on the DUT.
11. Wait for DUT to complete booting.
12. The DUT should begin beaconing 802.11 beacons including the Device IE indicating it is non-configured and advertising as an 802.11 network with an SSID that is descriptive of the DUT. At minimum the indication of the manufacturer should be present, with no security enabled.
13. The product mode indicator must show that the accessory is in WAC mode or else FAIL.
14. The DUT must show up in the AirPort Utility under "Other Wi-Fi Devices" as a "New Wi-Fi Device" indicating it is a non-configured accessory or else FAIL.

2.6.1.2 802.11b/g Association Verification

For the Test Environment, see Figure 2-1.

If the DUT supports 802.11b/g the following test must be run.

1. Power on the Base Station and connect to it via the Apple AirPort Utility. In the AirPort Utility select "Manual Setup".
2. On the bar across the top of the AirPort Utility, select "Wireless"
3. Set Base Station to Network Mode "Create a wireless network".
4. Under the Section that says "Wireless Network Name:" change it to "Soundwave24€".
5. Under the section that says "Wireless Security:" change it to "None"
6. Click "Wireless Options".

7. Check the box that says "5 GHz Network Name" and the box should be come editable. Change the name to "Soundwave5".
8. Then under the "Radio Mode:" pull down menu select, 802.11a - 802.11b/g.
9. Then click save on the AirPort Utility. The AirPort Utility may prompt for various errors and all of them can be ignored. Be sure to click "Update" and wait for the Base Station to reboot.
10. Power on the DUT. Wait for DUT to complete booting. Note the MAC address of the DUT.
11. The DUT should begin beaconing 802.11 beacons including the Device IE indicating it is non-configured and advertising as an 802.11 network with an SSID that is descriptive of the DUT. At minimum the indication of the manufacturer should be present, with no security enabled.
12. The product mode indicator must show that the accessory is in WAC mode or else FAIL.
13. The DUT must show up in the AirPort Utility under "Other Wi-Fi Devices" as a "New Wi-Fi Device" indicating it is a non-configured accessory or else FAIL.
14. Select the DUT in the AirPort Utility.
15. Set the DUT's Wi-Fi Network to "Soundwave24€".
16. Give the DUT the Accessory Name "WAC DUT".
17. Click next in the AirPort Utility.
18. Verify that a setup complete message is displayed.
19. If any error messages are displayed, FAIL.
20. Wait for DUT to complete booting and indicate that it has joined a network.
21. If DUT does not join the network, FAIL.
22. Using the AirPort Utility verify the DUT has joined the network.
23. In the AirPort Utility, select the Base Station. Verify that the DUT is present as a wireless client with the Accessory Name "WAC DUT".
24. If the DUT is not present or if the MAC address is not present, FAIL.
25. Manually put the DUT into Wi-Fi Accessory Configuration mode according to the accessory's instructions.
26. The DUT should begin beaconing 802.11 beacons including the Device IE indicating it is non-configured and advertising as an 802.11 network with an SSID that is descriptive of the DUT. At minimum the indication of the manufacturer should be present, with no security enabled.
27. The product mode indicator must show that the accessory is in WAC mode or else FAIL.
28. The DUT must show up in the AirPort Utility under "Other Wi-Fi Devices" as a "New Wi-Fi Device" indicating it is a non-configured accessory or else FAIL.

2.6.1.3 802.11 Non-broadcast SSID Association Verification

For the Test Environment, see Figure 2-1.

1. Power on the Base Station and connect to it via the Apple AirPort Utility. In the AirPort Utility select "Manual Setup".
2. On the bar across the top of the AirPort Utility, select "Wireless"
3. Set Base Station to Network Mode "Create a wireless network".
4. Under the Section that says "Wireless Network Name:" change it to "Soundwave24€".
5. Under the section that says "Wireless Security:" change it to "None"
6. Click "Wireless Options".
7. Check the box that says "5 GHz Network Name" and the box should be come editable. Change the name to "Soundwave5".
8. Check the box "Create hidden network".
9. Then click save on the AirPort Utility. The AirPort Utility may prompt for various errors and all of them can be ignored. Be sure to click "Update" and wait for the Base Station to reboot.
10. Join the hidden network "Soundwave24€" from the Test System.
11. Power on the DUT. Wait for DUT to complete booting. Note the MAC address of the DUT.
12. The product mode indicator must show that the accessory is in WAC mode or else FAIL.
13. The DUT must show up in the AirPort Utility under "Other Wi-Fi Devices" as a "New Wi-Fi Device" indicating it is a non-configured accessory or else FAIL.
14. Select the DUT in the AirPort Utility.
15. Set the DUT's Wi-Fi Network to "Soundwave24€".
16. Give the DUT the Accessory Name "WAC DUT".
17. Click next in the AirPort Utility.
18. Verify that a setup complete message is displayed.
19. If any error messages are displayed, FAIL.
20. Wait for DUT to complete booting and indicate that it has joined a network.
21. If DUT does not join the network, FAIL.
22. Using the AirPort Utility verify the DUT has joined the network.
23. In the AirPort Utility, select the Base Station. Verify that the DUT is present as a wireless client with the Accessory Name "WAC DUT".
24. If the DUT is not present or if the MAC address is not present, FAIL.

2.6.2 2.4 GHz vs 5 GHz Beaconing Tests

For the Test Environment, see Figure 2-1.

If the DUT supports 802.11 2.4 GHz but not 5 GHz the following test must be run.

1. Power on the Base Station and connect to it via the Apple AirPort Utility. In the AirPort Utility select "Manual Setup".
2. On the bar across the top of the AirPort Utility, select "Wireless"
3. Set Base Station to Network Mode "Create a wireless network".
4. Under the Section that says "Wireless Network Name:" change it to "Soundwave24€".
5. Under the section that says "Wireless Security:" change it to "None"
6. Click "Wireless Options".
7. Check the box that says "5 GHz Network Name" and the box should be come editable. Change the name to "Soundwave5".
8. Then click save on the AirPort Utility. The AirPort Utility may prompt for various errors and all of them can be ignored. Be sure to click "Update" and wait for the Base Station to reboot.
9. Power on the DUT. Wait for DUT to complete booting. Note the MAC address of the DUT.
10. The DUT should begin beaconing 802.11 beacons including the Device IE indicating it is non-configured and advertising as an 802.11 network with an SSID that is descriptive of the DUT. At minimum the indication of the manufacturer should be present, with no security enabled.
11. The product mode indicator must show that the accessory is in WAC mode or else FAIL.
12. The DUT must show up in the AirPort Utility under "Other Wi-Fi Devices" as a "New Wi-Fi Device" indicating it is a non-configured accessory or else FAIL.
13. Select the DUT in the AirPort Utility.
14. Open the list to set the DUT's Wi-Fi Network.
15. Verify that "Soundwave24€" is displayed in the dropdown list of networks in the WAC configuration dialog window.
16. If not displayed, FAIL.
17. Verify that "Soundwave5" is NOT displayed in the list.
18. If displayed, FAIL.

2.6.3 Security Mode Verification Tests for WPA2 Personal

All Wi-Fi Accessory Configuration enabled DUTs must support no security (None) and WPA2 Personal at minimum. Other security modes are supported by the Apple Base Station and other 3rd party AP products however only those two will be tested.

For the Test Environment, see Figure 2-1.

1. Power on the Base Station and connect to it via the Apple AirPort Utility. In the AirPort Utility select "Manual Setup".
2. On the bar across the top of the AirPort Utility, select "Wireless"
3. Set Base Station to Network Mode "Create a wireless network".
4. Under the Section that says "Wireless Network Name:" change it to "Soundwave24€".
5. Under the section that says "Wireless Security:" change it to "WPA/WPA2 Personal"
6. Click "Wireless Options".
7. Check the box that says "5 GHz Network Name" and the box should be come editable. Change the name to "Soundwave5".
8. Then under the "Radio Mode:" pull down menu select, 802.11a/n - 802.11b/g/n.
9. Then click save on the AirPort Utility. The AirPort Utility may prompt for various errors and all of them can be ignored. Be sure to click "Update" and wait for the Base Station to reboot.
10. Power on the DUT. Wait for DUT to complete booting. Note the MAC address of the DUT.
11. The DUT should begin beaconing 802.11 beacons including the Device IE indicating it is non-configured and advertising as an 802.11 network with an SSID that is descriptive of the DUT. At minimum the indication of the manufacturer should be present, with no security enabled.
12. The product mode indicator must show that the accessory is in WAC mode or else FAIL.
13. The DUT must show up in the AirPort Utility under "Other Wi-Fi Devices" as a "New Wi-Fi Device" indicating it is a non-configured accessory or else FAIL.
14. Select the DUT in the AirPort Utility.
15. Set the DUT's Wi-Fi Network to "Soundwave24€".
16. Give the DUT the Accessory Name "WAC DUT".
17. Click next in the AirPort Utility.
18. Verify that a setup complete message is displayed.
19. If any error messages are displayed, FAIL.
20. Wait for DUT to complete booting and indicate that it has joined a network.
21. If DUT does not join the network, FAIL.
22. Using the AirPort Utility verify the DUT has joined the network.
23. In the AirPort Utility, select the Base Station. Verify that the DUT is present as a wireless client with the Accessory Name "WAC DUT".
24. If the DUT is not present or if the MAC address is not present, FAIL.

2.6.4 IP Connectivity Tests

IP connectivity is required for all Wi-Fi Accessory Configuration enabled accessories, with a minimum of IPv4 with a DHCP client to be implemented. It is additionally required that Link Local addressing and configuration is allowed on IPv4 stack.

2.6.4.1 IPv4 DHCP

For the Test Environment, see Figure 2-1.

1. Power on the Base Station and connect to it via the Apple AirPort Utility. In the AirPort Utility select "Manual Setup".
2. On the bar across the top of the AirPort Utility, select "Wireless"
3. Set Base Station to Network Mode "Create a wireless network".
4. Under the Section that says "Wireless Network Name:" change it to "Soundwave24€".
5. Under the section that says "Wireless Security:" change it to "None"
6. Click "Wireless Options".
7. Check the box that says "5 GHz Network Name" and the box should be come editable. Change the name to "Soundwave5".
8. Then under the "Radio Mode:" pull down menu select, 802.11a/n - 802.11b/g/n.
9. Then click save on the AirPort Utility. The AirPort Utility may prompt for various errors and all of them can be ignored. Be sure to click "Update" and wait for the Base Station to reboot.
10. Power on the DUT. Wait for DUT to complete booting. Note the MAC address of the DUT.
11. The DUT should begin beaconing 802.11 beacons including the Device IE indicating it is non-configured and advertising as an 802.11 network with an SSID that is descriptive of the DUT. At minimum the indication of the manufacturer should be present, with no security enabled.
12. The product mode indicator must show that the accessory is in WAC mode or else FAIL.
13. The DUT must show up in the AirPort Utility under "Other Wi-Fi Devices" as a "New Wi-Fi Device" indicating it is a non-configured accessory or else FAIL.
14. Select the DUT in the AirPort Utility.
15. Set the DUT's Wi-Fi Network to "Soundwave24€".
16. Give the DUT the Accessory Name "WAC DUT".
17. Click next in the AirPort Utility.
18. Verify that a setup complete message is displayed.
19. If any error messages are displayed, FAIL.
20. Wait for DUT to complete booting and indicate that it has joined a network.
21. If DUT does not join the network, FAIL.
22. Using the AirPort Utility verify the DUT has joined the network.

23. In the AirPort Utility, select the Base Station. Verify that the DUT is present as a wireless client with the Accessory Name "WAC DUT". Take note of the DUT's IP Address.
24. If the DUT is not present or if the MAC address is not present, FAIL.
25. On the Test Machine connected to the Base Station ping the IP address that was just noted.
26. If all the pings are successful, then PASS, else FAIL.
27. Reboot the DUT and wait for it to come back up.
28. Once connected to the network, open the AirPort, select the Base Station. Verify that the DUT is present as a wireless client with the Accessory Name "WAC DUT". Take note of the DUT's IP Address.
29. If the DUT is not present or if the MAC address is not present, FAIL.
30. On the Test Machine connected to the Base Station ping the IP address that was just noted.
31. If all the pings are successful, then PASS, else FAIL.

2.6.4.2 IPv4 Link Local

For the Test Environment, see Figure 2-1.

1. Power on the Base Station and connect to it via the Apple AirPort Utility. In the AirPort Utility select "Manual Setup".
2. On the bar across the top of the AirPort Utility, select "Network".
3. Under the section that says "Router Mode:" change it to "Off (Bridge Mode)" and ensure that there is no Wide Area Network attached to the Base Station.
4. On the bar across the top of the AirPort Utility, select "Wireless"
5. Set Base Station to Network Mode "Create a wireless network".
6. Under the Section that says "Wireless Network Name:" change it to "Soundwave24€".
7. Under the section that says "Wireless Security:" change it to "None"
8. Click "Wireless Options".
9. Check the box that says "5 GHz Network Name" and the box should be come editable. Change the name to "Soundwave5".
10. Then under the "Radio Mode:" pull down menu select, 802.11a/n - 802.11b/g/n.
11. Then click save on the AirPort Utility. The AirPort Utility may prompt for various errors and all of them can be ignored. Be sure to click "Update" and wait for the Base Station to reboot.
12. Power on the DUT. Wait for DUT to complete booting. Note the MAC address of the DUT.
13. The DUT should begin beaconing 802.11 beacons including the Device IE indicating it is non-configured and advertising as an 802.11 network with an SSID that is descriptive of the DUT. At minimum the indication of the manufacturer should be present, with no security enabled.
14. The product mode indicator must show that the accessory is in WAC mode or else FAIL.

15. The DUT must show up in the AirPort Utility under "Other Wi-Fi Devices" as a "New Wi-Fi Device" indicating it is a non-configured accessory or else FAIL.
16. Select the DUT in the AirPort Utility.
17. Set the DUT's Wi-Fi Network to "Soundwave24€".
18. Give the DUT the Accessory Name "WAC DUT".
19. Click next in the AirPort Utility.
20. Verify that a setup complete message is displayed.
21. If any error messages are displayed, FAIL.
22. Wait for DUT to complete booting and indicate that it has joined a network.
23. If DUT does not join the network, FAIL.
24. Using the AirPort Utility verify the DUT has joined the network.
25. In the AirPort Utility, select the Base Station. Verify that the DUT is present as a wireless client with the Accessory Name "WAC DUT". Take note of the DUT's MAC Address and IP Address.
26. If the DUT is not present or if the MAC address is not present, FAIL.
27. On the Test Machine connected to the Base Station ping the IP address that was just noted using ping6.
28. If all the pings are successful, then PASS, else FAIL.
29. Reboot the DUT and wait for it to come back up.
30. Once connected to the network, open the AirPort, select the Base Station. Verify that the DUT is present as a wireless client with the Accessory Name "WAC DUT". Take note of the DUT's MAC Address and IP Address.
31. If the DUT is not present or if the MAC address is not present, FAIL.
32. From a Terminal window of the Test System connected to the Base Station enter:
    - `arp -a -i $INTERFACE`
    - where `$INTERFACE` is the identifier for your AirPort card
33. If all the MAC address associated with the DUT is present and the IP address displayed is of the format 169.254.XX.XX, then PASS, else FAIL.

2.6.5 Bonjour TXT Records Tests for ADD and RMV

If the DUT is not based on the Microchip Binary platform, the following test must be run. This test checks bonjour fields that contain information related to the POSIX Source release version numbers. The valid POSIX Source releases are:

- 1.14
- 1.20
- 1.22

For the Test Environment, see Figure 2-1.

1. Power on the DUT.
2. Wait for DUT to complete booting.
3. On the Test System, issue the following command in a Terminal and leave it running.

```
dns-sd -B _mfi-config
```

4. From a second Terminal window of the Test System enter:

```
networksetup -setairportnetwork $INTERFACE $SSID
```

5. Where `$INTERFACE` is the identifier for your AirPort card and `$SSID` is the DUT Network name.
6. A Bonjour record should appear with the following format:

Timestamp, A/R, Flags, if, Domain, Service Type, Instance Name

7. The A/R should have "Add" below it, if this is true, PASS.
8. The Service Type should have _mfi-config._tcp below it, if this is true, PASS.
9. The Instance should have "`$INSTANCENAME–` below it, which must be the Friendly Name of the DUT. If this is true, PASS.
10. From the Terminal of the Test System enter:
    - `dns-sd -L $INSTANCENAME _mfi-config local`
    - where `$INSTANCENAME` is collected earlier.
11. The Bonjour record needs to contain a minimum of the following TXT records (a value is specified that is the requirement for field):
    - deviceid=<MAC address>
    - features=<Feature flag bits>
    - seed=<Configuration seed number>
    - srcvers=<Source release version> See Bonjour TXT Records Tests for ADD and RMV for the list of valid POSIX Source release versions. (Populated by WAC source code.)
12. If all of the fields are present then PASS, else FAIL.

2.6.6 Certification Procedure

Accessory submission must be accompanied by proof of Wi-Fi Certification for the product.

Full product documentation must be provided in both printed and soft copy form (all customer facing documents such as user manuals and quick start guides).

Revision History

This chapter describes changes to the Accessory Interface Specification - Wi-Fi Accessory Configuration Addendum

from the previous revision.

- Revised macOS 12.5.1 Monterey and AirPort Utility to 6.3.9 to reflect current compatibility.

Apple Inc.

Apple Inc.
One Apple Park Way
Cupertino, CA 95014
408-996-1010