Wi-Fi Simple Configuration Protocol and Usability Best Practices for the Wi-Fi Protected Setup™ Program

Version 2.0.1
Wi-Fi Alliance®
April 2011

Revision History

Date	Version	Author	Summary of Changes
Dec 20, 2010	2.0.0	Kevin Robinson	Initial release for WSC 2.0
Apr 20, 2011	2.0.1	Giao Pham	Added sections 3.20 and 3.21

Table of Contents

1 Introduction

1.1 Purpose

The purpose of this document is to provide additional technical guidance and recommended best practices for specific features of the Wi-Fi Simple Configuration specification.

Although the guidelines mentioned in this document are not mandatory for Wi-Fi Protected Setup certification, their use will contribute towards enhancing the robustness and flexibility of Wi-Fi Simple Configuration implementations.

1.2 Scope

This document applies to Wi-Fi Simple Configuration implementations of Enrollees, Access Points and Registrars where applicable.

This document contains clarifications, guidelines, and recommendations for Wi-Fi Simple Configuration. These recommendations are not normative, and they do not supersede the generic protocol specification. For example, this document gives recommendations on interactions between Wi-Fi Simple Configuration and 802.1X/802.11 protocols that apply only to Wi-Fi Simple Configuration use.

1.3 Related Documents

Document	Date	Location
Wi-Fi Simple Configuration Specification v2.0.0	Dec 2010	WFA Website - Testing Information Page
Wi-Fi Alliance Brand Styleguide	Jun 2010	WFA Website

2 List of Acronyms and Definitions

AP	Access Point
CRC	Cyclic Redundancy Check
EAP	Extensible Authentication Protocol
GUI	Graphical User Interface
IE	Information Element
LED	Light Emitting Diode
Legacy Client	Client that does not support Wi-Fi Protected Setup
MODP	Modular Exponential
PBC	Push Button Configuration
PIN	Personal Identification Number
RSSI	Receive Signal Strength Indicator
SSID	Service Set Identifier
UI	User Interface
UUID	Universally Unique Identifier
WFA	Wi-Fi Alliance®
Wi-Fi Protected Setup™	Used to refer to the certification program and certified products
Wi-Fi Simple Configuration	Used to refer to the protocol certified in the Wi-Fi Protected Setup program
WLAN	Wireless LAN
WPA2™	Wi-Fi Protected Access® version 2
WSC	Wi-Fi Simple Configuration

3 Wi-Fi Simple Configuration Best Practices

3.1 Push Button Configuration

The Push Button Configuration requires the user to press a button on both the Enrollee and on the AP (or Registrar) within the two-minute interval called the Walk Time. The user can trigger this sequence from either the AP or the Enrollee. The recommended sequence for a typical Wi-Fi Simple Configuration Enrollee addition follows:

3.1.1 The user purchases a new WSC device and triggers an Enrollee addition with either a physical button press or an appropriate alternative option (e.g. a soft button on a display UI).

- Certified Wi-Fi Protected Setup Enrollees should clearly designate the Wi-Fi Protected Setup button, preferably using the Wi-Fi Protected Setup Identifier Mark(see Section 3.18).
- The device may conditionally present the WSC trigger sequence if WSC-capable APs are detected in the vicinity. Alternately, the Enrollee may allow a manual WSC connection with any AP in an 802.11 channel scan list in order to accommodate environments where interference from multiple APs on the same channel may reduce the ability for Enrollees to see WSC IEs.
- The user typically presses the button until the device WSC visual indicator activates, indicating a WSC session.
- The WSC visual indicator should change status less than one second from the time it is triggered by a button press.
- If capable, the device UI should next direct the user to trigger the AP's button.

3.1.2 The user triggers the WSC process with a button press on their WSC AP.

- Certified Wi-Fi Protected Setup APs should clearly designate the Wi-Fi Protected Setup button, preferably using the Wi-Fi Protected Setup Identifier Mark(see Section 3.18).
- The user should be able to trigger a WSC AP with a single simple button press. WSC ease-of-use will be drastically degraded if long vs. short or single vs. multiple button presses are required. The recommended maximum required press time should be less than two seconds.
- Push Buttons should not be dual-purposed (i.e. a button that activates more than one function on the device, depending on condition or length of button press). This is especially problematic if the alternative purpose of the button is to reset security or reset the device to factory defaults.

3.1.3 The user confirms the successful completion of the WSC sequence through the Enrollee's WSC visual indicator.

- When providing instructions, vendors should not assume the presence or behavior of any WSC visual indicators on other vendors' devices, as visual indicators may vary from vendor to vendor.
- The following recommended WSC visual indicator LED flashing frequencies make WSC In-Progress and WSC Error conditions more distinguishable to the user:

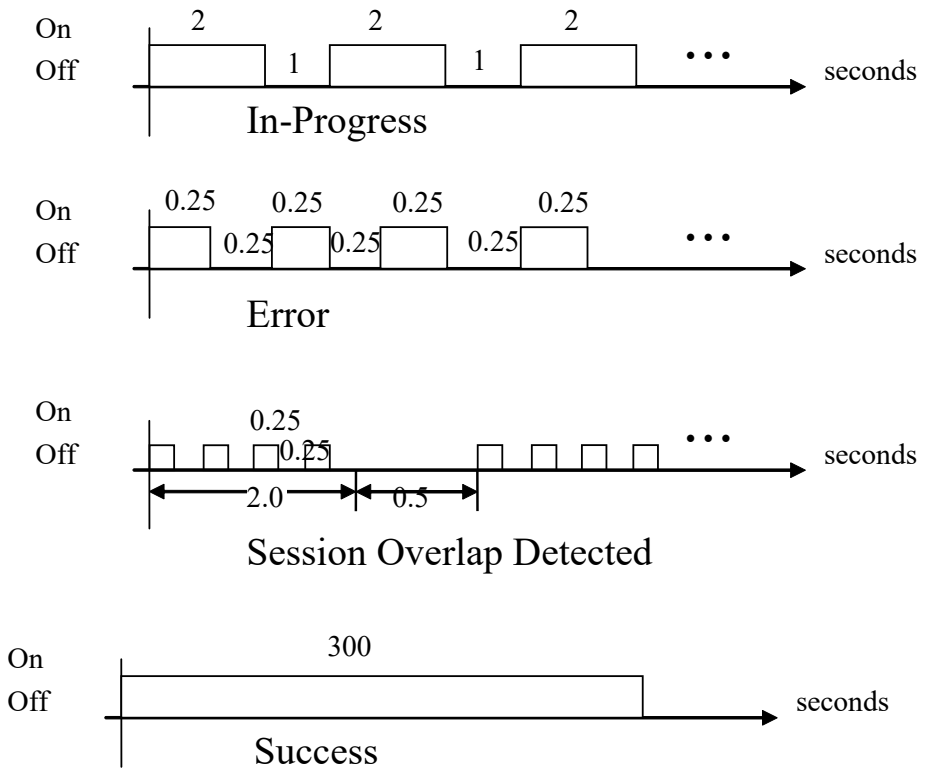

Figure 1 – WSC Visual Indicator LED Flashing Frequencies

3.2 AP Static PINs and Lock-down State

Issue:

An AP that uses a static label PIN must track multiple failed attempts to authenticate an external Registrar and then enter a lock-down state (see Section 4.3.1 of the WSC 2.0 specification). After three failed PIN authentication attempts within 60 seconds, an AP must enter the lock-down state for 60 seconds. The AP may be designed to stay in lock-down state for a longer or indefinite period, depending on security requirements.

Some external Registrars may make continuous failed PIN attempts over a period of some minutes when supplied with an incorrect PIN by a legitimate user. This may cause an AP to go into lock-down state unless the AP has the capability to distinguish between failed PIN attempts using the same PIN and failed PIN attempts using different PINs. If the AP is designed to stay in lock-down state for an extended or indefinite period then the user experience may be adversely affected.

Solution:

External Registrars that receive a WSC NACK after sending message M2 or M4 should signal the user that the PIN may be incorrect and should not make further PIN attempts until the correct PIN is re-entered.

An AP that stays in lock-down state for an extended or indefinite period should either have the capability to distinguish between failed PIN attempts using the same PIN (indicating mistyping) versus failed PIN attempts using different PINs (indicating an attack), or use a different heuristic for locking the AP for long periods. For example, the first lock-down period could be 60 seconds with each successive lock-down period being progressively longer (e.g. multiplied by two on each successive attack).

3.3 PIN Checksum Calculation

Issue:

The WSC specification defines both default and user-specified PIN types for entry into a Registrar by the user (machine PIN is intended to be a large number not entered manually by the user). Although length is not specified, four or eight digits are recommended for both default and user-specified PIN values. Moreover, 8-digit default PIN values require a checksum, but user-specified PIN values do not. A Registrar may not know whether an Enrollee PIN is a user-specified or default PIN and, therefore, would not know whether to apply the checksum calculation.

When an Enrollee PIN is entered in a Registrar before the M1 message is sent by the Enrollee, the Registrar cannot bind the anonymous PIN to a specific Enrollee UUID or PIN type. If the Registrar then receives a subsequent M1 message from an Enrollee, the Registrar cannot determine whether the pre-entered PIN value is associated with that specific Enrollee and, therefore, cannot assume the PIN type.

Solution:

To avoid usability issues between default and user-specified PIN values, an AP should only provide a warning to the user on a PIN checksum failure rather than prevent the user from using the PIN value. PIN checksums and associated warnings should only be performed on 8-digit PIN values. The only time the AP can apply the PIN checksum with certainty is when the PIN is input in response to a M1 message from the Enrollee with a Device Password ID of “default PIN.”

3.4 WSC 2.0 Discovery Phase for PIN Method

Issue:

As shown in Figure 2, the WSC 1.0 discovery phase for PIN method required an Enrollee to associate with each WSC-capable AP within range and initiate the Registration Protocol by sending M1 in order to discover which Registrar was ready to run the Registration Protocol. For PIN method, APs were not required to include the Selected Registrar attribute set to TRUE in Beacons and Probe Responses.

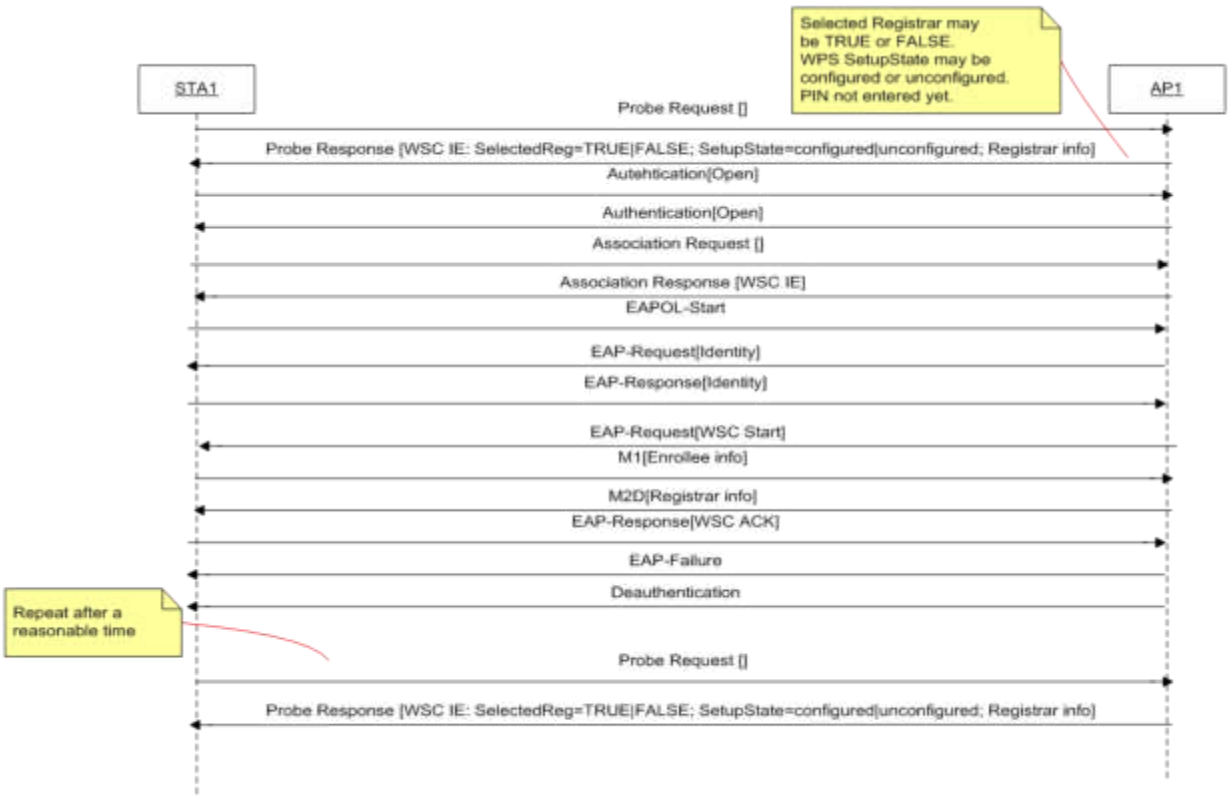

Figure 2 – WSC 1.0 PIN Method Discovery Phase

Solution:

The following paragraphs summarize the PIN method discovery phase for a WSC 2.0 Enrollee, as per the WSC 2.0 specification. The summary is followed by a recommendation for PIN method discovery when the environment includes both WSC 1.0 and WSC 2.0 APs.

As shown in Figure 3, the WSC 2.0 discovery phase was modified to allow an Enrollee to more easily identify which Registrar is ready to run the Registration Protocol for PIN method (see WSC 2.0 Section 4.2). Information about the Enrollee, equivalent to the information in message M1, is now sent by the Enrollee in the WSC IE in its Probe Requests. The Enrollee may include the optional Request To Enroll sub-element set to TRUE to indicate that it is specifically requesting to start Registration and not just performing discovery. This allows the AP or external Registrar user interfaces to provide the user with specific indicators containing details of the prospective Enrollee, for example.

The AP must proxy the Enrollee's Probe Request to the internal or any attached external Registrar. The AP must include the Selected Registrar attribute set to TRUE in Beacons and Probe Responses when it receives a SetSelectedRegistrar message with the Selected Registrar attribute TRUE from a Registrar. Note that some Registrars may send a SetSelectedRegistrar message with the Selected Registrar attribute TRUE when the user navigates to a GUI page that allows selection of the Enrollee, so for PIN method the presence of the Selected Registrar attribute TRUE alone in Beacons and Probe Responses does not guarantee that the Registrar is ready to run the Registration Protocol.

Once the PIN is entered into the Registrar, it must send a SetSelectedRegistrar message to the AP with the Selected Registrar attribute TRUE and an AuthorizedMACs sub-element which includes either the Enrollee MAC address or the wildcard MAC address (FF:FF:FF:FF:FF:FF). The Registrar will include the wildcard MAC address in cases where the Registrar does not know

the Enrollee MAC address yet, for example when the Registration Protocol is started on the Registrar side first. The AP or external Registrar user interface may also have an option to specifically enter the Enrollee MAC address to be included in the AuthorizedMACs sub-element, or the user interface may allow the selection of the Enrollee MAC address from a list of those Enrollees currently performing discovery.

On receiving the SetSelectedRegistrar message with the Selected Registrar attribute TRUE and an AuthorizedMACs sub-element with a list of MAC addresses, the AP will include the Selected Registrar attribute and the AuthorizedMACs sub-element in Beacons and Probe Responses to indicate that the Registrar is ready to start the Registration Protocol.

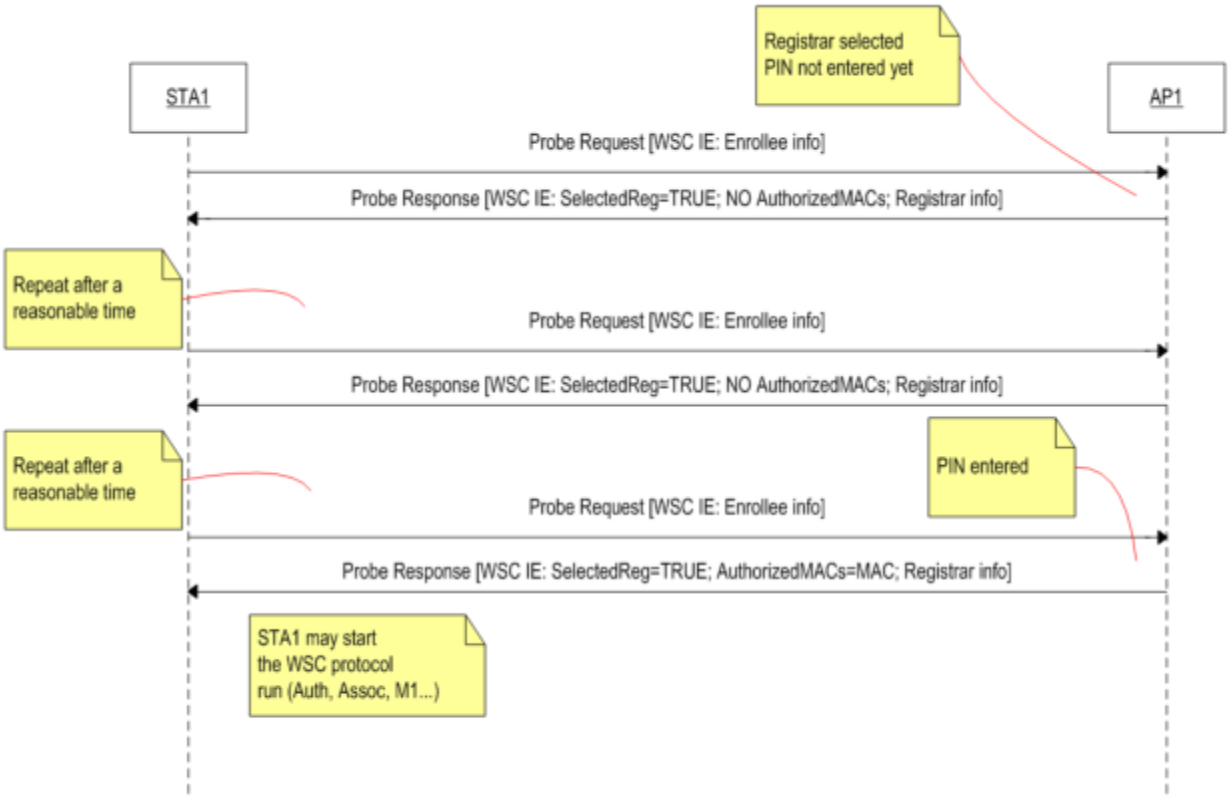

Figure 3 - WSC 2.0 PIN Method Discovery Phase

Once the Enrollee receives a Beacon or Probe Response with the Selected Registrar attribute TRUE and with an AuthorizedMACs sub-element containing either its own MAC address or the wildcard MAC address, it may start the Registration Protocol. In the case where the wildcard MAC address is advertised, and not the Enrollee's MAC address, the PIN attempt may fail if the Registrar is expecting a different Enrollee. In another case, the Enrollee may receive an M2D message following its M1 message if a WSC 1.0 external Registrar is attached to the AP and the external Registrar is not yet ready to run the Registration Protocol. An Enrollee must handle both cases.

Note that for the PIN method, an Enrollee may also perform discovery as for WSC 1.0 by associating and sending M1, i.e. before receiving a Beacon or Probe Response with the Selected Registrar attribute TRUE and an AuthorizedMACs sub-element containing either its own MAC address or the wildcard MAC address. An Enrollee may use this form of discovery to discover available Registrars.

In a mixed environment with both WSC 1.0 and WSC 2.0 APs, an Enrollee should be prepared to run both the WSC 1.0 and WSC 2.0 forms of discovery. An Enrollee may scan available channels and then order PIN attempts with prospective APs as follows:

1. WSC 2.0 AP with the Selected Registrar attribute TRUE and the Enrollee's MAC address in the AuthorizedMACs sub-element in Beacons and Probe Responses.
2. WSC 2.0 APs with the Selected Registrar attribute TRUE and the wildcard MAC address in the AuthorizedMACs sub-element in Beacons and Probe Responses, ordered by decreasing RSSI.
3. WSC 1.0 APs, ordered by decreasing RSSI.

If option 1 is available, options 2 and 3 should be unnecessary.

3.5 Weak Diffie-Hellman Private Key

Issue:

Any vendor using a weak Diffie-Hellman Private Key could be vulnerable to an exploit that would allow the compromise of any WSC transactions involving that vendor.

If the Diffie-Hellman Private Key value used in WSC is too short or the value is not random, the cryptographic security of the WSC message exchange is compromised and the network key is more easily discovered by a third party who is observing the WSC message exchange.

WSC uses 1536-bit MODP group 5 from RFC 3526. The security level of this group is about 60-80 bits. The advised length of the private exponent is two times this value, which equates to a length of 160 bits for this group. As such, the minimum recommended length of Diffie-Hellman Private Key is 160 bits.

The Diffie-Hellman Private Key may have been made deliberately short in a particular implementation because it reduces the processing time required for cryptographic operations when there is limited processing power available on the target platform.

It is also important that the Diffie-Hellman Private Key is generated randomly. Implementations should not restrict the private key value to numbers whose binary representation has low Hamming weight to speed up exponentiation. It is very important to advise against such special choices.

Solution:

The WFA recommends using a high-entropy private key with a length more than 160 bits for security. Any vendor not following the recommendation needs to be aware that this may compromise the security of any WSC procedures in which they participate.

3.6 Registrar Support for all PIN Implementations

Issue:

Some Registrar implementations may prefer or limit connections to Enrollees that have a dynamic PIN (and are advertising "display" in their probe request or association request) over Enrollees that have a static PIN (and are advertising "label").

For example, a vendor may implement an External Registrar that prefers Enrollees with dynamic PINs, (e.g. for security reasons) but this will cause user experience issues. Both static and dynamic PINs are allowed in WSC and both should be supported. Headless devices may be unable to generate or display a dynamic PIN, and a user may be unable to change the PIN from static to dynamic. As a result an Enrollee may be unable to join the network at all.

Solution:

Registrars should allow an Enrollee to join with any valid PIN method.

3.7 Option to Disable Wi-Fi Simple Configuration

Issue:

Users have requested the option to disable Wi-Fi Simple Configuration.

As Enrollees are not required to have Wi-Fi Simple Configuration enabled out-of-box, many implementations allow a user to enable and disable this feature. However, as APs are required to have WSC enabled out-of-box, many AP implementations do not provide an option to disable it.

Solution:

All Wi-Fi Simple Configuration devices and software should provide the user with the option to disable and re-enable this feature (e.g. in the device UI) if possible.

3.8 Consistent Push Button LED Implementation

Issue:

Push Button LED implementations are not mandated due to vendor needs and vendor differentiation. Users are unable to differentiate between multiple flashing (or blinking) states.

Solution:

Recommendation for a two-color LED:

	Blink	***Solid***
Color 1	In Progress	Success For secure networks, the LED should stay solid until WSC is In Progress again. For Open (no security-enabled) networks, the LED should stay solid for 120 seconds and then revert back to the previous (off) state
Color 2	Session Overlap The LED should Blink for 120 seconds, and then revert back to the previous state	Error The LED should be Solid for 120 seconds and then revert back to the previous state

3.9 Dual-band AP & Client Implementations

Issue:

A dual-band AP may appear as two APs to a Client, possibly causing an erroneous Session Overlap failure in PBC mode.

A dual-band AP may appear as two APs to a Client, requiring the Client to select which AP to join in PIN mode.

In addition, the specification does not explicitly define how dual-band devices will behave while executing WSC.

Solution:

In PBC mode, all Clients should compare the UUIDs in AP beacons to determine Session Overlaps (and non-Session Overlaps).

In PIN mode with AP Embedded Registrars, all Clients should compare the UUIDs in AP beacons to determine which bands are available for that AP.

All permutations of dual-band APs and Clients in both PBC and PIN modes are included in Section 4.1 for completeness.

3.10 Use of Dynamic PIN by Mobile APs with Display Capability

Issue:

Mobile APs that support configuration or Enrollee addition by an External Registrar require a PIN. Static PINs are vulnerable to brute force attack by attackers posing as External Registrars. In addition, it may not be convenient to place a static label PIN on the outside of some devices that may have Mobile AP functionality, such as dual-mode phones or smartphones.

Solution:

Mobile AP devices that support configuration or Enrollee addition by an external Registrar, and which have a display, should use dynamic PINs and generate a new PIN each time they run the Registration protocol as Enrollee in initial AP setup mode (see Section 4.3.1 of the WSC 2.0 specification).

3.11 Required and Optional User Actions

Issue:

Some implementations require the user to select either PIN or PBC before the protocol will run. While device UIs are not defined by Wi-Fi Simple Configuration, this is an unnecessary extra step for the user to take.

Solution:

AP, Client, and Registrar devices should not require the user to select a specific WSC method before starting the protocol. The user interface should be as simple as possible and the number of steps should be minimized based on individual device requirements.

3.12 Required and Optional User Actions in PIN Method

Issue:

The WSC specification allows the implementation of multiple user interaction models. As a result, some current implementations of the PIN method require user action at the Enrollee or Registrar before the Enrollee can be added via PIN to a Registrar.

Examples are:

1. Requiring a user to "enable" Wi-Fi Protected Setup or the WSC protocol
2. Requiring a user to "enable" the PIN method
3. Requiring a user to "select" a PIN
4. Requiring a user to "activate" a PIN
5. Requiring a user to pre-select the SSID of the target AP before the PIN is active

Requiring user actions at the Enrollee or Registrar before an Enrollee can be added via PIN decreases the ease-of-use of the Wi-Fi Simple Configuration system. These additional tasks can be even more difficult in the case of a headless Enrollee.

One of the primary goals of the Wi-Fi Protected Setup certification program was to allow a user to configure and add devices to a secure WLAN without prior knowledge of the SSID and security settings.

Another primary goal is to decrease the number of steps a user must take in order to configure and add devices to a secure WLAN. However, in some circumstances additional steps may be considered an improvement to the user experience.

Solution:

The preferred implementation for an Enrollee, particularly a headless Enrollee, would be to have the PIN always active when Wi-Fi Simple Configuration is enabled. The Enrollee should attempt to associate with (1) any WSC 2.0 AP that advertises the AuthorizedMACs attribute, containing either the Enrollee's MAC address or the wildcard MAC address, and advertises SelectedRegistrar equal to TRUE, or with (2) any WSC 1.0 AP that advertises SelectedRegistrar equal to TRUE until it finds a Registrar that has its (the Enrollee's) PIN correctly entered (also see Section 3.4).

3.13 User-facing Error Messaging

Issue:

Inconsistent user-facing instructions and error messaging decrease the ease-of-use of the Wi-Fi Simple Configuration system.

Solution:

When possible, vendors should provide clear and consistent user-facing messaging in response to system errors. Recommended messaging text for error codes provided in Table 33 of the Wi-Fi Simple Configuration Specification is included below. Messaging is conditional based on the current logical function of the device displaying the message. For example, when an AP is acting as a Registrar, it should display the Registrar messaging as appropriate; however, when the AP is acting as an Enrollee, it should display the Enrollee messaging as appropriate. In some cases, the Enrollee or Registrar messages may only apply to an AP or Client acting in those functions as indicated below.

#	Description	Enrollee Text (Client or AP)	Registrar Text (AP or Client)
0	No error	(no message) or In Progress	(no message) or In Progress
1	Out-of-band Interface Read Error	Error, the security settings cannot be detected. Please try again.	Error, the security settings cannot be configured. Please try again.
2	Decryption CRC Failure	Error, the security settings cannot be detected. Please try again.	Error, the security settings cannot be configured. Please try again.
3	2.4 channel not supported	The 2.4 GHz band is not supported by the current network.	The 2.4 GHz band is not supported by the current network.
4	5.0 channel not supported	The 5.0 GHz band is not supported by the current network.	The 5.0 GHz band is not supported by the current network.

#	Description	Enrollee Text (Client or AP)	Registrar Text (AP or Client)
5	Signal too weak	N/A	N/A
6	Network auth failure	N/A	N/A
7	Network association failure	N/A	N/A
8	No DHCP response	N/A	N/A
9	Failed DHCP config	N/A	N/A
10	IP address conflict	N/A	N/A
11	Couldn’t connect to Registrar	AP: Error, this device was unable to join the network.	Client/ER: N/A
12	Multiple PBC sessions detected	Error. Multiple devices in your area have had their buttons pushed recently, which may be a security risk. Please wait two minutes and try again.	Error. Multiple devices in your area have had their buttons pushed recently, which may be a security risk. Please wait two minutes and try again.
13	Rogue activity suspected	(vendor specific)	(vendor specific)
14	Device busy	Error. Another session of Wi-Fi Protected Setup is running; this device is busy at this time. Please wait and try again.	Error. Another session of Wi-Fi Protected Setup is running; this device is busy at this time. Please wait and try again.
15	Setup locked	AP: Error. This device has been locked due to multiple failed configuration attempts that may indicate a security risk. Please (insert vendor specific instructions for continuing)	Client/ER: Error. Due to multiple failed configuration attempts, the device you are attempting to access has been locked. Please wait two minutes and try again, or read the device's user guide for further instructions.
16	Message timeout	N/A	N/A
17	Registration session timeout	N/A	N/A
18	Device password auth failure	Error. The PIN used to add this device may have been entered incorrectly. Please check the PIN and try again.	Error. The PIN used to add the new device may have been entered incorrectly. Please check the PIN and try again.

3.14 Client Joining via PIN Method

Issue:

The WSC specification does not define how and when an Enrollee must begin "listening" for (1) an WSC 2.0 AP that is advertising the AuthorizedMACs attribute, containing either the Enrollee's MAC address or the wildcard MAC address, and SelectedRegistrar equal to TRUE, or for (2) an WSC 1.0 AP that is advertising SelectedRegistrar equal to TRUE, and as a result, there are inconsistent implementations and inconsistent user actions required. For example, a headless Enrollee may not have a UI option to pre-select an AP, but still should be able to automatically discover and connect to the correct WLAN.

There is no definition for:

1. How does the Client automatically "start" listening for any AP advertising the AuthorizedMACs attribute and/or SelectedRegistrar equal to TRUE?
2. How/when does the Client select an AP to associate to?
3. How often does the Client begin listening again? And when does the Client associate to another AP? (e.g. when a Client is inadvertently already associated with an incorrect (open) AP)

Solution:

Recommendations for Client (also see Section 3.4):

Start listening:

- on boot
- on idle (connected, but no data frames exchanged for x time, or predefined timer) if connected to an open AP

1. Connect to (or stay connected to): previously connected (or currently connected) profile if profile is for a secure AP
2. If not connected (and no profile for a secure AP is retained): search for an AP advertising the AuthorizedMACs attribute and/or SelectedRegistrar equal to TRUE
3. If no WSC 2.0 AP or WSC 1.0 AP advertising the required attributes and values is found then go back to vendor defaults or last connected profile

3.15 Enrollee Session Overlap Detection after WSC Protocol Run (Multiple Registrars Detected)

Issue:

The current specification includes a two-minute Walk Time during which an Enrollee can find a Registrar.

However, there is an opportunity for the Enrollee to join a rogue network if a rogue Registrar initiates PBC mode before the legitimate Registrar does.

Solution:

The specification requires the Enrollee to scan through all channels to verify that there is only one AP/Registrar in PBC mode before starting the WSC protocol run. Vendors may improve security by requiring the Enrollee to do a full scan (but without PBC request in Probe Request frames) after a successfully completed protocol run. If another PBC Registrar is found at that point, the Enrollee should report session overlap to the user and may reject the credentials received during the protocol run.

There would be no changes to the actual WSC protocol run and from the Enrollee view point there would simply be one more standard scan afterward.

3.16 AP/Registrar Session Overlap Detection after WSC Protocol Run (Multiple Enrollees Detected)

Issue:

The current specification includes a two-minute Monitor Time which is intended to determine that one (and only one) Enrollee is in PBC mode. Otherwise, the specification requires the Registrar to declare a Session Overlap. In addition, the specification requires the AP/Registrar to continue to monitor for additional Enrollees during the WSC protocol run.

However, there is still an opportunity for a rogue Enrollee to join the network if the rogue Enrollee initiates PBC mode during the Monitor Time, but the legitimate Enrollee initiates PBC mode after the Registrar successfully completes the protocol run with the rogue Enrollee.

In addition, there is another opportunity for a rogue Enrollee to join the network if the rogue Enrollee initiates PBC mode after the Registrar initiates PBC mode and successfully completes the protocol run before the legitimate Enrollee initiates PBC mode.

Solution:

The specification requires the AP/Registrar to verify that there is only one Enrollee in PBC mode before starting and during the WSC protocol run. Vendors may improve security by requiring the AP/Registrar to continue to monitor for Enrollees attempting to associate via PBC mode after a successfully completed protocol run for up to two minutes.

If another PBC Enrollee is found at that point, the AP/Registrar may message to the user that there may be a problem. The message may indicate that another Enrollee has been found and that the user should confirm that the intended Enrollee has joined the network. The device can provide additional information about what the user can do if a rogue Enrollee has joined the network.

However, vendors are cautioned that providing this additional Monitor Time might increase security at the risk of confusing or unnecessarily alarming the user. It is possible for the AP/Registrar to falsely identify a second (legitimate) Enrollee that is attempting to start a new WSC session if the user presses the Enrollee's button within two minutes of the previous WSC session ending, and before pressing the button on the AP/Registrar again. For this reason, if vendors do choose to implement this additional security feature, it is strongly recommended that vendors keep the messaging as informational only and avoid alarming language.

There would be no changes to the actual WSC protocol run and from the AP/Registrar view point there would simply be an additional verification afterward.

3.17 External Registrar Configuration of AP in "Configured" State

Issue:

When an External Registrar registers with an AP which is in the “Not Configured” state, the External Registrar provides the AP with configuration settings and may then re-associate (if connected via wireless) and add Enrollees using those settings. The AP moves from the “Not Configured” to the “Configured” state after being provisioned by the External Registrar, or for other reasons listed in the WSC 2.0 specification (see Wi-Fi Simple Configuration State in Section 12 Data Element Definitions, p125).

When an External Registrar registers with an AP which is in “Configured” state it may either (1) discover the AP’s current settings and then re-associate (if connected via wireless) and add Enrollees using those settings, or (2) both discover and change the current settings before re-associating (if connected via wireless) and adding Enrollees. In the latter case, the user may or may not be aware that the AP’s configuration has changed.

Solution:

It is recommended that an External Registrar should inform the user before changing the configuration of an AP that is in the “Configured” state. This is to prevent a user from unknowingly

reconfiguring their AP. An implementer may also choose to prompt the user before changing the AP configuration, i.e. the External Registrar user interface could require the user to confirm a configuration change to an AP that is in “Configured” state before it is committed by the External Registrar. Note that the user would need to confirm the change before the AP’s WSC state machine times out waiting for message M8 from the External Registrar.

3.18 Consistent Visual Identification on Labels and UIs for PIN and Push Button

Issue:

A user may be unable to locate the correct PIN or the correct button to press for Wi-Fi Simple Configuration.

Devices (APs and clients) from different manufacturers label the PIN differently. Some common ways of indicating the PIN are WPS PIN, PIN, PIN CODE, and SECURITY CODE. Also, the labels on devices often have additional numbers such as serial numbers and MAC addresses that can confuse the user.

Solution:

For Wi-Fi CERTIFIED™ devices, the Wi-Fi Protected Setup Identifier Mark PIN method Physical Label should be printed along with the PIN to clearly provide a visual indication to the user. Additional numbers, such as serial numbers or MAC addresses, should not be combined with the label. Software Labels should replicate as closely as possible the layout of the Physical Labels.

A physical Push Button should have the Wi-Fi Protected Setup Identifier Mark or Solo Mark printed directly on it, if possible, or immediately adjacent. Software buttons should replicate as closely as possible the layout of the physical Push Buttons.

Manufacturers should refer to the Wi-Fi Alliance Brand Styleguide for additional detail.

3.19 Device Identification Fields

Issue:

There are WSC protocol fields that are available in the discovery process that vendors will choose to display in device user interfaces. The user may identify and connect to devices based on this device description information. If the device description information is not correct or not consistent, users will have difficulty identifying and connecting their WSC enabled devices.

Solution:

The following guidelines are recommended for each of the device description fields:

UUID (UUID-E and UUID-R)	The UUID must be unique. It is recommended that the UUID field be based on the MAC Address of one interface on the device and that the UUID must be used on all interfaces. It is recommended that the UUID is derived as Version 5 Name-based UUID as described in RFC 4122, Chapter 4.3.
Manufacturer, Model Name and Model Number	The Manufacturer, Model Name and Model Number should match any similar information displayed on the outside of the device or its packaging.
Serial Number	Where this information is available, the Serial Number should be included. If it is not available, the field should be empty.
Primary Device Type	The Primary Device Type field should be populated with a value that best represents the user’s view of the type of the device.

Device Name	Where possible the default value of this field should be populated with a fairly unique friendly name for the device. The user should have the able to rename the device by changing this field.

3.20 Dual-band AP Possible Configurations

Issue:

There are four possible combinations of SSID and security settings for a dual-band AP:

- SSIDs are different, security settings are different
- SSIDs are the same, security settings are different (Note: this combination is strongly discouraged)
- SSIDs are different, security settings are the same
- SSIDs are the same, security settings are the same

This list obviously expands with multi-band (three or more) APs, and can also apply to an AP with multiple "virtual APs" in the same band.

The WSC specification does not define how the AP should be configured by WSC when multiple virtual or physical APs are supported. WFA baseline certifications do not mandate how an AP should be configured by default, nor do they mandate what combinations end customers are allowed to configure.

Solution:

There are use cases that benefit from creating different SSIDs. For example, a vendor might wish to encourage the end customer to connect to one band for media and another band for data, using the SSID as a method of identifying which band should be used. As another example, when virtual APs are used on the same band, a different SSID could be used to identify which virtual network should be used for "guests". When different SSIDs are used, the security settings can be the same or different.

There are use cases that benefit from using the same SSID on both (or all) bands. For example, a vendor might wish to allow data offloading from one band to another, or otherwise hide the fact that there are multiple wireless networks to choose from. When the same SSIDs are used, the security settings should also be the same.

3.21 AP With Multiple Credentials (e.g. Dual-band or Virtual APs)

Issue:

If an AP is dual- or multi-band, or has virtual APs in the same band, each supported AP may have different credentials (i.e. SSID and security settings).

The WSC specification defines how multiple credentials can be shared during WSC negotiation.

Solution:

During WSC, if the SSID and security settings are the same, the AP’s Registrar provides the credential for all bands or virtual APs.

During WSC, if the SSID and security settings are different, the AP’s Registrar may provide all credentials for all bands and all virtual APs. However, the AP vendor may choose to include only a single credential based on which band or virtual AP the client device used to initiate WSC, or if WSC is intended to only apply to one of the networks. For example the push button might only apply to the local home network and not a guest network.

4 Appendices

4.1 Dual-band AP and Client Implementations

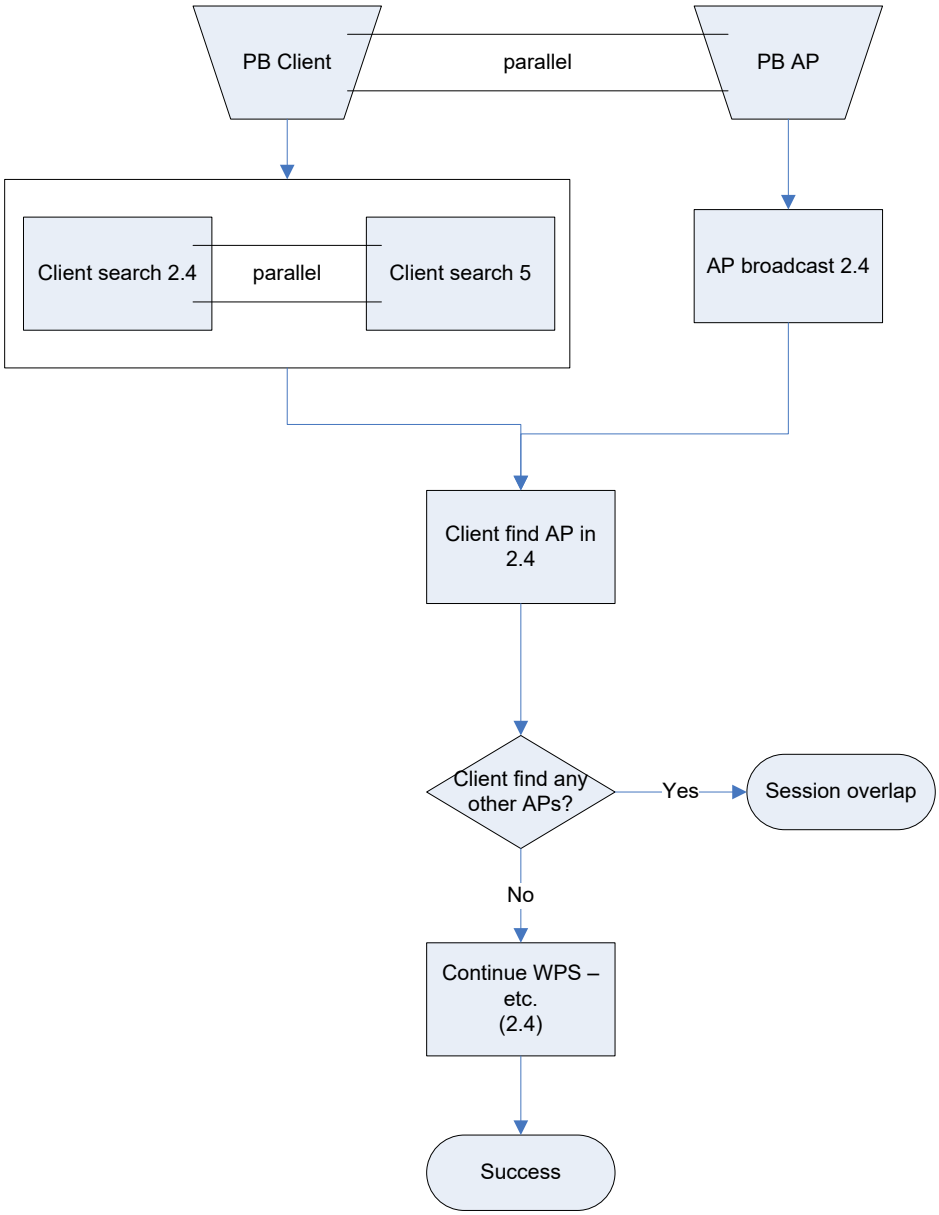

Figure 4 – Scenario 1: PBC → PBC, Client = 2.4 GHz / 5 GHz, AP = 2.4 GHz

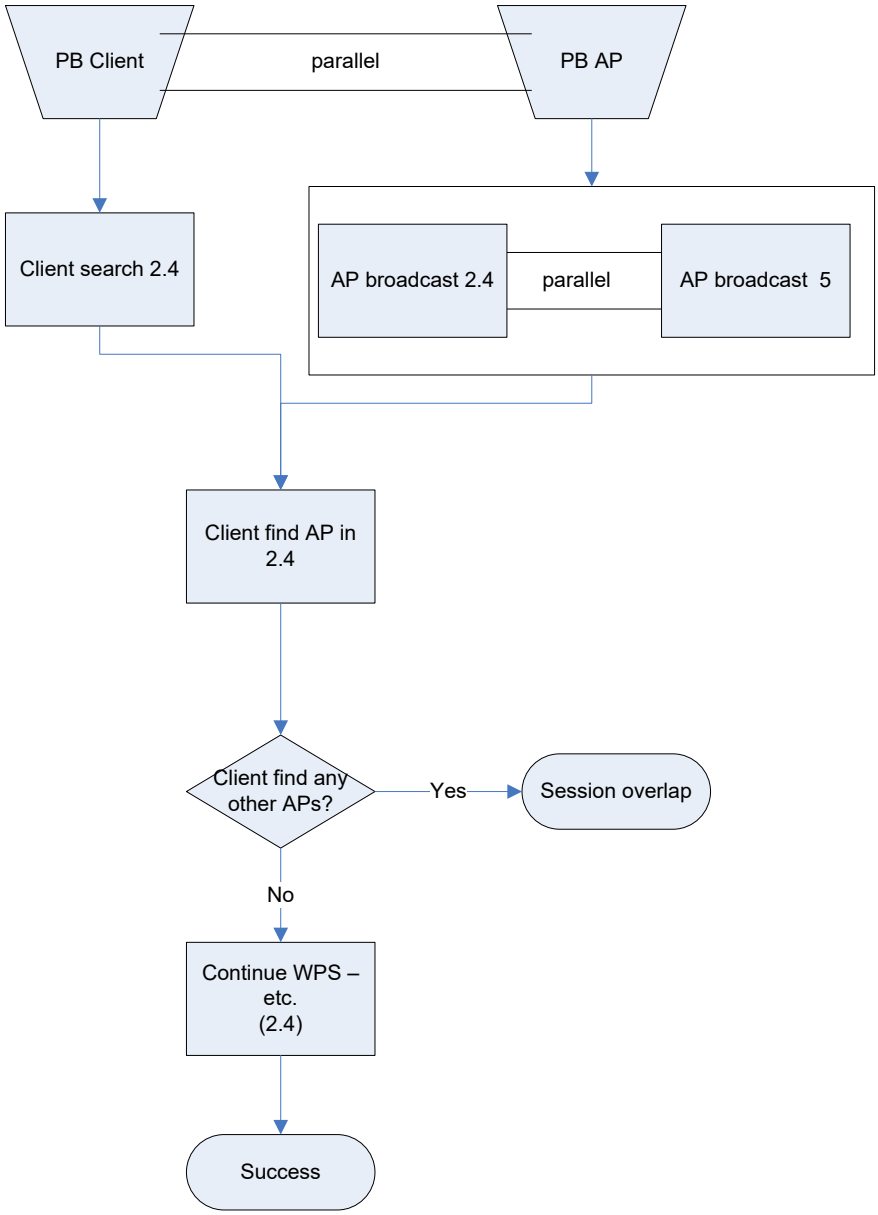

Figure 5 – Scenario 2: PBC → PBC, Client = 2.4 GHz, AP = 2.4 GHz / 5 GHz

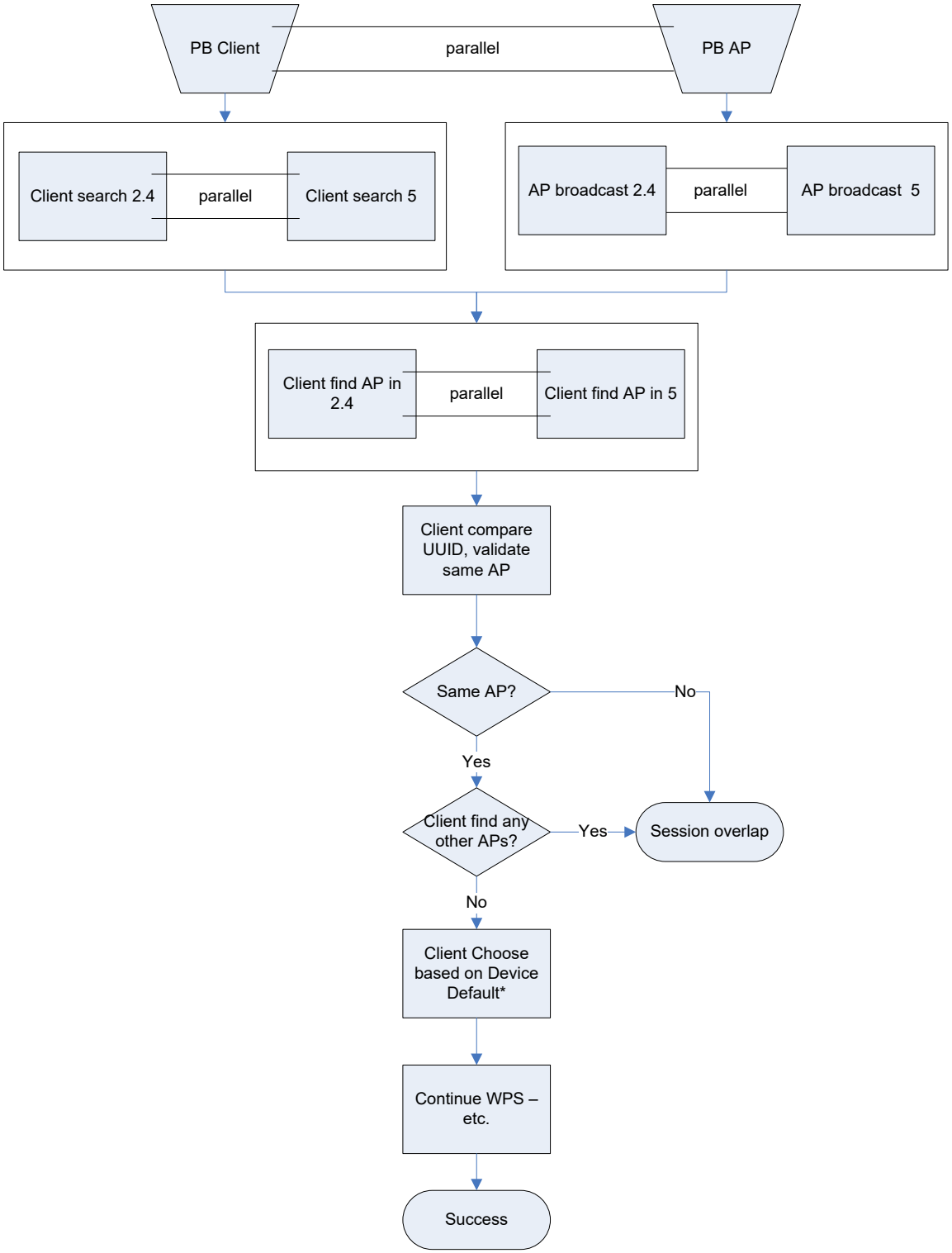

Figure 6 – Scenario 3: PBC → PBC, Client = 2.4 GHz / 5 GHz, AP = 2.4 GHz / 5 GHz

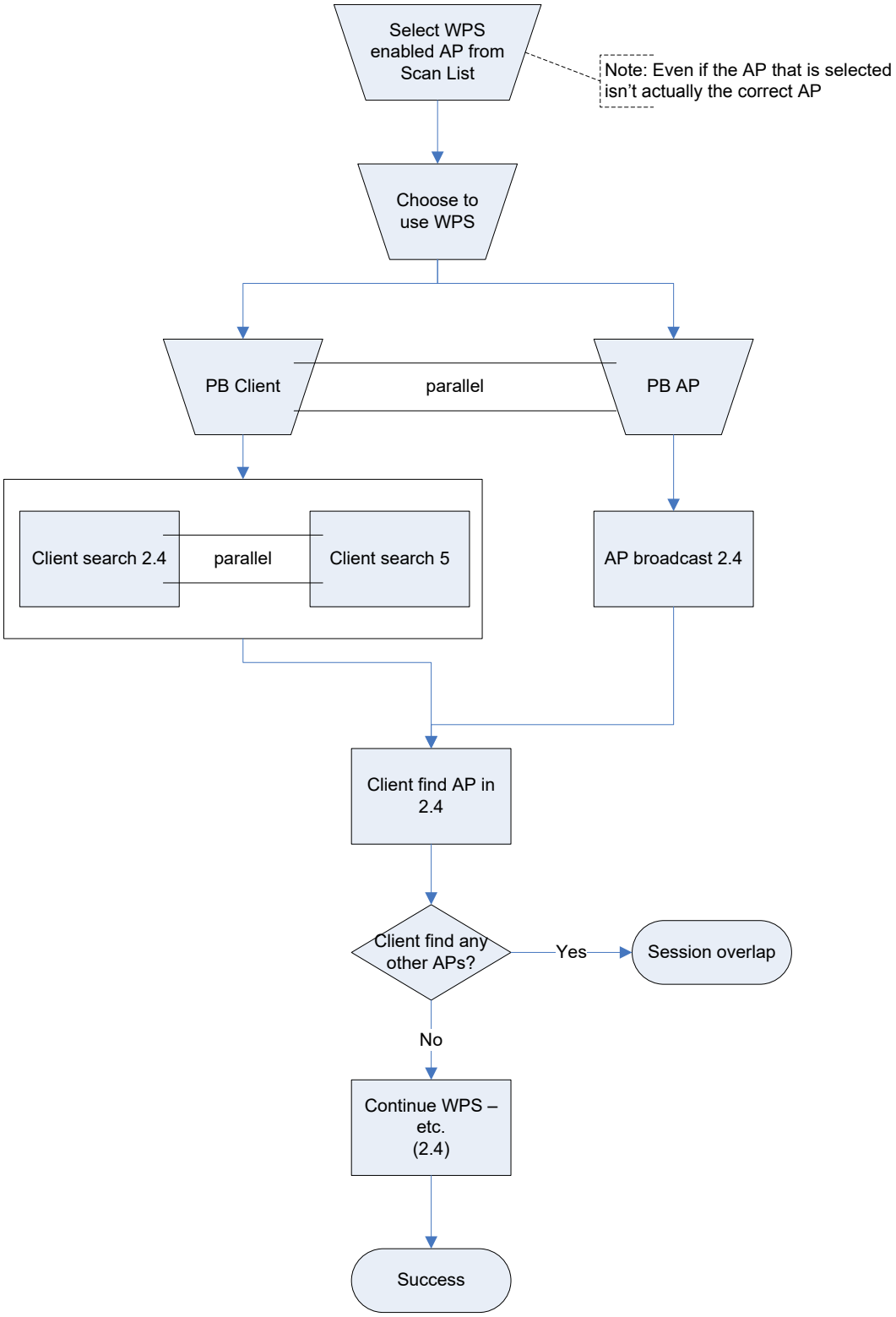

Figure 7 – Scenario 4: PBC from Scan List on Client, Client = 2.4 GHz / 5 GHz, AP = 2.4 GHz

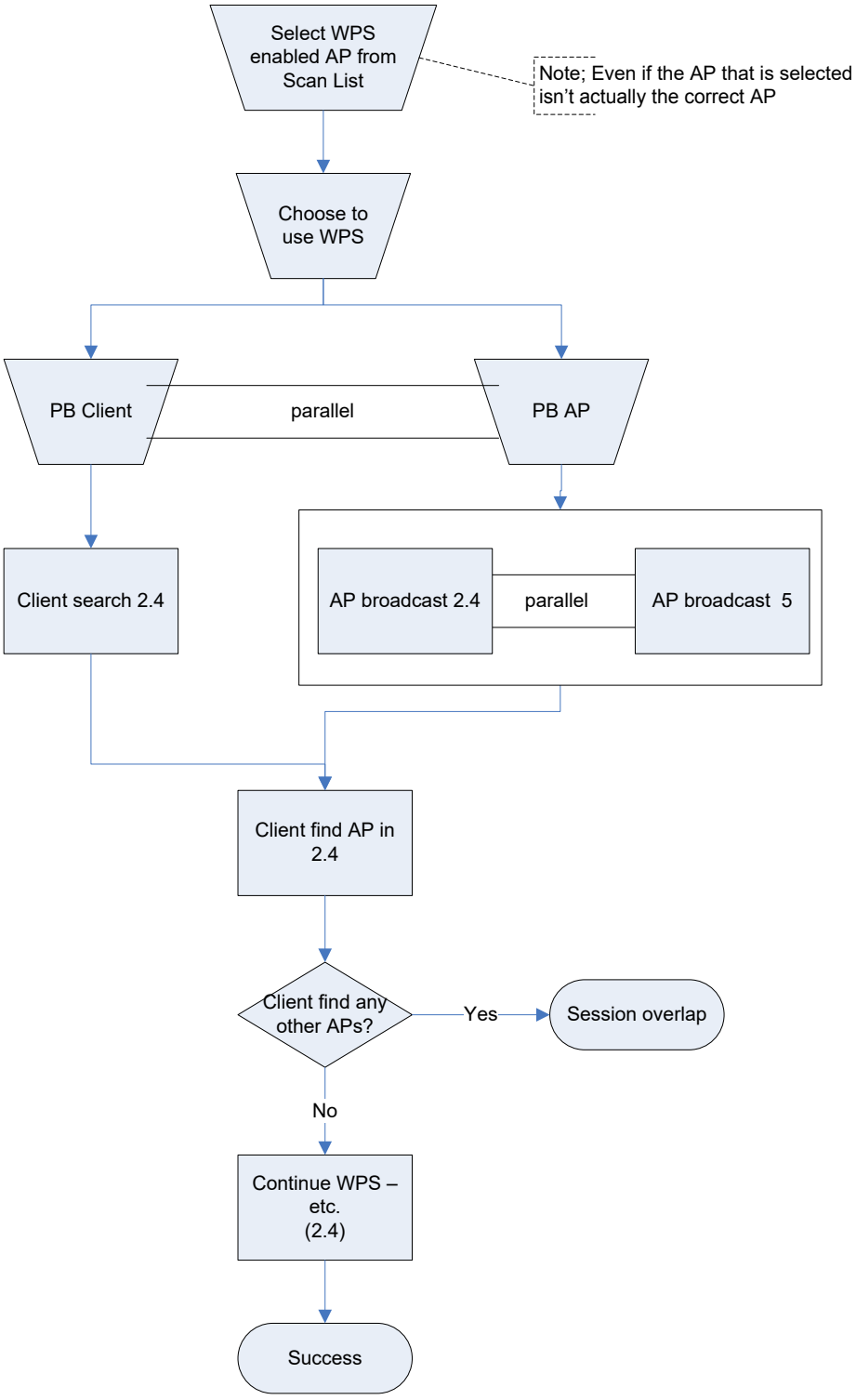

Figure 8 – Scenario 5: PBC → PBC from Scan List on Client, Client = 2.4 GHz, AP = 2.4 GHz / 5 GHz

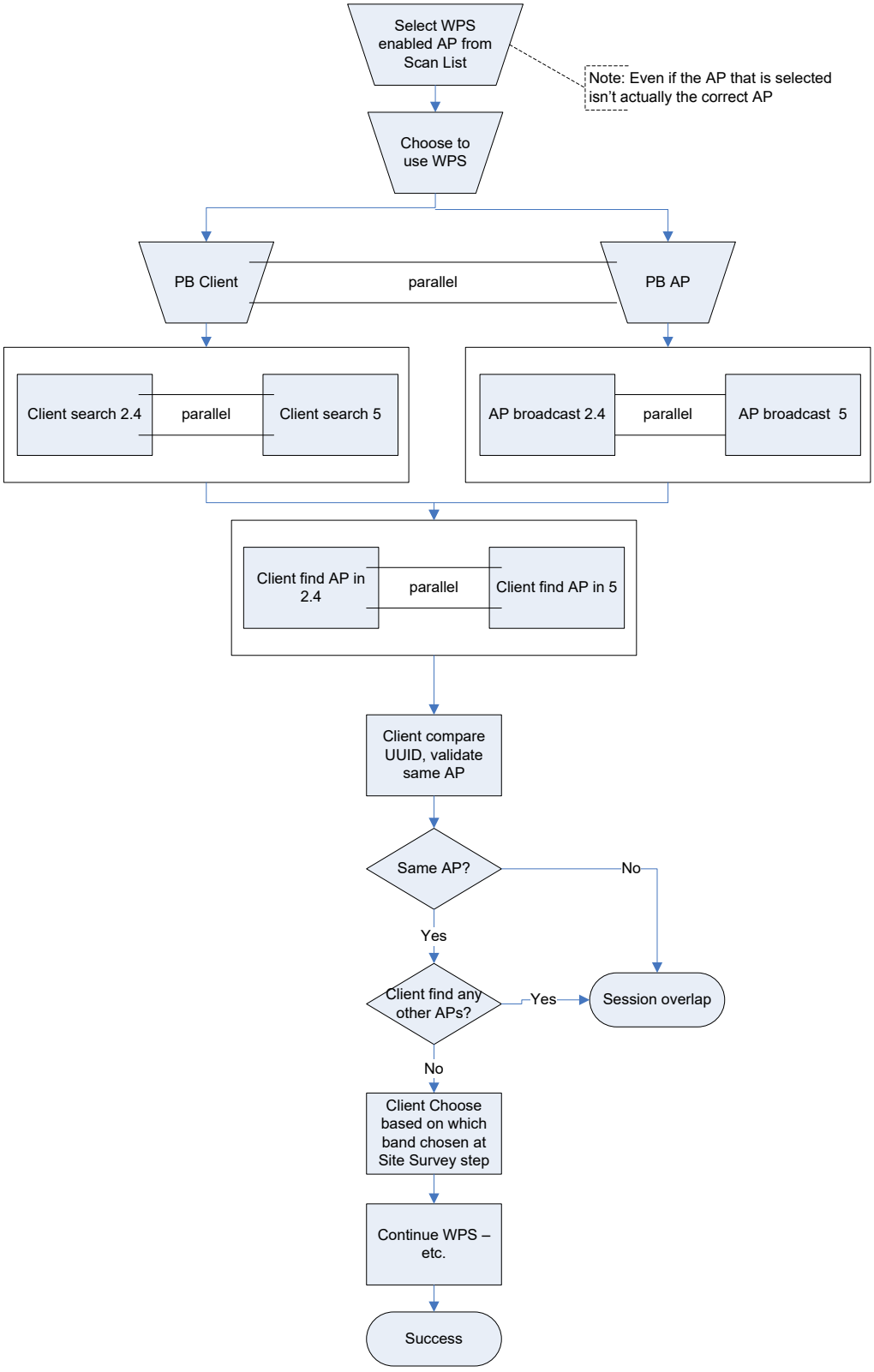

Figure 9 – Scenario 6: PBC → PBC from Scan List on Client, Client = 2.4 GHz / 5 GHz, AP = 2.4 GHz / 5 GHz

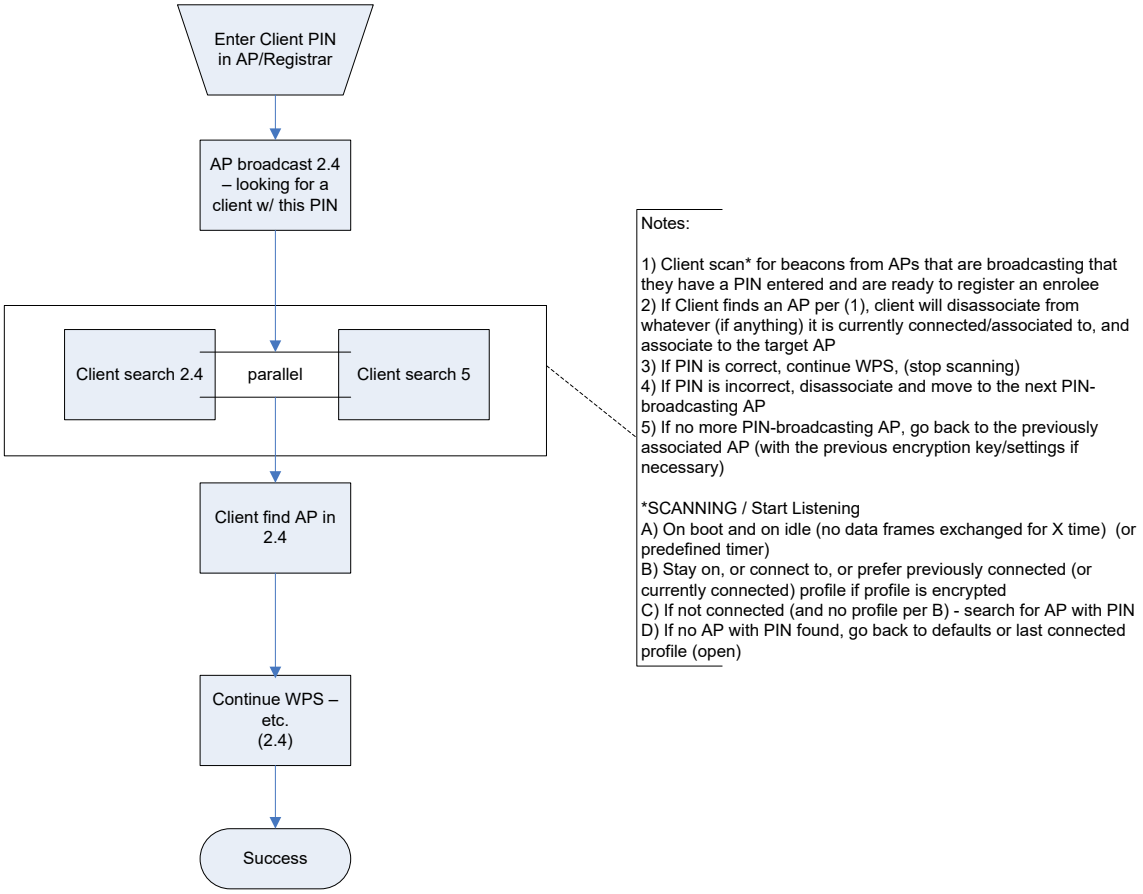

Figure 10 – Scenario 7: PIN (Client as Enrollee), Client = 2.4 GHz / 5 GHz, AP = 2.4 GHz

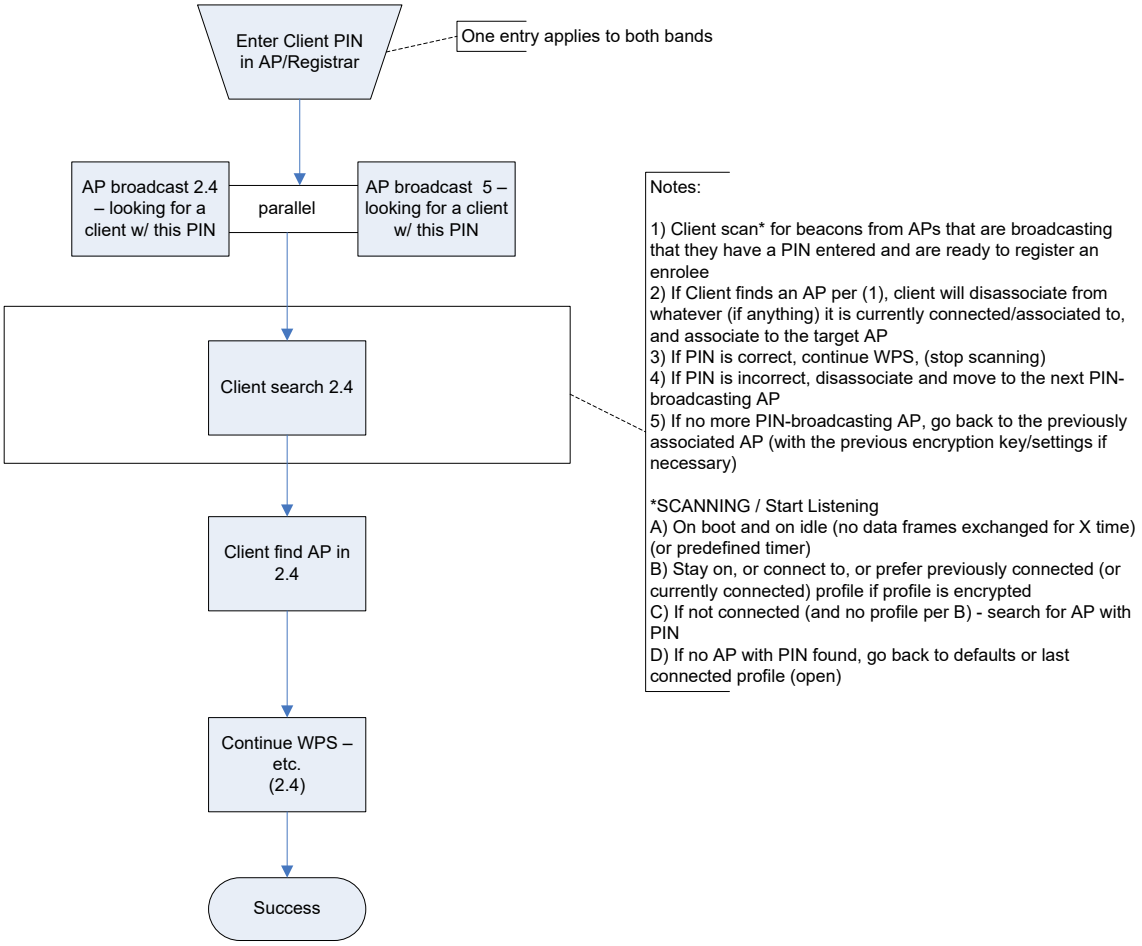

Figure 11 – Scenario 8: PIN (Client as Enrollee), Client = 2.4 GHz, AP = 2.4 GHz / 5 GHz

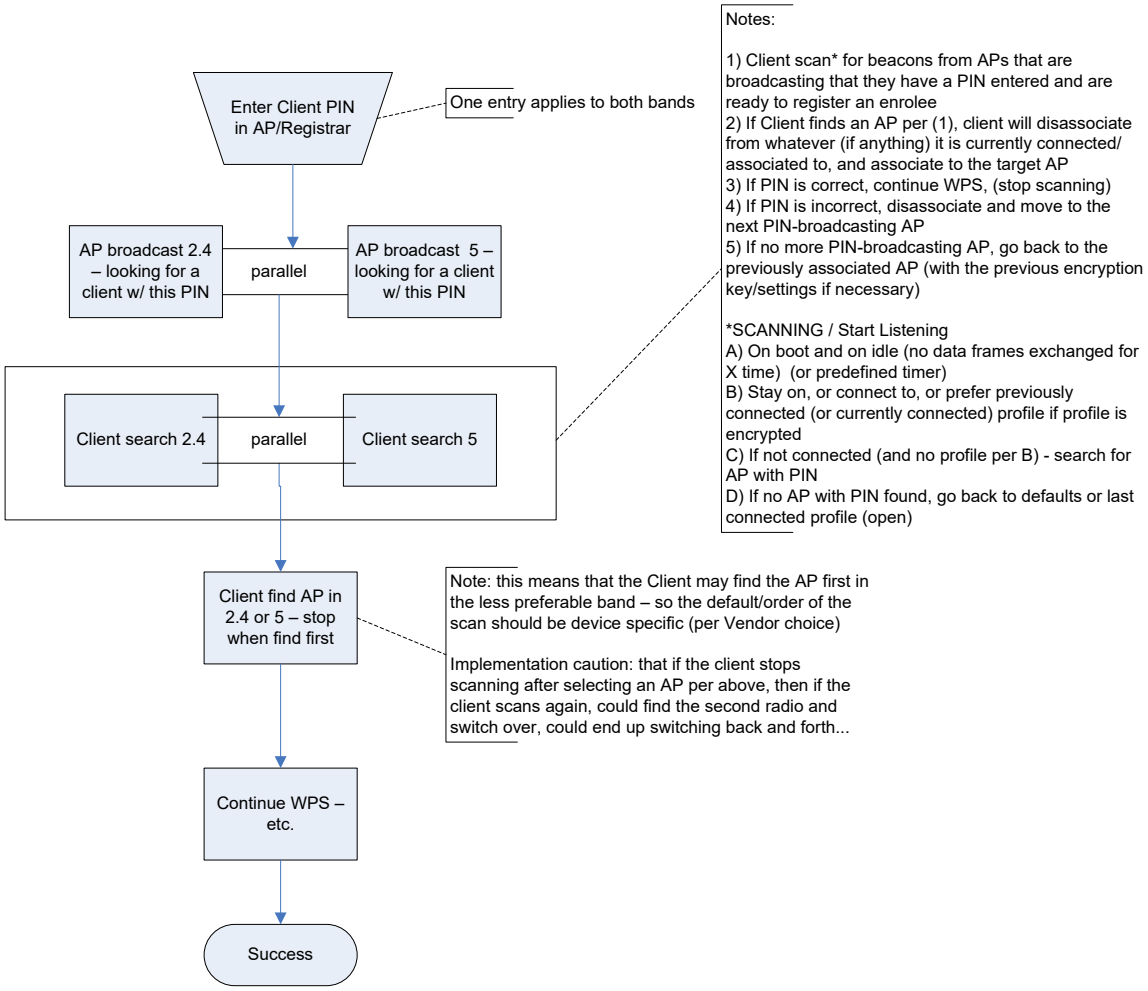

Figure 12 – Scenario 9: PIN (Client as Enrollee), Client = 2.4 GHz / 5 GHz, AP = 2.4 GHz / 5 GHz

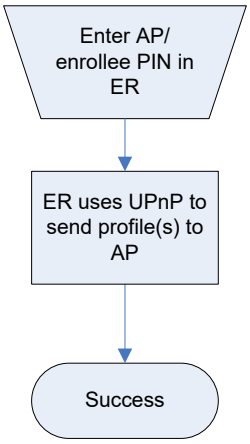

Figure 13 – Scenario 10: PIN (AP as Enrollee), Client = 2.4 GHz and/or 5 GHz, AP = 2.4 GHz and/or 5 GHz