Wi-Fi Alliance® Technical Committee
IBSS with Wi-Fi Protected Setup™ Technical Task Group

IBSS with Wi-Fi Protected Setup™
Technical Specification
Version 1.0.0

This specification describes extensions to the Wi-Fi Simple Configuration protocol to simplify the setup, security and management of IBSS Wi-Fi® networks.

Document History

Version	Date	Remarks
1.0.0	11/20/2012	Initial release

Table of Contents

Tables

Figures

1. Introduction

For infrastructure Wi-Fi networks, where a number of devices are connected to an access point, Wi-Fi Simple Configuration has been available since early 2007, allowing easy setup of the network, and with security enabled.

IBSS connectivity has existed for some time in the Wi-Fi world, but Wi-Fi Simple Configuration cannot be used, and instead there are various proprietary methods used to set up an Ad-hoc network. There are also some known interoperability issues with IBSS (also known as Ad-hoc), not covered by the underlying 802.11 specifications.

The purpose of this annex is to create extensions to Wi-Fi Simple Configuration for IBSS networking. The extensions will be based on the existing IEEE 802.11 IBSS mode, without the need (or use) of infrastructure. This specification creates a simple standardized method for the setup and configuration of IBSS networks and also addresses the known interoperability issues.

1.1. Scope

The primary goal of these extensions to Wi-Fi Simple Configuration is to simplify the setup, security and management of Ad-hoc Wi-Fi networks. It is also the goal that this specification provides users with the assurance that their Ad-hoc wireless networks are protected against unauthorized access and disclosure of private information.

The scope of this document is limited to that outlined by the IBSS with Wi-Fi Protected Setup Specification Requirements Document.

1.2. Definitions

Credential: A data structure issued by a Registrar to an Enrollee, allowing the latter to gain access to the network.

Device: An independent physical or logical entity capable of communicating with other Devices across a LAN or WLAN.

Domain: A set of one or more Devices governed by a common authority for the purpose of gaining access to one or more WLANs.

Enrollee: A Device seeking to join a WLAN Domain. Once an Enrollee obtains a valid credential, it becomes a Member.

In-band: Data transfer using the WLAN communication channel.

IWSC: Wi-Fi Simple Configuration for IBSS.

Limited UI Device: – A device that has no keypad, but may have a display.

Member: A WLAN Device possessing Domain credentials.

NFC: Near Field Communication, a short-range wireless communication technology.

Out-of-band: Data transfer using a communication channel other than the WLAN.

Push Button Configuration (PBC): A configuration method triggered by pressing a physical or logical button on the Enrollee and on the Registrar.

Registrar: An entity with the authority to issue and revoke Domain Credentials.

Registration Protocol: A Registration Protocol is an in-band protocol to assign a Credential to the Enrollee.

Rich UI Device: A device that has a keypad to be able to accept PIN entry by the user. It may also have a display.

Simultaneous Multi-user Push Button Configuration (SMPBC): A variation of PBC that allows multiple users to be enrolled with fewer user operations.

1.3. References

1. IEEE Std 802.11–2007 IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks-Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.
2. IEEE Std 802.11k–2008 IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Radio Resource Measurement.

2. Architecture for Ad-hoc Setup

2.1. Use Cases

Ad-hoc use cases can be classified into two categories: Initial setup of a new Ad-hoc network and subsequent operation of an Ad-hoc network.

2.1.1. Initial Setup of a new Ad-hoc Network

Context 1 (PBC): the user buys a new printer and would like to allow his/her guests to use this printer without the need to connect to the office network. The user has a cell phone that he/she wants to connect to this printer to support anonymous printing. This user prioritizes convenience over security, so decides to use the push button configuration method for setting up between the printer and the cell phone.

Setup steps

1. User presses the PBC button on the printer.
2. User presses the PBC button on the cell phone.
3. The printer and the cell phone display the progress of the PBC method on their respective user interfaces. Upon completion of the protocol, both indicate “connection success”.

Context 2 (PIN Random Generated): the user goes to a stadium with his/her friends. They take pictures and notes using cell phones with camera functionality and input functionality. They would like to share the pictures only with their friends. They prioritize security to create a limited friends network, so decide to use PIN for validation.

Setup steps

1. User activates “Wi-Fi IBSS Setup” on their cell phone.
2. Another user activates “Wi-Fi IBSS Setup” on their cell phone also.
3. The devices discover each other and determine roles for operation.
4. Based on the determined roles, one device displays a PIN number for setting up.
5. The other device prompts the user to enter the same PIN number.
6. The cell phones display the setup progress, and upon successful completion of the protocol, both devices indicate “connection success”.

Context 3 (*NFC*): The user has a cell phone with an NFC interface and wants to use a wireless kiosk printer to print images stored on the phone. The kiosk printer operator can only accept secure network provisioning methods and has decided to offer NFC out-of-band method for its simplicity.

Setup Steps

1. User touches their cell phone against the kiosk printer (which may include activation of the printer, if it was in low-power mode).
2. The printer exchanges WLAN configuration and printing profile information with the cell phone.
3. The user selects images for printing and sends the images to the printer for printing.

2.1.2. Subsequent operation of an Ad-hoc Network

Context 1 (*SMPBC*): a party with several members goes to a theme park. One person asks for a stranger to take a picture using a party member's camera. After taking the picture, the camera's owner offers to share it through SMPBC, the others then take their cameras out of their pocket. The owner chooses SMPBC mode as an initiator and the others choose SMPBC mode as followers to set up an Ad-hoc connection, so as to be able to exchange the picture among themselves. After some time, the number of devices in the SMPBC appears on the owner's camera display, and the owner realizes that an Ad-hoc network has successfully been created, and the picture can now be shared.

Setup Steps

1. One of party members chooses the SMPBC mode as an initiator using the user interface on his camera, Camera A.
2. The other members each choose the SMPBC mode as followers on their cameras, Camera B and Camera C.
3. The setup process begins without any Session Overlap having occurred.
4. The three cameras are successfully joined to the same network and the Camera A displays the number of members on its user interface.

Context 2 (*PIN*): the user buys a new projector and would like to share this projector, which is deployed in a shared meeting space. This meeting space will be used by various project teams, so this user prioritizes security for setting up projector access for this meeting.

Setup Steps

1. Meeting owner turns on the projector and the projector displays a meeting PIN number for setting up.
2. Meeting owner sets up this meeting network between his/her laptop PC and the projector by inputting the displayed PIN on his/her laptop PC.
3. Meeting members come into the meeting room.
4. They turn on their laptop PC.

5. Meeting owner decides to allow members' laptop PCs into the meeting network and the projector displays a meeting PIN number for adding members.

6. Each meeting member activates Wi-Fi IBSS Setup on their laptop PC and inputs the same PIN number to join the meeting network.

7. Meeting owner's laptop PC and each member's laptop PC display the progress of the PIN setup on their respective user interfaces. Upon completion of the protocol, both indicate "connection successful".

Context 3 (*NFC*): A user wants to join a multi-player video game that two other players have already started after wirelessly connecting their video game devices. So as to not interrupt the two players, the new user decides to use the NFC interface to connect to the existing wireless network.

Setup Steps

1. The user turns on his/her video game device and touches it against the device of one of the existing players.

2. Both devices discover their status and the new player's device receives the WLAN configuration from the existing player's device.

3. The user joins the network and enjoys the multi-player game with the other players.

2.1.3. Use cases from the view point of Device and Network status

The above use cases are classified into five types from the view point of the status of the devices and the Ad-hoc network.

This classification will be used as a baseline criterion for this protocol in later sections.

Table 1: Use Cases

Use case	Device A status	Device B status	Basic Actions
1	NOT IBSS Member	NOT IBSS Member	New IBSS is created with both A and B as the first members
2	NOT IBSS Member	IBSS 2 Member	Device A joins IBSS 2
3	IBSS 1 Member	NOT IBSS Member	Device B joins IBSS 1
4	IBSS 1 Member	IBSS 1 Member	No Action
5	IBSS 1 Member	IBSS 2 Member	No action without user input

Use case 1 will occur when device A and device B begin the setup up process.

Use cases 2 and 3 will occur when one device is already deployed in an Ad-hoc network, and the other device wishes to become a member of that same Ad-hoc network.

Use case 4 will occur when both devices are already members of the same IBSS network and a user attempts to join this existing network.

Use case 5 will occur when both devices are members of different IBSS network and the users attempt to join the other IBSS network. User input is required to explicitly leave a network since the two networks cannot be directly joined.

2.1.4. User Feedback

2.1.4.1. Protocol Initiation

When the user wishes to connect to a network or other device, he/she will not necessarily care or know what type of network is to be connected to. This network may be an IBSS Ad-hoc network, or it may be some other type of network such as a conventional BSS infrastructure network, or a mesh network.

Therefore, where a device has a UI that will allow text display, it is recommended to show the user the network or device names available to connect to (friendly names, rather than MAC addresses), and the actual type of connection may be secondary or hidden. The user may select the desired connection, and the appropriate protocol (WSC, Wi-Fi IBSS, etc) may be initiated accordingly.

For devices with a minimal UI using PBC, in this case it may not be possible to display device or network names, and the protocol may be initiated with whichever other device(s) also initiate PBC at the same time. Again, the appropriate protocol (WPS, Wi-Fi IBSS, etc) may be selected automatically.

2.1.4.2. Protocol Completion

Each device shall indicate the status of the configuration to the user through a user interface, and provide a clear indication of the protocol success or failure, for each supported usage model.

For devices implementing PBC, the requirements of section 10.4 in the Wi-Fi Simple Configuration specification shall be applicable.

2.2. Functional Model and Interfaces

Wi-Fi IBSS devices implement the following functional elements to support the secure setup of an IBSS network:

- IEEE 802.11 STA (IBSS)
- Wi-Fi IBSS Discovery

- IWSC Enrollee
- IWSC Registrar
- WPA™ Supplicant
- WPA Authenticator

Figure 1 illustrates the functional elements and their associated interfaces.

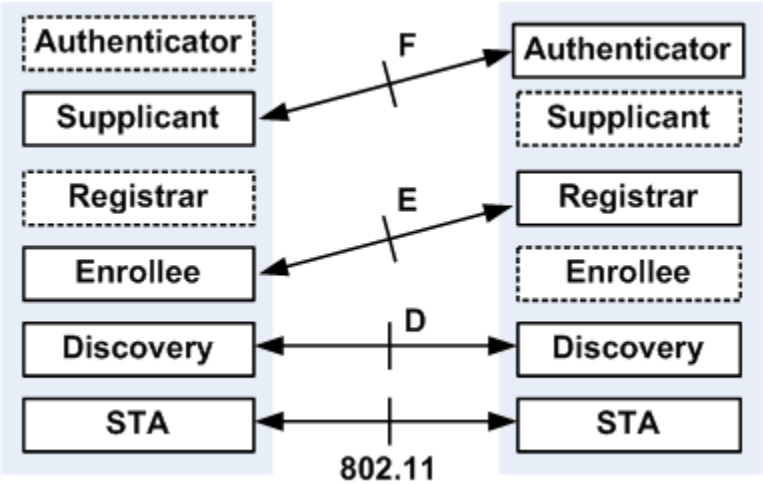

Figure 1: Components and Interfaces

This specification does not preclude a Wi-Fi IBSS device from supporting other modes of operation and other functional elements. Such operation is out of scope of this specification.

2.2.1. Functional Elements

2.2.1.1. IEEE 802.11 STA

Wi-Fi IBSS devices are IEEE 802.11 STA that use the protocol mechanisms described herein (D and E interfaces) to configure the network operation. The extensions specifically extend the WPS process and protocol messages to support IBSS.

The setup process defined herein establishes the network and security configuration of a device. IEEE 802.11 security is used after discovery and enrollment to support RSNA security of the communications using AES-CCMP. The IEEE 802.11 RSNA establishment procedure (4-way handshake) is required for each communicating device to complete the initialization of the device-to-device communications.

2.2.1.2. Discovery

The Wi-Fi IBSS Discovery functional element enhances IEEE 802.11 operation by adding procedures and information elements to standard 802.11 management and data frames to support the discovery of peer devices. The discovery includes the determination of the subsequent role of the device when the WPS enrollment process is initiated (interface E).

Discovery is used by a Wi-Fi IBSS STA to connect to a single peer device or an existing Wi-Fi IBSS initiated network. The Discovery component implements Interface D by:

1. Controlling the IBSS STA functionality and alternating between:
    a. Scanning for a peer Wi-Fi IBSS device that is acting as a selected Registrar.
    b. Announcing a new Wi-Fi IBSS network as a selected Registrar
2. The D interface discovers peer Wi-Fi IBSS devices and determines if setup should continue by the use of optional Wi-Fi IBSS information elements carried in IEEE 802.11 management frames.
3. Discovery is completed when the Wi-Fi IBSS device has identified an appropriate peer.
    a. If the peer device is a Registrar which sends a probe response with IWSCIE, the device stops Discovery and continues the enrollment process as an Enrollee using the E interface.
    b. If the peer device is an Enrollee which sends a probe request with IWSCIE, the device stops Discovery and continues the enrollment process as a Registrar using the E interface.
4. After the completion of the discovery and device setup the Enrollee device acts as the 802.1X supplicant for subsequent WPA2 key setup (interface F).

2.2.1.3. Enrollee and Registrar

The Enrollee functional element communicates with a Registrar to exchange configuration and security parameters to setup the configuration of a device. Interface E is logically located between the Enrollee and the Registrar and is directly specified by the E interface in the Wi-Fi Simple Configuration specification. Every Wi-Fi IBSS device contains the functional elements for both the Enrollee and the Registrar, but only one of these elements is active at a time. Interface E may include only WLAN communication or it may also include communication across an out-of-band channel. The Wi-Fi Simple Configuration specification includes additional interfaces (M and A) that are not used in this specification.

The Registrar functionality is extended for IBSS with Wi-Fi Protected Setup to optionally provide unique IP addresses to all devices.

2.2.1.4. Supplicant and Authenticator

The Supplicant functional element communicates with an Authenticator to setup the security association for WPA2 security. Every Wi-Fi IBSS device contains the functional elements for both the Supplicant and the Authenticator, but only one of these elements shall be active at a time. The STA with the highest MAC address shall initiate the first 4-Way handshake.

The behavior described herein only describes the selection of the Supplicant and Authenticator for the first 4-Way handshake. All subsequent behavior remains unaltered from the IEEE 802.11.

In an IBSS, a secure link exists between two STAs when both 4-Way Handshakes have completed successfully. The Supplicant and Authenticator 4-Way Handshake state machines interact so the IEEE 802.1X variable portValid is not set to 1 until both 4-Way Handshakes complete.

2.3. Protocol Phases

Protocol Phases consist of four phases to set up devices, as follows:

- *Device Discovery* - Discovery of peer device(s).
- *Role Determination* - The device determines if it is to operate as a Registrar or Enrollee.
- *Select Setup Method* - Select one of the following a setup methods: PBC, SMPBC, PIN or NFC.
- *WPS EAP Registration Protocol* - To start the EAP registration protocol as per Wi-Fi Simple Configuration.

Figure 2 shows these phases.

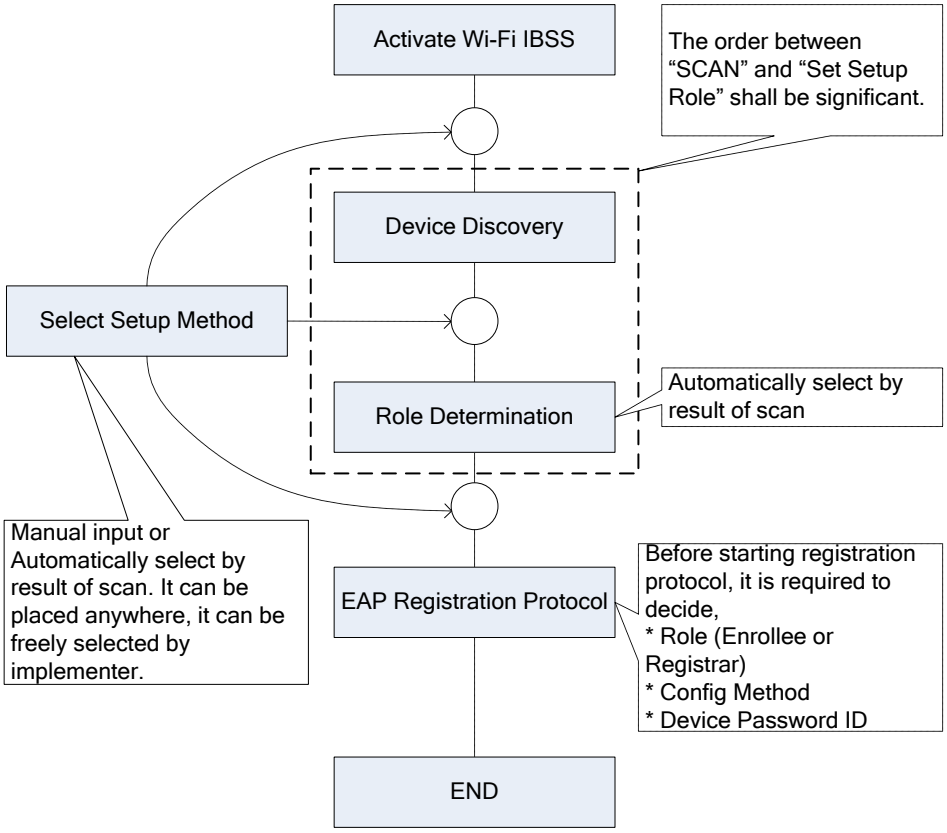

Figure 2: Protocol Phases

2.3.1. Discovery and Role Determination

After Wi-Fi IBSS is activated on a device, the first protocol phase to be triggered is device discovery. The purpose of this phase is to discover a peer device in the vicinity with activated Wi-Fi IBSS mode. This discovery phase is different to the Wi-Fi Simple Configuration discovery phase primarily due to the unique attribute of Ad-hoc networks where devices are considered peers. Users are not required to setup or be aware of which device is the Enrollee and which device is the Registrar and hence the discovery method is enhanced and modified to make discovery and role assignment seamless. Figure 3 shows a detailed flow diagram of the discovery protocol phase.

If a device is a current member of an existing IBSS network, then it takes up a Registrar role and waits for probe requests from an Enrollee. On the other hand, if a device is not a member of an existing IBSS, the device alternates between scanning (operating as an Enrollee) and waiting (operating as a Registrar on a new established initial network) within a specified T1 timer interval.

A device acting as a Registrar in an IBSS network might not be the same device in the network currently sending beacons, hence an Enrollee would not be able to discover that Registrar by simply listening to a beacon from a single device.

Two timers, T1 and T2 are used in the discovery process as shown in Figure 3.

Timer	Value (s)
T1	120 s
T2	Random between 2s and 6s

The following steps describe the discovery flow in more details.

1. After Wi-Fi IBSS is activated, the device starts timer T1 and checks if it is currently a member of an IBSS.
2. If the device is a member of an IBSS, the device becomes a Registrar and sends the Selected Registrar Start Notification action frame to notify active peers in the IBSS, then waits for probe requests.
3. If the device is not a member of an IBSS, then it creates a new base IBSS network, starts timer T2, becomes a Registrar and waits for probe requests.
4. If the device finds the right Enrollee within T2 time interval, Registration protocol phase starts.
5. If T2 time interval expires without finding an Enrollee, device switches to Enrollee mode and starts the scanning process to find a Registrar.
6. If the right Registrar is found, Registration protocol phase starts.
7. If T1 timer did not expire and scanning did not find the right Registrar, then the device rotates back to the Registrar role on the base network.
8. If T1 timer expires before a Registrar or Enrollee is found, then failure is assumed.
9. If the device is a member of an IBSS and Registration protocol phase completes by failure or successful, then it sends the Selected Registrar Finish Notification action frame to notify active peers in the IBSS.

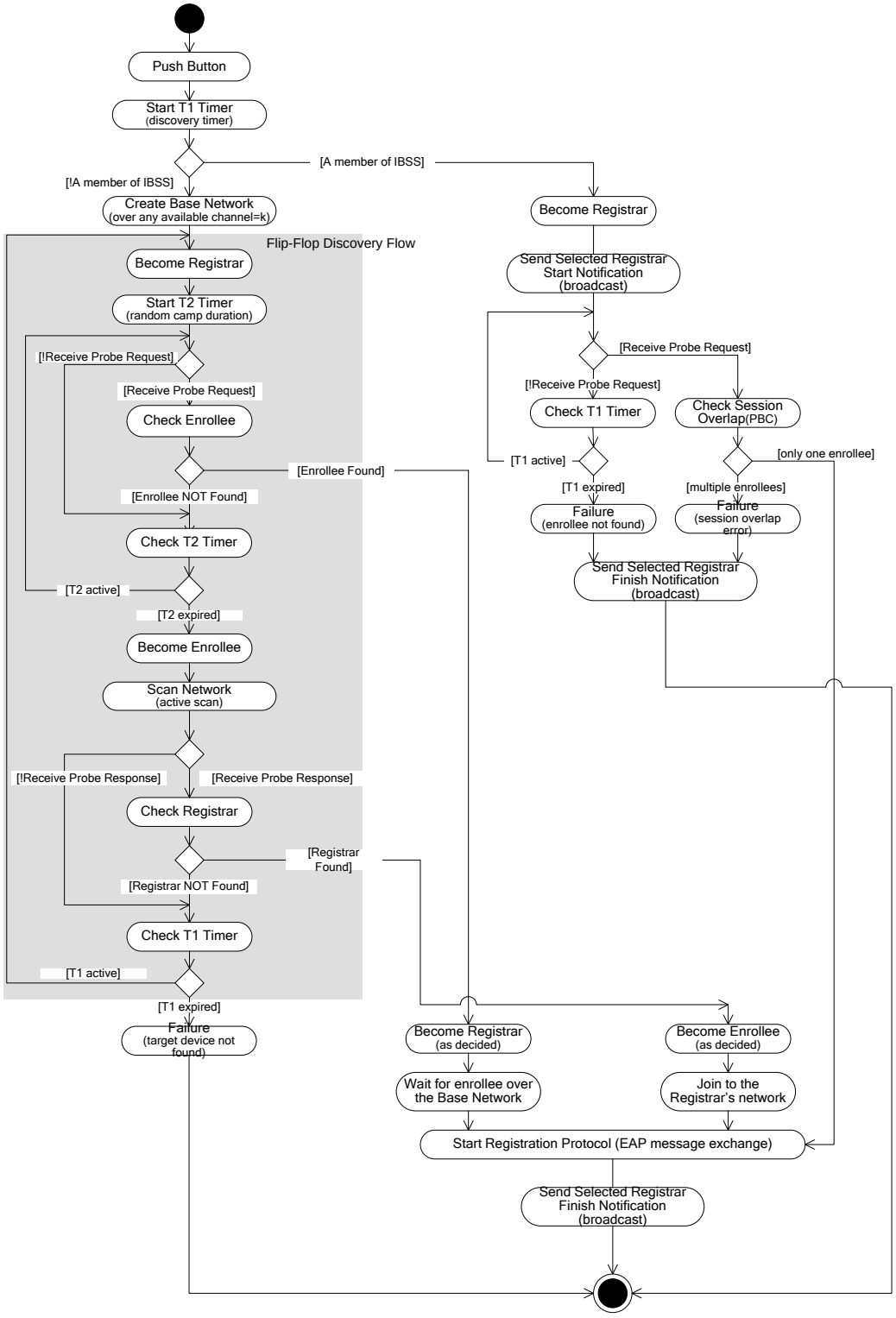

Figure 3: Example Discovery Process

2.3.1.1. Selected Registrar Start/Finish Notification for IBSS member

This section describes using multiple probe responses to find the selected Registrar, and it can use the method of notification for an active Registrar as shown in Figure 4.

When the device in an IBSS network activates the enrollment as the Registrar, the active Registrar shall send a broadcast frame of Selected Registrar Start Notification with the Registrar's MAC address to notify active peers in the IBSS network.

If the active Registrar is not the current beaconing device, then the beaconing device would reply with a probe response containing the MAC address of the active Registrar with Response Type set to Notifier. In this case, the Enrollee can receive a probe response to identify the active Registrar with MAC address even if the selected Registrar is not the current beaconing device. After registration has completed, the active Registrar shall send a broadcast frame of Selected Registrar Finish Notification with the Registrar's MAC address to notify active peers in the IBSS network. If the active peers receive a broadcast frame of the Selected Registrar Finish Notification, the peers shall unset the selected Registrar flags and the current beaconing device would reply with a probe response without the MAC address of the active Registrar.

Security consideration:

An attacker may navigate to connect with a malicious Registrar while the attacker runs as Notifier with a malicious Registrar's MAC address.

In this case, an Enrollee may detect multiple Notifiers which are running on different IBSS networks. To address this vulnerability, if the Enrollee detects multiple Notifiers which announce different MAC addresses of the active Registrars and are running over different IBSS networks, the Enrollee MUST stop the enrollment and signal a "session overlap" error. If the Registrar receives a signal with "session overlap", the Registrar MUST also stop the enrollment.

PBC can be implemented in a variety of ways. On a limited-UI device, it could be implemented using only a button and a LED. The end user should be instructed to check the LED(s) on both the Registrar and the Enrollee in case there is a success indication on one and a failure indication on the other. Users should also verify that the device is connected to the correct network when PBC is used. The user may, for example, print a page on the newly connected printer from another network device, or view content on a media device.

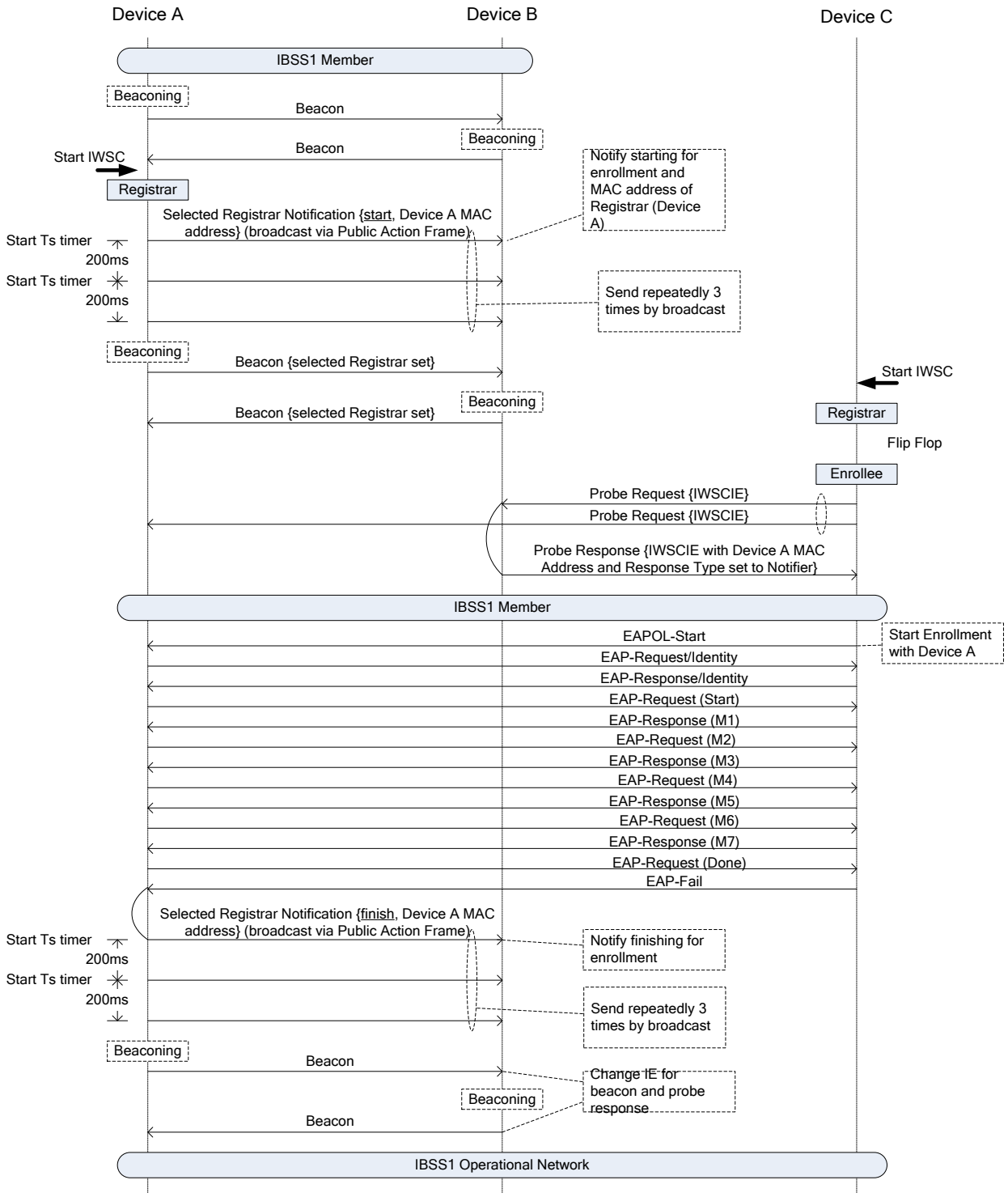

Figure 4: Notification for Active Registrar

2.3.2. Select Setup Method

2.3.2.1. Use Case 1 - Devices not currently IBSS members

This section describes the initial WLAN setup, to create a new Ad-hoc network, as shown in Figure 5.

This first use case is Use case 1 in Table 1, where neither device is already a member of an existing IBSS network. In this case, which device shall be the Registrar is not yet known, and this shall be decided as the initial setup proceeds. The agreed Registrar then issues Credentials directly to an Enrollee.

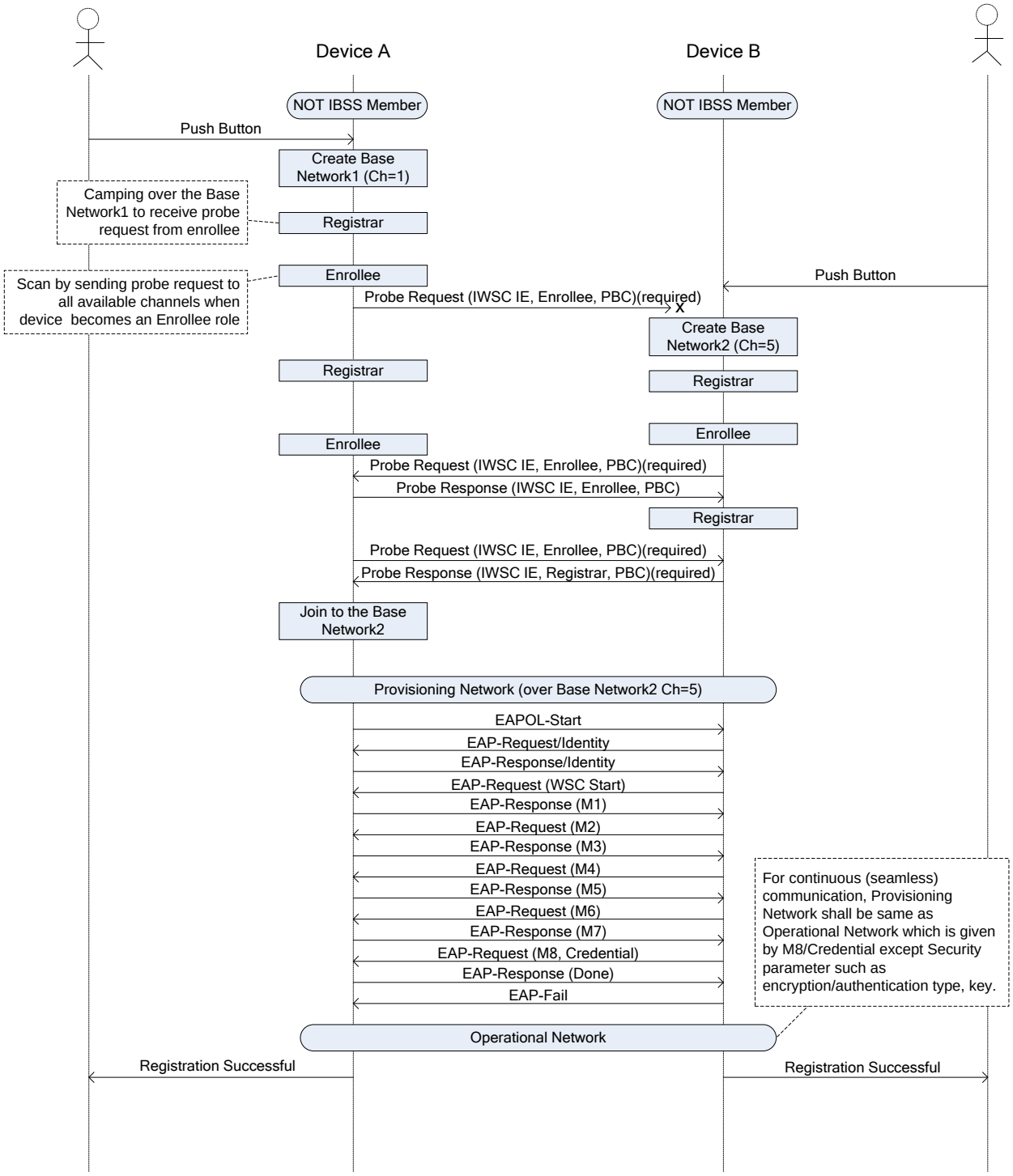

Figure 5: Initial WLAN Setup for Use Case 1.

Initial WLAN Setup Scenario:

1. User presses the PBC button of Device A to activate Wi-Fi IBSS setup, and Device A creates a base network 1 over the first channel to announce or respond its own capability to other devices.

2. Then Device A becomes a Registrar, and Device A sends a beacon that includes IWSCIE with indication Registrar and PBC.

3. User presses the PBC button of Device B to activate Wi-Fi IBSS setup, and Device B creates a base network 2 over the second channel to announce or respond its own capability to other devices. Then Device B becomes a Registrar, and Device B sends a beacon that includes the IWSCIE with indication Registrar and PBC.

4. The devices alternate between Enrollee and Registrar roles. A randomized timer ensures that these device alternations will not be synchronized. When the two devices are in complementary states (one as Enrollee and one as Registrar) the enrollment process can continue.

5. When the device becomes an Enrollee alternative, the device sends a probe request that includes IWSCIE with indication Enrollee and PBC. On the other hand, when the device becomes a Registrar alternative, the device responds with a probe response to a peer's probe request.

6. Device A detects a Registrar's network 2 that is created by Device B. Then Device A joins to the network 2 for registration as Enrollee.

7. EAP Registration protocol will be done over provisioning network 2 (for example channel=5).

8. Finally, both Device A and Device B display the progress of the registration on their respective user interfaces. Upon completion of the protocol, both indicate "registration successful".

For seamless communication, the provisioning network shall be the same as the operational network given by Credential from Device B to Device A, except for security parameters such as encryption and authentication. Otherwise, if operational network parameters such as SSID or channel are different from the provisioning network, it will be necessary to join the new network, and this will take additional time.

2.3.2.2. Use Cases 2 and 3 – One device is an IBSS member

This section describes the process of adding new members to an already established Wi-Fi ad-hoc network. One of the requirements for Wi-Fi IBSS is that any existing member must be capable of adding another device to the network. The challenge that comes with this requirement is that the current node that is sending Beacons in the target IBSS network might not necessarily

be the same as the selected member node (Registrar) for starting the Wi-Fi IBSS process with an Enrollee.

1. Only an active Registrar (Activate Wi-Fi IBSS as in Figure 2) sends Beacons with the IWSC IE.

2. If an activated Registrar receives a Probe Request, it sends a Probe response with IWSC IE.

3. An Enrollee must use active scan for discovering an activated Registrar and that requires actively sending out Probe Requests with IWSC IE. But the Enrollee should still process Beacons for IWSC IE.

4. Registrar sends notification of start/end of an enrollment.

2.3.2.3. In-band Setup

Adding new members using in-band setup can be divided into two sections depending on whether we are adding one member at a time or multiple members (SMPBC)

- Adding Single Member (PIN or PBC)
- Adding Multiple Members (SMPBC)

1. Adding Single Member (PIN or PBC)

This covers the use case when a single member wishes to join an existing IBSS network. The member becomes an Enrollee and picks an existing member of the target IBSS networks and activates Wi-Fi IBSS process. The following are the steps (as shown in Figure 6):

1. Wi-Fi IBSS is activated on both Enrollee and Registrar

2. Enrollee sends a probe request with the appropriate discovery data to discover the target IBSS network

3. Registrar receives the probe request and responds with a probe response that includes the appropriate discovery data.

4. If the Registrar discovery data is in accordance with what the Enrollee is looking for (such as the right WSC method, PIN or PBC) then the Device Discovery Phase is completed (Figure 2).

5. If PIN is used, then the user is prompted to enter the Enrollee's PIN at the Registrar or enter the Registrar's PIN at the Enrollee.

6. The Enrollee connects and initiates 802.1X using the identity "WFA-SimpleConfig-Enrollee-1-0".

7. Enrollee and Registrar exchange messages M1-M8 to provision the Enrollee.

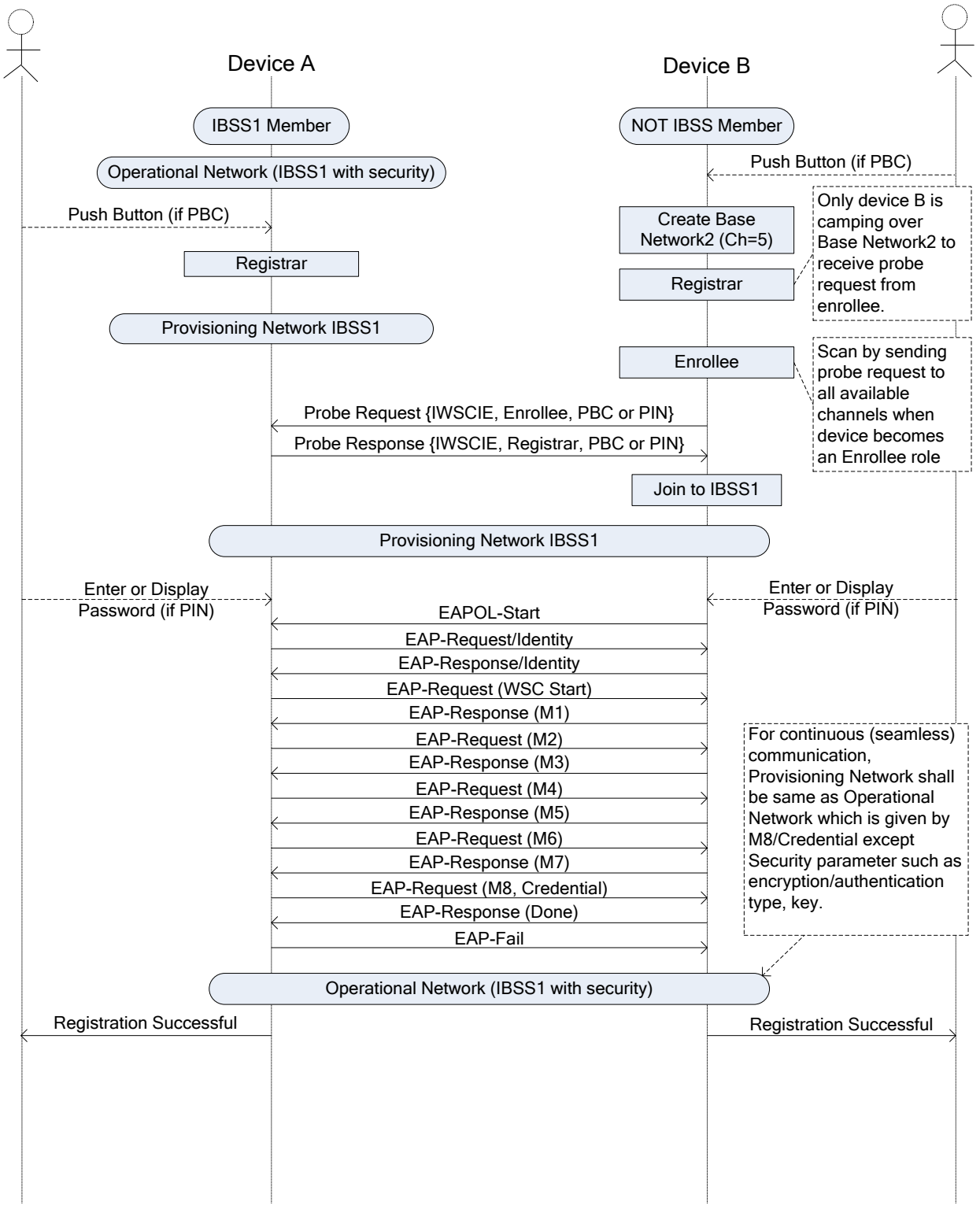

Figure 6: Adding a new member using In-band setup with PIN or PBC.

2. Adding Multiple Members (SMPBC)

   This covers the use case when multiple members wish to create a new IBSS network, requiring only a single choice between SMPBC initiator and its follower through the user interface on each device. The initiator then automatically becomes a Registrar and the followers become Enrollees after this selection. The Enrollees then pick the Registrar and activate IWSC process sequentially. The steps are as follows:

   1. Wi-Fi IBSS is activated on each Enrollee and the Registrar.
   2. Enrollee sends a probe request with the appropriate discovery data to discover the target SMPBC Registrar within a predefined period.
   3. Registrar receives the probe request and responds with a probe response that includes the appropriate discovery data.
   4. If the Registrar discovery data is in accordance with what the Enrollee is looking for (such as the correct WSC method, SMPBC) then the Device Discovery Phase of the Enrollee-side is completed (Figure 2). The Registrar then repeats step 3 with the other Enrollees as long as the received request indicates that the relevant Enrollee is running SMPBC.
   5. The Enrollee connects and initiates 802.1X using the identity “WFA-SimpleConfig-Enrollee-1-0” when the Registrar is ready to run 802.1X.
   6. Enrollee and Registrar exchange messages M1-M8 to provision the Enrollee.
   7. The Registrar repeats the step 5 and 6 with other Enrollees until all Enrollees have completed the registration process.

Refer to the section 3.2 for more details regarding SMPBC.

2.3.3. Wi-Fi Simple Configuration EAP Registration

The Wi-Fi Simple Configuration EAP registration phase is the last protocol phase after the devices have discovered each other, determined which is Registrar and which is Enrollee, and selected a setup method (PBC, PIN, or SMPBC). The IWSC EAP registration phase starts when the Enrollee sends an EAPOL-Start and ends when the Registrar sends an EAP-Fail to the Enrollee as shown in Figure 6. Note that the Enrollee must always be the supplicant, and the registrar must always be the authenticator during a Wi-Fi Simple Configuration EAP registration.

This protocol phase is similar to Wi-Fi Simple Configuration as described in section 7.10 of the Wi-Fi Simple Configuration specification v2.0, with the exception of no support for external Registrars and no APs. Wi-Fi Simple Configuration EAP registration flow is described in detail for each setup method in section 3 of this specification.

3. IBSS Configuration Methods

3.1. PIN Based Setup

There are three primary scenarios for IWSC (Wi-Fi Simple Configuration for IBSS) using the PIN method. The first scenario is between two Rich UI devices that support Wi-Fi IBSS. A Rich UI device such as a PC, cell phone or TV set allows PIN number input using a keypad. The second scenario is between a Rich UI device that supports Wi-Fi IBSS and a Limited UI device that supports Wi-Fi IBSS. In this scenario, it might be difficult to enter the PIN into the Limited UI device such as a camera, wireless headset or wireless display. The PIN is conveyed from a Limited UI device to a Rich UI device via the user or other way such as NFC. The third scenario is between two Limited UI devices that support Wi-Fi IBSS. In this case, other configuration methods such as PBC and NFC must be used instead of the PIN method, because neither device provides a keypad for PIN entry.

Primary scenarios:

1. Rich UI device – Rich UI device
2. Rich UI device– Limited UI device
3. Limited UI device – Limited UI device

Using IWSC, there is no assumption of a role (Enrollee or Registrar) prior to role determination between devices. PIN input by keypad may be required after role determination.

Moreover, to ensure as wide as possible interoperability with a Limited UI device, the PIN number may be entered not only into a Registrar device using Enrollee's PIN, but also into an Enrollee device using Registrar's PIN, according to device capabilities. This specification does not require the user to know which device is a Registrar or an Enrollee.

Device Definitions (Rich UI device/Limited UI device):

In this specification, devices are distinguished by whether they have a keypad for PIN entry or not. A "Config Method" attribute is used to indicate if the device has a keypad or not.

Rich UI device – this device has a keypad and can accept PIN entry by the user. It may also have a display.

Limited UI device – this device has no keypad, but may have a display.

Any IBSS device can become a Registrar, even if it has no keypad capability. In the case of BSS, a Registrar device generally enters a PIN code by reading from an Enrollee device Display or Label. However an IBSS device does not always enter a PIN code in the case of Limited UI capability.

The following are recommendations on the use of the Device Password ID (DPID) in beacons, probe request and probe response.

1. An IBSS Registrar device has a responsibility to decide the DPID in the PIN mode after role negotiation and determination has completed.
2. In beacons and probe request, probe response, an IBSS device with a Rich UI will specify DPID=registrar-specified and (Selected Registrar) Configuration Methods has Keypad and Display bit as default value during Discovery and Role Determination Phase.
    a. If a peer device with Rich UI becomes an Enrollee, both devices proceed to step 3 of section 3.1.1 and the peer device will prompt the user to enter PIN by reading from the Registrar.
    b. If a peer device with Rich UI becomes a Registrar, both devices proceed to step 3 of section 3.1.1 and the peer device will display the PIN.
    c. If a peer device with Limited UI becomes an Enrollee, both devices proceed to step 3 of section 3.1.2.1. The peer device changes the DPID to default(PIN) for probe request to meet with the Registrar UI capability and the Registrar with a Rich UI changes the DPID to default(PIN) for beacon and probe response to meet with the Enrollee UI capability. Then the peer device will display the PIN. The peer device should initiate EAP registration after confirmation that the Registrar with a Rich UI changes the DPID to default(PIN).
    d. If a peer device with Limited UI becomes a Registrar, both devices proceed to step 3 of section 3.1.2.2 and the peer device will display the PIN.
3. In beacons and probe request, probe response, an IBSS device with Limited UI will specify DPID=registrar-specified and (Selected Registrar) Configuration Methods has only the Display bit as default value during Discovery and Role Determination Phase.
    a. If a peer device with a Rich UI becomes an Enrollee, both devices proceed to step 3 of section 3.1.2.2 and the peer device will prompt the user to enter the PIN by reading from a Registrar.
    b. If a peer device with a Rich UI becomes a Registrar, both devices proceed to step 3 of section 3.1.2.1. The peer device changes the DPID to default(PIN) for beacon and probe response to meet with the Enrollee UI capability and the Enrollee with a Limited UI changes the DPID to default(PIN) for probe request to meet with the Registrar UI capability. Then the peer device will prompt the user to enter the PIN by reading from an Enrollee. The Enrollee with a Limited UI device should initiate EAP registration after confirmation that the peer device changes the DPID to default(PIN).
    c. If a peer device also has a Limited UI, both devices will only support Display. In this case, registration must be using PBC.

3.1.1. Rich UI device – Rich UI device

In this scenario, the PIN can be entered at either device. Figure 7 illustrates the setup process.

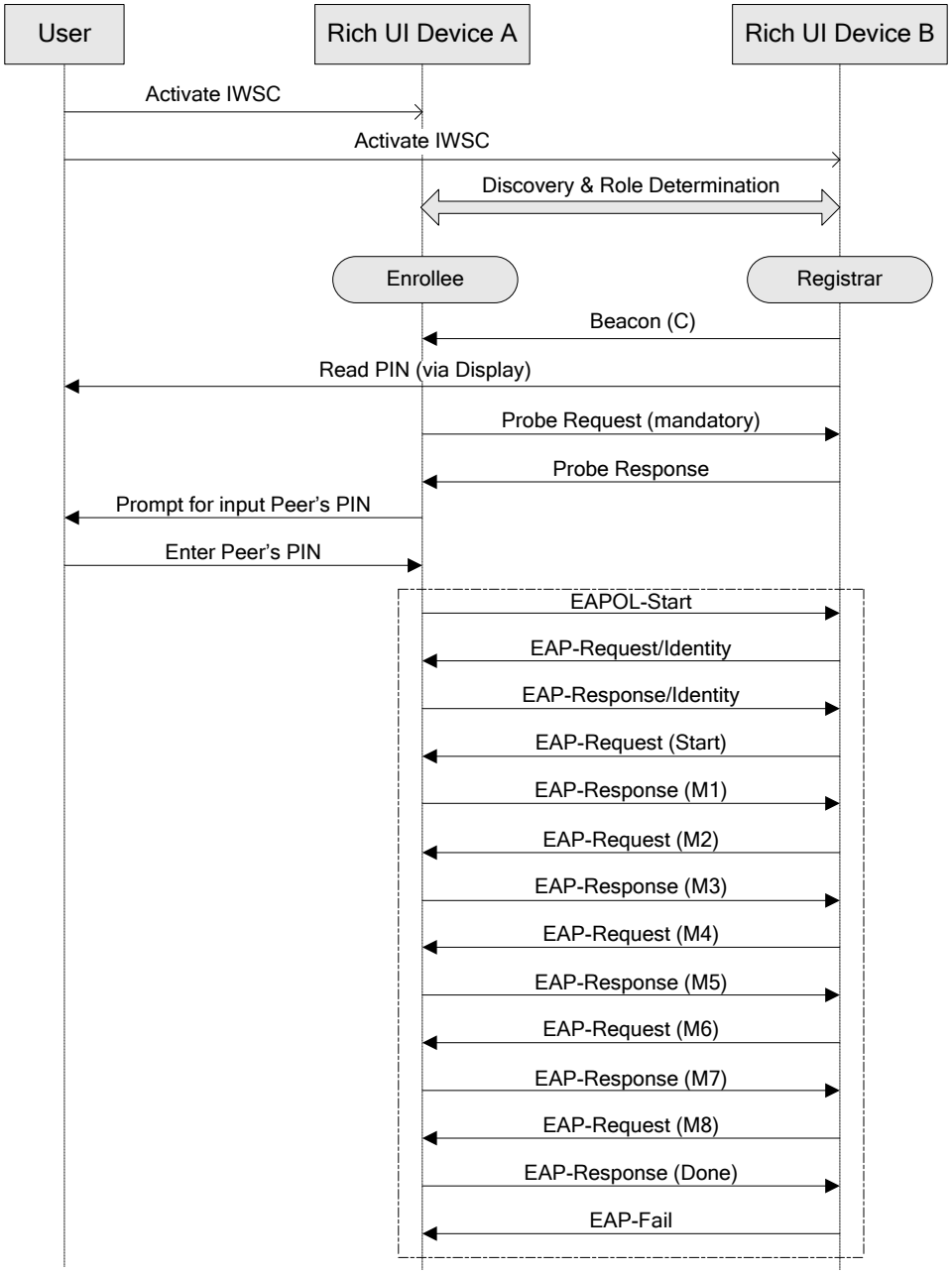

Figure 7: PIN-base Setup of Rich UI Devices

1. The user explicitly activates IWSC on both IWSC enabled devices.
2. [Discovery & Role Determination Phase] Regarding DPID and (Selected Registrar) Config Methods during this phase, refer to step 2 of section 3.1.
3. The Registrar sends out a beacon that includes an Information Element indicating IWSC capability with
    - Selected Registrar set to TRUE

- DPID set to PIN (Registrar-specified)
- Selected Registrar Config Methods set to Display

4. The Registrar generates a fresh PIN for this IWSC provisioning, and shows it to the user via a display. <The Registrar cannot activate Label PIN to avoid security vulnerability.>
5. The Enrollee sends an IWSC probe request to the IBSS WLAN with:
    - Request Type set to Enrollee
    - Config Methods set to Display and Keypad (at least)
    - Device Password ID set to PIN (Registrar-specified).
6. The Registrar sends an IWSC probe response to the Enrollee with
    - Response Type set to Registrar.
    - Selected Registrar Config Methods set to Display
    - Device Password ID set to PIN (Registrar-specified).
7. The Enrollee prompts the user for peer's (Registrar's) PIN entry.
8. The user obtains the PIN from peer (Registrar) via display on the Registrar and enters the PIN into the Enrollee.
   Above step 3 to step 8 may be occurred during discovery.
9. The Enrollee initiates an 802.1X connection using EAPOL-Start message once the PIN is entered.
10. The Registrar sends EAP-Request/Identity message and the Enrollee reply's with name "WFA-SimpleConfig-Enrollee-1-0" as it's EAP-Response/Identity.
11. The Enrollee and Registrar exchange message M1-M8, in accordance with the Registration Protocol. Message M7 includes the preferred settings of the Enrollee. Message M8 includes new wireless settings specified by the Registrar.
12. The Enrollee sends EAP-Response (Done), and the Registrar sends EAP-Fail to indicate the end of the Registration Protocol session.
    Above step 9 to step 12 (framed by dashed line in Figure 7 are same message sequence as Wi-Fi Simple Configuration Specification).
13. The Enrollee and Registrar set their configuration according to the settings delivered in M7 or M8. The Enrollee and Registrar start to connect using the new Credentials with the authentication method supported by both devices.

Mental model mapping:

Wi-Fi IBSS provides an easy way to transfer wireless settings and security keys to new devices. The Enrollee needs the password of the Registrar to make sure that it gets the WLAN keys from an intended device.

Device Password Usage:

Enrollee and Registrar select a configuration method of registration process according to their device capabilities and security policy on their devices. This decision process shall be implemented in the Discovery and Role Determination phase because both devices are able to know each other at that time. To encourage interactions between the user and the device smoothly, Enrollee and Registrar may make use of Beacon and Probe message. This is applicable to any use cases subsequently.

In M1, Enrollee sends DPID=Registrar-specified, Config Methods has Keypad bit set. Registrar checks to see if it knows the Registrar-specified password for the Enrollee. If so, it sends M2 with DPID=Registrar-specified. If not, it sends M2D or WSC_NACK.

Enrollee accepts user input of 8-digit PIN if Config Methods from Registrar does not include Display bit. Enrollee checks the checksum bit and warns user if checksum does not match.

Enrollee accepts user input of 4- or 8-digit PIN if Config Methods from Registrar has Display bit set. If 8-digit, Enrollee checks the checksum bit and warns user if checksum does not match.

User input is allowed prior to registration process.

3.1.2. Rich UI device – Limited UI device

In this scenario, there are two different internal states depending on the result of role determination. The PIN must be entered into a Registrar if the Rich UI device becomes a Registrar after role determination. On the one hand, the PIN must be entered into an Enrollee if the Rich UI device becomes an Enrollee after role determination.

In other words, there are two patterns below according to the result of role determination:

1. Rich UI device (Registrar) – Limited UI device (Enrollee)
2. Limited UI device (Registrar) – Rich UI device (Enrollee)

In the first case, PIN method is implemented in entering Enrollee's PIN into Registrar device. In the second case, PIN method is implemented in entering Registrar's PIN into Enrollee device. From the user point of view, the user always enters PIN into Rich UI device by Limited UI device's PIN regardless the result of role determination.

3.1.2.1. Rich UI device (Registrar) – Limited UI device (Enrollee)

Figure 8 illustrates the process to setup where a Rich UI device operates as a Registrar and a Limited UI device operates as an Enrollee during registration process.

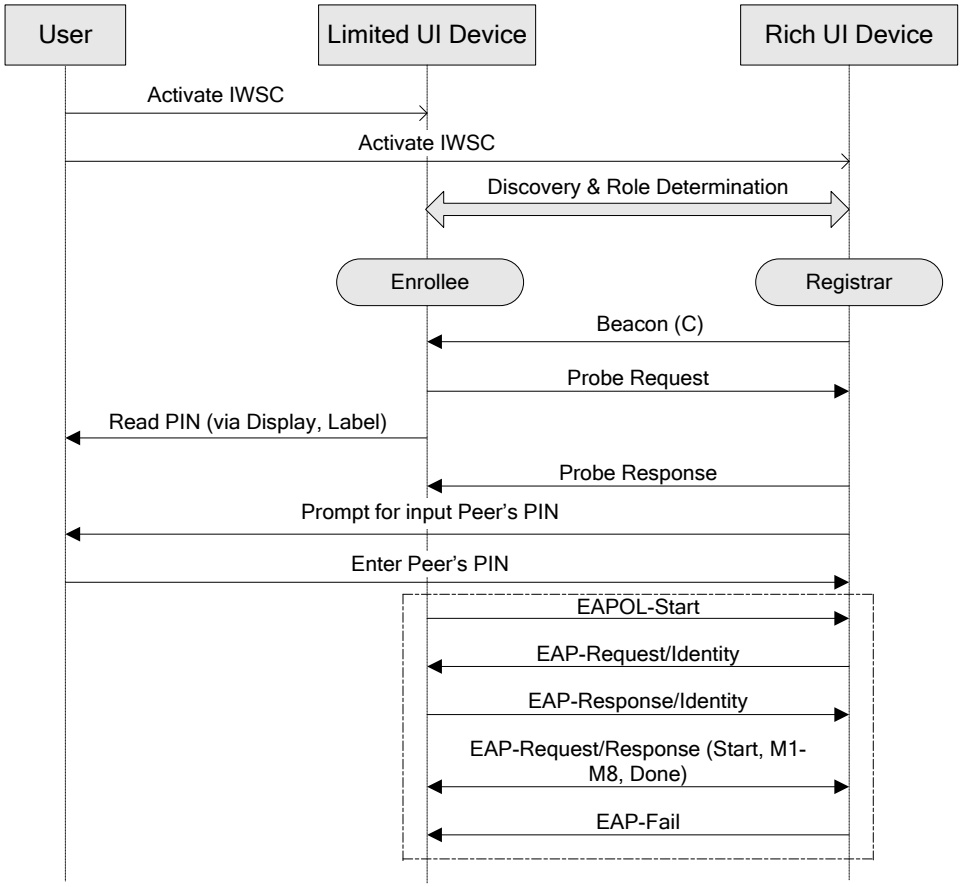

Figure 8: PIN-based Setup with Limited UI Device (Enrollee)

1. The user explicitly activates IWSC on both IWSC enabled devices.
2. [Discovery & Role Determination Phase] Regarding DPID and (Selected Registrar) Config Methods during this phase, refer to step 2 of section 3.1 if the device is Rich UI Device or to step 3 of section 3.1 if the device is Limited UI Device.
3. The Registrar sends out a beacon that includes an Information Element indicating IWSC capability with
    - Selected Registrar to TRUE
    - DPID to PIN (default)
    - Selected Registrar Config Methods to Display and Keypad.
4. The Enrollee sends an IWSC probe request to the IBSS WLAN with
    - Request Type set to Enrollee
    - Config Methods set to Label or Display if supported, but not to Keypad
    - Device Password ID to PIN (default).

5. The Enrollee generates a fresh PIN for this WPS provisioning, and shows it to the user via display if it supports a Display.
6. The Registrar sends an IWSC probe response to the Enrollee with:
    - Response Type set to Registrar
    - Selected Registrar Config Methods to Display and Keypad
    - Device Password ID to PIN (default).
7. The Registrar prompts the user for peer's (Enrollee's) PIN entry.
8. The user obtains the PIN from the Enrollee by reading a label or display on the Enrollee and enters the PIN into the Registrar.
9. The Registrar initiates an 802.1X connection using EAP-Request/Identity message without receiving EAPOL-Start message and the Enrollee reply the name "WFA-SimpleConfig-Enrollee-1-0" as its EAP-Response/Identity. The Enrollee may use EAPOL-Start message to initiate an 802.1X connection.
10. The Enrollee and Registrar exchange message M1-M8, in accordance with the Registration Protocol. Message M7 includes the preferred settings of the Enrollee. Message M8 includes new wireless settings specified by the Registrar.
11. The Enrollee sends EAP-Response (Done), and the Registrar sends EAP-Fail to indicate the end of the Registration Protocol session.
12. The Enrollee and Registrar set their configuration according to the settings delivered in M7 or M8. The Enrollee and Registrar start to connect using its new Credential with the authentication method supported by both devices.

Device Password Usage:

In M1, Enrollee sends DPID=Default (PIN), Config Methods does not include Keypad bit. Registrar accepts user input of PIN. Registrar sends M2 with DPID=Default to Enrollee. User input is allowed prior to registration process.

Registrar accepts user input of 8-digit PIN if Config Methods from Enrollee does not include Display bit. Registrar checks the checksum bit and warns user if checksum does not match.

Registrar accepts user input of 4- or 8-digit PIN if Config Methods from Enrollee has Display bit set. If 8-digit, Registrar checks the checksum bit and warns user if checksum does not match.

3.1.2.2. Limited UI device (Registrar) – Rich UI device (Enrollee)

Figure 9 illustrates the process to setup where a Limited UI device operates as a Registrar and a Rich UI device operates as an Enrollee during registration process.

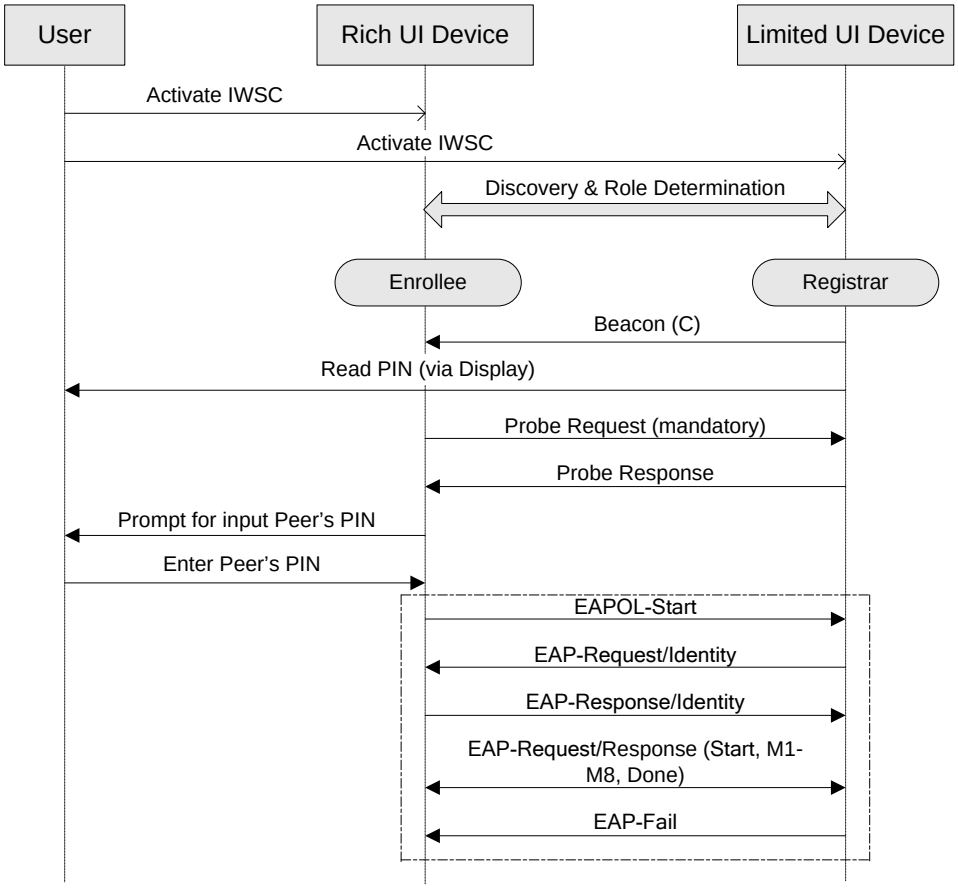

Figure 9: PIN-based Setup with Limited UI Device (Registrar)

1. The user explicitly activates IWSC on both IWSC enabled devices.
2. [Discovery & Role Determination Phase] Regarding DPID and (Selected Registrar) Config Methods during this phase, refer to step 2 of section 3.1 if the device is Rich UI Device or to step 3 of section 3.1 if the device is Limited UI Device.
3. The Registrar sends out a beacon that includes an Information Element indicating IWSC capability with
    - Selected Registrar to TRUE
    - DPID to PIN (Registrar-specified)
    - Selected Registrar Config Methods to Display
4. The Registrar generates a fresh PIN for this IWSC provisioning, and shows it to the user via display.
5. The Enrollee sends an IWSC probe request to the IBSS WLAN with
    - Request Type set to Enrollee,
    - Config Methods to Display and Keypad at least

- Device Password ID to PIN (Registrar-specified).

6. The Registrar sends an IWSC probe response to the Enrollee with
    - Response Type set to Registrar
    - Selected Registrar Config Methods to Display
    - Device Password ID to PIN (Registrar-specified).
7. The Enrollee prompts the user for input Peer's (Registrar's) PIN.
8. The user obtains the PIN from the peer (Registrar) by reading a label or display on the Registrar and enters the PIN into the Enrollee.
9. The Enrollee initiates an 802.1X connection using EAPOL-Start message once entered the PIN.
10. The Registrar sends EAP-Request/Identity message and the Enrollee reply the name "WFA-SimpleConfig-Enrollee-1-0" as its EAP-Response/Identity.
11. The Enrollee and Registrar exchange message M1-M8, in accordance with the Registration Protocol. Message M7 includes the preferred settings of the Enrollee. Message M8 includes new wireless settings specified by the Registrar.
12. The Enrollee sends EAP-Response (Done), and the Registrar sends EAP-Fail to indicate the end of the Registration Protocol session.
13. The Enrollee and Registrar set their configuration according to the settings delivered in M7 or M8. The Enrollee and Registrar start to connect using its new Credential with the authentication method supported by both devices.

Device Password Usage:

In M1, Enrollee sends DPID=Registrar-specified, Config Methods has Keypad bit set. Registrar checks to see if it knows the Registrar-specified password for the Enrollee. If so, it sends M2 with DPID=Registrar-specified. If not, it sends M2D or WSC_NACK.

Enrollee accepts user input of 8-digit PIN if Config Methods from Registrar does not include Display bit. Enrollee checks the checksum bit and warns user if checksum does not match.

Enrollee accepts user input of 4- or 8-digit PIN if Config Methods from Registrar has Display bit set. If 8-digit, Enrollee checks the checksum bit and warns user if checksum does not match.

User input is allowed prior to registration process.

{This Usage is similar to the usage in case of Rich UI devices.}

3.1.3. Limited UI device – Limited UI device

The PIN method is not available in the scenario where both devices are Limited UI devices. In this case, other methods such as PBC and NFC should be used for provisioning.

The IWSC Devices should not choose a PIN-based configuration method if both two devices do not support a keypad as a configuration method during the Discovery and Role Determination.

See the PBC and NFC sections for further information.

3.1.4. Multiple registrations using PIN method with Single PIN

This section describes advanced use cases such as multiple consecutive registrations of multiple Enrollees using single Registrar's PIN.

Use Case:

A meeting is held at a meeting room where members come into the meeting room with their communication devices such as laptop PCs and try to setup an IBSS WLAN network to share the meeting materials. In this case, a *single PIN number* generated by the meeting owner will be used for IBSS WLAN network provisioning by each member without interruption. Each member can enter the same PIN number shown by the meeting owner into their device respectively. The meeting owner can communicate the PIN number orally or write it on a white board.

The meeting owner assumes that the IBSS WLAN Network will consist of two or more devices. The meeting owner starts IWSC with Registrar to accept multiple consecutive registration requests from IWSC devices. The device acting as the Registrar generates a new PIN and displays it to the user. The devices that are trying to connect to this IBSS WLAN Network will use the PIN generated by the Registrar.

Figure 10 illustrates how the process operates with multiple Enrollees.

NOTE: How to decide on a Registrar device out of a member device is out-of-scope of this specification.

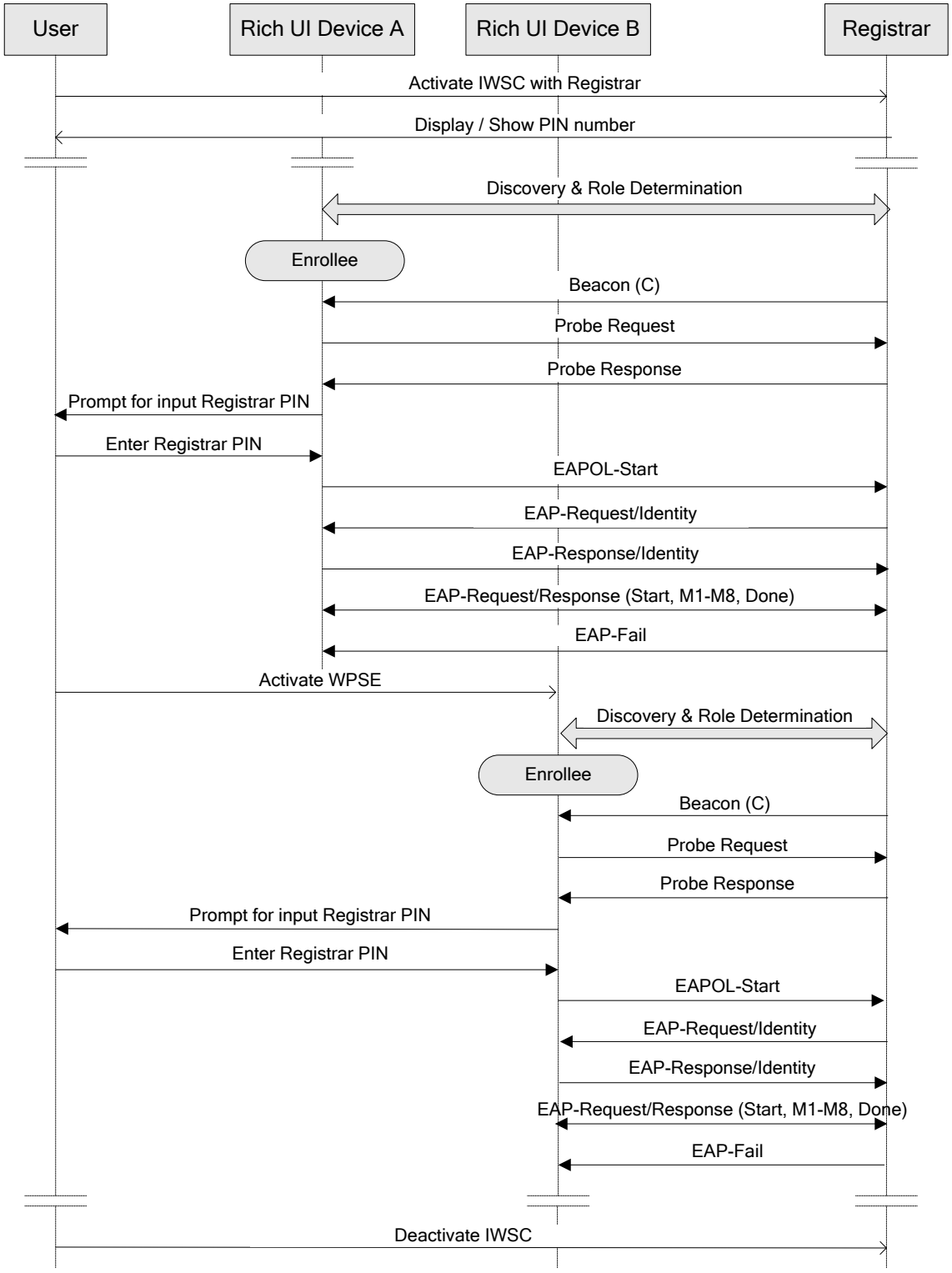

Figure 10: PIN-based Setup with Multiple Registrations

1. The user explicitly activates IWSC with multiple registrations using PIN method on a Registrar device. The user assumes that IWSC process on the Registrar would accept multiple consecutive registration requests from IWSC devices with the PIN generated by the Registrar.
2. The Registrar generates a fresh PIN for this consecutive IWSC provisioning and shows it to the user via the display.
3. The Registrar sends out a beacon that includes an Information Element indicating IWSC capability with
    - Selected Registrar to TRUE,
    - DPID to PIN (Registrar-specified)
    - Selected Registrar Config Methods to Display.
4. The user activates IWSC on a device. The user may enter Registrar's PIN into the device. (*If a device knows for certain in advance that it will function as an Enrollee, it may be activated directly as an Enrollee.)
5. The Enrollee sends an IWSC probe request to the IBSS WLAN with
    - Request Type set to Enrollee,
    - Config Methods set to Display and Keypad at least
    - Device Password ID set to PIN (Registrar-specified).
6. The Registrar sends an IWSC probe response to the Enrollee with
    - Response Type set to Registrar
    - Config Methods to Display
    - Device Password ID to PIN (Registrar-specified).
7. The Enrollee prompts the user to input the Registrar's PIN if it has not been entered by the user yet.
8. The user obtains the PIN from the Registrar by display on the Registrar or other means and enters the PIN into the Enrollee.
9. The Enrollee initiates an 802.1X connection using EAPOL-Start message once entered the PIN.
10. The Registrar sends EAP-Request/Identity message and the Enrollee reply the name "WFA-SimpleConfig-Enrollee-1-0" as its EAP-Response/Identity.
11. The Enrollee and Registrar exchange messages M1-M8, in accordance with the Registration Protocol. Message M7 includes the preferred settings of the Enrollee. Message M8 includes new wireless settings specified by the Registrar.
12. The Enrollee sends EAP-Response (Done), and the Registrar sends EAP-Fail to indicate the end of the Registration Protocol session.

13. The Enrollee sets their configuration according to the settings delivered in M7 or M8. The Enrollee starts to connect with the Registrar using its new Credentials with the authentication method supported by the Registrar.

The user may activate IWSC on another device in parallel while the above process is in progress, or after the above process has completed.

1. The user activates IWSC on another device. The user may enter same Registrar's PIN as previous provisioning into the device. (*If a device knows for certain in advance that it will function as an Enrollee, it may be activated directly as an Enrollee.)
2. The Enrollee sends an IWSC probe request to the IBSS WLAN with
    - Request Type set to Enrollee
    - Config Methods set to Display and Keypad at least
    - Device Password ID set to PIN (Registrar-specified).
3. The Registrar sends an IWSC probe response to the Enrollee with
    - Response Type set to Registrar
    - Config Methods set to Display
    - Device Password ID set to PIN (Registrar-specified).
4. The Enrollee prompts the user to input the Registrar's PIN if it has not been entered by the user yet.
5. The user obtains the PIN from the Registrar by display on the Registrar or other means and enters the PIN into the Enrollee.
6. The Enrollee initiates an 802.1X connection using EAPOL-Start message once entered the PIN.
7. {and so on}
8. The Registrar must deliver the same Credential as previous provisioning to the Enrollee during this registration process.
9. After the registration process, the Enrollee sets their configuration according to the settings delivered in M7 or M8. The Enrollee starts to connect with the Registrar using its new Credential with the authentication method supported by the Registrar.

The user indicates to the Registrar to deactivate the enrollment process when the user stops the enrollment process, otherwise, any Enrollee can be still registered by entering Registrar’s PIN. The Registrar should not include an Information Element indicating IWSC capability with Selected Registrar to TRUE on their beacon after the deactivation.

NOTE: The above two or more registrations may occur in a sequential order or in parallel, depending on the Registrar's processing power.

Device Password Usage:

In M1, Enrollee sends DPID=Registrar-specified, Config Methods has Keypad bit set. Registrar checks to see if it knows the Registrar-specified password for the Enrollee. If so, it sends M2 with DPID=Registrar-specified. If not, it sends M2D or WSC_NACK.

Enrollee accepts user input of 8-digit PIN if Config Methods from Registrar does not include Display bit. Enrollee checks the checksum bit and warns user if checksum does not match.

Enrollee accepts user input of 4- or 8-digit PIN if Config Methods from Registrar has Display bit set. If 8-digit, Enrollee checks the checksum bit and warns user if checksum does not match.

User input is allowed prior to registration process.

Security consideration:

An attacker may try to connect with the Registrar while the Registrar is in this multiple registrations state.

In this state, the Registrar should track multiple failed attempts to authenticate and then enter a lock-down state. This state is signified by not including an Information Element indicating IWSC capability with Selected Registrar to TRUE. To address this vulnerability, if the Registrar tracks multiple failed attempts, the Registrar MUST warn the user.

In this state, the Registrar MUST refuse to run the Registration Protocol in adding member setup mode. This technique protects the Registrar's single PIN against brute force attack by an attacker posing as a new adding member.

3.1.5. Registrar functionality for Limited UI with Label PIN

If the device that ends up being Registrar has a static PIN (say, on a Label), an attacker can learn it much more easily with the reversed order of operations (device password = Registrar PIN). This section describes the availability of a Label PIN for each use case.

The relationship between use cases and allowed the configuration methods are shown in the following table:

Use case	Label PIN	PBC (as reference)
Not IBSS Member	Yes, only if the device is an Enrollee	Yes
IBSS Member	No	Yes

There are two use cases, as follows:

In the first use case, the device is not an IBSS Member and it starts discovery and role determination while flip-flopping in this process.

- If the device becomes a Registrar while listening on flip-flopping, device shall not activate Label PIN, even if it supports Label PIN. It means when device receives probe request at that time, the device shall send a probe response without Label PIN in Config Methods.

- If the device becomes an Enrollee while scanning on flip-flopping, the device may activate Label PIN. It means the device shall send a probe request at that time with Label PIN in Config Methods.

In the second use case, the device is already an IBSS Member and it starts discovery and role determination as Registrar role without flip-flopping. At that time, the device shall not support the PIN method with a Label PIN, it shall only support PBC to add a new member to the existing network.

3.2. Push Button Setup

3.2.1. Objective

This section describes IBSS extensions to the existing Push Button Configuration (PBC) that allows a device with a very simple user interface (for example, a button and a LED) and no additional out-of-band channel to provide Credentials to other PBC-capable devices. PBC requires only a single button press on both devices to be paired, in arbitrary order.

In addition, this section also specifies an option called Simultaneous Multi-user PBC (SMPBC) that enables an IBSS network setup between multiple devices at a time. The SMPBC method simplifies setup by allowing a group to be formed with fewer user interactions.

For more detailed and comprehensive information on the PBC Use Cases for IBSS network and its setup flow including the user actions, refer to sections 2.1 Use Cases and 2.2.1.4 Supplicant and Authenticator.

The Supplicant functional element communicates with an Authenticator to setup the security association for WPA2 security. Every IWSC device contains the functional elements for both the Supplicant and the Authenticator, but only one of these elements shall be active at a time. The STA with the highest MAC address shall initiate the first 4-Way handshake.

3.2.2. User Experience

The PBC method requires the user to press a button on both the devices to be connected together within a two-minute interval called the Walk Time. Figure 11 below illustrates an example of the user actions and relative timings of PBC for the case where the Device A button is pressed first. The case where the Device B button is pressed first is similar, but not shown here. Section 3.2.3 contains a more detailed explanation of the protocol.

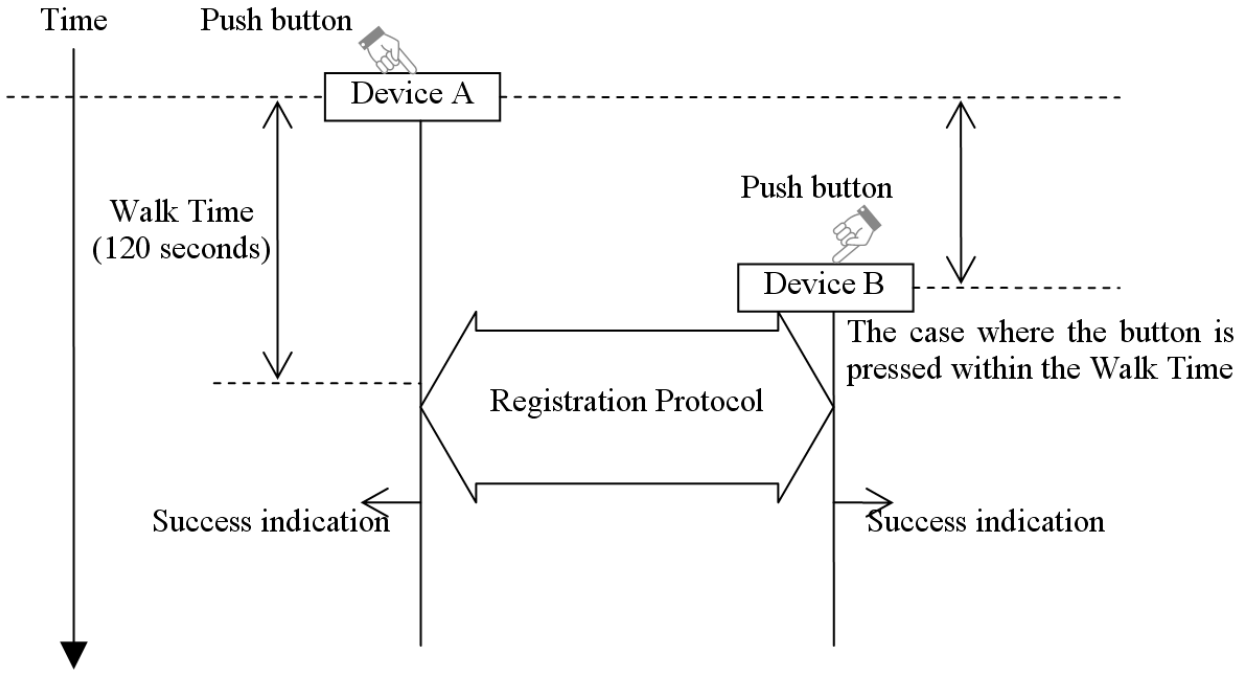

Figure 11: PBC User Actions

In this example, a user first pushes the button on the Device A and then another user pushes the Device B button. The latter user must complete the second button push within the Walk Time period**,** a maximum of 120 seconds, or the Device A times-out and indicates failure. Similarly, if a user first pushes the Device B button, the Device A button must be pushed within the Walk Time or the Device B will indicate failure.

When the SMPBC is activated, it enables the user to setup an IBSS network between multiple devices at a time. SMPBC is defined to create an expected IBSS network without complicated user interaction such as additional button presses or menu choices. Once the SMPBC is selected from the user interface on each device within the specified duration, called Entry Time, all the relevant devices will be registered even after the Entry Time period has expired, which is described in more detail in the following subsection.

3.2.3. PBC Technical Description

Most of the existing 1:1 pairing mechanisms, except Discovery and Role Determination specified in Section 2 and the following definitions, can be applied to the IBSS extension.

Walk Time

Walk Time is equivalent to the timeout duration of the T1 timer shown in Figure 3, Discovery Process. The duration is 120 seconds as defined in the WSC specification.

Monitor Time

If a device is a member of an IBSS network, the device must examine whether probe requests have been received from multiple devices within 120 seconds prior to the PBC button press on the device. The period is called PBC Monitor Time.

Session Overlap

There are three Session Overlap scenarios. The first scenario is that an Enrollee has found multiple Registrars on separate networks after the scanning process. The second scenario is that a Registrar has found multiple Enrollees within the above mentioned Monitor Time.

In addition, the Session Overlap in the SMPBC will be defined later.

Device Password

The Device Password for PBC is '00000000', which is used in the Registration Protocol after the M3 message.

Note: This value is exactly the same as the value specified in the WSC specification.

SMPBC

The objective of this mode is to setup an IBSS network between multiple devices by simply selecting SMPBC initiator or follower on the menu on each device and to create an expected IBSS network at a time. SMPBC, however, only allows one initiator per IBSS network. Once the selection is made on each device, the initiator becomes a Registrar and the followers become Enrollees immediately. This means SMPBC allows multiple devices to join an IBSS network at the same time without any Session Overlap having occurred. The feature becomes available only during the SMPBC open registration period (Entry Time). If multiple Registrars are found during the period, the situation is disallowed and treated as a Session Overlap error (SMPBC specific).

Entry Time is a new term introduced to define the SMPBC setup.

Entry Time

The Registration period begins when the Registrar role is assigned. All devices need to be registered if the Probe Requests and its Responses were exchanged during the Entry Time (even after the period has expired). The Entry Time value may depend on the number of devices, however, it is recommended that the Entry Time value is 15seconds for up to 15 devices.

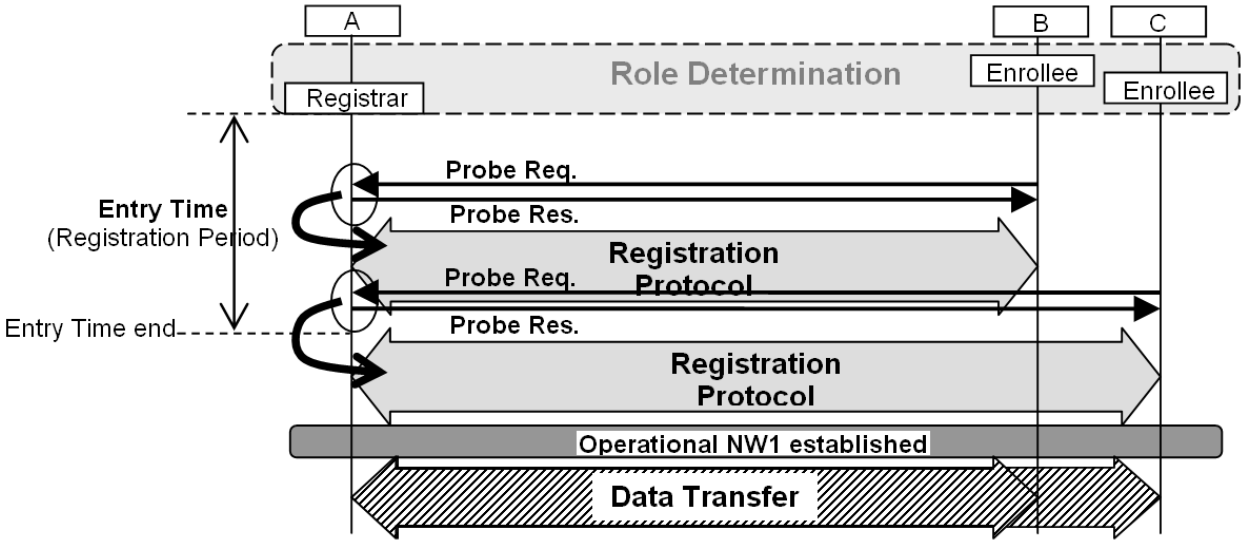

Figure 12: Setup Operation Overview

Preconditions

If a device supports SMPBC, it must meet the following minimum requirements.

To initiate the SMPBC mode, a user who wants to communicate with other members must first select the initiator role from their menu (or some sort of user interface). Other members then must select the follower role from their user interface within the Entry Time. Once the selection is made on each device, the initiator becomes a Registrar and the followers become Enrollees immediately. Accordingly, the role determinations are completed prior to the expiration of the Entry Time.

When running the SMPBC, any devices that are already connected to a network should be disconnected first, and then begin the registration process as Not IBSS Members.

Registrar creates a New Base Network through the above process.

SMPBC specific registration is permitted only during the Entry Time period.

After the completion of the SMPBC registration process, the existing 1:1 pairing mechanism (Adding New Members) should be used to add members.

Co-existence of PBC and SMPBC

Even if a PBC-based existing registration process happens separately but concurrently to the SMPBC registration, devices will not be able to interact with each other because they both have different Device Password IDs. Besides, even if the devices find each other, it doesn't cause a Session Overlap error as long as they conform to each requirement. Session Overlap must be detected and processed according to the corresponding setup methods.

See Figure 13 for examples of co-existence of PBC and SMPBC.

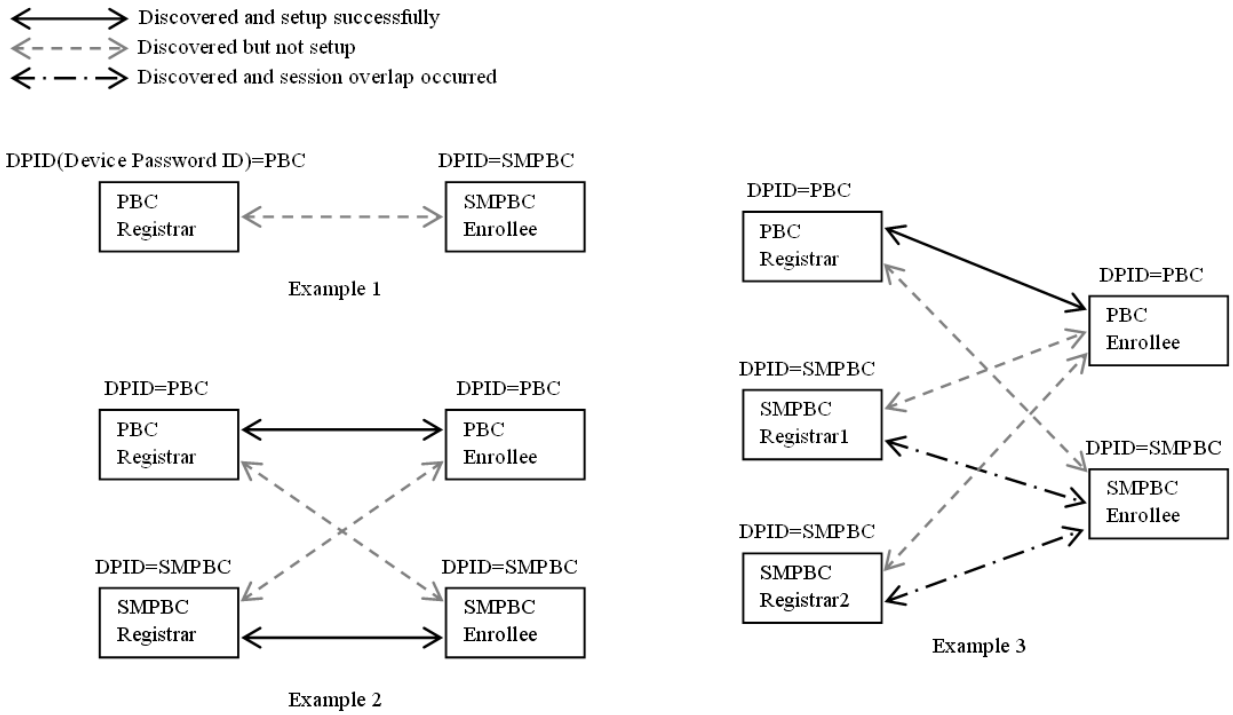

Figure 13: Examples of Co-existence of PBC and SMPBC

3.2.4. SMPBC Operation

A rough outline of the SMPBC Operation Flow is shown in Figure 14. SMPBC specific Discovery Control Flow needs to be added on the basic flow defined in the Core Architecture. For further details of the Discovery Control Flow see Figure 15 (Enrollee-Side) and Figure 16 (Registrar-Side).

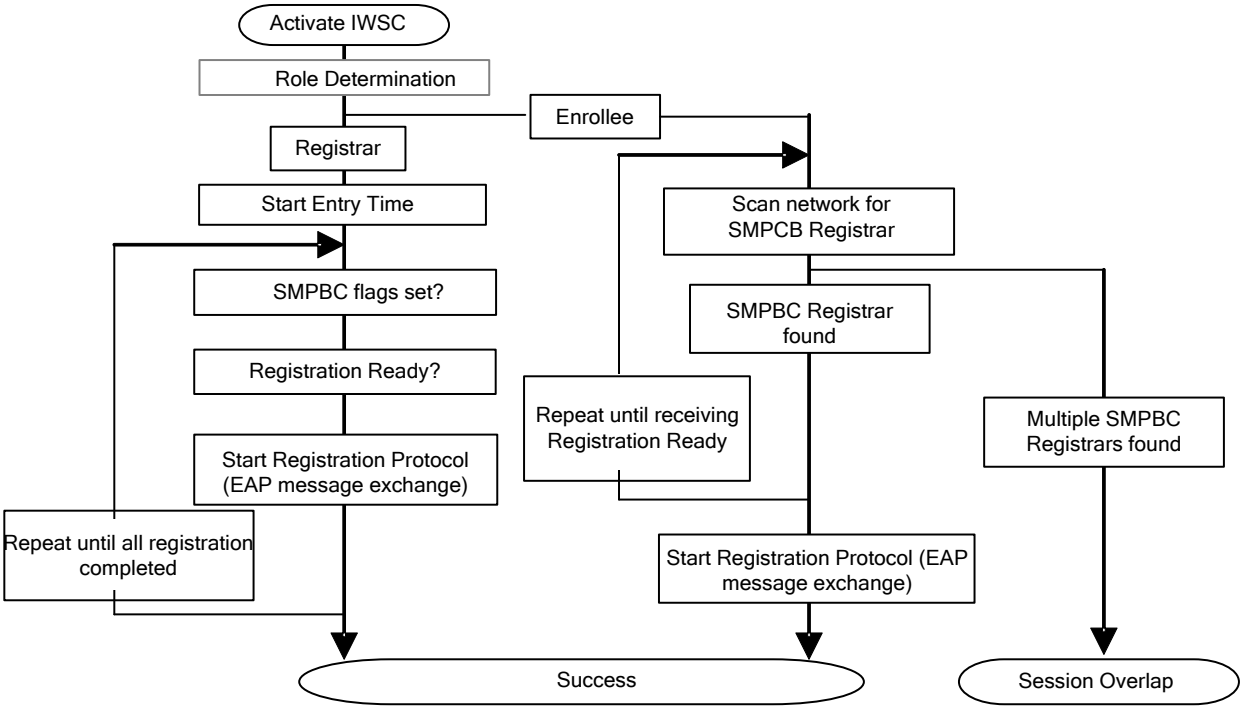

Figure 14: Outline of SMPBC Operation Flow

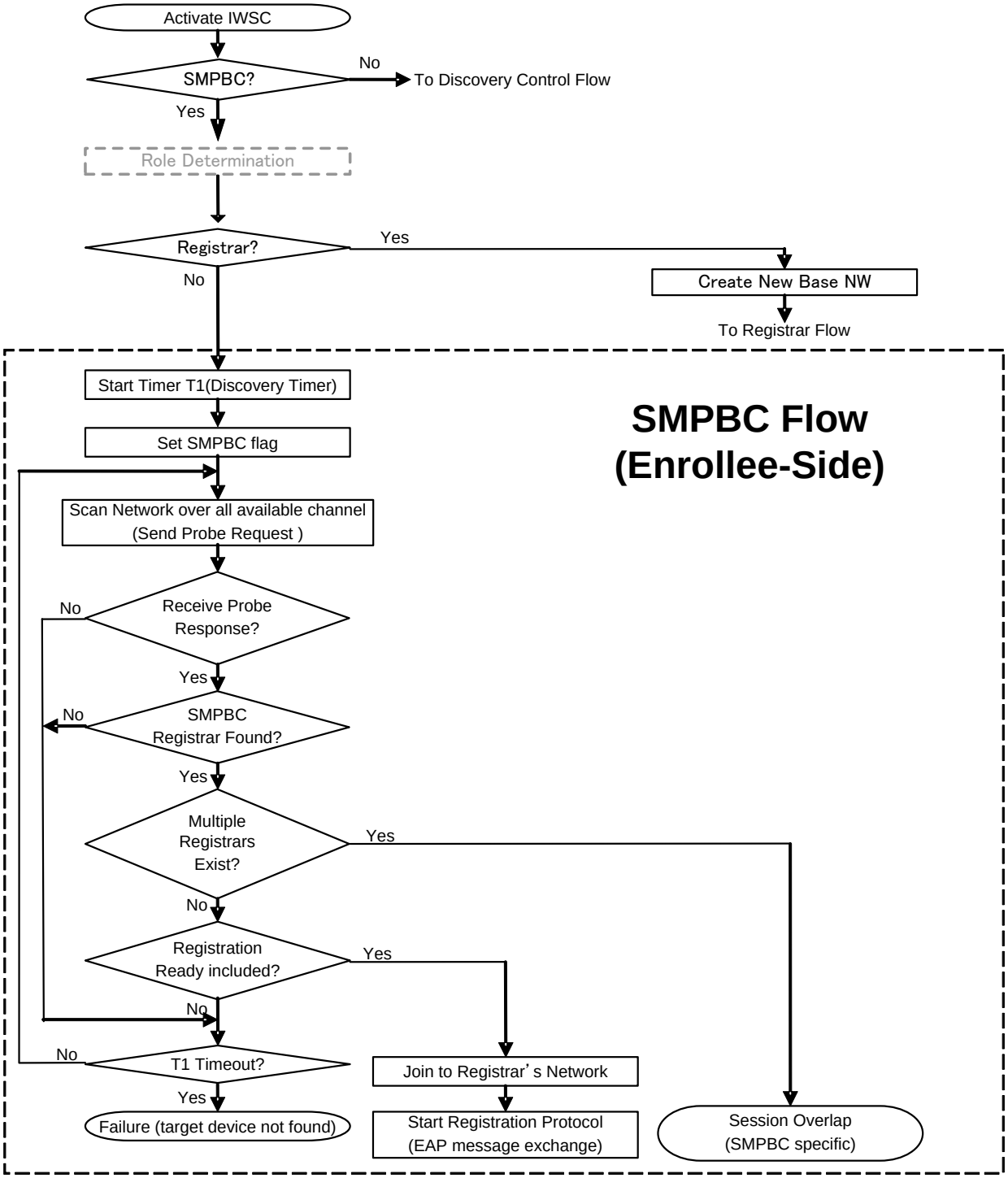

Figure 15: Enrollee-side SMPBC Discovery Control Flow

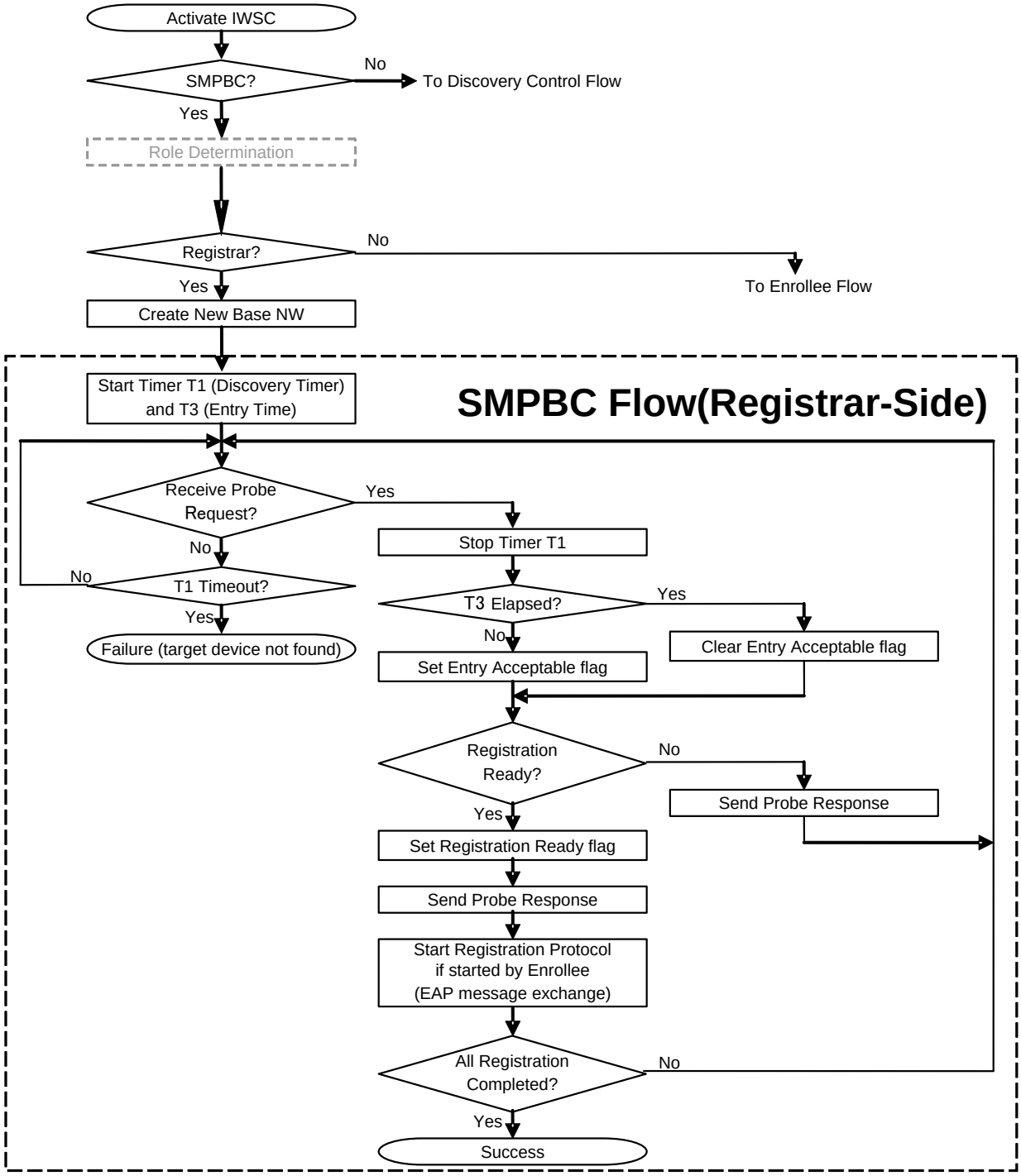

Figure 16: Registrar-side SMPBC Discovery Control Flow

The detailed description of the Discovery Control Flow is as follows:

1. IWSC is activated by choosing SMPBC and the individual roles (initiator and followers).
2. Any devices that are already connected to an IBSS network should be disconnected first, and then begin the registration process as Not IBSS Members.
3. If a user selects the initiator role, then the device becomes a Registrar:
   a. The Registrar creates a Base Network and starts the Entry Time timer when the Registrar role is assigned, then waits for a Probe Request from a SMPBC Enrollee.
   b. If a SMPBC Enrollee is found, the Registrar responds with a Probe Response, containing Entry Acceptable, Registration Ready, SMPBC for Selected Registrar Configuration Methods (0x0880) and SMPBC for Device Password ID (0x0006). Entry Acceptable indicates the Entry Time period is still open.
   c. The Registrar repeats the above mentioned process with other Enrollees as long as the received request includes SMPBC, even after the Entry Time timer has timed out.
4. If a user selects the follower role, the device becomes an Enrollee:
   a. The Enrollee repeatedly scans the network to find a SMPBC Registrar by sending a Probe Request that contains SMPBC as IWSCIE attributes for both Config Methods (0x0880) and Device Password ID (0x0006). SMPBC indicates SMPBC Setup.
   b. Once a SMPBC Registrar has been found and its Probe Response contains Registration Ready that indicates the Registrar is ready to run the Registration Protocol, the Enrollee initiates the Protocol.
   c. If multiple SMPBC Registrars are found, the situation is disallowed and must be treated as a Session Overlap error (SMPBC specific).

An example of the SMPBC setup operation is shown below. In this case, there are three devices attempting to create an IBSS network.

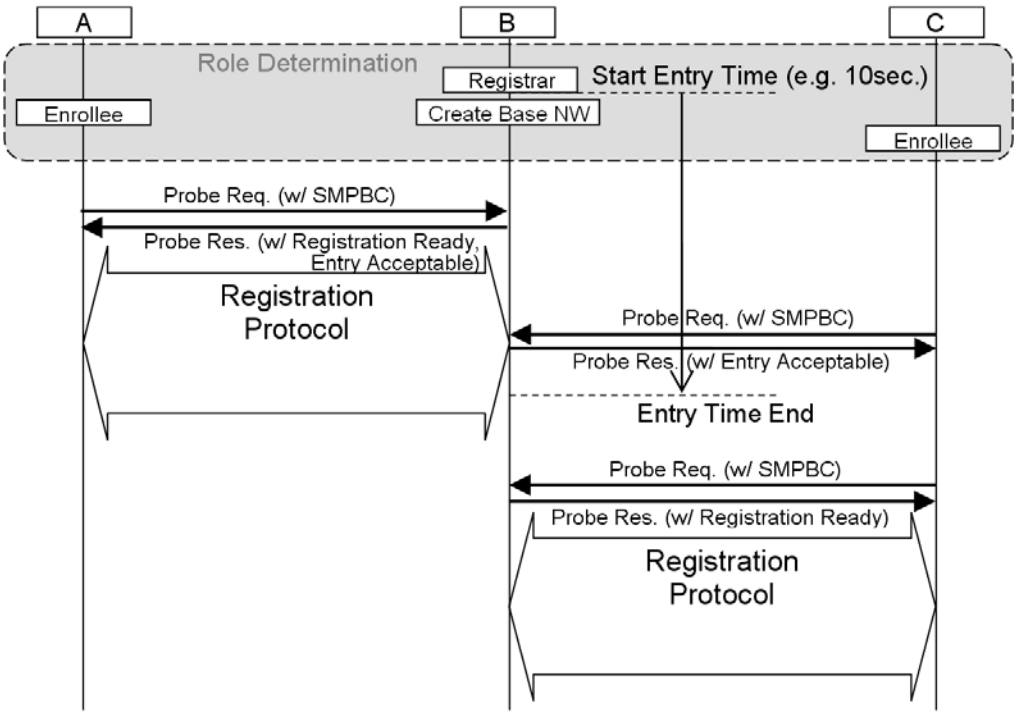

Figure 17: Example for the SMPBC Setup Operation

The overall flow of the SMPBC Setup Operation is as follows:

1. Activate IWSC by choosing SMPBC and the individual roles (initiator and followers) from the user interface (User Action). In this case, the device B user chooses initiator and the device A and C users choose follower respectively.
2. Any devices that are already connected to some network should be first disconnected.
3. The device B becomes a Registrar as a result of the Role Determination and starts the Entry Time timer, then creates Base Network.
4. The device A becomes an Enrollee, and then sends a Probe Request with Request Type set to Enrollee and with both Config Methods and Device Password ID set to SMPBC.
5. The Registrar (device B) sends a Probe Response to the Enrollee (device A) with Response Type set to Registrar and with both Entry Acceptable and Registration Ready set to true because the Entry Time period is still open and the Registrar is ready to run the Registration Protocol.
6. The Enrollee (device A) initiates the Registration Protocol after receiving the above mentioned Probe Response.
7. The device C becomes another Enrollee, then sends a Probe Request with Request Type set to Enrollee and with both Config Methods and Device Password ID set to SMPBC.
8. The Registrar (device B) sends a Probe Response to the Enrollee (device C) with Response Type set to Registrar and with Entry Acceptable set to true. However Registration Ready is not set to true because the registration process for the device A is still under way (unless the Registrar has the ability to run the registration against multiple Enrollees).

9. The Enrollee (device C) sends the Probe Request repeatedly until the Registration Ready is set to true.
10. After the completion of the device A's registration process, the Enrollee (device C) receives a Probe Response with Response Type set to Registrar and with Registration Ready set to true.
11. The Enrollee (device C) initiates the Registration Protocol even after Entry Time has expired (Entry Acceptable is not set to true).
12. The Registrar (device B) finishes the SMPBC setup if all the device registrations are completed.

3.2.5. SMPBC Implementation Requirements

To support the SMPBC Setup, a device must be capable of displaying the number of devices in the SMPBC.

A device may optionally also be capable of displaying the device name of each of the target devices.

A SMPBC Registrar must indicate how many devices are joined through the SMPBC Setup. In addition, the display may also show information regarding the Device Names of the relevant devices. These features will allow users to be easily notified when someone is trying to join their network.

In order to minimize security vulnerabilities and risks, SMPBC-enabled devices must meet the following requirements:

- Entry Time window must be less than or equal to 15sec, that is one-eighth of the Walk Time interval.
- All the security parameters must be deleted every time the device leaves the IBSS network. This means SMPBC only allows devices to establish one-time session and to prevent the reuse of credentials.

3.2.6. SMPBC Security Considerations

SMPBC reduces security risks and vulnerabilities and takes measures to minimize the possibility of someone else gaining access to the network. Allowing overlapping sessions, however, means that the security of this mode would be worse than normal PBC.

SMPBC is more susceptible to an active attack than normal PBC. If, for example, the end user presses the Registrar button first, the attacker has an opportunity to connect to the device during the Entry Time interval.

The end user should be instructed to use this mode for communication among devices located close enough to each other. Users should also verify that the device is connected to the correct network when SMPBC is used. The user may, for example, share a collection of photos with a newly connected camera.

If a device tries to enroll after the Entry time has expired, the Registrar shall reject or ignore that device and should inform the user of an attempted enrollment.

If an Enrollee device detects multiple Registrars with Registration Ready set in the same network, there might be a man-in-the-middle attack from one of the Registrars, because any device can be enrolled to the SMPBC network. At that case, the Enrollee should notify the user of the existence of a possible suspicious attack.

Because of the vulnerabilities to active attack, users who are concerned about the security of their network should be advised to use one of the other IWSC methods rather than SMPBC. Client devices are required to support the PIN-based 1:1 pairing method. Therefore, as long as the network includes at least one Registrar capable of PIN entry, users have a viable option of setting up the network securely.

3.3. NFC Connection Handover

This section details the use of Near Field Communication (NFC) technology for Wi-Fi IBSS network provisioning based on NFC Forum Connection Handover.

3.3.1. Background

Near Field Communication (NFC) is a short range wireless communication technology which enables the exchange of data between devices in close proximity, i.e. when two devices are literally “touched”. The NFC Forum industry association has created a number of specifications for the interoperable use of near field communication technology in electronics devices. The NFC Forum Connection Handover specification defines the structure and sequence of interactions that enable two NFC-enabled devices to establish connectivity on other wireless communication carriers.

The NFC Forum specifications differentiate between NFC Forum Devices and NFC Forum Tags. An NFC Forum Device is able to communicate with an NFC Forum Tag or another NFC Forum Device. An NFC Forum Tag can only be read or written by an NFC Forum Device, two NFC Forum Tags cannot communicate. An NFC Forum Device communicates with a Tag in NFC Forum Reader/Writer Mode, whereas two NFC Forum Devices communicate in NFC Forum Peer Mode. An NFC Forum Device is required to implement both modes.

Note: NFC can only be used to provision a network between two devices at a time, and is not applicable to the SMPBC mode.

3.3.2. User Experience

Setup of Wi-Fi IBSS networking using NFC negotiated handover assumes physical proximity of the devices. A user of an NFC-enabled IBSS device may touch its device to another NFC-enabled IBSS device to setup a new IBSS network, if none of the two devices is currently associated with an IBSS network, or to join an existing IBSS network. To ensure a consistent user experience, all NFC-enabled IBSS devices shall support NFC Forum Peer Mode, thus being

able to perform NFC negotiated handover based IBSS setup with every other NFC-enabled IBSS device.

NFC negotiated handover does not require Wi-Fi communication, i.e. Wi-Fi communication radios may be activated after an NFC negotiated handover succeeded. However, an implementation must be able to finally activate Wi-Fi communication if it supports this behavior.

3.3.3. Carrier Identification

In the context of NFC negotiated handover, Wi-Fi carriers are identified by the media type "application/vnd.wfa.wsc" defined in the Wi-Fi Simple Configuration Specification v2.0. To determine a Wi-Fi IBSS network as defined in this specification, the media type shall be extended with a "mode" parameter set to "ibss", i.e. the media type for an IBSS network shall be specified as "application/vnd.wfa.wsc;mode=ibss".

3.3.4. Connection Handover Operation

NFC Connection Handover is performed between two NFC-enabled IBSS devices if at least one of the devices operates in a context that intentionally leads the device into attempting IBSS connectivity. The context is usually set by a human interaction with the device, such as operating into a "touch to connect" or "touch to share" state.

An NFC-enabled device that initiates a negotiated handover operation is termed a Handover Requester. An NFC-enabled device that reacts on a connection handover request is termed a Handover Selector. If both devices operate in the intentional state then they will equally attempt a connection handover request. The Connection Handover specification requires that receipt of a handover request before sending shall make the receiver assume the role of the Handover Selector and refrain from sending a handover request. If this is impossible, for example if both devices sent handover requests at the same time, an automatic role selection will be performed based on random numbers.

A handover request message transmits a proposal for alternative carriers, each carrier being a suitable choice of connectivity for the requester. Carriers may be proposed with configuration data (as defined in section 10.2.2 of the Wi-Fi Simple Configuration specification v2.0) or without configuration data (as defined in NFC Forum Connection Handover specification); the presence of configuration data determines a carrier's connectivity status.

- An IBSS carrier shall be proposed without configuration data if it is unconditionally available for connecting to an IBSS network configuration that may be returned by the Handover Selector.

- An IBSS carrier shall be proposed with network configuration data if that carrier is presently associated with an IBSS network.

Note that the same carrier may be proposed both with and without configuration data if the Handover Requester is able and willing to disconnect from the IBSS network, if necessary.

A handover select message transmits an alternative carrier with configuration data selected from the alternative carriers received with the handover request. Configuration data may refer to an IBSS network provided by the Handover Requester or the Handover Selector device.

- If a proposed IBSS carrier without configuration data is selected, the handover select message shall contain an IBSS carrier with configuration data for an IBSS network provided by the Handover Selector device. The Handover Requester device shall subsequently connect to that IBSS network.

- If a proposed IBSS carrier with configuration data for an IBSS network provided by the Handover Requester is selected, the handover select message shall contain an IBSS carrier with the same configuration data. However, the MAC address attribute shall be replaced with the MAC address of the Handover Selector. The Handover Selector device shall subsequently connect to that IBSS network.

If the only choice of common connectivity is a proposed IBSS carrier with configuration data but the Handover Selector is presently connected to an IBSS network and unwilling to disconnect, the handover select message shall transmit the IBSS network configuration of the Handover Selector. Both devices then determine that IBSS connectivity is impossible unless one of the devices disconnects from its current IBSS network. Typically this requires an implementation to ask for user guidance and let the user perform a second touch. However, if any of the devices is able to disconnect from its current IBSS network, it may immediately send a new handover request message with proposing an IBSS carrier without configuration data.

3.3.5. Configuration Token

As described in section 10.2 of the Wi-Fi Simple Configuration Specification v2.0, an NFC Forum Tag (named NFC Token), may be used by a Registrar to provide unencrypted WLAN configuration data to Enrollees. This setup method may be used to configure an IBSS network if the user can be guided to first present the NFC Token to the Registrar before presenting it to the Enrollee, or if the user has previously created a Configuration Token with some Registrar and wants to enroll other IBSS devices to the IBSS network controlled by that Registrar.

The Configuration Token must embed the WSC setup data as defined in section 10.2.2 of the Wi-Fi Simple Configuration Specification v2.0 using the Wi-Fi Simple Configuration mime type with the mode parameter “ibss”, i.e. “application/vnd.wfa.wsc;mode=ibss”, and the record shall either be a standalone NDEF message or embedded into a Handover Select message (described as static handover in the NFC Forum Connection Handover specification).

3.3.6. IP Address Assignment and Device Identity Exchange using NFC

NFC Connection Handover may be used for the IP address assignment (section 3.3.6.1) and/or device identity exchange (section 3.3.6.2).

IP address assignment and device identity exchange uses the Auxiliary Data record of the Connection Handover message. This Auxiliary Data record is referenced from the Alternative Carrier record which is used for the IBSS carrier configuration. An Auxiliary Data record used

for IP address assignment or device identity exchange shall use the following media type; “application/vnd.wfa.wsc”.

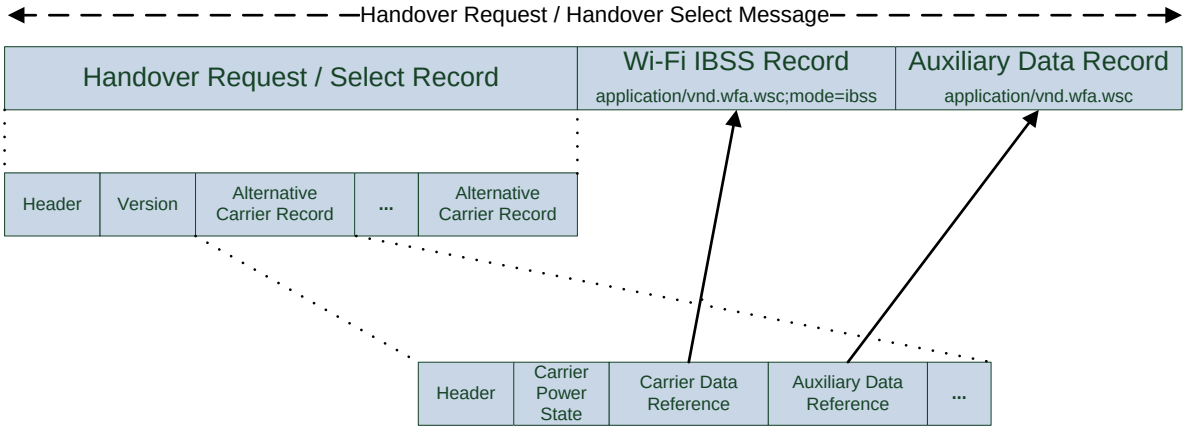

Figure 18: Example for Connection Handover Message Structure

If Connection Handover collision happens, i.e. both touching devices send a Handover Request message, then collision resolution is handled according to the NFC Forum Connection Handover specification. After collision resolution the device that takes the role of the Handover Selector shall ignore all its prior actions (e.g. IP address assignment) related to sending the Handover Request message.

3.3.6.1. IPv4 Address Assignment using NFC

The following IP address assignment methods are supported by the NFC Connection Handover;

- NFC WSC IPv4 Address Assignment; compliant to in-band WSC IPv4 Address Assignment.
- NFC Link Local IPv4 Address Assignment; compliant to RFC3927.

If a device supports an IP address assignment using NFC, then the both of the above methods shall be supported. The NFC WSC IPv4 Address Assignment method is the preferred method to use, because it guarantees unique IP addresses within an IBSS network in all scenarios. The NFC Link Local IPv4 Address Assignment method is reliable only when a device in a Registrar role is aware of the IP addresses of all other devices within the IBSS network.

If a certain IP address assignment method is already used within IBSS network, the later assignments shall use the same method. However, the IP address assignment method may vary between a Wi-Fi in-band and compliant NFC method. For example; if the first assignment is done by the in-band WSC IPv4 method (section 4), then subsequent assignment may use the NFC WSC IPv4 assignment, or vice versa.

When using NFC, the following scenarios for IP address assignment are possible;

Scenario 1 - Handover Requester is not member of IBSS network;

If the Handover Requester is not member of IBSS network, it shall act as an Enrollee during IP address assignment. The Handover Selector shall then act as a Registrar.

An Enrollee shall include the following attributes to the Auxiliary Data Record of the Handover Request message:

- IP Address Configuration Methods; this indicates the supported IP address assignment methods, and it should indicate also supported in-band methods.

Note: The Handover Request message should include also MAC address and optionally other identity parameters as described in section 3.3.6.2.

If the Handover Selector chooses to use NFC WSC IPv4 Address Assignment method, then it shall include the following attributes to the Auxiliary Data Record of the Handover Select message:

- IP Address Configuration Methods; this indicates the chosen IP address assignment method, in this case value shall 0x0010
- Registrar IP Address
- Subnet Mask
- Enrollee IP Address
- Available Submask List

Actual IPv4 address assignment is the same as in the in-band WSC method. The definition and usage of attributes are described in section 4.

If the Handover Selector chooses to use NFC Link Local IPv4 Address Assignment method, and if the Handover Selector i.e. Registrar is not member of any IBSS network then it shall generate random link local IP addresses to itself and Enrollee, and ensure that the addresses are different. However, if the Registrar is already member of an IBSS network, then it shall use existing IP address and only generate a new unique IP address for the Enrollee (the IP address is not used by the any device within the IBSS network). In both cases the Registrar shall include the following attributes to the Auxiliary Data Record of the Handover Select message:

- IP Address Configuration Methods; this indicates the chosen IP address assignment method, in this case value shall 0x0020
- Registrar IP Address
- Enrollee IP Address

If the Handover Selector does not choose any NFC method for the IP address allocation, then Handover Select message shall not include Enrollee IP Address, Subnet Mask and Available Submask List attributes. However, the following attributes are recommended to include in the Handover Select message (Auxiliary Data Record);

- IP Address Configuration Methods; In-band IP address assignment methods that the Enrollee is allowed to use.
- Registrar IP Address; if the Handover Selector has already an IPv4 address, then this attribute should be included, see section 3.3.6.2.

Note: IP Address Configuration Method in above case is needed especially to indicate whether IPv4 or IPv6 addresses are used within IBSS network.

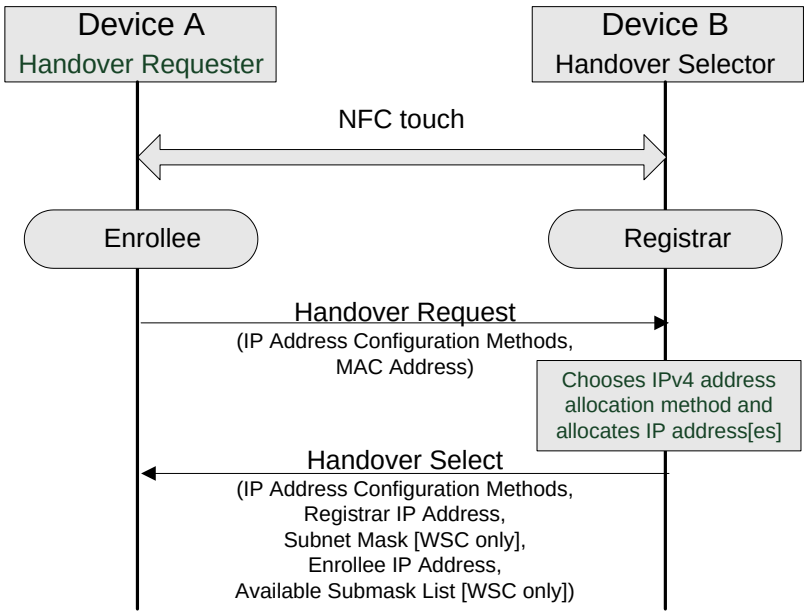

Figure 19: Connection Handover in Scenario 1

Scenario 2 - Handover Requester is member of IBSS network;

If the Handover Requester is already member of IBSS network, it shall act as a Registrar during IP address assignment. In this scenario the Registrar chooses method and assigns an IP address for the Enrollee without knowledge of supported methods by the Enrollee.

If the Handover Requester chooses to use NFC WSC IPv4 Address Assignment method, then it shall include the following attributes to the Auxiliary Data Record of the Handover Request message:

- IP Address Configuration Methods; this indicates the used IP address assignment method, in this case value shall 0x0010
- Registrar IP Address
- Subnet Mask
- Enrollee IP Address

- Available Submask List

Actual IPv4 address assignment is the same as in the in-band WSC method. The definition and usage of attributes are described in section 4.

If the Handover Requester chooses to use NFC Link Local IPv4 Address Assignment method, then it shall generate random link local IP addresses to Enrollee include the following attributes to the Auxiliary Data Record of the Handover Request message:

- IP Address Configuration Methods; this indicates the used IP address assignment method, in this case value shall 0x0020
- Registrar IP Address
- Enrollee IP Address

If the Handover Requester does not choose any NFC method for the IP address allocation, then Handover Request message shall not include Enrollee IP Address, Subnet Mask and Available Submask List attributes. However, the following attributes are recommended to include in the Handover Request message (Auxiliary Data Record);

- IP Address Configuration Methods; In-band IP address assignment methods that the Enrollee is allowed to use.
- Registrar IP Address; if the Handover Selector has already an IPv4 address, then this attribute should be included, see section 3.3.6.2.

Note: IP Address Configuration Method in above case is needed especially to indicate whether IPv4 or IPv6 addresses are used within IBSS network.

The Handover Selector response depends whether it is able to use assigned IP address, and whether it is member of IBSS network.

If the Handover Selector is not member of IBSS network and it is able to use the assigned IP address i.e. it can act as an Enrollee, then it shall send the Handover Select message with the Auxiliary Data record including the IP Address Configuration Methods attribute. This attribute confirms to the Registrar that the Enrollee supports the used assignment method and is able to use the assigned IP address.

- IP Address Configuration Methods; confirms usage of an assigned IP address and only the used assignment method bit shall be set. Other bits shall be set to zero.

If the Handover Selector is not member of IBSS network, but does not support used NFC specific IP address allocation method, then the following attributes are recommended to include in the Handover Select message (Auxiliary Data Record);

- IP Address Configuration Methods; if the Enrollee is able to perform any in-band IP address assignment method allowed by the Registrar, then this attribute is recommended. Only the bit of the in-band allocation method that the Enrollee is going to use shall be set. Other bits shall be set to zero.

If the Handover Selector is also member of IBSS network, then the IP address assignment cannot be performed (both devices have already an IP address). However, if the Handover Selector is member of the same IBSS network as the Handover Requester (SSIDs are the same), then the Handover Selector should send its own IP address using Registrar IP Address attribute within Auxiliary Data Record for the device identity exchange purposes (see section 3.3.6.2). But if the Handover Selector is member of different IBSS network, then Handover Select message shall not include Auxiliary Data Record at all. However, in this case a new Connection Handover may be triggered as described in section 3.3.4 and the Handover Requester shall then act as an Enrollee, and IP address assignment can be made according to scenario 1.

Note: In cases where the Handover Selector does not use the assigned IP address, this IP address shall be assumed to be free in subsequent assignments.

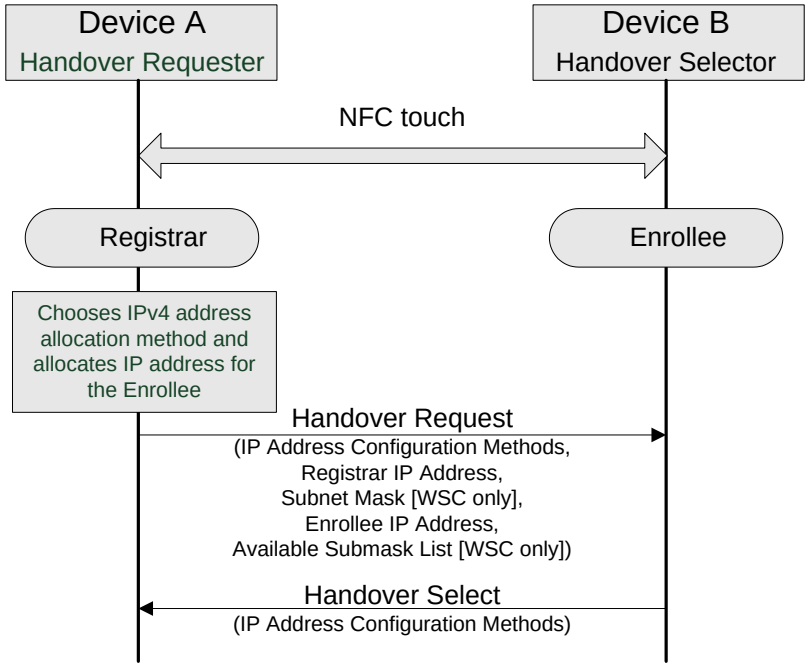

Figure 20: Connection Handover in Scenario 2

3.3.6.2. Device Identity Exchange

Device identity exchange is recommended in the IBSS mode to identify the touched peer device.

The Handover Requester / Selector should include the following attributes on the Auxiliary Data record of the Handover Request / Select message;

- MAC Address - this parameter is recommended to include when the IP address of the device is not available, and if MAC Address is not exchanged within other Connection Handover records, see details from section 3.3.6.1.

- Registrar IP Address - this parameter is recommended to include on specific scenarios as described in section 3.3.6.1.

If device supports device identity exchange over NFC, it shall support also ARP to resolve peer device's IP address from the MAC address.

The same Auxiliary Data record shall be used to carry identity attributes as used for the IP address assignment.

3.4. RSNA Key management in an IBSS Network

This section describes RSN IBSS network operation to improve connectivity between peers.

When the device in an IBSS network starts to setup the security association for WPA security, the device shall be required to find peers to initiate the 4-Way handshake. One option may be confirmed by receiving beacons from devices in the IBSS network, however, it depends on the probability for beaconing. If many devices have already joined the IBSS network, the device may be slower to detect and connect with an expected peer STA. On the other hand, the device can freely join and leave an IBSS network. In an RSN IBSS network, the remaining devices shall be disabled for the IEEE802.1X Controlled Port for a peer STA and deletes the PTKSA to manage RSNA Key when a peer STA completely leaves the IBSS network.

3.4.1. IBSS Device Query

This section describes using public action frames to find the existing IBSS devices in the IBSS network. This functionality is optional as a hint to initiate the 4-Way handshake, but the device is required to recognize and send a response.

In this scenario, the device initiates the 4-Way handshake with the other device after an IBSS Device Query. Figure X illustrates the step.

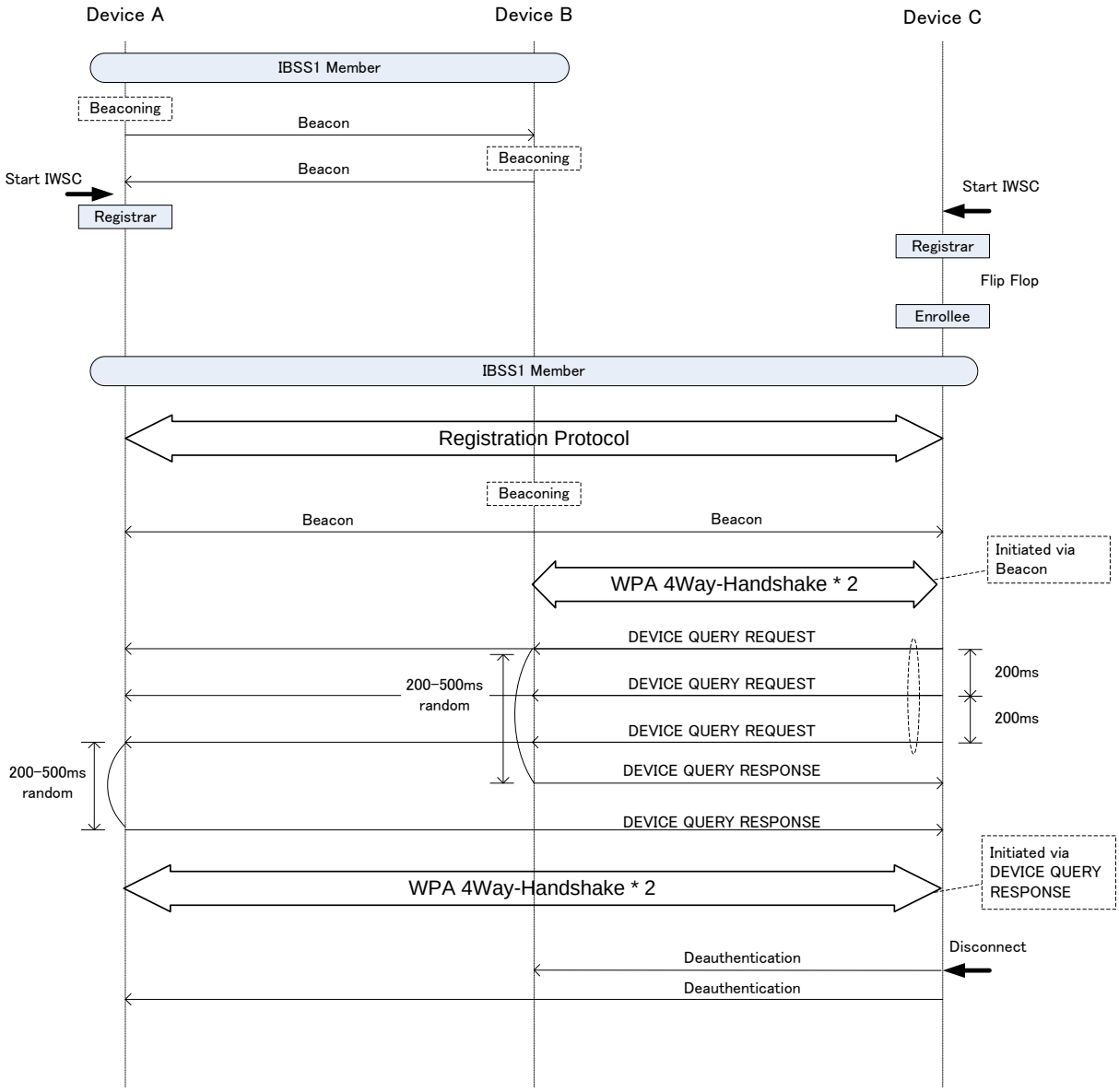

Figure 21: IBSS Device Query Scenario

1. Device C completes EAP registration protocol with Device A in an IBSS network.
2. Device C receives beacon from Device B and initiates WPA 4-Way Handshake with Device B.
3. Device C sends out IBSS Device Query Request via broadcast packet to detect peer devices in the IBSS network.
4. Device A receives IBSS Device Query Request, it replies with IBSS Device Query Response via unicast packet to Device C.
5. Device C can initiate 4-Way handshake with Device A if Device C becomes an Authenticator first.

The IBSS Device Query Request is sent via public action frame with a MAC Address of the Request device. If a device supports IBSS Device Query Request, it shall send out three times via broadcast packet every 200ms. The broadcast packet is assumed to send to the targeted BSSID to avoid response packet congestion. If the broadcast packet with the wildcard BSSID value is transmitted, a peer device may ignore the IBSS Device Query Request.

If a device receives an IBSS Device Query Request, the device shall reply with an IBSS Device Query Response. The IBSS Device Query Response shall send out via public action frame with a MAC Address of the Response device within 200-500ms random time to avoid response packet collision. The new IBSS device can detect peer devices to initiate the 4-Way handshake.

3.4.2. IBSS deauthentication

The deauthentication service is invoked when an existing Open System or Shared Key authentication is to be terminated.

In an RSN IBSS, an IBSS STA is required to recognize Deauthentication frames. Deauthentication results in the IEEE 802.1X Controlled Port for that STA being disabled and deletes the PTKSA.

It is strongly recommended that if the device specifically leaves an RSN IBSS, the device should send out deauthentication frames to manage RSNA key.

4. IP Address Assignment

The mobile nature of IBSS networks complicates the assignment of IP addresses to devices. There will not be a well identified DHCP server. Determining the uniqueness of link local addresses is making zero-config assignment problematic.

It is recommended that IBSS networks implement either:

- IPv6 device unique addresses
- IPv4 addresses assigned using the WSC protocol

The use of IPv6 device unique layer 3 addresses provides a simple means to establish layer 3 communication where IPv6 is supported. The IPv6 would be able to support very large IBSS networks.

A layer 3 IPv4 address may be assigned by the Wi-Fi Simple Configuration protocol. The WSC protocol carries the IP address information in the M8 message of the WSC protocol. This enables the Registrar to coordinate the assignment of an IPv4 address. Every device may act as a registrar and each registrar has a unique set of addresses that it may provide to Enrollees. Assignment of IPv4 addresses by the Registrar is suitable for moderate sized networks.

Devices supporting WSC may determine a peer devices ability to support different mechanisms for IP addresses using the IP Address Configuration Methods data component. The IP Address Configuration Methods data component should be carried in the WSC IE in the Beacons, Probe Requests and Probe Responses.

IP Address Configuration Methods

The IP Address Configuration Methods Data component lists the methods the Enrollee or Registrar supports. The list is a bitwise OR of values from the table below.

Table 2: IP Address Configuration Methods

Value	Configuration Method	Description
0x0001	WSC IPv4 Assignment	Hierarchical IPv4 address assignment using WSC 2.0
0x0002	DHCP IPv4	DHCP IPv4 address assignment. Support indicates the ability of a Registrar to act as a DHCP server and a Enrollee functions as a DHCP client
0x0004	Static IPv4	Static IP address assignment
0x0008	Link Local IPv4	Link Local IP address allocation using RFC3927
0x0010	NFC WSC IPv4 Assignment	Hierarchical IPv4 address assignment using NFC Connection Handover
0x0020	NFC Link Local IPv4	Link Local IP address allocation using NFC Connection Handover
0x0040	IPv6 Device Unique	IPv6 device unique address assignment

The first Registrar in an IBSS network selects one of methods from the IP Address Configuration Methods. It should pick one of the mechanisms advertised by the Enrollee. The confirmed single method is sent in the IP Address Configuration Method field that is included in the M2 and M8 messages from the Registrar to the Enrollee. Once a network configuration is established by the first Registrar the IP Address Configuration Method should not change and the advertised values should be set to a single value that matches the established IBSS configuration method.

IP Address Configuration Method

This attribute contains a specific value from IP Address Configuration Methods table for the Registrar to use.

4.1. WSC Assignment of IP Addresses

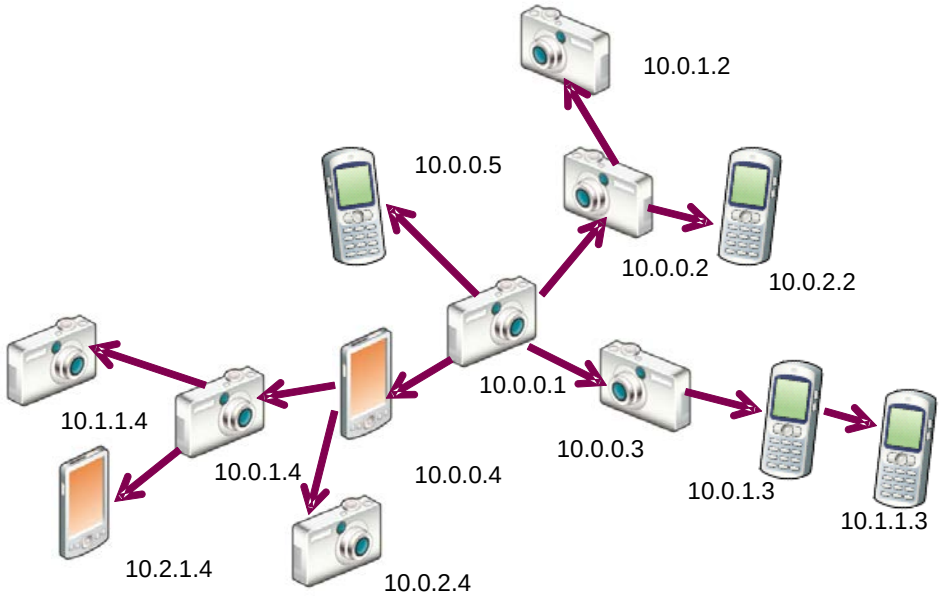

Figure 22: Hierarchical Address Assignment using 3 x 8-bit Submasks

The first Registrar in a new IBSS network that is using WSC IPv4 Assignment shall assign it's self the lowest address in a valid private subnet. It is recommended that 10.0.0.1 be used by the initiating Registrar using WSC IPv4 address assignment. The subnet mask is recommended to be 24 bits (10.0.0.0/24). Other starting addresses and subnet masks are possible using this protocol.

Every Registrar maintains a bit mask that defines the set of IP address that it may assign to enrollees. An additional list of submasks (Available Submask List) is given to each Enrollee when by the Registrar when it assigns the Enrollee an IP address. An Enrollee then uses the first submask for its range of IP address assignment when it acts as a Registrar. This mask is removed from the list and the reduced list is then provided when the device acts as a Registrar. When the list provided to an Enrollee is empty or all IP addresses in the range are assigned, the device it is not able to act as a Registrar.

The assignment of IP addresses is supported by additional fields carried in the WSC M8 in Encrypted Settings

- Registrar IPv4 Address
- IPv4 Subnet Mask
- Enrollee IPv4 Address
- Available IPv4 Submask List

Registrar IPv4 Address

The Registrar IPv4 Address component contains the IP address of the Registrar (for example the 32 bit value representing the address 10.0.0.1).

IPv4 Subnet Mask

The IPv4 Subnet Mask component contains the IP subnet mask used for the IBSS network.

Enrollee IPv4 Address

The Enrollee IPv4 Address component contains the value of the IP address that is assigned by the Registrar to the Enrollee.

Available IPv4 Submask List

The Available IPv4 Submask List provides the definition of address ranges that can be used by subsequent Registrars for IP address assignment. A Submask is constructed in a similar manner to a Subnet Mask where binary one values represent fixed values and zeros define the bits that are part of the range assignment.

The Submask List sent from a Registrar to an Enrollee partitions the available IP address space in the hierarchical address assignment. The following is an example set the four mash values that could be used five levels of hierarchical

11111111 00000011 11111111 11111111

11111111 11111100 00001111 11111111

11111111 11111111 11110000 00111111

11111111 11111111 11111111 11000000

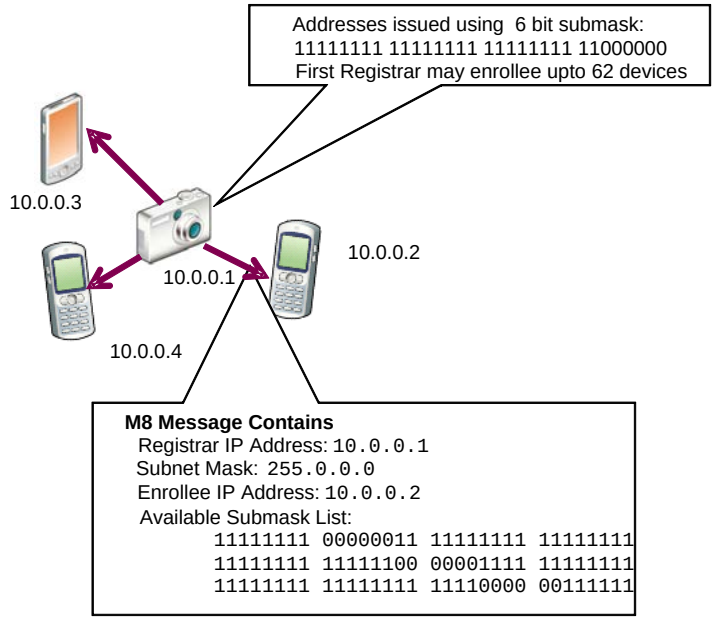

Figure 23: Example Hierarchical Address Assignment First Tier

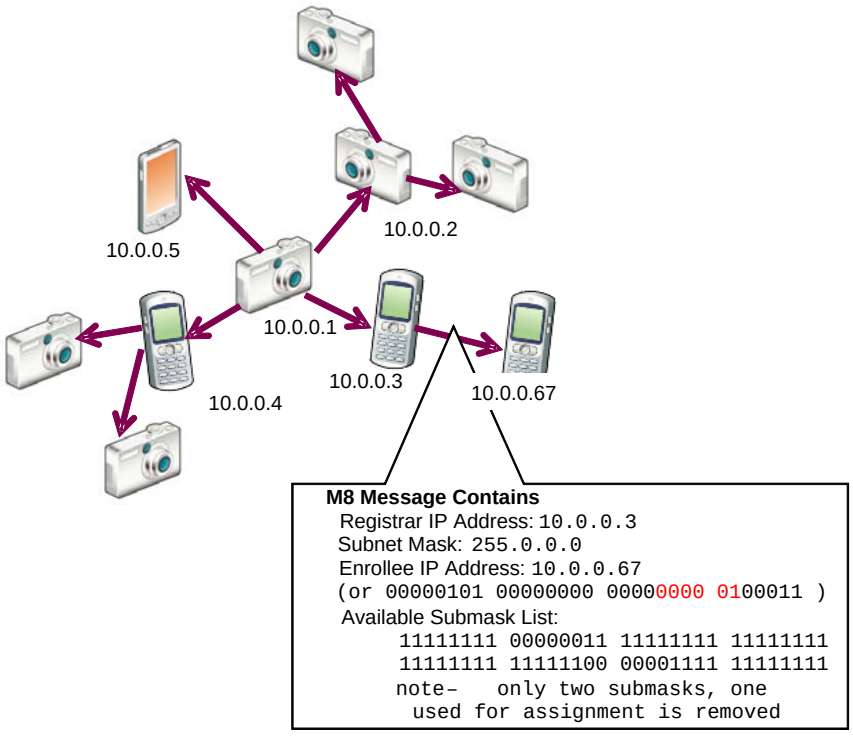

Figure 24: Example Hierarchical Address Assignment Second Tier

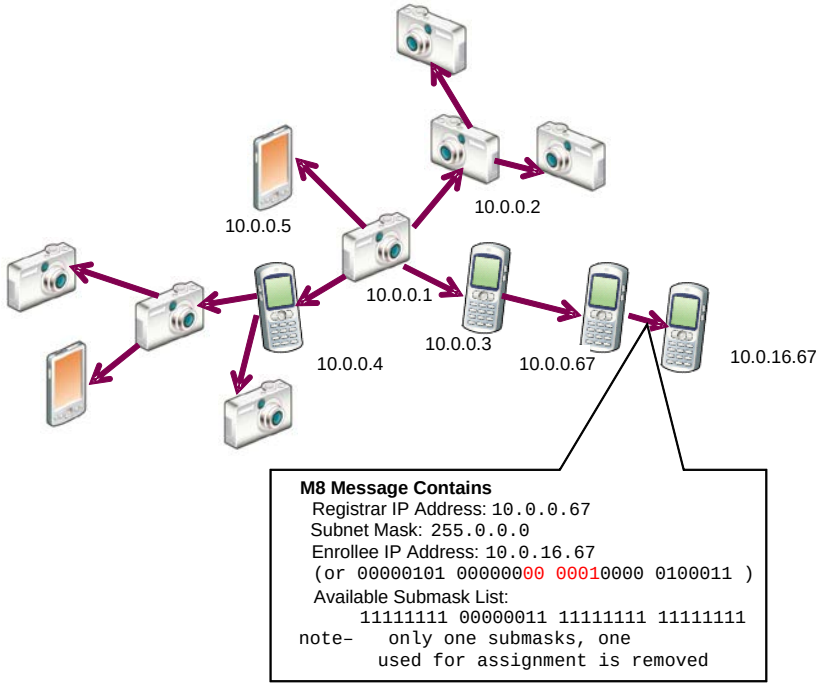

Figure 25: Example Hierarchical Address Assignment Third Tier

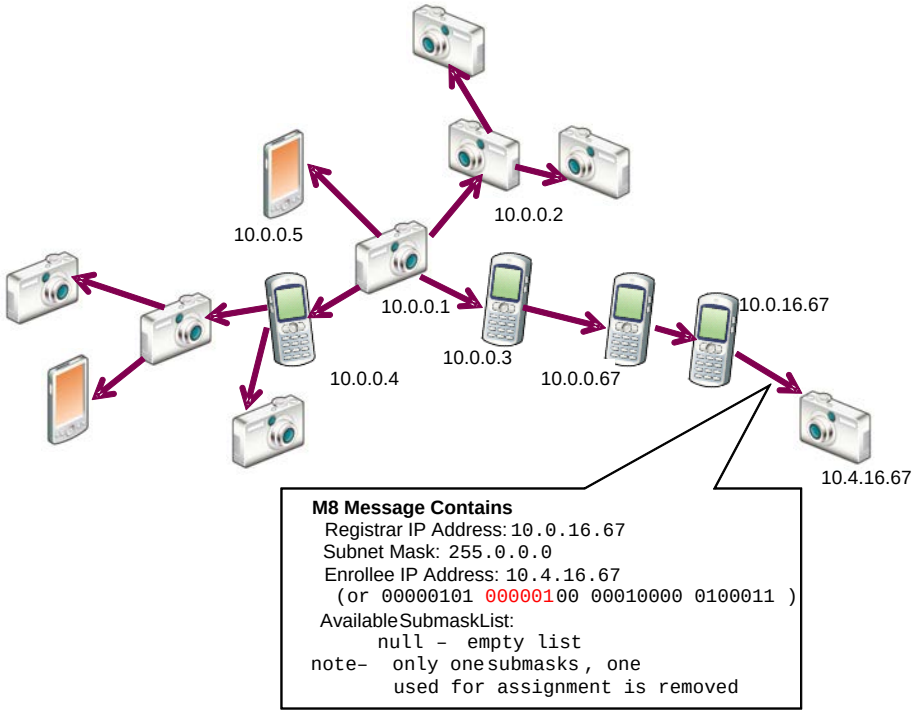

Figure 26: Example Hierarchical Address Assignment Fourth Tier

4.2. WSC 2.0 Specification Changes

These tables document the attributes that are specific to IWSC that are incorporated into the WSC 2.0 specification.

Table 3: Attributes in Encrypted Settings of M2, M8 if Enrollee is STA (in Table 21 in WSC specification)

Attribute	R/O	Notes
Credential	R	May include multiple instances of Credential
New Password	O	
Device Password ID	O	Required if New Password is included.
IP Address Configuration Method	R	Specified mechanism selected by Registrar
Registrar IPv4 Address	O	Must be included when Registrar supports WSC_IP
IPv4 Subnet Mask	O	Must be included when Registrar supports WSC_IP
Enrollee IPv4 Address	O	Must be included when WSC_IP is selected
Available IPv4 Submask List	O	A list of address submasks that may be used by the Enrollee.
<other…>	O	Multiple attributes are permitted.
Key Wrap Authenticator	R	

Table 28 (in WSC specification) – Attribute types and sizes defined for Wi-Fi Simple Configuration

Description	ID (Type)	Length
Entry Acceptable (only for IBSS)	0x106D	1B
Registration Ready (only for IBSS)	0x106E	1B
Registrar IPv4 Address	0x106F	4B
IPv4 Subnet Mask	0x1070	4B
Enrollee IPv4 Address	0x1071	4B
Available IPv4 Submask List	0x1072	N*4B
IP Address Configuration Methods	0x1073	2B

Table 4 (in WSC specification) – Configuration Methods

Value	Configuration Method	Description
0x0880	SMPBC	The device supports SMPBC(Simultaneous Multi-user PBC) functionality. This is an optional mode that is only used with IBSS.

Table 5 (in WSC specification) – Device Password ID

Value	Description
0x0006	SMPBC
0x0007 – 0x000F	Reserved

Table 6 (in WSC specification) – Response Type

Response Type Value	Description
0x04	Notifier

5. Message Encoding

This section will describe the changes and additions to the protocol messages introduced by IWSC. This section is based on section 8. Message Encoding of the Wi-Fi Simple Config specification v2.0.

The ordering of the attributes in messages described in the section of the WSC specification MUST match the order given in the tables. To be consistent with the WSC specification, IWSC IE attributes MUST contain the WSCIE attributes first followed by the additional optional attributes for IWSC in this section.

5.1. 802.11 Management Frames

5.1.1. IWSC Information Elements

IWSC Information Element only extends the WSC Information Element by adding additional attributes to the IE that is sent in Beacons, Probe Requests and Probe Responses. The structure of the Information Element is the same as WSC Information Element except having IWSC OUI value of hex 00-50-F2-10. The IWSC IE contains additional attributes and modified behavior for WSC attributes which are described in the following sections.

5.1.2. Beacon Frame

The following attribute definitions extend the base set of WSC attributes in a Beacon.

Table 7: Attributes extension in IWSC in the Beacon

Attribute	R/O/C	Allowed Values	Notes
AP Setup Locked	C	Must be included if value is TRUE. There is no AP in IBSS devices, however, if IBSS device has locked its PIN, such as due too many authentication failures. AP Setup Locked must be included.	Modify to WSC
Connection Type	R	Required for an IWSC device. This field is the XOR of the network types supported. The bit value Ox02 must be included for Wi-Fi IBSS devices.	Add for IWSC (new attribute for IWSC)
IP Address Configuration Methods	R	Required attribute indicates the supported methods for IP address determination. Devices that support IBSS must support WSC IP address assignment and may support other mechanisms.	

5.1.3. Probe Request

The following attribute definitions extend the base set of WSC attributes in a Probe Request. If the device has IWSC active, it must send the probe request with the IWSC IE. If the device does

not activate IWSC, the device must send the Probe Request without an IWSC IE when the device runs an active scan.

Table 8: Attributes extension in IWSC in the Probe Request

Attribute	R/O/C	Allowed Values	Notes
Association State	O	This attribute is optional for IWSC devices. If included, the value is ignored for IBSS connectivity.	Modify to WSC
Connection Type	R	Required for an IWSC device. This field is the XOR of the network types supported. The bit value Ox02 must be included for Wi-Fi IBSS devices.	Add for IWSC (new attribute for IWSC)
IP Address Configuration Methods	R	Required attribute indicates the supported methods for IP address determination. Devices that support IBSS must support WSC IP address assignment and may support other mechanisms.	

5.1.4. Probe Response

The following attribute definitions extend the base set of WSC attributes in a Probe Response.

Table 9: Attributes extension in IWSC in the Probe Response

Attribute	R/O/C	Allowed Values	Notes
AP Setup Locked	C	Must be included if value is TRUE. There is no AP in IBSS devices, however, if IBSS device has locked its PIN, such as due too many authentication failures. AP Setup Locked must be included.	Modify to WSC (No AP in IBSS)
Response Type	R	The response type for IWSC devices is extended to include the Notifier role. If the device receives a Selected Registrar Start Notification, this value is set to Notifier.	Modify to WSC (new value for IBSS)
UUID-E	R	Unique identifier of own device.	Modify to WSC
Configuration Methods	O	This attribute is OPTIONAL for IWSC devices only in Probe Response. If included, the value is ignored for IBSS connectivity.	Modify to WSC
Connection Type	R	Required for an IWSC device. This field is the XOR of the network types supported. The bit value Ox02 must be included for Wi-Fi IBSS devices.	Add for IWSC (new attribute for IWSC)
MAC Address	O	This attribute contains the MAC Address of a Selected Registrar device if the device receives a Selected Registrar Start Notification from the Selected Registrar device.	Add for IWSC (new attribute for IWSC)

Entry Acceptable	O	Required if a device supports SMPBC. 1 = Entry Time period is open to Enrollees for SMPBC registration. 0 = Entry Time period is closed.	Add for IWSC (new attribute for IWSC)
Registration Ready	O	Required if a device supports SMPBC. 1 = Registrar is ready to run the Registration Protocol. 0 = Registrar is busy and not able to run the Registration Protocol.	Add for IWSC (new attribute for IWSC)
IP Address Configuration Methods	R	Required attribute indicates the selected methods for IP address determination.	

5.1.5. Wi-Fi IBSS Public Action Frames

The Public Action frame format (as defined in IEEE Standard 802.11k [2]) is used to define the IWSC public action frames in this specification. The general format of the IWSC public action frames is shown in Table 9.

Table 10: Wi-Fi IBSS Public Action Frame Format

Field	Size (octets)	Value (Hexadecimal)	Description
Category	1	0x04	IEEE 802.11 public action usage.
Action field	1	0x09	(IEEE 802.11) vendor specific usage
OUI	3	50 6F 9A	WFA specific OUI. Note this is not the same OUI as used in the IWSCIE.
OUI type	1	0x10	Identifying Wi-Fi IBSS Usage
OUI Subtype	1		Identifying the type of Wi-Fi IBSS public action frame. The specific value is defined in Table 4.
Dialog Token	1		Set to a nonzero value to identify the request/response transaction.
Elements	variable		Including IWSCIE or any information elements defined in IEEE Std 802.11-2007 in reference [1] .In the IWSCIE, it has the Element ID(hex DD), Length, OUI(hex 00 50 F2 10), followed by the Data part of the attributes the same as WSC2.0 specification.

Table 11: Wi-Fi IBSS Public Action Frame Types

Type	Notes
0	Selected Registrar Start Notification
1	Selected Registrar Finish Notification
2	Device Query Request
3	Device Query Response
4 - 255	Reserved

5.1.5.1. Selected Registrar Start Notification

The Selected Registrar Start Notification action frame uses the Wi-Fi IBSS Public Action frame format and may be transmitted by a Wi-Fi IBSS Registrar device to notify active peers of enrollment activation in an IBSS network. The elements in the Selected Registrar Start Notification shall contain an IWSC IE containing the attributes in Table 11.

Table 12: Selected Registrar Start Notification Attributes

Attribute	R/O/C	Notes
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
Request Type	R	
Config Methods	R	
UUID-(E or R)	R	
Primary Device Type	R	
RF Bands	R	Specific RF band used for this message
Configuration Error	R	
Device Password ID	R	
MAC Address	R	Registrar's (self) MAC Address
<other…>	O	Multiple attributes are permitted

5.1.5.2. Selected Registrar Finish Notification

The Selected Registrar Finish Notification action frame uses the IWSC Public Action frame format and may be transmitted by an IWSC Registrar device to notify active peers of enrollment completion in an IBSS network. The elements in the Selected Registrar Finish Notification shall contain an IWSC IE containing the attributes in Table 12.

Table 13: Selected Registrar Finish Notification

Attribute	R/O	Notes
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
Wi-Fi Simple Configuration State	R	1 = unconfigured, 2 = configured.
MAC Address	R	Registrar's (self) MAC Address
<other…>	O	Multiple attributes are permitted

5.1.5.3. Device Query Request

The Device Query Request action frame uses the IWSC Public Action frame format and can get peer devices information in an IBSS network. The elements in the Device Query Request shall contain an IWSC IE containing the attributes in Table 13.

Table 14: Device Query Request

Attribute	R/O	Notes
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
Wi-Fi Simple Configuration State	R	1 = unconfigured, 2 = configured.
MAC Address	R	MAC Address for Request device
Primary Device Type	R	
Manufacturer	R	
Model Name	R	
Model Number	R	
Device Name	R	
<other…>	O	Multiple attributes are permitted

5.1.5.4. Device Query Response

The Device Query Response action frame uses the IWSC Public Action frame format and can inform the device information to the originating device. The elements in the Device Query Response shall contain an IWSC IE containing the attributes in Table 14.

Table 15: Device Query Response

Attribute	R/O	Notes
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
Wi-Fi Simple Configuration State	R	1 = unconfigured, 2 = configured.

MAC Address	R	MAC Address for Response device
Primary Device Type	R	
Manufacturer	R	
Model Name	R	
Model Number	R	
Device Name	R	
<other…>	O	Multiple attributes are permitted

5.2. Registration Protocol Message Definitions

These definitions are the same as defined in the Wi-Fi Simple Configuration specification v2.0, section 8.3 Registration Protocol Message Definitions, except there are no configuration parameters for an AP to support an external Registrar.