Руководство по инициализации подключения к Wi-Fi для устройств из мира IoT

Wi-Fi — наиболее широко распространенная на сегодня технология беспроводного подключения к сети. Став стандартной функцией всех переносных компьютеров, смартфонов и планшетов, Wi-Fi завоевывает бытовые приборы, термостаты и многие другие устройства автоматизации жилищ и зданий, заполняющие бурно развивающийся «Интернет вещей» (IoT). Простая и надежная инициализация подключения к сети устройств IoT, которые не имеют клавиатуры и дисплея в качестве пользовательского интерфейса, представляет собой достаточно сложную задачу. В статье рассматриваются основные имеющиеся на рынке способы инициализации подключения к Wi-Fi, даны рекомендации по правильному выбору способа подключения устройств.

Джил Рейтер (Gil Reiter)

Что такое инициализация подключения к Wi-Fi?

Процесс подключения нового устройства Wi-Fi (станции) к сети Wi-Fi — это и есть инициализация. Данный процесс предполагает загрузку в станцию имени сети (часто его называют SSID — идентификатор набора служб) и ее учетных данных безопасности. Стандарт безопасности Wi-Fi проводит различие между персональной безопасностью, используемой, в основном, в домах и на небольших предприятиях, и корпоративной безопасностью, политики которой применяются в больших офисах и кампусах. В случае корпоративной безопасности инициализация станции обычно предполагает установку сертификатов, используемых для проверки целостности станции и сети путем взаимодействия с сервером безопасности, находящимся под управлением ИТ-отдела. С другой стороны, персональную безопасность Wi-Fi должны обеспечивать сами пользователи у себя дома, и это предполагает просто ввод заданного пароля. Чтобы надежно обеспечить безопасность, пароль может иметь длину до 64 символов.

В статье мы ограничимся персональной безопасностью сети Wi-Fi и задачей простой загрузки пользователем имени сети и пароля в Wi-Fi-станцию IoT.

Задача инициализации беспроводного подключения в устройствах IoT

Технология Wi-Fi была создана для того, чтобы переносные устройства, такие как ноутбуки, а позже и более продвинутые мобильные устройства, такие как сотовые телефоны и планшеты, могли подключаться к Интернету без проводов. Такие персональные девайсы по определению имеют дисплей и клавиатуру в качестве интерфейса пользователя. Например, обычная процедура подключения сотового телефона к Wi-Fi осуществляется через страницу настроек этого устройства. Телефон выполняет поиск сетей Wi-Fi и предоставляет пользователю список доступных. После того как сеть выбрана, пользователю предлагается ввести пароль. Если пароль введен правильно, инициализация подключения считается успешной и часто указывается значком Wi-Fi на панели состояния.

Если же говорить об устройствах IoT, трудность заключается в том, что многие из них не имеют дисплея и клавиатуры, а зачастую у них вообще нет никакого пользовательского интерфейса. Таким «безголовым» устройствам нужны другие способы получения имени сети и пароля от пользователя. Альтернативный способ подключения должен быть простым и надежным. В большинстве случаев он предполагает использование ПК, телефона или планшета в качестве расширенного интерфейса пользователя для IoT-устройства, который позволяет ввести информацию о сети с помощью дисплея и клавиатуры ПК, телефона или планшета.

Далее мы приведем краткий обзор широко распространенных на рынке способов инициализации подключения. Затем рассмотрим ключевые аспекты выбора правильных спосо-

бов инициализации и дадим рекомендации разработчику системы.

Безопасная настройка Wi-Fi

Безопасная настройка беспроводной сети (Wi-Fi Protected Setup, или WPS) — единственный промышленный стандарт, существующий сегодня для подключения к сети «безголовых» устройств, т. е. устройств, как уже было сказано, не имеющих пользовательского интерфейса. Он был введен объединением крупнейших производителей компьютерной техники и беспроводных устройств Wi-Fi (Wi-Fi Alliance) в 2006 г. в качестве простого и безопасного способа инициализации подключения, не требующего знания имени сети и ввода длинных паролей. Этот стандарт устанавливает два обязательных варианта для точек доступа (ТД), поддерживающих WPS: с использованием персонального идентификационного номера (Personal Identification Number, PIN) или подключение нажатием кнопки (Push-Button-Connect, PBC).

В первом случае восьмизначный PIN печатается на стикере (рис. 1), на ТД либо на подключаемом устройстве. Пользователь должен прочитать этот PIN на устройстве, не имеющем клавиатуры, и набрать его на клавиатуре подключаемого устройства. Очевидный недостаток этого метода иниацилизации заключается в том, что он не работает, если отсутствует пользовательский интерфейс (как уже было сказано, нужна клавиатура, чтобы ввести PIN).

В случае PBC пользователь нажимает кнопку как на ТД, так и на подключаемом устройстве. Как только кнопка на ТД будет нажата, устройство, поддерживающее WPS, сможет свободно подключиться к сети в течение 2 мин. Недостаток этого способа, помимо отсутствия защиты в течение двухминутного периода, заключается в том, что пользователь должен иметь физический доступ к ТД. Если ТД находится в труднодоступном месте, этот способ может оказаться неудобным.

При использовании как PIN, так и PBC, ТД и подключаемое устройство обмениваются серией сообщений для установления временного защищенного соединения, которое используется для передачи SSID и пароля из ТД в подключаемое устройство.

Основная проблема стандарта WPS была вскрыта в 2011 г. Стефаном Фибеком (Stefan Viehböck) [1], который обнаружил, что в случае использования PIN можно получить сетевой пароль менее чем за четыре часа путем простого перебора. Поскольку использование PIN обязательно для получения сертификации WPS, все новые ТД, выпускаемые на рынок начиная с 2007 г., поддерживали этот способ по умолчанию. Более того, во многих ТД не была предусмотрена возможность отключения функций WPS.

Сразу же после того как была обнаружена эта прореха в защите, большинство поставщиков ТД рекомендовали отключить поддержку WPS, и, хотя большинство из них выпустили обновления своих изделий, предотвращающие взлом, стандарт WPS приобрел плохую репутацию в отрасли и некоторые страны до сих пор не используют его.

Рис. 1. Пример для варианта инициализации с использованием PIN: PIN WPS напечатан на точке доступа D-Link (слева), а кнопка подключения WPS находится на точке доступа Cisco (справа)

Режим точки доступа

Режим точки доступа (AP) — наиболее широко применяемый сегодня способ подключения устройств, не имеющих пользовательского интерфейса. В режиме AP неподключенное (неинициализированное) устройство сначала запускается как ТД с SSID, который задан изготовителем оборудования. Прежде чем впервые попытаться подключиться к домашней сети, неинициализированное устройство создает свою собственную сеть, позволяя ПК или смартфону подключиться к ней напрямую, чтобы выполнить его начальное конфигурирование.

В этом режиме неинициализированное устройство включает в себя также встроенный веб-сервер. После того как пользователь подключит свой смартфон к ТД неинициализированного устройства, он открывает веб-браузер смартфона и входит на веб-сайт устройства, используя заданный локальный URL или IP-адрес.

На встроенном веб-сайте пользователь выбирает (или вводит) имя домашней сети и пароль. Устройство сохраняет сетевые реквизиты в энергонезависимой памяти, а затем переходит из режима AP в режим станции, чтобы подключиться к домашней сети с использованием сохраненных сетевых реквизитов.

На рис. 2 показан снимок экрана iPad, на который выведена вкладка настройки микроконтроллера CC3200 семейства SimpleLink с интегрированным модулем Wi-Fi корпорации Texas Instruments (TI) с реализованного в микросхеме веб-сайта. Эта вкладка настройки дает пользователю возможность ввести SSID и ключ безопасности для нескольких профилей сети.

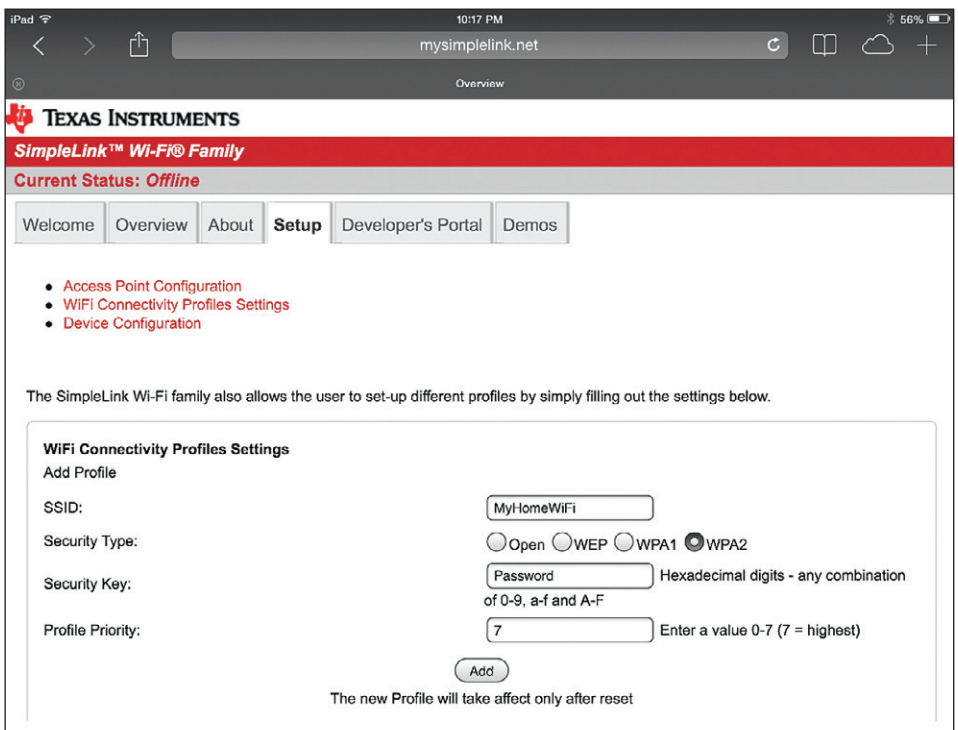

Рис. 2. Страница настройки реализованного в микросхеме веб-сервера микроконтроллера CC3200 семейства SimpleLink с модулем Wi-Fi

После того как конфигурирование будет завершено, микроконтроллер CC3200 (или CC3100) автоматически подключится к одной из доступных сетей на основании задаваемых пользователем приоритетов [2].

Основное преимущество подключения в режиме ТД заключается в том, что в нем используются стандартные возможности, которые имеются во многих смартфонах, планшетах и ПК. Еще одно преимущество — поставщики могут добавлять дополнительные параметры к встроенному веб-сайту для конфигурирования других функций устройства одновременно с регистрацией в сети Wi-Fi.

Для повышения безопасности на устройстве может использоваться кнопка для активации режима ТД, а для ее конфигурирования может использоваться заранее заданный пароль.

Недостаток режима AP заключается в том, что при подключении к конфигурационной сети AP неинициализированного устройства телефон отключается от домашней сети. Это может вызвать перерывы в передаче данных и привести к появлению сообщений об ошибках. На ПК, если активны и Wi-Fi-, и Ethernet-соединение, браузер может отдать приоритет Ethernet-соединению и не подключиться к неинициализированному устройству по Wi-Fi. Пользователь должен отключить Ethernet-соединение, прежде чем использовать инициализацию Wi-Fi в режиме AP (ТД).

Появившиеся недавно смартфоны проверяют, действительно ли сеть Wi-Fi подключена к Интернету. Если интернет-соединение прерывается (как это бывает, когда телефон соединяется с ТД неинициализированного устройства), эти смартфоны отключаются от сети Wi-Fi, а затем принудительно устанавливают соединение сотовой системы передачи данных. Заблокировать такое поведение телефона можно, но для этого требуются расширенные настройки на странице конфигурации устройства, что усложняет пользование устройством для потребителя.

Функция конфигурирования беспроводных устройств Apple

Функция конфигурации беспроводных устройств (Wireless Access Controller, WAC) — это лицензированная технология Apple MFi, предназначенная для принадлежностей MFi, которые подключаются к iPod, iPhone и iPad. Принадлежности MFi, поддерживающие WAC, можно легко сконфигурировать с помощью iPod, iPhone и iPad, при этом от пользователя не требуется вводить имя сети и пароль. Подробная информация о функции WAC доступна обладателям лицензий на разработку и изготовление устройств Apple MFi.

Технология SmartConfig

Технология SmartConfig — это фирменный способ инициализации подключения от корпорации TI, предназначенный для устройств без пользовательского интерфейса. Он был предложен еще в 2012 г. и предполагает использование мобильного приложения для передачи сетевых реквизитов из смартфона или планшета в неподключенное Wi-Fi-устройство корпорации. Когда SmartConfig включается в неподключенном устройстве, оно входит в специальный режим сканирования, ожидая получения информации о сети, которая передается телефонным приложением. Телефон должен быть подключен к сети Wi-Fi, чтобы он мог передавать сигнал SmartConfig по беспроводным каналам. Обычно это та же домашняя сеть, к которой новое устройство собирается подключиться.

Имя сети Wi-Fi (SSID), к которой подключен телефон, автоматически появляется в телефонном приложении. После этого пользователь вводит пароль сети и нажимает кнопку «Пуск», чтобы начать процесс. Также есть вариант добавления имени устройства, которое передается телефоном вместе с информацией о сети и программируется в памяти устройства Wi-Fi.

Для повышения безопасности SmartConfig имеет возможность шифровать передаваемые между устройством и телефоном данные с помощью предварительно выданного ключа. Предварительно выданный ключ обычно печатается на этикетке коробки устройства и может быть отсканирован телефонным приложением до запуска процесса SmartConfig.

После того как устройство SimpleLink (см. рис. 2) получит сетевые реквизиты, оно автоматически подключается к сети и отправляет сообщение об обнаружении сервисов обратно на телефон. Телефонное приложение, получив это сообщение, извещает пользователя о том, что новое устройство успешно подключилось к сети.

На рис. 3 показаны снимки с экрана приложения SmartConfig. На экране слева показано, как пользователь вводит пароль и имя устройства. На экране справа мы видим уведомление, полученное после успешного подключения устройства.

TI предлагает библиотеку SmartConfig для операционных систем iOS и Android, а также демонстрационное приложение в App Store и в Google Play. Исходный код приложения можно загрузить с веб-сайта [2].

Ключевые преимущества SmartConfig — простота использования и возможность беспрепятственной интеграции в телефонное приложение устройства. Кроме того, если несколько устройств Wi-Fi одновременно находятся в режиме SmartConfig, одно телефонное приложение может обеспечить подключение их всех одновременно.

Однако следует отметить и некоторые немаловажные минусы. Помимо того что SmartConfig работает только в устройствах TI, основной недостаток этой технологии заключается в том, что телефон должен подключаться к сети, используя ту полосу частот и ту скорость передачи данных, которые поддерживаются неподключенным устройством. Например, если неподключенное устройство поддерживает диапазон 2,4 ГГц, а телефон использует для связи с двухдиапазонной сетью диапазон 5 ГГц, SmartConfig не будет работать просто потому, что неподключенное устройство не принимает сигналы в диапазоне 5 ГГц. Некоторые новые маршрутизаторы и телефоны для увеличения пропускной способности используют собственные скорости передачи данных, поэтому и здесь SmartConfig не справится с задачей. Но поскольку подавляющее большинство маршрутизаторов работает в диапазоне 2,4 ГГц и использует стандартные скорости передачи данных Wi-Fi, технология SmartConfig в большинстве ситуаций работает.

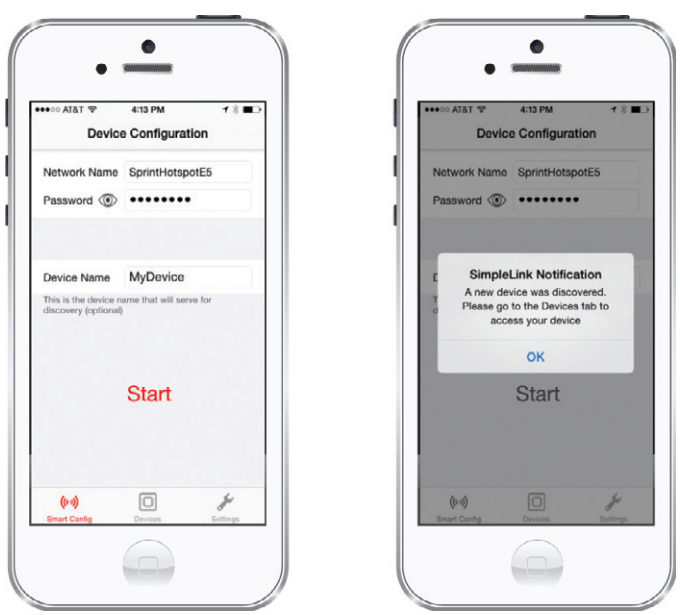

Рис. 3. Телефонное приложение SmartConfig от TI

Внеполосное подключение

Способы подключения, о которых шла речь выше, можно назвать «внутриполосным» подключением, потому что в них используется радиосвязь Wi-Fi для передачи информации

о сети в неподключенное устройство. Его преимущество состоит в том, что не требуется дополнительных интерфейсов или элементов системы для осуществления подключения, а используются средства радиосвязи Wi-Fi, встроенные в устройство.

Внеполосные способы подключения используют для передачи информации о сети в подключаемое устройство среду, отличную от Wi-Fi. Внеполосное подключение может быть проводным, например с помощью интерфейса USB, или беспроводным, например с помощью технологии радиосвязи ближнего радиуса действия (NFC) или Bluetooth. Добавление в устройство возможности внеполосного первичного подключения повышает его надежность и универсальность, но увеличивает стоимость решения.

Аспекты проектирования

Рассмотрим аспекты, которые разработчику обязательно следует учитывать при выборе способа(ов) инициализации подключения, и дадим рекомендации по выбору наиболее подходящего для различных систем. Мы сосредоточимся на внутриполосных способах подключения, поскольку они вызывают большинство вопросов и трудностей.

Простота использования

Простота использования — важная характеристика потребительских товаров. Многие простые IoT-устройства рассчитаны на обычных домашних пользователей, которые не обладают глубоким пониманием процесса подключения и иногда имеют ограниченные навыки работы на компьютере либо не имеют их вообще. Так как подключение — это первое, что пользователи делают, когда открывают коробку с устройством, оно может сформировать их общее мнение о нем.

Говоря о простоте использования, мы рассматриваем такие тривиальные вещи, как количество операций, которые должен выполнить пользователь, чтобы подключить устройство. Важно, сможет ли пользователь воспользоваться средствами, с которыми он уже знаком, или ему придется приобретать новые навыки, чтобы решить эту задачу.

WPS, WAC и технология SmartConfig — самые простые в использовании способы. Хотя WPS не требует никаких знаний и средств, для него требуется физический доступ к маршрутизатору Wi-Fi, чтобы нажать кнопку WPS. Поскольку большинство пользователей смартфонов знают, как загружать и использовать телефонные приложения, технология SmartConfig предлагает пользователю знакомый интерфейс, но требует, чтобы он ввел пароль сети.

Безопасность

С точки зрения безопасности с подключением к Wi-Fi связаны следующие два главных риска: во-первых, любитель подслушивать может получить пароль и воспользоваться им для подключения к домашней сети, а во-вторых, злоумышленник может использовать окно подключения устройства, чтобы взять его под контроль. В большинстве случаев первый риск вызывает наибольшие опасения.

Можно обоснованно утверждать, что угрозы безопасности при подключении к Wi-Fi IoT-устройств ограничены при всех способах подключения, рассмотренных в этой статье, если эти способы используются правильно, поскольку подключение осуществляется только один раз за весь срок службы устройства или очень редко. Кроме того, во время подключения пароль сети передается в течение короткого времени в момент, контролируемый пользователем. Злоумышленник должен точно знать, когда произойдет подключение, и у него будет очень мало времени на то, чтобы провести атаку. Более того, злоумышленник должен находиться в радиусе действия сети Wi-Fi в тот момент, когда осуществляется подключение. Тем не менее значение безопасности никогда не следует недооценивать, и во многих случаях это имеет решающее значение.

Режим AP, WAC и технология SmartConfig имеют встроенную защиту. В случае режима AP и технологии SmartConfig разработчик должен выбрать использование защиты (то есть в режиме AP ТД должна быть сконфигурирована для применения защиты, а в SmartConfig шифрование должно быть выбрано явным образом). В WAC защита подключения используется всегда.

В случае способа подключения с помощью кнопки WPS риск с точки зрения безопасности заключается в том, что, когда ТД находится в режиме WPS, любое устройство Wi-Fi, находящееся поблизости, может использовать WPS для подключения к этой сети Wi-Fi.

Надежность и универсальность

Надежность и универсальность тесно связаны с простотой использования, поскольку существует вероятность того, что подключение не будет работать или потребует каких-либо действий по устранению проблем. Но это заслуживает отдельного разговора, так как каждому из способов подключения присущи собственные уникальные ограничения.

Очевидное ограничение WPS заключается в том, что не все ТД его поддерживают. Во многих ТД, которые не поддерживают WPS, эта поддержка отключена по умолчанию из-за бреши в защите способа подключения с использованием PIN, которая обсуждалась выше. Если поддержка WPS отключена, пользователю потребуется войти на веб-портал ТД, чтобы включить функцию WPS. Для многих пользователей это слишком сложно.

Технология SmartConfig имеет некоторые присущие ей ограничения, которые были рассмотрены выше и могут не позволить ей выполнить подключение к некоторым ТД, использующим диапазон 5 ГГц или свои собственные скорости передачи данных.

Режим AP, вероятно, является наиболее надежным и универсальным способом подключения к Wi-Fi. Подключение в режиме AP будет работать в большинстве случаев, за исключением некоторых новых моделей телефонов, которые отключают сеть Wi-Fi, не подключенную к Интернету (как указано выше, такой режим можно отключить). Вероятно, в этом заключается причина того, что большинство устройств и систем IoT на сегодня используют именно этот способ подключения.

В тех случаях, когда надежность не является самым важным аспектом, следует рассмотреть способ внеполосного подключения, например с помощью USB.

Унификация

WPS и WAC выполняют единственную функцию — подключение к Wi-Fi, а режим AP и технологию SmartConfig вполне можно интегрировать в систему управления устройства и уподобить другим его функциям. Технологию SmartConfig можно интегрировать в телефонное приложение устройства, чтобы обеспечить его единообразное восприятие пользователем, позволяющее реализовать несколько вариантов конфигурирования с помощью одного и того же пользовательского интерфейса. Режим AP дает аналогичные преимущества при использовании веб-браузера для взаимодействия с несколькими функциями устройства из одной позиции.

Подключение с помощью микроконтроллеров CC3100 и CC3200 семейства SimpleLink с модулем Wi-Fi

Платформы CC3100 и CC3200 семейства SimpleLink с модулем Wi-Fi обеспечивают потребителям наибольшую гибкость с точки зрения способов подключения, так как поддерживают все рассмотренные выше внутриполосные способы. Благодаря своим новым интерфейсам прикладного программирования SimpleLink и возможностям автономного модуля управления Wi-Fi, микроконтроллеры CC3100 и CC3200 делают подключение простой задачей для разработчика устройств. Приложение может включить использование любого способа подключения с помощью простых вызовов интерфейса прикладного программирования, а корпорация TI предлагает типовое программное обеспечение для SmartConfig, режима AP и WPS. Имя сети Wi-Fi и пароль автоматически и надежно записываются во flash-память последовательного доступа и используются встроенным модулем управления Wi-Fi для подключения к сети безо всякого участия пользователя и без кода приложения.

Встроенный в микросхему веб-сервер микроконтроллеров CC3100 и CC3200 делает проектирование подключения точки доступа чрезвычайно простым. Разработчик может включить заранее заданные элементы конфигурации в HTML-страницы, которые хранятся во flash-памяти последовательного доступа и автоматически загружаются веб-сервером. Чтобы еще больше упростить работу, микроконтроллеры CC3100 и CC3200 имеют в своем составе реализованный в микросхеме веб-сайт для подключения, который выполняет работу по подключению точки доступа без кода пользователя и вообще без каких-либо усилий с его стороны.

Заключение

Мы рассмотрели основные способы инициализации подключения к Wi-Fi для устройств, не имеющих собственного пользовательского интерфейса, и рассмотрели их достоинства и связанные с ними трудности. Поскольку ясно, что ни один из способов подключения не является идеальным, на практике правильным подходом была бы поддержка в устройстве нескольких вариантов подключения.

В случае профессиональных или промышленных устройств может быть достаточно режима AP, так как он обеспечивает наилучшую надежность и универсальность. Во многих IoT-устройствах на сегодня режим AP выбран в качестве единственного способа их подключения.

В случае аксессуаров MFi, которые подключаются к iPod, iPhone и iPad, естественным вариантом выбора является WAC. Для поддержки подключения с использованием других телефонов, планшетов или ПК в аксессуар следует добавить дополнительный способ подключения.

Если важна простота использования, подходят WPS или технология SmartConfig, потому что они обеспечивают наибольшее удобство для пользователя. Технология SmartConfig является естественным выбором, если нужно организовать подключение как работу с телефонным приложением. Если использование телефонного приложения не является обязательным, правильным вариантом выбора будет WPS.

WPS или SmartConfig смогут охватить большинство вариантов установки устройств, но, поскольку они не будут работать в 100% всех случаев, рекомендуется добавить в устройство режим AP в качестве варианта «режима для продвинутых пользователей». Пользователям можно дать указание использовать режим AP, если им не удается подключиться с помощью WPS или SmartConfig. ■

Литература

1. https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf
2. www.ti.com