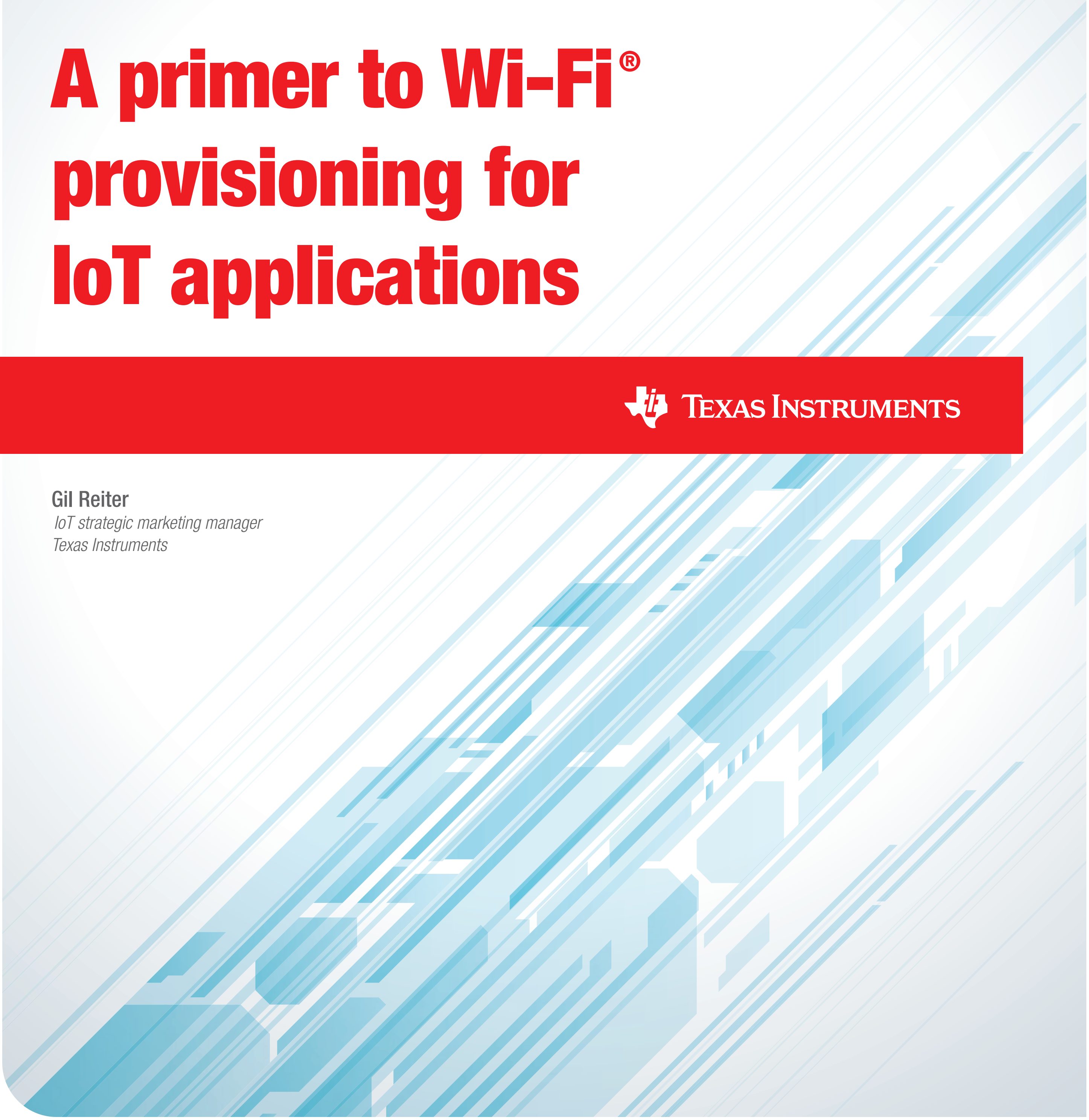
A primer to Wi-Fi® provisioning for IoT applications

Gil Reiter
IoT strategic marketing manager
Texas Instruments



Wi-Fi® is the most ubiquitous wireless connectivity technology today. After becoming a standard feature in all laptops, smartphones and tablets, Wi-Fi is being added to simpler products like home appliances, thermostats and many other home and building automation products that are feeding the exploding Internet of Things (IoT).

Provisioning IoT products, that do not have a keyboard and display as a user interface, in a simple and robust way is a significant challenge. In this paper, we review the main Wi-Fi provisioning methods that are available in the market and provide guidelines for choosing the right provisioning method for your product.

What is Wi-Fi provisioning?

Wi-Fi provisioning is the process of connecting a new Wi-Fi device (station) to a Wi-Fi network. The provisioning process involves loading the station with the network name (often referred to as SSID) and its security credentials.

We will restrict the discussion in this paper to personal Wi-Fi security networks and to the challenge of easily loading an IoT Wi-Fi station with the network name and password by the user.

The challenge of wireless provisioning in IoT applications

Wi-Fi was created to allow nomadic devices such as laptops, and later on mobile devices such as cellphones and tablets, to wirelessly connect to the Internet. These personal computing devices naturally include a display and a keyboard for the user interface. The usual procedure for provisioning a cellphone, for instance, on a Wi-Fi network is done via the phone's Wi-Fi setting page.

The challenge in IoT products is that many of them do not have a display and a keyboard, and sometimes they don't even have a user interface at all. These *headless* devices need alternate methods to obtain the network name and password from the user. The alternate provisioning method has to be simple to use and secure. In most cases it uses a PC, phone or tablet as an extended user interface for the IoT device, allowing the user to provide the network information using the display and the keypad of the PC, phone or tablet.

In the next few paragraphs, we provide a brief overview of the popular provisioning methods in the market. Later we discuss the key considerations for choosing the right provisioning methods and provide guidelines to the system designer.

Wi-Fi protected setup

Wi-Fi Protected Setup (WPS) is the most common standard available today for provisioning headless devices. It was introduced by the Wi-Fi Alliance in 2006 as an easy and secure method to provision devices without knowing the network name and

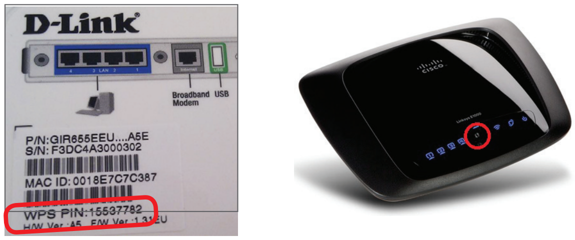


Figure 1. *WPS PIN printed on a D-Link® AP (left) and WPS push button on a Cisco AP (right).*

without typing long passwords. The standard defines two mandatory methods for WPS-enabled Access Points (APs): *Personal Identification Number (PIN) method* and *Push-Button-Connect (PBC) method,* **Figure 1**.

In the PIN method, an 8-digit PIN is printed on a sticker on either the Access Point or the provisioned device. The user needs to read the PIN from one device and type it using a keypad on the other device. Since APs do not have keypads, the PIN is usually printed on the AP and typed by the user at the provisioned device. The obvious drawback of this is that it doesn't work for headless devices – it requires at least a numerical key pad to type the PIN.

In the PBC method, the user pushes a button on both the AP and the provisioned device. Once the button on the AP is pushed, WPS-enabled devices can freely join the network for a period of two minutes. The drawback of this method, beyond the lack of security during the two-minute period, is that the user must have physical access to the AP. If the AP is located in a hard-to-reach place, the method can be cumbersome.

A major problem in WPS was unveiled in 2011 by Stefan Viehböck[1], who found a design flaw in the PIN method that allowed brute-force attack to expose the network password in less than four hours. Since the PIN method is mandatory to achieve WPS certification, all new APs released to the market starting in 2007 supported this method by default. Furthermore, many APs did not have an option to disable the WPS functionality.

Right after the security breach was discovered, most AP vendors came out with recommendations to disable WPS, and although most of them released product upgrades that prevented hacking, WPS received a bad reputation in the industry and is still avoided in some countries.

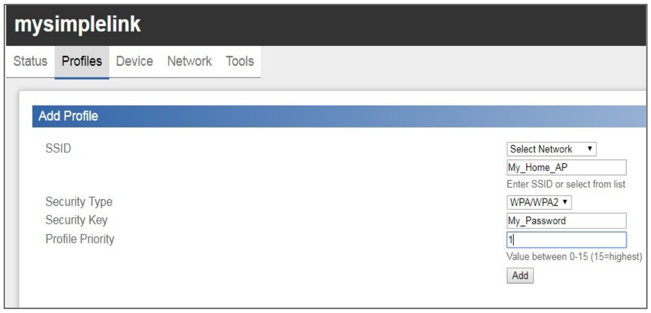
Access point mode

Access Point (AP) mode is the most common provisioning method today for headless devices. In AP mode the un-provisioned device wakes-up initially as an AP with an SSID defined by the equipment manufacturer.

In this mode, the un-provisioned device also includes a secured embedded web server. After the user connects his smartphone to the un-provisioned device's AP, he opens the smart phone's web browser and browses into the device's web site via a pre-defined local URL or IP address.

In the embedded web site, the user chooses (or types in) the home network name and password. The device stores the network credentials in nonvolatile memory and then it switches from AP mode to Station mode in order to connect to the home network using the stored network credentials.

Figure 2 is an iPad screen capture of the setup tab of the on-chip web site for Texas Instruments' SimpleLink™ Wi-Fi CC3235SF wireless MCU. The setup tab allows the user to provide the SSID and the security key for multiple network profiles. After the configuration is done, the SimpleLink Wi-Fi devices



Add Profile

SSID: Select Network ▾ / My_Home_AP
Enter SSID or select from list
Security Type: WPA/WPA2 ▾
Security Key: My_Password
Profile Priority: 1
Value between 0-15 (15=highest)
Add

Figure 2. *The SimpleLink Wi-Fi CC3235 wireless MCU on-chip web server setup page.*

will automatically connect to one of the available networks, based on a user-configurable priority[2].

The primary benefit of AP mode provisioning is that it uses standard capabilities that exist in any smart phone, tablet and PC. Another benefit is that the vendors can add additional parameters to the embedded web site to configure other device functions at the same time when the device is provisioned on the Wi-Fi network.

For increased security, a push button on the device can be used to activate the Access Point mode. It is recommended to use HTTPS secure connection to ensure that the user's network credentials are being used securely during the provisioning process.

Apple Wireless Accessory Configuration (WAC) feature

The Wireless Accessory Configuration (WAC) feature is an Apple MFi licensed technology designed for MFi accessories that connect to iPod, iPhone and iPad. MFi accessories that support WAC can be easily configured by an iPod, iPhone and iPad, without requiring the user to type in the network name and password. Detailed information about the WAC feature is available to Apple MFi Development and Manufacturing licensees.

SmartConfig™ technology

SmartConfig technology is a TI proprietary provisioning method designed for headless devices introduced in 2012. It uses a mobile app to broadcast the network credentials from a smartphone, or a tablet, to an un-provisioned TI Wi-Fi device.

The Wi-Fi network name (SSID), that the phone is connected to, shows up automatically on the phone app. The user then adds the network password and presses the "Start" button to begin the process. There is also an option to add a device name, which is broadcasted by the phone, together with the network information and programmed to the Wi-Fi device memory. For enhanced security, SmartConfig has an option to encrypt the broadcast data with a pre-shared key between the device and the phone. The pre-shared key is typically printed on a label on the device box, and could be scanned by the phone app before the SmartConfig process starts.

After the network credentials are picked up by the SimpleLink device, it connects automatically to the network and sends out a service discovery message back to the phone.

TI provides a SmartConfig library for iOS and Android™ and demo apps on the Apple App store and Google Play. The source code of the app is available to download from the TI website. Vendors can use the SmartConfig library to easily integrate the SmartConfig function into their own apps.

The two key benefits of SmartConfig are ease of use and the potential to integrate seamlessly into the phone app of the product. Another unique capability of SmartConfig technology is the ability to provision multiple devices simultaneously. If multiple Wi-Fi devices are in SmartConfig mode at the same time, one phone app can provision all of them at the same time.

Out-of-band provisioning

The provisioning methods mentioned so far can be referred to as *in-band provisioning* because they are using the Wi-Fi radio to deliver the network information to the un-provisioned device. The benefit of in-band provisioning is that it does not require additional interfaces or system components to perform provisioning, but rather it uses the same Wi-Fi radio built into the product.

Out-of-band provisioning methods use a non-Wi-Fi medium to deliver the network information to the provisioned device. Out-of-band provisioning can be wired (i.e. using a USB interface), or wireless (i.e. using a near field communication (NFC) radio or *Bluetooth*®). Adding out-of-band provisioning to a product adds robustness and flexibility but increases the solution cost.

Design consideration

So far we reviewed the leading Wi-Fi provisioning methods in the market and discussed some of their key properties, their advantages and weaknesses. In the following sections we cover the essential considerations one should contemplate when choosing the provisioning method(s) and provide guidelines for choosing the right method for different applications. We will focus on the in-band provisioning methods, as they introduce the most questions and challenges.

Ease of use

Ease of use is a critical consideration in consumer products. Many simple IoT devices are targeting common home users, who have limited understanding of the provisioning process and sometimes have no or limited skills to operate computers.

In considering ease of use, we look at trivial things like the number of steps a user undergoes to provisioning a device. We also ask ourselves, if the user needs to exercise tools he already knows, or does he need to learn new tools to accomplish the task.

WPS, WAC and SmartConfig technology are the easiest to use methods. While WPS requires no knowledge and no tools what so ever, it does require physical access to the Wi-Fi router to push the WPS button. Since most smartphone users are familiar with downloading and using phone apps, SmartConfig technology offers a familiar interface to the user, but it does require the user to type in the network password.

Security

The two main security risks related to Wi-Fi provisioning are: (i) an eavesdropper can obtain the network password and use it to connect to the home network, and (ii) a malicious attacker can use the provisioning window of the device to take it over. In most cases the former risk is of most concern.

It is reasonable to say that security risks in Wi-Fi provisioning of IoT devices are limited in all provisioning methods that were covered in this paper, if used correctly. Since the provisioning is done only once in a product lifetime, or at least very rarely. Additionally, during provisioning the network password is transmitted over a short period, at a time controlled by the user. An attacker needs to know exactly when the provisioning is happening, and has a very short period of time to perform the attack. Moreover, the attacker needs to be within the Wi-Fi range of the network at the time the provisioning is taking place. Nevertheless, the importance of security should never be underestimated, and it is critical in many applications.

AP mode, WAC and SmartConfig technology have built-in security. While in AP mode and in SmartConfig the designer must choose to use security in WAC, provisioning security is always used.

The security risk in the WPS push button method is that while the AP is in WPS mode, any Wi-Fi device around can use WPS to connect to the Wi-Fi network.

Robustness and flexibility

Robustness and flexibility are tightly coupled to ease of use, because they relate to the chances that provisioning won’t work or will require troubleshooting. Yet, it deserves a parted discussion, as each of the provisioning methods bears some unique limitations.

The evident limitation of WPS is that not all APs support it. Many of the APs that do support WPS have disabled it by default because of the security breach in the PIN method that was discussed earlier.

AP mode is probably the most robust and ubiquitous Wi-Fi provisioning method. Excluding some new phones that disconnect a Wi-Fi network that is not connected to the Internet, behavior that can be disabled, AP mode provisioning will work in most cases. This is probably the reason most IoT devices and products today use it as their provisioning method.

In cases where robustness is the utmost consideration, an out-of-band provisioning method such as USB should be considered.

Conclusion

We've discussed the predominant Wi-Fi provisioning methods for headless devices and highlighted their merits and challenges. As it is palpable that no provisioning method is perfect, a good practical approach could be supporting more than one option in the product.

In the case of professional or industrial products, AP mode may be sufficient, as it has the best robustness and flexibility. Many IoT products today choose AP mode as their only provisioning method.

In the case of MFi accessories that connect to iPod, iPhone and iPad, WAC is the natural choice. To support provisioning with other kinds of phones, tablets or PCs, an additional provisioning method should be added to the accessory.

When ease of use is critical, WPS or SmartConfig technology are appropriate, because they provide the simplest user experience. SmartConfig technology is a natural choice when phone app experience is desired. WPS is the right choice when phone app is not mandated.

WPS or SmartConfig will cover the majority of products' installations but since they do not work in 100% of all cases, it is recommended to add AP mode as an option to the product as an "expert mode". Users can be directed to guidelines for operating AP mode in case they cannot run WPS or SmartConfig.

Provisioning with SimpleLink Wi-Fi

The SimpleLink Wi-Fi platforms provide customers the most flexibility with provisioning methods by supporting all of the in-band methods discussed here. Through its novel SimpleLink APIs and autonomous Wi-Fi manager capabilities, SimpleLink Wi-Fi makes provisioning a simple task to the product designer. The application can trigger any of the provisioning methods through simple API calls, and TI provides sample software for SmartConfig, AP mode and WPS. The Wi-Fi network name and password are automatically and securely stored in a serial Flash and used by the embedded Wi-Fi manager to connect to the network without any user involvement and with no application code.

The on-chip secured web server (HTTPS) makes AP provisioning extremely easy to design. The designer can incorporate pre-defined configuration tokens into HTML web pages that are stored in the serial Flash and loaded automatically by the web server. To make things even easier, the SimpleLink Wi-Fi devices include a default on-chip web site for provisioning that makes AP provisioning work with no user code or effort at all. Learn more at www.ti.com/simplelinkwifi.

References

[1] Viehböck, Stefan (2011-12-26). "Brute forcing Wi-Fi Protected Setup" (PDF)

[2] Watch this video for a TI provisioning illustration.

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, or other requirements. These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale (www.ti.com/legal/termsofsale.html) or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265