SILICON LABS

The Future of Wi-Fi in Low-Power IoT Devices

Wi Fi™

Importance of Low Power in Wi-Fi

- Wi-Fi is continuously evolving and adding more features like higher throughput, support for denser deployments, and support for low-power devices – all while staying backward compatible with previous versions. As a result, Wi-Fi has emerged as the best wireless protocol to connect devices to the internet.

- Wi-Fi wasn't necessarily thought of as being a battery-friendly solution, but things are changing.

- With new developments, coupled with vendors like Silicon Labs innovating on new solutions, Wi-Fi has become a very viable choice for low-power or battery-operated devices.

Introduction to Wireless Connectivity

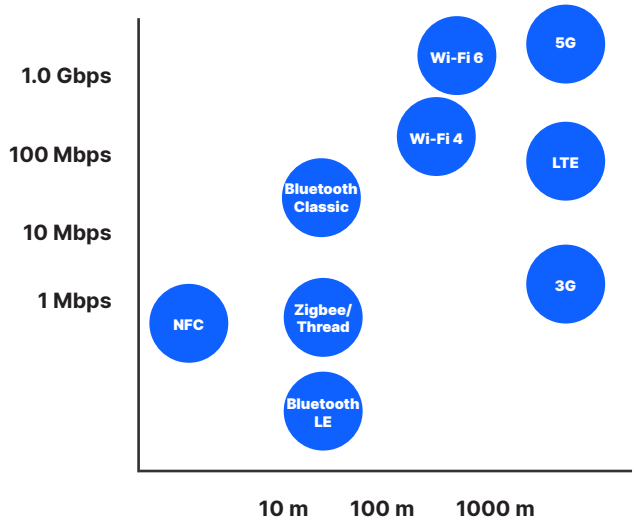
There are a large number of wireless protocols being used in IoT devices, including Wi-Fi, classic Bluetooth, Bluetooth Low Energy (LE), Zigbee, Thread, and cellular. The choice of wireless communication protocols for a particular device depends upon the application, size, cost, power, and several other factors. For example, Bluetooth LE is a good choice for short range, low throughput communication because it doesn't consume much power and it is lower in cost than some other protocols.

Of the protocols mentioned above, Wi-Fi is the most ubiquitous. Commonly used to connect wireless 'things' to the internet, Wi-Fi uses existing infrastructure and is experiencing massive growth in annual deployments:

- **3-4 billion units per year (smartphones, etc.)**
- **800 million are "things" (IoT type products)**
- **200 million are battery powered (need low power)**

Significant gains in power efficiency and cost reduction in Wi-Fi solutions have enabled this growth. Wi-Fi 4 is widely deployed today, and Wi-Fi 6 will further increase the deployment of IoT products.

The chart below shows a simplified view of various protocols and their applications. On the X axis is the effective range of a protocol, and the Y axis shows the application throughput provided by a protocol. Both are in logarithmic scale, so the range on X axis goes over 1,000 meters, and the throughput on Y axis goes over one gigabit per second. As you can see, NFC is at the bottom left of the matrix because it provides the lowest throughput and the shortest range, making it ideal for applications like contactless payment. On the top right with the longest range and highest throughput is 5G.



Between 5G and NFC are a large number of protocols in the middle. For example, Bluetooth Classic is used primarily for audio applications, while Bluetooth LE and Zigbee are primarily used for sensor and control applications due to their low data throughput and low medium range. On the right side of the chart are cellular networks, which provide wide area connectivity and features a range of technologies, including LPWA. This provides low throughput to 5G which, in turn, provides very high throughput. Cellular is typically used as the Internet backbone for mobile IoT devices.

Wi-Fi falls in the middle of the spectrum and provides medium-to-high throughput based on the application requirements. It's also the most widely used wireless standard in the world today. However, it was not the primary protocol for IoT devices until just a few years ago due to its high cost and power requirements. With the reduction in these parameters, 802.11n, also called Wi-Fi 4, has become the dominant protocol in IoT devices. Of the 3-4 billion Wi-Fi deployments annually, 800 million are IoT devices. Two hundred million of those are battery-powered devices. Wi-Fi 6 is expected to further increase this growth trend.

Requirements for Low-Power IoT Devices

As stated before, while Wi-Fi is the most prevalent wireless technology in the world, it was not originally conceived for IoT, but rather for higher power, high throughput applications like personal computers and mobile phones. Generally, the requirements to be met by Wi-Fi solutions tailored for IoT applications are as follows:

- Power consumption in battery-powered IoT devices such as sensors and smart locks require **low power**, and traditional Wi-Fi is not suited for such applications.
- It's important to simplify the IoT development process. Hence, **wireless and networking stack integration** is expected to form a part of any suitable wireless solution.
- Complete **cloud connectivity** with the major cloud providers is a key requirement.
- **Security** from online and physical attacks is necessary in IoT applications where personal information and security of users is required.
- **Cost and size** are also key factors in IoT products, and they vary depending upon the use case.
- **AI (Artificial Intelligence) and ML (Machine Learning)** at the network edge is becoming important. Bringing AI/ML algorithms closer to IoT devices reduces latency and throughput.

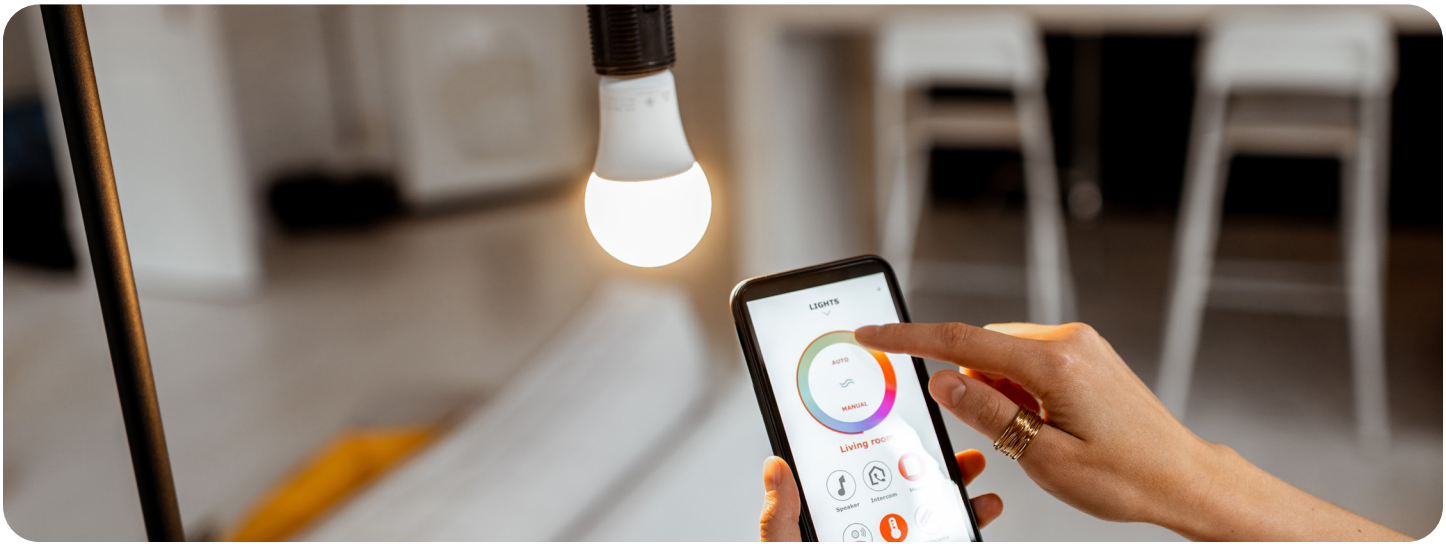
Other requirements for IoT products to be deployed within smart homes are shown in the table below:

Requirements of an IoT Device in a Smart Home

Technical Requirements	Ease of Use	Software and Security
• Ultra-low power for long battery life • Design simplicity • Reduced time to market	• Wi-Fi + Bluetooth LE and IP embedded networking stack • Local and cloud connectivity • Install and Wi-Fi commissioning using Bluetooth LE	• Intuitive software tools for easy programming • Wireless and system security – WPA 2/3, AES encryption, secure boot, key space etc.

The following table gives more specific requirements for specific IoT product types:

Product Type	Requirements
Smart Locks	• Typically battery powered, so low power is a requirement • Low throughput requirements for daily needs, but high throughput requirements for firmware upgrading • Security requirements (SSL/TLS, WPA2/WPA3) are very important • Connection to the cloud is needed for remote control • Bluetooth LE integration for provisioning to Wi-Fi network
Wireless Sensors	• Wall powered, low power may be a requirement due to thermal considerations • Low throughput requirement needs for day-to-day operation, but high throughput needs for firmware upgrades • Connection to the cloud is needed for remote control
Smart Thermostats	• Both battery and line-powered cameras exist. Low power is a requirement for the former • Connection to the cloud is needed for remote monitoring and firmware upgrades
Wearable Devices	• Ultra-low power required for longer battery life • Coexistence with Bluetooth, Bluetooth LE is critical as wearable devices incorporate multiple wireless technologies to meet their application needs • Connection to the cloud for notifications, downloads, streaming, and firmware upgrading • Variable throughput requirements (high throughput for streaming, firmware upgrades, low throughput needed for notifications)
Medical Devices (Insulin Pumps, Glucose Meters, etc.)	• Ultra-low power required for longer battery life • Extensive security requirements as devices are life-critical • Low throughput required



Wi-Fi Operation from a Power Consumption Perspective

There are multiple flavors of Wi-Fi based on different IEEE standards. These typically operate on the 2.4 and 5 GHz bands, using a multitude of modulation schemes. The maximum data rates range from single-digit Mbps to hundreds of Mbps, depending on the antenna configuration and modulation scheme employed. Before developers can understand the best practices for optimizing power consumption and system efficiency, they must first understand the different Wi-Fi technologies and why certain ones have advantages for power-constrained devices.

The following table lists the most common flavors of Wi-Fi:

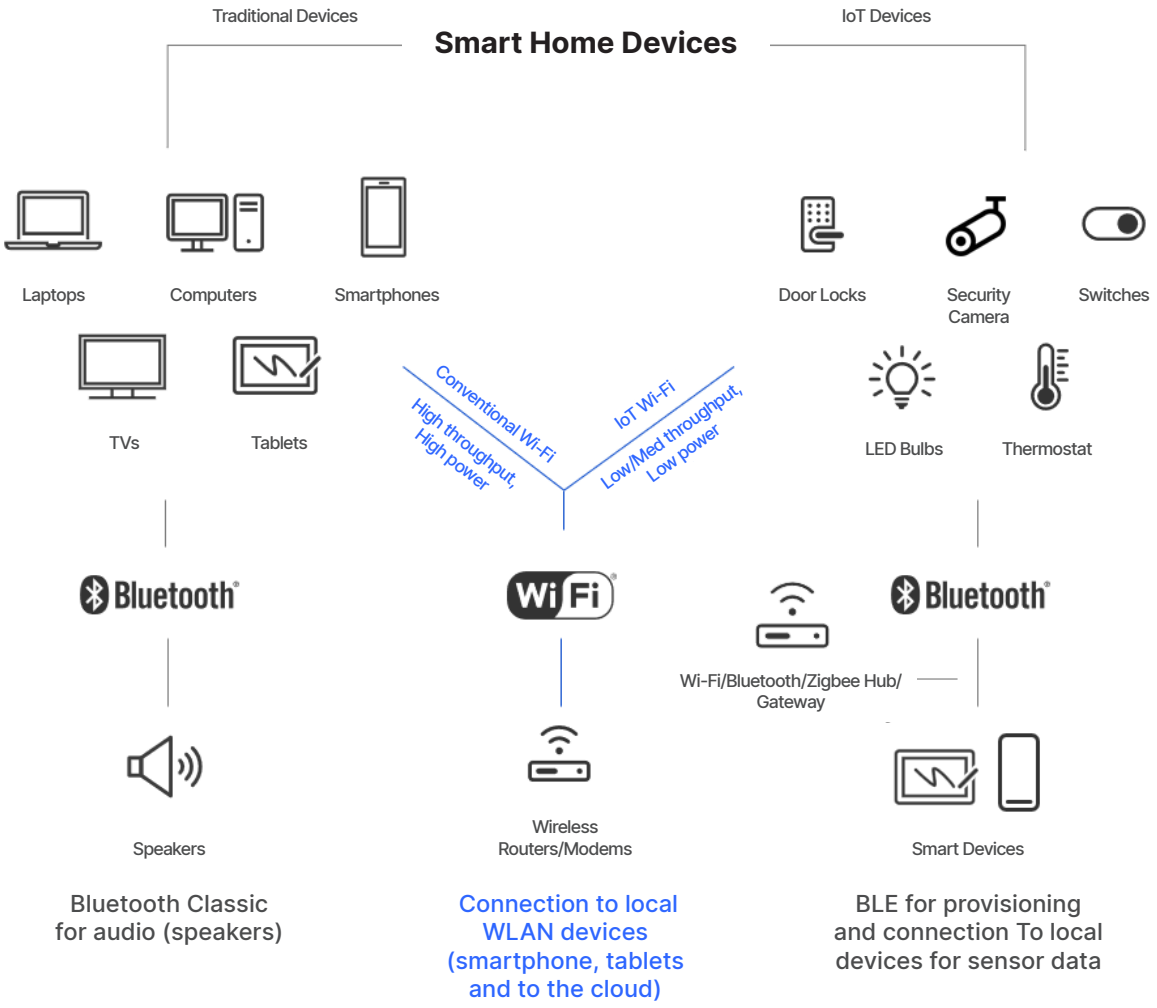
Brand	Technology	Max Speed (Mbps)	Comments
2.4 GHz	802.11 b/g	11-54 Mbps	Historical standard. Superseded by 802.11n (good for IoT Devices)
2.4 & 5 GHz	802.11n	72-600 Mbps	Faster speeds, MIMO support (for higher throughput)
5 GHz	802.11a	54 Mbps	Original 5 GHz standard
5 GHz	802.11ac	Gigabit	Flagship 5 GHz high speed standard (video streaming)
2.4 & 5 GHz	802.11ax	Gigabit	Next-gen Wi-Fi standard (good for IoT and video streaming)
Sub-GHz	802.11ah	< 40 Mbps	New standard designed for sub-GHz Wi-Fi operation

These are some of the key aspects to consider while selecting Wi-Fi standards for IoT applications:

- 802.11 b/g/n are the most popular Wi-Fi standards used in IoT devices and meet the power, range, and throughput requirements for most IoT use cases. They operate on the 2.4 GHz band, which is universally available and widely deployed, making them ubiquitous and ideal for IoT applications
- 5 GHz offers high throughput but shorter range, thus it requires more output power for the same range compared to 2.4 GHz
- MIMO offers higher throughput and range but with higher power consumption and BOM cost
- 802.11ax is a new standard that provides a number of advantages regarding density that are beneficial for IoT application. While most APs currently on the market do not support it yet, and thus IoT devices cannot currently take advantage of it, support for it is increasing, so it will become more prevalent in the future for IoT applications, with expected widescale deployment in the next few years.

802.11 b/g/n are the most popular Wi-Fi standards used in IoT applications.

The Difference Between Traditional Wi-Fi and IoT Wi-Fi



In our homes, we're accustomed to using desktop PCs, laptops, tablets, and smartphones, which connect to the internet using our home Wi-Fi router connected to an ISP. These devices use Wi-Fi solutions that generally focus on high throughput and low latency because they are primarily used for streaming, video conferencing, and other high throughput applications. They require high resource usage, consume a lot of power, require multiple antennas – characteristics that are not suited for typical IoT devices where size, efficiency, and reliable communication are key.

But we're also introducing more and more IoT products into our homes including smart locks, sensors, bulbs, thermostats, and switches. They're generally battery-powered embedded devices that require ultra-low power capabilities and use Bluetooth LE, Zigbee, or Z-Wave. These devices support low power and low throughput, but are not natively IP-based, so they cannot connect directly to the internet for cloud or remote access. Because of this, they require a hub or gateway device to be installed that does the conversion from Bluetooth/Zigbee/Z-Wave to Wi-Fi in order to access the cloud via the home Wi-Fi router. This extra gateway adds cost and complexity to home IoT deployments. Which means that even though these protocols are well fitted for the IoT thanks to their low power, they're not ideal for cloud connectivity.

IoT Wi-Fi devices use standard Wi-Fi protocols and can thus directly connect to the home wireless router, providing a straightforward connection to the cloud. These devices support low-to-medium throughput and provide ultra-low power capability to help bridge the gap in current consumption between the other protocols and Wi-Fi, as well as offer longer range capability through the use of Wi-Fi. Further, since Wi-Fi is the wireless technology being used, there is no added cost of a hub or a gateway. Some devices support multiprotocol operation such as Wi-Fi + Bluetooth and enable easy provisioning of the IoT device to the home wireless router. Since these use standard Wi-Fi protocols, they're compatible with future standards rolled out by the Wi-Fi Alliance and, with their ultra-low power, low resource usage, security capabilities, long-range and low-cost, they're ideal for developing IoT devices. It must be noted that battery life is extremely important as the user should not have to change the battery of such devices very often.

Some IoT applications like wireless sensors are especially cost and space sensitive. Since the number of IoT devices is increasing every day, there's significant crowding in the RF spectrum. IoT devices have to be able to provide robust connectivity in already crowded environments while still using limited power and computing resources. Simplicity is also important for developers and today's wireless and networking stacks are expected to be integrated with the wireless solution as well as provide complete cloud connectivity to providers as well.

Security is becoming more and more important as hackers are trying to break into IoT devices with increasing frequency. In a recent incident, for example, hackers broke into the temperature control system of a hotel and asked for money to fix it. In the case of a smart lock, you do not want any unauthorized person to enter the house or office by hacking into the lock. Because of this, it's important to have the highest possible security.

Because of all of these requirements, the needs of traditional Wi-Fi and IoT are completely opposite to each other, so a one-size-fits-all approach doesn't work. IoT Wi-Fi needs to be different, and this is where Silicon Labs comes in.

We have the industry's lowest power Wi-Fi solutions, which have been deployed in a large number of home, industrial, and commercial applications. These solutions take care of all the requirements mentioned here for IoT in cost competitive packages.

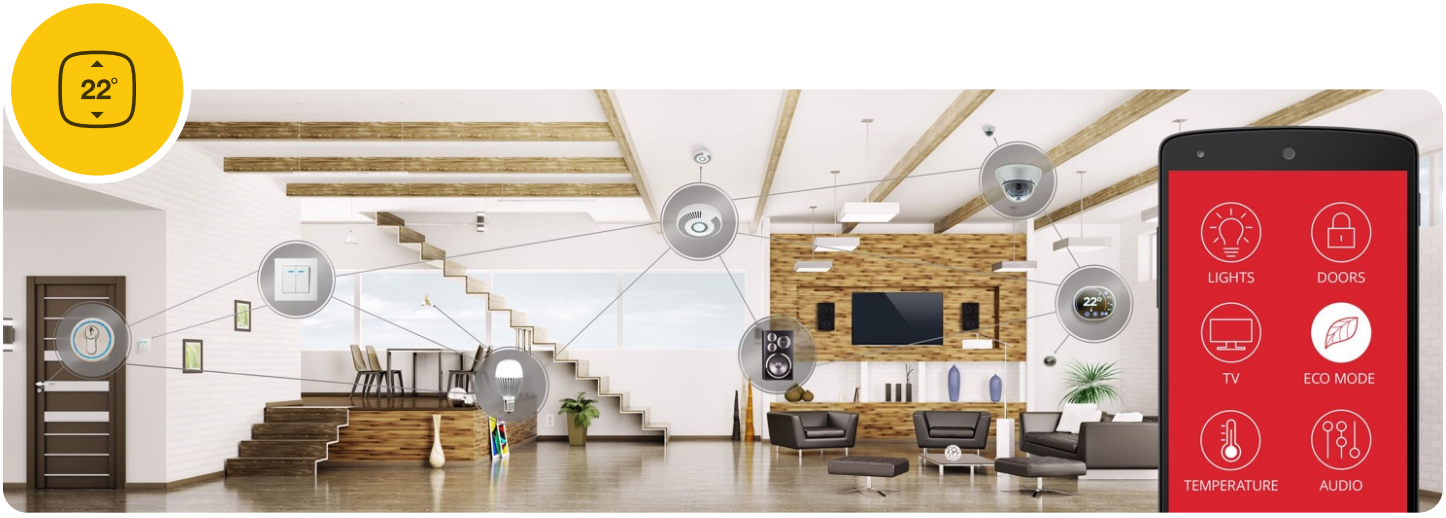
Interoperability of IoT devices is extremely critical, as these devices need to talk to each other to accomplish specific functions. For example, a smartphone may need to communicate to a lightbulb, or a temperature sensor may need to communicate to an AC or heating unit. These devices also use multiple wireless protocols, making it difficult for them to interoperate. This also needs to be taken into consideration when designing Wi-Fi solutions for IoT applications, as coexistence with other technologies such as Bluetooth LE and Bluetooth Classic needs to be factored in with an IoT product's other requirements.

Wi-Fi in IoT Applications

To illustrate the use of traditional and IoT Wi-Fi devices within IoT applications, we'll use the smart home as an example. The image below shows a traditional device, along with IoT Wi-Fi devices like smart locks, security cameras, switches, and lightbulbs. The IoT devices on the diagram may use Wi-Fi and/or other wireless protocols, depending upon their application.

A smart thermostat, for example, is used to control the AC and heating units. It connects to the home router using Wi-Fi, which in turn provides connectivity to local devices, such as smartphones, and cloud connectivity for remote monitoring and control of the thermostat. During regular operation, Wi-Fi throughput requirements for such a device are extremely limited because the communications provided by it are used only for monitoring and controlling of the device. But this changes while the firmware of such a device is upgraded, as the throughput requirements are much higher during such times. At that point, having Wi-Fi is beneficial because it can adapt the used throughput and data rate easily to meet such temporary higher throughput requirements.

Most IoT devices use 2.4 GHz Wi-Fi because it's lower in cost, lower in power, more prevalent in end user's homes, and can provide longer range than 5 GHz solutions. However, the 2.4 GHz spectrum is becoming more crowded, as it has a limited number of Wi-Fi channels and several other protocols, including Bluetooth Classic, Bluetooth LE, and Zigbee, operate in the same spectrum. This is where Wi-Fi 6 comes in.



Wi-Fi 6 Benefits for IoT Devices

Most of today's IoT devices use Wi-Fi 4, and most traditional Wi-Fi devices use either Wi-Fi 4 or Wi-Fi 5. Wi-Fi 6 was introduced in 2019 and infrastructure deployments are currently ongoing. Like 802.11n (Wi-Fi 4), 802.11ax (Wi-Fi 6) operates in both the 2.4 GHz and 5 GHz spectrum. However, it provides several advantages over 802.11n regarding the access of the medium that are particularly useful to IoT devices. The biggest benefit of Wi-Fi 6 is that it can support a large number of coexisting devices in a dense environment, even in the 2.4 GHz spectrum due to its support of orthogonal frequency division multiple access (OFDMA), and MU-MIMO technologies. Since the number of IoT devices is multiplying every year, Wi-Fi 6 will enable them to perform well and coexist without the need to move to either the 5 GHz or 6 GHz spectrum, which would add to the cost and power of IoT devices and typically reduce their range.

Wi-Fi 6 also has a new feature called Target Wake Time, or TWT, which enables the device to wake at target times and look for data instead of periodically waking up. This reduces the power consumption significantly, which is critical for battery operated IoT devices. Additionally, the usage of beamforming and MU-MIMO capabilities in Wi-Fi 6 provides improvements in density and range for indoor deployments. This is especially important as the number of IoT devices deployed is increasing significantly, and thus the importance of density and range is heightened. Thus, having Wi-Fi 6 allows for even more reliable connectivity compared to previous generation of Wi-Fi technologies which is beneficial for IoT applications.

Wi-Fi 6 (802.11ax) is also backward compatible with Wi-Fi 4 (802.11n), which is important because there is already a large number of Wi-Fi 4 devices of all types (access points, computers, mobile devices, IoT devices) deployed across the world, so updating any or all of them to Wi-Fi 6 would not impact compatibility in any significant way.

Optimizing Sleep Mode Power in Wi-Fi IoT Applications

For many IoT applications, most of their time is spent in idle mode and not transmitting data. Wi-Fi standards have several mechanisms to reduce power consumption when devices are not sending or receiving data: Wi-Fi Multimedia (WMM) Power Save, Delivery Traffic Indication Message (DTIM) Intervals, and Unscheduled Automatic Power Save Delivery (U-APSD).

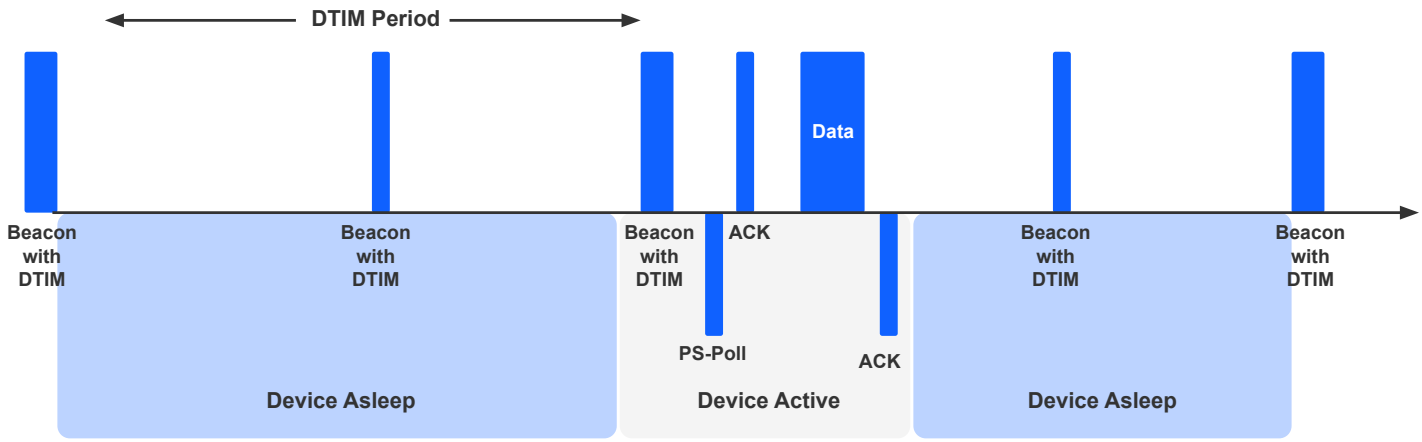
- **Wi-Fi Multimedia (WMM) Power Save:** This approach allows the access point to buffer downlink frames (based on the QoS parameters defined in WMM), making it possible for the client device to doze between packets to save power. WMM doesn't need to send specific PS-Poll requests because it can be triggered with any data frame. Also, for integration with 802.11e QoS, different application types can use different queues so services that can tolerate higher latency will let the device stay asleep longer.

- **Delivery Traffic Indication Message (DTIM) Intervals:** Commercial Wi-Fi APs typically transmit beacons every 100 mSec. DTIM allows Wi-Fi access points to send broadcast or multicast data every 'n' beacons (defined as the DTIM interval), allowing the client to sleep for multiple beacons. This is valuable for power saving since listening to each beacon consumes a lot of receive current and this receive current typically dominates average current consumption. The longer the DTIM interval, the higher the power savings that can be achieved. This, however, comes at the cost of higher latency.

- **Unscheduled Automatic Power Save Delivery (U-APSD):** U-APSD is a part of the 802.11e standard that allows a client to go to sleep when it doesn't have anything to transmit. As soon as the client has data to transmit to the access point, this feature allows it to wake up to do so. After waking up, the client will also check if there is any outstanding data to be recieved. This allows devices with sporadic traffic needs to remain in low power mode for longer periods of time.

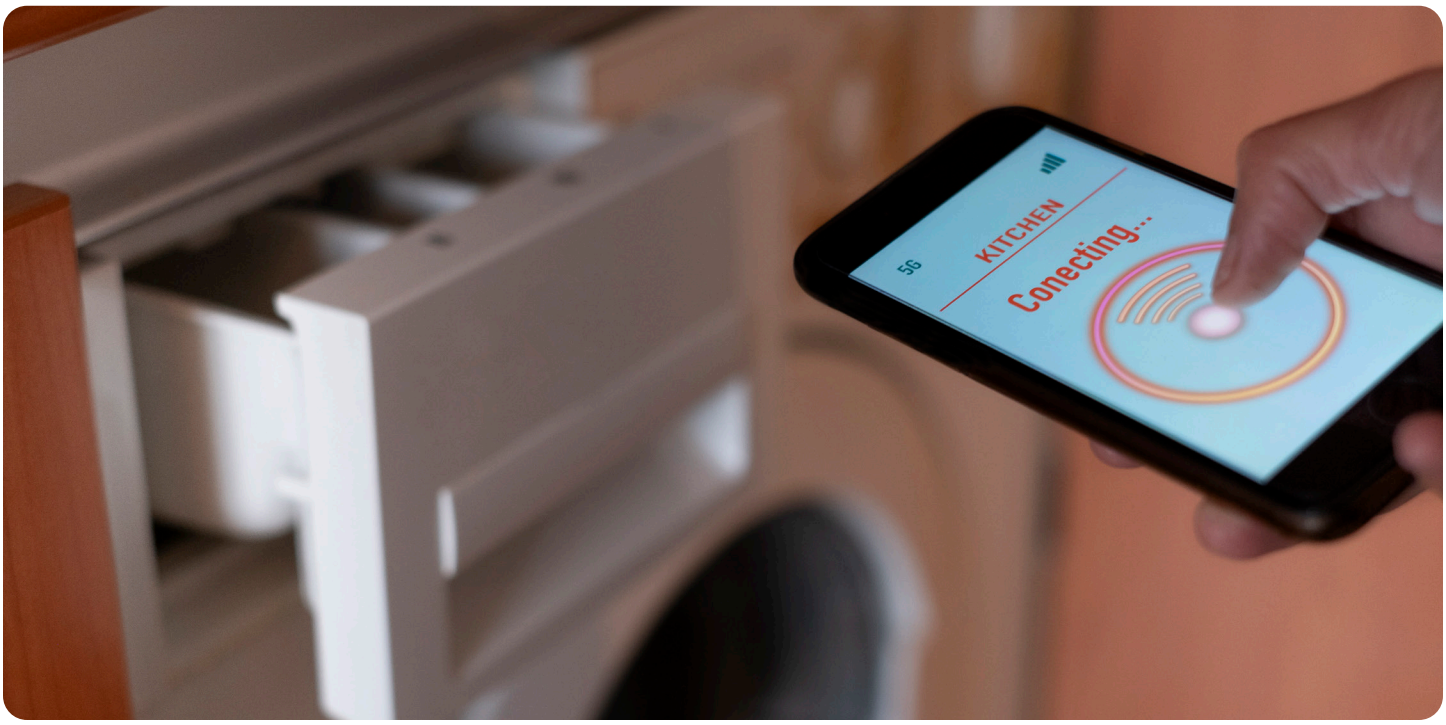
By using the above power-saving mechanisms, the device can remain asleep most of the time it is not sending or receiving data, thus reducing power consumption dramatically. Keep in mind that the device must retain connection information (SSID, keys, IP addresses, etc.) even when asleep. Because of this, this type of sleep mode (often referred to as "associated sleep") consumes a bit more power than a true shutoff mode (as memory must be retained). However, this current is far smaller than the receive or transmit current. For example, an average sleep current number may be < 100 µA, compared to 10's to 100's of mA in TX and Receive modes. This can enable average power consumption for sleepy applications to drop well below 1 mA in many cases, thus increasing battery life for low-power devices.

The illustration below shows an example of a Wi-Fi client achieving energy savings through one of these mechanisms.



What is shown by this graph is the following:

- **Wi-Fi clients (stations) can go to 'sleep' when they have nothing to send**
- **They wake up at 'Listen' Intervals and 'DTIM' Intervals to check whether any data is pending for them**
- **They send 'PS-POLL/NULL' to the AP to retrieve their data**
- **They go to sleep again after retrieving all available data. This enables power savings between data transfers**



The Leader in Low Power Wi-Fi Solutions for IoT Devices

From a design perspective, most IoT devices need to provide robust cloud connection, a good user experience, and get to market as fast as possible. Hence for designers, IoT Wi-Fi or Low Power Wi-Fi solutions are the best choice to enable IoT devices to natively connect to the internet, as Wi-Fi is the most prevalent protocol already available in home and office and takes advantage of the low power mechanisms available with the Wi-Fi protocol to enabled battery operated devices to last longer for an overall better user experience. Designers should look to integrate low power Wi-Fi as part of their design in conjunction with other protocols such as Bluetooth, Zigbee, Thread, Matter, and Z-wave to enable true IoT devices.

Silicon Labs' portfolio of SoCs and modules is the quickest way to build and connect your Wi-Fi, Bluetooth, Zigbee, Thread, Z-Wave, or Matter applications to the internet. Our solutions are designed specifically solutions are designed specifically for the IoT, where RF performance, low power consumption, and fast time-to-market are critical. Created to be scalable and compatible with all major ecosystems and emerging standards, our low-power Wi-Fi solutions are also designed to simplify coexistence with the other protocols. Today's devices need to be able to manage a lot of operations across standards, and as a full-system provider we've removed the complexity of this design challenge so you can focus on your application. Silicon Labs has put in a significant amount of time in creating the hardware and software solutions needed to optimize power in IoT devices. Because of this, we're the leader in low-power Wi-Fi 4 for IoT and look forward to our Wi-Fi 6 solutions reducing power consumption even further.

For a closer look at our approach to low-power IoT Wi-Fi development, explore our portfolio and read Novus Labs' AWS IoT Wireless interoperability Report, which looked at Silicon Labs' RS9116 Wi-Fi module and its performance across a variety of conditions that IoT devices face in the home or office.