SILICON LABS

Transform Wi-Fi Gateways into Multiprotocol IoT Infrastructure for Smart Homes

How to turn legacy Wi-Fi-only gateways into an energy- efficient, high-performing, and future-proof multiprotocol IoT infrastructure and roll it out to millions of smart homes.

This whitepaper discusses the key challenges of introducing Matter and Thread 802.15.4 protocols on Wi-Fi gateways. It describes three solutions for manufacturers and Internet service providers (ISP) to optimize Wi-Fi coexistence, antenna coverage, and energy consumption on IoT-enabled Wi-Fi home gateways. Test results and calculations are included to quantify the potential wireless performance gains, antenna coverage improvements, and gateway energy savings.

Authors: Christopher Ince, Wael Guibene, Kornel Nagy, Kris Young, Mikko Nurmimaki

Introduction

From Broadband to Smart Home

The number of global fixed broadband internet connections grew from 200 million to 1.5 billion during the first two decades of the 2000s. However, according to the OECD Broadband Portal, the fixed broadband markets in most developed countries have now saturated. This has intensified competition among internet service providers (ISPs), increasing customer acquisition costs, price erosion, and churn, finally impacting the ISP's financial performance.

Smart home services and IoT connectivity technologies have quickly emerged as one of the most promising business areas for internet and telecom service providers to expand their broadband business. The benefits make it clear why, including:

Business – Smart home and IoT help service providers enable new revenue sources, improve customer value-add, and strengthen customer retention, thus improving their subscription business.

Retention – The Smart home IoT device offering proliferates rapidly, expanding from Wi-Fi devices to devices using Thread, Zigbee, Bluetooth, and other IoT protocols. ISPs will want to deliver home connectivity for all types of IoT devices today and in the future to increase subscription retention.

Positioning – Owning the home IoT infrastructure, e.g., OpenThread Border Router (OTBR) capability, allows service providers to claim a strategic position in the greater smart home ecosystem and do meaningful and sustained business alongside global smart home ecosystem brands such as Amazon, Apple, Google, and Samsung.

Data – Controlling and monitoring IoT smart home devices can provide service providers with invaluable user behavior data, allowing them to better position future offerings.

From Wi-Fi to Multiprotocol IoT

The smart home consumer device market is proliferating rapidly, and high-bandwidth, power-hungry Wi-Fi will not be the optimal connectivity protocol for all device types. In fact, many emerging IoT devices, such as smart locks, thermostats, and contact sensors, will benefit from more energy-efficient and lightweight mesh connectivity technologies including Thread, Zigbee, Z-Wave, and Bluetooth Low Energy (LE).

The leading ISPs and Telcos are now integrating new IoT capabilities on their legacy Wi-Fi customer premises equipment (CPE) to prepare for the smart home business and claim their position in the ecosystem play.

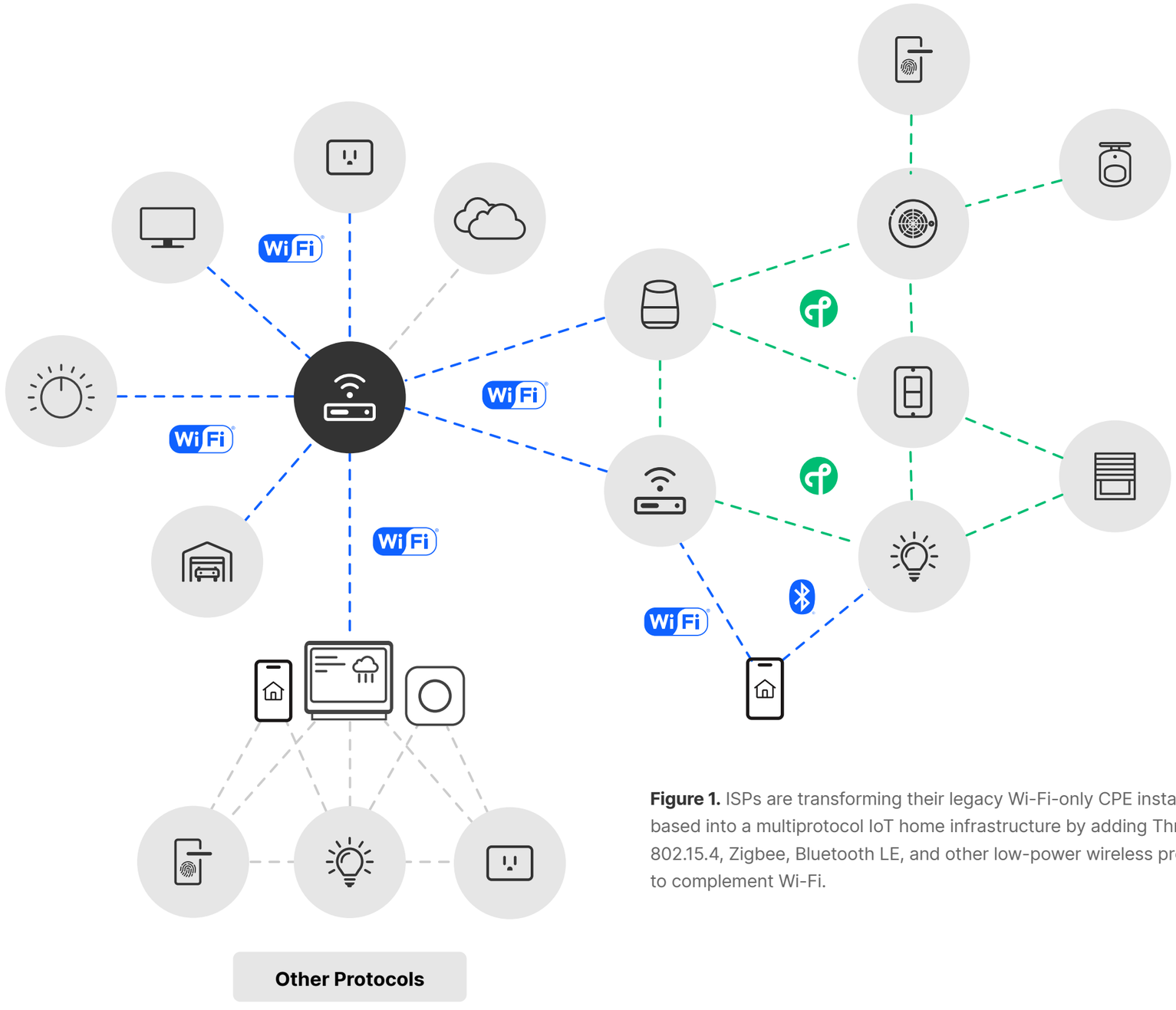


Figure 1. ISPs are transforming their legacy Wi-Fi-only CPE installed based into a multiprotocol IoT home infrastructure by adding Thread 802.15.4, Zigbee, Bluetooth LE, and other low-power wireless protocols to complement Wi-Fi.

ISP Smart Home Challenge

We are witnessing a trend of ISPs recognizing that it's their role to own the wireless IoT infrastructure of connected smart homes. However, the main challenge many of them face is their legacy Wi-Fi-only CPE infrastructure, which historically does not support low-power IoT connectivity technologies such as Thread, Zigbee, Z-Wave, or Bluetooth LE. Consequently, moving from Wi-Fi-only to a multiprotocol IoT world introduces new technical challenges, including:

- How to establish an IoT anchor point such as an OpenThread Border Router (OTBR) in homes
- How to optimize wireless co-existence on the shared 2.4GHz band
- How to maximize low-power IoT performance without compromising Wi-Fi throughput
- How to increase gateway antenna coverage to improve wireless user experience at homes
- How to reduce gateway power consumption to align with new energy regulations

Building a Multiprotocol IoT Infrastructure

IoT Protocols

The smart home IoT device market is proliferating rapidly, and Wi-Fi will be just one of the many wireless protocols used. Ecosystem providers such as Amazon, Apple, Google, and others have arrived to unify the siloed smart home ecosystem industry through the unified Matter protocol, where devices can communicate across ecosystem boundaries via a common device data model over Wi-Fi, Thread, and Bluetooth LE protocols.

At the same time, global consumer device manufacturers such as Apple are incorporating Thread into smartphones, tablet computers, laptops, and TVs, enabling their users to control smart home devices easily. Thus, they are accelerating the evolution toward a multiprotocol smart home reality.

While Matter is becoming a major smart home wireless technology, it will not be the only one. Zigbee remains an established ultra-lightweight mesh protocol ideal for smart lights, switches, and many other applications. Z-Wave, the sub-GHz mesh protocol, continues to support applications that need ultra-low power and ultra-long range, e.g., home security and monitoring. In conclusion, many relevant protocols will coexist with Matter and can even be integrated into the ecosystem via standard-based bridging solutions.

This whitepaper, however, focuses on helping service providers explore the challenges and opportunities in Matter. It introduces solutions for expanding their existing Wi-Fi offering with Thread, thus allowing them to cover both wireless connectivity technologies in Matter.

Matter Gateway

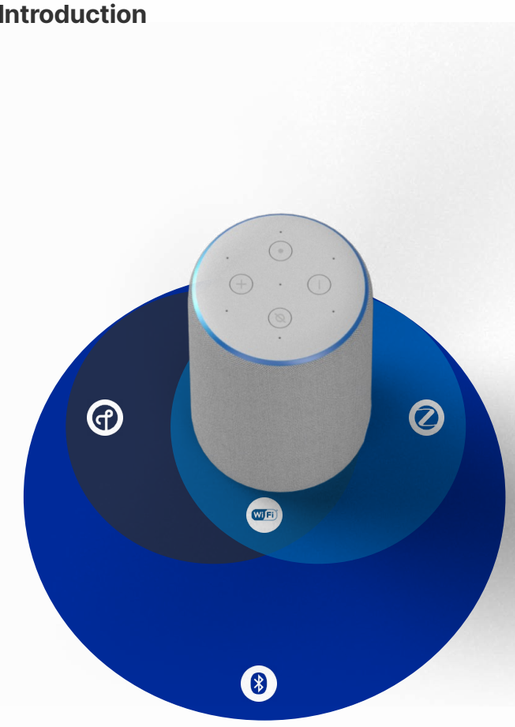
Enabling the wireless IoT infrastructure is the first step toward a scalable and future-proof smart home business. Wi-Fi has proven to be the most ubiquitous foundation for the home network and virtually all service providers already offer Wi-Fi in their consumer home gateways. However, the future of smart home devices does not lie in Wi-Fi alone. It is not an optimal wireless protocol for all device types. If we assume that Matter will continue to gain momentum and proliferate the home, then it would make sense for the home infrastructure to support all things that Matter is comprised of – Wi-Fi, Thread, and Bluetooth LE.

To participate in the Thread network, a Thread radio would need to be incorporated into the home gateway or router. This will allow for the gateway or router to become an Open Thread Border Router (OTBR). An OTBR is an open-source implementation of a Thread Border Router that acts as a gateway between a Thread network and other IP networks, such as Wi-Fi. In addition, this radio will allow for the OTBR to also be a Thread network controller or access point (AP). Like the Wi-Fi ap, a chip is integrated into the gateway, and the Thread chip similarly controls the Thread network and Thread devices entering that network.

If you want to enhance your business role from a Wi-Fi-only connectivity provider to offering value-added complete smart home applications to your customers, the Silicon Labs MG21 and MG24 will enable the Matter Gateway capability on your CPE. This will allow you to see the entire IoT network in the home, gather data from that network, control it, and ultimately increase revenue through your branded Matter ecosystem of bundled devices and applications.

Wi-Fi Coexistence on Gateways

Introduction

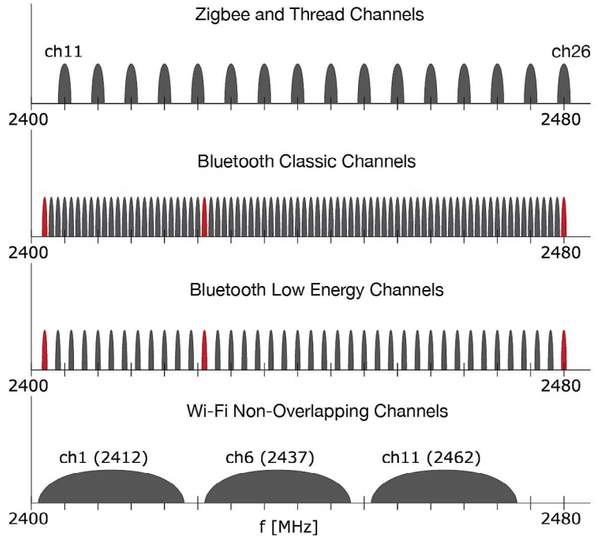


From Broadband to Smart Home

With the legacy Wi-Fi-only CPEs, service providers didn't have to worry about multi-radio/multiprotocol interference on the 2.4GHz band. The entire band was available for Wi-Fi. However, with new smart home gateways combining Wi-Fi and IoT radios such as 802.15.4 and Bluetooth LE, service providers will face new challenges:

- How to increase receiver (RX) sensitivity to optimize IoT network performance on gateways
- How to optimize the RF performance for the IoT protocols without compromising the Wi-Fi throughput

Wi-Fi and wireless IoT protocols have different modulation schemes, channel frequencies, and bandwidth, but they can overlap when co-located on the 2.4GHz band. Signals from one wireless protocol appear as unwanted noise for the other protocols. The radio cannot properly receive messages if the desired receive signal is weaker than the noise.



Wireless coexistence technologies allow multiple technologies, including Wi-Fi, Thread, Zigbee, and Bluetooth LE, to operate on the 2.4GHz band without signals from one radio interfering with adjacent radios. Several alternatives exist to implement Wi-Fi coexistence on gateways and they are generally divided into **unmanaged** and **managed** techniques.

Unmanaged Wi-Fi Coexistence

Unmanaged Wi-Fi coexistence techniques typically involve separating the radios using different frequency bands, tuning protocol stack parameters, and increasing antenna isolation. The table below gives an overview of unmanaged Wi-Fi coexistence solutions.

Smart home devices and gateways are trending toward higher Wi-Fi transmit powers and throughputs. Unmanaged coexistence techniques do not scale for these high-duty-cycle Wi-Fi use cases. Silicon Labs recommends deploying managed coexistence solutions on multiprotocol IoT gateways. Yet unmanaged coexistence techniques are still recommended to complement managed solutions.

UNMANAGED COEXISTENCE TECHNIQUES

Frequency Separation	20MHz Wi-Fi Bandwidth	Antenna Isolation	Optimize Protocol Configurations
Wi-Fi and IoT protocols are configured far apart from each other on the pass band (low vs. high channel frequencies) to minimize Wi-Fi blocking other protocols.	Set Wi-Fi to run on 20MHz to avoid the side bands of the third-order distortion products from the OFDM sub-carriers block IoT protocols.	Minimize the Wi-Fi energy seen by the IoT radio by increasing antenna isolation (distance, direction) to improve the EFR32 receive range.	Configuring protocol parameters to minimize interfering transmission overlaps.

Managed Wi-Fi Coexistence

Managed Wi-Fi coexistence is a prerequisite for multiprotocol IoT gateways with high-power Wi-Fi radio and throughput-intensive traffic. Managed coexistence technology actively coordinates access to the shared frequency band for the co-located Wi-Fi, 802.15.4, and Bluetooth radios, preventing overlapping transmission.

The table below describes the main aspects of three advanced managed Wi-Fi coexistence solutions, which are available on Silicon Labs EFR32 multiprotocol wireless IoT products:

- Packet Transmission Arbitration (PTA)
- Duty-cycled PTA (a.k.a. PWM)
- Signal Identifier (Silicon Labs patented).

MANAGED COEXISTENCE SOLUTIONS

PTA	Duty-Cycled PTA	Signal Identifier
PTA coordinates actively access to the shared 2.4GHz band for Wi-Fi and IoT protocols (802.15.4, Bluetooth). Requests idle time slots to allow TX and RX windows for IoT High duty-cycle Wi-Fi transmit from the gateway blinds IoT radio, resulting in low probability of IoT protocol accessing the shared 2.4 GHz band. Decreases IoT throughput.	Duty-cycled PTA interrupts the Wi-Fi periodically to acquire ample idle windows for the IoT signal (802.15.4, Bluetooth). Regular interruptions degrade Wi-Fi throughput even if there were no IoT packets to be received.	Signal Identifier detects IoT signal (802.15.4, Bluetooth) from any part of the packet during Wi-Fi inter-frame spacing (IFS). Interrupts Wi-Fi only when an IoT signal is detected. Minimizes Wi-Fi throughput degradation. Only halts Wi-Fi when there is active IoT traffic. Provides the most optimized balance for co-located high duty-cycle Wi-Fi and low-power IoT.

Packet Transmission Arbitration

Packet Transmission Arbitration (PTA) is a recommendation that was originally described in the IEEE 802.15.2 (2003) specification, in clause 6, to address coexistence between 802.11b (Wi-Fi) and 802.15.1 (Bluetooth Classic) to reduce packet collisions between co-located radios using different wireless protocols in the same frequency band.

Silicon Labs EFR32 products support PTA to coordinate shared media access between the 802.15.4 (Thread, Zigbee), and Bluetooth LE protocols and an adjacent Wi-Fi radio. When the EFR32 requires access to the shared band, it sends a signal to the Wi-Fi device (through GPIO), postponing Wi-Fi transmission to free up the media. Multiple PTA negotiation protocols are available: 1-wire, 2-wire, 3-wire, and 4-wire.

How does PTA work?

PTA coordinates transmissions between main and secondary radios that are co-located and share a common frequency band. The PTA main decides which of the two radios can transmit at any given time based on handshake signals exchanged over GPIO connections between the two radio devices. The PTA secondary responds with handshake signals based on the packet transfer requirements of both devices. The PTA works along the following process:

1. IoT device asserts a **request** to transmit/receive packets. The request can optionally include a **priority** level
2. Wi-Fi radio device accepts the request and **grants** a time slot for IoT transmit/receive
3. Wi-Fi device stops transmitting, allowing the IoT device to transmit/receive
4. When done IoT device de-asserts the request, and the Wi-Fi device releases grant.

Duty-Cycled PTA

The IoT radio does not know when an incoming packet will arrive and must capture the preamble portion of the packet to detect and receive it. When the Wi-Fi transmit duty cycle increases, idle periods adequate for a successful preamble capture decrease, thus increasing IoT packet loss and retries.

In duty-cycled PTA (a.k.a. PWM), the EFR32 IoT radio has a regular and periodic time slot to request media access from the adjacent Wi-Fi radio. However, Wi-Fi will still decide whether to grant access to each PTA request based on its discretion.

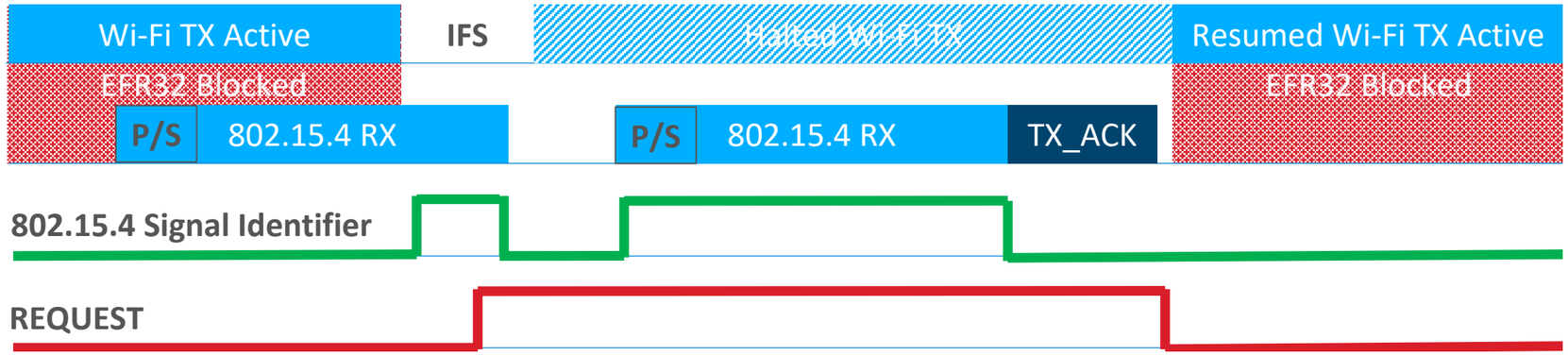
Thanks to the periodic requests to interrupt the Wi-Fi transmission, the duty-cycled PTA increases the opportunities for the IoT radio to access the shared medium in case of intense 2.4 GHz Wi-Fi transmission from the gateway. The downside of duty-cycled PTA is Wi-Fi 2.4 GHz performance degradation even if there is no IoT activity. Additionally, the exact PTA request time window and duty cycle must be coordinated with Wi-Fi beacons to avoid collapsing the Wi-Fi network.

Signal Identifier

While the duty-cycled PTA improves the IoT performance during periods of intense Wi-Fi 2.4 GHz transmissions, it can have a drawback in some cases: It reduces Wi-Fi throughput even if there is no active IoT traffic. Signal Identifier is a patented technology by Silicon Labs that detects IoT signals (802.15.4, Bluetooth) during Wi-Fi inter-frame spacing (IFS). It interrupts the Wi-Fi radio only when an IoT signal is detected. Signal Identifier can detect an IoT signal from any part of the packet stream, i.e., capturing the protocol preamble header is not a prerequisite, increasing the detection probability and reducing retries. Signal Identifier works together with PTA. Upon positive signal detection, a PTA request is asserted to halt Wi-Fi transmission to free up the shared media.

How Signal Identifier works?

When the 802.15.4 signal detector detects a signal during the Wi-Fi IFS, a PTA request is asserted to halt Wi-Fi transmission and allow the retransmitted IoT packet to be received. The request is de-asserted after the device has successfully received the IoT packet, confirmed by an acknowledgement. If an 802.15.4 packet is not received within the programmable Receive Retry timeout, the PTA request is de-asserted, allowing Wi-Fi operation to resume.



Comparison of Managed Wi-Fi Coexistence Solutions

The following test showcases the pros and cons of the duty-cycled PTA, and Signal Identifier managed coexistence solutions compared to a scenario without a managed coexistence solution. The test setup uses Silicon Labs WF200 running Wi-Fi 4 and EFR32MG24 running Zigbee to simulate a multiprotocol IoT gateway comprising a co-located Wi-Fi 2.4 GHz radio and 802.15.4 radio. The WF200 streams Wi-Fi 2.4 GHz data at a high transmit duty cycle. The EFR32MG24 is being sent periodic 802.15.4 packets at a low signal level to simulate packets arriving at a gateway from a remote device.

Test Cases	Test results - Performance impact		Conclusions
	Wi-Fi 2.4 GHz	802.15.4	
No Managed Coexistence	Wi-Fi dominates the band. **Almost no degradation of maximum throughput**	Low 802.15.4 performance. **~20-30% packet loss (application level) ~200-400% retries (MAC level)**	High Wi-Fi throughput but severely degraded 802.15.4 performance.
Duty-cycled PTA (80%Wi-Fi, 20% 802.15.4)	Wi-Fi grants idle time for 802.15.4 regularly even if no IoT traffic is present. **~7-15% degradation of maximum throughput**	Improved performance. 802.15.4 has dedicated time slots for listening. **~0% packet loss ~40% retries**	Wi-Fi throughput is clearly impacted due to allowing 802.15.4 regular band access
Signal Identifier	Wi-Fi grants idle time for 802.15.4 when IoT traffic is present. **Almost no degradation of maximum throughput**	Improved performance. 802.15.4 radio listens for IoT traffic during Wi-Fi IFS. **~0% packet loss ~30-50% retries**	**Signal Identifier provides optimal balance: Highest Wi-Fi throughput with ample capacity for 802.15.4 when there is active traffic.**

Conclusion – Choosing the Right Wi-Fi Coexistence Solution

A gateway manufacturer or service provider can choose between multiple managed Wi-Fi coexistence solutions when developing a multiprotocol IoT gateway. However, not all solutions are alike.

- Choosing **no managed coexistence** delivers end users ample Wi-Fi 2.4 GHz throughput with a minor degradation for this test case. However, users of 802.15.4 devices could suffer severe performance degradation because Wi-Fi 2.4 GHz tends to blind out IoT traffic.
- **Duty-cycled PTA** significantly improves 802.15.4 performance with regular listen intervals for IoT traffic. However, because Wi-Fi transmission is halted regularly (even if no IoT traffic is present), users can experience a degradation of the maximum throughput of up to ~7-15% for Wi-Fi 2.4 GHz.
- The managed coexistence solution based on **Signal Identifier** and PTA provides an optimal balance for Wi-Fi and 802.15.4 performance. It minimizes Wi-Fi 2.4 GHz impact with almost no degradation of maximum throughput for this test case while allowing 802.15.4 (Zigbee, Thread) protocols ample access to the shared media whenever there is active IoT traffic.

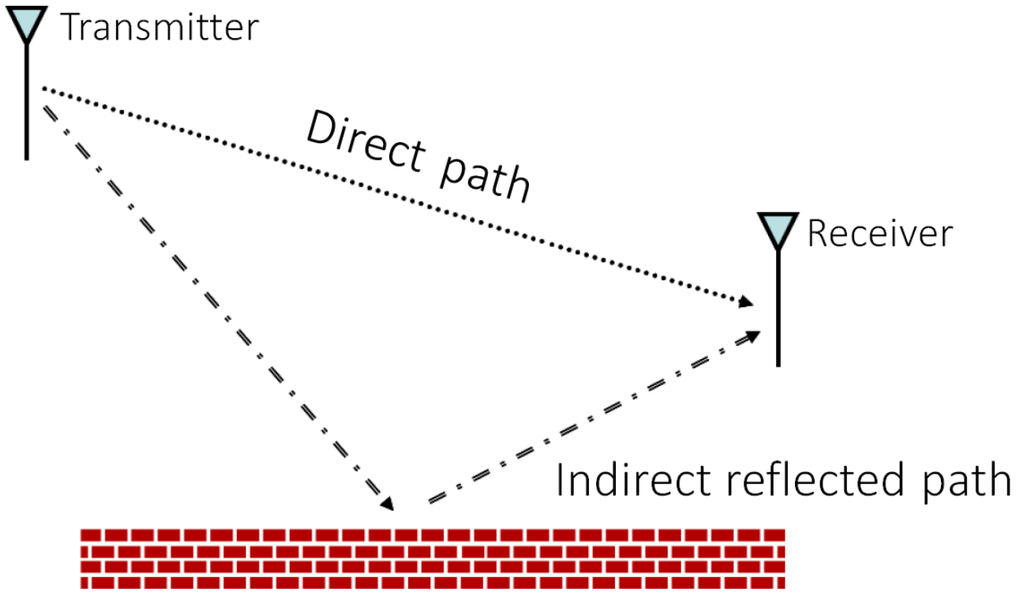
Learn more about Wi-Fi coexistence:
UG103.17 Wi-Fi Coexistence Fundamentals

Gateway Antenna Coverage

Every home imposes a unique combination of wireless challenges to Internet Service Providers. They have no control over where CPEs are placed in homes (subscribers typically place the CPE near their broadband wall outlet). Consequently, gateway antenna coverage varies from one home to another, leading to unpredictable wireless IoT connectivity and user experience.

Multipath Propagation

Metal objects in the home will reflect radio waves, causing multiple transmission paths, which can lead to deep attenuation due to destructive interference at the antenna. IoT devices will have various antenna types and placements, potentially leading to polarization losses between the gateway and the device. The compact form factor from the industrial design of most routers and gateways can lead to deep nulls on the opposite side of the assembly from the IoT antenna. Every home has a unique RF environment and RF issues can deteriorate user experience, cause frustration, and thus can burden service providers' customer service centers, and increase operational costs.

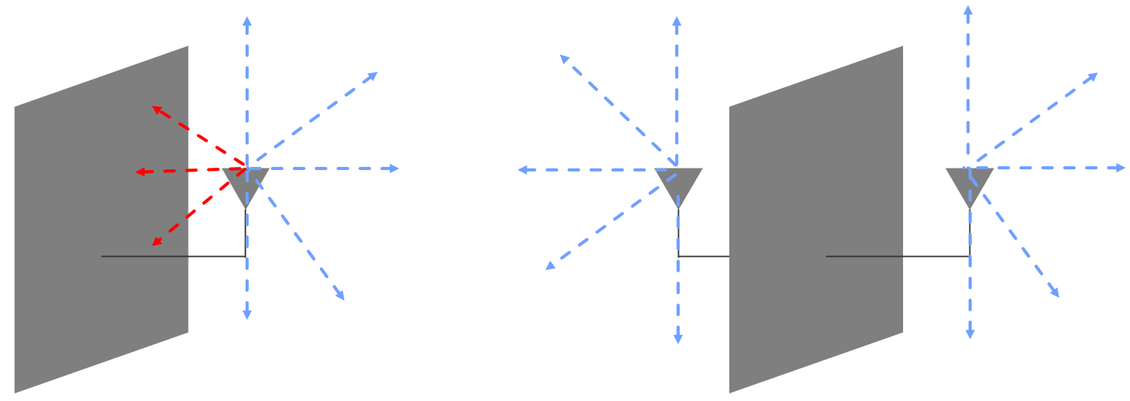


Multipath propagation: Line of sight (LOS) signal path vs. reflected signal

Antenna Diversity

Antenna diversity, available for 802.15.4 on the Silicon Labs MG24 multiprotocol SoCs, is a technique for using two antennas to help overcome potential RF issues in a home environment. Antenna diversity works to help improve reception by constantly switching between two antennas. When a signal is detected on one antenna, the other antenna is sampled to determine which has a better signal. The antenna with the best signal is then used to receive the remainder of the packet. The switching of the antennas can impact sensitivity. However, the positive RF performance improvement provided by antenna diversity exceeds the disadvantages of a potential sensitivity loss.

Antennas can be spaced apart to help avoid destructive interference from multi-path due to reflections. Depending on the gateway device's form factor, spacing the antennas apart can also achieve a more uniform antenna pattern around the gateway (see figure below). In the figure, signals from the single antenna are blocked in some directions by the body of the gateway unit. With diversity, signal coverage is provided in all directions. The diversity antennas can be implemented with opposite polarizations, which can help recover polarization losses between the gateway antennas and the antenna of the IoT end device.



No Antenna Diversity

Antenna Diversity

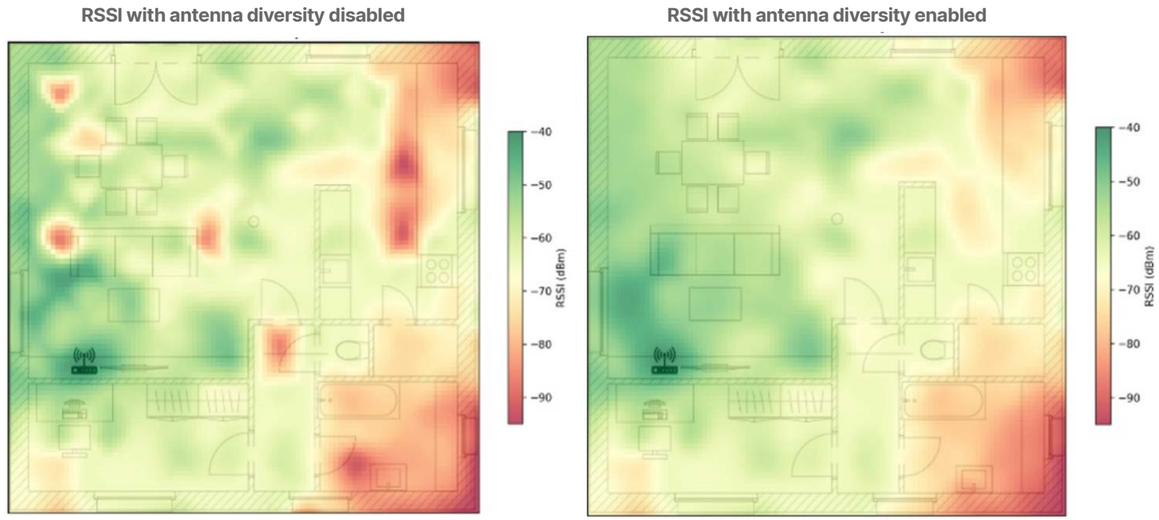
Antenna diversity can deliver significant wireless link budget and range improvements for IoT home gateways, especially when signal conditions are near end-of-range sensitivity levels and in challenging RF conditions. Silicon Labs provides a built-in antenna diversity algorithm that removes the need for the service provider to implement any additional firmware on their gateway microcontroller. This unlocks the benefits of antenna diversity without algorithm development and debugging, resulting in a more robust solution and a faster time to market.

Gateway Antenna Coverage Test in Real Home

To evidence the advantages of antenna diversity in real home environment, a test was conducted to compare antenna coverage in two scenarios: an IoT hub with antenna diversity and an IoT hub without antenna diversity.

A series of Received Signal Strength Indicator (RSSI) measurements were conducted in multiple locations in an apartment with two EFR32MG24 devices. One of the devices was equipped with an antenna diversity radio board (BRD4188B) and it was placed in a fixed location to simulate an IoT hub (see the router/hub icon on the floor layout diagrams). The other device was moved around the apartment to simulate an arbitrary IoT device. Otherwise, the environment was stationary during the time of taking the RSSI measurements. Both devices ran a range test application (available in Simplicity Studio), which simplified measuring RSSI values in multiple locations.

The two heatmap diagrams below represent the RSSI values measured in different locations of the apartment in both scenarios. Red denotes areas of low RSSI values, representing low power (receiver sensitivity) and weak antenna coverage. Green denotes areas of high RSSI values, representing high power (receiver sensitivity) and strong antenna coverage. Yellow denotes areas with acceptable power level (receiver sensitivity).



No Antenna Diversity

Antenna Diversity enabled on the 802.15.4 hub

In some areas of the floor plan in the no antenna diversity scenario, there are “blind” spots where the RSSI values drop drastically (red spots on the floor map). This is due to the destructive interference caused by multipath propagation.

This test clearly evidences the greatest advantage of antenna diversity: it generates a stronger and more evenly spread antenna coverage across the apartment floor plan. The antenna diversity heatmap shows that there are no weak RSSI spots thanks to two antennas in the hub device. Antenna diversity in the IoT hub device does not increase receiver sensitivity, which is why it does not technically extend coverage in the apartment. However, it significantly improves the quality of the coverage within the range of the apartment.

Conclusions on Antenna Diversity

Internet service providers typically find homes challenging RF environments. They have no control over how well CPEs can connect to IoT devices. Yet customer satisfaction and customer care costs are highly dependent on the quality of connectivity. Antenna Diversity on Silicon Labs MG24 multiprotocol SoCs delivers a stronger and more uniform antenna radiation pattern up to 360 degrees around the gateway, improving the quality of antenna coverage, enhancing user experience and decreasing operational support costs for service providers.

More about Antenna Diversity:

Read our App Note 882 for an in-depth overview of Antenna Diversity on Silicon Labs MG24. If you want to know how to use Antenna Diversity with MG24, check out App Note 1294 for configuring Antenna Diversity for OpenThread.

Gateway Energy Consumption

Introduction

IoT devices such as smart thermostats, lights, security sensors, and cameras offer unprecedented convenience for their users. However, the proliferation of smart home devices also increases energy consumption directly and indirectly. CPE, such as gateways and routers, is the backbone of a connected home. CPEs are typically always on to ensure critical applications like security cameras and leak detectors remain operational in all circumstances. However, CPE draws full power even when there is no activity in the network, like at night or when the user is away on vacation, increasing energy costs.

Energy regulations, such as the new, stricter EU Ecodesign Standby Regulation 2023/826 (HiNA), effective 2027, will limit the standby power consumption of consumer CPE significantly to save household energy consumption. It forces service providers to reduce gateway energy consumption to the extent that a significant share of the CPE elements, such as the microprocessor and Wi-Fi radio, must be put to sleep during inactivity. However, CPE sleep mode leads to complex challenges for service providers: how can critical applications such as security systems be kept operational during gateway sleep? How do you wake up the gateway when a need arises?

Wake on Thread/Matter solution

Silicon Labs' patent-pending Wake on Thread/Matter solution can significantly improve gateway energy efficiency by enabling CPE to sleep during idle periods and wake up instantly when necessary. The mesh connectivity allows IoT devices to trigger wake-ups autonomously and automatically when they need connectivity. While saving gateway energy consumption, this solution also keeps critical smart home applications operational and improves the user experience – users don't have to worry about switching the CPE on or off.

How Does it Work?

The intelligent wake-up trigger feature allows the CPE to go into a deep sleep, drawing minimal power while remaining ready to wake up in response to activity within the smart home. For instance, if a motion sensor detects movement or the homeowner opens a smart lock, the CPE instantly wakes up and resumes full connectivity. This seamless transition between sleep and active modes ensures that users experience the convenience and security of a smart home without unnecessary energy costs.

Matter and Thread Integration

Silicon Labs' Wake on Thread/Matter solution fully exploits the capabilities of the Matter and Thread protocols by enabling wake-up events triggered by these protocols. For example, a device that supports Matter or Thread—such as a smart thermostat or security sensor—can signal to wake the CPE from its sleep mode. This ensures that while the CPE is in a power-saving state, it can still respond instantly to critical events without users worrying about losing functionality.

This approach is particularly beneficial for applications like security systems and energy management. Security cameras or motion sensors can remain connected to the network while consuming minimal power, waking up the CPE only when activity is detected. Similarly, environmental controls such as smart thermostats can wake the CPE when temperature adjustments are needed, ensuring a comfortable home environment without wasting energy.

Estimating Gateway Energy Savings

This section describes three example use cases for the Low-Power Mesh Technology and estimates how much energy a CPE could save if the technology were used, and the gateway operated in sleep mode.

Night Mode

At night, most homes see minimal activity. Devices like smart lights, security cameras, and sensors typically remain in standby mode, drawing power to stay connected. In homes with a traditional always-on CPE, the gateway remains fully operational, even though the network sees little to no traffic. With Silicon Labs' Low-Power Mesh Technology, the CPE can enter sleep mode during these periods of inactivity. The CPE only wakes up when e.g., a motion sensor detects activity or when a user interacts with the system. This drastically reduces power consumption while ensuring that essential functions, such as security, remain operational:

Vacation Mode

During vacations or extended periods of absence, smart home devices such as lights and HVAC systems may not be actively used. Yet, the CPE remains fully operational and consumes power. Silicon Labs' solution allows the CPE to hibernate when the home is unoccupied, waking up only when a critical event occurs—such as an alert from a Thread-enabled security sensor or a remote temperature adjustment from a Matter-enabled thermostat. This significantly reduces energy consumption while keeping the home secure and responsive.

Secondary Home

Secondary homes or vacation properties often have connected devices, such as security systems or environmental monitors, that remain on standby for long periods. Traditionally, the CPE remains operational around the clock, ensuring these systems can communicate.

Silicon Labs' technology allows the CPE in a secondary home to enter a deep sleep state while maintaining network connectivity through Matter or Thread. Devices such as smart locks or environmental sensors can wake the CPE when needed, but until then, the CPE draws minimal power.

Calculated Estimations

The calculated estimations below illustrate the potential gateway energy savings that could be achieved with Wake on Thread/Matter with the given assumptions.

	Night Mode (8 hours)	Vacation Mode (2 weeks)	Secondary Home (8 months)
Energy consumption without sleep mode assuming 15W gateway power.	120 Wh	5040 Wh	86400 Wh
Energy consumption with sleep mode assuming 0.3W gateway power.	2.4 Wh	100 Wh	1728 Wh
Potential saving estimation	~98% power consumption reduction during low-activity periods	~98% energy consumption saving during vacations	~98% energy consumption reduction during un-occupancy

Night Mode Cost Saving per 1 Million Gateways

- **Energy reduction:** 117,600 kWh per night
- **Energy cost saving:** ~ €30,000 per night (€0.25 per kWh)
- **Yearly cost saving:** ~ €10 million

Conclusion – Gateway Energy Consumption

The upcoming EU Ecodesign Regulation 2023/826 mandates stricter energy consumption limits for electronic devices. This introduces a complex challenge for Internet service providers: How can CPEs be put to sleep during inactivity and woken up when needed without compromising Smart Home functionalities and user experience? Silicon Labs' Low-Power Mesh Technology introduces a new innovative, intuitive, and automated way to manage gateway sleep mode. The mesh connectivity allows IoT devices to wake CPE up when they need connectivity. It saves gateway energy consumption and keeps critical smart home applications operational while improving the user experience.

Complete Single-chip Solution for Multiprotocol IoT Gateways

Building an energy-efficient, high-performing, and future-proof multiprotocol IoT gateway that scales to millions of homes is challenging. Silicon Labs MG24 offers you a complete single-chip solution to enhance your Wi-Fi gateway with high-performance multiprotocol IoT and many valuable add-on features, reducing time to market, development costs, and bill of material.

From Wi-Fi to Multiprotocol IoT with a Single Chip – **Go to MG24!**

Signal Identifier
MG24 supports the patent-pending Wi-Fi coexistence solution providing an optimal balance for Wi-Fi and 802.15.4 throughput.

Antenna Diversity
With MG24 you can improve gateway antenna coverage in the most challenging RF environment, home!

Automated Gateway Power Management
MG24 enables Thread and Matter devices to switch Wi-Fi gateway sleep mode on/off based on their connectivity needs.

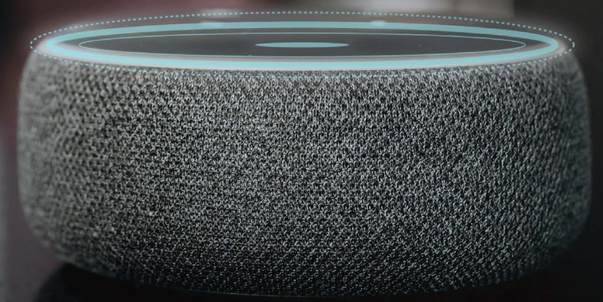
Multiprotocol IoT
MG24 supports all wireless IoT protocols you need in a gateway with industry's most advanced management techniques.

Large Memory
MG24 offers large flash and RAM to accommodate space for all the protocols, application, power management, OTA, and future code growth.

AI Edge Computing
The dedicated AI/ML hardware accelerator on MG24 enables fast and low-power AI/ML inferencing on your gateway.

Location Tracking
Offer customers location tracking services on your gateway using MG24 Bluetooth Channel Sounding.

Superior Wireless Performance
Industry leading IoT Link Budget on MG24 enhances wireless experience for smart home users.



See also **MGM240 modules** with worldwide RF-certifications and integrated antenna to accelerate IoT gateway launch and reduce your development costs!