AN1138: Zigbee Mesh Network Performance

This application note details methods for testing Zigbee mesh network performance. With an increasing number of mesh networks available in today's wireless market, it is important for designers to understand the different use cases among these networks and their expected performances. When selecting a network or device, designers need to know the network's performance and behavior characteristics, such as battery life, network throughput and latency, and the impact of network size on scalability and reliability.

This application note demonstrates how the Zigbee mesh network differs in performance and behavior from other mesh networks. Tests were conducted using Silicon Labs' Zigbee Mesh software stacks and the Wireless Gecko SoC platform capable of running Zigbee Mesh and Proprietary protocols. The test environment was a commercial office building with active Wi-Fi and Zigbee networks in range. Wireless test clusters were deployed in hallways, meeting rooms, offices, and open areas. The methodology for performing the benchmarking tests is defined so that others may run the same tests. These results are intended to provide guidance on design practices and principles as well as expected field performance results.

Additional performance benchmarking information for other technologies is available at http://www.silabs.com/mesh-performance.

KEY POINTS

- Wireless test network in Silicon Labs Research and Development (R&D) is described.
- Wireless conditions and environments are evaluated.
- Mesh network performance including throughput, latency, and large network scalability is presented.

1. Introduction and Background

Silicon Labs provides performance testing results from embedded mesh networks as part of developer conferences and industry white papers. The basic performance data of throughput, latency, and impact of security can be used by system designers to define expected behavior. Testing was done across our different mesh network technologies – Zigbee, Thread, and Bluetooth - and each are presented separately. This application note presents the Zigbee network performance.

1.1 Underlying Physical Layer and Packet Structure

Network performance is based on payload sizing since the application usage does not account for the packet overhead.

Zigbee uses IEEE 802.15.4 2006 with 127-byte packets and an underlying data rate of 250 kbps. The Zigbee packet format is shown below and results in a 68-byte payload. For payloads above 68 bytes, Zigbee fragments into multiple packets. Our data on performance is based on payload size as this is the design parameter of concern when building an application.
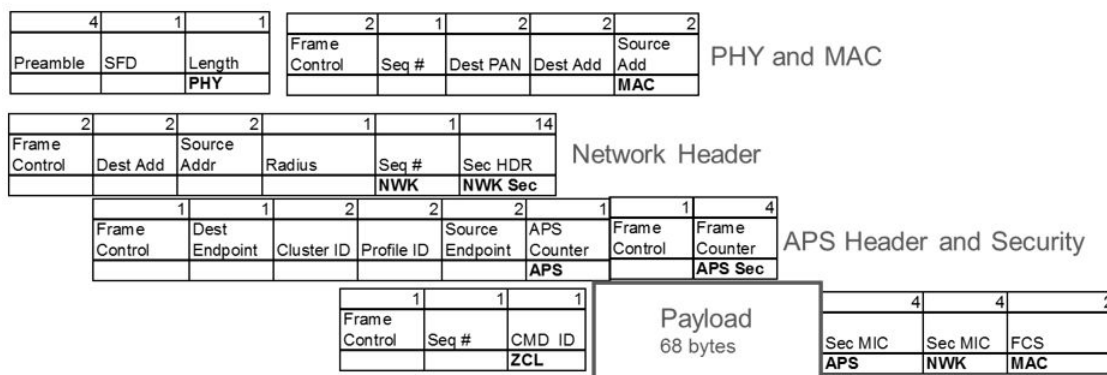

Figure 1.1. Zigbee Packet Format

1.2 Network Routing Differences

Zigbee was designed for home and building automation. Zigbee supports several routing techniques including flooding of the mesh for route discovery or group messages, next hop routing for controlled messages in the mesh, and many-to-one routing to a gateway which then uses source routing out to devices. It is normal for a Zigbee network to use these methods at the same time.

Networks fragment larger messages into smaller ones. For Zigbee, fragmentation is done at the application layer and is end-to-end from the source to the destination.

For unicast forwarding within these networks, the message is forwarded as soon as the device is ready to send. For multicast forwarding, there are generally networking requirements for how messages are forwarded. For Zigbee devices, a multicast message is forwarded by a device only after a jitter of up to 64 milliseconds. However, the initiating device has a gap of 500 milliseconds before retransmitting the initial message.

Note: This performance data is for the Silicon Labs implementation of these mesh networking stacks. As is shown in the test network and infrastructure provided for this testing, no tests were performed with other stacks or systems.

2. Goals and Methods

This application note defines a set of tests performed to evaluate mesh network performance, scalability, and reliability. The test conditions and infrastructure are described, in addition to the message latency and reliability. This testing is conducted over actual wireless devices in test networks and not in simulation.

This testing is done to provide a relative comparison between the different mesh technologies to better understand and recommend their usage. Different network and system designs have different requirements for devices and networks. As such, no one network fulfills all possible network requirements. However, the three mesh networking technologies we are comparing are all aimed at low power and battery-operated mesh networks used for control and monitoring in the home and commercial buildings.

Normally, when analyzing data on network performance, we then consider what improvements can be made in the network to improve performance. Because of the limited data available publicly on mesh network performance in large networks today, it is difficult to have industry discussions on possible improvements or changes. For example, in commercial buildings there is concern over:

- Other network traffic, since there may be many subnets that interfere with each other.
- Wi-Fi interference from the normal building Wi-Fi infrastructure as these technologies are generally operating in the 2.4 GHz ISM band.
- Network throughput and latency as well as large network multicast latency and reliability, since multicasts are commonly used for lighting controls in dense office environments and users of the system expect responsiveness in lighting controls.

Note: The test results here are limited to comparisons of system performance under normal operating conditions, or under stress as noted in particular tests. This application note does not specifically address system interference or other such effects that have been addressed in other published results. However, testing is done in our Silicon Labs R&D facility where there are more than 100 Wi-Fi access points within RF range. The facility also has a 300-node Zigbee lighting network that is not part of this testing but is used for normal lighting control.

2.1 Review of Other Performance Testing

There are no specific, defined methods for evaluating and reporting large network reliability, scalability, or latency. Silicon Labs has published papers in the past comparing network performances based on network testing. This testing is focused on device behavior and impact on battery life, and network throughput and latency. Large scale multicast testing also requires capturing accurate timing and reliability information from large distributed networks. All testing was conducted using the Silicon Labs' Wireless Gecko SoC platform capable of running Zigbee, Thread, Bluetooth Mesh and Proprietary RF protocols to eliminate the device itself as a difference in the testing. Previously published results showed differences between transceivers, network co-processors and System-on-Chip designs. These tests all use System-on-Chip designs.

Other papers published on performance include a master's thesis paper on Zigbee network performance, "Performance Evaluation of Zigbee Network for Embedded Electricity Meters", by Kui Liu, which was published by the Department of Electrical Engineering at the Royal Institute of Technology in Sweden. For round trip time in open-air within a single hop, they tested at different ranges with the following results:

Table 2.1. Packet Loss for Distance and Average Round Trip

Distance	Average Round Trip	Packet Loss
20 meters	18.0 milliseconds	0%
50 meters	17.9 milliseconds	0%
75 meters	17.9 milliseconds	0.75%
85 meters	18.6 milliseconds	1.65%

This test was for 50 bytes of payload unicast at a 100-millisecond interval with security off. Note that Zigbee does not allow security to be turned off. The results show a 1 hop test consistently takes ~18 milliseconds round trip time. This testing was repeated indoors with various interference conditions, but the round trip time for 1 hop did not vary much from the 18 milliseconds. Multi-hop test results were not presented.

3. Test Network and Conditions

To minimize variability, device testing can also be performed in fixed topologies where the RF paths are wired together through splitters and attenuators to ensure the topology does not change over time and testing. This method is used for 7-hop testing to ensure network topology. MAC filtering can also be used to achieve the network topology.
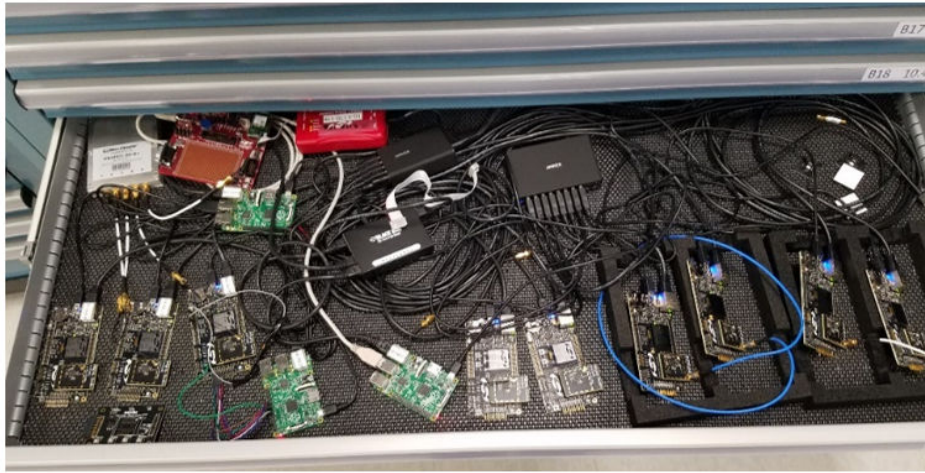
A typical wired test configuration is shown below:

Figure 3.1. Wired RF devices in drawer with splitter and coax cable connectivity

Large network testing is best conducted in an open-air environment where device behavior is based on the existing and varying RF conditions. The Silicon Labs R&D facility is used for this open-air testing.

## 3.1 Facility and Test Network Conditions

The Silicon Labs R&D facility consists of a central core with an elevator shaft, other services with an open floor plan on the west end of the building, and offices and conference rooms on the east end. The overall facility measures approximately 120 feet by 200 feet. The image below shows the facility layout. The darker lines represent hard walls and everything else is split up with cube partitions.

Figure 3.2. Silicon Labs facility layout used for wireless testing

The testing devices are installed at various locations around the facility. These devices all have Ethernet backchannel connectivity to allow:

• Firmware updates
• Command line interface
• Scripting
• Timing analysis
• Packet capture
• Energy measurements
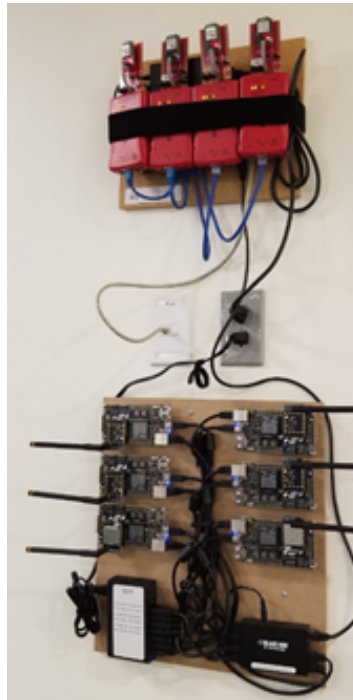
Four EM35x Devices using PoE

Six EFR32MG (Mighty Gecko) Devices

Multi-band support to allow testing both
2.4 GHz (PCB antenna) and proprietary sub-GHz
protocols (external antenna)

USB power and Ethernet connectivity

Figure 3.3. Typical Testing Cluster

The testing clusters are spread throughout the facility in both high and low locations, open areas, and enclosed meeting rooms and offices.

Figure 3.4. Testing Clusters in the Silicon Labs R&D Facility

This test network has devices added or removed from it on a regular basis, but at the time of this testing it consisted of the following devices:

- EM35xx devices
- EFR32 ^{TM} Mighty Gecko devices

This network represented devices that were used for open-air testing by the networking and software quality assurance teams. All devices are controlled from a central test server and infrastructure, which allows scripted regression testing or manual testing by engineers.

3.2 Wireless Conditions in the Facility

The Silicon Labs R&D facility has a full Zigbee lighting control system including motion and lighting sensors and switches. This is not part of the test network and is used as a normal building control system independent of any testing being run.

The Silicon Labs R&D facility is also downtown and, in addition to our existing Wi-Fi infrastructure, there are over 100 Wi-Fi access points within RF distance of the facility. The following charts were taken as a snapshot of a normal work day Wi-Fi scan. This is considered the normal Wi-Fi background traffic.
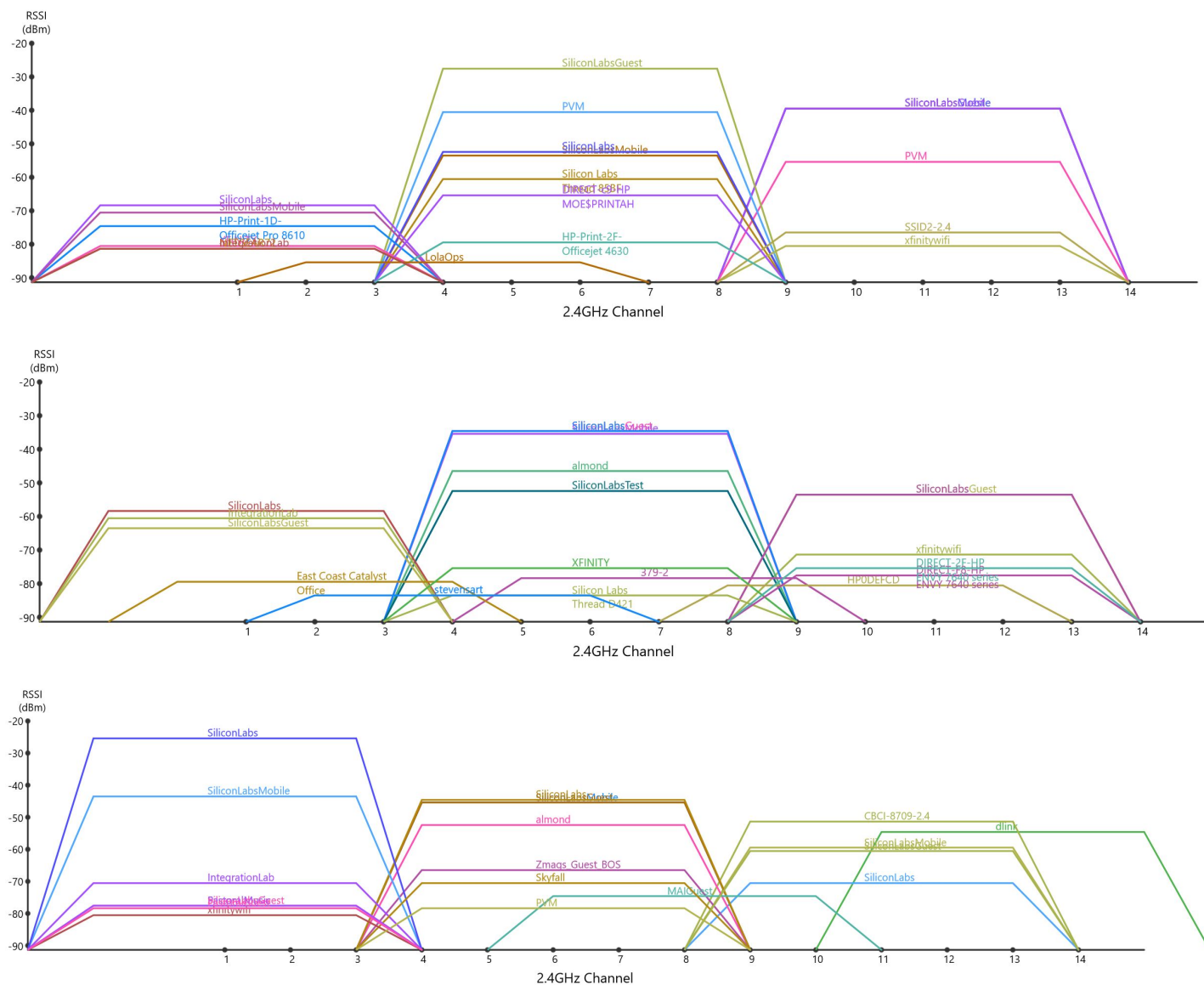
Figure 3.5. Wi-Fi Scans on a Normal Day

These Wi-Fi scans were taken at the southeast corner office, the west side, and the north side in the main conference room, respectively. These locations showed 62, 104, and 83 Wi-Fi access points within RF range.

3.3 Typical Test Network

Within the test network, a given test can be selected and used for a given set of devices. The network is established and devices joined using the Ethernet backchannel to send commands to devices. A typical network during testing is shown below. The black and grey lines show the router connectivity and strength.
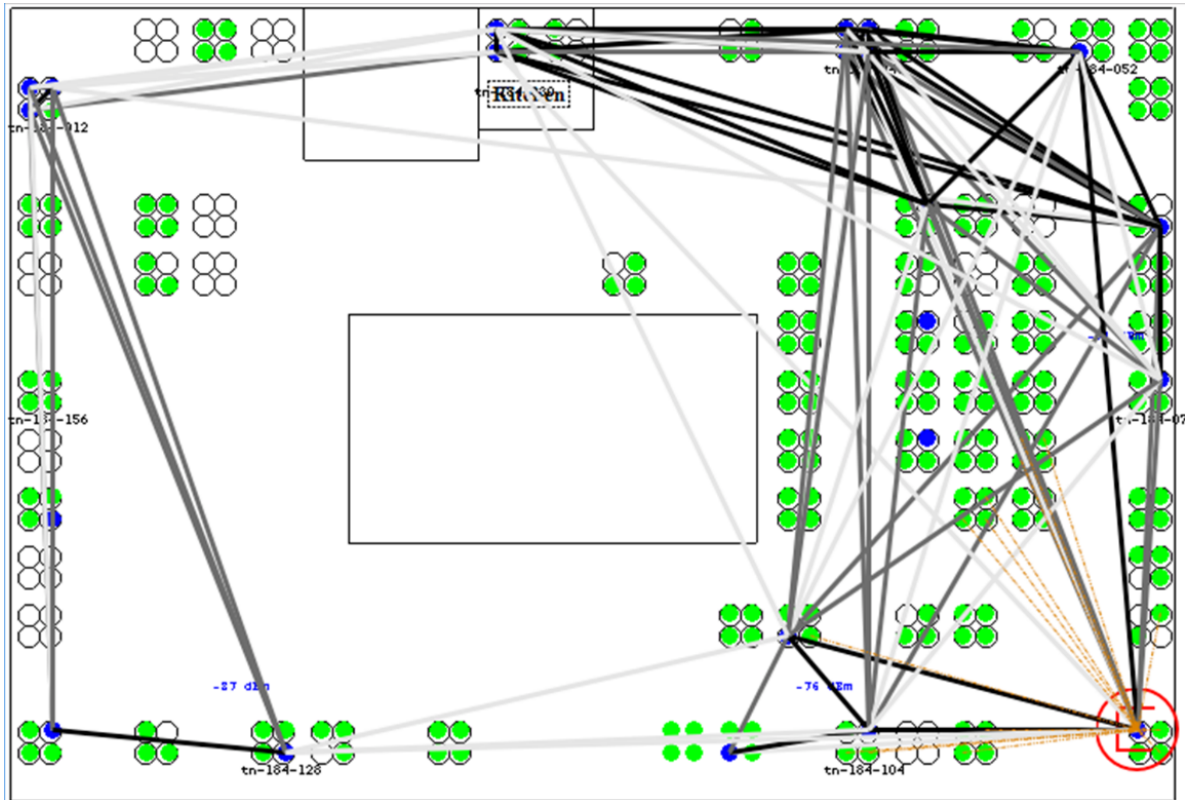

Figure 3.6. A Typical Network During Testing

4. Testing and Results

4.1 Throughput and Latency

The throughput and latency is tested in a controlled network (wired configuration) to test each hop against different packet payloads.

The normal configuration is to test to 6 hops. Testing is done with one source node and a series of routing nodes to allow the number of hops to be varied.
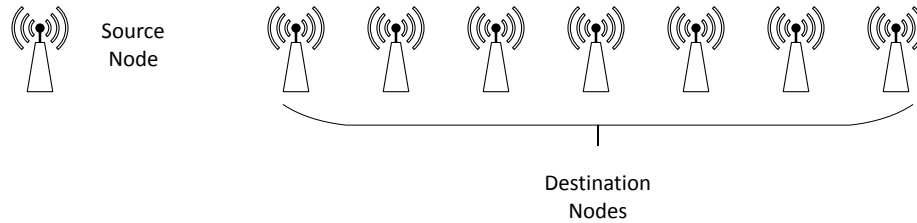
This testing is done using the following configuration:

1. Zigbee application layer messages
2. Packet payload from 50 bytes to up to 300 bytes in 50 byte increments for the latency test
3. Testing is done with security on
4. From 1 to 6 hops
5. Using 2 packets in flight (3rd send when ack received from 1st…)
6. Sending as fast as possible given ack timing
7. Measuring round trip latency (source to destination to source) in milliseconds

For each of these different mesh networks, packet fragmentation occurs differently as we increase payload size as noted above. The use of larger packet sizes is up to the application layer, but we provide comparison data here to indicate relative performance as fragmentation occurs.
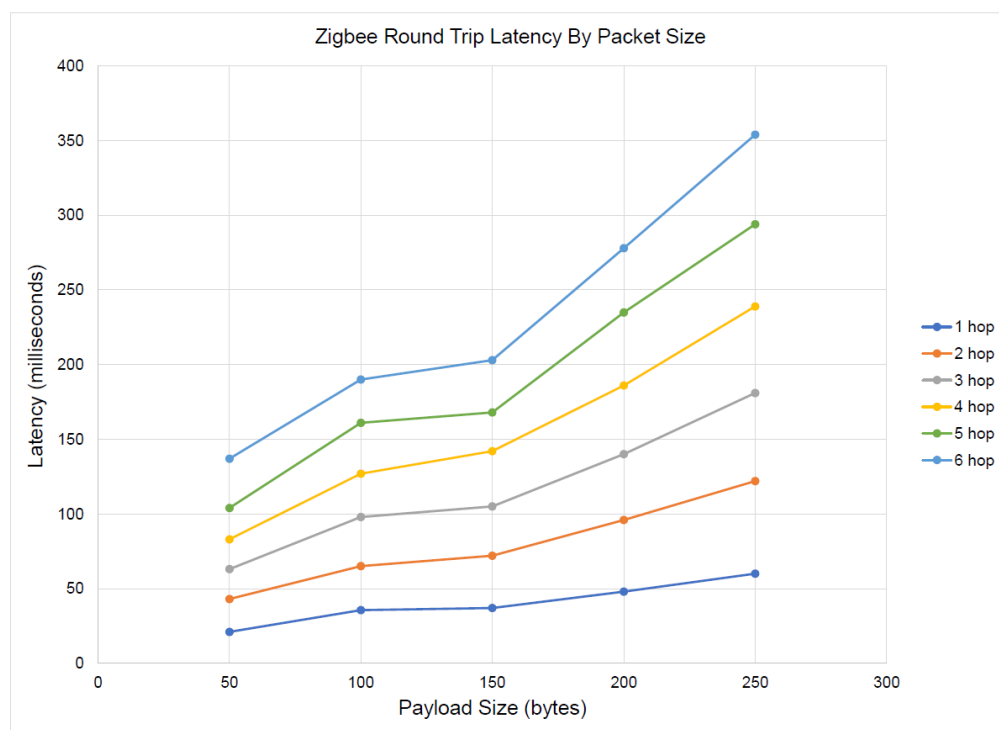
4.1.1 Zigbee Multi-hop Latency

Figure 4.1. Zigbee Round Trip Latency by Packet Size

Several items are worth noting in this multi-hop latency test as follows:
- For 1 hop payload out to 250 bytes, we see very low latency (60 milliseconds).
- With 50 bytes of payload (contained within 1 packet), Zigbee maintains the latency below 140 milliseconds out to 6 hops.
- Latency remains below 200 milliseconds except when the payload gets over 150 bytes and the number of hops is more than 5.

4.2 Network Tests versus Network Size

Open-air large network testing is required to validate stack performance under less controlled conditions. These networks are configured within normal Silicon Labs office space with normal Wi-Fi interference, other network operations, and building control systems. No attempt is made to isolate these network RF conditions.

The networks to be tested for each stack include:
- Small network: 24 devices
- Medium network: 1 – 48 devices
- Medium network: 2 – 96 devices
- Large network: 1 – 144 devices
- Large network: 2 – 192 devices

Note: For any of these tests, the specific number of devices is acceptable within +/- 10% of these test network targets for a given set of testing. Testing in this large network is done in SoC mode for devices.

These networks are all configured as powered devices unless there is specific testing for sleeping end devices.

For each of these networks, the testing will validate reliability and latency for a set of traffic conditions. Testing is intended to be done over 100 messages, but longer runs with 10000 messages for reliability are also done. The same devices were used across the tests to keep the topology and density of the different test runs similar. The actual over-the-air conditions will vary and cannot be controlled in these tests.

4.2.1 Zigbee Large Network Testing Results

Zigbee testing was done with the latest version of the Zigbee stack. Zigbee network testing was done with 5, 25, and 50-byte payloads with a normal broadcast transmission interval of 3 seconds. The histograms of results are shown below.
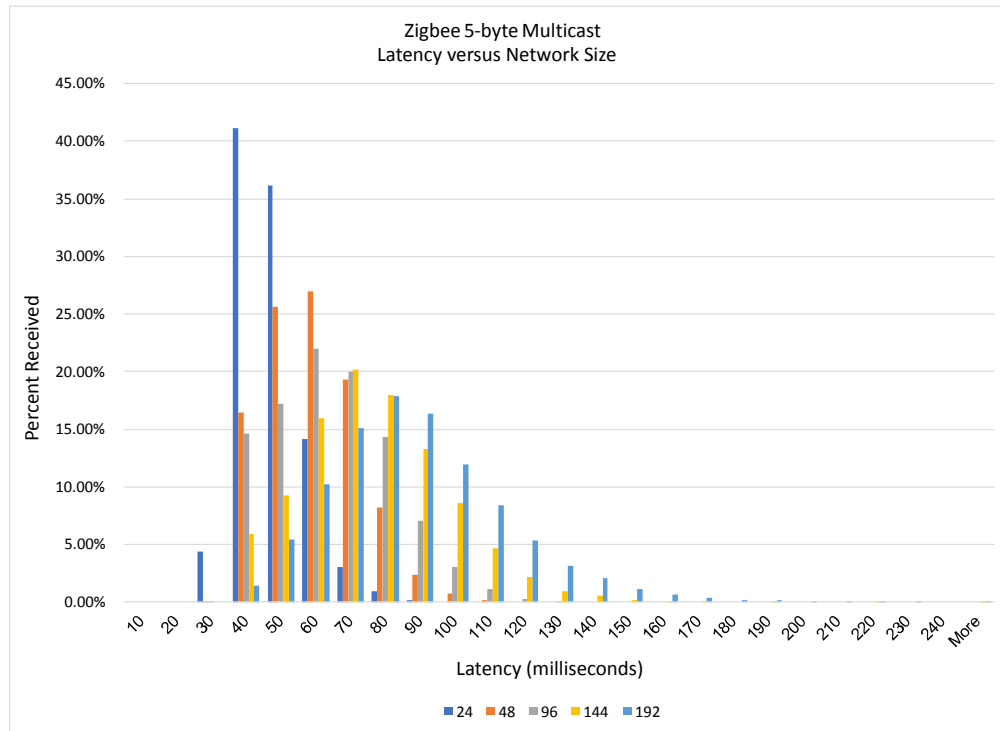

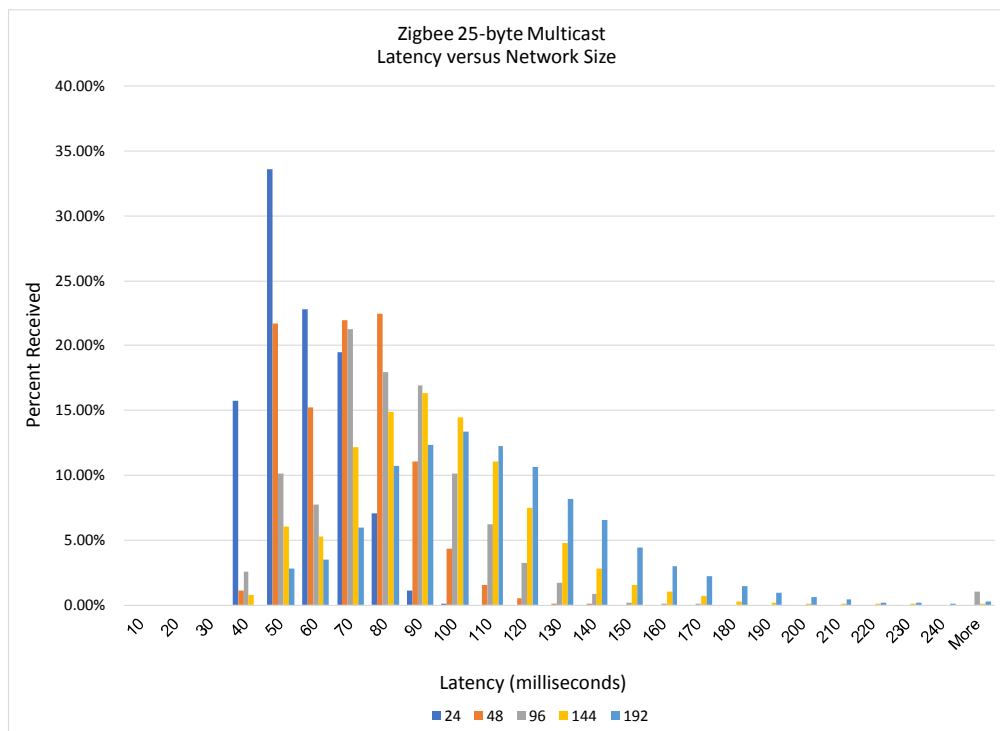**Figure 4.2. Zigbee Network Testing with 5-byte Payload**

Figure 4.3. Zigbee Network Testing with 25-byte Payload
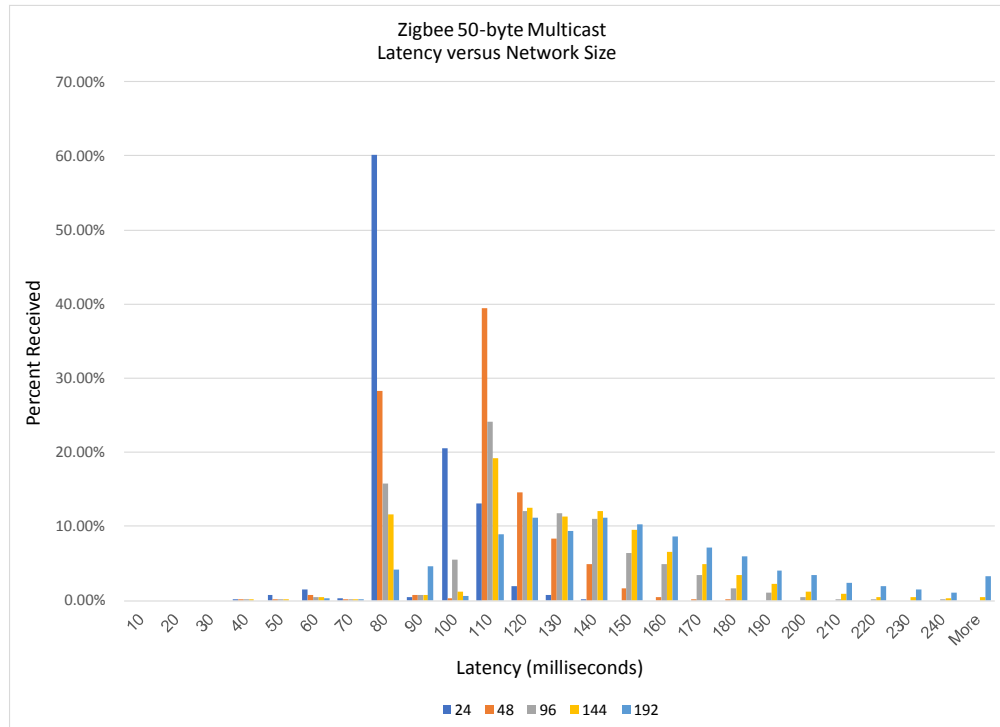
Figure 4.4. Zigbee Network Testing with 50-byte Payload

The following should be noted from this testing:

- As packet payload increases, latency to the devices increases. This is expected and normal behavior as it takes more time to transmit larger packets.
- We see 100% reliability in all of these tests. Note these are 100 broadcasts tests. Larger tests to better measure reliability are available for tests below 100 broadcasts.
- As the network size grows, we see an increase and spreading out of latency as it takes multiple hops to deliver all the messages. Larger networks also have more contention over the air as all devices are trying to repeat the message.
- This testing was also conducted with 3 seconds between broadcasts, giving the network some time to recover before sending the next message. Separate testing is shown below on what happens when the interval between broadcasts is decreased.

4.2.2 Zigbee Network Testing with Shorter Interval

It is a known issue that the use of broadcasts in 15.4 networks should be minimized as they can cause temporary flooding of the network. Zigbee networks have a broadcast transaction record to prevent broadcasts from being processed that have already been forwarded by the device. This broadcast table must contain a minimum of 9 entries and they are aged out after 9 seconds, meaning on average only 1 broadcast per second is supported in the network. As the above testing was done with 3 seconds between broadcasts, additional testing was done with 2 second and 1 second intervals to show the impact versus network size.

The following charts show the latency for a 25-byte payload using 2 second and 1 second intervals between broadcasts.
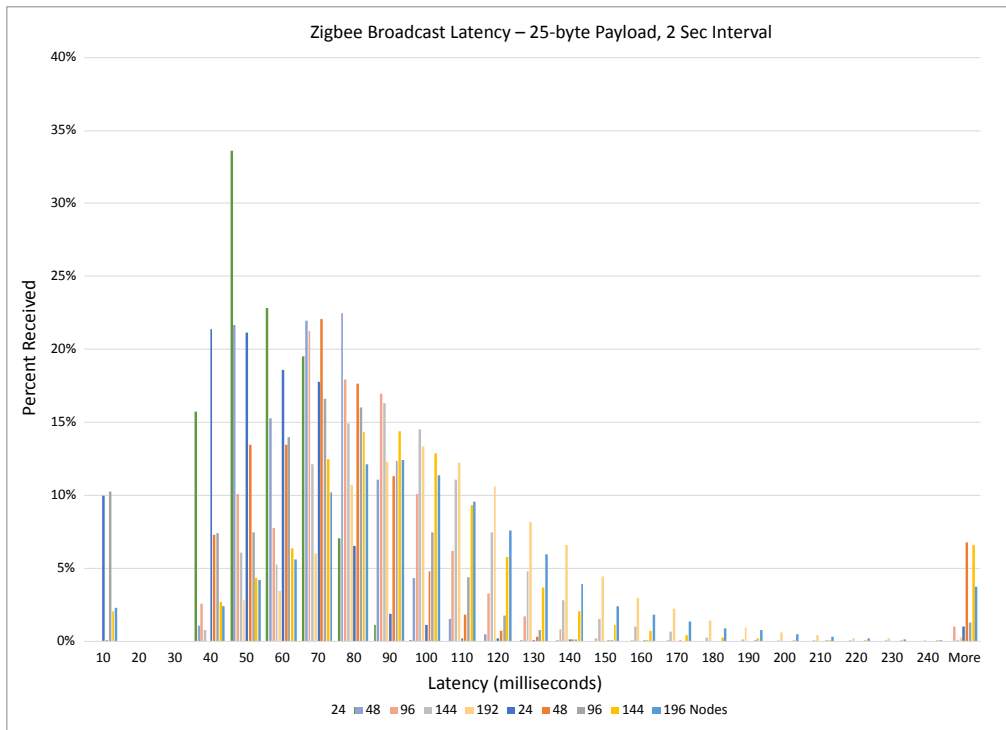

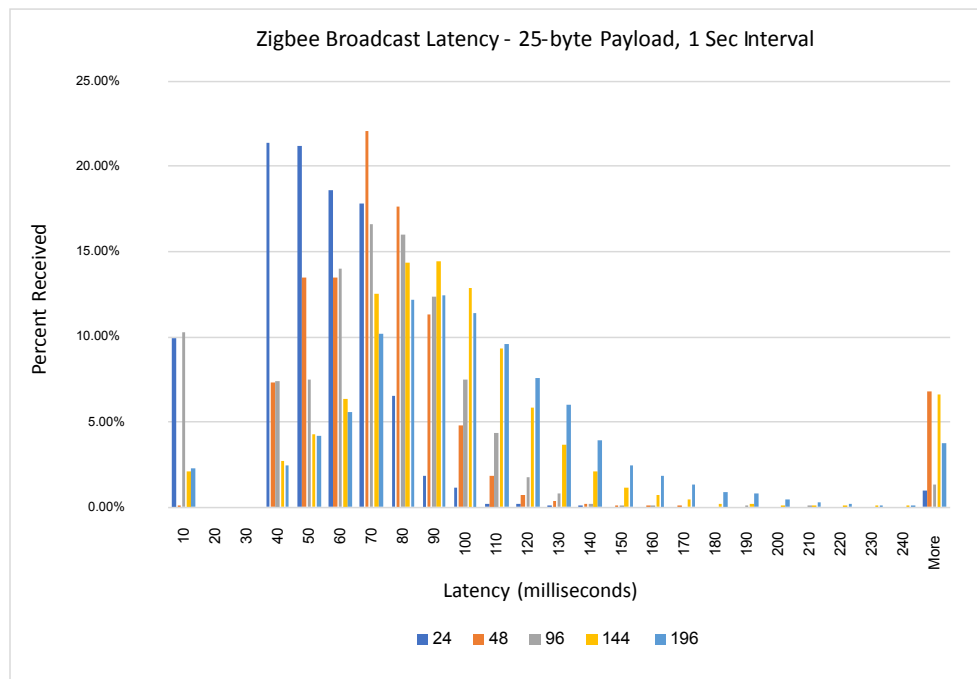**Figure 4.5. Zigbee Broadcast Latency - 25-byte Payload, 2 Sec Interval**

Figure 4.6. Zigbee Broadcast Latency - 25-byte Payload, 1 Sec Interval

From this reduction in broadcast intervals, we see the following:

- We still observe 100% reliability in these tests. These tests are 100 sample tests and are not extended tests for reliability.
- There is little difference between the original 3 second and 2 second intervals. Both operate reasonably well across different network sizes and the average latency in the plots centers around 70-80 milliseconds.
- When the broadcast interval gets down to 1 second, we see quite a bit more of the traffic heading into larger than 250 millisecond latency indicating the network is getting congested. This supports why Zigbee originally sets the broadcast table size and timeout to average 1 broadcast per second. The average packet is still getting through in a similar time, but there are some that are delayed. The large network extended testing in the following section 4.2.3 Large Network Extended Testing shows this result in more detail.

4.2.3 Large Network Extended Testing

Testing with the 192-node network was extended to run over 10000 multicasts to evaluate performance over a longer time period. These tests are also used to show reliability as some failures can be expected in longer tests.

For Zigbee, this testing was done with the 3 second interval between broadcasts as follows:
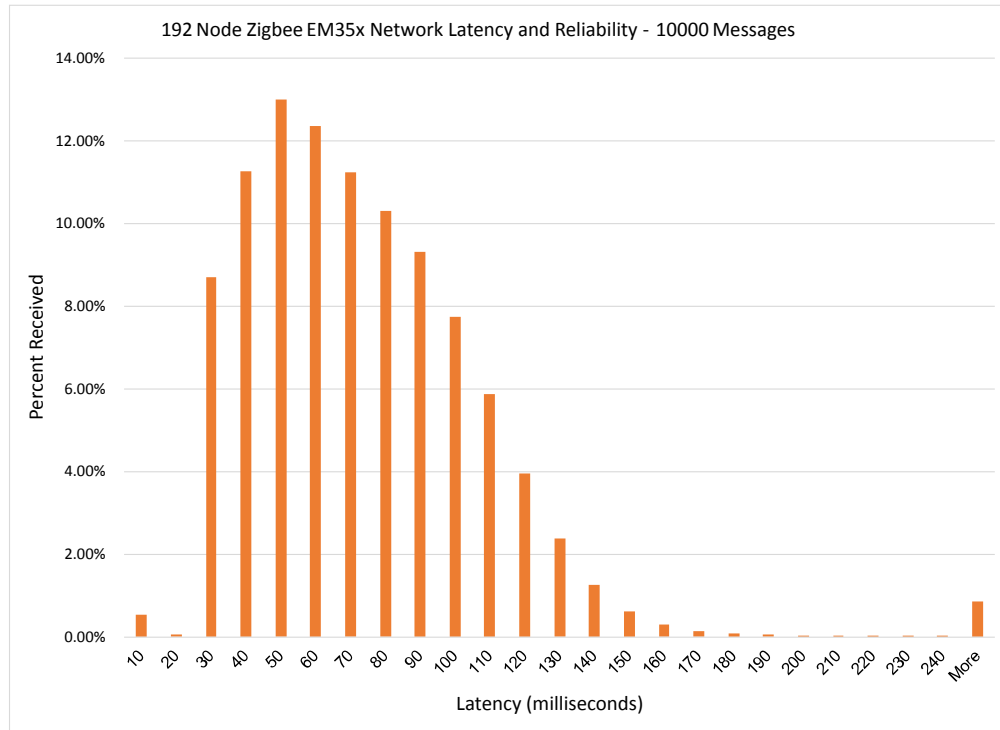

Figure 4.7. 192 Node Zigbee EM35x Network Latency and Reliability

We see a very smooth distribution in this larger data set, but there are 0.85% of messages that are greater than 250 milliseconds in delivery time. When we change the histogram, we see the distribution as follows:
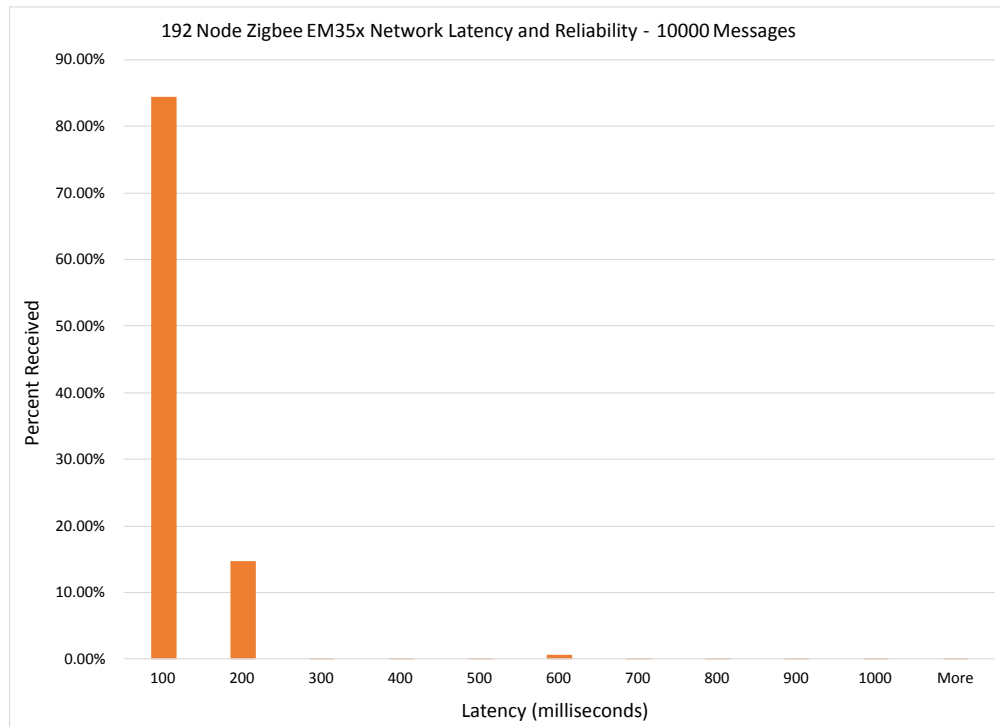

Figure 4.8. 192 Node Zigbee EM35x Network Latency and Reliability - Modified

This testing shows 99% of packets are delivered under 200 milliseconds, but there is a small group out at 600 and 700 milliseconds and longer. In looking at the data, there are 67 broadcasts from the 10000 (0.67%) that did not leave the originating node for 500 milliseconds. The Zigbee standard has a passive ack timeout of 500 milliseconds, so if the originating device does not hear the broadcast replicated by a neighbor within that time it retransmits. Over the course of the longer testing this occurred a small fraction of the time, but it can be seen in the testing data and will result in a stepped increase in latency for those transmissions.

In this large test for Zigbee, 15 packets were lost overall resulting in a 99.9992% reliability for multicast delivery. This is the targeted behavior in our experience with these networks. However, 0.9% of messages were received after 200 milliseconds and if these were counted as failures, the reliability would decrease to 99.1% which is lower than desired. Almost all of these longer latency packets can be attributed to the specification backoff of 500 milliseconds for the initial send noted above.

5. Summary

Zigbee shows excellent reliability and latency below the 200-millisecond timing typically required for human interaction with devices. The Zigbee networks are well behaved up through the 192 node networks we have tested, unless the broadcast frequency is pushed too high and then Zigbee shows increased latency.

As networks scale up, the added hops and broadcast congestion result in some increased latency. As packet payload increases, the latency across the network also increases, but this is a smaller impact when testing 5, 25, and 50 bytes of payload. When the broadcast interval is lowered to 1 second, there is an increase in maximum latency that may be undesirable for some applications.

5.1 Follow-up Testing Considerations

The testing described in this application note requires follow-up tests to further define the device behavior and network operations. The following specific items are noted for follow-up testing:

1. Failure testing can also be added by dropping nodes out of this network during these tests to evaluate recovery time and impact on reliability.
2. Testing should be performed with different device types running in System-on-Chip and Network Co-Processor (NCP) modes. Previous testing has revealed some differences between these modes of operation, so this should be further characterized.

5.2 Related Literature

This application note has provided information on Zigbee mesh networking. For information on Zigbee and Thread mesh networking, and a comparison of all three technologies, refer to the following application notes:

- AN1137: Bluetooth Network Performance
- AN1141: Thread Mesh Network Performance
- AN1142: Mesh Network Performance Comparison
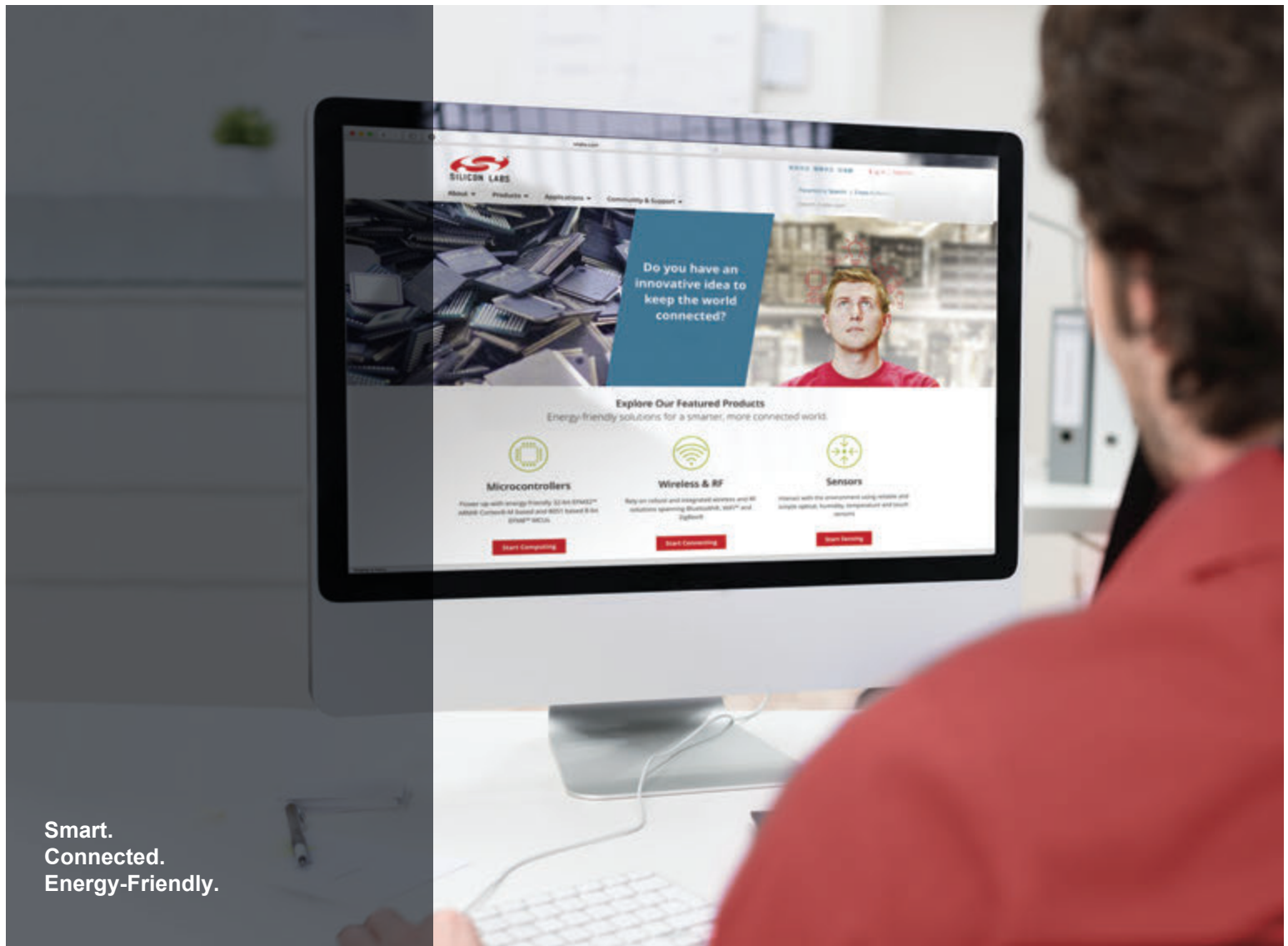
Smart.
Connected.
Energy-Friendly.

Disclaimer

Silicon Labs intends to provide customers with the latest, accurate, and in-depth documentation of all peripherals and modules available for system and software implementers using or intending to use the Silicon Labs products. Characterization data, available modules and peripherals, memory sizes and memory addresses refer to each specific device, and "Typical" parameters provided can and do vary in different applications. Application examples described herein are for illustrative purposes only. Silicon Labs reserves the right to make changes without further notice and limitation to product information, specifications, and descriptions herein, and does not give warranties as to the accuracy or completeness of the included information. Silicon Labs shall have no liability for the consequences of use of the information supplied herein. This document does not imply or express copyright licenses granted hereunder to design or fabricate any integrated circuits. The products are not designed or authorized to be used within any Life Support System without the specific written consent of Silicon Labs. A "Life Support System" is any product or system intended to support or sustain life and/or health, which, if it fails, can be reasonably expected to result in significant personal injury or death. Silicon Labs products are not designed or authorized for military applications. Silicon Labs products shall under no circumstances be used in weapons of mass destruction including (but not limited to) nuclear, biological or chemical weapons, or missiles capable of delivering such weapons.

Trademark Information

Silicon Laboratories Inc.® , Silicon Laboratories®, Silicon Labs®, SiLabs® and the Silicon Labs logo®, Bluegiga®, Bluegiga Logo®, Clockbuilder®, CMEMS®, DSPLL®, EFM®, EFM32®, EFR, Ember®, Energy Micro, Energy Micro logo and combinations thereof, "the world's most energy friendly microcontrollers", Ember®, EZLink®, EZRadio®, EZRadioPRO®, Gecko®, ISOmodem®, Micrium, Precision32®, ProSLIC®, Simplicity Studio®, SiPHY®, Telegesis, the Telegesis Logo®, USBXpress®, Zentri, Z-Wave and others are trademarks or registered trademarks of Silicon Labs. ARM, CORTEX, Cortex-M3 and THUMB are trademarks or registered trademarks of ARM Holdings. Keil is a registered trademark of ARM Limited. All other products or brand names mentioned herein are trademarks of their respective holders.

Silicon Laboratories Inc.
400 West Cesar Chavez
Austin, TX 78701
USA

http://www.silabs.com

SILICON LABS