Microchip ZigBee® RF4CE Performance under Wi-Fi® Interference

Author: *Yifeng Yang*
Microchip Technology Inc.

INTRODUCTION

To overcome the limitations of InfraRed (IR) remote control technology, ZigBee® RF4CE specification was first published in May 2009. It quickly became the dominant core technology that drives development of next generation remote control applications. ZigBee RF4CE technology uses IEEE 802.15.4 as its PHYsical (PHY) and Medium Access Control (MAC) layers, and builds network layer on top of them. As one of the first companies that supports a complete ZigBee RF4CE development platform, Microchip Technology provides the most competitive RF4CE solution in the market with eXtreme Low-Power (XLP) microcontrollers, IEEE 802.15.4 compliant RF transceiver, and ZigBee certified RF4CE protocol stack with the smallest memory footprint in the industry. For more details on Microchip RF4CE solution and other related information, refer to:

http://www.microchip.com/rf4ce

The fact that ZigBee RF4CE remote controls work on globally available 2.4 GHz Industrial, Scientific and Medical (ISM) band is one of its advantages for easy deployment. On the other hand, ZigBee RF4CE also generates some speculations of unwanted interference between RF4CE and other technologies that work on the same ISM frequency band, Bluetooth® and Wi-Fi®. It is of less concern for Bluetooth as it is a frequency hopping narrow band technology that only introduces short and temporary signal at any frequency. However, Wi-Fi introduces consistent wide band signal potentially with high power up to 20 dBm - 30 dBm (depending on geography) at the same frequency that IEEE 802.15.4 radio operates. A systematic research on the impact of Wi-Fi interference over Microchip ZigBee RF4CE solution may be helpful to ease the worry from potential user of RF4CE technology.

In this application note, we first introduce the mechanisms to share frequency, which are designed in MAC layers of both IEEE 802.15.4 (RF4CE) and IEEE 802.11 (Wi-Fi) specifications. Then, additional efforts of RF4CE network layer to choose proper channels and ensure message delivery have been discussed. Finally, the application note details the worst case scenario and perform tests to evaluate performance of Microchip ZigBee RF4CE solution under strong Wi-Fi interference. Detailed test setups, test procedures and test results are also documented in this application note. For Microchip customers, the test firmware can be provided to help reproducing the test results under same condition. For more details, please contact your nearest Microchip sales office.

DESIGNED TO SHARE

MAC Layers – Listen Before Talk

Both IEEE 802.15.4 – the lower layer of ZigBee RF4CE and IEEE 802.11 – the lower layer of Wi-Fi, are designed to share the frequency with other signals by executing Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism in MAC layer. In general, CSMA/CA mechanism is to listen before talk.

For IEEE 802.15.4 compliant transceivers working on non-beacon mode, that the ZigBee RF4CE specification follows, majority of the transmitting packets other than acknowledgement frame follow the CSMA/CA procedure. The following procedure summarizes the CSMA/CA in IEEE 802.15.4 specification:

1. Randomly back-off between 0 to (2^{BE} - 1) time unit. Back-off Exponential (BE) start with MAC constant macMinBE. Each back-off time unit is 20 symbols or 320 µs.
2. Perform Clear Channel Assessment (CCA) for 128 µs. If medium is idle, CSMA/CA succeeds.
3. If medium is busy, and BE is less than MAC constant aMaxBE, increase BE by one.
4. If the loop counter Number of Back-off (NB) exceeds MAC constant macMaxCSMABackoffs, exit CSMA/CA with status failure.
5. If maximum CSMA back-off time is not exceeded, increase NB by one, and then perform step 1.

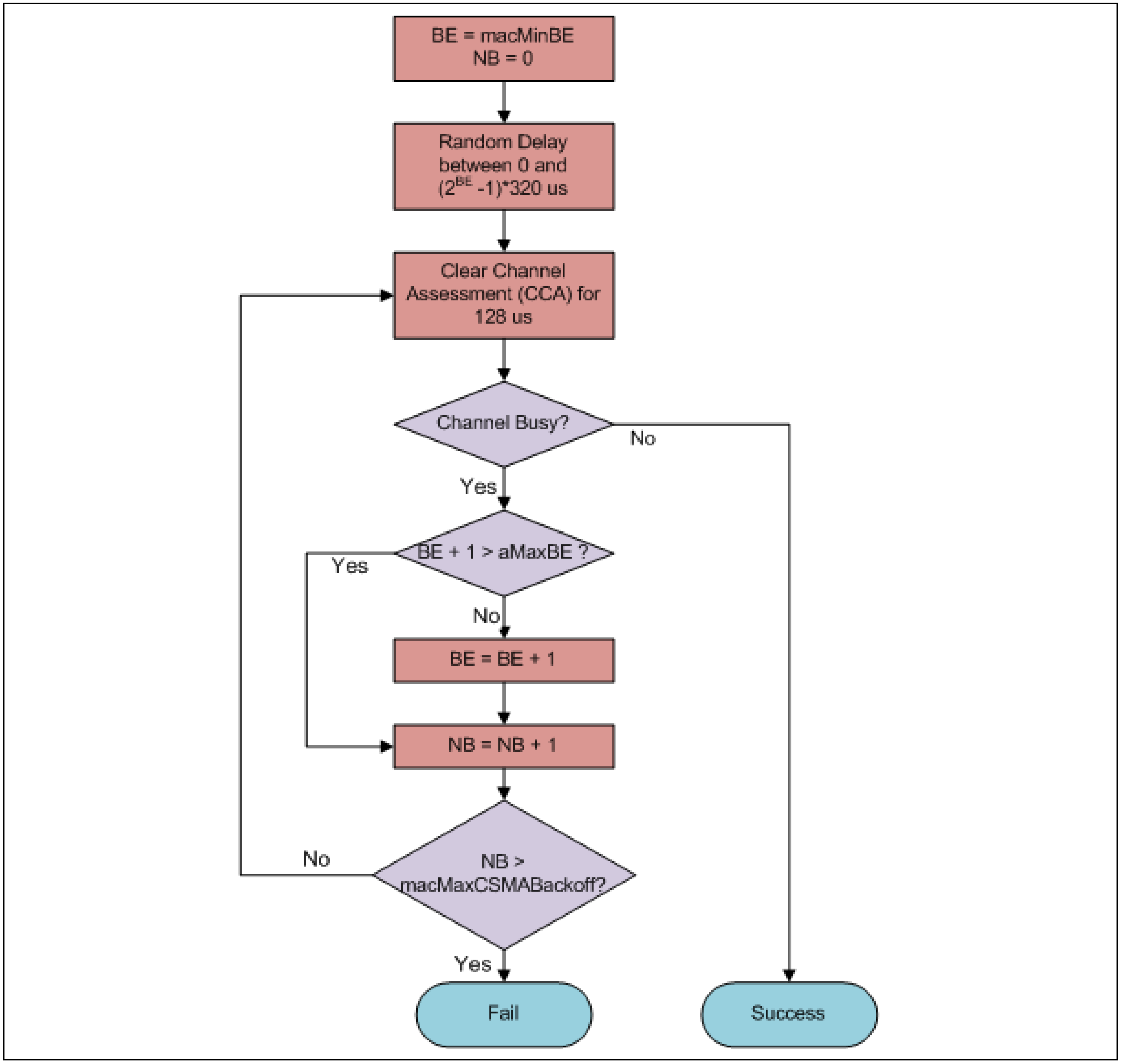
When CCA is performed, there are three CCA modes:

- CCA mode 1 – Energy Detection (ED)
- CCA mode 2 – Carrier Sense (CS)
- CCA mode 3 – Combination of above two

Of the three modes, mode 1 is the most valuable for IEEE 802.15.4 transceiver to co-exist with IEEE 802.11 signals. IEEE 802.15.4 transceivers are not able to detect IEEE 802.11 signals in carrier sense mode due to differences in modulation. Therefore, CCA mode 2 and mode 3 might not detect medium busy, even if strong IEEE 802.11 signal exists. Setting CCA mode 1 in IEEE 802.15.4 transceiver enables it to detect higher energy in the medium when IEEE 802.11 transceivers are transmitting, and therefore avoid direct packet collision and share the frequency. Figure 1 illustrates the IEEE 802.15.4 CSMA/CA procedure.

Although few differences exist in details, IEEE 802.11 transceivers use similar way in random back-off and to listen before talk. Both IEEE 802.15.4 and IEEE 802.11 have been designed in the beginning to co-exist and co-operate at the same frequency. Both protocols are built to tolerate interference at operating channel, and avoid transmission when such interferences are detected. When both protocols are polite and hold their own conversations while peers are still talking, packet collision and congestion can be greatly reduced.

FIGURE 1: CSMA/CA FLOW CHART (SOURCE: IEEE 802.15.4 SPECIFICATION)



Failure Recovery

This application note has so far discussed how the two protocols prevent confliction and share the same medium and same frequency. In addition, a fault tolerant system not only prevents possible confliction, but also recovers after such an unlikely confliction occurs. For both IEEE 802.15.4 and IEEE 802.11 protocols, the recovery is handled by the acknowledgement/retransmission procedure. Typically, an acknowledgement frame is used to confirm the reception of unicasting messages. A MAC layer sequence number is used to identify individual packet and acknowledgement frame duplicates the MAC sequence number to pinpoint the unicast message to be confirmed. However, if no desired acknowledgement packet is received by the transmitting side after a predefined time period threshold, retransmission of identical packet will be performed. Such transmission and waiting for acknowledgement can be repeated a few times until a confirmation acknowledgement is received, or the process runs out of retry limits.

Besides CSMA/CA, to actively prevent packet collision among IEEE 802.15.4 and IEEE 802.11 communications, acknowledgment mechanism ensures packet delivery of unicast frame, the majority of both IEEE 802.15.4 and IEEE 802.11 traffic. In rare case, CSMA/CA mechanism does not prevent a packet collision, no acknowledgement will be generated and received. The mechanism of retransmission will be invoked and will retry the complete transmission process. The retransmission process significantly increases the chances of message delivery of IEEE 802.15.4 packets under strong interference of IEEE 802.11 signals.

Both CSMA/CA and acknowledgment/retransmission are the mechanisms implemented in the MAC layer. When user tries to send a message, CSMA/CA and acknowledgment/retransmission will be executed in the MAC layer, without additional effort from the application layer. With the mechanisms building in both IEEE 802.15.4 and IEEE 802.11 MAC layers, both protocols are designed to be working together to share the same frequency.

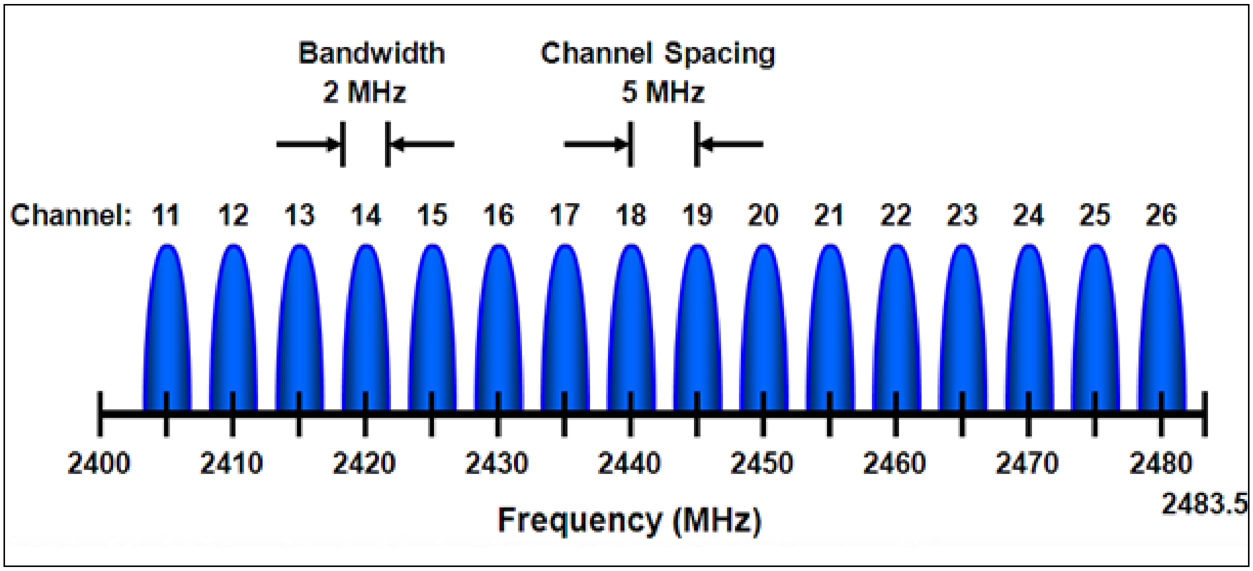
ZigBee RF4CE LAYER

Both IEEE 802.15.4 and IEEE 802.11 are designed to act politely and share the frequency with other protocols. Both preventive and recovery steps have been implemented in the MAC layers of both protocols so that they avoid confliction at first and then are able to recover if confliction occurs in the worst case. ZigBee RF4CE protocol, built on top of IEEE 802.15.4 specification, has already inherited all benefits in the MAC layer to co-exist with Wi-Fi (IEEE 802.11) signal. Further, ZigBee RF4CE protocol walks additional distance to implement more features to be able to share the frequency with Wi-Fi (IEEE 802.11) protocol.

Channel Selection

The first step to avoid Wi-Fi interference is to avoid overlapping the RF4CE signal against that of Wi-Fi. IEEE 802.15.4 has defined 16 channels in 2.4 GHz ISM band. Each channel is 2 MHz wide with 5 MHz channel spacing between channels. Figure 2 illustrates IEEE 802.15.4 2.4 GHz ISM band channel definition.

FIGURE 2: IEEE 802.15.4 2.4 GHz ISM BAND CHANNEL DEFINITION



IEEE 802.11 specification defines 14 channels in 2.4 GHz ISM band. The availability of those 14 channels depends on local government regulations. Each channel has typical bandwidth of 22 MHz. However, center frequency of each channel is only 5 MHz apart. It is obvious that one Wi-Fi channel is overlapping with multiple channels.

To ensure coexistence of Wi-Fi signals between channels, it is required to have at least 25 MHz between center frequencies of operating channels. Combining the above information, United States and Europe have both recommended the Wi-Fi channel settings. Consequently, different Wi-Fi channel settings create different overlaps over IEEE 802.15.4 channels, as illustrated in Figure 3 and Figure 4.

FIGURE 3: OVERLAPPING OF IEEE 802.11 AND IEEE 802.15.4 CHANNELS IN UNITED STATES

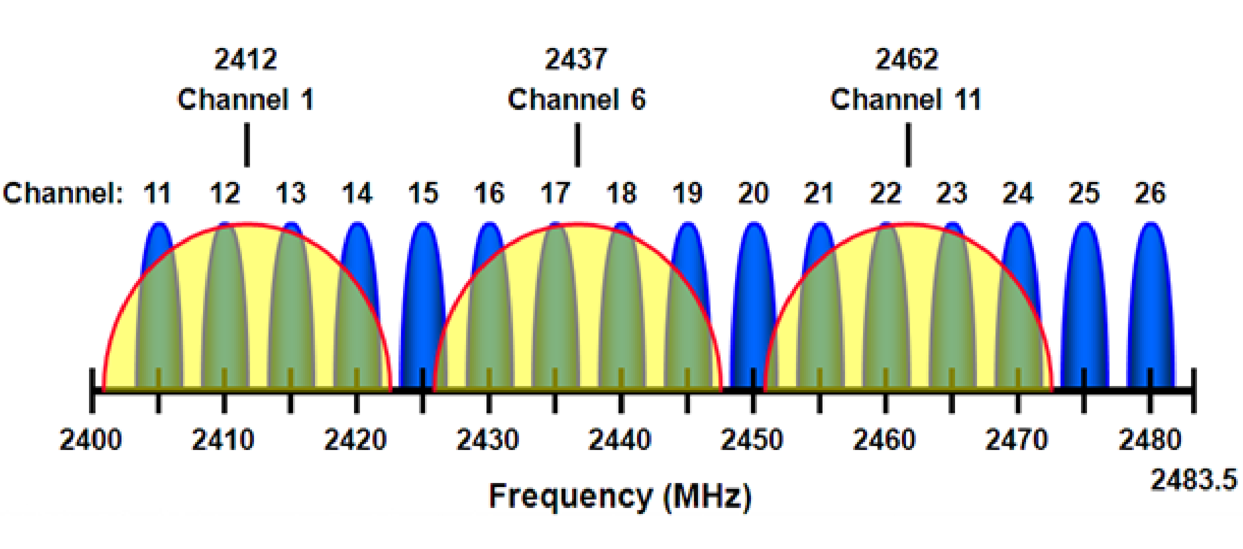
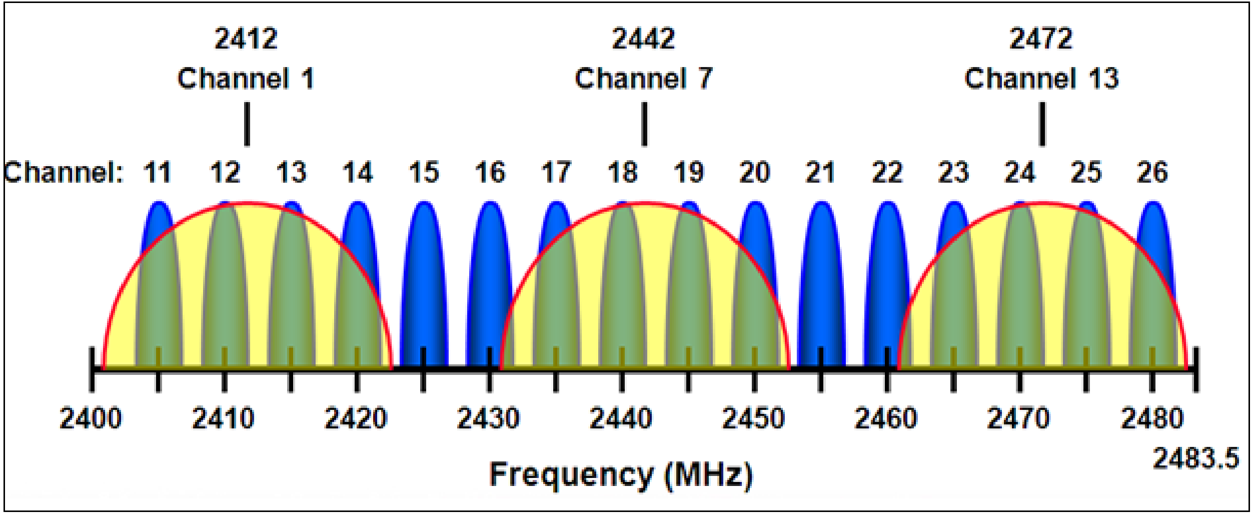


FIGURE 4: OVERLAPPING OF IEEE 802.11 AND IEEE 802.15.4 CHANNELS IN EUROPE



As per Figure 3 and Figure 4, not all IEEE 802.15.4 channels overlap with IEEE 802.11 channels in the same way. Further, different IEEE 802.15.4 channels overlap with IEEE 802.11 channels in different regions. For those IEEE 802.15.4 channels that are not overlapping with IEEE 802.11 channels, it is obvious that there is less interference. ZigBee RF4CE specification selects three IEEE 802.15.4 channels, channel 15, 20 and 25, to be used in communication. As displayed in Figure 3 and Figure 4, these channels are least affected by the Wi-Fi interference both in U.S. and Europe.

By selecting channels which are least overlapping with Wi-Fi channels in the U.S. and Europe, ZigBee RF4CE specification deliberately avoids direct interference with Wi-Fi. When ZigBee RF4CE target devices perform cold start, all three channels will be scanned and the least noisy channel will be located and is used to start the Wireless Personal Area Network (WPAN). In addition to ensure all three available channels have least potential to overlap an operating Wi-Fi channel, the energy scan procedure during ZigBee RF4CE target cold start ensures that ZigBee RF4CE WPAN operate as far from an operating Wi-Fi channel as possible to avoid the confliction. Furthermore, during ZigBee RF4CE normal operating, additional functionalities have been defined in ZigBee RF4CE specification to ensure the WPAN working in the channel with least amount of interference:

- ZigBee RF4CE target device can perform frequency agility periodically to move the WPAN to a channel with less interference
- ZigBee RF4CE controller device can merge multiple ZigBee RF4CE target devices into one single channel that has less interference

In summary, all the mechanisms that are specified above are to assist ZigBee RF4CE WPAN operating on the channel that has least interference with Wi-Fi signal. The collections of mechanisms that ZigBee RF4CE specification defines include:

- Allow ZigBee RF4CE WPAN operating on only three IEEE 802.15.4 channels (channel 15, 20 and 25) that have least potential to overlap Wi-Fi channels in the U.S. and Europe
- When starting a ZigBee RF4CE WPAN, within available three channels, choose one with least noise by energy scanning all three channels
- When operating a ZigBee RF4CE WPAN, a ZigBee RF4CE target device can perform frequency agility and move the WPAN to one of the three channels that has less interference
- When operating in multiple ZigBee RF4CE WPANs, a ZigBee RF4CE controller device can merge multiple WPAN to a single channel that has least interference

Failure Recovery

Similar to MAC layer described in previous section, ZigBee RF4CE network layer also defines preventive steps to avoid confliction, such as multiple steps of optimal channel selection process. ZigBee RF4CE network layer also implements failure recovery mechanism to ensure that the message can still be delivered even when preventive steps fail.

In the worst case that ZigBee RF4CE channel overlaps with Wi-Fi channel, further both CSMA/CA and acknowledgement/retransmission mechanism fail to deliver the message after multiple attempts, ZigBee RF4CE protocol defines multi-channel transmission to recover from the failure. ZigBee RF4CE protocol defines a few different ways to transmit packets, including single-channel transmission and multi-channel transmission. Single-channel transmission depends on IEEE 802.15.4 MAC layer to send messages. On the other hand, as one of the many purposes of multi-channel transmission, failure recovery for ZigBee RF4CE communication has been defined and implemented.

The first step of multi-channel transmission uses the identical process as MAC layer transmission. If MAC layer transmission succeeds, no further operation is necessary. If the first step fails in multi-channel transmission, the second step for multi-channel transmission will try to transmit the packet within all three ZigBee RF4CE supported channels continuously up to one second, until either it receives the desired acknowledgement, or one second is complete. In the second step of transmission, no CSMA/CA is performed; therefore, the packet is guaranteed to be sent under any situation. ZigBee RF4CE specification requires that transmission without the CSMA/CA mechanism must be completed in all of the three channels within 16.8 ms, so that up to 60 attempts can be transmitted on any possible channel until a desired acknowledgment is received. Due to innovative stack structure and code efficiency, Microchip RF4CE stack is capable of completing the transmission in all of the three supported channels within 12 ms to 13 ms. As a result, up to 77 attempts, 28% more than required by ZigBee RF4CE specification, can be performed within one second to further increase the chance of delivery even under extreme interferences.

PERFORMANCE TEST

As discussed in the previous sections, both IEEE 802.15.4 and IEEE 802.11 MAC layers are designed to be able to co-exist in the same frequency by preventive measures, listening before talk and failure recovery mechanisms of acknowledgement/retransmission. In addition to MAC layer, ZigBee RF4CE protocol implements its own preventive measure to limit operating channels to those with least interference with Wi-Fi channels. ZigBee RF4CE protocol also defines multi-channel transmission as backup plan in the case that MAC layer transmission and ZigBee RF4CE channel selection fails to generate favorable results. With all the mechanisms have been designed and implemented, ZigBee RF4CE solution is supposed to be very robust and fault tolerant in the practical environment settings with Wi-Fi interferences.

In this section, we put Microchip ZigBee RF4CE solution up to the test against the worst case severe Wi-Fi interference and check its capability of delivering messages as well as how fast the message can be delivered. The testing environments, setups, procedures and results are documented in detail, so the testing results can be reproduced and verified. After reading the mechanisms for ZigBee RF4CE and Wi-Fi to co-exist by design and implementation, hope that the real world testing results are able to give RF4CE users the full confidence to use Microchip ZigBee RF4CE platform in their practical applications.

Test Environment

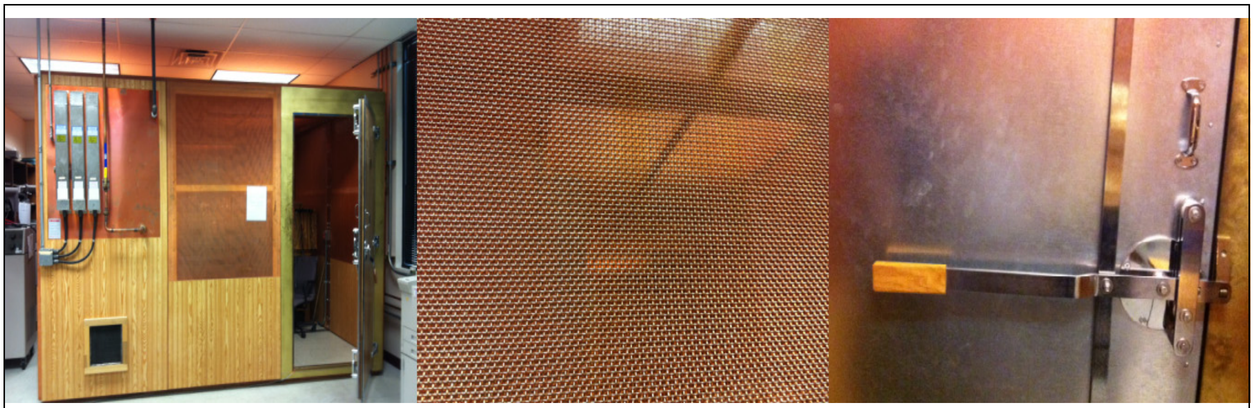
TEST LOCATION

ZigBee RF4CE performance tests with Wi-Fi interference are performed under strictly controlled environment. All tests are performed in an RF shielded chamber. Covered by multi-layer of copper net, the RF shielded chamber is designed to block all of the RF signals exchange between inside and outside of the room; therefore making the RF environment inside of the RF shielded chamber in a controlled known state. When the door of shield chamber is latched and there is no RF activity inside, nearly zero signals are detected with spectrum analyzer. Figure 5 illustrates the Microchip RF shielded chambers.

TEST EQUIPMENT

ZigBee RF4CE protocol defines two kind of devices in the network, target and controller. In this test, two Microchip PIC18 Explorer demonstration boards (DM183032) with MRF24J40 PICtail™ RF daughter card (AC164134-1) are used to simulate both the target and controller. As illustrated in Figure 6, the MRF24J40 PICtail RF daughter card is plugged into the PIC18 Explorer demonstration board, and is ready to perform test.

FIGURE 5: MICROCHIP RF SHIELDED TESTING CHAMBER

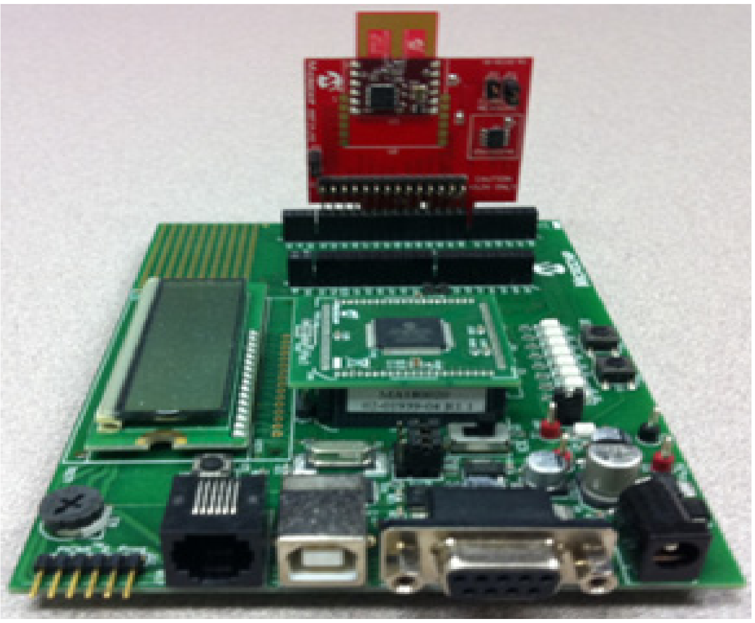


Microchip RF Shielded Test Chamber

Details of Shield in RF Shielded Chamber

Door Latch of RF Shielded Chamber

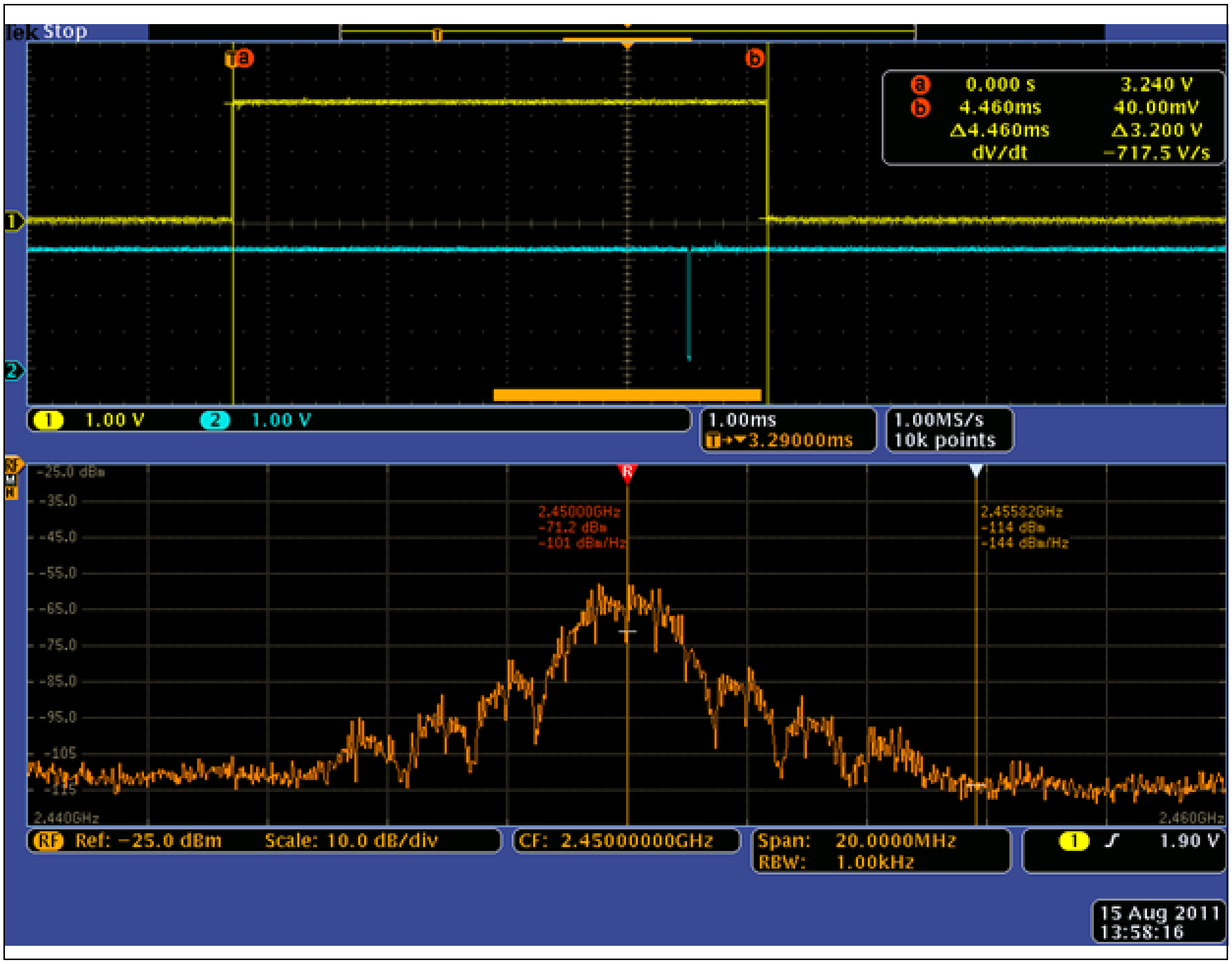
FIGURE 6: MICROCHIP ZigBee® RF4CE TEST PLATFORM: PIC18 EXPLORER DEMO BOARD (DM183032) WITH MRF24J40 PICtail™ RF DAUGHTER CARD (AC164134-1)



Both the ZigBee RF4CE target and controller are programmed with the Microchip ZigBee RF4CE stack. The controller is programmed to transmit 1000 different unicast RF4CE packets to the target, once tests are initiated. The payload of 1000 RF4CE packets is standard High-Definition Multimedia Interface (HDMI) control codes defined in HDMI v1.3a specification. The control code in the payload increases one for each consecutive packet and restarts from zero once the biggest control code 0x76 is reached. The HDMI control code that is transmitted will be shown on LEDs D1 to D7 on the controller board. Similarly, once received, the HDMI control code will also be shown on LEDs D1 to D7 on the target board. The LED patterns on the controller and target boards, therefore, should be matching.

When measuring transmission latency, the straightforward way is the direct measurement of timing from transmitting a packet from the sender until the packet is received by the receiver. This can be usually done by an oscilloscope with at least two channels. One channel is used to monitor the transmission side when operation is started; the other channel is used to monitor the receiving side once packet is received. The difference in timing is the transmission latency. This is the Duo-measurement method that involves two separate measurements in two channels, and is considered to be accurate. However, this measurement must be performed manually as there is no good way to record, process and analyze the data automatically. A different approach is to measure the transmission latency from the transmission side by timing the difference between starting to send a message and receiving the acknowledgement. The timing difference can be recorded and later processed by the MCU. The transmission latencies can then be recorded and analyzed for thousands of packets easily. Because there is only one measurement in single channel, we call this method as Single-measurement method. Due to the time period from acknowledgment frame transmission and MCU process time, it is likely that the transmission latency values from this method are 0.5 ms to 1 ms higher than the actual latency. For automated testing, the Single-measurement method is highly preferred. A comparison between the Duo-measurement method and the Single-measurement method has been performed on Tektronix MDO4104-6 Mixed Domain Oscilloscope, and the results are illustrated in Figure 7.

FIGURE 7: TRANSMISSION LATENCY DIFFERENCE BETWEEN TWO MEASUREMENT METHODS



Tek Stop

a	0.000 s	3.240 V
b	4.460ms	40.00mV
	Δ4.460ms	Δ3.200 V
	dV/dt	-717.5 V/s

1 1.00 V 2 1.00 V

1.00ms
T→▼3.29000ms

1.00MS/s
10k points

2.45000GHz
-71.2 dBm
-101 dBm/Hz

2.45582GHz
-114 dBm
-144 dBm/Hz

RF Ref: -25.0 dBm Scale: 10.0 dB/div

CF: 2.45000000GHz

Span: 20.0000MHz
RBW: 1.00kHz

1 ⌠ 1.90 V

15 Aug 2011
13:58:16

Tektronix MDO4104-6 Mixed Domain Oscilloscope offers measurements from both analogue and radio frequencies. As illustrated in Figure 7, the orange waveform at the bottom is the IEEE 802.15.4 signal transmitted in channel 20. The top section has signals from two analogue channels, indicating the timing of transmission and receiving.

Channel 1 is connected to an I/O pin on the transmission side programmed to go high when a transmission is started, and go low when an acknowledgement has been received. This pin is controlled by the application layer. Channel 2 is connected to the interrupt pin on the receive side.

The yellow line is channel 1 from the transmission side. When transmission started from the application layer, the input jumps to high. When transmission finishes at the application layer, the input line falls back to low. The timing measured here is using the Single-measurement method that has been described earlier. The transmission timing is accurately labeled by marker ‘a’ and marker ‘b’. The total latency for this transmission from the Single-measurement method is 4.460 ms from the oscilloscope. MCU measured the latency to be 4.468 ms, very close to what the oscilloscope reported.

On the other hand, the blue line is channel 2 from the radio interrupt pin of the receiving side. When receiver side receives the message, an interrupt is generated from the radio to the MCU. The actual transmission latency should be the timing from marker ‘a’ to where the interrupt line drops to low, as the Duo-measurement method has been described earlier. By the Duo-measurement method, we measure that the actual latency from this transmission is 3.79 ms. The difference of 0.67 ms between the Duo-measurement method and the Single-measurement method varies very little between different transmissions as the sole delays – acknowledgment delay (no CSMA/CA) and MCU processing delay, are both close to constants between different transmissions.

In this application note, the Single-measurement method is used to perform automated testing over transmission delays of thousands of packets. The latency got from the MCU is 0.67 µs ± 0.3 µs longer than the actual latency. As the unmodified latency data from MCU timestamp is used in test result analysis and report, the user can expect that the latency value in the practical application may be slightly better than the test results.

In this application note, the transmission status on the controller is verified by receiving desired acknowledgement packet. The MAC sequence number varies for each transmission packet, so acknowledgement frame can identify the unicast packet to be acknowledged and there is no ambiguity in transmission status. The transmission status of each packet will be recorded and the total successful transmission will be reported after test is finished. In addition, the latency of the transmission is also recorded. The latency is calculated at application layer. The first time stamp is recorded before calling the function to transmit a packet, and the second time stamp is recorded after the function returns, which means transmission finished. The difference between two time stamps is the transmission latency. Furthermore, if the transmission status is successful, then the latency value is valid. Then the latency value is put into one of the following 11 latency brackets for further data analysis as detailed in Table 1.

TABLE 1: ZigBee® RF4CE LATENCY TEST RESULT BRACKETS

<10 ms
10 ms to 20 ms
20 ms to 30 ms
30 ms to 40 ms
40 ms to 50 ms
50 ms to 60 ms
60 ms to 70 ms
70 ms to 80 ms
80 ms to 90 ms
90 ms to 100 ms
>100 ms

After 1000 RF4CE packets finish transmission, the test results will be printed out on the hyper terminal through the RS232 serial interface. As described before, the test results include number of successful transmission and latency distribution among the 11 brackets.

As illustrated in Figure 3 and Figure 4, of the three supported ZigBee RF4CE channels, the maximum interference between IEEE 802.15.4 and IEEE 802.11 signal in both U.S. and European region is at IEEE 802.15.4 channel 20. For this application note, both ZigBee RF4CE target and controller are programmed to operate on channel 20 and Wi-Fi interference is introduced at IEEE 802.11 channel 7.

WI-FI INTERFERENCE

The Wi-Fi interference source is chosen to be IEEE 802.11n streaming traffic in the format of User Datagram Protocol (UDP). Usually, Wi-Fi traffic for web browsing and/or e-mail reading have relatively low data throughput requirements, therefore do not generate as much interference with ZigBee RF4CE communication. More severe Wi-Fi interference is typically generated by streaming audio and/or video wirelessly through the Wi-Fi network. Table 2 lists the bit-rates of various streaming audio/video sources.

TABLE 2: BIT RATE OF VARIOUS STREAMING SOURCE

STREAMING SOURCES	BIT RATE
MP3	192 Kbps
Video Conference	128 Kbps to 384 Kbps
YouTube Video	0.25 Mbps to 1 Mbps (Standard Definition up to 480P) 2 Mbps to 5 Mbps (High Definition up to 1080P)
Netflix HD	2.6 Mbps to 3.8 Mbps
DVD (MPEG2)	4 Mbps to 5 Mbps (Typical), 10 Mbps (Max)
HDTV (MPEG-4 AVC Encoding)	8 Mbps to 15 Mbps (Typical)
Blu-ray	10 Mbps to 25 Mbps (Typical), 40 Mbps (Max)

In this test, two UDP streaming bit rates are selected to represent different streaming scenario. The lower bit rate of 6 Mbps is typically found in streaming TV programs, DVD videos and on-line video source such as YouTube. On the other hand, higher bit rate of 15 Mbps may be seen in streaming HDTV programs or typical Blu-ray videos.

To generate UDP traffic of desired bit rate, a wireless router/Access Point (AP) and a wireless node is necessary to transmit and receive. In addition, two computers need to connect to the two wireless devices to control them. In this test, we use Linksys E1200 Wireless-N router from Cisco Systems, Inc as the IEEE 802.11n AP. The Linksys router is connected to a laptop computer by Ethernet cable, so that the laptop can have the full control over the AP. Through the Ethernet interface and HyperText Transfer Protocol (HTTP) based browser Graphics User Interface (GUI), the Linksys router is configured to be IEEE 802.11n only mode with frequency bandwidth of 40 MHz at channel 7 to maximize the interference with IEEE 802.15.4 channel 20, which is set for the ZigBee RF4CE communication. On the other side of wireless communication, we use MacBook Pro laptop from Apple Inc. with IEEE 802.11n compatible wireless adaptor. MacBook Pro laptop is configured to join the Linksys AP in IEEE 802.11n mode before the tests.

Open source network testing tool iPerf (http://en.wikipedia.org/wiki/Iperf) is used to generate desired network traffic between the two wireless nodes. The iPerf tools are installed on both the MacBook Pro and Windows-based laptop that is connected to the Linksys AP with Ethernet cable. The Linksys AP with laptop serves as iPerf server, which is started with the command line from DOS command console, as shown in Equation 1.

EQUATION 1:

```
iPerf -s -u -p 2000
```

The server side command line above means to start a UDP server at port 2000. The port number is adjustable for custom setup. On the other hand, the MacBook Pro serves as iPerf client, which is started with the command line from the terminal, shown in Equation 2.

EQUATION 2:

```
iPerf -c 192.168.1.126 -u -p 2000 -b 6M
              -i 5 -t 600
```

The client side iPerf command line means to start the UDP client at port 2000 and connect to the server at IP address 192.168.1.126 with streaming bit rate 6 Mbps, report status every 5 seconds and streaming lasts 600 seconds. The server IP address 192.168.1.126 varies in different setup of Linksys AP. The server IP address can be obtained by type “ipconfig” command from the DOS command console from server side. The port number is adjustable for custom setup, but it has to match the same port number from the server side. When testing with 15 Mbps bit rate, the command line option “-b 6M” must be changed to “-b 15M”.

TEST MONITOR

When the testing is in progress, there are two separate ways to monitor the test. Microchip Wireless Development Studio (WDS) with ZENA™ Wireless Adaptor is used to monitor the IEEE 802.15.4 traffic. WDS is Java-based software tool developed by Microchip to configure MiWi™ Development Environment as well as sniffing the network traffic. Working with Microchip ZENA Wireless Adaptor (2.4 GHz MRF24J40) as hardware sniffer, WDS can catch and save the IEEE 802.15.4 packets. Using the sniffing functionality of WDS, timings of transmission/acknowledgement and retransmissions can be analyzed later. Figure 8 illustrates the WDS and ZENA USB adaptor.

FIGURE 8: MICROCHIP WIRELESS DEVELOPMENT STUDIO AND ZENA™ WIRELESS ADAPTOR

Microchip Wireless Development Studio

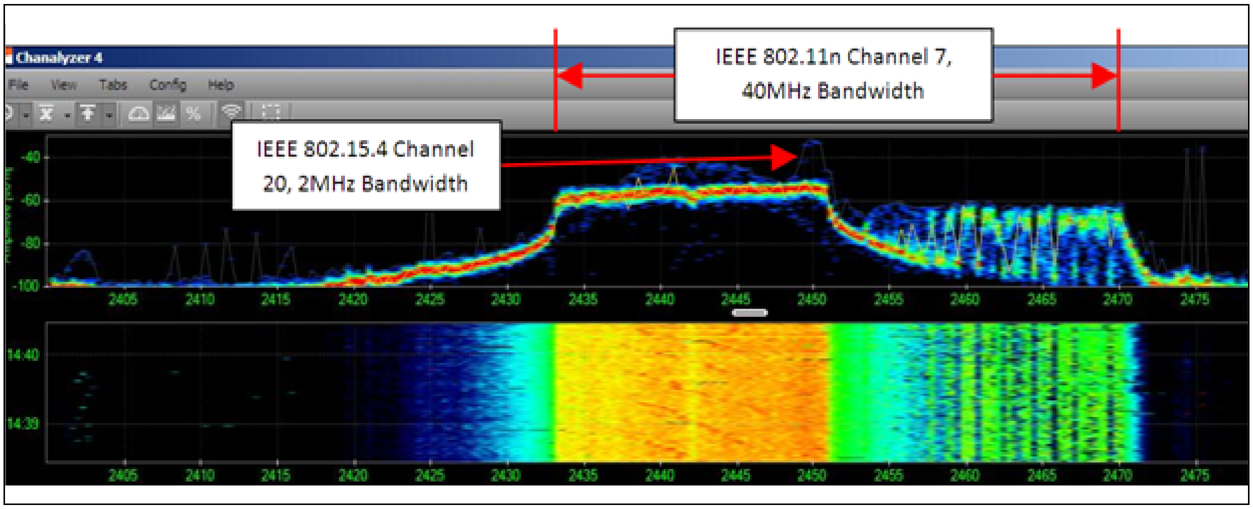
Microchip Wireless ZENA™ Wireless Adaptor

Spectrum monitor is another way to verify the following essential test environment:

- Intense IEEE 802.11 traffic at configured frequency
- IEEE 802.15.4 traffic at configured frequency
- Channels of IEEE 802.15.4 and IEEE 802.11 overlap and interference is likely to occur.

In this application, Wi-Spy 2.4 x 2.4 GHz spectrum sniffer and Channelizer 4 software (http://www.metageek.net/) are used to perform spectrum monitoring. Wi-Spy and Channelizer 4 monitors the spectrum utilization when tests are going on and ensure that the ZigBee RF4CE communication and Wi-Fi interference are performing according to prior configurations. Figure 9 illustrates the testing spectrum with signal identification labels, where the IEEE 802.15.4 channel 20 overlaps with IEEE 802.11n channel 7. As orange/red color of IEEE 802.11 signal indicates, there is high output power intense Wi-Fi traffic when Microchip ZigBee RF4CE latency tests are performed.

FIGURE 9: 2.4 GHz SPECTRUM IN TEST WITH SIGNAL IDENTIFICATION LABEL

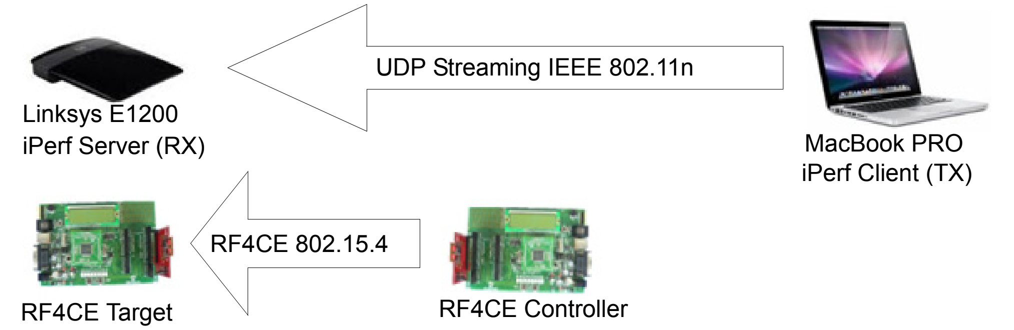
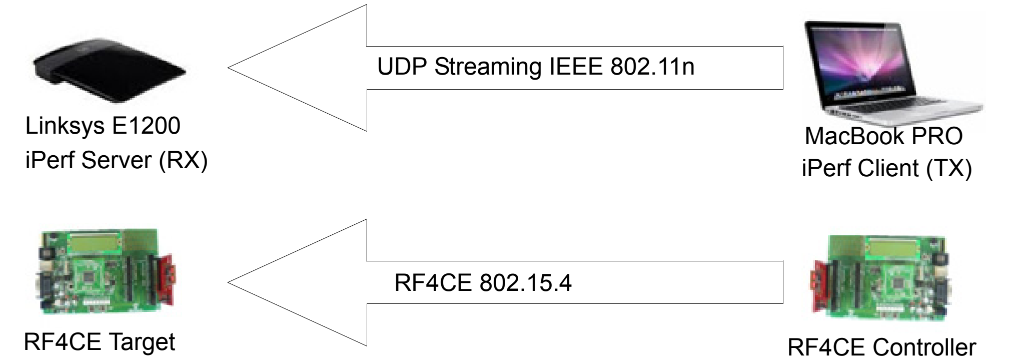
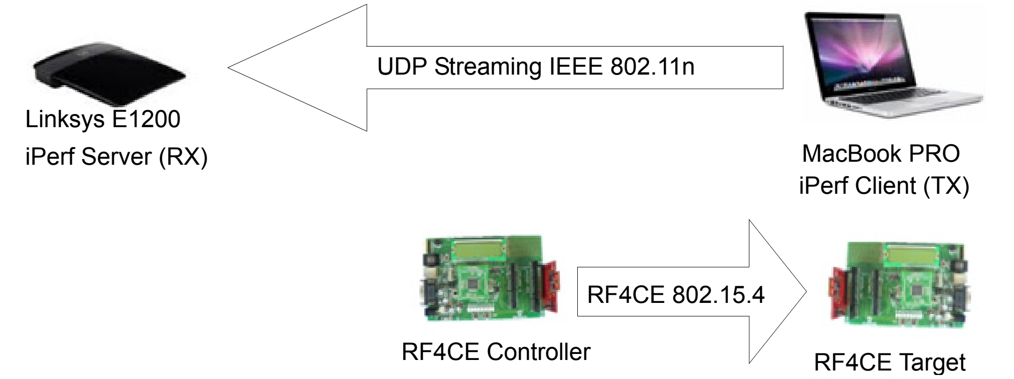
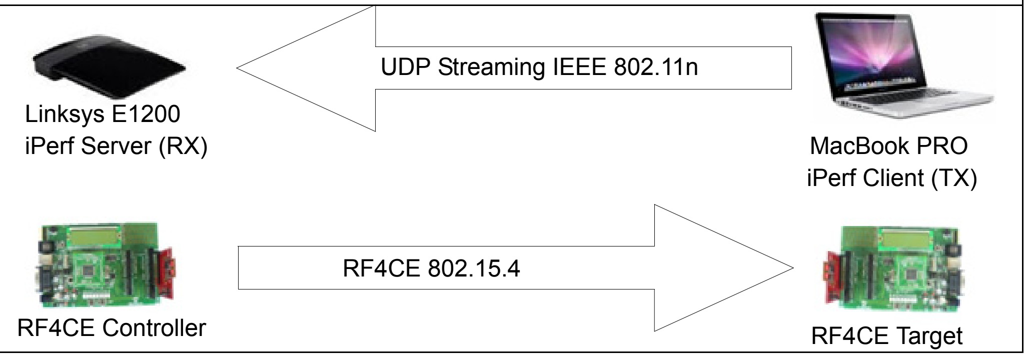


TEST SETUP

To simulate Wi-Fi signals with IEEE 802.15.4 communications under different conditions, four different scenarios are set up to perform the tests. The two Wi-Fi nodes are located 4 meters apart, streaming UDP data in the bit rate of either 6 Mbps or 15 Mbps.

The ZigBee RF4CE target and controller devices are either put 20 cm away from the Wi-Fi node, or at center location between the two Wi-Fi nodes. The different scenarios are illustrated in Figure 10.

FIGURE 10: TESTING SETUP SCENARIO

Setup Number	Hardware Setups
Setup 1	 Linksys E1200 iPerf Server (RX) UDP Streaming IEEE 802.11n MacBook PRO iPerf Client (TX) RF4CE Target RF4CE 802.15.4 RF4CE Controller
Setup 2	 Linksys E1200 iPerf Server (RX) UDP Streaming IEEE 802.11n MacBook PRO iPerf Client (TX) RF4CE Target RF4CE 802.15.4 RF4CE Controller
Setup 3	 Linksys E1200 iPerf Server (RX) UDP Streaming IEEE 802.11n MacBook PRO iPerf Client (TX) RF4CE Controller RF4CE 802.15.4 RF4CE Target
Setup 4	 Linksys E1200 iPerf Server (RX) UDP Streaming IEEE 802.11n MacBook PRO iPerf Client (TX) RF4CE Controller RF4CE 802.15.4 RF4CE Target

Test Results

As described in the previous sections, the firmware on ZigBee RF4CE controller is programmed to send 1000 RF4CE packets. After the test is finished, the following two test results are reported:

- The total number of successful transmission, verified by desired acknowledgement frame
- The transmission latency distribution for packets transmitted successfully

The first set of test result, total number of successful transmission, is easy to report. Of more than 25000 packets that are sent under various conditions in our tests, not a single packet transmission failure is observed. The 100% RF4CE packet delivery rate proves that ZigBee RF4CE protocol specification is very robust and Microchip ZigBee RF4CE implementation is exceptionally reliable.

When there is no interference with other sources in the Microchip RF shielded chamber, the transmission latency is consistently 100% less than 10 ms. When testing is performed under moderate Wi-Fi interferences, such as office environment in Microchip Chandler office, more than 99% of RF4CE packets are verified to be delivered within 10 ms and 100% within 20 ms.

However, transmission latency under strong Wi-Fi interference has wider distribution. In this application note, tests are performed three times under each test configuration and report the test results in the tables Table 3, Table 4, Table 5 and Table 6. Even though there are variations between different runs of the same test configuration, general trend of latency distributions is still clearly visible.

TABLE 3: RF4CE TRANSMISSION LATENCY DISTRIBUTIONS UNDER TEST SETUP 1

Latency (ms)	Packets Received (%)					
	Wi-Fi® Interference: 6 Mbps			Wi-Fi Interference: 15 Mbps		
<10	94.2	89.6	99.1	81.3	78.4	89.4
<20	99.5	98.2	99.9	96.1	96	98.1
<30	99.8	98.7	99.9	97.2	96.9	98.4
<40	99.9	99.4	99.9	99.2	98.5	99.8
<50	99.9	99.8	100	99.9	99.8	99.9
<60	100	100	100	100	100	100
<70	100	100	100	100	100	100
<80	100	100	100	100	100	100
<90	100	100	100	100	100	100
<100	100	100	100	100	100	100
>100	100	100	100	100	100	100

TABLE 4: RF4CE TRANSMISSION LATENCY DISTRIBUTIONS UNDER TEST SETUP 2

Latency (ms)	Packets Received (%)					
	Wi-Fi® Interference: 6 Mbps			Wi-Fi Interference: 15 Mbps		
<10	87.1	86.5	84.1	83.1	77.1	90
<20	98.5	98.3	96.9	97.6	95.4	99.1
<30	99.1	99	98.2	97.9	96.2	99.4
<40	99.4	99.7	99.6	99.7	98.2	99.8
<50	99.6	99.8	99.8	100	98.9	99.8
<60	100	100	100	100	99.5	100
<70	100	100	100	100	100	100
<80	100	100	100	100	100	100
<90	100	100	100	100	100	100
<100	100	100	100	100	100	100
>100	100	100	100	100	100	100

TABLE 5: RF4CE TRANSMISSION LATENCY DISTRIBUTIONS UNDER TEST SETUP 3

Latency (ms)	Packets Received (%)					
	Wi-Fi® Interference: 6 Mbps			Wi-Fi Interference: 15 Mbps		
<10	95.8	98.7	93.8	82.2	88.1	83.6
<20	99.7	99.9	99.4	97	97.4	97.9
<30	99.8	99.9	99.6	97.6	98.4	98.3
<40	100	100	99.9	99.5	99.5	99.3
<50	100	100	100	99.6	99.7	99.9
<60	100	100	100	100	99.9	100
<70	100	100	100	100	100	100
<80	100	100	100	100	100	100
<90	100	100	100	100	100	100
<100	100	100	100	100	100	100
>100	100	100	100	100	100	100

TABLE 6: RF4CE TRANSMISSION LATENCY DISTRIBUTIONS UNDER TEST SETUP 4

Latency (ms)	Packets Received (%)					
	Wi-Fi® Interference: 6 Mbps			Wi-Fi Interference: 15 Mbps		
<10	86.6	86	88.4	76.4	75	80.3
<20	98.4	97.4	98.3	94.5	94.8	96.5
<30	99.3	98.6	98.9	95.4	95.7	97.4
<40	99.9	99.6	99.4	98.2	98.8	98.9
<50	99.9	99.9	99.6	99.3	99.7	99.7
<60	100	100	99.9	99.8	100	99.8
<70	100	100	100	100	100	100
<80	100	100	100	100	100	100
<90	100	100	100	100	100	100
<100	100	100	100	100	100	100
>100	100	100	100	100	100	100

TEST RESULT ANALYSIS

As numerous researches have shown, typical human response time is about 100 ms to 200 ms. Any transmission latency shorter than 100 ms for a remote control application will not have noticeable difference to user experience. In our tests of heavy interference when Wi-Fi is streaming data, we find that very close to 100% of all RF4CE packets are delivered successfully within 50 ms and in the worst case 100% packets are delivered within 70 ms. For a classic remote control application to replace IR based technology, Microchip's ZigBee RF4CE solution provides exceptionally reliable communication with no control lag in the user experience even under the most severe Wi-Fi interference.

For certain non-traditional remote control application, such as wireless game controller, low latency of less than 20 ms is preferred. Our latency distribution test results show that more than 99% of RF4CE packets can be delivered within 10 ms and 100% within 20 ms under normal conditions. Very good gaming experience should be ensured under such conditions. Under intense Wi-Fi interferences, around 95% RF4CE packets are still delivered within 20 ms in the worst scenario. Such latency results from Microchip ZigBee RF4CE solution should still provide acceptable gaming experiences to the user.

As shown in the test results, there are some variations between different runs of the identical test configuration. Those variations may due to the random CSMA/CA back-offs in both IEEE 802.15.4 and IEEE 802.11 transceivers, and different timing of streaming UDP data. By duplicating the same test environments and setups in this application note, users should be able to reproduce the tests and expect similar results. The test firmware is available by contacting your nearest Microchip sales representatives. Microchip sales offices are listed at the end of this application note.

CONCLUSION

IEEE 802.15.4 and IEEE 802.11 specifications implement both preventive and failure recovery mechanisms in the MAC layer to share the frequency. Similarly, ZigBee RF4CE protocol, building on top of IEEE 802.15.4 MAC, further extends the preventive and failure-recovery capabilities in the network layer to share the same frequency. By design, ZigBee RF4CE and Wi-Fi are able to share the same frequency in 2.4 GHz ISM band.

In this application note, Microchip's ZigBee RF4CE solution has been put to the test with Wi-Fi signals under various setups. As the testing result indicates, even under strong Wi-Fi signals, Microchip ZigBee RF4CE solution still provides robust and reliable communication with low transmission latency. Microchip RF4CE solution provides not only unnoticeable control lag to traditional IR replacement remote control, but also good experience to those applications that are sensitive to transmission latency.

Note the following details of the code protection feature on Microchip devices:

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as "unbreakable."

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

Information contained in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION, INCLUDING BUT NOT LIMITED TO ITS CONDITION, QUALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR PURPOSE**.** Microchip disclaims all liability arising from this information and its use. Use of Microchip devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights.

QUALITY MANAGEMENT SYSTEM
CERTIFIED BY DNV
ISO/TS 16949:2009

Trademarks

The Microchip name and logo, the Microchip logo, dsPIC, KEELOQ, KEELOQ logo, MPLAB, PIC, PICmicro, PICSTART, PIC^{32} logo, rfPIC and UNI/O are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

FilterLab, Hampshire, HI-TECH C, Linear Active Thermistor, MXDEV, MXLAB, SEEVAL and The Embedded Control Solutions Company are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Analog-for-the-Digital Age, Application Maestro, chipKIT, chipKIT logo, CodeGuard, dsPICDEM, dsPICDEM.net, dsPICworks, dsSPEAK, ECAN, ECONOMONITOR, FanSense, HI-TIDE, In-Circuit Serial Programming, ICSP, Mindi, MiWi, MPASM, MPLAB Certified logo, MPLIB, MPLINK, mTouch, Omniscient Code Generation, PICC, PICC-18, PICDEM, PICDEM.net, PICkit, PICtail, REAL ICE, rfLAB, Select Mode, Total Endurance, TSHARC, UniWinDriver, WiperLock and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

All other trademarks mentioned herein are property of their respective companies.

Printed on recycled paper.

ISBN: 978-1-61341-905-2

Microchip received ISO/TS-16949:2009 certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona; Gresham, Oregon and design centers in California and India. The Company's quality system processes and procedures are for its PIC® MCUs and dsPIC® DSCs, KEELOQ® code hopping devices, Serial EEPROMs, microperipherals, nonvolatile memory and analog products. In addition, Microchip's quality system for the design and manufacture of development systems is ISO 9001:2000 certified.

Worldwide Sales and Service

AMERICAS

Corporate Office
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 480-792-7200
Fax: 480-792-7277
Technical Support:
http://www.microchip.com/support
Web Address:
www.microchip.com

Atlanta
Duluth, GA
Tel: 678-957-9614
Fax: 678-957-1455

Boston
Westborough, MA
Tel: 774-760-0087
Fax: 774-760-0088

Chicago
Itasca, IL
Tel: 630-285-0071
Fax: 630-285-0075

Cleveland
Independence, OH
Tel: 216-447-0464
Fax: 216-447-0643

Dallas
Addison, TX
Tel: 972-818-7423
Fax: 972-818-2924

Detroit
Farmington Hills, MI
Tel: 248-538-2250
Fax: 248-538-2260

Indianapolis
Noblesville, IN
Tel: 317-773-8323
Fax: 317-773-5453

Los Angeles
Mission Viejo, CA
Tel: 949-462-9523
Fax: 949-462-9608

Santa Clara
Santa Clara, CA
Tel: 408-961-6444
Fax: 408-961-6445

Toronto
Mississauga, Ontario,
Canada
Tel: 905-673-0699
Fax: 905-673-6509

ASIA/PACIFIC

Asia Pacific Office
Suites 3707-14, 37th Floor
Tower 6, The Gateway
Harbour City, Kowloon
Hong Kong
Tel: 852-2401-1200
Fax: 852-2401-3431

Australia - Sydney
Tel: 61-2-9868-6733
Fax: 61-2-9868-6755

China - Beijing
Tel: 86-10-8569-7000
Fax: 86-10-8528-2104

China - Chengdu
Tel: 86-28-8665-5511
Fax: 86-28-8665-7889

China - Chongqing
Tel: 86-23-8980-9588
Fax: 86-23-8980-9500

China - Hangzhou
Tel: 86-571-2819-3187
Fax: 86-571-2819-3189

China - Hong Kong SAR
Tel: 852-2401-1200
Fax: 852-2401-3431

China - Nanjing
Tel: 86-25-8473-2460
Fax: 86-25-8473-2470

China - Qingdao
Tel: 86-532-8502-7355
Fax: 86-532-8502-7205

China - Shanghai
Tel: 86-21-5407-5533
Fax: 86-21-5407-5066

China - Shenyang
Tel: 86-24-2334-2829
Fax: 86-24-2334-2393

China - Shenzhen
Tel: 86-755-8203-2660
Fax: 86-755-8203-1760

China - Wuhan
Tel: 86-27-5980-5300
Fax: 86-27-5980-5118

China - Xian
Tel: 86-29-8833-7252
Fax: 86-29-8833-7256

China - Xiamen
Tel: 86-592-2388138
Fax: 86-592-2388130

China - Zhuhai
Tel: 86-756-3210040
Fax: 86-756-3210049

ASIA/PACIFIC

India - Bangalore
Tel: 91-80-3090-4444
Fax: 91-80-3090-4123

India - New Delhi
Tel: 91-11-4160-8631
Fax: 91-11-4160-8632

India - Pune
Tel: 91-20-2566-1512
Fax: 91-20-2566-1513

Japan - Osaka
Tel: 81-66-152-7160
Fax: 81-66-152-9310

Japan - Yokohama
Tel: 81-45-471- 6166
Fax: 81-45-471-6122

Korea - Daegu
Tel: 82-53-744-4301
Fax: 82-53-744-4302

Korea - Seoul
Tel: 82-2-554-7200
Fax: 82-2-558-5932 or
82-2-558-5934

Malaysia - Kuala Lumpur
Tel: 60-3-6201-9857
Fax: 60-3-6201-9859

Malaysia - Penang
Tel: 60-4-227-8870
Fax: 60-4-227-4068

Philippines - Manila
Tel: 63-2-634-9065
Fax: 63-2-634-9069

Singapore
Tel: 65-6334-8870
Fax: 65-6334-8850

Taiwan - Hsin Chu
Tel: 886-3-5778-366
Fax: 886-3-5770-955

Taiwan - Kaohsiung
Tel: 886-7-536-4818
Fax: 886-7-330-9305

Taiwan - Taipei
Tel: 886-2-2500-6610
Fax: 886-2-2508-0102

Thailand - Bangkok
Tel: 66-2-694-1351
Fax: 66-2-694-1350

EUROPE

Austria - Wels
Tel: 43-7242-2244-39
Fax: 43-7242-2244-393

Denmark - Copenhagen
Tel: 45-4450-2828
Fax: 45-4485-2829

France - Paris
Tel: 33-1-69-53-63-20
Fax: 33-1-69-30-90-79

Germany - Munich
Tel: 49-89-627-144-0
Fax: 49-89-627-144-44

Italy - Milan
Tel: 39-0331-742611
Fax: 39-0331-466781

Netherlands - Drunen
Tel: 31-416-690399
Fax: 31-416-690340

Spain - Madrid
Tel: 34-91-708-08-90
Fax: 34-91-708-08-91

UK - Wokingham
Tel: 44-118-921-5869
Fax: 44-118-921-5820

11/29/11