

ZENA[™] Wireless Network Analyzer User's Guide

© 2007 Microchip Technology Inc.

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in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates.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 16949:2002

Trademarks

The Microchip name and logo, the Microchip logo, Accuron, dsPIC, KEELOQ, microID, MPLAB, PIC, PICmicro, PICSTART, PRO MATE, PowerSmart, rfPIC and SmartShunt are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

AmpLab, FilterLab, Migratable Memory, MXDEV, MXLAB, SEEVAL, SmartSensor 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, CodeGuard, dsPICDEM, dsPICDEM.net, dsPICworks, ECAN, ECONOMONITOR, FanSense, FlexROM, fuzzyLAB, In-Circuit Serial Programming, ICSP, ICEPIC, Linear Active Thermistor, Mindi, MiWi, MPASM, MPLIB, MPLINK, PICkit, PICDEM, PICDEM.net, PICLAB, PICtail, PowerCal, PowerInfo, PowerMate, PowerTool, REAL ICE, rfLAB, rfPICDEM, Select Mode, Smart Serial, SmartTel, Total Endurance, UNI/O, 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.

© 2007, Microchip Technology Incorporated, Printed in the U.S.A., All Rights Reserved.

Printed on recycled paper.

Microchip received ISO/TS-16949:2002 certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona, Gresham, Oregon and Mountain View, California. 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.



ZENA™ WIRELESS NETWORK ANALYZER USER'S GUIDE

Table of Contents

reface1
hapter 1. ZENA™ Wireless Network Analyzer Overview
1.1 Introduction
1.2 ZENA™ Wireless Network Analyzer Kit Contents
1.3 ZENA™ Analyzer Overview
hapter 2. Getting Started
2.1 Introduction
2.2 Installing ZENA™ analyzer software9
hapter 3. ZigBee™ Protocol Tools
3.1 Introduction11
3.2 Microchip Stack Configuration Tool11
3.3 Basic Network Monitoring25
3.4 Advanced Network Monitoring and Analysis
hapter 4. MiWi™ Wireless Networking Protocol Tools
4.1 Introduction
4.2 Microchip Stack Configuration Tool51
4.3 Basic Network Monitoring60
4.4 Advanced Network Monitoring62
dex65
orldwide Sales and Service68

NOTES:



ZENA™ WIRELESS NETWORK ANALYZER USER'S GUIDE

Preface

NOTICE TO CUSTOMERS

All documentation becomes dated, and this manual is no exception. Microchip tools and documentation are constantly evolving to meet customer needs, so some actual dialogs and/or tool descriptions may differ from those in this document. Please refer to our web site (www.microchip.com) to obtain the latest documentation available.

Documents are identified with a "DS" number. This number is located on the bottom of each page, in front of the page number. The numbering convention for the DS number is "DSXXXXA", where "XXXXX" is the document number and "A" is the revision level of the document.

For the most up-to-date information on development tools, see the MPLAB[®] IDE on-line help. Select the Help menu, and then Topics to open a list of available on-line help files.

INTRODUCTION

This chapter contains general information that will be useful to know before using the *"ZENA™ Wireless Network Analyzer User's Guide"*. Items discussed in this chapter include:

- Document Layout
- · Conventions Used in this Guide
- Recommended Reading
- The Microchip Web Site
- Development Systems Customer Change Notification Service
- Customer Support
- Document Revision History

DOCUMENT LAYOUT

This document describes how to use the ZENA Wireless Network Analyzer as a development tool to monitor and analyze wireless network traffic. The manual layout is as follows:

- Chapter 1. ZENA[™] Wireless Network Analyzer Overview This chapter introduces the ZENA Wireless Network Analyzer hardware and software, and briefly describes their capabilities.
- Chapter 2. Getting Started This chapter describes how to install the ZENA software.
- Chapter 3. ZigBee[™] Protocol Tools This chapter describes how to use the ZigBee protocol tools provided with the ZENA analyzer. Both basic and advance monitoring techniques are shown.
- Chapter 4. MiWi™ Wireless Networking Protocol Tools This chapter describes how to use the MiWi protocol tools provided with the ZENA analyzer. Both basic and advance monitoring techniques are shown.

CONVENTIONS USED IN THIS GUIDE

This manual uses the following documentation conventions:

DOCUMENTATION CONVENTIONS

Description	Represents	Examples
Arial font:		
Italic characters	Referenced books	MPLAB [®] IDE User's Guide
	Emphasized text	is the only compiler
Initial caps	A window	the Output window
	A dialog	the Settings dialog
	A menu selection	select Enable Programmer
Quotes	A field name in a window or dialog	"Save project before build"
Underlined, italic text with right angle bracket	A menu path	<u>File>Save</u>
Bold characters	A dialog button	Click OK
	A tab	Click the Power tab
N'Rnnnn	A number in verilog format, where N is the total number of digits, R is the radix and n is a digit.	4'b0010, 2'hF1
Text in angle brackets < >	A key on the keyboard	Press <enter>, <f1></f1></enter>
Courier New font:		
Plain Courier New	Sample source code	#define START
	Filenames	autoexec.bat
	File paths	c:\mcc18\h
	Keywords	_asm, _endasm, static
	Command-line options	-Opa+, -Opa-
	Bit values	0, 1
	Constants	0xFF, `A'
Italic Courier New	A variable argument	<i>file.o</i> , where <i>file</i> can be any valid filename
Square brackets []	Optional arguments	<pre>mcc18 [options] file [options]</pre>
Curly brackets and pipe character: { }	Choice of mutually exclusive arguments; an OR selection	errorlevel {0 1}
Ellipses	Replaces repeated text	<pre>var_name [, var_name]</pre>
	Represents code supplied by user	void main (void) { }

RECOMMENDED READING

This user's guide describes how to use the ZENA Wireless Network Analyzer. Other useful documents are listed below. The following Microchip documents are available and recommended as supplemental reference resources.

Readme for ZENA Wireless Network Analyzer

For the latest information on using the ZENA Wireless Network Analyzer, read the Readme file in the ZENA software installation directory. The Readme file contains update information and known issues that may not be included in this user's guide.

PIC[®] MCU Data Sheets and Family Reference Manuals

See the Microchip web site for complete and updated versions of device data sheets and related device family reference manuals.

Microchip 8-Bit PIC® Microcontroller Solutions (DS39630)

This document provides an overview of the features and functionality of the 8-bit PIC microcontroller product family. It highlights its powerful architecture, flexible memory technologies and easy-to-use development tools.

AN965, Microchip Stack for the ZigBee™ Protocol (DS00965)

This application note describes how you can use the Microchip Stack for the ZigBee protocol to quickly build your application. To illustrate the usage of the Stack, working demo applications are included.

ZigBee[™] Protocol Specification

See the ZigBee protocol web site for the complete and most recent revisions of the ZigBee protocol (http://www.zigbee.org).

PICDEM[™] Z Demonstration Kit User's Guide (DS51524)

The PICDEM Z Demonstration Kit is designed to allow developers to evaluate and experiment with Microchip solutions for the ZigBee protocol. The PICDEM Z Demonstration Kit provides two ZigBee protocol nodes to create a simple, two-node network.

AN1066, MiWi™ Wireless Networking Protocol Stack (DS01066)

This application note describes how you can use the Microchip Stack for the MiWi protocol to quickly build your application. To illustrate the usage of the Stack, working demo applications are included.

IEEE 802.15.4[™] Specification

See the IEEE web site for the complete and most recent revisions of the IEEE 802.15.4 specification (http://www.ieee.org).

THE MICROCHIP WEB SITE

Microchip provides online support via our web site at www.microchip.com. This web site is used as a means to make files and information easily available to customers. Accessible by using your favorite Internet browser, the web site contains the following information:

- **Product Support** Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software.
- General Technical Support Frequently Asked Questions (FAQs), technical support requests, online discussion groups, Microchip consultant program member listing.
- **Business of Microchip** Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives.

DEVELOPMENT SYSTEMS CUSTOMER CHANGE NOTIFICATION SERVICE

Microchip's customer notification service helps keep customers current on Microchip products. Subscribers will receive e-mail notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, access the Microchip web site at www.microchip.com, click on Customer Change Notification and follow the registration instructions.

The Development Systems product group categories are:

- Compilers The latest information on Microchip C compilers and other language tools. These include the MPLAB[®] C18 and MPLAB C30 C compilers; MPASM[™] and MPLAB ASM30 assemblers; MPLINK[™] and MPLAB LINK30 object linkers; and MPLIB[™] and MPLAB LIB30 object librarians.
- **Emulators** The latest information on Microchip in-circuit emulators. This includes the MPLAB ICE 2000 and MPLAB ICE 4000.
- In-Circuit Debuggers The latest information on the Microchip in-circuit debugger, MPLAB ICD 2.
- MPLAB[®] IDE The latest information on Microchip MPLAB IDE, the Windows[®] operating system Integrated Development Environment for development systems tools. This list is focused on the MPLAB IDE, MPLAB SIM simulator, MPLAB IDE project manager and general editing and debugging features.
- **Programmers** The latest information on Microchip programmers. These include the MPLAB PM3 and PRO MATE[®] II device programmers and the PICSTART[®] Plus and PICkit[™] 1 development programmers.

CUSTOMER SUPPORT

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Field Application Engineer (FAE)
- Technical Support
- Development Systems Information Line

Customers should contact their distributor, representative or field application engineer (FAE) for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in the back of this document.

Technical support is available through the web site at: http://support.microchip.com.

DOCUMENT REVISION HISTORY

Revision A (April 2006)

• Initial Release of this Document.

Revision B (January 2007)

• Updated existing ZigBee protocol Stack information and added MiWi™ protocol chapter.

NOTES:



ZENA™ WIRELESS NETWORK ANALYZER USER'S GUIDE

Chapter 1. ZENATM Wireless Network Analyzer Overview

1.1 INTRODUCTION

This chapter introduces the ZENA Wireless Network Analyzer hardware and software, and briefly describes their capabilities. The ZENA analyzer provides three main tools to develop IEEE 802.15.4 solutions quickly and efficiently with the free Microchip Stacks for the ZigBee[™] protocol and the MiWi[™] protocol. The ZENA analyzer enables developers to quickly modify and adapt the Stacks to suit application requirements. The ZENA analyzer is also an IEEE 802.15.4 packet analyzer, currently supporting the 2.4 GHz spectrum. The ZENA analyzer is capable of decoding ZigBee protocol v1.0 and MiWi protocol packets. The ZENA analyzer also provides network analysis support. The ZENA analyzer draws the network topology of the network as it is formed and allows users to watch packet transactions as they occur, record the packet transactions and play these packets back at variable speeds. These tools, combined, form a powerful tool in wireless development for the IEEE 802.15.4 protocol.

Note: The ZENA Wireless Network Analyzer board does not have to be attached to the computer to use the configuration tool or the playback functionality.

1.2 ZENA™ WIRELESS NETWORK ANALYZER KIT CONTENTS

The ZENA Wireless Network Analyzer kit contains the following items:

- ZENA Wireless Network Analyzer
- USB mini-B cable
- ZENA Wireless Network Analyzer CD-ROM

1.3 ZENA™ ANALYZER OVERVIEW

The ZENA Wireless Network Analyzer board, seen in Figure 1-1, combines the PIC18LF2550 for full-speed, USB support with an IEEE 802.15.4 transceiver.

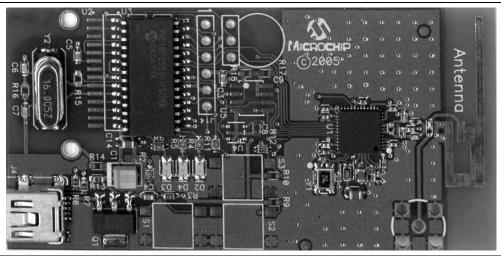


FIGURE 1-1: ZENA™ WIRELESS NETWORK ANALYZER BOARD

The ZENA Wireless Network Analyzer uses a USB mini-B cable to connect to the PC. The ZENA analyzer is powered by the USB bus. A PCB trace antenna receives the packets on the specified channel and sends the information over USB to the PC computer using the HID standard class.



ZENA™ WIRELESS NETWORK ANALYZER USER'S GUIDE

Chapter 2. Getting Started

2.1 INTRODUCTION

This chapter describes how to install the ZENA Wireless Network Analyzer software.

2.2 INSTALLING ZENA™ ANALYZER SOFTWARE

Since the ZENA analyzer software can be used independently of the hardware, it is available from multiple sources, including the ZENA Wireless Network Analyzer CD-ROM, the installation for source files of *AN965, "Microchip Stack for the ZigBee™ Protocol"*, and the installation for source files of *AN1066, "MiWi™ Wireless Networking Protocol Stack"*. The version shipped with the application notes is a demo version, which provides Stack configuration and packet playback capability, but does not allow real-time network monitoring with the ZENA Wireless Network Analyzer hardware. The full version is shipped with the ZENA Wireless Network Analyzer board.

If you are installing the software from the ZENA Wireless Network Analyzer CD-ROM, insert the CD-ROM into your computer's CD-ROM drive. If the installation program does not start automatically, browse to the CD ROM directory and execute the ZENAvn.nn.exe program, where n.nn is the version number of the ZENA analyzer software. Follow the on-screen directions to install the software.

If you have installed the source code for one of the Microchip supported IEEE 802.15.4 protocols, the demo version of ZENA analyzer software is installed automatically in the root directory of the application source code. The demo version of the software allows access to the Stack configuration and message playback features, but it will not communicate with the ZENA Wireless Network Analyzer hardware.

The ZENA Wireless Network Analyzer license agreement is presented. Read the agreement, then click **I Accept** to continue.

The ZENA Wireless Network Analyzer Readme file contains important information about the most recent release of the ZENA Wireless Network Analyzer, such as new features and known issues. The Readme file will change with each release.

Once the ZENA software is installed, use the Start Menu item to launch the software. The introductory screen appears as follows.



FIGURE 2-1: ZENA™ ANALYZER SOFTWARE MAIN WINDOW

NOTES:



ZENA™ WIRELESS NETWORK ANALYZER USER'S GUIDE

Chapter 3. ZigBee[™] Protocol Tools

3.1 INTRODUCTION

This chapter describes how to use the ZigBee[™] protocol tools provided by the ZENA Wireless Network Analyzer. Both basic and advance monitoring techniques are demonstrated.

3.2 MICROCHIP STACK CONFIGURATION TOOL

Microchip provides a freely available Stack as part of application note, *AN965*, *"Microchip Stack for the ZigBee™ Protocol"*. The application note and source code are available for download from the Microchip web site (www.microchip.com). After you have reviewed the application note and studied the demonstration projects, you will be ready to start your own ZigBee protocol application.

The ZENA analyzer will greatly assist you with configuring the Microchip Stack by automatically generating a portion of the source code for your ZigBee protocol application. Be sure to refer to *AN965, "Microchip Stack for the ZigBee™ Protocol"* for details about each ZigBee protocol configuration option. Select <u>ZigBee™ Tools>Stack Configuration</u> from the main ZENA[™] Stack Configuration window. The ZENA[™] Stack Configuration - ZigBee[™] Protocol window will be displayed. Using the tabbed dialog, you can select all of the options required for your ZigBee protocol application. The ZENA software will automatically enable and disable certain options depending on the selections you have made.

3.2.1 Specifying ZigBee Protocol Device Information

Select the **ZigBee Device** tab.

FIGURE 3-1: ZENA™ STACK CONFIGURATION WINDOW, ZIGBEE DEVICE TAB

MAC Address 00 04 A3 Radix • Hex	O Decimal	Transceiver Power Periodically On Initial Power Source Disposable Battery
ZigBee Device Type C ZigBee <u>C</u> oordinator C ZigBee R <u>o</u> uter C ZigBee End De <u>v</u> ice ZD0/APS/NWK/MAC D	IEEE Device Type <u>F</u> FD <u>B</u> FD efaults for Device Type	Available Power Sources Mains Power Disposable Battery Rechargeable Battery Alternate PAN Coordinator
RFD Internal Data Request Manufacturer Code (Hex)	0000	оснір

Using this window, you can configure the following items:

TABLE 3-1 :	ZigBee™ PROTOCOL DEVICE CONFIGURATION SELECTION
--------------------	---

Configuration	Option Description
MAC Address	Each and every ZigBee protocol device must have its own, unique MAC address. The Microchip OUI is provided as a default for development purposes only. Please see <i>AN965, "Microchip Stack for the ZigBee™ Protocol"</i> for additional information.
ZigBee Device Type	ZigBee protocol defines three different types of devices. Select the device type of your application.
IEEE Device Type	Some ZigBee protocol devices have the option of selecting the IEEE device type. Select the appropriate IEEE device type for your application.
ZDO/APS/NWK/MAC Defaults for Device Type	When you change the device type, the ZENA [™] analyzer will automatically set many options to their default settings unless you have altered them. Click this button if you have altered them and would like to restore them to their default values.
Transceiver Power	Offers transceiver power selection. Selects how the transceiver is powered.
Initial Power Source	Offers power source selection. Selects your application's power source.
Available Power Sources	Selects the power sources that are available to your application.
Alternate PAN Coordinator	This option is currently not supported by the Microchip Stack for ZigBee protocol.
Manufacturer Code (Hex)	Each manufacturer of ZigBee protocol devices is assigned a manufacturer code by the ZigBee Alliance. Enter the four-digit hex value.
RFD Internal Data Request Rate (seconds)	If your device is an RFD, it must explicitly request data to receive messages. Some messages sent internally by the Stack itself will generate a response from the recipient that must be received. Enter the internal poll rate for these messages. Note that this polling is independent from the message polling required by the application.

3.2.2 Specifying Transceiver Information

Select the **Transceiver** tab.

FIGURE 3-2: ZENA™ STACK CONFIGURATION WINDOW, TRANSCEIVER TAB

Transceiver Microchip MRF24J40	Frequency Band	Allowed Channels
Output Power -0.00 dBm		▼ 13 ▼ 14 ▼ 15 ▼ 15 ▼ 16 ▼ 17 ▼ 18 ▼ 18
The application code is resp	CS LATCO RESETN LATC2 WAKE LATC1 Allow Shared SPI Check device information before enabling this option.	<u>C</u> lear All Select <u>A</u> ll

Using this window, you can configure the following items:

TABLE 3-2: ZigBee[™] PROTOCOL TRANSCEIVER CONFIGURATION SELECTION

Option Description
Selects one of the transceivers supported by the Stack.
This combo box shows the various available frequency bands of the selected transceiver. If the transceiver supports only one frequency band, that frequency will be displayed and the combo box will be disabled.
Selects the initial output power of the transceiver.
This panel shows the required pins for the selected transceiver. The Stack allows you to change these pin connections to application-specific port pins.
Click this button to restore the pin assignments to the connections used by the PICDEM Z Demonstration Board.
This area shows the channels that are supported by the selected frequency band. Selecting channels here will generate a label that can be used to specify the allowed channels for network formation and network discovery. Click Clear All to uncheck all channels and click Select All to check all channels. Each channel can also be checked or unchecked individually by clicking on the checkbox that precedes the channel number.
Some transceivers require a dedicated SPI unless additional hardware is provided. If you are using an SPI serial EEPROM for external nonvolatile storage, and you want the transceiver and EEPROM to use the same SPI peripheral, select this option to allow additional option selection on the PIC [®] MCU page.

Note 1: Ensure the pin exists on the target device. The application code is responsible for configuring the pin as a digital input or output as appropriate.

3.2.3 Specifying Profile and Endpoint Information

Select the **Endpoints** tab.

FIGURE 3-3: ZENA™ STACK CONFIGURATION WINDOW, ENDPOINTS TAB

		urity ZDO/APS <u>N</u> WK/MAC <u>I</u>	
Profile Header File C:\	MpZBee\ZigBeeStack\	zHCLighting.h	Browse
Profile: Home Contro	al Lighting	Device	
	Endpoint Name	Dimming Load Controller	•
Input Clusters ON or OFF commands for S ON or OFF commands for D DIM or BRIGHT commands Presets lighting level for Dim		er Remote Control (1) Dimmer Remote Control (1) Remote Control (1)	
Presets lighting level for D	occupancy state for Oc		*
	FF commands for Switc FF commands for Dimm 3RIGHT commands for I	er Remote Control (1) Dimmer Remote Control (1)	^
	light level reading for Lig	ht Sensor Monochromatic (2)	~
	Sa <u>v</u> e Endpoint	<u>B</u> emove Endpoint	

Using this window, you can specify the profile and endpoint structure that your application is using. See Table 3-3 for configuration options.

CAUTION

It is critical for ZigBee protocol interoperability that this section be accurate.

Configuration	Option Description	
Profile Header File	 Click Browse to browse to and select the header file for the application's profile. This file has profile information in a specific format which the ZENA[™] analyzer uses to configure many items, including: Profile name The list of devices supported by the profile Allowable input and output clusters Range checking for various parameters on other tabs 	
Device ⁽¹⁾	Select the profile device that describes the application.	
Endpoints ⁽²⁾	 To define an endpoint: Enter the endpoint's numerical value (1-240) in the "Endpoint" edit box. In the "Endpoint Name" edit box, enter a valid C language label for that endpoint. Select all of the input and output clusters that are supported by that endpoint under "Input Clusters" and "Output Clusters". Click Save Endpoint to save the endpoint. The endpoint number will be added to the "Endpoints" list box. To define another endpoint: Click New in the "Endpoints" list box. All of the endpoint information will be cleared. Enter the new endpoint's information and click Save Endpoint. To view a previously defined endpoint: Click on the endpoint number in the "Endpoints" list box. To remove a specified endpoint: Click the desired endpoint: Click the desired endpoint: 	

TABLE 3-3:	ZigBee™ PROTOCOL PROFILE/ENDPOINTS CONFIGURATION SELECTION
-------------------	--

Note 1: The ZENA analyzer does not confirm that all mandatory clusters are supported for the selected device.

2: Be sure to click **Save Endpoint** when you are finished defining an endpoint. If the endpoint information has been entered but not saved, the endpoint will not be included in the generated output files.

Profile Hea	ider File C:\MpZBee\ZigBeeStack	\zHCLighting.h	Browse
Profile: H Endpoints (New) 8	Iome Control, Lighting Endpoint Endpoint Name 8 EP_LIGHT	Device Switch Load Controller	•
	Input Clusters ON or OFF commands for Switc ON or OFF commands for Dimm DIM or BRIGHT commands for Presets lighting level for Dimme Current light level reading for Lig Current occupancy state for Oc	ner Remote Control (1) Dimmer Remote Control (1) r Remote Control (1) ght Sensor Monochromatic (2)	~
	Output Clusters ON or OFF commands for Switc ON or OFF commands for Dimm DIM or BRIGHT commands for Presets lighting level for Dimme Current light level reading for Li Current occupancy state for Oc	ner Remote Control (1) Dimmer Remote Control (1) r Remote Control (1) ght Sensor Monochromatic (2)	<
	Save Endpoint	<u>R</u> emove Endpoint	

FIGURE 3-4:	ENDPOINT SPECIFICATION

3.2.4 Specifying Security Information

Select the **Security** tab.

Security Capable	
Security Mode	Trust Center
<u>B</u> esidential	🔲 I am the Trust Center
C Commercial	Trust Center Address
Security features require that the APS Address Map be utilized. Set Max APS Addresses appropriately.	☐ Trust Center Address Present 00 04 A3 A3 Radix ⓒ Hex ⓒ Decimal
Network Key (Hex)	Sequence Number
00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00
	one additional bank of RAM. The available heap eighbor table size is limited to 32.

FIGURE 3-5: ZENA™ STACK CONFIGURATION WINDOW, SECURITY TAB

This tab is used to configure the security features of the ZigBee protocol Stack. If your application will utilize security, select the "Security Capable" option. Security imposes the following constraints:

- · The Stack requires one additional bank of RAM
- Neighbor table size is limited to 32 (see Table 3-7)
- The APS Address Map must be used (see Max APS Addresses in Table 3-6)

Using this window, you can configure the following items:

TABLE 3-4: ZigBee™ PROTOCOL DEVICE CONFIGURATION SELECTION

Configuration	Option Description
Security Capable	Select this option if your application will utilize security and send and receive encrypted messages.
Security Mode	Only "Residential" mode is currently supported by the Stack.
Trust Center	Select this option if this device is the trust center.
Trust Center Address	If the address of the trust center is known, enter it here.
Network Key Present	If the network key is known, enter it here with the "Sequence Number".
Key present in all devices on the network	Select this option if the device is a ZigBee Coordinator or a ZigBee Router and it contains the network key and all devices on the network contain the network key.

3.2.5 Specifying ZDO and APS Layer Information

Click on the **ZDO/APS** tab.

FIGURE 3-6:	ZENA™ STACK CONFIGURATION WINDOW, ZDO/APS TAB
	,,

ZigBee <u>D</u> evice <u>T</u> ransceiver <u>E</u> ndpoin	its <u>5</u> ecurity	/MAC <u>P</u> IC	I
ZDO Configuration			
🔽 Include Optional Service Discove	ry Requests		
☐ Include Optional Node <u>M</u> anageme	ent Services		
Support End Device Binding			
End Device Bind Timeout (second	is) 5		
Max APS Addresses Binding Support Binding Configuration Max Buffered Indirect Messages Binding Table Size	5	annen son an	
Ga	nerate Files		3

This tab is used to configure the ZDO (ZigBee Device Object) and APS (Application Sub-Support) Stack layers. Many options on this tab are enabled or disabled based on the "ZigBee Device Type" specified on the **ZigBee Device** tab.

Many of these options have a direct correlation to the amount of RAM or nonvolatile memory required by the application. To view the associated cost in the status bar at the bottom of the window, hold the mouse over the appropriate edit box. This feature only functions if the edit box is enabled. See Table 3-5 and Table 3-6 for ZDO and APS option selections.

Configuration	Option Description
Include Optional Service Discovery Requests	If selected, the application will support the optional ZDO service discovery requests. <i>This feature is not yet supported by the Microchip Stack</i> .
Include Optional Node Management Services	If selected, the application will support the optional ZDO node management services. This feature is not yet supported by the Microchip Stack
Support End Device Binding	This function is available only on ZigBee protocol coordinators. If selected, enter the "End Device Bind Timeout (seconds)" in seconds.

TABLE 3-5:ZigBee™ PROTOCOL ZDO CONFIGURATION SELECTION

TABLE 3-6: ZigBee™ PROTOCOL APS CONFIGURATION SELECTION

Configuration	Option Description
Max Frames From APL Layer	Each frame sent down from the Application layer must be buffered for retransmission on failure and for reporting back transmission confirmation status. Enter the number of frames that can be in the process of transmitting at the same time.
Max APS ACK Frames Generated	If messages are received from other nodes with APS level Acknowledgement requested, the APS layer will automatically transmit the Acknowledge; however, space is still required in the confirmation queue. Enter the number of APS level Acknowledges your application is expected to be in the process of transmitting at the same time.
Max APS Addresses	ZigBee protocol allows the Application layer to specify a message destination using a node's 64-bit MAC address, rather than the 16-bit network address. If a 64-bit MAC address is specified, the APS layer searches an application maintained table for the corresponding 16-bit network address. Enter the size of that table in this field. If security is being used, regardless of device type or functionality, the value must be non-zero. If security is <i>not</i> being used and either the Application layer will use only 16-bit network addresses to send messages, or the application is an IEEE Reduced Function Device, the value may be zero. This address map is mandatory if security is supported. It must be large enough to contain one entry for each device that the application will communicate with.
Binding Support ⁽¹⁾	If the device will support bindings, select this option and enter the "Binding Table Size". If a device supports bindings, it must be able to buffer all incoming indirect messages for retransmission. Enter the number of indirect messages the application is expected to handle concurrently in the "Max Buffered Indirect Messages" edit box.

Note 1: Binding support is required for ZigBee protocol coordinators.

3.2.6 Specifying NWK and MAC Layer Information

Click on the **NWK/MAC** tab.

NWK Configuration Neighbor Table Size 24 Max Buffered Broadcast Messages 3	Routing4Route Discovery Table Size4Routing Table Size16Reserved Routing Table Entries8Max Buffered Routing Messages4
MAC Configuration 112 Channel Energy Threshold 112 Transaction Persistence (seconds) 7.68 Receive Buffer Size 256 Beacon Order 15 Superframe Order 15	Superframe Structure Sjotted Non-slotted Battery Life Extension Mode
<u>G</u> enerate	e Files

FIGURE 3-7: ZENA™ STACK CONFIGURATION WINDOW, NWK/MAC TAB

This tab is used to configure the NWK (Network) and MAC (Medium Access Controller) Stack layers. Many options on this tab are enabled or disabled based on the "ZigBee Device Type" specified on the **ZigBee Device** tab.

Many of these options have direct correlation to the amount of RAM or nonvolatile memory required by the application. To view the associated cost in the status bar at the bottom of the window, hold the mouse over the appropriate edit box. This feature only functions if the edit box is enabled. See Table 3-7 and Table 3-8 for NWK and MAC option selections.

Configuration	Option Description
Neighbor Table Size ⁽¹⁾	All ZigBee protocol devices contain a neighbor table where they store information about other nodes in the network.
Max Buffered Broadcast Messages	When a ZigBee protocol device initiates or receives a broadcast message, it must periodically retransmit that message until it hears all of its Full Function Device neighbors retransmit the message or the message times out. Enter the number of broadcast messages that the application is expected to process concurrently.
Route Discovery Table Size ⁽¹⁾	If the device supports routing, it must have a route discovery table.
Routing Table Size ⁽¹⁾	If the device supports routing, it must have a routing table.
Reserved Routing Table Entries ⁽¹⁾	If the device supports routing, it must reserve some of the routing table entries for route repair.
Max Buffered Routing Messages	If the device supports routing, it must be able to buffer messages while awaiting route discovery. Enter the number of messages that can be concurrently buffered awaiting route discovery.

TABLE 3-7: ZigBee™ PROTOCOL NWK CONFIGURATION SELECTION

Note 1: The minimum size of this item is specified in the selected profile. See Section 3.2.3 "Specifying Profile and Endpoint Information".

TABLE 3-8:	ZigBee™ PROTOCOL MAC CONFIGURATION SELECTION
-------------------	--

Configuration	Option Description
Channel Energy Threshold	This option is available for ZigBee protocol coordinators only. Enter the maximum amount of energy allowable for a channel to be selected for a new network.
Minimum Join LQI	This option is only available for devices other than ZigBee protocol coordinators. Enter the minimum link quality from a received beacon for that device to be selected as a potential place to join the network.
Transaction Persistence (seconds)	This option is available for devices with children whose receivers are off when the device is Idle and must buffer messages for those children until the children request them. Enter the amount of time in seconds that messages must be buffered before they can be discarded.
Receive Buffer Size	As bytes are received from the transceiver, they are buffered until an entire message is received and the application is finished processing the previous message. Enter the size of this buffer.
Beacon Order ⁽¹⁾	This value is fixed for non-beacon networks.
Superframe Order ⁽¹⁾	This value is fixed for non-beacon networks.
Superframe Structure ⁽¹⁾	Only non-beacon networks are supported; therefore, the superframe structure is non-slotted.
Battery Life Extension Mode ⁽¹⁾	This feature is only used in beacon networks.

Note 1: The Microchip Stack for ZigBee protocol currently supports only non-beacon networks.

3.2.7 Specifying PIC MCU Information

Select the **PIC** tab.

FIGURE 3-8:	ZENA™ STACK CONFIGURATION WINDOW,
	PIC TAB

Target Device PIC18F4620 💌	Non-volatile Storage		
Speed Settings	Program <u>M</u> emory		
	Erase Block Size		
Clock Frequency (Hz)	Write Block Size 64		
UART Baud Rate 19200 -	C SPI Serial EEPROM		
Device Memory Sizes	Serial EEPROM 25LC256		
Heap Size (banks) 8 💌	Number of Bytes 32768		
Stack Size (banks)	Page Size 64		
Build Target	nCS LATDO		
MPLAB(TM) ICD 2	SPI SPI1 🔽		
C Production <u>R</u> elease	Ensure that the selections exist on the target device. Transceiver choice may affect availabliity.		
5	MAC Address Stored Externally		
Marca water	☐ <u>V</u> erify Writes		

This tab is used to configure basic PIC MCU options (see Table 3-9).

Configuration	Option Description
Target Device	Select the PIC [®] MCU device used by the target application. If the exact device is not available, select a similar device and refer to <i>AN965, "Microchip Stack for the ZigBee™ Protocol"</i> for information on modifying the linker script for the target device.
Clock Frequency (Hz) ⁽¹⁾	Specify the input clock frequency to the PIC MCU in Hertz. It is important that this value be accurate as all internal ZigBee protocol timing will be based off of this value.
UART Baud Rate	If you are using the UART of the target device and you are using the interface code pro- vided in <i>AN965, "Microchip Stack for the ZigBee™ Protocol"</i> , specify the UART baud rate. If your application does not use the UART, this value is irrelevant.
Heap Size (banks)	Specify the number of banks of heap space required by the application. Refer to <i>AN965, "Microchip Stack for the ZigBee™ Protocol"</i> for information on setting the heap size.
Stack Size (banks)	Specify the number of banks required for the C software Stack. Refer to AN965, "Microchip Stack for the ZigBee TM Protocol" for information on setting the Stack size.
Build Target	Select whether you want the linker script generated for a debug environment using MPLAB [®] ICD 2 or for a production build.
Program Memory	Select this radio button if all nonvolatile tables will be stored in program memory. This option may not be available depending on the Target Device family and erase block size.
SPI Serial EEPROM	Select this radio button if all nonvolatile tables will be stored in an SPI serial EEPROM. This option may not be available depending on transceiver settings.
Serial EEPROM	Select the serial EEPROM that will be used. If your EEPROM is not listed, select Other and specify the Number of Bytes and Page Size .
nCS	Select the serial EEPROM's chip select pin. ⁽²⁾
SPI	Select which SPI module to use for the serial EEPROM. The availability of this option depends on transceiver selection and whether shared SPI has been enabled. See Allow Shared SPI in Table 3-2.
MAC Address Stored Externally	Select this option if the device's MAC address will be preprogrammed into the serial EEPROM.
Verify Writes	Select this option to write to the nonvolatile storage until the data reads back identically. This ensures accuracy, but could result in an infinite loop.

TABLE 3-9:	ZigBee™ PROTOCOL PIC [®] MCU CONFIGURATION SELECTION
-------------------	---

Note 1: The PICDEM[™] Z Demonstration Board has a clock frequency of 16 MHz (16000000 Hz) if the PLL is enabled. If the PLL is not enabled, the clock frequency is 4 MHz.

2: Ensure the pin exists on the target device. The application code is responsible for configuring the pin as a digital output.

3.2.8 Generating the Configuration Files

When all of the options on all of the tabs are set appropriately, generate the Stack configuration files by clicking **Generate Files**. The ZENA Wireless Network Analyzer will first perform a validity check to ensure that all required fields have appropriate values and all profile-specific ranges are met. If no endpoints are specified, the ZENA analyzer will generate a warning, but will still generate the output files.

Note: Many options, including endpoint specification, affect multiple output files. Therefore, it is recommended not to mix and match files from different ZENA analyzer sessions.

If the validity check passes, ZENA analyzer will prompt for an output directory for the configuration files. These files are:

- zigbee.def Provides basic definitions for Stack configuration.
- myZigBee.c Provides all ROM initialization for the Stack, including ZigBee protocol device descriptors.
- zLink.lkr Project linker script.

Each of these files has a time and date stamp included in the file. Refer to *AN965*, *"Microchip Stack for the ZigBee™ Protocol"* for more information about these files.

3.3 BASIC NETWORK MONITORING

The ZENA Wireless Network Analyzer hardware and software provide a powerful network monitoring tool for use from development through installation.

Connect the ZENA Wireless Network Analyzer hardware to the PC using the supplied USB mini-B cable. From the ZENA Analyzer Software Main window, select ZigBee™ Tools>Network Monitor. The following window will open:

FIGURE 3-9:	ZigBee™ PROTOCOL NETWORK MONITOR WINDOW								
	ZigBee(TM) Network I	Monitor 🔲 🗙							
	File View Operation Tools Help								
	■ <u>R</u> eal Time Display Channel 12 (0x0C) ▼ Speed Manual ▼	Verboseness Level MAC Condensed NWK Condensed APS Condensed							
	 ✓ Clear Messages on Start ✓ Clear NCD on Start 	☐ Ignore Invalid Packets ▼ Auto <u>S</u> croll							

A blank Packet Sniffer window for displaying network messages will also open. If this window is closed, it can be reopened, either by clicking the **Network Messages** button, or by selecting the <u>View>Network Messages</u> menu option.

The ZigBee[™] Network Monitor window can be used to start and stop real-time network analysis, save and load data and configure the display of the messages.

The following table describes the toolbar functions:

TABLE 3-10: REAL-TIME NETWORK MONITOR TOOLBAR FUNCTIONS

lcon	Menu Equivalent	Function
à	<u>File>Open</u>	Load a previously saved file for display and analysis.
	<u>File>Save</u>	Save the currently loaded information.
	Operation>Start Sniffing/Playback	If "Real-Time Display" is selected, begin packet sniffing. Otherwise, play back the current information as specified by the "Speed" pull-down.
	Operation>Stop Sniffing/Playback	Stop real-time monitoring or playback.
	View>Network Messages	Open the Packet Sniffer window.
83 0	View>Network Configuration Display	Open the Network Configuration Display window.
ē	<u>Tools>Filter</u>	Display or hide filter options.
~ 0	Tools>Security	Enable or disable secure packet decrypting.
	View>Show/Hide Settings	Display or hide the settings of the Network Monitor window.

© 2007 Microchip Technology Inc.

3.3.1 Real-Time Network Monitoring

Before initiating real-time monitoring, set the following options on the ZigBee™ Network Monitor window:

TABLE 3-11: REAL-TIME NETWORK MONITORING CONFIGURATION SELECTION

Configuration	Option Description
Real-Time Display	Select this option to display on-air messages that are received by the Network Analyzer hardware.
Channel	Select the desired channel to monitor. Note that if your application specifies more than one allowable channel to form or join a network, you may have to try multiple channels to find the network. This selection can be changed only while real-time monitoring is stopped.
Clear Messages on Start	Select this option if you want all previously displayed messages to be erased when you start monitoring. If you want the messages to be retained, clear this option.
Ignore Invalid Packets	Select this option if you want packets with invalid checksums to be ignored. If you want all network traffic and noise to be displayed, clear this option.
Auto Scroll ⁽¹⁾	Select this option if you want the Packet Sniffer window to automatically scroll, such that the newest message always appears on the bottom of the Packet Sniffer window.

Note 1: If "Auto Scroll" is selected, system response may slow. "Auto Scroll" can be disabled while real-time monitoring is in progress.

Click the **Play** button or select the <u>Operation>Start Sniffing/Playback</u> menu option to begin real-time monitoring. The received messages are then displayed on the Packet Sniffer window. Figure 3-10 shows a typical sequence of a new node joining a ZigBee protocol network.

Note: It may be necessary to disable "Auto Scroll" on certain PCs.

		•	Beacon Payload p Depth RtrCap NVKVer StkPro 0x0 Y 0x1						T	•
			ITS Specification PendAddr Spec Beacon Payload Permit Count ExtAddr ShortAddr DevCap Depth RtrCap NWKVer StkPro N 0x0 0x0 0x1 0x1	seoclation Request Sec RXOn Pover Dev AltCoord N On Mains FED N 0xFAEC		Nest RSSI 0xF7EB		Association Response RSSI Status Address D00054 Success 0x0001 0xEBEC		
ID RESPONSE		sacon RSSI oxEFEC	Source Superframe Specification GTS Specification Addr B0 SO CAP Batt Ccord Assoc Permit 0x00000 None None OxF N Y N	Dest Source Source Addr As Addr PAII 0x0000 0xFFFF 0x0004Å300000001 A11000		Dest Addr Source PAII Source Addr Data Reg 0x0000 0x1234 0x000443000000001 Data Reg		Dest Addr Source Source Addr Association 0x000043000000001 0x1000443000000054 Status		
REQUEST AND RES		(PAN Rest Dest Dest Dest N N 0xB0 0xFFF 0xFFF	Source PAN 0x1234	Dest PAII 0x1234	IFAN Num N 0xB1 0xE9EB	Dest PAII 0x1234	PAN Aum RSSI Num 0xB2 0xE9EB	Dest PAN 0x1234	AN Num I Dx25 0xF8EB	
ASSOCIATION REQUEST AN	ZENA(TM) Packet Sniffer - ZigBee(TM) Protocol	AC Frame Control - Sec Pend ACK I N N N	AC Frame Control 5 Sec Pend ACK I N N N	Type Sec Pend ACK IPAN Num CMD N N Y N 0xB1	MAC Frame Control Type Sec Pend ACK 1 ACK N Y N	AC Frame Control 5 Sec Pend ACK 1 N N Y	MAC Frame Control Type Sec Pend ACK 1 ACK N Y N	C Frame Control Sec Pend ACK I N N Y	Type Sec Pend ACK IPAN Num ACK N Y N N 0x29	
FIGURE 3-10:	ZENA(TM) Packet Si	Frame Time(us) Len M +1000000 1000000 Type 00002 =3000000 10 CMD	Frame Time(us) Len M +3712 +3712 15 BCN	Frame Time(us) Len +295376 00004 =3299088 21	Frame Time(us) Len +560 +560 3299648 5	Frame Time(us) Len M +11920 +11920 Type 00006 =3311568 20 CMD	Frame Time(us) Len +560 -3312128 5	Frame Time(us) Len MA +5104 13317232 29 CMD	Frame Time(us) Len +560 -	

The various portions of the message are color coded for clarity.

Field	Color
MAC Header	White
MAC Commands and Beacons	Red
NWK Header	Lime
NWK Commands	Fuchsia
APS Header	Yellow
APS Payload/Decoding	Aqua
Security Header and Encrypted Data	Blue
Unknown	Olive

Figure 3-11 shows a message being routed from the originator to the final destination and an APS level Acknowledge being routed back. Note that by using the ZENA analyzer, we can see that the first message is being routed along the network tree, while the Acknowledge is being routed more directly.

Γ		1									F	
		Data 1 0x00 F		Data 1 0x00 F		Data 1 0x:00 F						
		Attrib 0x0000		Attrib 0x0000		Attrib 0x0000						
		Type À UINT8 0		Type A UINT8 0		Type A UINT8 0						
		USa		nsa		nsa		CRC OK		CRC OK		
		0.0.		0.0.		0.0.		FCS Corr 0x6B		FCS [Corr 0x6B		
											•	
		0		0		0		0		9		
				L		L		-				
		Dest Cluster (EP ID 0x08 0x13		Cluster EP ID 0x08 0x13		Dest Cluster (EP ID 0x08 0x13		Dest Cluste EP ID 0x08 0x13		Dest Cluster (EP ID 0x08 0x13		
בחפנ		Sec ACF		Sec ACK N Y		Sec ACI N Y		Sec ACK N N		Sec ACI N N		
		Seq APS Frame Control Dest Itum Type Deliv Mode Sec ACK EP 0x02 DAT UNI N/A N 0x0		Seq APS Frame Control Dest Num Type Deliv Mode Sec ACK EP 0x02 DAT UNI N/A V 0x02		Seq APS Frame Control Dest Num Type Deliv Mode Sec ACK EP 0x02 DAT UNI N/A N 0x00		Seq APS Frame Control Dest Num Type Deliv Mode Sec ACK EP Dx24 ACK UNI N/A N N 0x08		See APS Frame Control Dest Num Type Deliv Mode Sec ACK EP 0x24 ACK UNI N/A N 0x0		
APPLICATION MESSAGE WITH APS LEVEL ACKNOWLEDGE		APS Framé pe Deliv T UNI		APS Fram pe Deliv T UNI		APS Frame pe Deliv T UNI		APS Fram pe Deliv K UNI		APS Fram pe Deliv K UNI		
		Dest Source Radius Seq / Addr Addr Num Type 0 0x0001 0x1ÅF9 0x0Å 0x02 DAT		Dest Source Radius Seq // Addr Addr Addr Type 0x00001 0x1AF9 0x02 DAT		Seq Num DAT		Seq Num Dx24 ACK		Seq Num Dx24 ACK		
APS		Source Radius Seq Addr 0x1AF9 0x0A 0x0		Source Radius Seq Addr 0x1AF9 0x09 0x0		Source Radius Seq Addr Dx1AF9 0x08 0x0		Source Radius Seq Addr 0x0001 0x0Å 0x2		Source Radius Seq Addr 0x0001 0x09 0x2		
		Source Addr 1 0x1AF		Source Addr 1 0x1AF						0		
PAGE		Dest Addr 0x000		Dest Addr 0x000		Dest Addr 0x000		Dest Addr 0x1AF		Dest Addr 0x1AF		
MEX	col	ontrol oute Se SUP N		ontrol oute Se SUP N		ontrol oute Se SUP N		ontrol oute Se EN N		ontrol oute Se EN N		
	M) Proto	IWK Frame Control Fype Ver Route AT 0x1 SUP		NWK Frame Control Type Ver Route MAT 0x1 SUP		NWK Frame Control Vppe Ver Route MT 0x1 SUP		NWK Frame Control Cype Ver Route AT 0x1 EN		NWK Frame Control Cype Ver Route DAT 0x1 EN		
	ZigBee(T	rce IWF Ir Typ∈ AF9 DAT	_	rce NWH Ir Typ∈ 13E DAT		rce IIWF Ir Type 000 DAT		rce NWF Ir Type 001 DAT		rce NWF Ir Typ∈ 13E DAT		
A	- ZENA(TM) Packet Sniffer - ZigBee(TM) Protocol	Dest Dest Source Source INWK Frame Control PAIN Addir PAIN Addir Type Ver Route Sec x1234 0x143E 0x1234 0x14F9 DAT 0x1 SUP N		Dest Dest Source Source INWK Frame Control PAN Addr PAN Addr Type Ver Route Sec x1234 0x00000 0x1234 0x143E DAT 0x1 SUP N		Dest Dest Source Source INWK Frame Control PAN Addr PAN Addr Type Ver Route Sec x1234 0x00001 0x1234 0x0000 DAT 0x1 SUP N		Dest Device Source Source NWK Frame Control PAII Addr PAII Addr Type Ver Route Sec x1234 0x1234 0x1034 0x001 DAT N		Dest Dest Source Source INWK Frame Control PAN Addr PAN Addr Type Ver Route Sec x1234 0x1AF9 0x1234 0x143E DAT 0x1 EN N		
:: 	I) Packet	st Source dr PAN 43E 0x1234		at Source dr PAN 000 0x1234	CRC	at Source dr PAN 001 0x1234	CRC	at Source dr PAN 43E 0x1234	CRC	at Source dr PAN AF9 0x1234	CRC	
	ZENA(TM	st Dest I Addr 234 0x143	PCS 0 X	st Dest I Addr 234_0x000	FCS SSI Corr CRC -15 0x6C 0K	st Dest I Addr 234 0x000	FCS SSI Corr CRC -10 0x6C 0K	st Dest I Addr 234 0x143	FCS SSI Corr CRC -10 0x6C 0K	st Dest 1 Addr 234 0x1AF	FCS SSI Corr CRC -17 0x6B 0K	
51	EI	Dest PAN Ix123	3SI -13	Dest PAN Ix123	SSI -15	Dest PAN Ix123	SSI 10	Dest PAN Ix123	SSI -10	Dest PAN Ix123	[20] [20] [17]	-

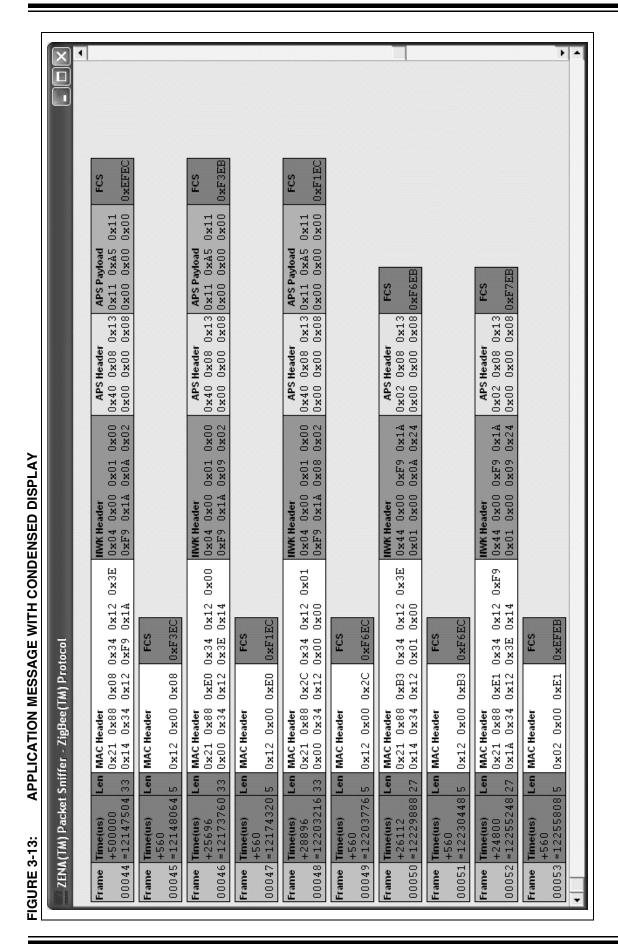
FIGURE 3-11: APPLICATION MESSAGE WITH APS LEVEL ACKNOWLEDGE

Each message can contain a great deal of information, making it difficult to view on the screen. The Packet Sniffer window can be scrolled, but the ZENA analyzer also offers three different levels of viewing the MAC, NWK and APS level information. Each layer can be configured separately on the Network Monitor window by adjusting the "Verboseness Level". There are three levels offered (see Table 3-13).

TABLE 3-13: ZigBee™ PROTOCOL VERBOSENESS LEVEL CONFIGURATION SELECTION

Configuration	Option Description						
Verbose	Headers for each field are provided with a description of the corresponding value below the header. Figure 3-11 shows all layers at the "Verbose" setting.						
Numeric	Headers for each field are provided with the numeric value of that field below the header. Refer to Figure 3-12.						
Condensed	No field headers are provided. All bytes of the field are represented numerically with the Least Significant Byte first. Refer to Figure 3-13.						

	×	RSS 0xE		RSS 0xF		RSS 0xF					•	
		Data 1 0x00 RS 03		Data 1 0x00 R: 03		Data 1 0x00 R: 03						
				8		237						
		action 1 Cmd Type Attrib 0x01 0x01 0x0000		saction 1 Cmd Type Attrib 0x01 0x01 0x0000		1 Type At 0x01 03						
		Transaction 1 SN Cmd T ¢Å5 0x01 0		Transaction 1 SN Cmd T &A5 0x01 0		Transaction 1 SN Cmd T XAS 0x01 0						
		E SN DI 0xA5		E SN 01 0xA5 1		E SN 01 0xA5		er CRC 5B 1		er CRC 5B 1		
		Source AF Header Transaction 1 EP Cnt Type SN Cmd Type Attrib 0x08 0x01 0x01 0x000		Source AF Header Transaction 1 EP Cnt Type SN Cmd Type Attrib 0x008 0x01 0x01 0x01 0x000 0		Source AF Header Transaction 1 EP Cnt Type SN Cmd Type Attrib 0x08 0x01 0x01 0x01		FCS RSSI Corr CRC 0xF6 0x6B 1		FCS RSSI Corr CRC 0xF7 0x6B 1		
		0		0		0		0		0		
		Cluster P ID Dx13 0		Cluster P Dx13 0		Cluster P ID Dx13 0		Cluster P D Dx13 0		Cluster P Dx13 0		
		Dest Cluster EP ID 0x08 0x13		e Dest Cluster EP ID 0x08 0x13		e Dest Cluster EP ID 0x08 0x13		Dest Cluster EP ID 0x08 0x13		e Dest Cluster EP ID 0x08 0x13		
		Source Radius Seq APS Frame Dest Cluster Profile Addr Num Control EP ID ID ID XIAF9 0x0A 0x2 0x40 0x88 0x13 0x000		APS Frame Dest Cluster Profile Control EP ID ID 0x40 0x08 0x13 0x000		APS Frame Dest Cluster Profile Control EP ID ID 0x40 0x08 0x13 0x000		APS Frame Dest Cluster Profile Control EP ID ID 0x02 0x08 0x13 0x000		APS Frame Dest Cluster Profile Control EP ID ID 0x02 0x08 0x13 0x000		
		International Association		Seq Num 0x02		Seq Num 0x02		Seq Num 0x24		Seq Num 0x24		
PLAY		e Radius '9 0x0A		Source Radius Seq Addr Dx1ÅF9 0x09 0x03		Source Radius Seq Addr Dx1ÅF9 0x08 0x02		Source Radius Seq Addr Dx0001 0x0A 0x24		Source Radius Seq Addr Dx0001 0x09 0x24		
		Source Addr 1 0x1AF		Source Addr 1 0x1AF		Sourc Addr 1 0x1AF		Sourc Addr 9 0x000		Sourc Addr 9 0x000		
		Dest Addr 0x000		Dest Addr 0x000		Dest Addr 0x000		Dest Addr 0x1AF		Dest Addr 0x1AF		
		Seq Dest Dest Source Source INW Frame Dest Source Radius Num PAII Addr PAII Addr Addr		Seq Dest Source Source INW Frame Dest Source Radius Num PAII Addr PAII Addr Control Addr Addr Addr Num Addr Addr		Seq Dest Source Source INW Frame Dest Source Radius Num PAII Addr PAII Addr Control Addr Addr Num 0x2C 0x1234 0x0001 0x1234 0x0001 0x14 0x08 0x8		INWK Frame Dest Source Radius Control Addr Addr Ox00 0x00 0x00 0x0A		Dest Dest Source Source NWK Frame Dest Source Radius PAII Addr PAII Addr Control Addr Addr Addr Addr No No		
		Source IN Addr C Dx1AF9 Dx		Source IN Addr (Dx143E 0x		Source IN Addr C				Source IN Addr (Dx143E 0x		
5AGC		Source So PAN A		Source So PAN A Dx1234 0x		Source So PAN A Dx1234 0x		34 (Source So PAN A Dx1234 0x		
ž Z	tocol	Dest So Addr P/ x143E 0x:	CRC 1	Dest Sour Addr PAN)x000000x12	CRC 1	Dest Sour Addr PAH 0x0001 0x12	CRC 1	Dest Sour Addr PAN)x143E 0x12	CRC 1	Dest Sour Addr PAN X1ÅF9 0x12	CRC 1	
	(TM) Pro	st De N Ac 234 0x1	FCS RSSI Corr 0xF3 0x6C	st Dest M Addr 234_0x000	FCS RSSI Corr 0xF1 0x6C	st De N Ac 234 0x(FCS RSSI Corr 0xF6 0x6C	st De N Ac 234 0x1	FCS I Corr 6 0x6C	st De N Ac 234 0x1	FCS I Corr F 0x6B	
APPLICATION MESSAGE WI	. ZigBee(Seq Dest Num PAN 0x08 0x123	Seq Num 0x08 0xF3	Seq Dest Num PAN 0xE0 0x123	Seq Num 0xE0 0xF1	Seq Dest Num PAN 0x2C 0x123	Seq Num RSSI 0x2C 0xF6	Seq Dest Num PAN 0xB3 0x123	Seq Num 0xB3 0xF6	Seq Dest Num PAN 0xE1 0x123	Seq Num DxE1 DxEF	
Ā	Sniffer -	e										
N I	Packet	Len MAC Frame Control 33 0x8821	Len MAC Frame Control 5 0x0012	Len MAC Frame Control 33 0x8821	Len MAC Frame Control 5 0x0012	Len MAC Frame Control 33 0x8821	Len MAC Frame Control 5 0x0012	Len MAC Frame Control 27 0x8821	Len MAC Frame Control 5 0x0012	Len MAC Frame Control 27 0x8821	Len MAC Frame Control 5 0x0002	
	ZENA(TM) Packet Sniffer - ZigBee(TM) Protocol	04	is) 48064	760	is) 74320	216	is) 03776	888	448	248	is) 55808	
	Z	ime(us) -500000 121475	ime(us) 560 12148	ime(us) 25696 12173	ime(us) 560 12174	ime(us) -28896 12203	ime(us) 560 12203	ime(us) -26112 12229	ime(us) 560 12230	ime(us) -24800 12255	ime(us) 560 12255	-



ZENA[™] Wireless Network Analyzer User's Guide

The data can be viewed and analyzed to some degree while real-time monitoring is in progress. For more advanced analysis, real-time monitoring must be halted by clicking the **Stop** button or selecting the <u>Operation>Stop Sniffing/Playback</u> menu option.

To save the data for analysis at a later time, click the **Save** button or select the *File>Save* menu option.

3.3.1.1 TIME-STAMPS

The displayed time-stamp is the time from the end of the previous message until the end of the current message. The time-stamp is displayed in microseconds, and can represent up to 71 minutes before rolling over.

3.3.2 Analyzing Previously Captured Data

When real-time network monitoring is stopped, the ZENA Wireless Network Analyzer can be used to perform further analysis of the captured data. If real-time monitoring is in progress, halt it by clicking the **Stop** button or by selecting the

<u>Operation>Start Sniffing/Playback</u> menu option. To analyze previously captured data, click **Open** or select <u>File>Open</u> and select the desired data file.

3.3.2.1 PACKET PLAYBACK

Captured data can be played back as if it were being received in real time. Playback can begin at any point in the data. To select the first packet to play back, click the desired packet in the Packet Sniffer window. The selected packet will then be outlined in red.

Note: If playback is currently in progress (the **Start** button is disabled and the **Stop** button is enabled), a packet cannot be selected by clicking it.

Select the desired playback speed using the "Speed" combo box. Available options are:

Packet	Option Description
x0.01	Packets are played back approximately 100 times faster than they were received.
x0.1	Packets are played back approximately 10 times faster than they were received.
x1	Packets are played back at approximately the same rate as they were received.
x10	Packets are played back approximately 10 times slower than they were received.
x100	Packets are played back approximately 100 times slower than they were received.
2 sec	Packets are played back at 2-second intervals between packets.
Instant	Packets are played back as quickly as possible.
Manual	Packet playback is controlled by the up and down arrow keys.

TABLE 3-14: ZigBee™ PROTOCOL PACKET PLAYBACK SELECTION

Packet playback is especially useful when using the filter option and performing more advanced network analysis.

3.3.2.2 USING THE PACKET FILTER

Click the **Filter** button or select the <u>*Tools>Filter*</u> menu option to enlarge the Network Monitor window and display the filter options.

ile View Operation Too		
Real Time Display Channel 12 (0x0C) Speed Instant	Verboseness Level MAC Verbose NWK Verbose APS Verbose	
 Clear Messages on Start Clear NCD on Start 	☐ Ignore Invalid Packets ✓ Auto Scroll	
Clear <u>N</u> CD on Start Filter Settings MAC NWK APS		CAND
 Clear <u>N</u>CD on Start Filter Settings 	Auto <u>S</u> croll Source Destination Beacon Request Coordinator Realignment GTS Request	C AND © OR Apply Eiter
Clear <u>N</u> CD on Start Filter Settings MAC <u>NWK</u> APS MAC Commands MAC Beacon Association Request Association Response	Auto Scroll Source Destination Geacon Request GTS Request GTS Request GTS Request GTS Request	

The filter is useful for displaying only selected packets in the Packet Sniffer window. For example, suppose we want to see all beacons generated by our network. Set up the filter as follows:

- 1. Clear all "MAC Commands" checkboxes except "MAC Beacon".
- 2. Clear all "NWK Commands" checkboxes.
- 3. Clear all "APS Commands", "Data" and "Acknowledge" entries.
- 4. Clear all "Source Address" and "Destination Address" entries.
- 5. Select the "OR" option.
- 6. Click **Apply Filter**.

The Packet Sniffer window will then display all beacon packets and hide all others. Refer to Figure 3-15.

Note: If the current data was loaded from a saved file, Source Addresses and Destination Addresses will be blank until packets are played back. It may be necessary to disable and re-enable the filter to display addresses.

FIGURE 3-15:	3-15:	FILTERED BEACONS	D BE	ACOI	NS																			
ZENA	TM) Packet S	ZENA(TM) Packet Sniffer - ZigBee(TM) Protocol	TM) Prote	ocol																			ē	×
																								4
2 Hic	2 Hidden Packet(s)	t(s)						\square																
frame 1 00003	Frame Time(us) Len Type +3712 00003 =3003712 16 BCN	AC Fram Sec 1 N	e Control Pend ACK N N	IPAN	Seq Num 0x24	Seq Source Num PAN 0x24 0x1234	Source Addr 0x0000	Sur BO None	SO C	e Specifi AP Bal xF N	cation bt Cool	ord Asso Y	DC Peri	Specificat nit Cou 03	tion Ext tunt Ext c0 0	PendAdd ExtAddr 9 0x0	h Spec ShortÅddr 0x0		DevCap De	Beacon Payloa Depth RtrCap 0x0 Y	-	NUKVer 9 0x1	StkPro 0x1	
7 Hic	7 Hidden Packet(s)	t(s)						Π																
Frame 00011	Frame Time(us) Len M +3712 00011 =4821504 16 BCN	AC Fram 9 Sec 1 N	e Control Pend ACK N N	IPAN N	Seq Num 0x26	Seq Source Num PAII 0x26 0x1234	Source Addr 0x0000	sur BO None	so d None 0	e Specifi AP Bar xF N	cation tt Cool Y	rd Ass	oc Pern N	Specificat nit Cou 03	tion tint Ext c0 0	PendAdd Addr x0	fr Spec ShortAd 0x0	ddr Dev(DevCap De	Beacon P.)epth Rtr 0x0 Y	ayload Cap NW	UKVer 9 0x1	StkPro 0x1	
7 Hic	7 Hidden Packet(s)	t(s)						Π																
Frame 00019	Frame Time(us) Len M +3712 +3712 Type 00019 =66332366 16 BCN	AC Fram Sec 1	Pend ACK	IPAN N	Seq Num 0xDB	Seq Source Num PAII 0xDB 0x1234	Source Addr 0x143E	B0 None	SO 0	e Specifi CAP Bat OxF N	cation ot Cool	rd Ass	pc Peri	Specificat nit Con 01	tion Ext	PendAddr Spec ExtAddr Short 0x0 0x0	~4	ddr Dev(evCap De	Beacon Payloa epth RtrCap 0x1 Y	- ×	UKVer 9 0x1	StkPro 0x1	
Frame 00020	Frame Time(us) Len M +5232 +5232 Type 00020 =6644528 16 BCN	AC Fram Sec 1	Pend ACK	IPAN N	Seq Num 0x28	Seq Source Num PAII 0x28 0x1234	Source SuperFran Addr BO SO 0x0000 None None	Sur BO None	so c So c None 0	SuperFrame Specification SO CAP Batt Co e None OxF N	cation tt Coord Y	rd Ass	DC Peri	GTS Specification Permit Count N 0x0	EX	PendAddr Spec ExtAddr Short 0x0 0x0	dr Spec ShortÅddr 0x0		DevCap De	Beacon Payload Depth RtrCap NUKVer 0x0 N 0x1	ayload Cap NU		StkPro 0x1	
53 H	53 Hidden Packet(s)	et(s)						Γ																
•																								Þ A
Note:		If the "Source Address" and "Destination Address" areas are empty and are needed for your desired filter, replay the network formation portion of the data. If you will be working with a network that maintains the same structure, you may want to save a captured data file that contains the network formation for populating these fields.	ess" al will be ion for	nd "D nork D	estin ing w ılatin	ation / ith a r g thes	Addre netwo se field	ss" ar rk tha Js.	eas a t mair	re em ntains	pty ar the s	ame :	e need structi	led for ure, y	່your ວu mຍ	desire ay wai	Address" areas are empty and are needed for your desired filter, replay the network formation portion network that maintains the same structure, you may want to save a captured data file that contains te fields.	r, replá ave a	ay the captu	netwo ired da	ork forr ata file	that o	n port conta	tion ains
			Ċ																					ĺ

ACON 2.15

To redisplay all messages, click Clear Filter.

To close the filter and return the Network Monitor window to its original size, click the Filter toolbar button.

3.3.2.3 HIDING AND UNHIDING PACKETS

Packets in the Packet Sniffer window can be hidden in two ways:

- · Using the filter function as described above
- Right clicking on a packet and selecting Hide from the pop-up menu
 - **Note:** Multiple packets can be selected for hiding by holding down the control key while clicking each desired packet. A range of packets can be selected by clicking on the first packet of the range, then holding down the shift key while clicking on the last packet of the range. Each selected packet will be outlined in red. When all desired packets have been selected, right click and select Hide to hide all selected packets.

The hidden packets can be redisplayed by right clicking on the appropriate "X Hidden Packet(s)" box in the Packet Sniffer window and clicking UnHide.

3.3.3 Analyzing Secure Transmissions

If the network key is available, the ZENA analyzer can decrypt the data and display it in the Packet Sniffer window.

A series of messages utilizing security is shown in Figure 3-16.

To decrypt these messages, enable decryption by clicking the **Security** button or by selecting the <u>*Tools>Security*</u> menu option. Enter the network key and security level used during the transmission and click **Accept Security Parameters**. The messages will now be displayed in their decrypted format, as shown by Figure 3-17.

- **Note 1:** This feature is intended to support development efforts only. Network transmissions cannot be decrypted unless both the network key and the encryption method (security level) are known.
 - **2:** The ZENA analyzer supports security decryption at the MAC and NWK layers. APS layer decryption is not currently supported.
 - **3:** Secure packet decryption is computation intensive. If network traffic is heavy, it may not be possible to decrypt data during real-time display without losing packets. Data should then be decrypted during packet playback.

JRITY	
2	
0	I
ш	I
ົ	I
ö	
÷	
~	
ო	
ш	
Ω.	l

FIGURE 3-16:	3-16:	S	SECURITY																
ZENA(Th	A) Packet	t Sniffer	_ZENA(TM) Packet Sniffer - ZigBee(TM) Protocol	rotocol														Ō	×□
																			•
Dest De PAN Ac 0x1234 0x(Dest Sol Addr Ad)x000000x2	Source II Addr Ty 0x287B DA	Dest Source INWK Frame Control Dest Source Radius Seq PAII Addr Type Ver Route Sec Addr Addr Mun Dx1234 0x00000 0x287B DAT 0x1 SUP Y 0x00000 0x287B DAG 0x51	el De De De V De	Dest So Addr Ac x000000x2	Source Radius Seq Addr Dx287B 0x0A 0x51	lius Seq Num DA 0x53	Securit ExtN t Y	y Control Key Lv. NWK 0	Security Control ExtN Key Lv1 Y NWK 0 0x006662A5	Seq Security Control Frame Counter Source Address Key Encrypted Data Num Ext N Key Incrypted Data 0xDC 0xED 0x70 0xEB 0x77 0x51 Y NWK 0 0x006662A5 0x0004300000088 0xF4 0xF5 0xD3 0x03 0x51 0x51	ess Key SN 000088 0x76	N Enery N 0xDC 76 0xF4	Encrypted Data 0xDC 0x6D 0x 0xF4 0xF5 0x	(28 0x7D D3 0x57	0×E9 03 0×D3 03	x70 0xE) x03 0xD)	B 0x77 5 0x51	RS: +1:
FCS RSSI Corr CRC +02 0x69 0K	CRC OK																		
Dest De PAN Ac 0x1234 0x(Dest Sol Addr Ad 0x000000x2	Source II Addr Ty 0x287B DA	Dest Dest Source INWR Frame Control Dest Source Radius Seq Security PAII Addr Addr Type Ver Route Sec Addr Addr Addr ExtN Nx1234 0x00000 0x287B Dx1 SUF Y 0x00000 0x287B 0x52 Y	el Di E Sec A	Dest So Addr Ac x000000x2	urce Rad Idr 87B 0x0	lius Seq Num DA 0x52	ExtN 2 Y	y Control Key Lv. NWK 0	Source Radius Seq Security Control Frame Counter Addr Num ExtN Key Lv1 Security 3x287B 0x0A 0x52 Y NUK 0 0x00666246	Seq Security Control Frame Counter Source Address Key Encrypted Data Num Ext N Key Incrypted Data 0x34 0x25 0xD1 0x26 0x50 0xC0 0x52 Y NUK 0 0x006662246 0x0000000088 0x76 0x28 0x26 0xF1 0xC0	ess Ke St 1000088 0x	Key Encry SH 0x34 0x76 0x28	Encrypted Data 0x34 0x25 0x 0x28 0x20 0x	D1 0xE0 5B 0xF8	0×26 0> 0×60 0>	xE8 0x51 xF1 0xC	0 0xC0 6 0xAD	RS: +2:
FCS RSSI Corr CRC +02 0x67 0K	CRC OK																		ł
-																			•
FIGURE 3-17:	3-17:		DECRYPTED																
1.1																		Č	

\mathbf{X}	- 1 1 1 1			F
	a1 00 RSS +17		a 1 FF RSS: +22	
	Data 1 0 x 0 0		Data 1 D OxFF	
	Attri] 0x000		Attrib 0x0000	
	Type Attrib Data1 UINT8 0x000 RSS		Type Attrib 0xFF UINT8 0x0000	
	nsaction 1 Cmd Set		nsaction 1 Cmd Set	
	E SN Dx68		E SN 0x69	
	RadiusSeqAPS Frame ControlDestClusterProfileSourceAF HeaderTransactionNumTypeDelivModeSecACKEPNCutTypeSNCmd0x00Å0x51ÅDX51DATUNIN/ANNDx008Dx010Dx018Dx018Dx68Set		Radius Seq APS Frame Control Dest Cluster Profile Source AF Header Transaction Num Type Deliv Mode Sec ACK EP ID ID EP Cut Type SN Cmd 0x00Å 0x52 DAT UNI N/A N 0x08 0x13 0x0000 0x08 0x69 Set	
	Source EP 0x08		Source EP 0x08	
	SeqAPS Frame ControlDestClusterProfileHumTypeDelivModeSecACKEPIDID0x51DATUNIN/AN0x080x130x00000		SeqAPS Frame ControlDestClusterProfileNumTypeDelivModeSecACKFPIDID0x52DATUNIN/AN0x0080x130x00000	
	Cluster ID 0x13		Cluster ID 0x13	
	Dest Dest Dest Dest		Dest Dest Dest Dest	
	Sec AC		Sec AC	
	e Control Mode N∕A		s Control Mode N/A	
	APS Frame Control De Deliv Mode : F UNI N/A		APS Frame Control pe Deliv Mode (F UNI N/A	
	Type Type		I Type 2 DAT	
	Radius Seq Num 0x0A 0x51		Radius Seq Num 0x0A 0x52	
	Source Rac Addr 0x287B 0x		Source Rad Addr 0x287B 0x	
otocol	Sec /		Sec /	
(TM) Pro	Control Route SUP		Control Route SUP	
ZigBee(K Frame e Ver Ox1		KFrame e Ver 0x1	
niffer -	Dest Source IIWK Frame Control Dest Addr Type Ver Route Sec Addr x00000 0x287B DAT 0x1 S00000		Dest Source INWK Frame Control Dest Addr Addr Type Ver Route Sec Addr 1x0000 0x287B DAT 0x1 SUP Y 0x0000	
acket Si	Sourc Addr 0x28:	<u> </u>	Sour Addr 0 0x28;	Q.
ZENA(TM) Packet Sniffer - ZigBee(TM) Protocol	Dest Addr 0x0000	FCS RSSI Corr CRC +02 0x69 0K	Dest Addr 0x0000	FCS RSSI Corr CRC +02 0x67 0K
ZEN	Dest PAII x1234	FCS 5SI Co 02 0x	Dest PAN x1234	FCS 5SI Co 02 0x

ZigBee[™] Protocol Tools

 $\ensuremath{\textcircled{}^{\circ}}$ 2007 Microchip Technology Inc.

3.4 ADVANCED NETWORK MONITORING AND ANALYSIS

3.4.1 Network Configuration Display Window

The ZENA Wireless Network Analyzer provides an extra level of network monitoring and analysis with the Network Configuration Display (NCD). Open the ZENA[™] Network Configuration Display window by clicking the **Network Configuration Display** button or by selecting the <u>View>Network Configuration Display</u> menu option on the Network Monitor window.

FIGURE 3-18:	NETWORK CONFIGURATION DISPLAY	

	ration Display - ZigBee(TM) Protocol	
Show Last Messages 🔲 💌	Clear All Lines Clear All Message Lines Clear NCD	
Unknown		

The NCD window can be used during both real-time network monitoring and packet playback. If the "Clear NCD on Start" checkbox on the Network Monitor window is selected, then the NCD window will be cleared when real-time monitoring is started. If you want the nodes to be retained, clear this checkbox.

Note: Due to heavy system loading during real-time monitoring, the NCD window may not update properly during real-time monitoring, particularly if there is a lot of network traffic and if "Auto Scroll" is enabled. For best results, disable "Auto Scroll" if network traffic is heavy. The NCD window will update properly during packet playback.

When the ZENA analyzer receives a message from a device, it creates a node in the NCD window. The label for the node will be its 64-bit MAC address. To see the node's PAN ID and 16-bit network address, hold the cursor over the node. If the node's MAC address is not available, the label for the node will be the node's PAN ID and 16-bit network address. If the ZENA analyzer monitors network creation, it can also color code the nodes according to device type.

Node Type	Color
ZigBee [™] Protocol Coordinator	Aqua
ZigBee Protocol Router	Fuchsia
FFD End Device	Lime
RDF End Device	Yellow
Unknown	White

When a message travels from one device to another, the NCD window will display a line from the source node to the destination node. If a device transmits a broadcast message, the NCD window will display a circle around the source node.

Note: Some messages, such as MAC Acknowledges, do not contain any address information. These messages are shown originating from the Unknown node.

Nodes can be hidden by right clicking the node and selecting Hide. A new node, named "Hidden", will be created and all lines that would normally be drawn to the hidden nodes will be drawn to that node. To unhide all hidden nodes, right click the "Hidden" node and select Unhide All.

When a device joins the network, the parent-child relationship of that device is shown by a silver line between the two devices. See Table 3-16 for NCD window controls.

 TABLE 3-16:
 ZigBee™ PROTOCOL NCD CONFIGURATION SELECTION

Control	Option Description
Show Last Messages	This combo box allows you to select how many message lines are displayed. When a new message line is drawn, the oldest line is removed. Several predefined options are available, or you may enter your own value. The silver network association lines are not affected by this setting.
Clear All Lines	Click this button to clear all message and network association lines. The nodes themselves are unaffected.
Clear All Message Lines	Click this button to clear all message lines. The network association lines and the nodes themselves are unaffected.
Clear NCD	Click this button to clear all message lines, all network association lines and all nodes.
Select Bitmap	Click this button to load a background image. This is described in more detail in Section 3.4.4 "Customizing the Network Configuration Display Window".
Clear Background	Click this button to remove the background image.

3.4.2 Viewing Network Formation

The following sequence of figures shows how network formation appears on the NCD window.

First, the ZigBee protocol coordinator sends a beacon request.

FIGURE 3-19:	NCD BEACON REQUEST
--------------	--------------------



Since there are no nodes on this channel, no beacons are received, and the ZigBee protocol coordinator forms a network.

Next, a ZigBee protocol router tries to find a network to join. It also emits a beacon request, which looks just like Figure 3-19, since the beacon request contains no source address information. Now, the ZigBee protocol coordinator responds with a beacon.

	ration Display - ZigBee(TM) Protocol	- DX
Show Last Messages 📋 🖵	Clear All Lines Clear All Message Lines Clear NCD	
Unknown		
1234:0000		

FIGURE 3-20: NCD BEACON

Note that the ZENA analyzer can tell from the beacon that this device is a ZigBee protocol coordinator, but it does not yet know its MAC address.

The ZigBee protocol router will now try to join the network by sending an Association Request. The ZENA analyzer can tell from the Association Request what type of device is trying to join the network.

ZENA(TM) Netwo	rk Configuration Display - ZigBee(TM) Protocol	
Show Last Messages 🔋	💌 🛛 Clear All Lines 🛛 Clear All Message Lines 🖉 Clear NCD 🛛 🖾 🗶	
	204.A3 00 0.00 00.01 V 234.0000	

FIGURE 3-21: NCD ASSOCIATION REQUEST

After a short time, the ZigBee protocol router will send a Data Request, asking for the Association Response. The ZigBee protocol coordinator will respond by sending the Association Response.

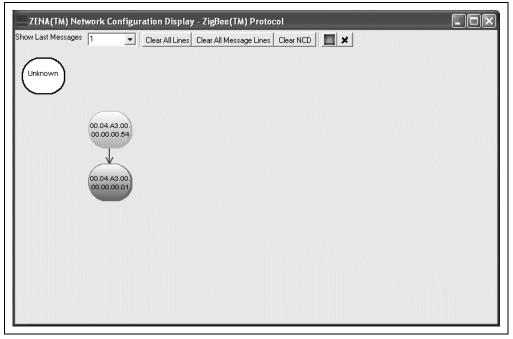


FIGURE 3-22: NCD ASSOCIATION RESPONSE

Now the device has joined the network. This relationship can be seen by clicking **Clear All Message Lines** to display only the network association lines.

FIGURE 3-23: TWO-DEVICE NETWORK

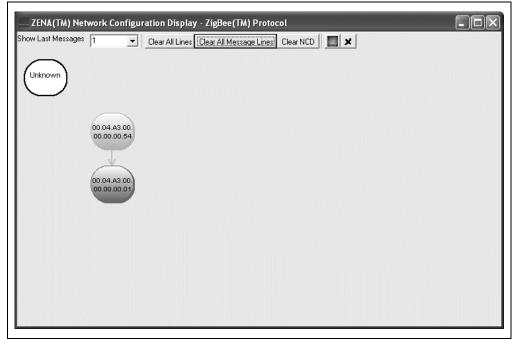


Figure 3-24 shows the NCD window after the creation of a four-device network.

and the second division of		
Contractory of the local division of the loc	ENA(TM) Network Configuration Display - ZigBee(TM) Protocol	
Show L	Last Messages 1 Clear All Lines Clear All Message Lines Clear NCD X	
	00.00.00.54 00.04.A3.00 00.00.00.01 00.00.03F 00.04.A3.00 00.00.03F 00.04.A3.00 00.00.03F	

FIGURE 3-24: FOUR-DEVICE NETWORK

Note: If you will be working with a network that maintains the same structure, you may want to save a captured data file that contains the network formation. You can play back this file to establish the devices on the network, and then play back the various data files containing the network traffic you would like to monitor.

3.4.3 Viewing Network Traffic

After the network above was created, one of the devices attempted to send a message to another device. The path that the message followed is shown in Figure 3-25.

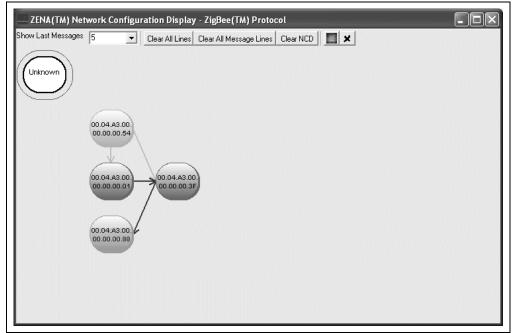
FIGURE 3-25: NCD MESSAGE PATH

ZENA(TM) Network Configuration Display - ZigBee(TM) Protocol	
Show Last Messages 5 🗾 Clear All Lines Clear All Message Lines Clear NCD 📰 🗶	
Unknown	
00.04.A3.00.	
00.00.00.54	
00.04.A3.00 00.00.00.01 00.00.00.05	
00.04.A3.00.	

The NCD window shows how the message went from device 00.04.A3.00.00.00.00.88 to device 00.04.A3.00.00.00.00.01, traveling through two other nodes.

This particular message requested an APS Acknowledge. Figure 3-26 shows the path of the APS Acknowledge. The ZENA analyzer illustrates that the APS Acknowledge followed a different route than the original message.

FIGURE 3-26: NCD APS ACKNOWLEDGE PATH



3.4.4 Customizing the Network Configuration Display Window

When analyzing network traffic, it is often helpful to understand the physical relationship between the devices. The ZENA analyzer allows you to select a bitmap as the background of the NCD window. The nodes can then be dragged so that they match their physical location.

For example, Microsoft[®] Visio[®] drawing and diagramming software can be used to generate a simple floor plan. The floor plan can then be exported as a bitmap.

FIGURE 3-27: FLOOR PLAN BITMAP

Load this floor plan as the NCD background by clicking the **Select Bitmap** button. The NCD window can be resized after loading the background to match the proportions of the bitmap.

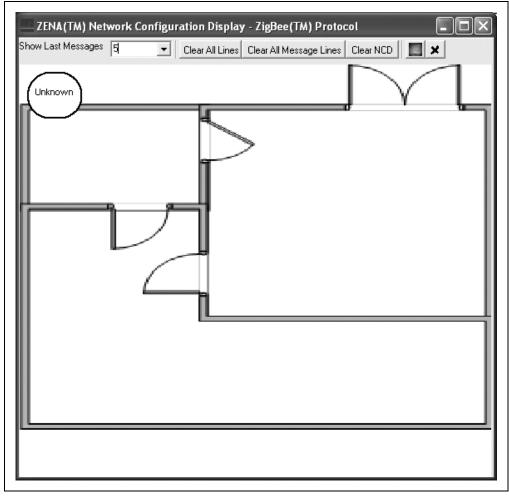


FIGURE 3-28: NCD WINDOW WITH FLOOR PLAN BACKGROUND

When network formation is played back and displayed on the NCD window, the nodes can be moved to the location on the bitmap that represents their physical location.

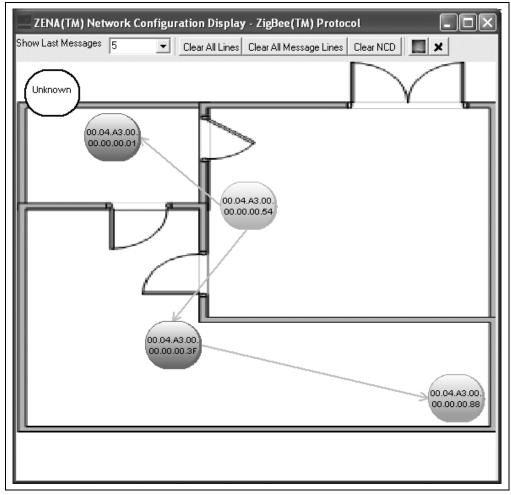


FIGURE 3-29: FOUR-NODE NETWORK WITH FLOOR PLAN BACKGROUND

Repeating the above example, Figure 3-30 and Figure 3-31 show the application message and APS Acknowledge as they are routed through the network.

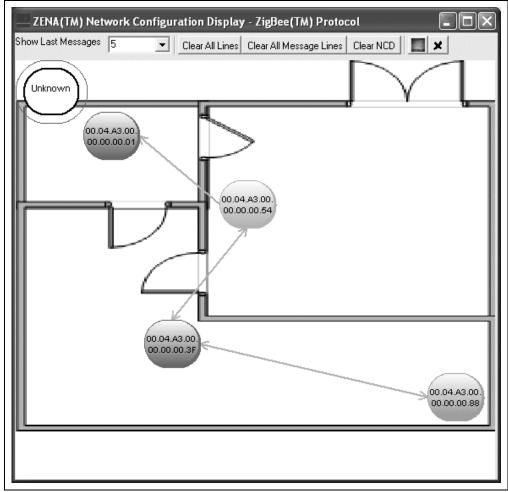
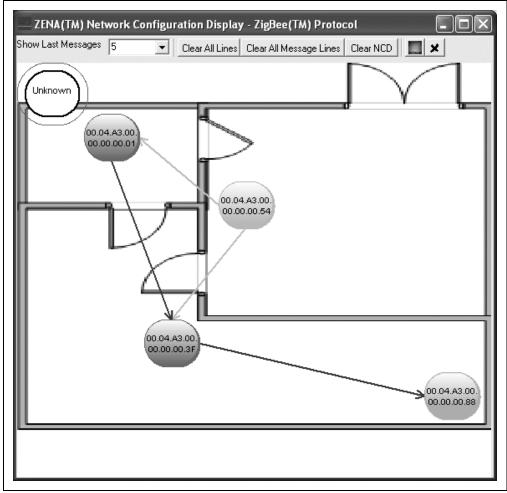


FIGURE 3-30: MESSAGE PATH WITH FLOOR PLAN BACKGROUND





3.4.5 Analyzing Network Traffic

The ZENA Wireless Network Analyzer can provide a great deal of information about device and network operation. The Packet Sniffer window can be used to ensure that messages are appearing on the air as expected, and that the messages have the correct format. The NCD window can be used to ensure the network is formed in the correct manner.

The ZENA analyzer can show how messages propagate through the network. In the examples above, we see by using the NCD window that the application message is routed along the network tree, while the Acknowledge is routed more directly. Using the Packet Sniffer window, we can determine if the message was sent with routing suppressed, or if routing was requested but a node in the path did not have routing capacity.

The ZENA analyzer can also provide insight as to physical barriers that are affecting the system. In the previous example, we can see that physical barriers are probably preventing two nodes from talking directly.

With a larger scale network, the ZENA analyzer can also help determine if device layout needs to be optimized for the system's required network traffic. If the ZENA analyzer indicates that a great deal of traffic is being routed through a single device, that device may be getting overloaded. An alternate arrangement of devices might generate more balanced network traffic.

3.4.6 Exporting Data

In some cases, it may be necessary to export the raw message data to another tool for further analysis. To export raw data, select the desired packets in the Packet Display window, right click on the packets and select **Copy To Clipboard**. The raw packet data will be exported to the clipboard in ASCII format, each packet on a new line, with a space after each byte.

The formatting of the data is:

- Packet ID (four bytes, least significant byte first)
- Time-stamp (four bytes, least significant byte first)
- Packet length (one byte)
- Packet data (transmission order)

Approximately 21000 bytes of packet information can be exported at one time.



ZENA™ WIRELESS NETWORK ANALYZER USER'S GUIDE

Chapter 4. MiWiTM Wireless Networking Protocol Tools

4.1 INTRODUCTION

This chapter describes how to use the MiWi protocol tools provided by the ZENA Wireless Network Analyzer. Both basic and advance monitoring techniques are demonstrated.

4.2 MICROCHIP STACK CONFIGURATION TOOL

Microchip provides a freely available Stack as part of application note, *AN1066*, *"MiWi™ Wireless Networking Protocol Stack"*. The application note and source code are available for download from the Microchip Web site (www.microchip.com). After you have reviewed the application note and studied the demonstration projects, you will be ready to start your own MiWi protocol application.

The ZENA analyzer will greatly assist you with configuring the Microchip Stack by automatically generating a portion of the source code for your MiWi protocol application. Be sure to refer to *AN1066, "MiWi™ Wireless Networking Protocol Stack"* for details about each MiWi protocol configuration option. Select <u>*MiWi Tools>Stack Configuration*</u> from the main ZENA Stack Configuration window. The ZENA[™] Stack Configuration - MiWi[™] Protocol window will be displayed. Using the tabbed dialog, you can select all of the options required for your MiWi protocol application. The ZENA software will automatically enable and disable certain options depending on the selections you have made.

4.2.1 Specifying MiWi[™] Protocol Device Information

Select the MiWi Device tab.

MWiDevice Transceiver Security NWK/	
MAC Address	IEEE Device Type
Radix ⓒ <u>H</u> ex ○ <u>D</u> ecimal	© <u>B</u> FD
Receive Network Address From Coordinate	Transceiver Power
Coordinator Capable	Power Source
 Cluster Sockets EUI Address Search 	Battery Power
	P t.
	Peer-to-peer Peer-to-peer Capa <u>b</u> le
	Peer-to-peer Soc <u>k</u> ets Peer-to-peer Only
	ROCHIP

FIGURE 4-1: ZENA[™] STACK CONFIGURATION - MiWi[™] PROTOCOL WINDOW, MiWi DEVICE TAB

Using this window, you can configure the following items:

Configuration	Option Description
MAC Address	Each and every MiWi protocol device must have its own, unique MAC address. The Microchip OUI is provided as a default for development purposes only. For additional information, see <i>AN1066, "MiWi™ Wireless Networking Protocol Stack</i> ".
Receive Network Address From Coordinator	MiWi protocol devices must always receive their network address from their parent.
Coordinator Capable	If your FFD is capable of becoming a coordinator, select this option. This option is not available for RFDs.
Cluster Sockets	Select this option if your application will support cluster sockets.
EUI Address Search	If your device will search for another device based on that device's MAC address, select this option.
IEEE Device Type	Select whether your application is a Full Function Device (FFD) or a Reduced Function Device (RFD).
Transceiver Power	How the transceiver is powered. This is selected automatically based on the IEEE device type.
Power Source	Select your application's power source.
Peer-to-peer Capable	Select this option if your application will be capable of peer-to-peer communication. ⁽¹⁾
Peer-to-peer Sockets	Select this option if your application will add support to receive and process peer-to-peer socket requests (coordinators only). ⁽¹⁾
Peer-to-peer Only	Select this option to limit the device to peer-to-peer communication only. ⁽¹⁾

TABLE 4-1: MIWI™ PROTOCOL DEVICE CONFIGURATION SELECTION

Note 1: May not be supported in this release.

4.2.2 Specifying Transceiver Information

Select the **Transceiver** tab.

FIGURE 4-2: ZENA[™] STACK CONFIGURATION - MiWi[™] PROTOCOL WINDOW, TRANSCEIVER TAB

Frequency Band Microchip MRF24J40 2.4 GHZ Output Power 0.00 dBm • 0.00 dBm • Pin Assignments • • PICDEM(TM) Z Demo Board • • Explorer 16 Demo Board • • Custom Hardware Demo Board Defaults CS LATCO Y RESETn LATC2 Y INT requires INTO on RB0 Transceiver requires SPI1 Ensure that each selected pin exists on the target device. The application code is responsible for configuring each pin for correct digital operation. Refer to the demo applications.	Allowed Channels
---	------------------

Using this window, you can configure the following items:

Configuration	Option Description
Transceiver	Select one of the transceivers supported by the Stack.
Frequency Band	This combo box shows the various available frequency bands of the selected transceiver. If the transceiver supports only one frequency band, that frequency will be displayed and the combo box will be disabled.
Output Power	Selects the initial output power of the transceiver.
Pin Assignments ⁽¹⁾	The Stack requires certain I/O pins to interface to the transceiver. If you are using the PICDEM [™] Z or Explorer 16 demo board, select that option to automatically configure the Stack for that board. If you are using custom hardware, select the "Custom Hardware" radio button and select the correct I/O pins for the indicated signals. These options will change based on the "Target Device Family" selected on the PIC tab.
Demo Board Defaults	Click this button to set the signals to the I/O pins used by the PICDEM Z and Explorer 16 demo boards.
Allowed Channels	This area shows the channels that are supported by the selected frequency band. Selecting channels here will generate a label that can be used to specify the allowed channels for network formation and network discovery. Click Clear All to clear all channels, and click Select All to select all channels. Each channel can also be selected or cleared individually by selecting the checkbox that precedes the channel number.

TABLE 4-2: MiWi™ PROTOCOL TRANSCEIVER CONFIGURATION SELECTION

Note 1: Ensure the pin exists on the target device. The application code is responsible for configuring the pin as a digital input or output as appropriate.

4.2.3 Specifying Security Information

Select the **Security** tab.

FIGURE 4-3: ZENA[™] STACK CONFIGURATION - MiWi[™] PROTOCOL WINDOW, SECURITY TAB

	A(TM) Stack Configuration - MiWi(TM) Protocol
	Security Capable
	Security Key (Hex) Sequence Number 00 00 00 00 00 00 00 00 00 00 00 00 00
L	Security Level
	<u>G</u> enerate Files

Using this window, you can configure the following items:

TABLE 4-3: MiWi™ PROTOCOL SECURITY CONFIGURATION SELECTION

Configuration	Option Description
Security Capable	Only "Residential" mode is currently supported by the Stack.
Security Key	If the network key is known, enter it here with the "Sequence Number".
Security Level	Select the IEEE "Security Level" of how the packets will be encrypted and decrypted.

4.2.4 Specifying NWK and MAC Layer Information

Select the NWK/MAC tab.

FIGURE 4-4: ZENA™ STACK CONFIGURATION - MiWi™ PROTOCOL WINDOW, NWK/MAC TAB

MWi Device Transceiver Security NWK/	MAC PIC
Message Buffers Transmit Bufer Size (bytes) Receive Buffer Size (bytes)	40 40
Timeouts Network Discovery Timeout (seconds) Open Cluster Socket Timeout (seconds)	0.5
Indirect Buffer Management Indirect Buffer Size (bytes) Indirect Buffer Timeout (seconds)	1.0
Data Request Rate (seconds) Network Table Size Maximum Message Hops	0.5 10 4 •
<u>G</u> enerate	Files

This tab is used to configure the NWK (Network) and MAC (Medium Access Controller) Stack layers. Many options on this tab are enabled or disabled based on the "MiWi Device Type" specified on the **MiWi Device** tab.

Many of these options have direct correlation to the amount of RAM required by the application. See Table 4-4 for NWK and MAC option selections.

Configuration	Option Description
Transmit Buffer Size (bytes)	Enter the number of bytes for the largest transmitted message. The largest possible message is 127 bytes.
Receive Buffer Size (bytes)	Enter the number of bytes for the largest received message. The largest possible message is 127 bytes.
Network Discovery Timeout (seconds)	Enter the length of time the application will scan each channel in search of networks to join.
Open Cluster Socket Timeout (seconds)	Enter the length of time the application will wait for a socket confirmation from the PAN coordinator.
Indirect Buffer Size (bytes)	FFDs only. Enter the number of bytes reserved for buffering messages for child devices.
Indirect Buffer Timeout (seconds)	FFDs only. Enter the length of time that the device will buffer a message for a child before discarding it.
Data Request Rate (seconds)	RDFs only. Enter the frequency at which the device will request data from its parent.
Network Table Size	The network table is used to store information about other devices on the network. The table must be large enough to hold one entry for each of the device's children and for any nodes the device communicates with either directly or indirectly.
Maximum Message Hops	Enter the maximum number of hops a message can travel.

TABLE 4-4: MiWi™ PROTOCOL NWK/MAC CONFIGURATION SELECTION

4.2.5 Specifying PIC MCU Information

Select the **PIC** tab.

FIGURE 4-5: ZENA™ STACK CONFIGURATION - MiWi™ PROTOCOL WINDOW, PIC TAB

 ZENA(TM) Stack Configuration - MiWi(TM) Protocol
Target Device Family PIC18F
Speed Settings Clock Frequency (Hz) 16000000
✓ Output stack messages to UART1
UART Baud Rate 19200
S S
<u>G</u> enerate Files

This tab is used to configure basic PIC MCU options.

TABLE 4-5: MiWi™ PROTOCOL PIC[®] CONFIGURATION SELECTION

Configuration	Option Description
Target Device Family	Select the device family of the application's target processor.
Clock Frequency (Hz)	Specify the input clock frequency to the PIC MCU in Hertz. It is important that this value be accurate as all internal MiWi protocol timing will be based off of this value.
Output stack messages to UART1	This option is targeted for use with either the PICDEM [™] Z or Explorer 16 demo board. If you want Stack operation messages to be sent to the UART so they can be displayed on a terminal, select this option and select the desired baud rate.

4.2.6 Generating the Configuration Files

When all of the options on all of the tabs are set appropriately, generate the Stack configuration file by clicking **Generate Files**. The ZENA Wireless Network Analyzer will first perform a validity check to ensure that all required fields have appropriate values and all protocol-specific ranges are met.

If the validity check passes, the ZENA analyzer will prompt for an output directory for the configuration file, MiWiDefs.h. This file has a time and date stamp included in the file.

4.3 BASIC NETWORK MONITORING

Basic monitoring of a MiWi protocol network is nearly identical to that of a ZigBee protocol network. Please review section **Section 3.3** "**Basic Network Monitoring**". This section will focus on the differences between the two protocols.

Select <u>MiWi Tools> Network Traffic Monitor</u> to perform real-time network monitoring or packet analysis of a MiWi protocol network. The fundamental MiWi Network Monitor window is nearly identical to the ZigBee Network Monitor window.

MiWi protocol beacons have a slightly different format from ZigBee protocol beacons, as shown in this sequence of a device joining a network.

FIGURE 4-6: MIWITM PROTOCOL ASSOCIATION REQUEST AND RESPONSE	
🔤 ZENA(TM) Packet Sniffer - MiWi(TM) Protocol	
	•
Frame Time(us) Len MAC Frame Control Seq Dest Dest Beaton FCS +3465584 Type Sec Pend ACK IPAN Addr Request RSSI CMC 00022 =72222496 10 KM N N 0.055C +0.4 0.4 0.5	
Frame Time(us) Len MAC Frame Control Seq Source Source Super Frame Specification GTS Specification +5696 Type Sec Pend ACK IPAN Addr BO SO CAP Batt Coord Assoc Fernit Count 00023 =72228192 16 BCN N N 0x0020 0x0000 None N N 0x0	GTS Specification PendAddr Spec Beacon Payload Assoc Pernit Count ExtAddr ShortAddr ProtID Version Coords RSS: Y N 0x0 0x0 0x1 ProtID Version Coords RSS:
Frame Time(us) Len MAC Frame Control Seq Dest Dest Source Source Address Association Request +469184 Type Sec Fend ACK IPAN Addr PAN Addr Addr PAN Addr PAN Addr PAN Addr Addr PAN <td< td=""><td>seciation Request FCS Sec RxOn Power Dev AltCoord RSSI Corr CRC N On Batt FFD Y +05 0x6B OX</td></td<>	seciation Request FCS Sec RxOn Power Dev AltCoord RSSI Corr CRC N On Batt FFD Y +05 0x6B OX
Frame Time(us) Len MAC Frame Control Seq FCS +576 Type Sec Pend ACK IPAN Num RSSI Corr CRC 000025 =72697952 5 ACK N N 0.8 mod	
Frame Time(us) Len MAC Frame Control Seq Dest Dest Source Address FCS +492544 Type Sec Pend ACK IPAN Addr Addr Addr FCS 00026 =73190496 18 N N Y 0.0020 0.0000 <td< td=""><td>FCS I Corr CRC Dx6B OK</td></td<>	FCS I Corr CRC Dx6B OK
Frame Timetus) Len MAC Frame Control Seq FCS +1008 Type Sec Pend ACK IPAN Num RSSI Corr CRC 00027 =73191504 5 ACK N N 0.0xEE -12 0.0x69 OK	
Frame Time(us) Len MAC Frame Control Seq Destination Address Source Source Address Association +6656 Type Sec Fend ACK INum PAII PAII Source Source Address Status 00028 =73138160 29 CMD N Y N 0x10 0x0020 0x0706050403020102 0x00004A31234567890 Success	ss Association Response FCS Status Address RSSI Corr CRC 567890 Success 0x0100 -12 0x68 OK
Frame Time(us) Len MAC Frame Control Seq FCS $+720$ $+720$ Type Sec Pend ACK IPAN Rum RSSI Corr CRC 000029 =731988801 5 ACK N <t< td=""><td></td></t<>	



The various portions of the message are color coded for clarity. The coloring is similar to the ZigBee protocol color coding.

Field	Color
MAC Header	White
MAC Commands and Beacons	Red
NWK Header	Lime
Message Header	Yellow
Message Data	Aqua
Security Header and Encrypted Data	Blue

TABLE 4-6: MIWI™ PROTOCOL PACKET SNIFFER COLOR CODING

The MiWi protocol filter options are slightly different from the ZigBee protocol filter options. Filter operation is identical.

4.4 ADVANCED NETWORK MONITORING

Since both the ZigBee protocol and the MiWi protocol are both based on IEEE 802.15.4, the Network Configuration Display window operates identically for both protocols. Refer to **Section 3.4 "Advanced Network Monitoring and Analysis**".

Secure MiWi protocol packets appear as shown in Figure 4-7.

When these packets are decrypted using the correct security key and security level, the packets appear as shown in Figure 4-8.

FIGURE 4-7: SECURE MIWITM PROTOCOL PACKETS	
ZENA(TM) Packet Sniffer - MiWi(TM) Protocol	
MAC Frame Control Seq Dest Source FCs rpe Sec Pani Addr Addr Addr Data Request RSSI Corr CRC fD N Y Y 0xcE 0xcB6FE 0x0000 0x0001 410 410 0x69 0K	•
MAC Frame Control Seq FCS Jpe Sec Pend ACK IPAN Num RSSI Corr CRC ZK N Y N N 0xCE +04 0xE 66 0K	
MAC Frame Control Seq Dest Source House Best Source Source Seq Frame Counter Source Address vpe Sec Pend Addr Addr Addr Addr Source Source Seq Frame Counter Source Address vpe Sec Fend Addr Addr Addr N	Source Address Key sll Encrypted Data 0x00004Å31234567892 0x00 0x22 0x82 0x6E +
MAC Frame Control Seq FCS JPE Sec Pend ACK IPAN Num RSSI Corr CRC ZK N N N N 0x44 +10 0x64 ACK	
MAC Frame Control Seq Dest Source Hops Frame Control Dest Source Source Source Key Encrypted Data vpe Sec Pail Addr PAII Addr Addr PAII PAII Num PAII PAII PAII Addr PAII PAII Num PAII PAII PAIII PAIIII PAIIII PAIIII PAIIII PAIIII PAIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Ince Address Key Encrypted Data FC 811 0xAA 0xA8 0x07 RSSI C 4A31234567891 0x00 0x7E 0x2C 0x9C +10 0:
MAC Frame Control Seq FCS JPE Sec Pend ACK IPM RSSI Corr CRC ZK N N N 0xcf +04 0xcf 40 K	
MAC Frame Control Seq Dest Source FCS ype Sec Pend Addr Addr Addr Addr Data Request RSSI Corr CRC 4D N Y N Y 0x2000 0x0000 0x0000 0x0001 0x6001	
MAC Frame Control Seq FCS ype Sec Pend ACK IPAN Num RSSI Corr CRC XK N Y N N ∩×D0 +14 0×66 0K	

© 2007 Microchip Technology Inc.

ZENA[™] Wireless Network Analyzer User's Guide

DECRYPTED OR UNSECURE MIWI'M PROTOCOL PACKETS
ZENA(TM) Packet Sniffer - MiWi(TM) Protocol
Frame Time(us) Len MAC Frame Control Seq Dest Source FCS 1 388272 Type Sec Fend ACK IPAIN Addr Addr Addr FCS 00011 =2369216 12 CMD N Y 0xCE 0xE0000 0x00001 0x60001 0x60001 40000 400001 400000 4
MAC Frame Control seq FCs Type Sec Fend ACK IPAN Num RSSI Corr CRC ACK N Y N 0xCE +04 0x66 0K
Frame Time(us) Len MAC Frame Control Seq Dest Source Hops Frame Control Dest Source Seq Report Data FCS +179184 Type Sec Pend Addr Addr Addr Addr Addr Addr Addr Addr Pall Pall Addr Pall Addr Pall Addr Pall Addr Pall Addr Pall Addr Pall Pall Addr Pall Addr<
MAC Frame Control seq FCS Type Sec Fend ACK IPAN Num RSSI Corr CRC ACK N N 0 244 +10 0x64 0K
MAC Frame Control Seq Dest Source Hops Frame Control Dest Source Source Source Source Frame Control Frame Control Dest Tage Source Source Source FCS FCS Type Sec Pend Addr Addr Addr Addr Addr PAII Type ID REST Corr CRC DATA N Y 0xCF 0xE000 0x0000 0x0001 0xU 0xU 0xE6FE 0x0001 0xE6FE 0x0001 </td
MAC Frame Control seq FCs Type Sec Fend ACK IPAN Num RSSI Corr CRC ACK N N N 0xCF +04 0x64 0K
MAC Frame Control Seq Dest Source FCS Type Sec Pend ACK IPAN Num PAII Addr Addr Data Request RSSI Corr CRC CMD N Y 0x200 0x266/EFE 0x0000 0x6001 +10 0x68 0K
MAC Frame Control seq FCS Type Sec Pend ÀCK IPÀN Num RSSI Corr CRC ÀCK N V N N ∩r≻D∩ ±∩4 ∩r≭66 ΩK



ZENA™ WIRELESS NETWORK **ANALYZER USER'S GUIDE**

Index

F

Α

Advanced Network Manitoring 29	60
Advanced Network Monitoring	
Analyzing Traffic	50
Configuration Display Window	38
Customizing Configuration	
Display Window	45
Viewing Formation	40
Viewing Traffic	44
APS Configuration Selection (ZigBee)	
Binding Support	20
Max APS ACK Frames Generated	20
Max APS Addresses	20
Max Frames From APL Layer	20
В	

Basic Network Monitoring	
--------------------------	--

С

Configuration File Generation	24
Customer Change Notification Service	4
Customer Support	5

D

Device Configuration Selection (MiWi)	
Cluster Sockets	53
Coordinator Capable	53
EUI Address Search	
IEEE Device Type	53
MAC Address	53
Peer-to-peer Capable	53
Peer-to-peer Only	53
Peer-to-peer Sockets	53
Power Source	53
Receive Network Address	
From Coordinator	53
Transceiver Power	53
Device Configuration Selection (ZigBee)	
Alternate PAN Coordinator	13
Available Power Sources	13
IEEE Device Type	13
Initial Power Source	
MAC Address	
Manufacturer Code (Hex)	
RFD Internal Data Request Rate	
Transceiver Power	
ZDO/APS/NWK/MAC	
ZigBee Device Type	13
Documentation	
Conventions	
Layout	1
Revision History	5

Four-Device Network	43
I	
Installation	
License Agreement	9
Readme File	9
ZENA Software	9
Internet Address	4
К	
Kit Contents	7
USB mini-B Cable	7
ZENA Wireless Network Analyzer	7
ZENA Wireless Network Analyzer	
CD-ROM	7

Μ

MAC Configuration Selection (ZigBee)	
Battery Life Extension Mode	22
Beacon Order	22
Channel Energy Threshold	22
Minimum Join LQI	
Receive Buffer Size	22
Superframe Order	22
Superframe Structure	22
Transaction Persistence (seconds)	22
Microchip Internet Web Site	4
Microchip Stack Configuration Tool	51
MiWi Protocol	
Information	51
MPLAB® IDE	1

Ν

NCD APS Acknowledge Path	44
NCD Association Request	41
NCD Association Response	42
NCD Beacon	41
NCD Beacon Request	40
NCD Configuration Selection (ZigBee)	
Clear All Lines	39
Clear All Message Lines	39
Clear Background	
Clear NCD	39
Select Bitmap	
Show Last Messages	39
NCD Message Path	
Network Monitoring	
Node Colors	39
NWK and MAC Layer	
Specifying	21

ZENA[™] Wireless Network Analyzer User's Guide

NWK Configuration Selection (ZigBee)	
Max Buffered Broadcast Messages	22
Max Buffered Routing Messages	22
Neighbor Table Size	22
Reserved Routing Table Entries	22
Route Discovery Table Size	22
Routing Table Size	22
NWK/MAC Configuration Selection (MiWi)	
Data Request Rate (seconds)	58
Indirect Buffer Size (bytes)	58
Indirect Buffer Timeout (seconds)	58
Maximum Message Hops	58
Network Discovery Timeout (seconds)	58
Network Table Size	58
Open Cluster Socket Timeout (seconds)	58
Receive Buffer Size (bytes)	58
Transmit Buffer Size (bytes)	58

P

Packet	
Exporting Data	50
Filter Use	
Hiding and Unhiding	
Playback	
Playback Selection (ZigBee)	
2 sec	33
Instant	33
Manual	33
x0.01	33
x0.1	33
x1	33
x10	33
x100	33
Packet Sniffer Color Coding (MiWi)	
MAC Commands and Beacons	
MAC Header	
Message Data	
Message Header	62
NWK Header	
Security Header and Encrypted Data	62
Packet Sniffer Color Coding (ZigBee)	
APS Header	
APS Payload/Decoding	
MAC Commands and Beacons	-
MAC Header	
NWK Commands	
NWK Header	
Security Header and Encrypted Data	
Unknown	28
PIC Configuration Selection (MiWi)	
Clock Frequency (Hz)	
Output stack messages to UART1	
Target Device Family	59
PIC Configuration Selection (ZigBee)	
Build Target	24
Clock Frequency (Hz)	
Heap Size (banks)	
MAC Address Stored Externally	
NCS	24

Program Memory	24
Serial EEPROM	24
SPI	
SPI Serial EEPROM	24
Stack Size (banks)	
Target Device	
UART Baud Rate	
Verify Writes	24
PIC MCU	
Specifying	23
Previously Captured Data	-
Analyzing	33
Profile and Endpoint	
Specifying	15
Profile/Endpoints Configuration	-
Selection (ZigBee)	
Device	16
Endpoints	
Profile Header File	
Protocol Device Configuration Selection (ZigBee)	
Key Present in All Devices on	
the Network	. 18
Network Key Present	
Security Capable	
Security Mode	
Trust Center	
Trust Center Address	
R	
Real-Time Network Monitoring	26
Real-Time Network Monitoring Configuration	
Selection (ZigBee)	

Selection (ZigBee)	
Auto Scroll	
Channel	
Clear Messages on Start	
Ignore Invalid Packets	
Real-Time Display	
Recommended Reading	3
AN1066, MiWi Wireless Networking	
Protocol Stack	3
AN965, Microchip Stack for the ZigBee	
Protocol	
IEEE 802.15.4 Specification	
Microchip 8-Bit Microcontroller Solutions	3
PIC MCU Data Sheets, Family	
Reference Manuals	
PICDEM Z Demonstration Kit User's Guide	ə 3
Readme for ZENA Wireless	
Network Analyzer	3
ZigBee Protocol Specification	3

S

Security Configuration Selection (MiWi)	
Security Capable	
Security Key	
Security Level	
Stack Configuration Tool	11

Т

•	
Time-Stamps	33
Transceiver	
Specifying	14
Transceiver Configuration Selection (MiWi)	
Allowed Channels	55
Demo Board Defaults	55
Frequency Band	
Output Power	55
Pin Assignments	55
Transceiver	55
Transceiver Configuration Selection (ZigBee)	
Allow Shared SPI	
Allowed Channels	
Frequency Band	14
Output Power	14
PICDEM Z Pins	14
Pin Assignments	14
Transceiver	14
Two-Device Network	42
U	
USB mini-B Cable	25

۷

Verboseness Level Configuration Selection (ZigBee)
Condensed
Numeric
Verbose
W
WWW Address
Z
ZDO and APS Layer
Specifying 19
ZDO Configuration Selection (ZigBee)
Include Optional Node Management

Include Optional Service Discovery

ZENA Analyzer

ZigBee Protocol Device

Services......20

Support End Device Binding 20

Overview7

Specifying 12



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://support.microchip.com 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

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

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

Kokomo Kokomo, IN Tel: 765-864-8360 Fax: 765-864-8387

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 Habour 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: 86-10-8528-2100 Fax: 86-10-8528-2104

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

China - Fuzhou Tel: 86-591-8750-3506 Fax: 86-591-8750-3521

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

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 - Shunde Tel: 86-757-2839-5507 Fax: 86-757-2839-5571

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

China - Xian Tel: 86-29-8833-7250 Fax: 86-29-8833-7256

ASIA/PACIFIC

India - Bangalore Tel: 91-80-4182-8400 Fax: 91-80-4182-8422

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

Korea - Gumi Tel: 82-54-473-4301 Fax: 82-54-473-4302

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

Malaysia - Penang Tel: 60-4-646-8870 Fax: 60-4-646-5086

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: 886-3-572-9526 Fax: 886-3-572-6459

Taiwan - Kaohsiung Tel: 886-7-536-4818 Fax: 886-7-536-4803

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