ZENA™ Wireless Network Analyzer User's Guide

© 2008 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in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates.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.

Trademarks

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

FilterLab, Linear Active Thermistor, 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, dsSPEAK, ECAN, ECONOMONITOR, FanSense, In-Circuit Serial Programming, ICSP, ICEPIC, Mindi, MiWi, MPASM, MPLAB Certified logo, MPLIB, MPLINK, mTouch, PICkit, PICDEM, PICDEM.net, PICtail, PIC^{32} logo, PowerCal, PowerInfo, PowerMate, PowerTool, REAL ICE, rfLAB, Select Mode, Total Endurance, 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.

© 2008, Microchip Technology Incorporated, Printed in the U.S.A., All Rights Reserved.

Printed on recycled paper.

QUALITY MANAGEMENT SYSTEM
CERTIFIED BY DNV
ISO/TS 16949:2002

Microchip received ISO/TS-16949:2002 certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona; Gresham, Oregon and design centers in California and India. The Company's quality system processes and procedures are for its PIC® MCUs and dsPIC® DSCs, KEELOQ® code hopping devices, Serial EEPROMs, microperipherals, nonvolatile memory and analog products. In addition, Microchip's quality system for the design and manufacture of development systems is ISO 9001:2000 certified.

Table of Contents

Preface **1**

Chapter 1. ZENA™ Wireless Network Analyzer Overview

1.1 Introduction 7
1.2 ZENA™ Wireless Network Analyzer Kit Contents 7
1.3 ZENA™ Analyzer Overview 7

Chapter 2. Getting Started

2.1 Introduction 9
2.2 Installing ZENA™ analyzer software 9

Chapter 3. ZigBee™ Protocol Tools

3.1 Introduction 11
3.2 Microchip Stack Configuration Tool 11
3.3 Basic Network Monitoring 28
3.4 Advanced Network Monitoring and Analysis 41

Chapter 4. MiWi™ Wireless Networking Protocol Tools

4.1 Introduction 55
4.2 Microchip Stack Configuration Tool 55
4.3 Basic Network Monitoring 64
4.4 Advanced Network Monitoring 66

Chapter 5. MiWi™ P2P Wireless Networking Protocol Tools

5.1 Introduction 69
5.2 MiWi™ P2P Stack Configuration Tool 69
5.3 Basic Network Monitoring 76
5.4 Advanced Network Monitoring 78

Index **81**

Worldwide Sales and Service **84**

© 2008 Microchip Technology Inc.

NOTES:

© 2008 Microchip Technology Inc.

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 "DSXXXXXA", 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.

© 2008 Microchip Technology Inc.

- **Chapter 5. MiWi™ P2P Wireless Networking Protocol Tools** - This chapter describes how to use the MiWi P2P protocol tools provided with the ZENA analyzer.

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	*File>Save*
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>
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	*`file`*`.o`, where *`file`* can be any valid filename
Square brackets [ ]	Optional arguments	`mcc18 [options]` *`file`* `[options]`
Curly brackets and pipe character: { | }	Choice of mutually exclusive arguments; an OR selection	`errorlevel {0|1}`
Ellipses...	Replaces repeated text	`var_name [, var_name...]`
	Represents code supplied by user	`void main (void) { ... }`

© 2008 Microchip Technology Inc.

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.

AN1232, Microchip ZigBee-2006 Residential Stack Protocol (DS01232)

This application note assists designers who are interested in adopting the ZigBee protocol in their applications.

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® 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.

© 2008 Microchip Technology Inc.

CUSTOMER SUPPORT

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Field Application Engineer (FAE)
- Technical Support

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.

Revision C (September 2008)

- Updated APO and ZDO screenshots and information.
- Updated existing ZigBee protocol Stack information.
- Added **Chapter 5. “MiWi™ P2P Wireless Networking Protocol Tools”**.

NOTES:

© 2008 Microchip Technology Inc.

Chapter 1. ZENA™ 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

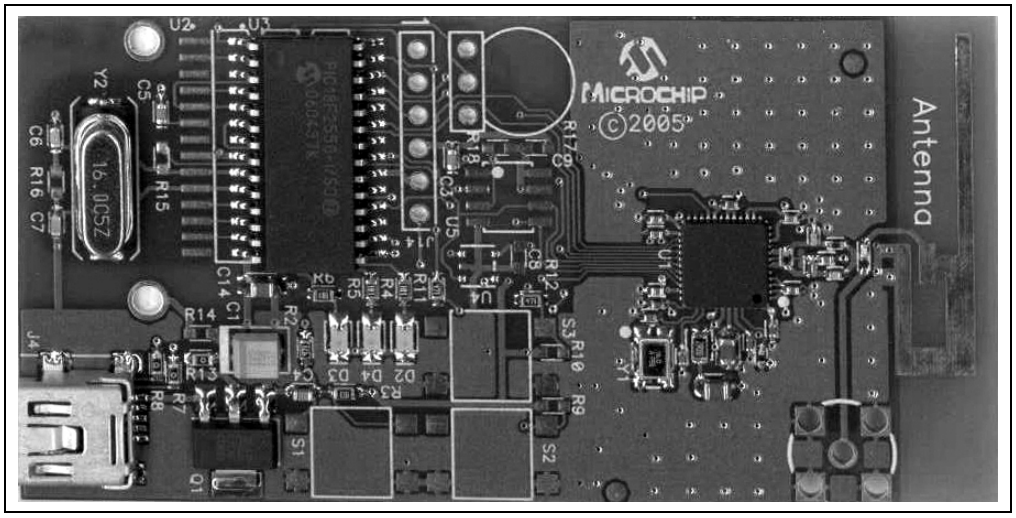
The ZENA Wireless Network Analyzer kit contains the following items:

- 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.

© 2008 Microchip Technology Inc.

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:

© 2008 Microchip Technology Inc.

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

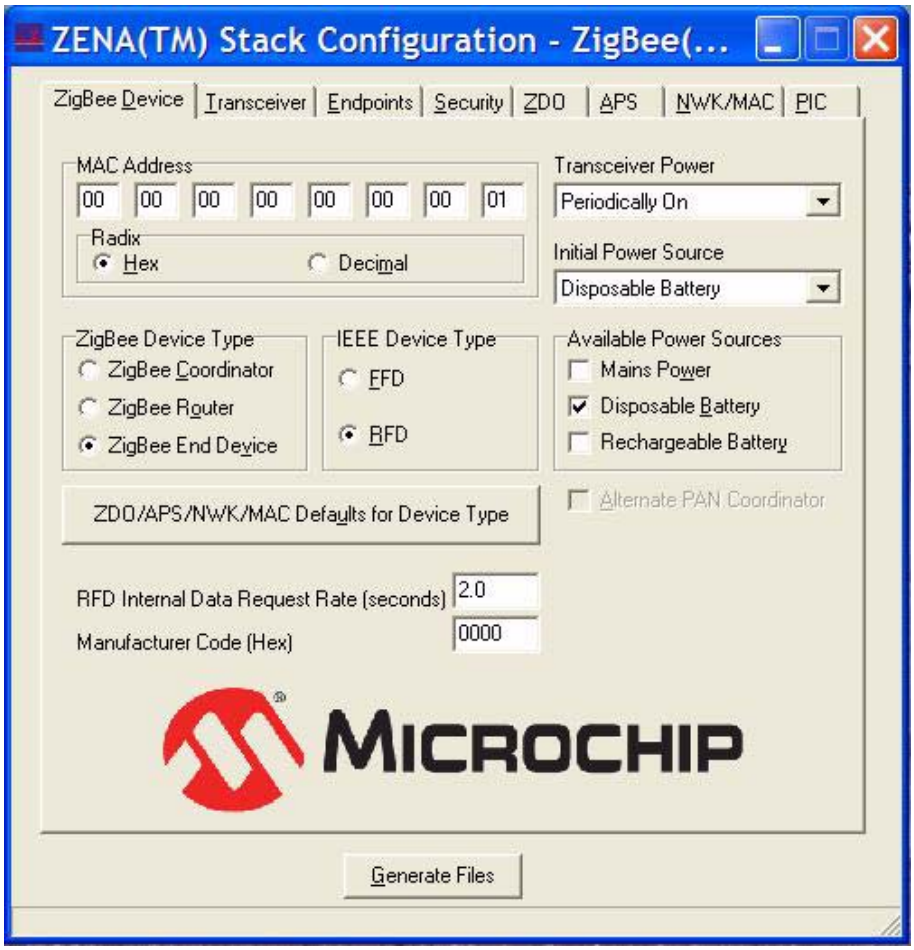
Microchip provides a freely available Stack as part of application note, *AN965, "Microchip Stack for the ZigBee™ Protocol"*. The application note and source code are available for download from the Microchip web site (www.microchip.com). After you have reviewed the application note and studied the demonstration 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 *ZigBee™ Tools>Stack Configuration* 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



© 2008 Microchip Technology Inc.

Using this window, you can configure the following items:

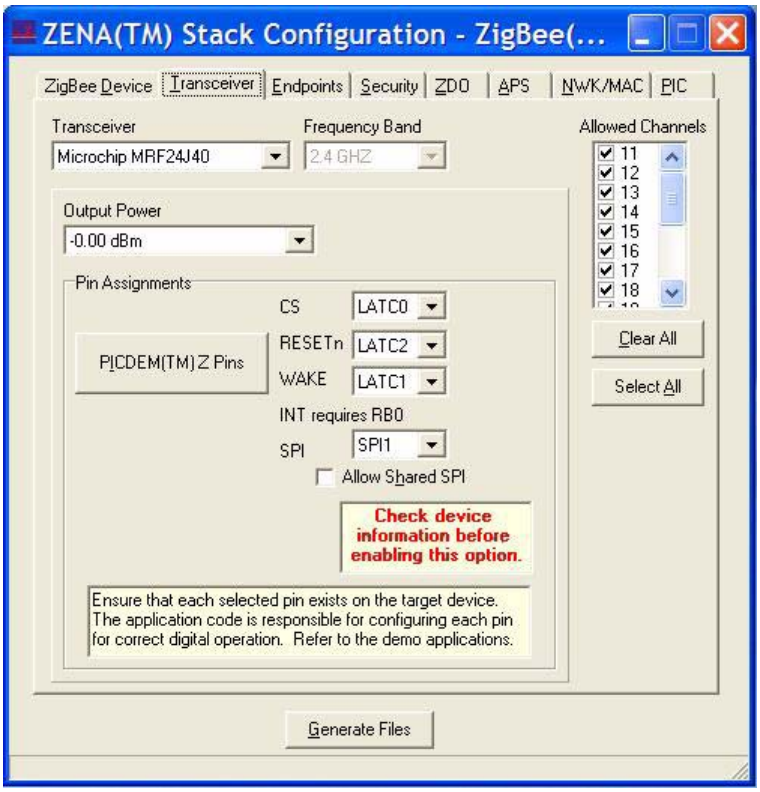
TABLE 3-1: ZigBee™ PROTOCOL DEVICE CONFIGURATION SELECTION

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 *AN1232, "Microchip ZigBee-2006 Residential Stack Protocol"* 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



Using this window, you can configure the following items:

TABLE 3-2: ZigBee™ PROTOCOL TRANSCEIVER CONFIGURATION SELECTION

Configuration	Option Description
Transceiver	Selects 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)	This panel shows the required pins for the selected transceiver. The Stack allows you to change these pin connections to application-specific port pins.
PICDEM™ Z Pins	Click this button to restore the pin assignments to the connections used by the PICDEM Z Demonstration Board.
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 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.
Allow Shared SPI	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.

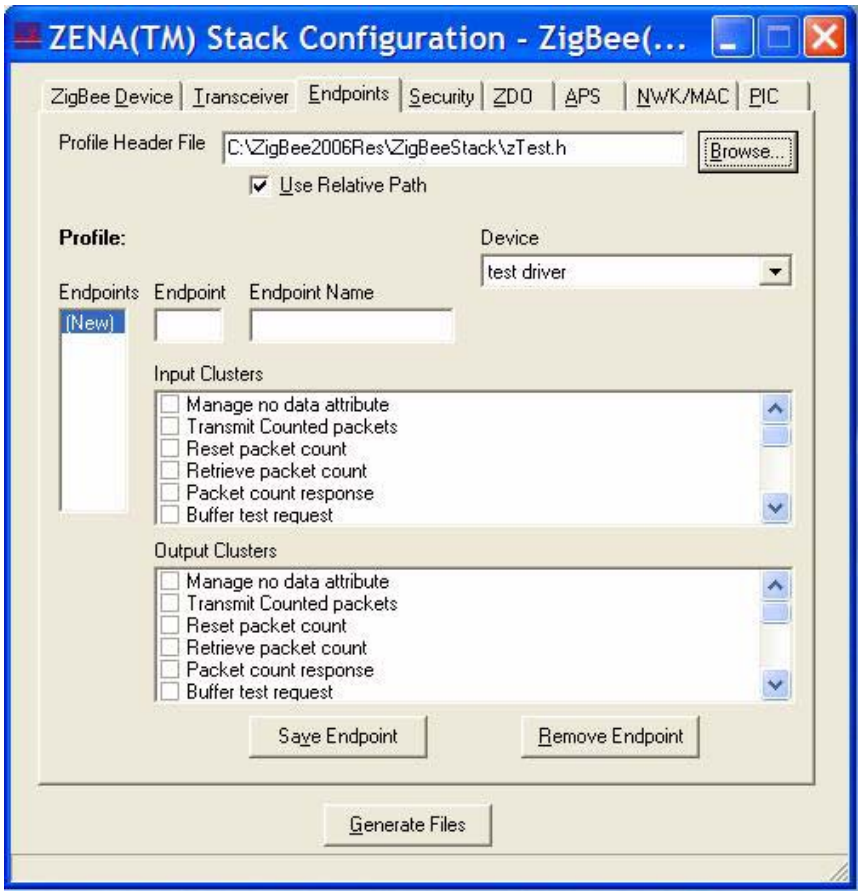
Note 1: Ensure the pin exists on the target device. The application code is responsible for configuring the pin as a digital input or output as appropriate.

© 2008 Microchip Technology Inc.

3.2.3 Specifying Profile and Endpoint Information

Select the **Endpoints** tab.

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



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.

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

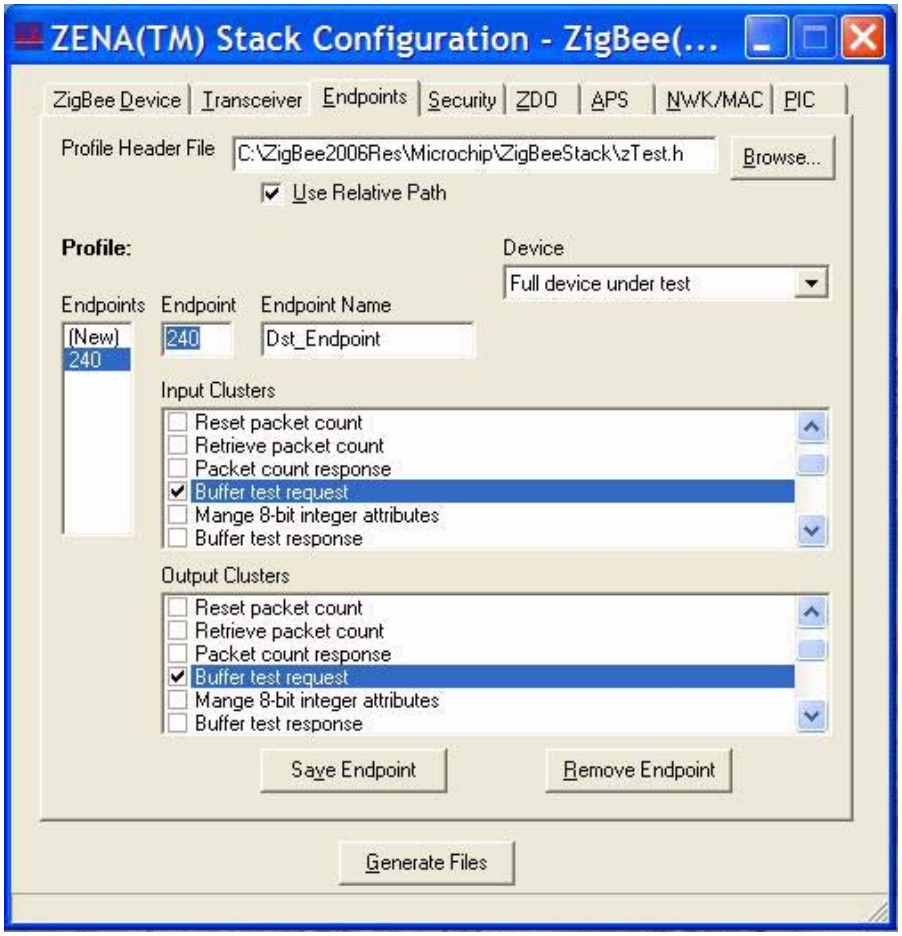
Configuration	Option Description
Profile Header File	Click **Browse** to browse to and select the header file for the application's profile. This file has profile information in a specific format which the ZENA™ analyzer uses to configure many items, including: - Profile name - The list of devices supported 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: 1. Enter the endpoint's numerical value (1-240) in the "Endpoint" edit box. 2. In the "Endpoint Name" edit box, enter a valid C language label for that endpoint. 3. Select all of the input and output clusters that are supported by that endpoint under "Input Clusters" and "Output Clusters". 4. Click **Save Endpoint** to save the endpoint. The endpoint number will be added to the "Endpoints" list box. To define another endpoint: 1. Click **New** in the "Endpoints" list box. All of the endpoint information will be cleared. 2. 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 number in the "Endpoints" list box and click **Remove Endpoint**.

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.

© 2008 Microchip Technology Inc.

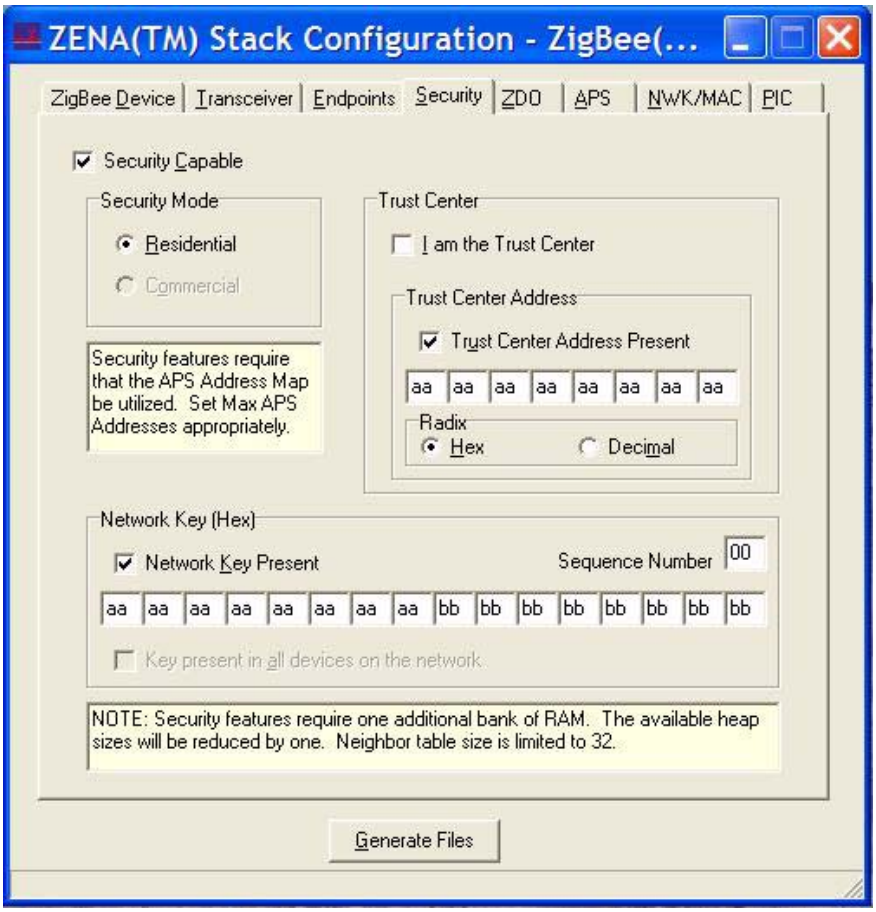
FIGURE 3-4: ENDPOINT SPECIFICATION



3.2.4 Specifying Security Information

Select the **Security** tab.

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 3-10)
- The APS Address Map must be used (see Max APS Addresses in Table 3-7)

Using this window, you can configure the following items:

TABLE 3-4: ZigBee™ PROTOCOL DEVICE CONFIGURATION SELECTION

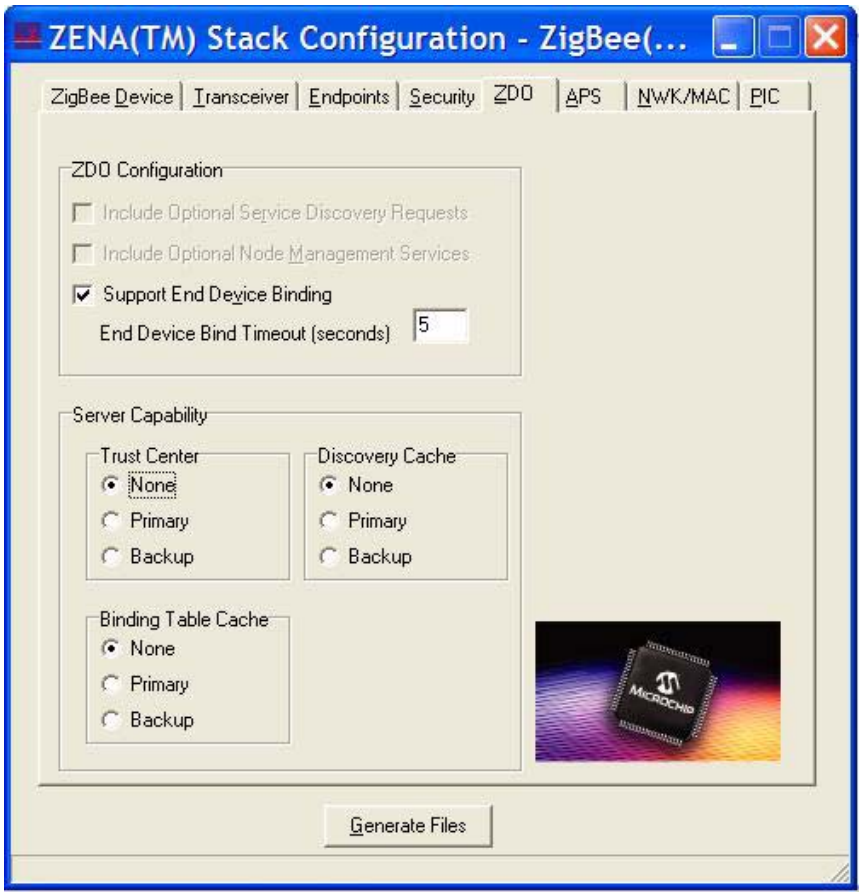
Configuration	Option Description
Security Capable	Select this option if your application will utilize security and send and receive encrypted messages.
Security Mode	Only "Residential" mode is currently supported by the Stack.
Trust Center	Select this option if this device is the trust center.
Trust 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.

© 2008 Microchip Technology Inc.

3.2.5 Specifying ZDO Layer Information

Click on the **ZDO** tab.

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



This tab is used to configure the ZDO (ZigBee Device Object) Layer of the Stack. Many options on this tab are enabled or disabled based on the “ZigBee Device Type” that is selected on the **ZigBee Device** tab.

ZigBee allows some network services to be distributed among different devices in the network. The Server Capability selection (refer to Table 3-6) is used to describe the specific additional services the device capable of providing.

TABLE 3-5: ZigBee™ PROTOCOL ZDO CONFIGURATION SELECTION

Configuration	Option Description
Include Optional Service Discovery Requests	If selected, the application will support the optional ZDO service discovery requests. *This feature is not yet supported by the Microchip Stack.*
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 3-6: ZIGBEE™ PROTOCOL ZDO SERVER CONFIGURATION SELECTION

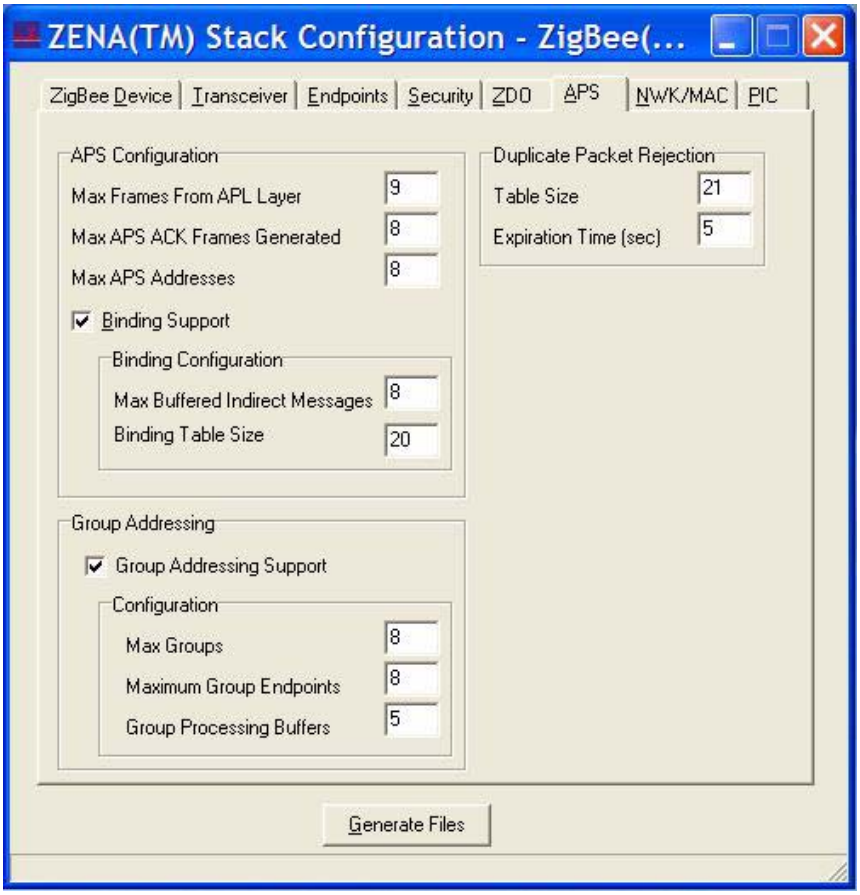
Configuration	Option Description
Trust Center	This specifies whether the device is capable of serving as a Trust Center. If yes, then indicate whether it is as a primary or a backup Trust Center. This feature is not yet fully supported by the Microchip Stack. The ZigBee Coordinator is the Trust Center within the Microchip Stack.
Binding Table Cache	This specifies whether the device is capable of serving as a Binding Table Cache i.e. a device that can store the Binding Table of other devices. This feature is not yet fully supported by the Microchip Stack. Devices can only store their own binding tables.
Discovery Cache	This specifies whether the device is capable of providing information that describes both the identity and services provided by other devices on the network. If yes, then indicate whether the device will operate as the primary or backup device, responding to discovery requests from other devices. This feature is not yet fully supported by the Microchip Stack. The Individual Routers and Coordinator may respond with service information regarding their own child devices, but not for the network as a whole.

© 2008 Microchip Technology Inc.

3.2.6 Specifying APS Layer Information

Click on the **APS** tab.

FIGURE 3-7: ZENA™ STACK CONFIGURATION WINDOW, APS TAB



This tab is used to configure the APS (Application Sub Support) Stack layer. Some options on this tab are enabled or disabled based on the “ZigBee Device Type” selected on the **ZigBee Device** tab.

Many of these options affect the amount of RAM and nonvolatile memory that is used by the application. To view the associated memory usage, hover the mouse over the appropriate edit box after the box has been enabled.

TABLE 3-7: 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 *not* 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	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.

TABLE 3-8: ZIGBEE™ PROTOCOL APS GROUP ADDRESSING SELECTION

Configuration	Option Description
Max Groups	If multicasting is supported, then the device can be a member of multiple groups. Enter the maximum number of groups that this device can be a member of.
Maximum Group Endpoints	If multicasting is supported, then for each individual group that the device is a member of, the ZigBee™ protocol allows the application layer to specify a list of endpoints that are associated with each group identifier, i.e. GroupID. Messages that are send using multicasting will be sent to all the endpoints associated with the group identifier that is used in the message's address. Enter the maximum number of endpoints that can be associated with a group identifier.
Group Processing Buffers	If multicasting is supported, then internal to the Microchip Stack are buffers that hold each group addressed message which subsequently will be directed to the associated endpoints. Enter the maximum number of messages that can be simultaneously buffered up, awaiting processing before they are sent to the appropriate endpoint.

© 2008 Microchip Technology Inc.

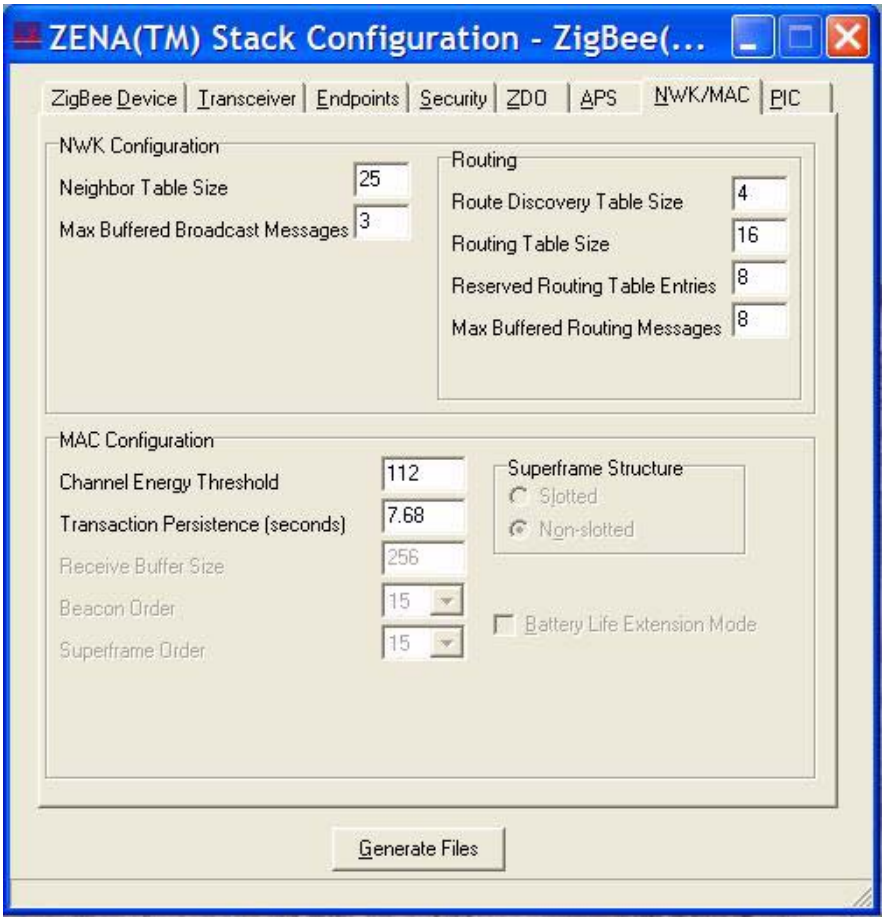
TABLE 3-9: ZIGBEE™ PROTOCOL APS DUPLICATE PACKET REJECTION SELECTION

Configuration	Option Description
Table Size	The ZigBee™ protocol allows the application layer to individually tag each packet to be transmitted with a unique identifier called a sequence number. The sequence number is used by the receiving application to distinguish among the many packets it asynchronously receives. Each device maintains a Duplicate table which contains the sequence numbers of the packets it receives. Upon receiving a new packet it compares the list of sequence numbers already stored against the new sequence number, and if there is a match, the new packet is tagged as a duplicate and is discarded. Enter the number of entries that will be maintained in the duplicate table.
Expiration Time (seconds)	Entries in the Duplicate Table are time-stamped and are kept for only a limited amount of time. After that time has elapsed the entry is marked as expired. This makes room for new entries to be added to the table, as well as allowing for the reuse of a sequence number after a certain amount of time has elapsed. Enter the time in seconds for how long any entry in the Duplicate Table will remain valid before being marked as expired.

3.2.7 Specifying NWK and MAC Layer Information

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

FIGURE 3-8: 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 3-10 and Table 3-11 for NWK and MAC option selections.

© 2008 Microchip Technology Inc.

TABLE 3-10: ZigBee™ PROTOCOL NWK CONFIGURATION SELECTION

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.

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 3-11: ZigBee™ PROTOCOL MAC CONFIGURATION SELECTION

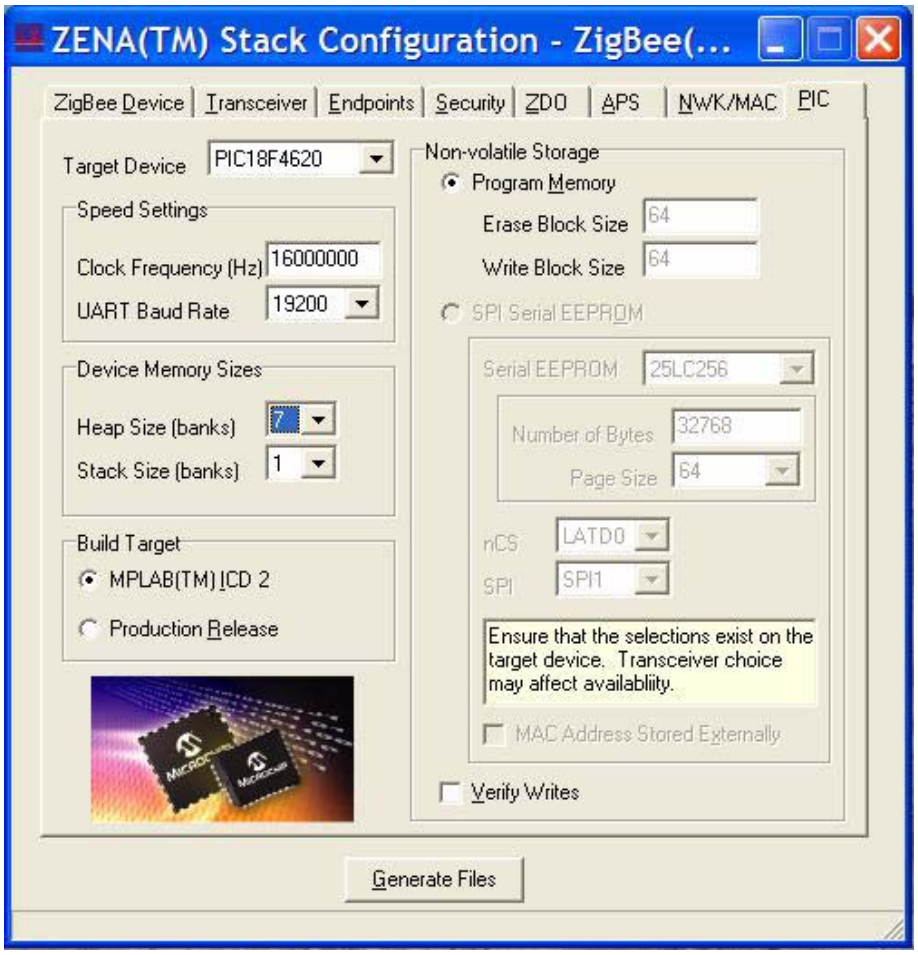
Configuration	Option Description
Channel Energy Threshold	This option is available for ZigBee™ protocol coordinators only. Enter the maximum amount of energy allowable for a channel to be selected for a new network.
Minimum Join LQI	This option is only available for devices other than ZigBee protocol 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.

3.2.8 Specifying PIC MCU Information

Select the **PIC** tab.

FIGURE 3-9: ZENA™ STACK CONFIGURATION WINDOW, PIC TAB



This tab is used to configure basic PIC MCU options (see Table 3-12).

© 2008 Microchip Technology Inc.

TABLE 3-12: ZigBee™ PROTOCOL PIC® MCU CONFIGURATION SELECTION

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 *AN965, "Microchip Stack for the ZigBee™ Protocol"* 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 provided in *AN965, "Microchip Stack for the ZigBee™ Protocol"*, 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 *AN965, "Microchip Stack for the ZigBee™ Protocol"* 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™ 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.

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.

3.2.9 Generating the Configuration Files

When all the options on all 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.

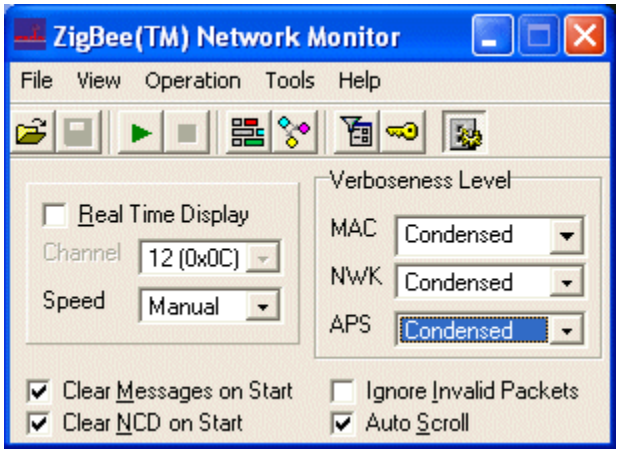
Each of these files has a time and date stamp included in the file. Refer to *AN965, "Microchip Stack for the ZigBee™ Protocol"* for more information about these files.

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 3-10: ZigBee™ PROTOCOL NETWORK MONITOR WINDOW



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 *View>Network Messages* 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 3-13: REAL-TIME NETWORK MONITOR TOOLBAR FUNCTIONS

Icon	Menu Equivalent	Function
	File>Open	Load a previously saved file for display and analysis.
	File>Save	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.
	View>Network Configuration Display	Open the Network Configuration Display window.
	Tools>Filter	Display or hide filter options.
	Tools>Security	Enable or disable secure packet decrypting.
	View>Show/Hide Settings	Display or hide the settings of the Network Monitor window.

© 2008 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 3-14: REAL-TIME NETWORK MONITORING CONFIGURATION SELECTION

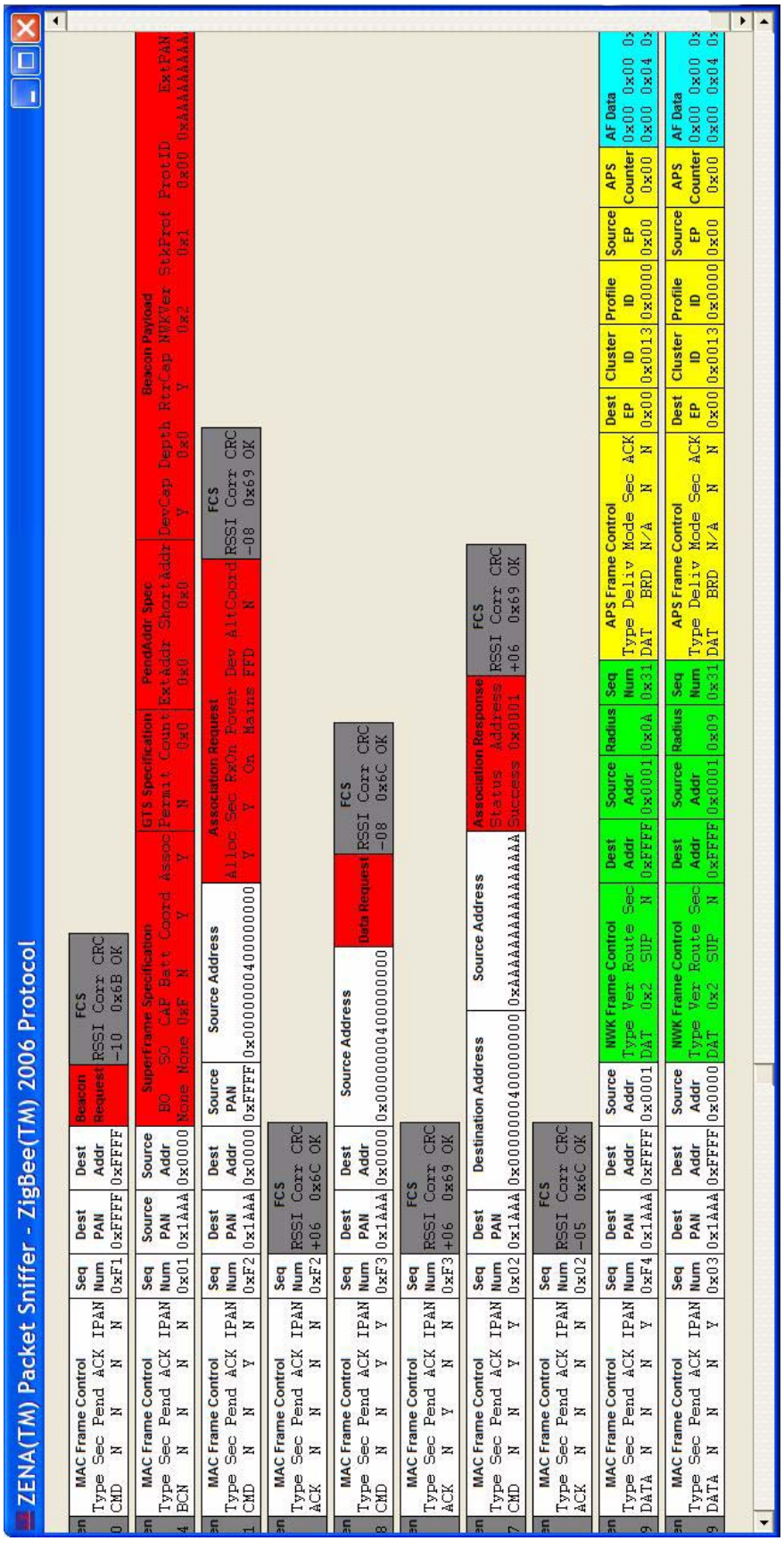
Configuration	Option Description
Real-Time Display	Select this option to display on-air messages that are received by the Network Analyzer hardware.
Channel	Select the desired channel to monitor. Note that if your application specifies more than one allowable channel to form or join a network, you may 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 *Operation>Start Sniffing/Playback* menu option to begin real-time monitoring. The received messages are then displayed on the Packet Sniffer window. Figure 3-11 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.

FIGURE 3-11: ASSOCIATION REQUEST AND RESPONSE



© 2008 Microchip Technology Inc.

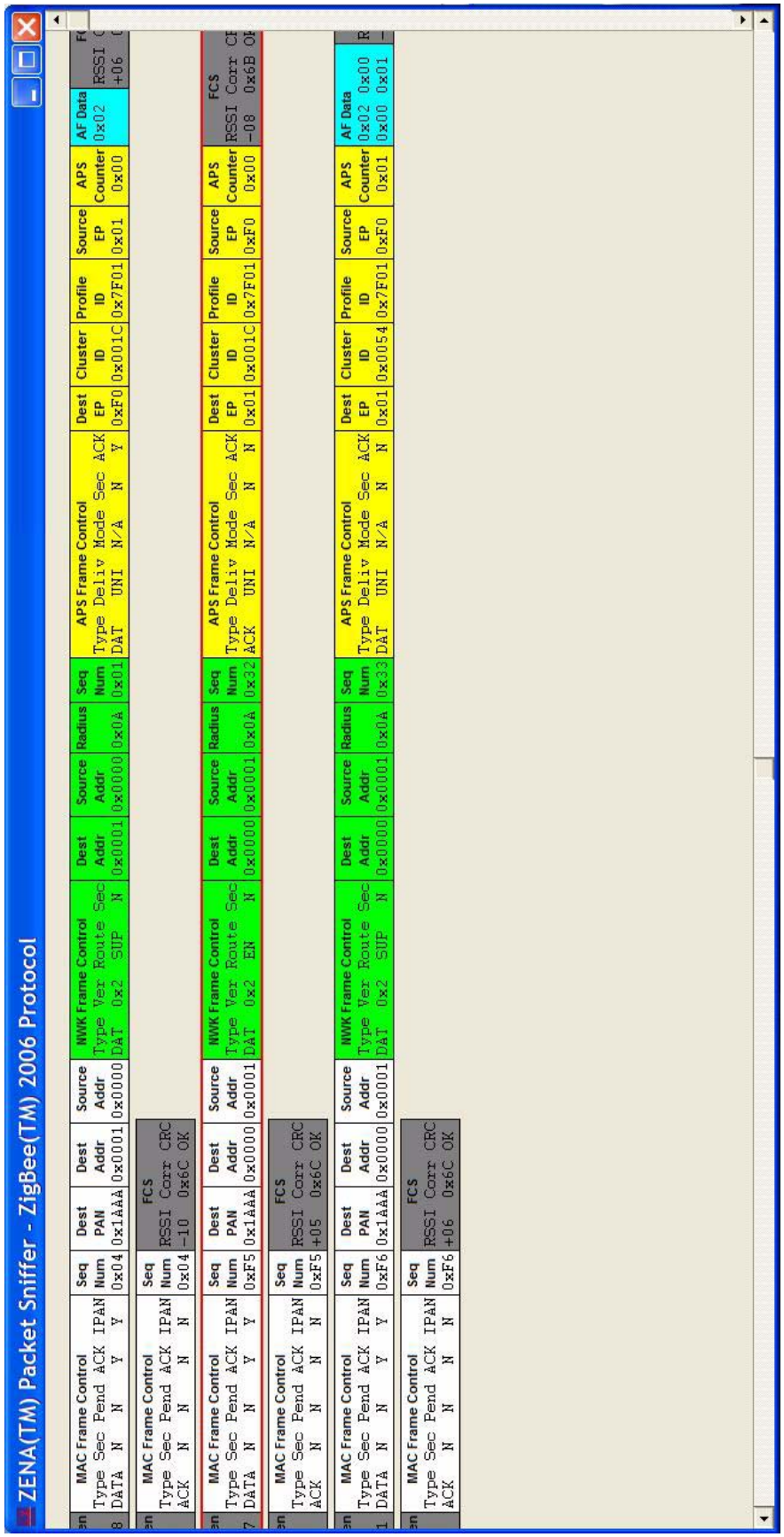
The various portions of the message are color coded for clarity.

TABLE 3-15: PACKET SNIFFER COLOR CODING

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 3-12 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.

FIGURE 3-12: APPLICATION MESSAGE WITH APS LEVEL ACKNOWLEDGE



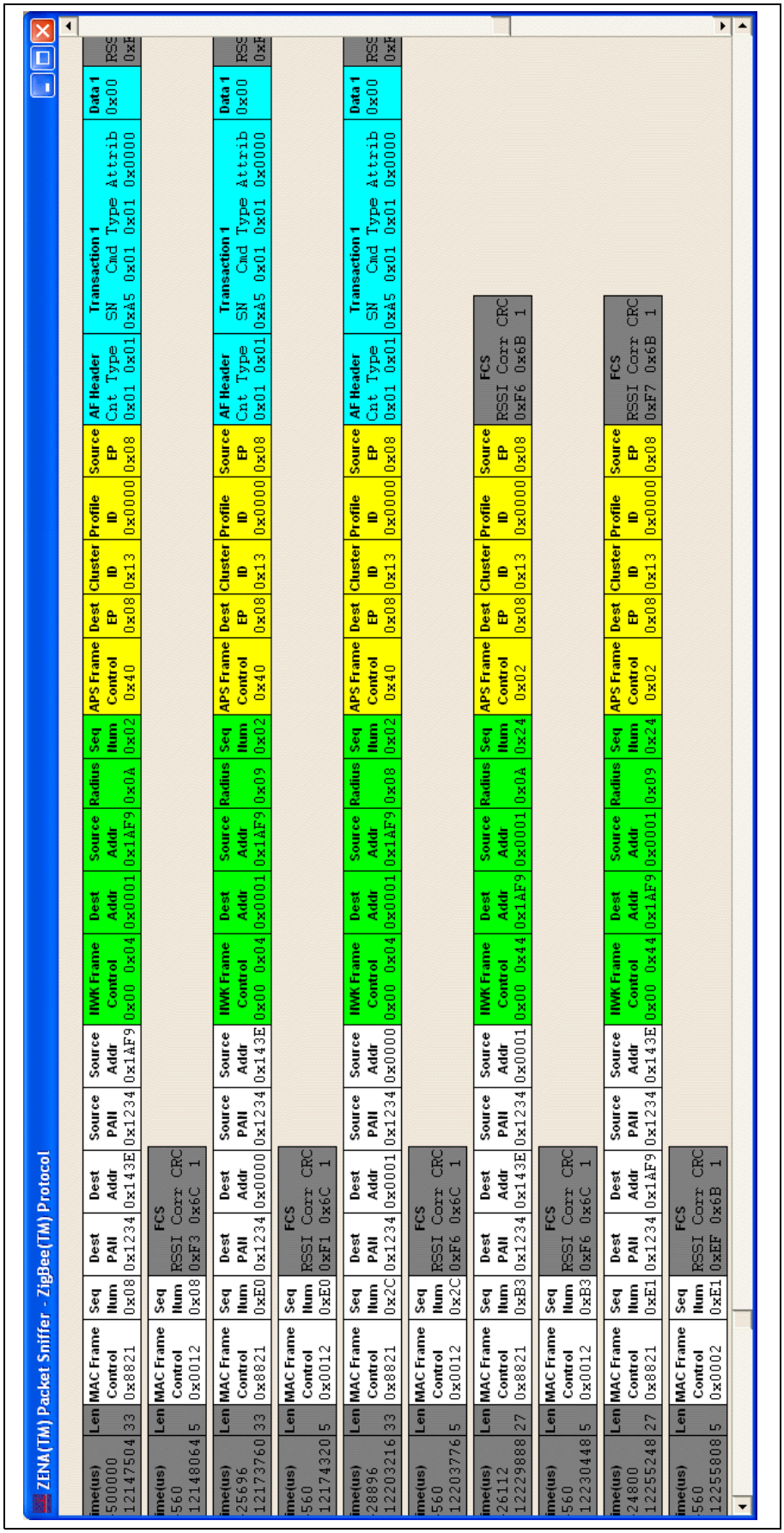
© 2008 Microchip Technology Inc.

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 3-16).

TABLE 3-16: ZigBee™ PROTOCOL VERBOSENESS LEVEL CONFIGURATION SELECTION

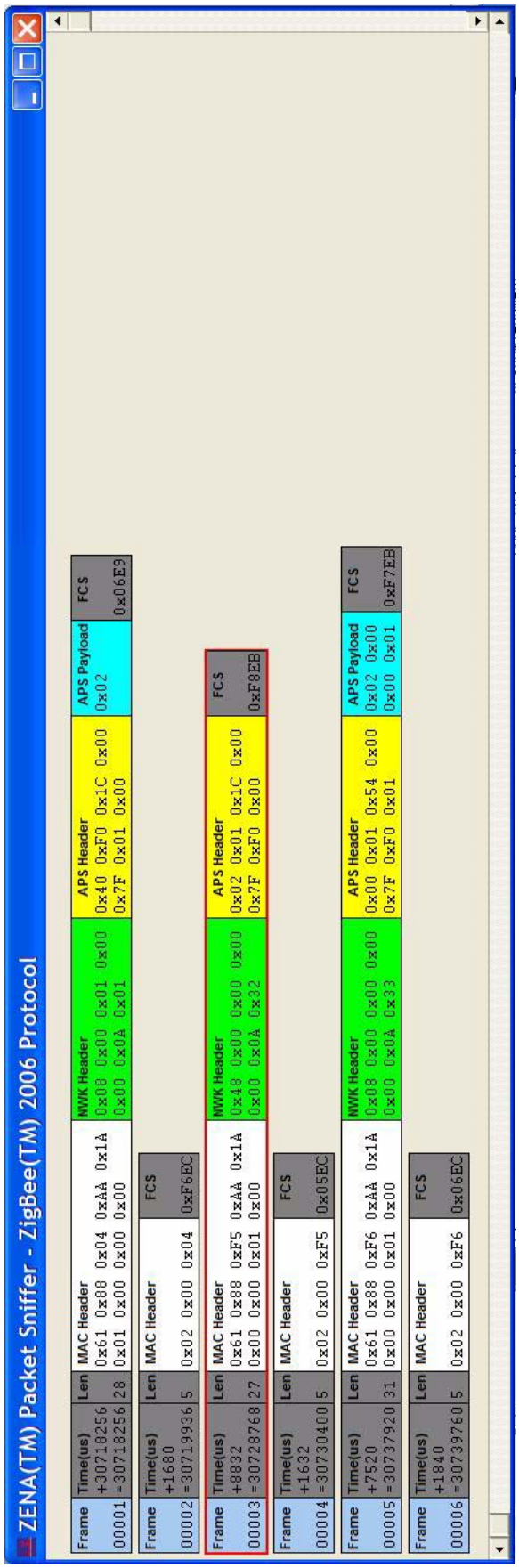
Configuration	Option Description
Verbose	Headers for each field are provided with a description of the corresponding value below the header. Figure 3-12 shows all layers at the “Verbose” setting.
Numeric	Headers for each field are provided with the numeric value of that field below the header. Refer to Figure 3-13.
Condensed	No field headers are provided. All bytes of the field are represented numerically with the Least Significant Byte first. Refer to Figure 3-14.

FIGURE 3-13: APPLICATION MESSAGE WITH NUMERIC DISPLAY



© 2008 Microchip Technology Inc.

FIGURE 3-14: APPLICATION MESSAGE WITH CONDENSED DISPLAY



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 *Operation>Stop Sniffing/Playback* 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 *Operation>Start Sniffing/Playback* menu option. To analyze previously captured data, click **Open** or select *File>Open* 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:

TABLE 3-17: ZigBee™ PROTOCOL PACKET PLAYBACK SELECTION

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.

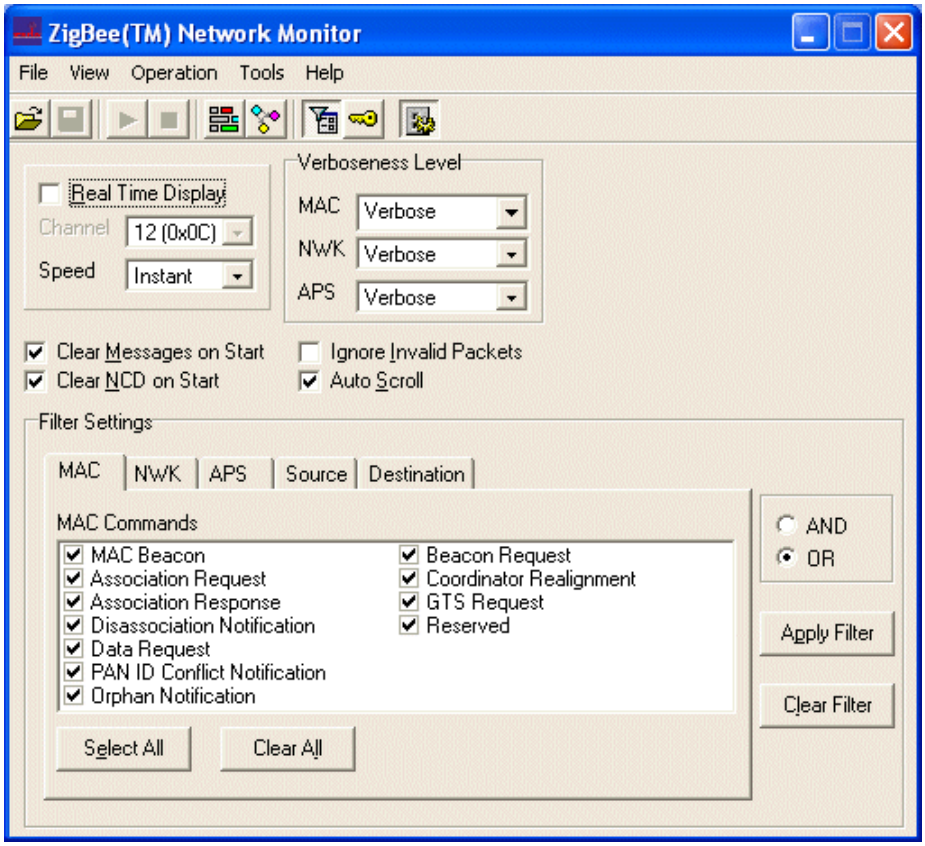
Packet playback is especially useful when using the filter option and performing more advanced network analysis.

© 2008 Microchip Technology Inc.

3.3.2.2 USING THE PACKET FILTER

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

FIGURE 3-15: NETWORK MONITOR WINDOW WITH FILTER



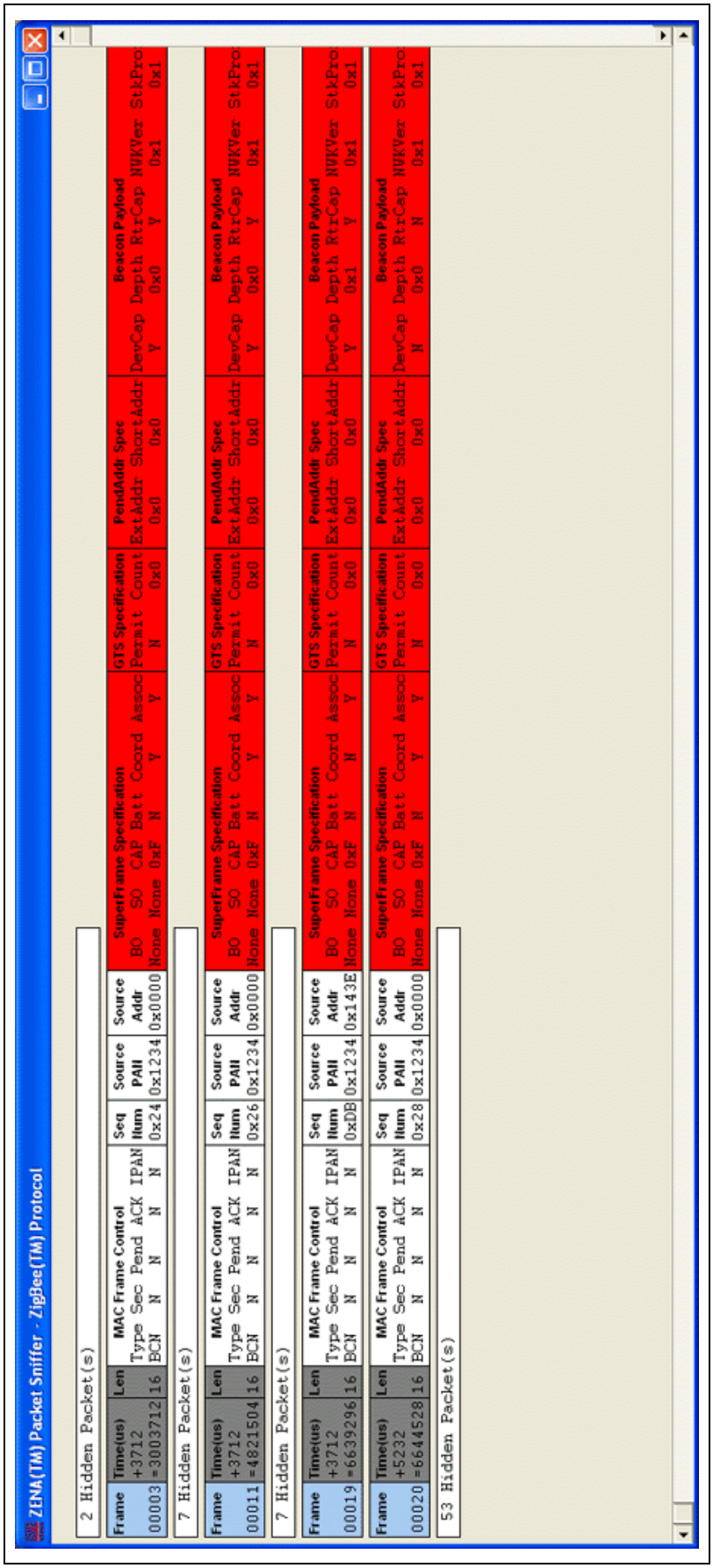
The filter is useful for displaying only selected packets in the Packet Sniffer window. For example, suppose we want to see all beacons generated by our network. Set up the filter as follows:

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 3-16.

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 3-16: FILTERED BEACONS



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.

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.

© 2008 Microchip Technology Inc.

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 in **Section 3.3.2.2 “Using the Packet Filter”**
- 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 3-17.

To decrypt these messages, enable decryption by clicking the **Security** button or by selecting the *Tools>Security* 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 in Figure 3-18.

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.

FIGURE 3-17: SECURITY

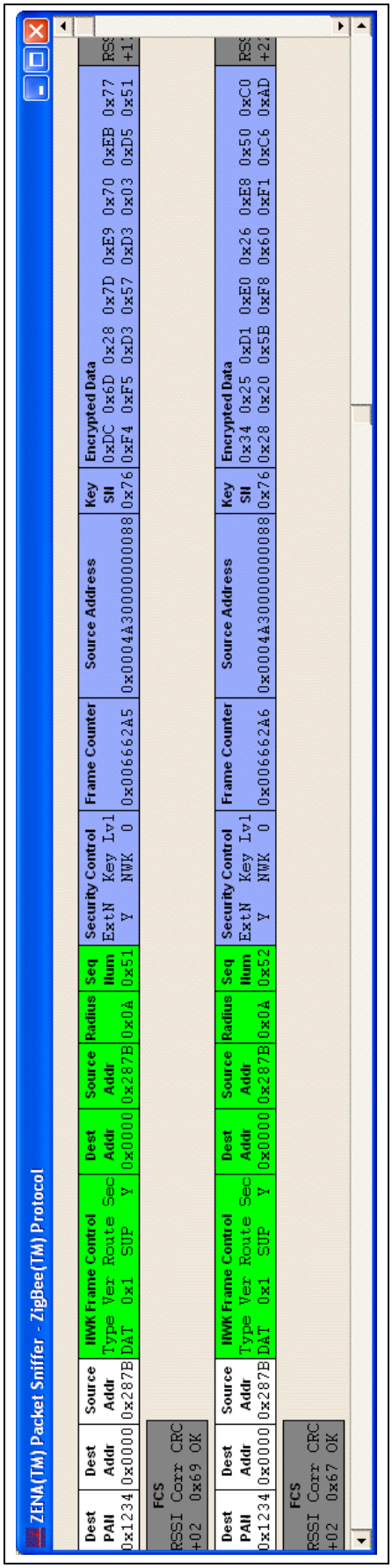
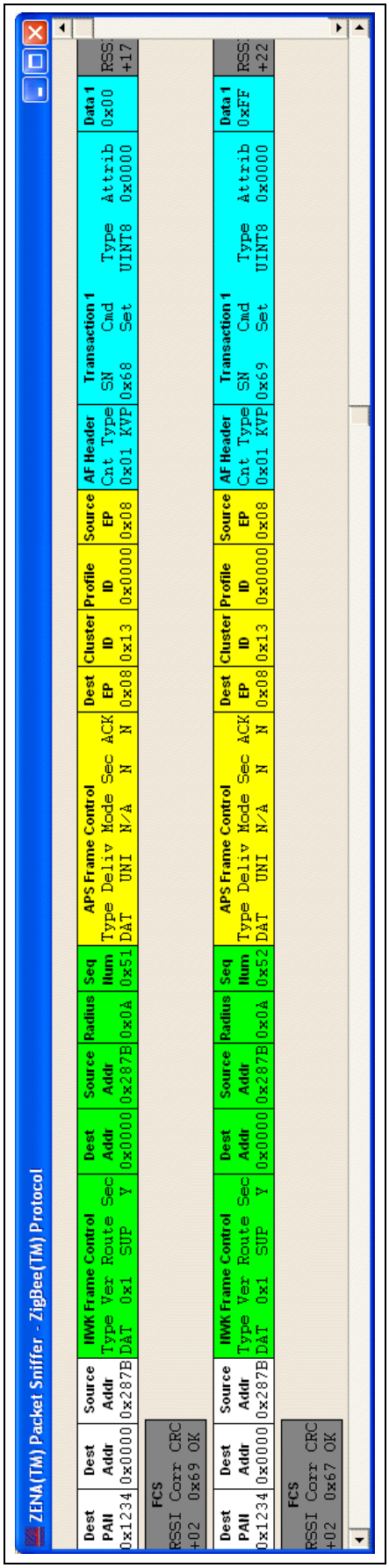


FIGURE 3-18: DECRYPTED



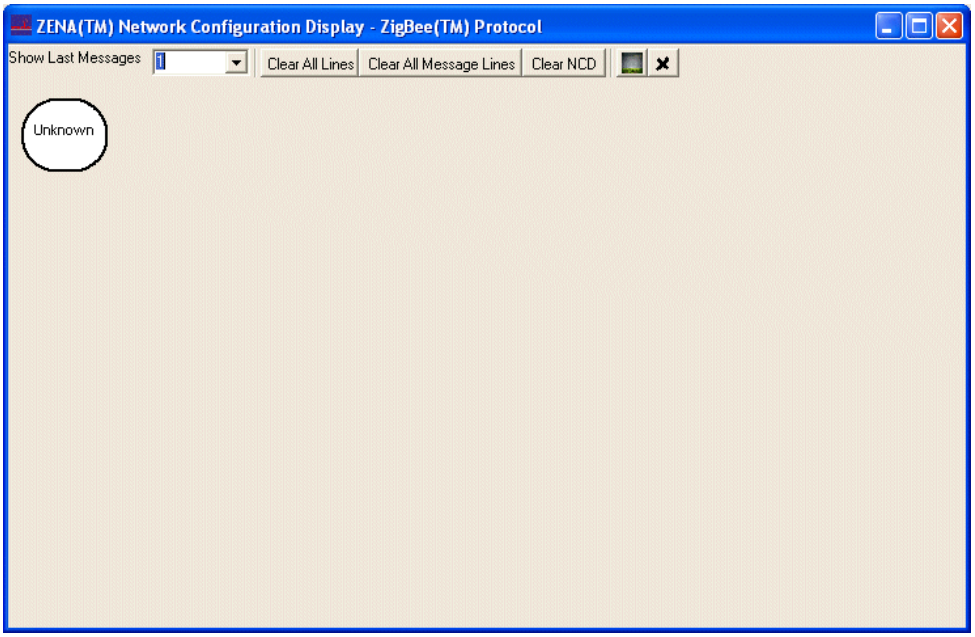
© 2008 Microchip Technology Inc.

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 *View>Network Configuration Display* menu option on the Network Monitor window.

FIGURE 3-19: NETWORK CONFIGURATION DISPLAY WINDOW



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.

TABLE 3-18: Node Colors

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 3-19 for NCD window controls.

TABLE 3-19: 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.

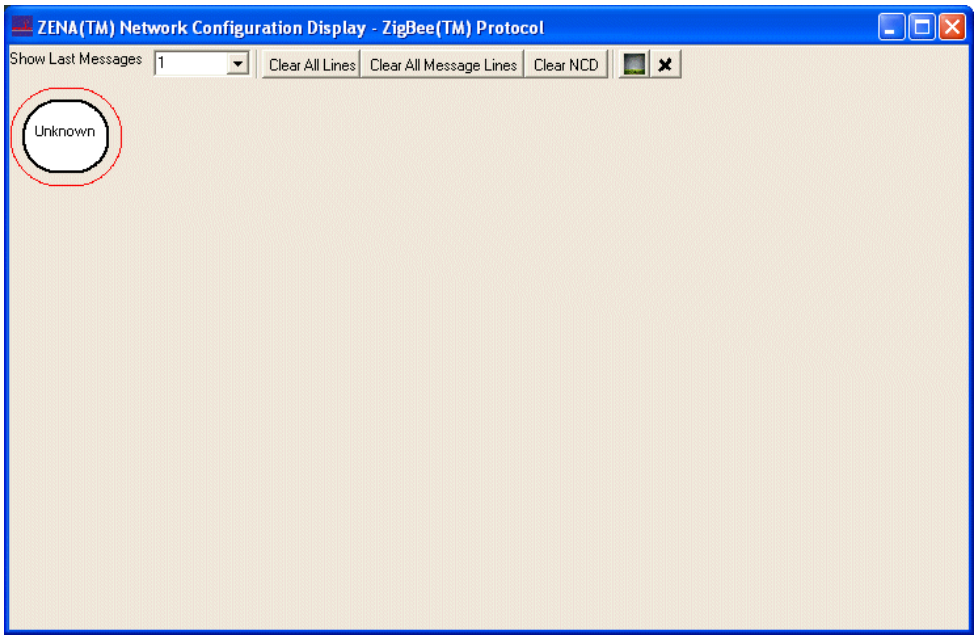
© 2008 Microchip Technology Inc.

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.

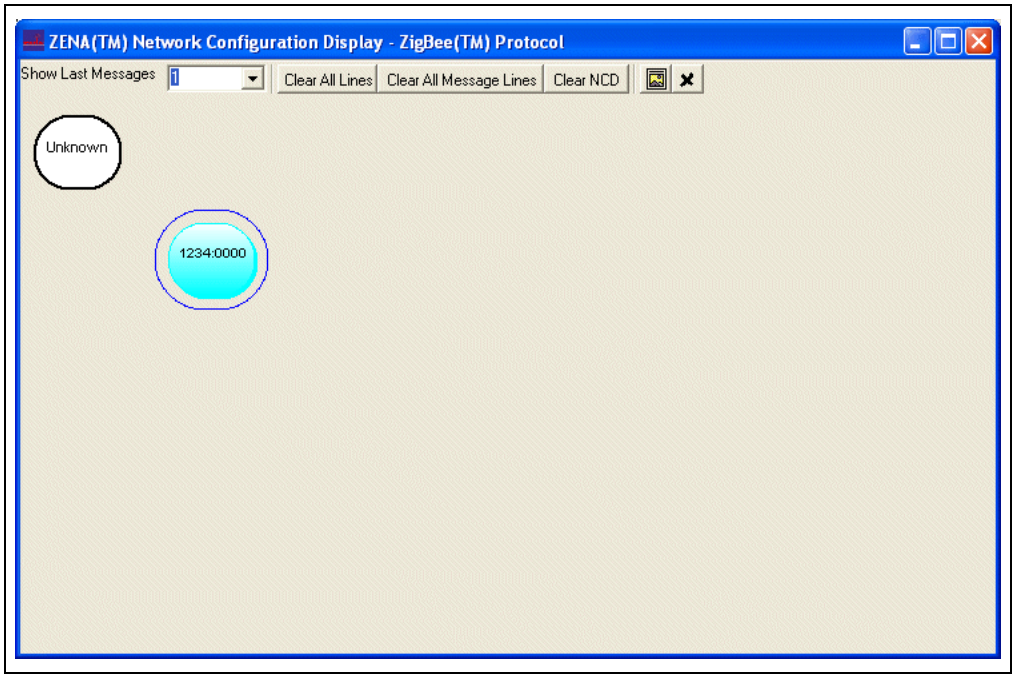
FIGURE 3-20: NCD BEACON REQUEST



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 3-20, since the beacon request contains no source address information. Now, the ZigBee protocol coordinator responds with a beacon.

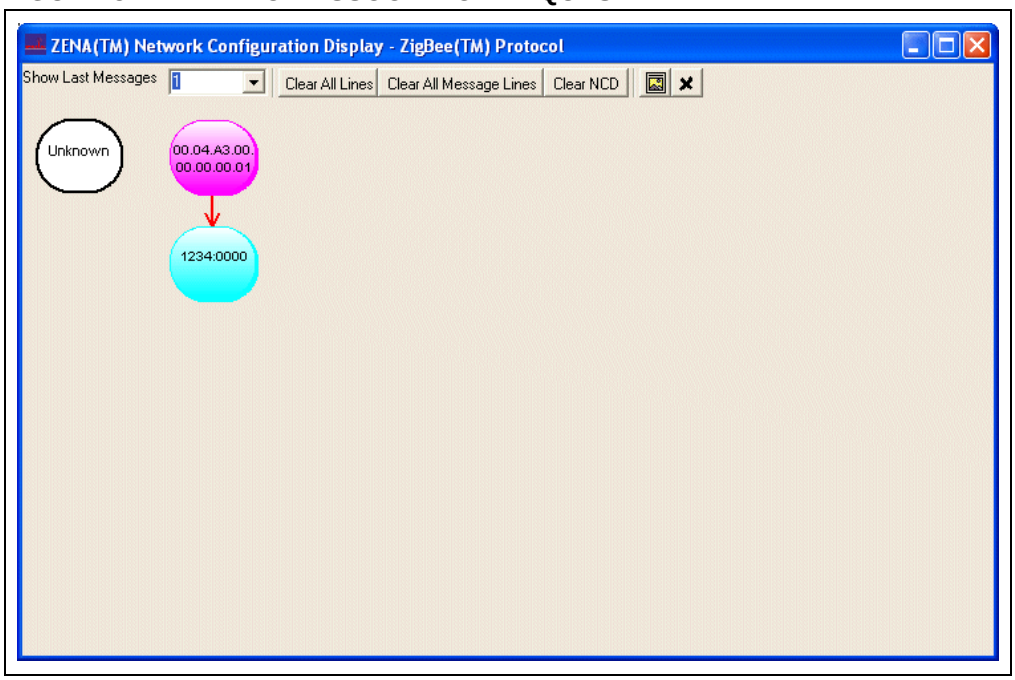
FIGURE 3-21: NCD BEACON



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.

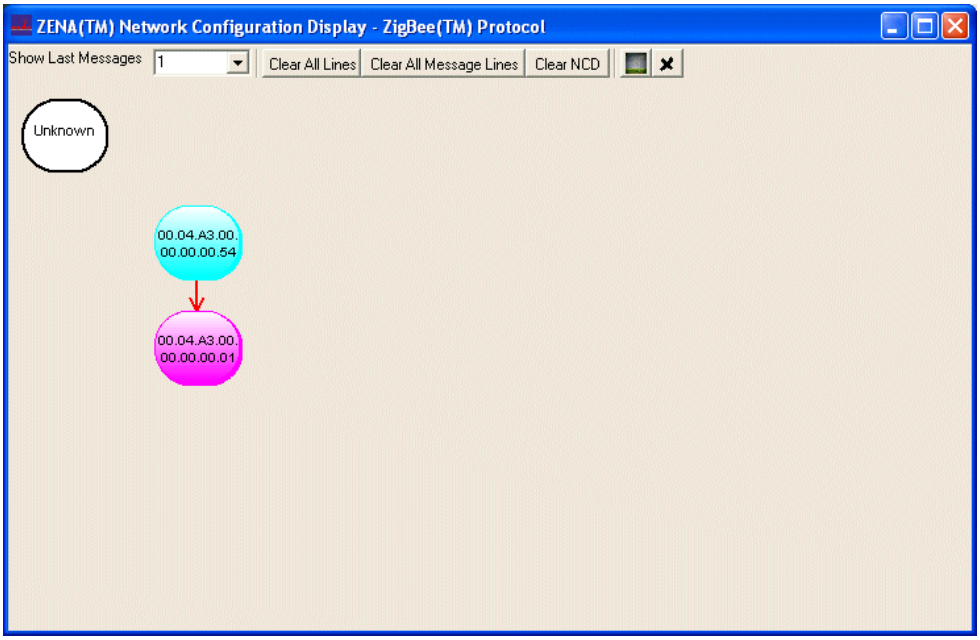
FIGURE 3-22: NCD ASSOCIATION REQUEST



© 2008 Microchip Technology Inc.

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 3-23: 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 3-24: TWO-DEVICE NETWORK

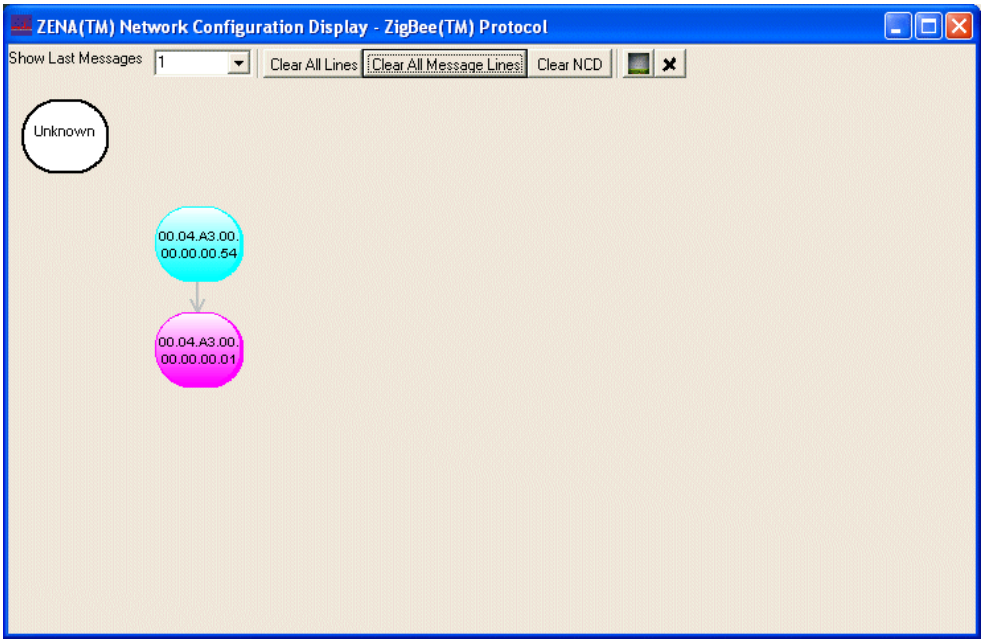
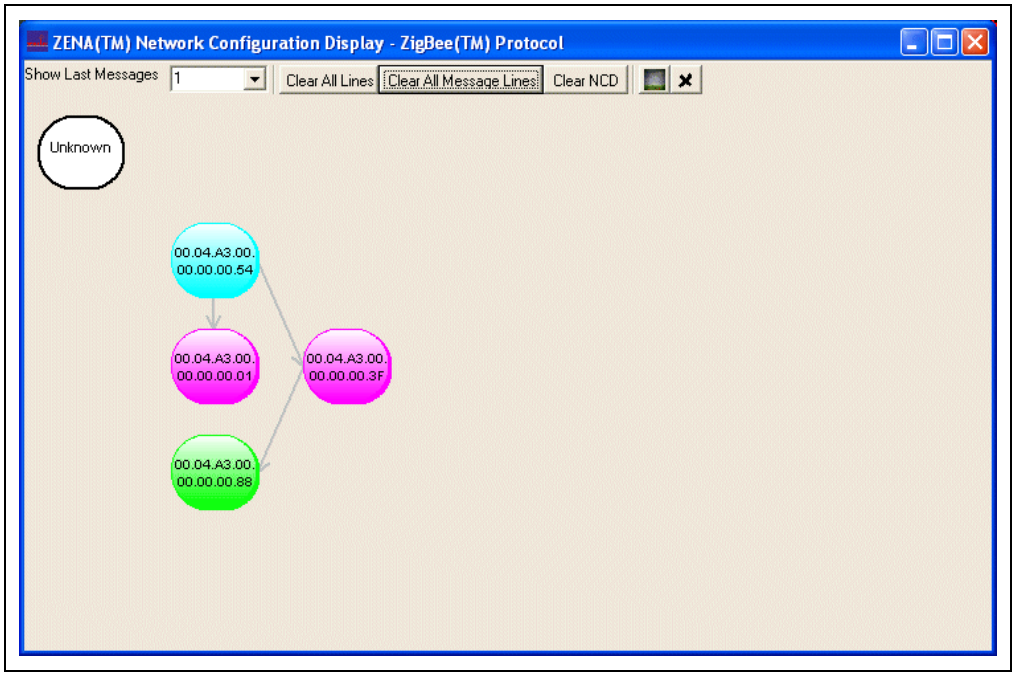


Figure 3-25 shows the NCD window after the creation of a four-device network.

FIGURE 3-25: FOUR-DEVICE NETWORK



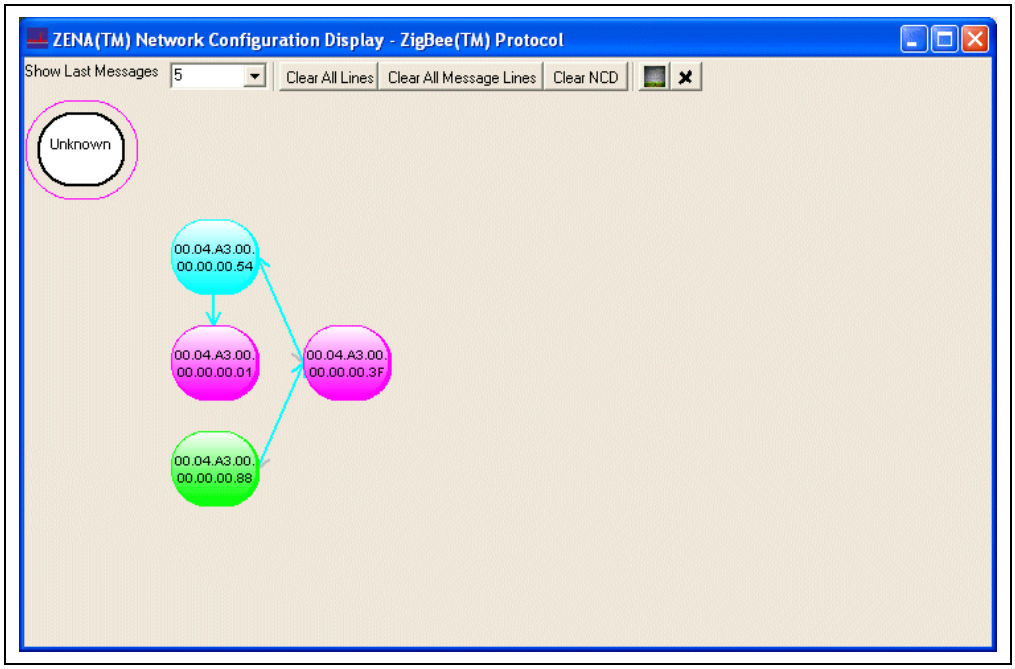
Note: If you will be working with a network that maintains the same structure, you may want to save a captured data file that contains the network formation. You can play back this file to establish the devices on the network, and then play back the various data files containing the network traffic you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

© 2008 Microchip Technology Inc.

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 3-26.

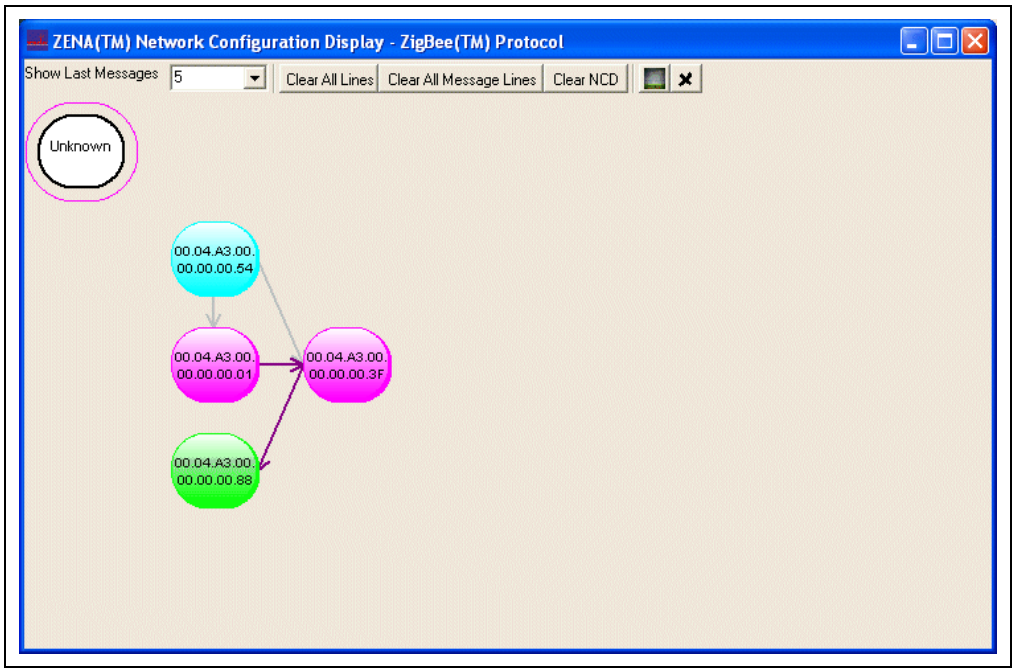
FIGURE 3-26: NCD MESSAGE PATH



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 3-27 shows the path of the APS Acknowledge. The ZENA analyzer illustrates that the APS Acknowledge followed a different route than the original message.

FIGURE 3-27: NCD APS ACKNOWLEDGE PATH

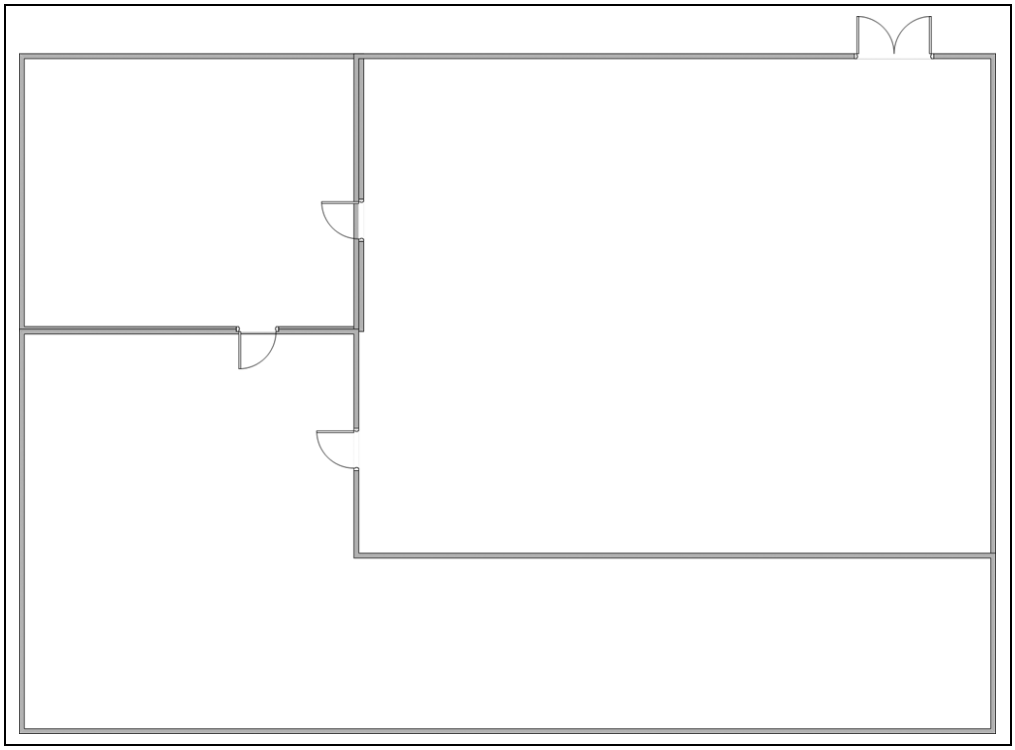


3.4.4 Customizing the Network Configuration Display Window

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.

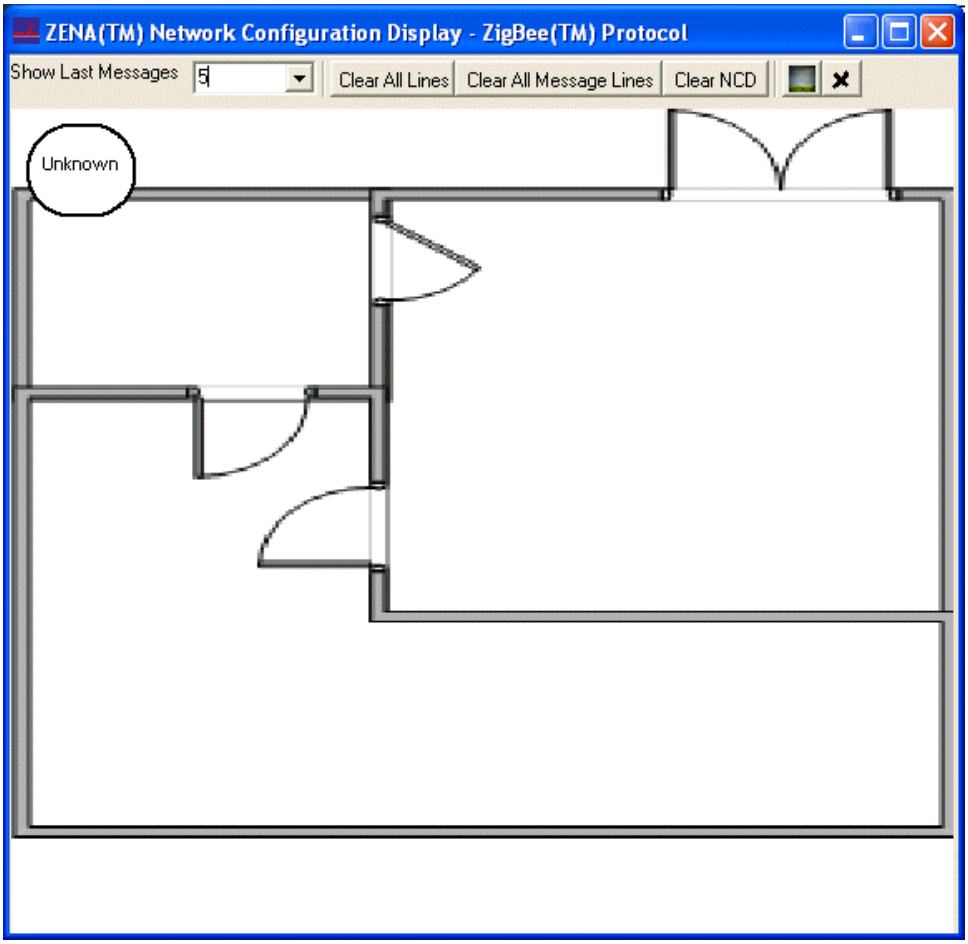
FIGURE 3-28: FLOOR PLAN BITMAP



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.

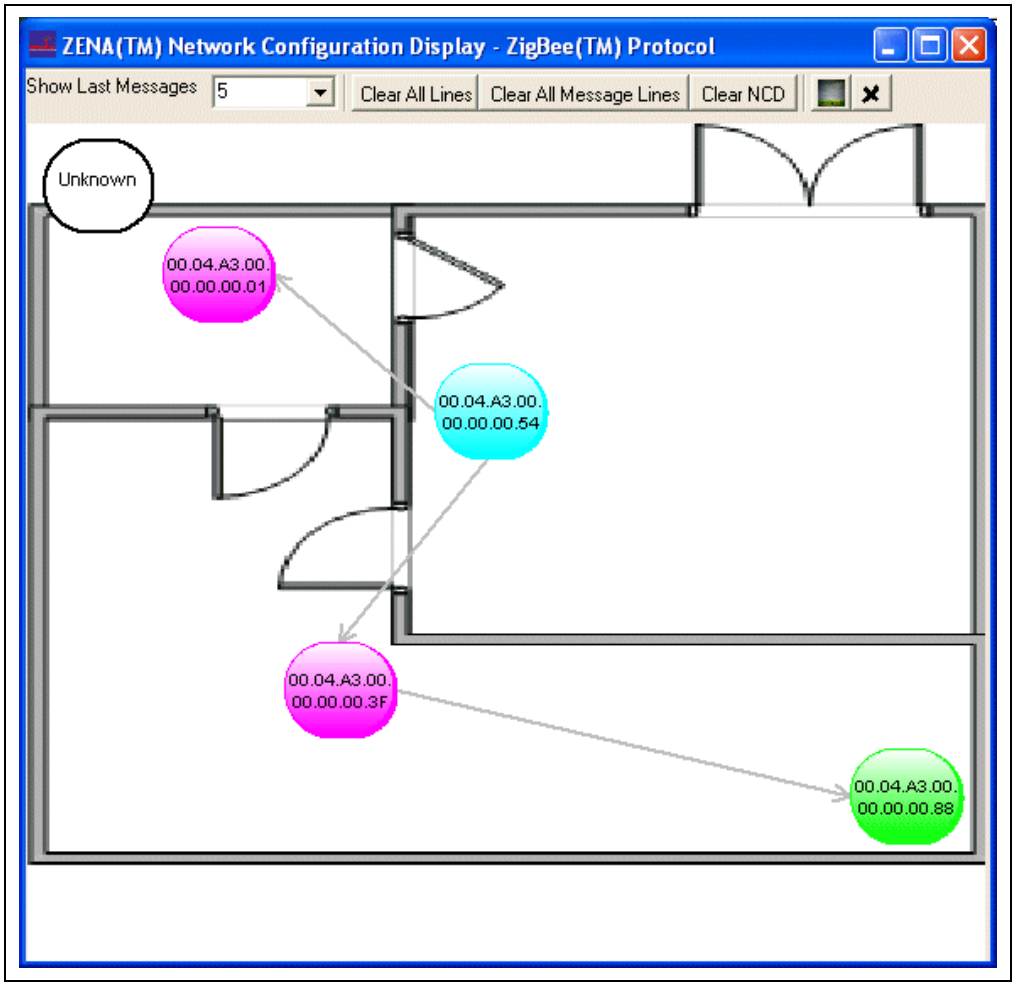
© 2008 Microchip Technology Inc.

FIGURE 3-29: 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 3-30: FOUR-NODE NETWORK WITH FLOOR PLAN BACKGROUND



Repeating the above example, Figure 3-31 and Figure 3-32 show the application message and APS Acknowledge as they are routed through the network.

© 2008 Microchip Technology Inc.

FIGURE 3-31: MESSAGE PATH WITH FLOOR PLAN BACKGROUND

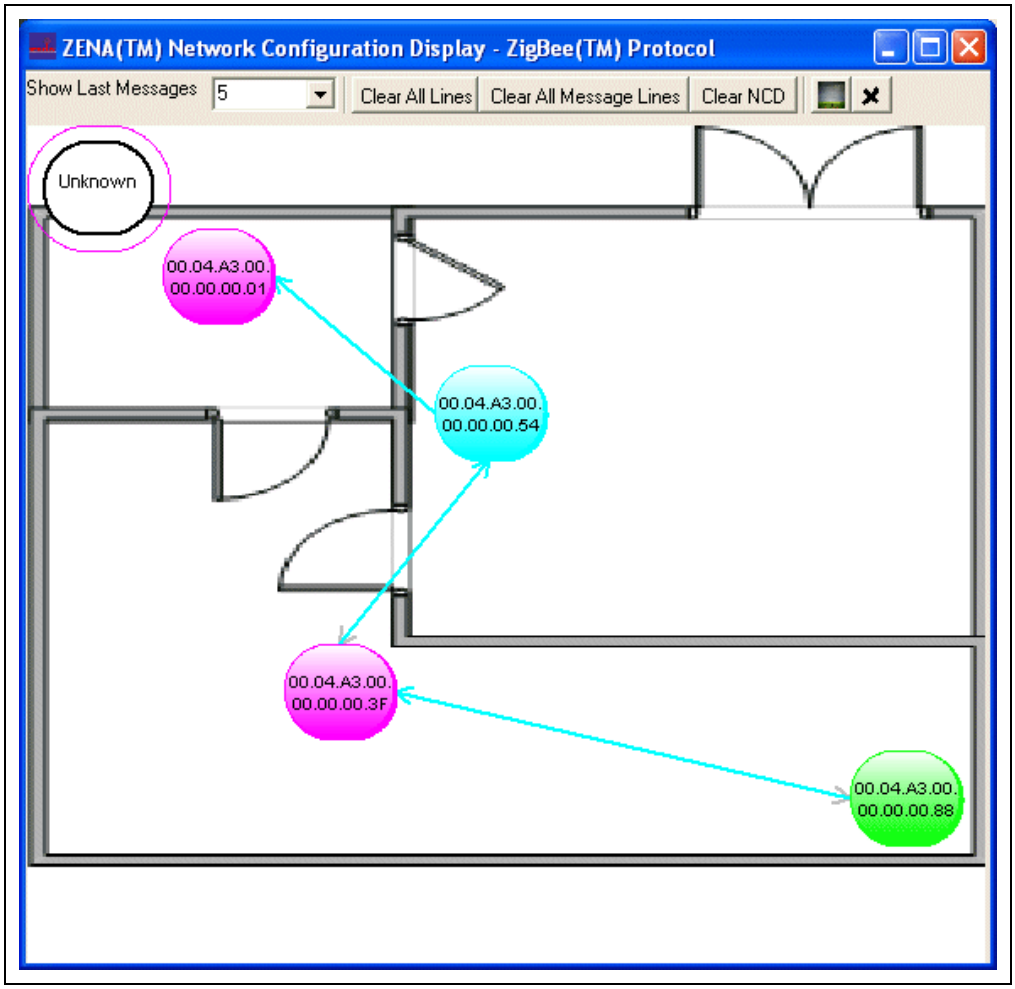
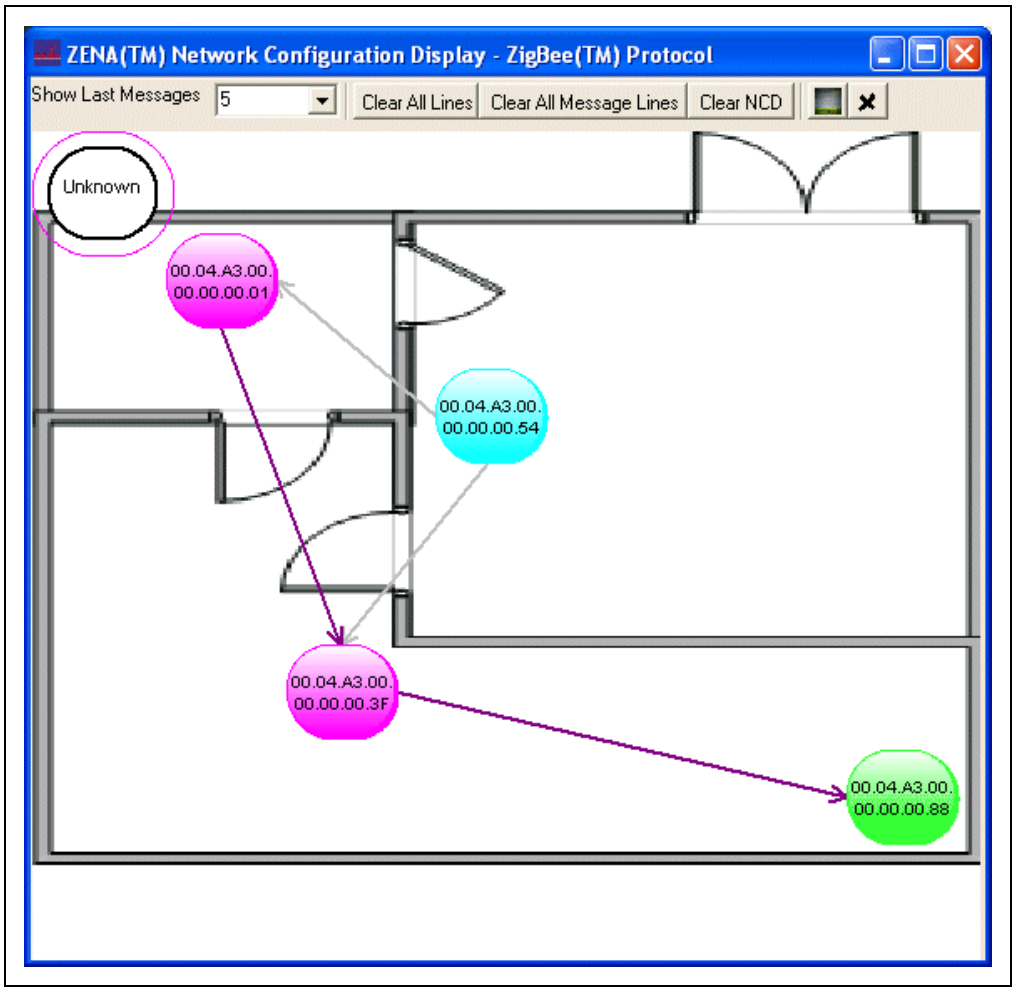


FIGURE 3-32: APS ACKNOWLEDGE PATH WITH FLOOR PLAN BACKGROUND



© 2008 Microchip Technology Inc.

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.

NOTES:

© 2008 Microchip Technology Inc.

Chapter 4. MiWi™ 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

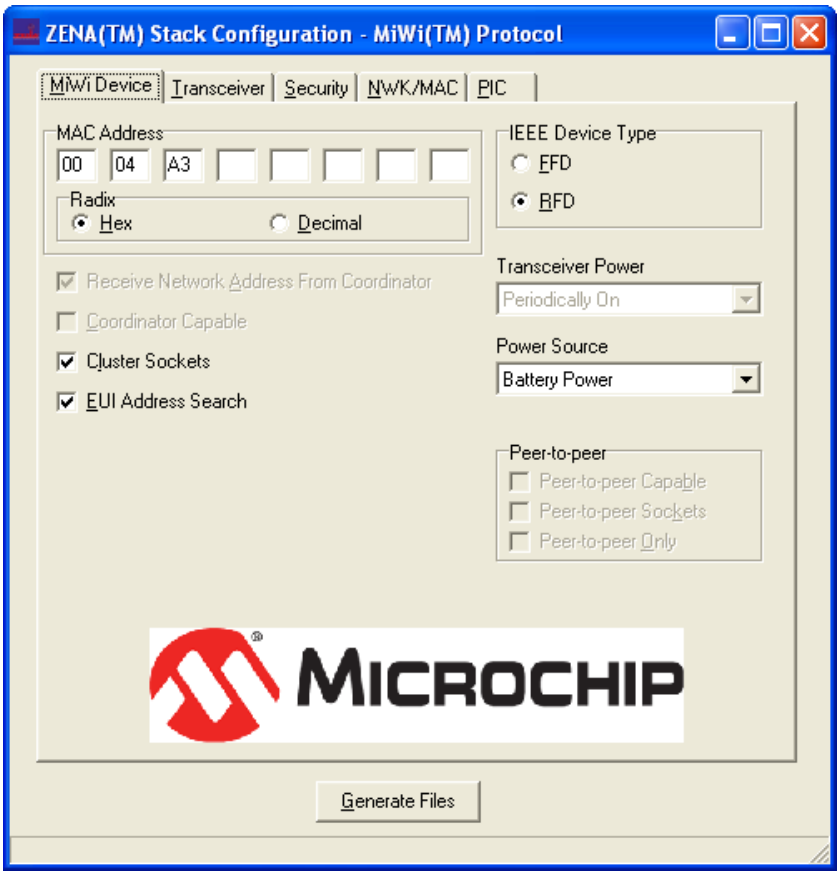
Microchip provides a freely available Stack as part of application note, *AN1066, "MiWi™ Wireless Networking Protocol Stack"*. The application note and source code are available for download from the Microchip Web site (www.microchip.com). After you have reviewed the application note and studied the 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 *MiWi Tools>Stack Configuration* 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.

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



© 2008 Microchip Technology Inc.

Using this window, you can configure the following items:

TABLE 4-1: MiWi™ PROTOCOL DEVICE CONFIGURATION SELECTION

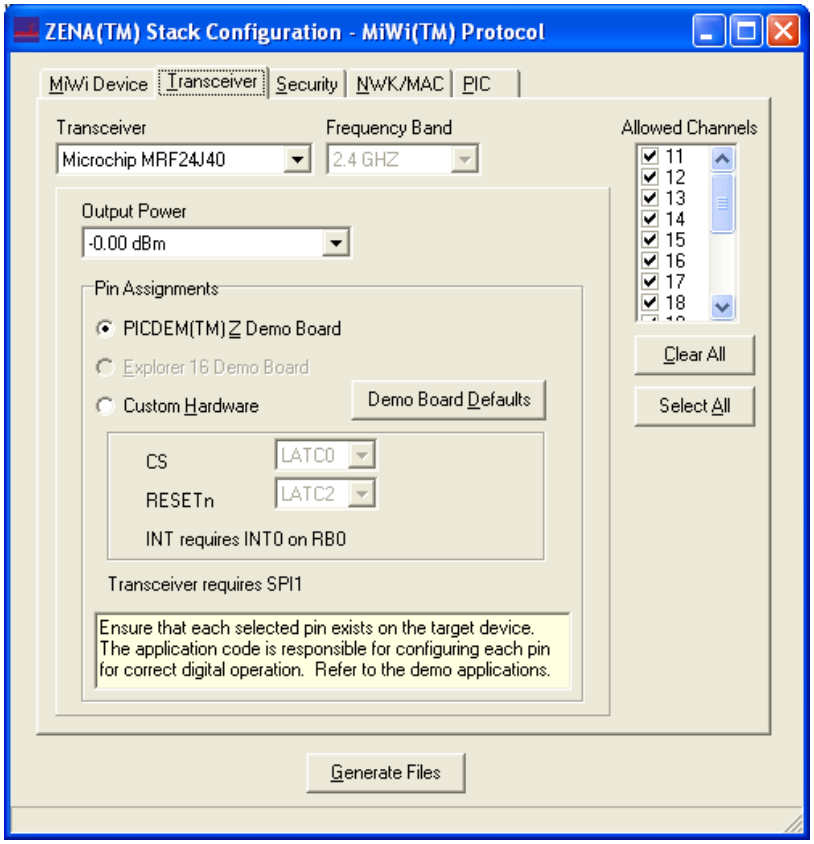
Configuration	Option Description
MAC Address	Each and every MiWi™ protocol device must have its own unique MAC address. The Microchip OUI is provided as a default for development purposes only. For additional information, see *AN1066, "MiWi™ Wireless Networking Protocol Stack"*.
Receive Network Address 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)

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



© 2008 Microchip Technology Inc.

Using this window, you can configure the following items:

TABLE 4-2: MiWi™ PROTOCOL TRANSCEIVER CONFIGURATION SELECTION

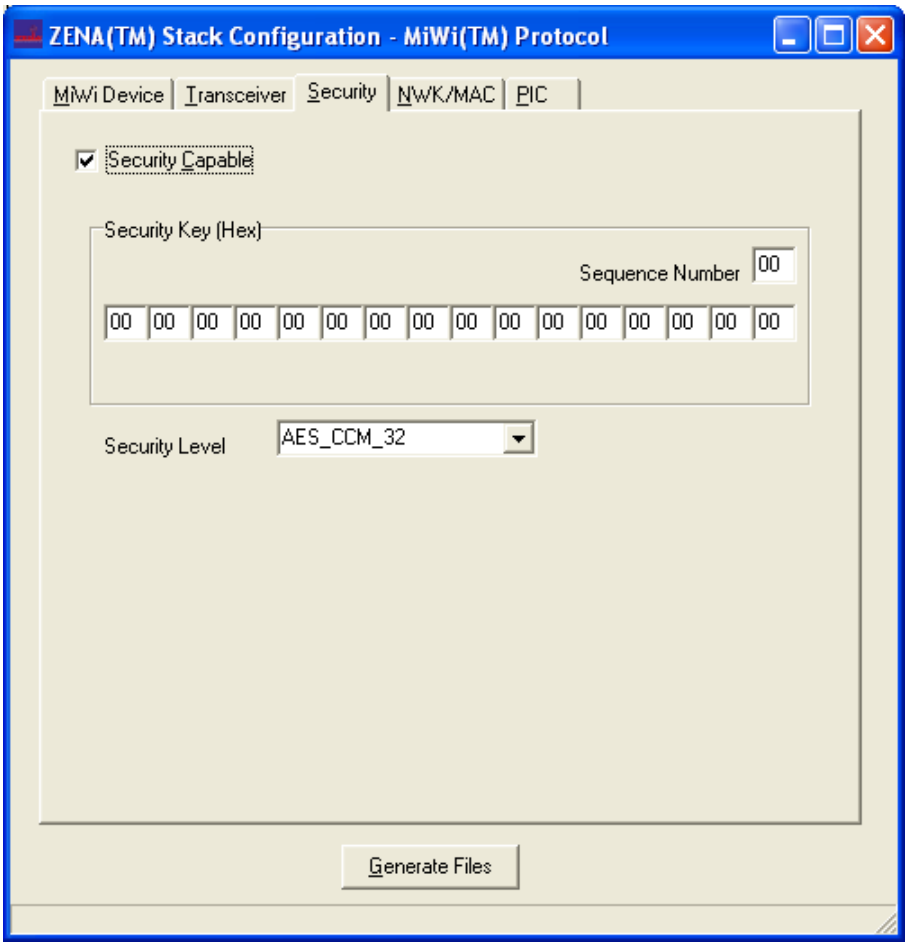
Configuration	Option Description
Transceiver	Select one of the transceivers supported by the Stack.
Frequency Band	This combo box shows the various available frequency bands of the selected transceiver. If the transceiver supports only one frequency band, that frequency will be displayed and the combo 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.

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



Using this window, you can configure the following items:

TABLE 4-3: MiWi™ PROTOCOL SECURITY CONFIGURATION SELECTION

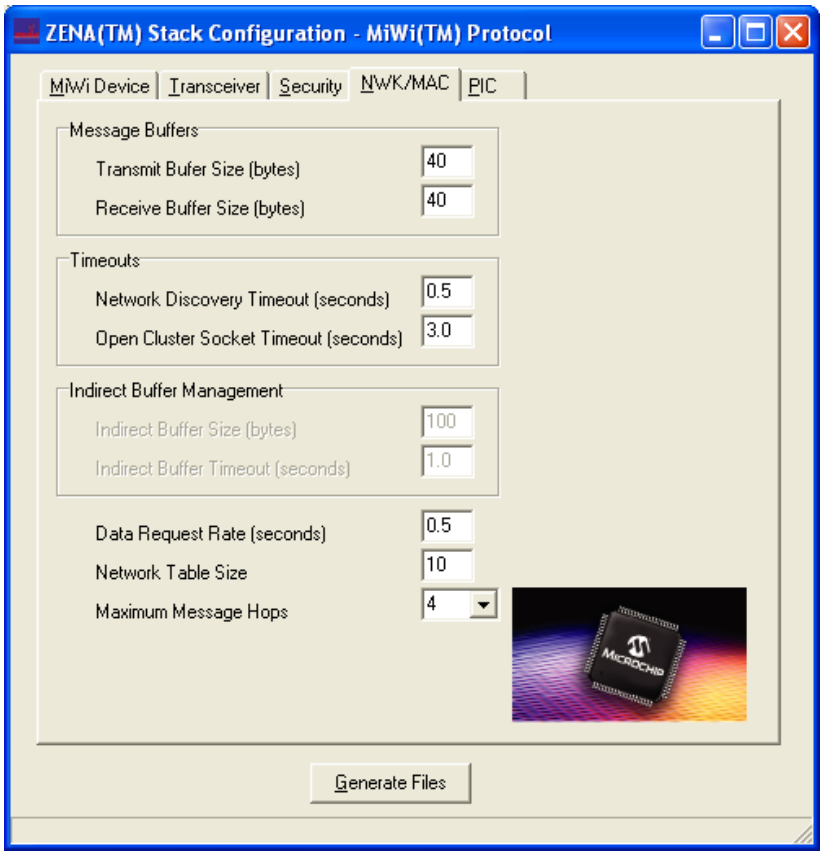
Configuration	Option Description
Security Capable	Only "Residential" mode is currently supported by the Stack.
Security Key	If the network key is known, enter it here with the "Sequence Number".
Security Level	Select the IEEE "Security Level" of how the packets will be encrypted and decrypted.

© 2008 Microchip Technology Inc.

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



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.

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

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.

© 2008 Microchip Technology Inc.

4.2.5 Specifying PIC MCU Information

Select the **PIC** tab.

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

This tab is used to configure basic PIC MCU options.

TABLE 4-5: MiWi™ PROTOCOL PIC® MCU 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

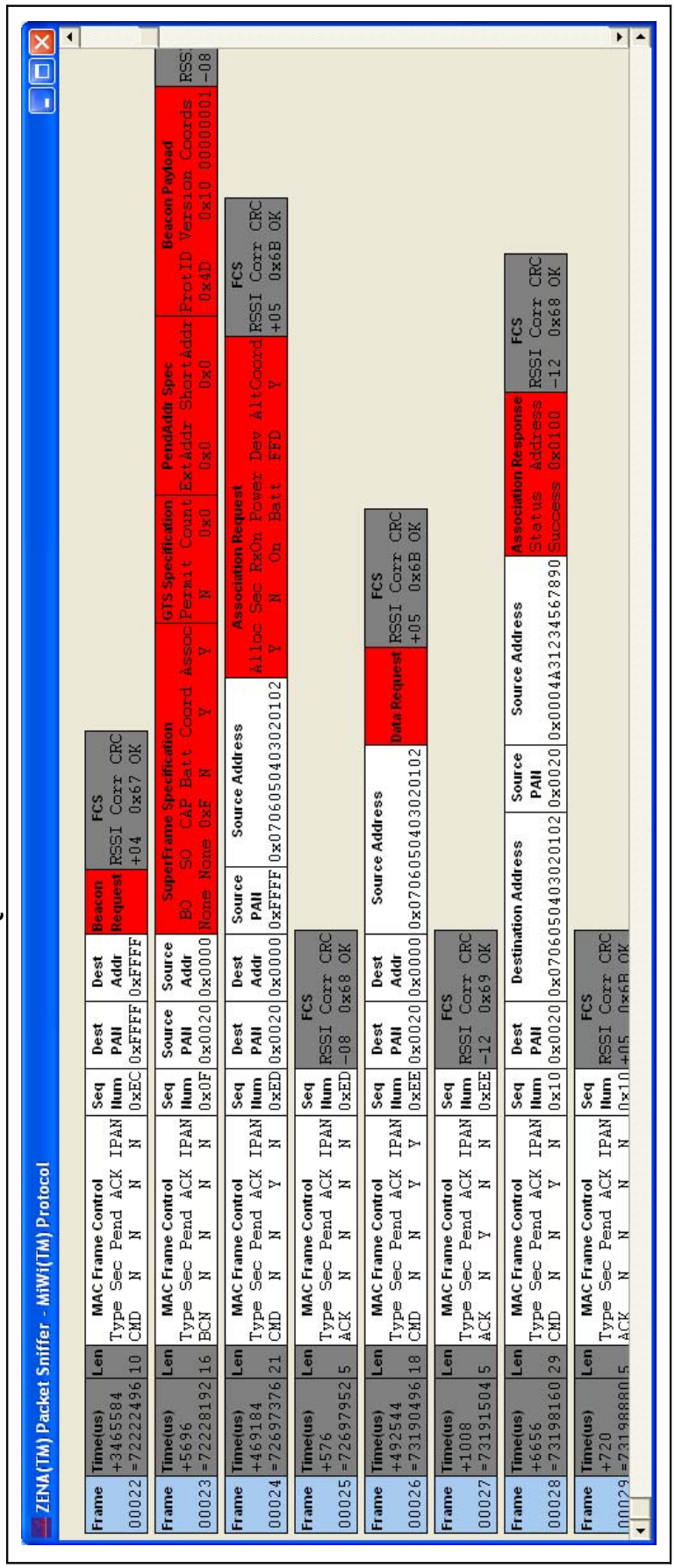
Basic monitoring of a MiWi protocol network is nearly identical to that of a ZigBee protocol network. Please review section **Section 3.3 "Basic Network Monitoring"**. This section will focus on the differences between the two protocols.

Select *MiWi Tools> Network Traffic Monitor* 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.

© 2008 Microchip Technology Inc.

FIGURE 4-6: MiWi™ PROTOCOL ASSOCIATION REQUEST AND RESPONSE



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

TABLE 4-6: MiWi™ PROTOCOL PACKET SNIFFER 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

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.

© 2008 Microchip Technology Inc.

FIGURE 4-7: SECURE MiWi™ PROTOCOL PACKETS

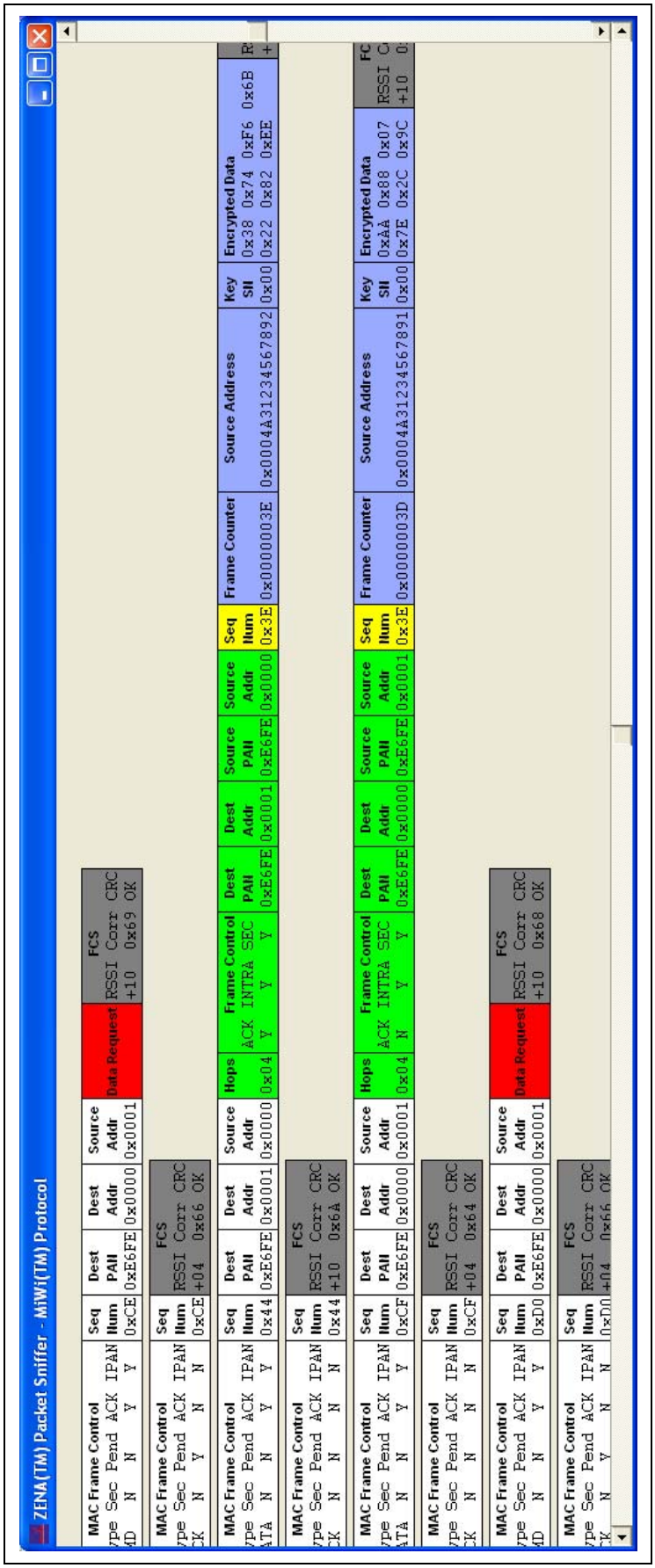
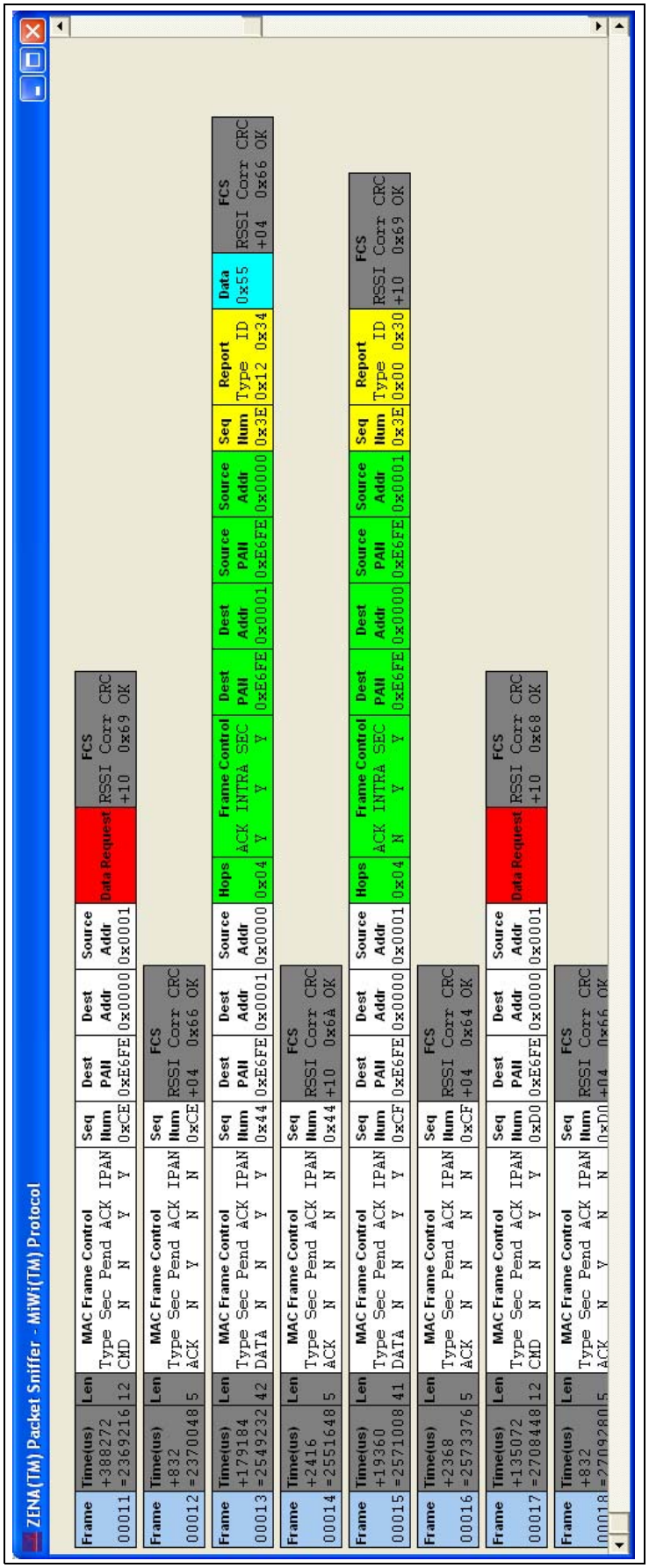


FIGURE 4-8: DECRYPTED OR UNSECURE MiWi™ PROTOCOL PACKETS



© 2008 Microchip Technology Inc.

Chapter 5. MiWi™ P2P Wireless Networking Protocol Tools

5.1 INTRODUCTION

This chapter describes how to use the MiWi P2P protocol tools provided by the ZENA Wireless Network Analyzer.

5.2 MiWi™ P2P STACK CONFIGURATION TOOL

The Microchip MiWi P2P Stack provides the user with the capability to communicate wirelessly in the star or P2P topology. For details on the MiWi P2P protocol, please refer to application note *AN1204 "Microchip MiWi P2P Wireless Protocol"* and the MiWi P2P Stack source code, which are both available for free download from the Microchip web site (www.microchip.com).

The ZENA analyzer assists you in configuring the Microchip Stack by automatically generating the configuration header file for your MiWi P2P protocol application. To start the Stack configuration tool from ZENA analyzer, select *MiWi P2P Tools>StackConfiguration* from the main ZENA window. The ZENA Stack Configuration – MiWi P2P Protocol window will be displayed. Using the tabbed dialog, you can select options that are configurable in the MiWi P2P Stack. The ZENA analyzer software will automatically enable/disable certain options depending on the selections that you have made. All enabled options will have default values. Users are encouraged to learn the meaning of the options by reading application note *AN1204 "Microchip MiWi P2P Wireless Protocol"*. After users understand all the options, the ZENA MiWi P2P Stack configuration tool can generate the configuration file that will be compiled with the MiWi P2P Stack, as well as the application, to enable or disable the options of your choice for the MiWi P2P Stack.

5.2.1 Specifying MiWi P2P Protocol Device Information

Select the **P2P Device** tab (refer to Figure 5-1). Refer to Table 5-1 for configuration options for MiWi P2P devices.

FIGURE 5-1: ZENA™ STACK CONFIGURATION – MiWi™ P2P PROTOCOL WINDOW, P2P DEVICE TAB

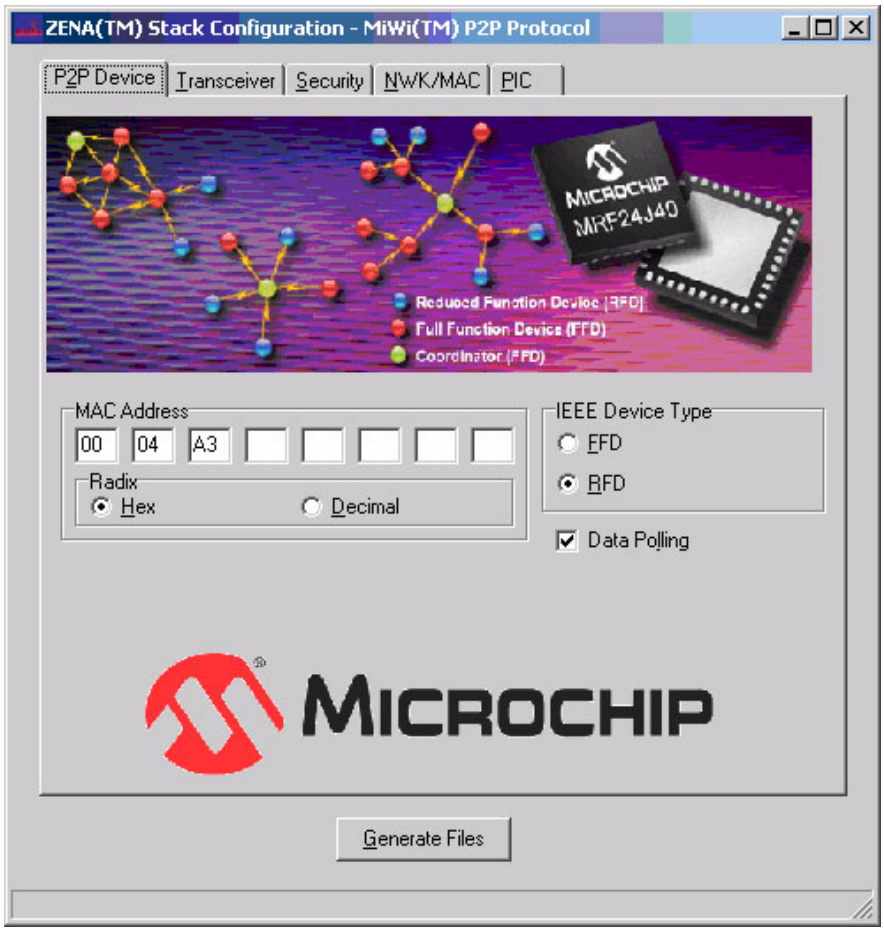


TABLE 5-1: MiWi™ P2P PROTOCOL DEVICE CONFIGURATION SELECTION

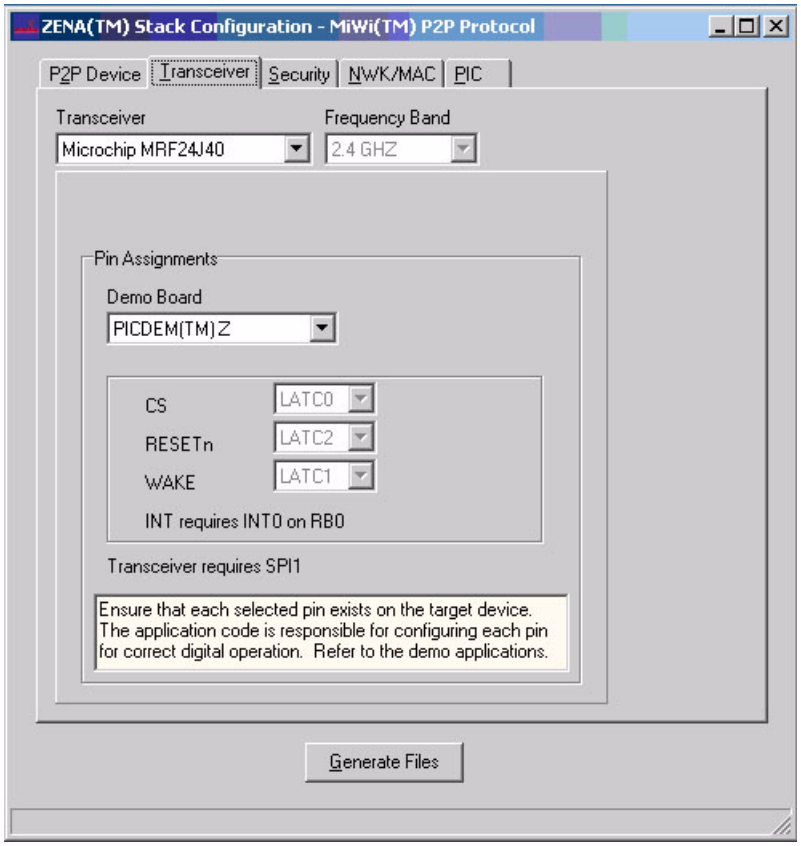
Configuration	Option Description
MAC Address	Each and every MiWi™ P2P protocol device must have its own unique MAC address. The Microchip OUI is provided as a default for development purpose only. For additional information, see *AN1204, "MiWi P2P Wireless Protocol"*.
IEEE Device Type	Select whether your application is a Full Function Device (FFD) or a Reduced Function Device (RFD). The difference between FFD and RFD in the MiWi P2P protocol is that an RFD goes to sleep periodically and thus can be powered by a battery.
Data Polling	Select this option to enable the RFD to poll data from its associated FFDs. This option needs to be checked if the RFD expects to receive messages from other devices.

© 2008 Microchip Technology Inc.

5.2.2 Specifying Transceiver Information

Select the **Transceiver** tab (refer to Figure 5-2).

FIGURE 5-2: ZENA™ STACK CONFIGURATION – MiWi™ P2P PROTOCOL WINDOW, TRANSCEIVER TAB



Using this window, you can configure the following items detailed in Table 5-2.

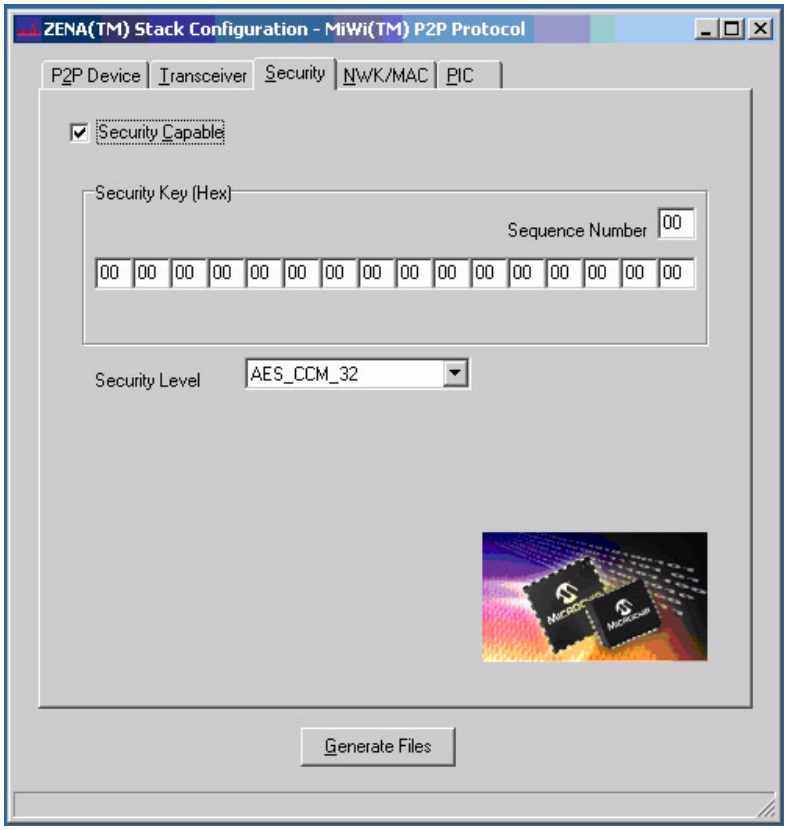
TABLE 5-2: MiWi™ P2P PROTOCOL TRANSCEIVER CONFIGURATION SELECTION

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.
Pin Assignments	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 the option to automatically configure the Stack for that board. If you are using custom hardware, select “Custom Hardware”. You are responsible for specifying the correct I/O pins for your custom hardware.

5.2.3 Specifying Security Information

Select the **Security** tab (refer to Figure 5-3).

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



Using this window, you can configure the following items:

TABLE 5-3: MiWi™ P2P PROTOCOL SECURITY CONFIGURATION SELECTION

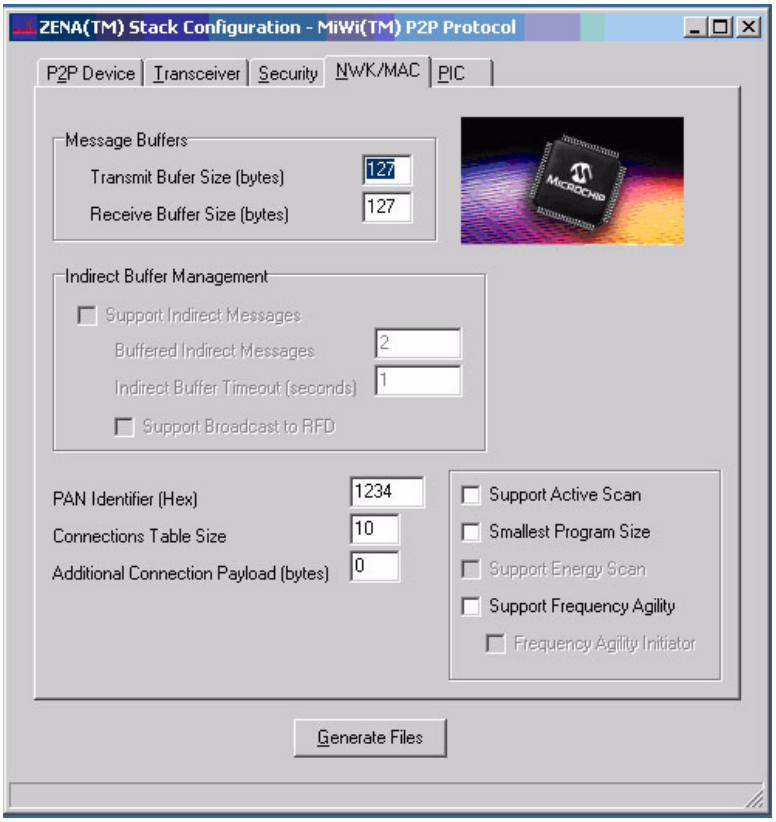
Configuration	Option Description
Security Capable	Check this option to enable security features in the MiWi™ P2P Stack.
Security Key	This is the 16 byte security key for the AES security engine, along with the security key sequence number.
Security Level	Select the IEEE security level defined in IEEE 802.15.4™ specification.

© 2008 Microchip Technology Inc.

5.2.4 Specifying NWK and MAC Layer Information

Select the **NWK/MAC** tab (refer to Figure 5-4).

FIGURE 5-4: ZENA™ STACK CONFIGURATION – MiWi™ P2P PROTOCOL 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 “IEEE Device Type” specified on the **P2P Device** tab.

This tab is used to configure the following options:

TABLE 5-4: MiWi™ PROTOCOL NWK/MAC CONFIGURATION SELECTION

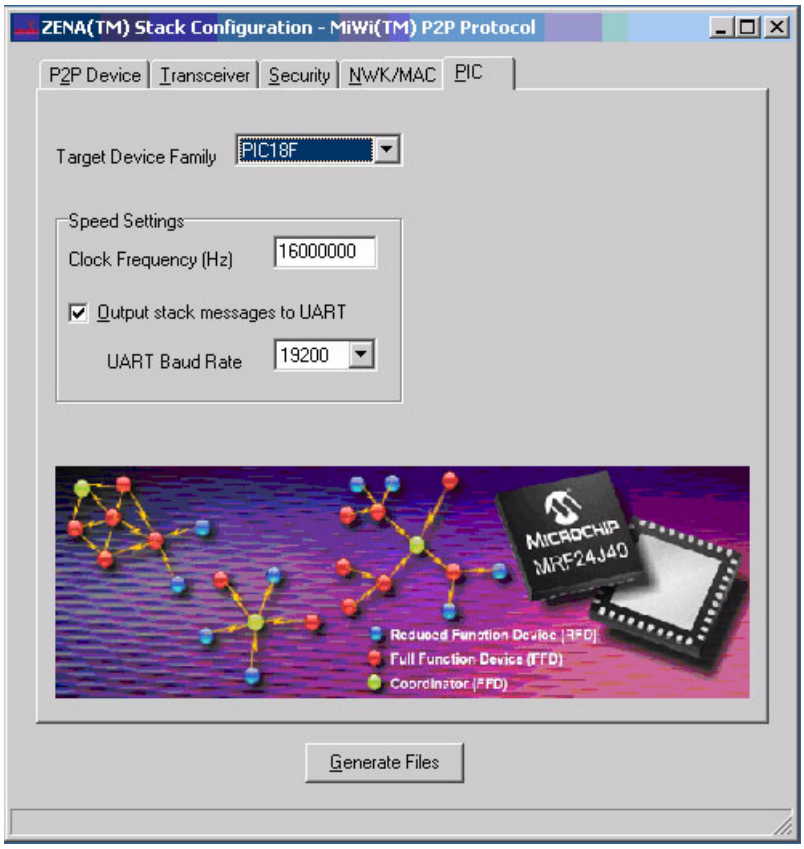
Configuration	Option Description
Transmit Buffer Size (bytes)	Enter the number of bytes for the largest transmitted message. The largest possible message is 127 bytes.
Receive Buffer Size (bytes)	Enter the number of bytes for the largest received message. The largest possible message is 127 bytes.
Indirect Buffer Management	This option is only available for FFDs defined in the P2P Device tab. If indirect messages are supported, the Buffered Indirect Messages and Indirect Buffer Timeout need to be defined.
PAN Identifier	Personal Area Network identifier used in the MiWi™ P2P Stack.
Connections Table Size	Defines the maximum number of P2P connections that the device can maintain.
Additional Connection Payload (bytes)	This is the additional information to be transferred during connection establishment to identify the device. This setting is purely application-specific and MiWi P2P Stack will not use the additional connection payload.
Support Active Scan	Checking this box will enable the MiWi P2P Stack to perform an active scan to acquire all MiWi P2P PANs in the neighborhood.
Smallest Program Size	Checking this box will enable the MiWi P2P Stack to shrink to the smallest size possible. Certain features in this mode will be disabled, such as inter PAN communication and packet freshness checking in Security mode.
Support Energy Scan	This box will only be enabled if the device is an FFD as defined in the P2P Device tab. Checking this box will enable the MiWi P2P Stack to perform an energy detection scan to survey noise levels in different frequencies. This function helps determine the optimal channel to use.
Support Frequency Agility	Checking this box will enable the device to hop channels during operation to adapt to the changing noise levels in the environment. If the device is an FFD, as defined in P2P Device tab, and the Support Energy Scan option is enabled, the Frequency Agility Initiator option can be checked to allow the frequency agility operation.

© 2008 Microchip Technology Inc.

5.2.5 Specifying PIC MCU Information

Select the **PIC** tab (refer to Figure 5-5).

FIGURE 5-5: ZENA™ STACK CONFIGURATION – MiWi™ P2P PROTOCOL WINDOW, PIC TAB



This tab is used to configure basic PIC MCU options.

TABLE 5-5: MiWi™ P2P PROTOCOL PIC® MCU 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 is accurate since all internal MiWi™ P2P protocol timing will be based off 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.

5.2.6 Generating the Configuration Files

When all of the options on the tabs are set appropriately, generate the Stack configuration file by clicking **Generate Files**. The ZENA analyzer will 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, `P2PDefs.h`. This file has a time and date stamp included in the file. This file is expected to be included in the application project to make all chosen configurations in the ZENA analyzer effective.

5.3 BASIC NETWORK MONITORING

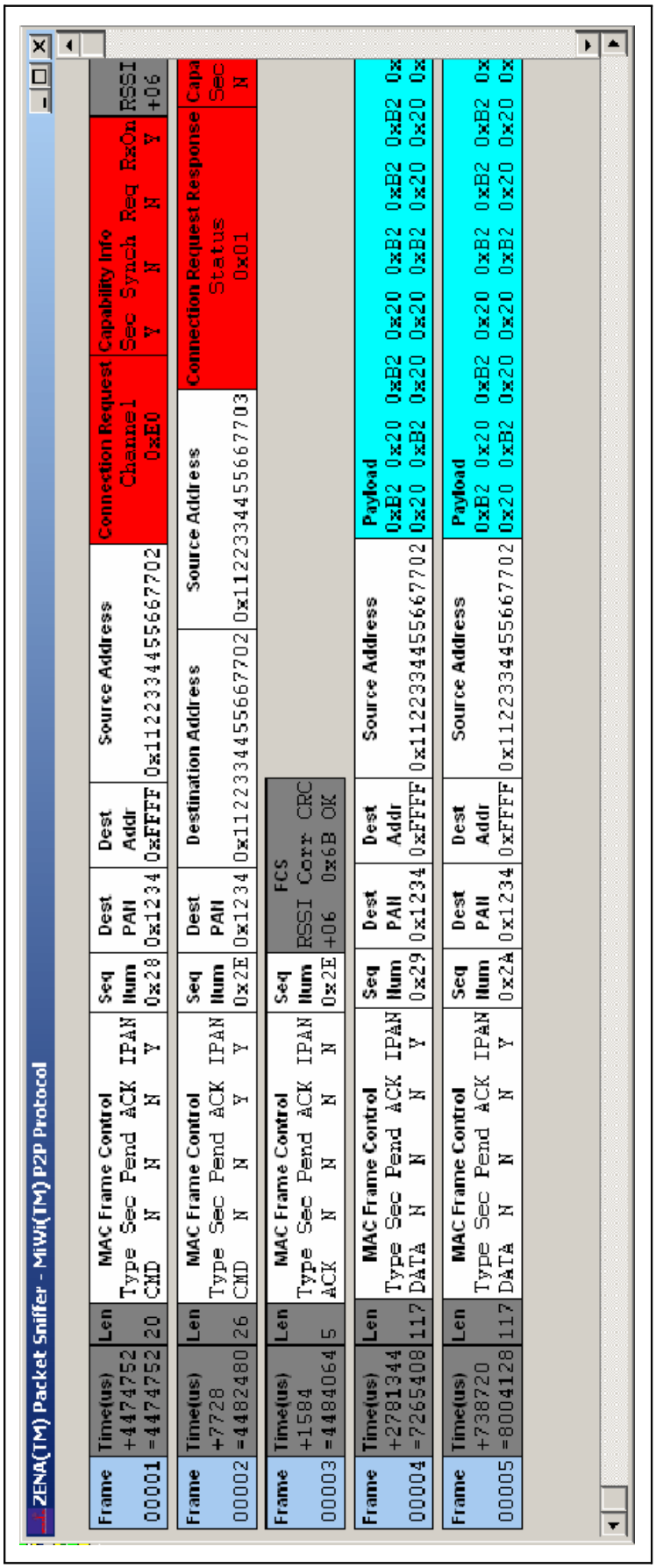
Basic monitoring of a MiWi P2P protocol network is nearly identical to that of a ZigBee protocol network. Please review **Section 3.3 "Basic Network Monitoring"**. This section focuses on the differences between the two protocols.

Select *MiWi P2P Tools> Network Traffic Monitor* to perform real-time network monitoring or packet analysis of a MiWi P2P protocol network. The fundamental MiWi P2P Network Monitor window is nearly identical to the ZigBee Network Monitor window.

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

© 2008 Microchip Technology Inc.

FIGURE 5-6: ZENA™ MiWi™ P2P PROTOCOL PACKET SNIFFER WINDOW



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

TABLE 5-6: MiWi™ P2P PROTOCOL PACKET SNIFFER COLOR CODING

Field	Color
MAC Header	White
MAC Commands	Red
MAC Data	Aqua
Encrypted Data	Blue

5.4 ADVANCED NETWORK MONITORING

Secure MiWi P2P protocol packets appear as shown in Figure 5-7.

When these packets are decrypted using the correct security key and security level, the packets appear as shown in Figure 5-8.

© 2008 Microchip Technology Inc.

FIGURE 5-7: SECURED MiWi™ P2P PROTOCOL PACKETS

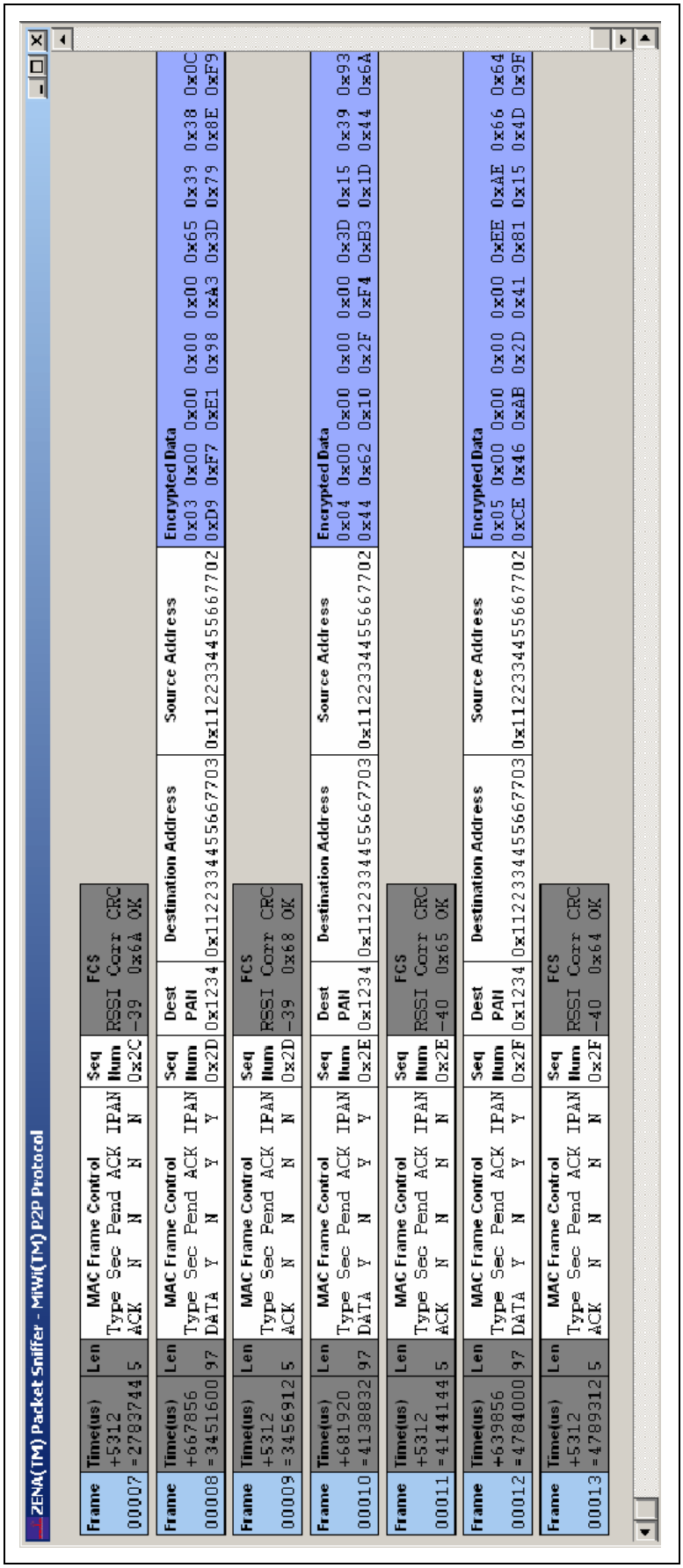


FIGURE 5-8: DECRYPTED OR UNSECURE MiWi™ P2P PROTOCOL PACKETS

ZENA(TM) Packet Sniffer - MiWi(TM) P2P Protocol

Frame	Time(us)	Len	MAC Frame Control					Seq Num	Dest PAN	FCS	Destination Address	Source Address	Payload
			Type	Sec	Pend	ACK	IPAN			RSSI Corr CRC			
00007	+5312 =27837444	5	ACK	N	N	N	N	0x2C	0x1234	-39 0x6A OK	0x1122334455667703	0x1122334455667702	0xB2 0xB2 0xB2 0xB2 0x20 0x20 0x20 0x20 0xB2 0xB2 0xB2 0xB2 0x20 0x20 0x20 0x20
00008	+667856 =35516009	97	DATA	Y	N	Y	Y	0x2D	0x1234				
00009	+5312 =34569125	5	ACK	N	N	N	N	0x2D	0x1234	-39 0x68 OK			
00010	+681920 =41388329	97	DATA	Y	N	Y	Y	0x2E	0x1234		0x1122334455667703	0x1122334455667702	0xB2 0xB2 0xB2 0xB2 0x20 0x20 0x20 0x20 0xB2 0xB2 0xB2 0xB2 0x20 0x20 0x20 0x20
00011	+5312 =41441445	5	ACK	N	N	N	N	0x2E	0x1234	-40 0x65 OK			
00012	+639856 =47840009	97	DATA	Y	N	Y	Y	0x2F	0x1234		0x1122334455667703	0x1122334455667702	0xB2 0xB2 0xB2 0xB2 0x20 0x20 0x20 0x20 0xB2 0xB2 0xB2 0xB2 0x20 0x20 0x20 0x20
00013	+5312 =47893125	5	ACK	N	N	N	N	0x2F	0x1234	-40 0x64 OK			

© 2008 Microchip Technology Inc.

Index

A

Additional Connection Payload 74
Advanced Network Monitoring 41, 66, 78
    Analyzing Traffic 53
    Configuration Display Window 41
    Customizing Configuration Display Window 48
    Viewing Formation 43
    Viewing Traffic 47
APS Configuration Selection (ZigBee)
    Binding Support 22
    Max APS ACK Frames Generated 22
    Max APS Addresses 22
    Max Frames From APL Layer 22

B

Basic Network Monitoring 64, 76

C

Configuration File Generation 27
Connections Table Size 74
Customer Change Notification Service 4
Customer Support 5

D

Data Polling 70
Device Configuration Selection (MiWi)
    Cluster Sockets 57
    Coordinator Capable 57
    EUI Address Search 57
    IEEE Device Type 57
    MAC Address 57
    Peer-to-Peer Capable 57
    Peer-to-Peer Only 57
    Peer-to-Peer Sockets 57
    Power Source 57
    Receive Network Address
        From Coordinator 57
    Transceiver Power 57
Device Configuration Selection (ZigBee)
    Alternate PAN Coordinator 13
    Available Power Sources 13
    IEEE Device Type 13
    Initial Power Source 13
    MAC Address 13
    Manufacturer Code (Hex) 13
    RFD Internal Data Request Rate 13
    Transceiver Power 13
    ZDO/APS/NWK/MAC 13
    ZigBee Device Type 13
Documentation
    Conventions 2
    Layout 1
    Revision History 5

F

Four-Device Network 46
Frequency Band 71

I

IEEE Device Type 70
Indirect Buffer Management 74
Installation
    License Agreement 9
    Readme File 9
    ZENA Software 9
Internet Address 4

K

Kit Contents 7
    USB mini-B Cable 7
    ZENA Wireless Network Analyzer 7
    ZENA Wireless Network Analyzer CD-ROM 7

M

MAC Address 70
MAC Configuration Selection (ZigBee)
    Battery Life Extension Mode 25
    Beacon Order 25
    Channel Energy Threshold 25
    Minimum Join LQI 25
    Receive Buffer Size 25
    Superframe Order 25
    Superframe Structure 25
    Transaction Persistence (seconds) 25
Microchip Internet Web Site 4
Microchip Stack Configuration Tool 55
MiWi P2P Protocol
    Additional Connection Payload 74
    Advanced Network Monitoring 78
    Basic Network Monitoring 76
    Connections Table Size 74
    Data Polling 70
    Device Configuration Selection 70
    Device Information 70
    Frequency Band 71
    Generating Configuration Files 76
    IEEE Device Type 70
    Indirect Buffer Management 74
    MAC Address 70
    NWK/MAC Configuration Setting 74
    Packet Sniffer Color Coding 78

PAN Identifier 74
PIC MCU Configuration Selection 75
Pin Assignment 71
Receive Buffer Size 74
Security Capable 72
Security Configuration Selection 72
Security Key 72
Security Level 72
Smallest Program Size 74
Specifying NWK and MAC Layer Information 73
Specifying PIC MCU Information 75
Specifying Security Information 72
Specifying Transceiver Information 71
Stack Configuration Tool 69
Support Active Scan 74
Support Energy Scan 74
Support Frequency Agility 74
Transceiver 71
Transceiver Configuration Selection 71
Transmit Buffer Size 74
MiWi Protocol Information 55
MPLAB IDE 1

N

NCD APS Acknowledge Path 47
NCD Association Request 44
NCD Association Response 45
NCD Beacon 44
NCD Beacon Request 43
NCD Configuration Selection (ZigBee)
Clear All Lines 42
Clear All Message Lines 42
Clear Background 42
Clear NCD 42
Select Bitmap 42
Show Last Messages 42
NCD Message Path 47
Network Monitoring 28
Node Colors 42
NWK and MAC Layer Specifying 24
NWK Configuration Selection (ZigBee)
Max Buffered Broadcast Messages 25
Max Buffered Routing Messages 25
Neighbor Table Size 25
Reserved Routing Table Entries 25
Route Discovery Table Size 25
Routing Table Size 25
NWK/MAC Configuration Selection (MiWi)
Data Request Rate (seconds) 62
Indirect Buffer Size (bytes) 62
Indirect Buffer Timeout (seconds) 62
Maximum Message Hops 62
Network Discovery Timeout (seconds) 62
Network Table Size 62
Open Cluster Socket Timeout (seconds) 62
Receive Buffer Size (bytes) 62
Transmit Buffer Size (bytes) 62

P

Packet
Exporting Data 53
Filter Use 37
Hiding and Unhiding 39
Playback 36
Playback Selection (ZigBee)
2 sec 36
Instant 36
Manual 36
x0.01 36
x0.1 36
x1 36
x10 36
x100 36
Packet Sniffer Color Coding (MiWi)
MAC Commands and Beacons 66
MAC Header 66
Message Data 66
Message Header 66
NWK Header 66
Security Header and Encrypted Data 66
Packet Sniffer Color Coding (ZigBee)
APS Header 31
APS Payload/Decoding 31
MAC Commands and Beacons 31
MAC Header 31
NWK Commands 31
NWK Header 31
Security Header and Encrypted Data 31
Unknown 31
PAN Identifier 74
PIC Configuration Selection (MiWi P2P)
Clock Frequency (Hz) 75
Output Stack Messages to UART1 75
Target Device Family 75
PIC Configuration Selection (MiWi)
Clock Frequency (Hz) 63
Output Stack Messages to UART1 63
Target Device Family 63
PIC Configuration Selection (ZigBee)
Build Target 27
Clock Frequency (Hz) 27
Heap Size (banks) 27
MAC Address Stored Externally 27
NCS 27
Program Memory 27
Serial EEPROM 27
SPI 27
SPI Serial EEPROM 27
Stack Size (banks) 27
Target Device 27
UART Baud Rate 27
Verify Writes 27
PIC MCU Specifying 26
Pin Assignment 71
Previously Captured Data Analyzing 36

© 2008 Microchip Technology Inc.

Profile and Endpoint
Specifying 15
Profile/Endpoints Configuration
Selection (ZigBee)
Device 16
Endpoints 16
Profile Header File 16
Protocol Device Configuration
Selection (ZigBee)
Key Present in All Devices on the Network..... 18
Network Key Present 18
Security Capable 18
Security Mode 18
Trust Center 18
Trust Center Address 18

R

Real-Time Network Monitoring..... 29
Real-Time Network Monitoring Configuration
Selection (ZigBee)
Auto Scroll 29
Channel 29
Clear Messages on Start 29
Ignore Invalid Packets 29
Real-Time Display 29
Receive Buffer Size 74
Recommended Reading 3
AN1066, MiWi Wireless Networking
Protocol Stack 3
AN965, Microchip Stack for the
ZigBee Protocol 3
IEEE 802.15.4 Specification 3
Microchip 8-Bit Microcontroller Solutions..... 3
PIC MCU Data Sheets, Family
Reference Manuals 3
PICDEM Z Demonstration Kit User's Guide 3
Readme for ZENA Wireless
Network Analyzer 3
ZigBee Protocol Specification 3

S

Security Capable 72
Security Configuration Selection 72
Security Configuration Selection (MiWi)
Security Capable 60
Security Key 60
Security Level 60
Security Key 72
Security Level 72
Smallest Program Size..... 74
Stack Configuration Tool.....11, 69
Support Active Scan 74
Support Energy Scan 74
Support Frequency Agility 74

T

Time-Stamps 36
Transceiver 71
Specifying 14
Transceiver Configuration Selection (MiWi)
Allowed Channels 59
Demo Board Defaults..... 59
Frequency Band..... 59
Output Power 59
Pin Assignments 59
Transceiver 59
Transceiver Configuration Selection (ZigBee)
Allow Shared SPI 14
Allowed Channels 14
Frequency Band..... 14
Output Power 14
PICDEM Z Pins..... 14
Pin Assignments 14
Transceiver 14
Transmit Buffer Size..... 74
Two-Device Network 45

U

USB mini-B Cable 28

V

Verboseness Level Configuration
Selection (ZigBee)
Condensed..... 33
Numeric..... 33
Verbose..... 33

W

WWW Address 4

Z

ZDO and APS Layer
Specifying 19
ZDO Configuration Selection (ZigBee)
Include Optional Node
Management Services..... 20
Include Optional Service
Discovery Requests..... 20
Support End Device Binding 20
ZENA Analyzer
Overview 7
ZigBee Protocol Device
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
Harbour City, Kowloon
Hong Kong
Tel: 852-2401-1200
Fax: 852-2401-3431

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

China - Beijing
Tel: 86-10-8528-2100
Fax: 86-10-8528-2104

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Taiwan - Hsin Chu
Tel: 886-3-572-9526
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

01/02/08

© 2008 Microchip Technology Inc.