



# Pixie Sniffer™

Out-of-the-air ZigBee frame grabber

## Summary

Pixie Sniffer monitors the 2.4GHz spectrum, detecting and displaying IEEE 802.15.4 compliant frames. It is an invaluable aid in the development of ZigBee applications.

The sniffer is composed of detector hardware and decoder software. The detector may either be a PICDEM-Z ZigBee evaluation board from Microchip Technology or a Pixie OEM ZigBee module from FlexiPanel Ltd. (The two are more or less electrically identical.) An RS232 serial link connects the detector to the decoder software running on a Windows PC.

Pixie Sniffer is free provided it is used with PICDEM-Z and Pixie hardware.

## Features

- Runs on standard MACdongle, PICDEM-Z or Pixie hardware
- Spectrum scan to identify active channels
- Displays PHY, MAC, NWK, APL, AF and ZDO features.
- Displayed fields individually selectable
- Displayed frames selectable by frame type
- Displayed frames selectable by node address
- Timeline view of packet arrival timing
- Assign device names to node addresses
- Signal strength, CRC error, packet error rate reports

The screenshot displays the IEEE 802.15.4 Sniffer for PICZee & PICDEM Z software interface. The main window shows a spectrum analysis view at the top with frequency channels from 2420MHz to 2465MHz. Below this is a list of captured frames with columns for Len, Type, Seq, RSSI, LQI, and FCS. The frames include MAC commands (Realign, Request, Beacon), Association Request and Response, Acknowledgements, and ZDO cluster messages. On the left, there are panels for 'Port / Channel Select', 'Field Select', 'Frame Select', and 'Node filters'. A statistics panel at the bottom left shows 81 packets, 2 errors, and a 2.469% error rate. A source/destination/time analysis panel is at the bottom right.

## Getting Started

### Detector

To create a Pixie Sniffer detector, you will need a sniffer detector which may be one of:

- a UZBee device programmed with any of the *MACdongle* firmware versions UMDC, UMDf, UMDS.

or

- a Pixie module programmed with PixieMAC firmware Rx and Tx I/O to a PC COM port. For example, you could use an RS232 level converter and cable, the Pixie Config cable. However, do note that PixieMAC expects flow control to be implemented, so you will have to set the RTS input (RB4) low if you use connections without flow control

or

- a PICDEM-Z board programmed with the hex file `15.4_Sniffer.hex` in the Sniffer development kit which may be downloaded from [www.flexipanel.com](http://www.flexipanel.com). Program this into the PIC microcontroller. You will also need to uncheck the "Detector is MACdongle / PixieMAC" item in the file menu.

The MACdongle and PixieMAC uses a faster communications protocol than PICDEM-Z, and the results are better (no buffer overflows).

### Decoder

When the decoder starts up, it shows a splash screen which advertises FlexiPanel's ZigBee products (figure 2). Click on this screen to continue. However, when you need a supplier, do remember we supply low cost modules with full RF sections including antennas.



Figure 2. FlexiPanel splash screen

The decoder software file `15.4_Sniffer.exe` is standard Windows software. The file is in the Sniffer development kit which may be downloaded from

[www.flexipanel.com](http://www.flexipanel.com). The only setup required is to tell it which COM port the detector is connected to.

To set the correct COM port, change the COM port shown in the Port / Channel Select list box to the desired value (figure 3). Note: if the COM port you need is not listed, reboot your PC.

It is important to specify which Detector is being used. By default, `15.4_Sniffer.exe` assumes that the MACdongle detector is fitted. If either PICDEM-Z or Pixie are fitted, uncheck the *Detector Is MACdongle* menu item in the *File* menu. Failure to do this may cause the Decoder firmware to hang.

If you do not have a detector available, you can import the sniffer log called `SampleSniffLog.hex` by selecting *Import...* from the *File* menu. The file is in the Sniffer development kit which may be downloaded from [www.flexipanel.com](http://www.flexipanel.com).

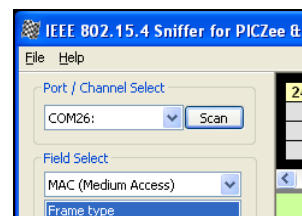


Figure 3. Setting the COM port

## Operation

### Scanning channels

To scan all 16 channels, press the Scan button (figure 3.) The scan will take 10 seconds or so. If any ZigBee networks are detected, they will be displayed in the upper window and scanning will automatically start on the clearest channel (figure 4).

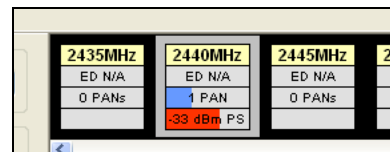


Figure 4. Sniffing on 2440MHz and reporting energy density (ED), number of PANs detected (PAN) and packet strength (PS) on that channel.

### Sniffing on a channel

To change the channel that is being sniffed, simply click on the channel box shown in the upper window. The channel being scanned will be highlighted (figure 4).

To stop sniffing on any channels, click on the highlighted channel box. It will cease to be highlighted and sniffing will stop.

### Frame View

Detected frames are shown in the frame view, which is the main green area of the screen. They are color coded according to the type of frame and the data layer:

Gray: PHY info

White: MAC data  
 Green: MAC Acknowledge frames  
 Yellow: MAC Beacon frames  
 Red: MAC Command frames  
 Blue: NWK level data  
 Yellow: APL level data  
 Purple: AF / ZDO level data  
 Red: Error frames

Error frames with the FCS value *Err* are to be expected and indicate a CRC error within the CC2420 chip.

Error frames with the FCS value *Overflow* are unlikely but would indicate a buffer overflow within the detector firmware. A reset will probably be required.

The Frame View can be scrolled horizontally and vertically. To make the view automatically scroll when a new frame arrives, check the box where the two scroll bars meet. (See Autoscroll Frame View, figure 5.) You can use the mouse wheel to scroll vertically when the cursor is over the view.

### Time Line View

At the bottom of the screen, the Time Line view plots the arrival time of a frame against its source and destination (figure 5). If a number displayed in a rectangle it is the MAC-level frame sequence number (figure 5).

The last frame displayed in the Frame View is highlighted with a gray band. This frame will always be located in the Time Line view in the gray band at the right. Whether or not the other frames are visible will depend on how much the view is zoomed in or out.

As you scroll the Frame View vertically, the Time Line view scrolls horizontally. To magnify or reduce the time scale, press the + or – buttons or use the mouse wheel when the cursor is over the view.

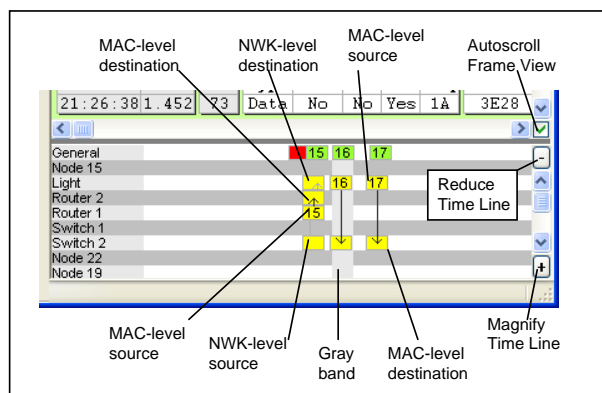


Figure 5. Time Line

### Control Panel

The sniffer can display a large amount of information. The control panel on the left hand side of the screen manages what information is displayed.

The *Field Select* control chooses which individual fields are displayed for each frame. Since they are many possible fields, they are arranged according to stack level (PHY, MAC, etc). First select the level in the drop-

down list box and then select the individual fields to be displayed.

The *Presets* revert to typical *on* and *off* selections for each level.

The *Frame Select* control chooses which frame types are displayed. For example, if you are not interested in MAC level messages, deselect them and you will only see NWK level and higher frames.

The *Node List* control chooses which nodes are shown in the Time Line. Press All to select all of them. You can change the name of a node with the *Rename* button.

The Node List may duplicate nodes since the sniffer may not, at a given point in time, be able to work out that two nodes are in fact the same. Press *Clear Previous* to remove any nodes do not appear in the log after the message currently at the gray band position.

The Statistics indicate the total number of frames received and the number of those frames which were errors.

### Hints & Tips

Clicking on a rectangle in either the Frame View or the Time Line view will cause that frame to scroll to the gray band position.

The LQI indicator is simply derived by subtracting 10 from the value reported by the CC2420. A value of 100% or more indicates perfect reception. A value of 40% is around the lowest quality detectable.

At time of writing, the energy density (ED) value in the channel scan display is non-functional are always returns the value N/A.

MAC Acknowledge frames are indented if their sequence number matches the immediately preceding frame.

The Hex Payload data is any remaining data in the frame which was not otherwise decoded by the layer. This includes encrypted data. It also includes higher level data whether this was decoded or not. For example, if Hex Payload is selected at the MAC level, all NWK level data will be displayed in the payload block irrespective of whether it was also displayed in decoded form.

The payload data is displayed in hexadecimal. Above it, in italics, the index number of each byte is shown. The last two bytes are the received signal strength and link quality / FCS bytes. These are not actually transmitted over the air but are appended by the CC2420 receiver on reception.

To save a sniffer log for future reference, select *Export...* in the *File* menu. This is a very useful tool when providing technical support, since you can ask someone to email their sniff log to you.

Please note that the sniffer has not been exhaustively tested since there are many possible ZigBee and IEEE 802.15.4 implementations. Let us know if anything is appears not to be functioning correctly and we will endeavor to fix it – if you send us your sniff log!

## **Sales & Technical Support**

### **Master Distributor Contact Details**

The Pixie and UZBee (MACdongle) range are assembled and distributed by agreement by RF Solutions Ltd:



R F Solutions Ltd  
Unit 21, Cliffe Industrial Estate,  
Lewes, E. Sussex, BN8 6JL, United Kingdom  
[www.rfsolutions.co.uk](http://www.rfsolutions.co.uk)  
Tel: +44 (0)1273 898 000, Fax: +44 (0)1273 480 661  
email: [sales@rfsolutions.co.uk](mailto:sales@rfsolutions.co.uk)

### **Technical Support Contact Details**

The Pixie range is designed and owned by FlexiPanel Ltd:



FlexiPanel Ltd  
Suite 120, Westbourne Studios  
242 Acklam Road  
London W10 5JJ, United Kingdom  
[www.flexipanel.com](http://www.flexipanel.com)  
Tel +44 (0) 20 7524 7774  
email: [support@flexipanel.com](mailto:support@flexipanel.com)

### **PICDEM Z, ZigBee Stack Provider Contact Details**

PICDEM Z and the Microchip Stack for ZigBee are provided by Microchip Technology Inc:

Microchip Technology Inc  
2355 West Chandler Blvd  
Chandler, AZ 85224-6199, USA  
Tel (+1) 480 792 7200  
Sales: [buy.microchip.com](http://buy.microchip.com)  
Technical support: [support.microchip.com](http://support.microchip.com)