FlexiPanel

Pixie Sniffer™

Out-of-the-air ZigBee frame grabber

Summary

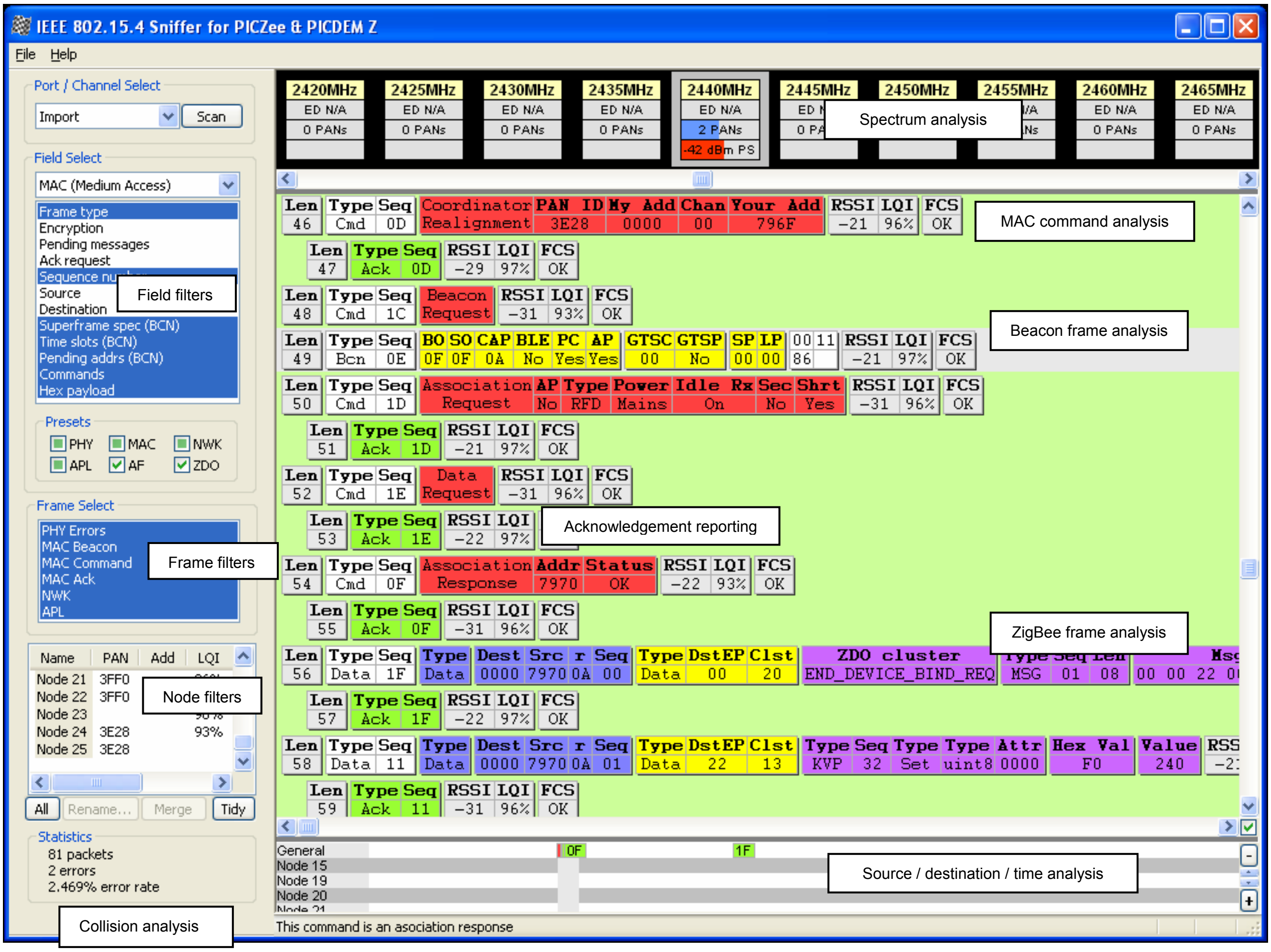
Pixie Sniffer monitors the 2.4GHz spectrum, detecting and displaying IEEE 802.15.4 compliant frames. It is an invaluable aid in the development of ZigBee applications.

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*



Port / Channel Select: Import — Scan

Field Select: MAC (Medium Access)

Frame type
Encryption
Pending messages
Ack request
Sequence number
Source
Destination
Superframe spec (BCN)
Time slots (BCN)
Pending addrs (BCN)
Commands
Hex payload

Presets: ■ PHY ■ MAC ■ NWK ■ APL ☑ AF ☑ ZDO

Frame Select:
PHY Errors
MAC Beacon
MAC Command
MAC Ack
NWK
APL

Name	PAN	Add	LQI
Node 21	3FF0		
Node 22	3FF0		
Node 23			
Node 24	3E28		93%
Node 25	3E28		

All — Rename... — Merge — Tidy

Statistics
81 packets
2 errors
2.469% error rate

```
2420MHz  2425MHz  2430MHz  2435MHz  2440MHz    2445MHz  2450MHz  2455MHz  2460MHz  2465MHz
ED N/A   ED N/A   ED N/A   ED N/A   ED N/A     ED N/A   ED N/A   ED N/A   ED N/A   ED N/A
0 PANs   0 PANs   0 PANs   0 PANs   2 PANs     0 PANs   0 PANs   0 PANs   0 PANs   0 PANs
                                    -42 dBm PS
```

```
Len Type Seq Coordinator PAN  ID My  Add Chan Your  Add RSSI LQI FCS
 46 Cmd  0D  Realignment  3E28    0000    00    796F     -21  96% OK
  Len Type Seq RSSI LQI FCS
   47 Ack  0D  -29  97% OK
Len Type Seq Beacon  RSSI LQI FCS
 48 Cmd  1C  Request -31  93% OK
Len Type Seq BO SO CAP BLE PC  AP  GTSC GTSP SP LP 00 11 RSSI LQI FCS
 49 Bcn  0E  0F 0F 0A  No  Yes Yes  00   No  00 00 86    -21  97% OK
Len Type Seq Association AP Type Power Idle Rx Sec Shrt RSSI LQI FCS
 50 Cmd  1D    Request   No RFD  Mains    On   No  Yes  -31  96% OK
  Len Type Seq RSSI LQI FCS
   51 Ack  1D  -21  97% OK
Len Type Seq  Data   RSSI LQI FCS
 52 Cmd  1E  Request -31  96% OK
  Len Type Seq RSSI LQI
   53 Ack  1E  -22  97%
Len Type Seq Association Addr Status RSSI LQI FCS
 54 Cmd  0F    Response  7970   OK   -22  93% OK
  Len Type Seq RSSI LQI FCS
   55 Ack  0F  -31  96% OK
Len Type Seq Type Dest Src  r  Seq Type DstEP Clst    ZDO cluster        Type Seq Len       Msg
 56 Data 1F  Data 0000 7970 0A 00  Data  00    20  END_DEVICE_BIND_REQ  MSG  01  08  00 00 22 0
  Len Type Seq RSSI LQI FCS
   57 Ack  1F  -22  97% OK
Len Type Seq Type Dest Src  r  Seq Type DstEP Clst Type Seq Type Type  Attr Hex  Val Value RSS
 58 Data 11  Data 0000 7970 0A 01  Data  22    13  KVP  32  Set  uint8 0000    F0    240  -2
  Len Type Seq RSSI LQI FCS
   59 Ack  11  -31  96% OK
```

```
General   0F   1F
Node 15
Node 19
Node 20
Node 21
```

This command is an asociation response

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 *MACdongle* firmware,

or

- a PICDEM-Z board and RS232 cable for connection to a PC,

or

- a Pixie module with means to connect the TTL level Rx and Tx I/O to a PC COM port. For example, you could use an RS232 level converter and cable, or a LinkMatik Bluetooth module from FlexiPanel Ltd.

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

For PICDEM-Z and Pixie, the hex file `15.4_Sniffer.hex` contains the required firmware. The file is in the Sniffer development kit which may be downloaded from *www.flexipanel.com*. Program this into the PIC microcontroller.

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*. 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).

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 have 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*.

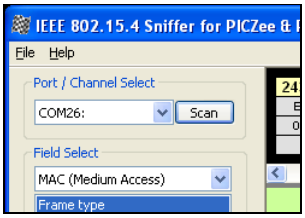


Figure 3. Setting the COM port

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).

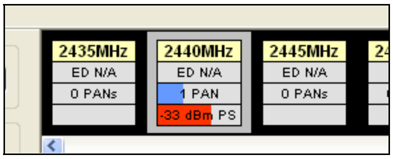


Figure 4. Sniffing on 2440MHz and reporting energy density (ED), number of PANs detected (PAN) and packet strength (PS) on that channel.

Sniffing on a channel

To change the channel that is being sniffed, simple 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 depends 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.

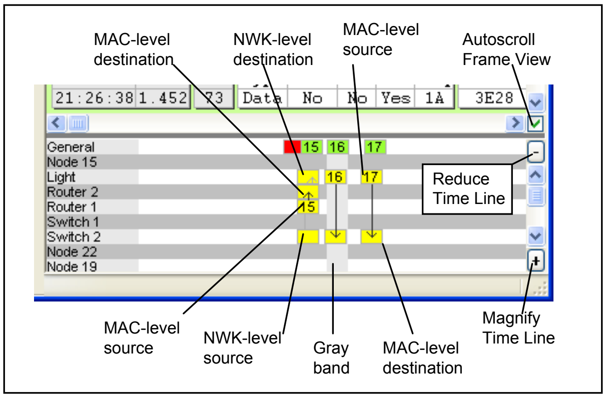


Figure 5. Time Line

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
Tel: +44 (0)1273 898 000, Fax: +44 (0)1273 480 661
email: sales@rfsolutions.co.uk

Technical Support Contact Details

The Pixie range is designed and owned by FlexiPanel Ltd:

FlexiPanel

FlexiPanel Ltd
Suite 120, Westbourne Studios
242 Acklam Road
London W10 5JJ, United Kingdom
www.flexipanel.com
Tel +44 (0) 20 7524 7774
email: 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*
Technical support: *support.microchip.com*