



ZB-2500 User Manual

For Packet Analysis!

ZB-2500 Wireless Detector User Manual

Warranty

All products manufactured by ICP DAS are warranted against defective materials for a period of one year from the date of delivery to the original purchaser.

Warning

ICP DAS assumes no liability for damages consequent to the use of this product. ICP DAS reserves the right to change this manual at any time without notice. The information furnished by ICP DAS is believed to be accurate and reliable. However, no responsibility is assumed by ICP DAS for its use, nor for any infringements of patents or other rights of third parties resulting from its use.

Copyright

Copyright © 2011 by ICP DAS. All rights are reserved.

Trademarks

Names are used for identification only and may be registered trademarks of their respective companies.

Table of Contents

1. Introduction	4
2. Specifications.....	5
2.1 Features	5
2.2 Specifications:	5
3. Product Description	6
3.1 Internal I/O Structure.....	6
3.2 Appearance	6
3.3 Dimensions (Units: mm).....	7
4. Quick Start for ZB-2500	8
4.1 Installing the ZB-2000 Driver	8
4.2 Installing the Hardware and Driver	10
4.3 Installing the ZB-2500 Utility.....	14
5. Instructions for using the ZigBee Sniffer Utility	16
5.1 Start the ZB-2500	16
5.2 The field of ZigBee Sniffer Utility Introduction.....	16
6. Applications and Usage.....	18
6.1 The ZigBee slave is not displayed in the Topology Tool	18
6.2 The quality of the communication is not good.....	19
6.3 Transmission is unstable, and the Net LED indicator of ZigBee slave sometimes begins blinking for a short time before returning to a steady state.	20
7. Appendix	21
8. Ordering Information	22
9. Accessories	22

1. Introduction

ZigBee is a specification based on the IEEE 802.15.4 standard for wireless personal area networks (WPANs). ZigBee operates in the ISM radio bands and its focus is to define a general-purpose, inexpensive, self-organizing, mesh network that can be used for industrial control, embedded sensing, medical data collection, smoke and intruder alerts, building automation, and home automation, etc.

The ZB-2500 is a ZigBee packet sniffer that is designed to provide detection and analysis of signal from for every ZigBee module in the ICPDAS. When install the ZigBee modules on-site, the ZB-2500 is helpful in identifying the best signal location which will allow optimum layout for best ZigBee network topology to be determined.

Another application of the ZB-2500 is in situations, when a ZigBee module fails or if transmission efficiency is bad. In this case, the ZB-2500 can be used to detect the signal from a specific ZigBee node to determine the reasons for the failure.

The ZB-2500 also works in an adjustable 16 RF Channels and USB 1.1 and 2.0 interfaces are provided, meaning that it can be easily operated via a Windows-base utility. With the ZB-2500 on hand, a solution can always be found when encountering an error while installing ZigBee modules on-site for the first time.

2. Specifications

2.1 Features:

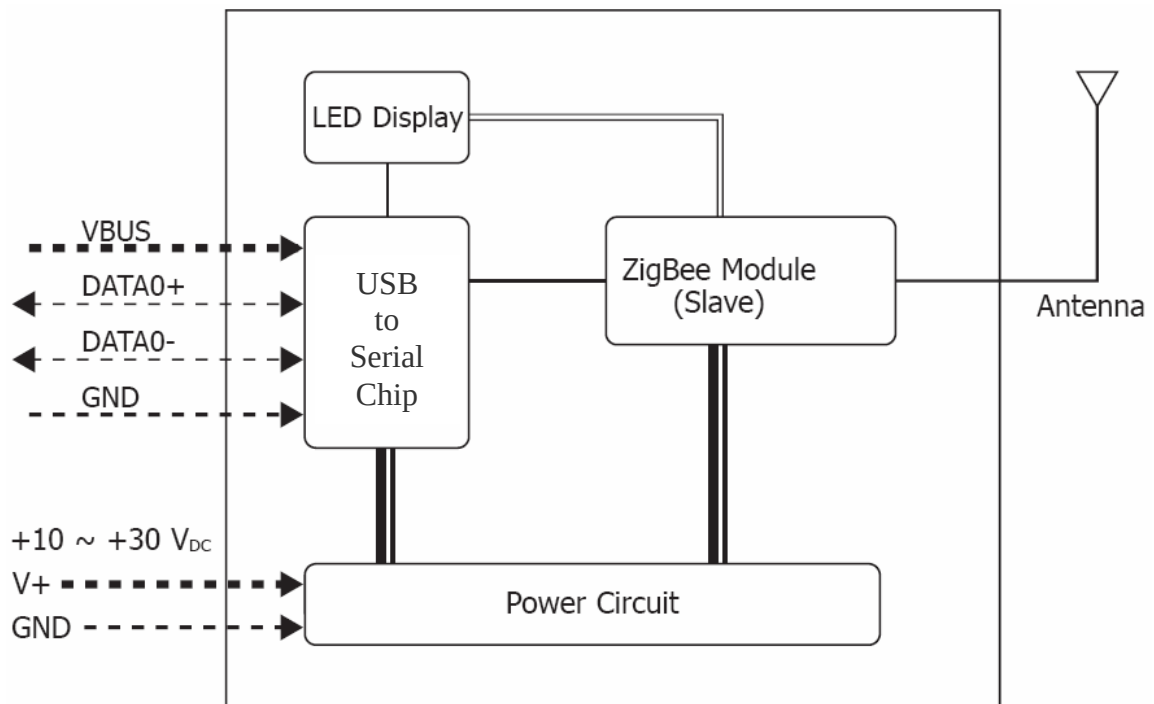
- ISM 2.4 GHz Operating Frequency
- Full Compliance with 2.4 G IEEE802.15.4/ZigBee Specifications
- USB Interface for configuration
- GUI Software (Windows Version)
- DIN-Rail Mountable

2.2 Specifications:

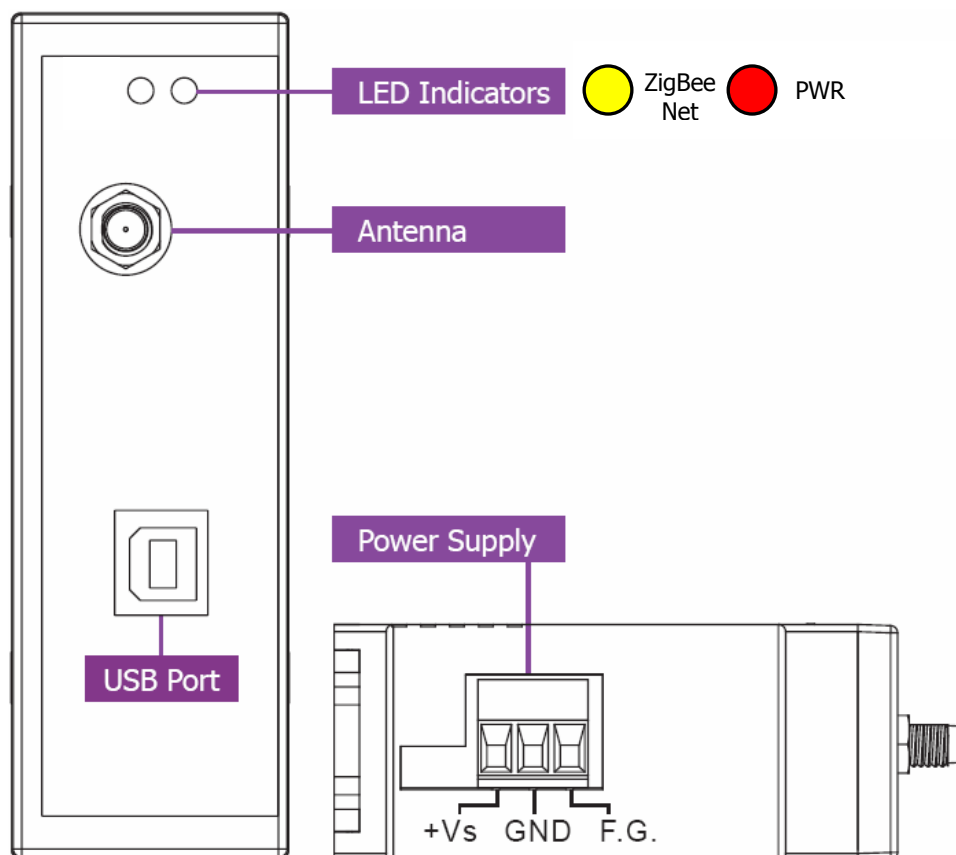
Wireless	
RF Channel	16
Receive Sensitivity	-102 dBm
Antenna (2.4 GHz)	3 dBi Omni-Directional antenna
Setting Interface	
USB	Type B
Included Cables	CA-USB18 (1.8 m Cable) x 1; USB Type A connector (Type A to Type B cable provided)
Compatibility	USB 1.1 and 2.0 standard
Supported Drivers	Windows 98/ME/2000/XP/Vista/Linux 2.6.19
LED Indicators	
Green	ZigBee Net State
Yellow	N/A
Red	Power
Power	
Protection	Power reverse polarity protection
EMS Protection	ESD, Surge, EFT
Required Supply Voltage	+10 V _{DC} ~ +30 V _{DC}
Power Consumption	1.5 W
Connection	3-pin 5.08 mm Removable Terminal Block
Mechanical	
Casing	Plastic
Flammability	UL 94V-0 materials
Dimensions (W × L × H)	33 mm × 78 mm × 107 mm
Installation	DIN-Rail
Environment	
Operating Temperature	-25°C ~ +75°C
Storage Temperature	-40°C ~ +80°C
Relative Humidity	5 ~ 95 % RH, non-condensing

3. Product Description

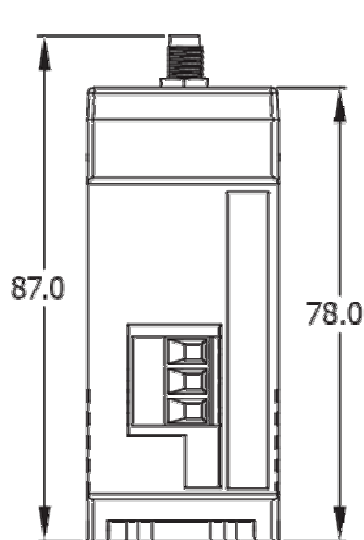
3.1 Internal I/O Structure



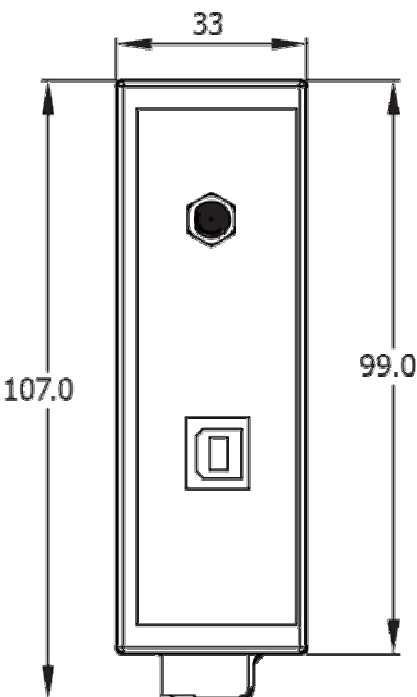
3.2 Appearance



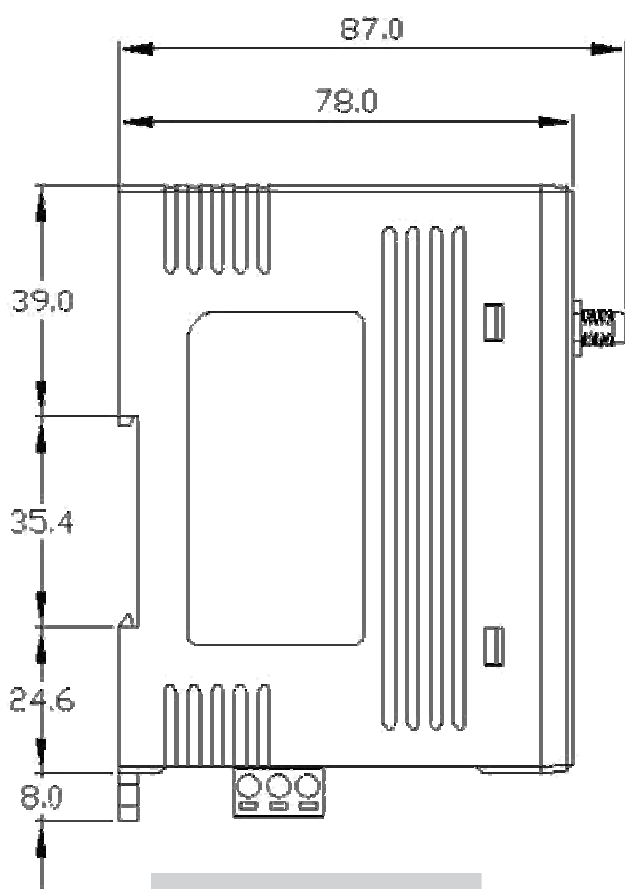
3.3 Dimensions (Units: mm)



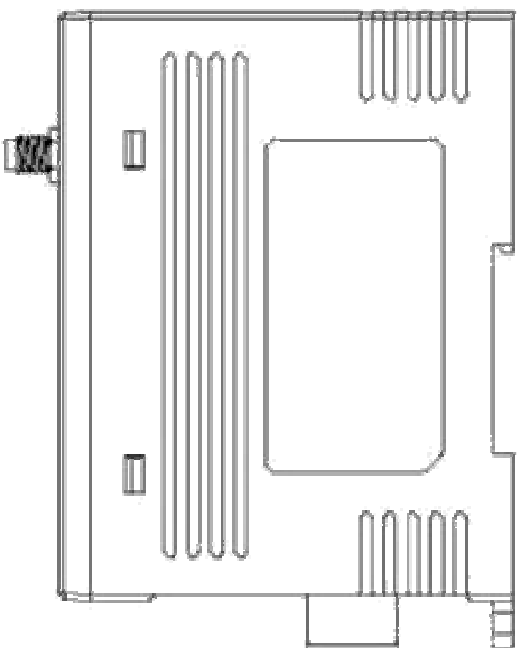
Bottom View



Front View



Left Side View



Right Side View

4. Quick Start for ZB-2500

4.1 Installing the ZB-2000 Driver

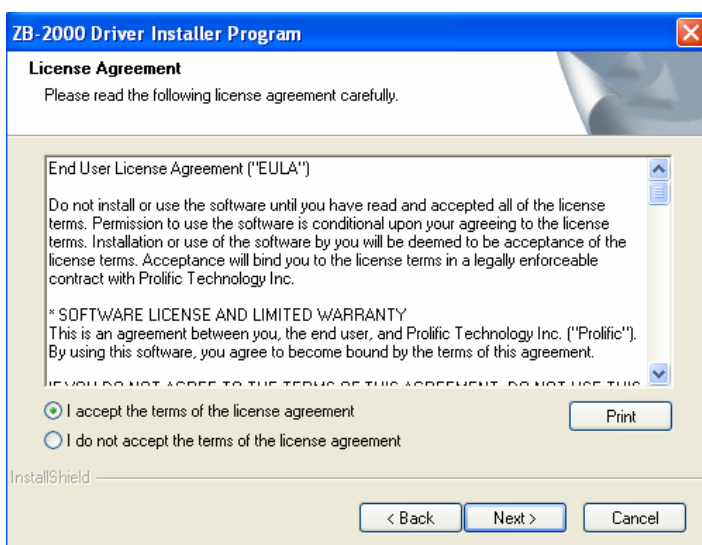
1. Download the driver file from:
http://ftp.icpdas.com.tw/pub/cd/usbcd/napdos/zigbee/zigbee_sniffer/zb-2500/driver
2. Uncompress the file and double click the "**ZB-2000 DriverInstaller.exe**" file to install the driver for the ZB-2500.



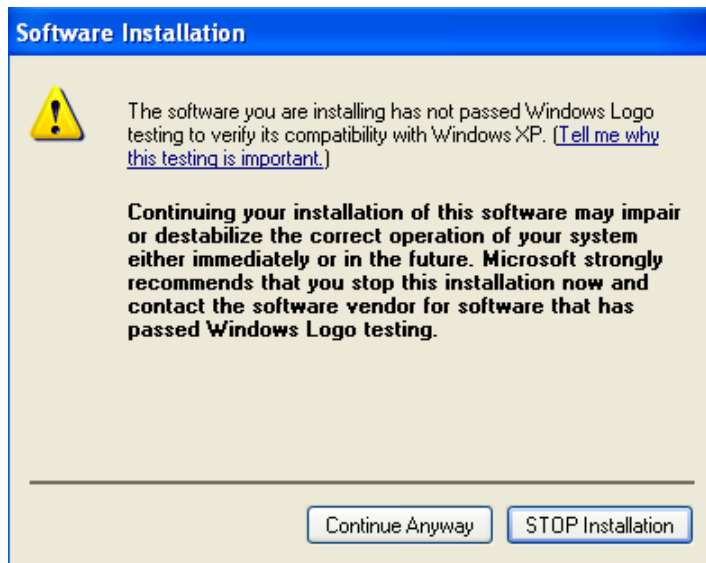
3. When the following screen is displayed, click the "**Next>**" button to continue the installation, or click the "**Cancel**" button to exit the installation.



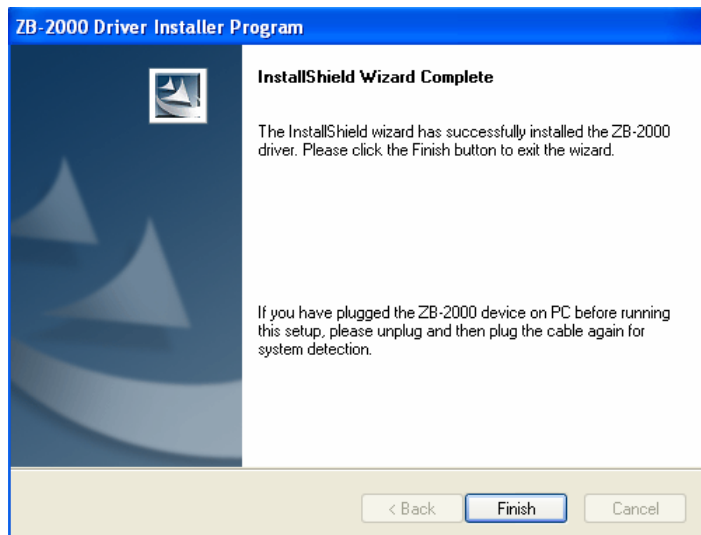
4. When the following screen is displayed, select the "I accept the terms of the license agreement." option, then click the "**Next>**" button to continue the installation, or click "**Cancel**" exit the installation.



5. When the following screen is displayed, click the “**Continue Anyway**” button to continue the installation, or click the “**STOP Installation**” button to exit the installation.



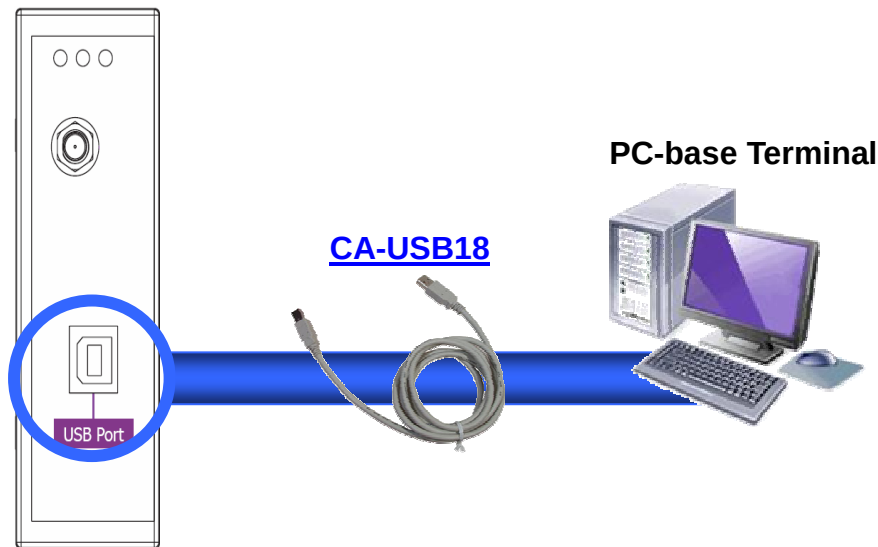
6. When the following screen is displayed, click the “**Finish**” button to finalize the software installation.



4.2 Installing the Hardware and Driver

1. Hardware Installation:

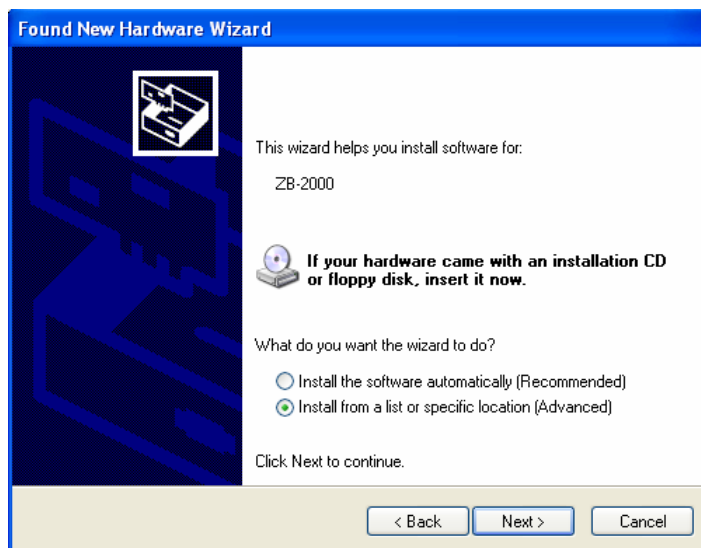
ZB-2500



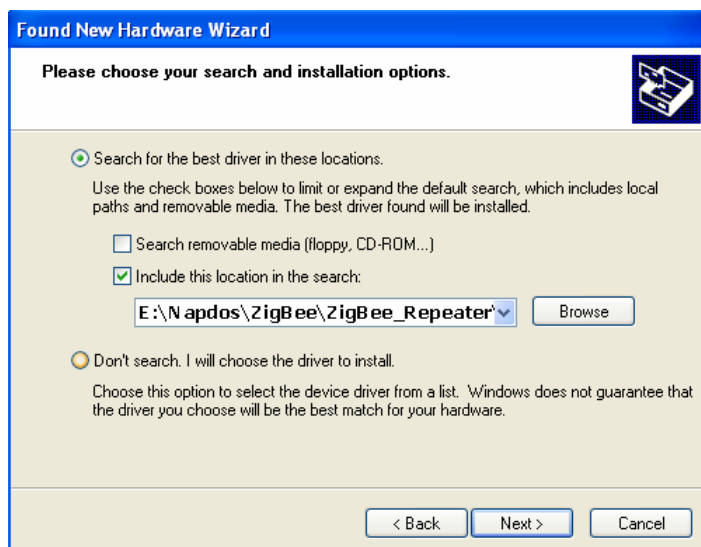
2. Once the module is connected and switched on the "Found New Hardware Wizard" prompting you to install the software for the detected USB Device. Select the "Yes, now and every time I connect a device" option and click the "**Next**" to button continue, or click the "**Cancel**" button to exit the installation.



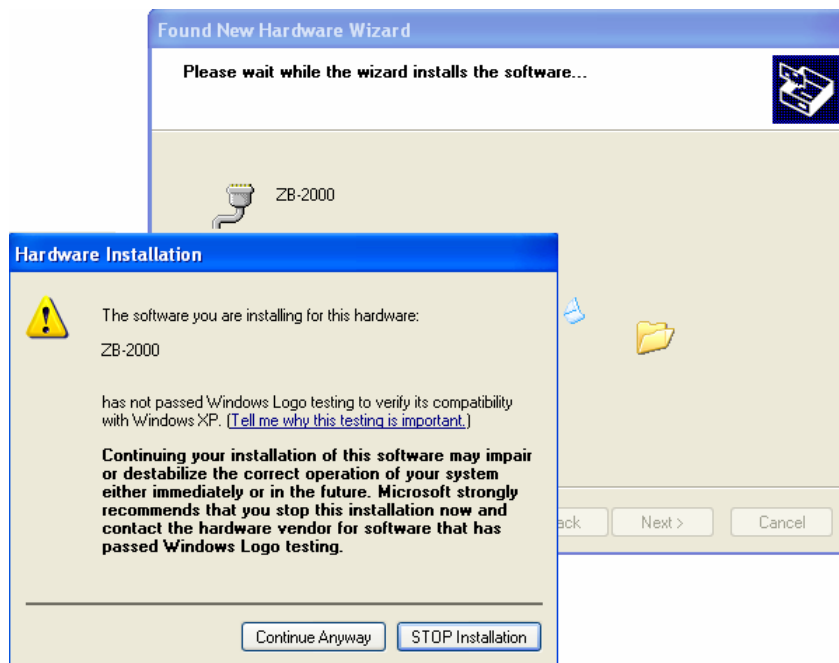
3. When the following screen is displayed, select the "Install from a list or specific location (Advanced)" option, then click the **"Next"** button to continue the installation. Click the **"Cancel"** button to exit the installation, or click the **"Back"** button to return to the previous screen.



4. Select the "Browse" button to the "Napdos\ZigBee\ZigBee_Sniffer\ZB-2500\Driver\ZB2000_Driver" folder to locate the installation file, and click the **"Next"** button to begin the search. Click the **"Cancel"** button to exit the installation, or click the **"Back"** button to return the previous screen.



5. When the following screen is displayed, click the **"Continue Anyway"** button to continue the installation, or click the **"STOP Installation"** button to exit the installation.

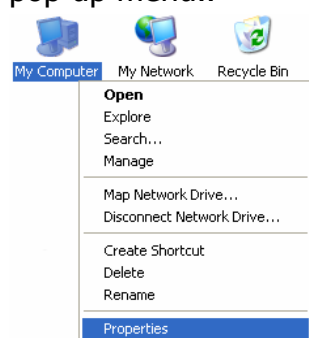


6. When the following screen is displayed, click the **"Finish"** button to finalize the software installation.



NOTE: When the driver installation is complete, disconnect the USB cable from the Host PC, and then reconnect it.

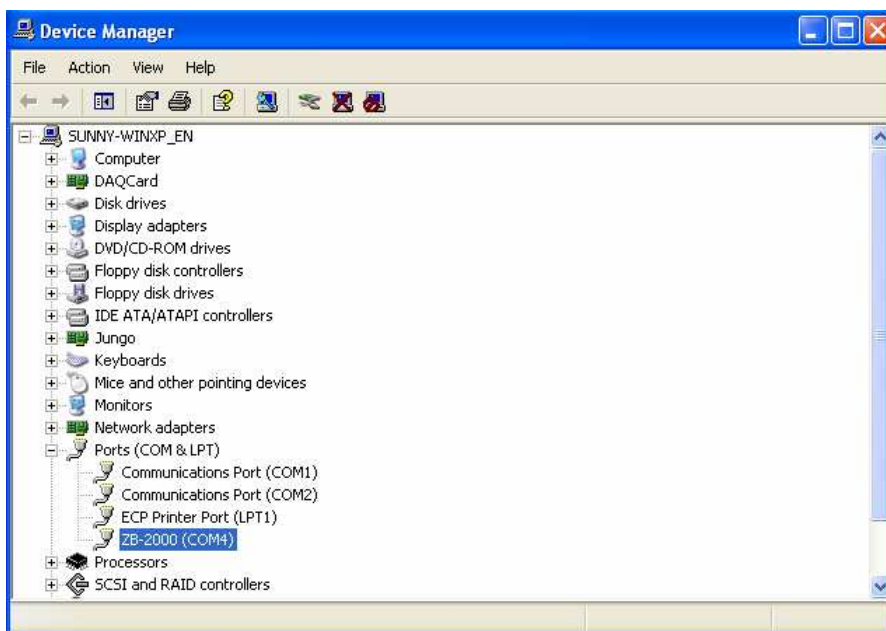
7. On your desktop, right click on the **"My Computer"** icon and select Properties from the pop up menu..



8. Click the **"Device Manager"** button in the System Properties dialog box.



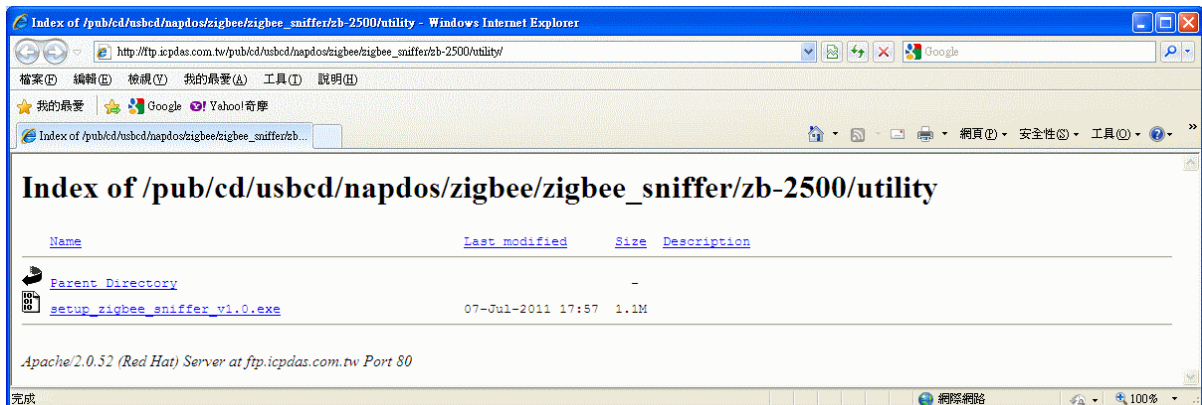
9. Confirm that the ZB-2000 (COM Number) driver is listed in the Ports (COM & LPT) section.



4.3 Installing the ZB-2500 Utility

- Download the installation file from:

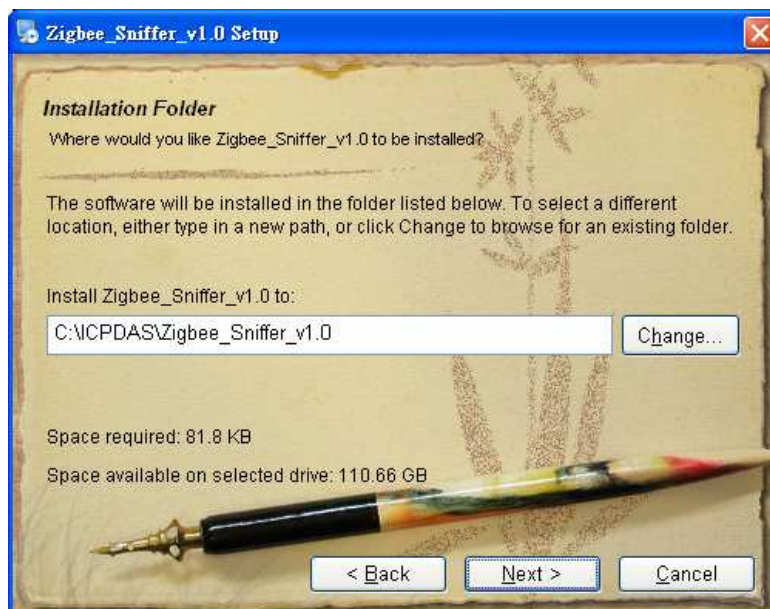
http://ftp.icpdas.com.tw/pub/cd/usbcd/napdos/zigbee/zigbee_sniffer/zb-2500/utility/



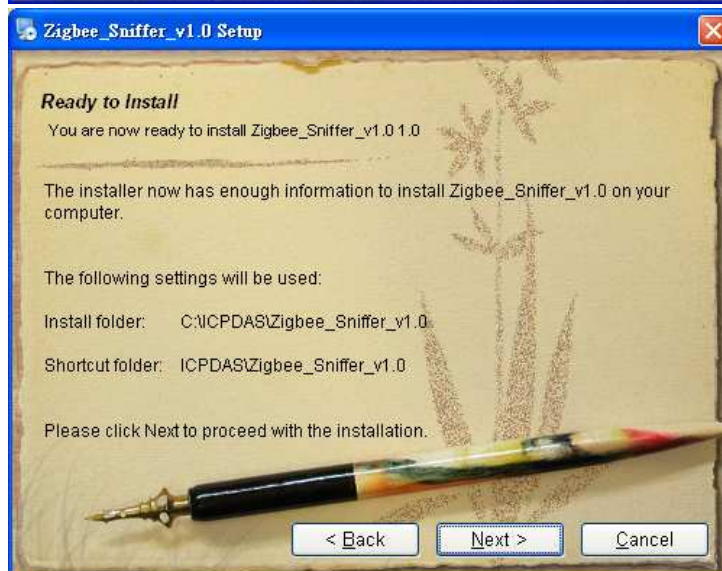
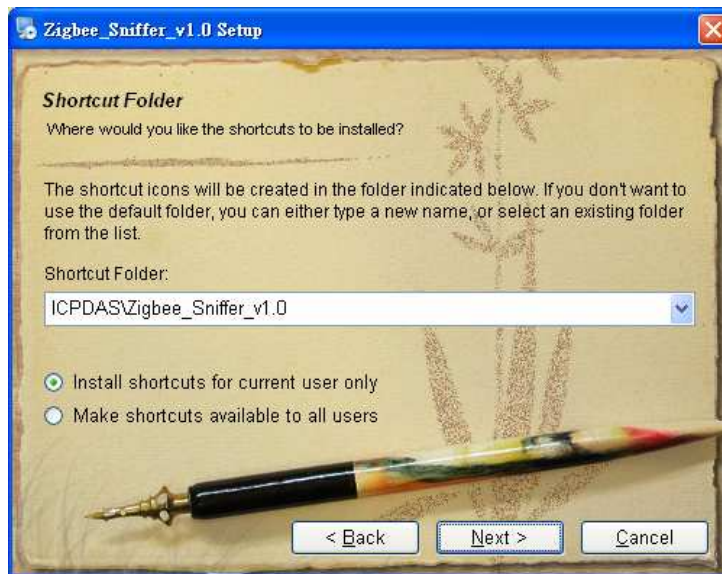
Double click the "**setup_zigbee_sniffer_vx.x.exe**" file to install the ZigBee Sniffer Utility for the ZB-2500 signal detector.



- When the following screen is displayed, either click the "**Next**" button to install the software into the default directory, or click the "**Change**" button to install the utility into an alternate location. Click the "**Cancel**" button to quit the installation, or click the "**Back**" button to return the previous screen.



- When the following screen is displayed, then click the **"Next"** button to continue the installation. Click **"Cancel"** button to exit the installation, or click the **"Back"** button to return the previous screen.



- When the following screen is displayed, click the **"Finish"** button to finalize the software installation.



5. Instructions for using the ZigBee Sniffer Utility

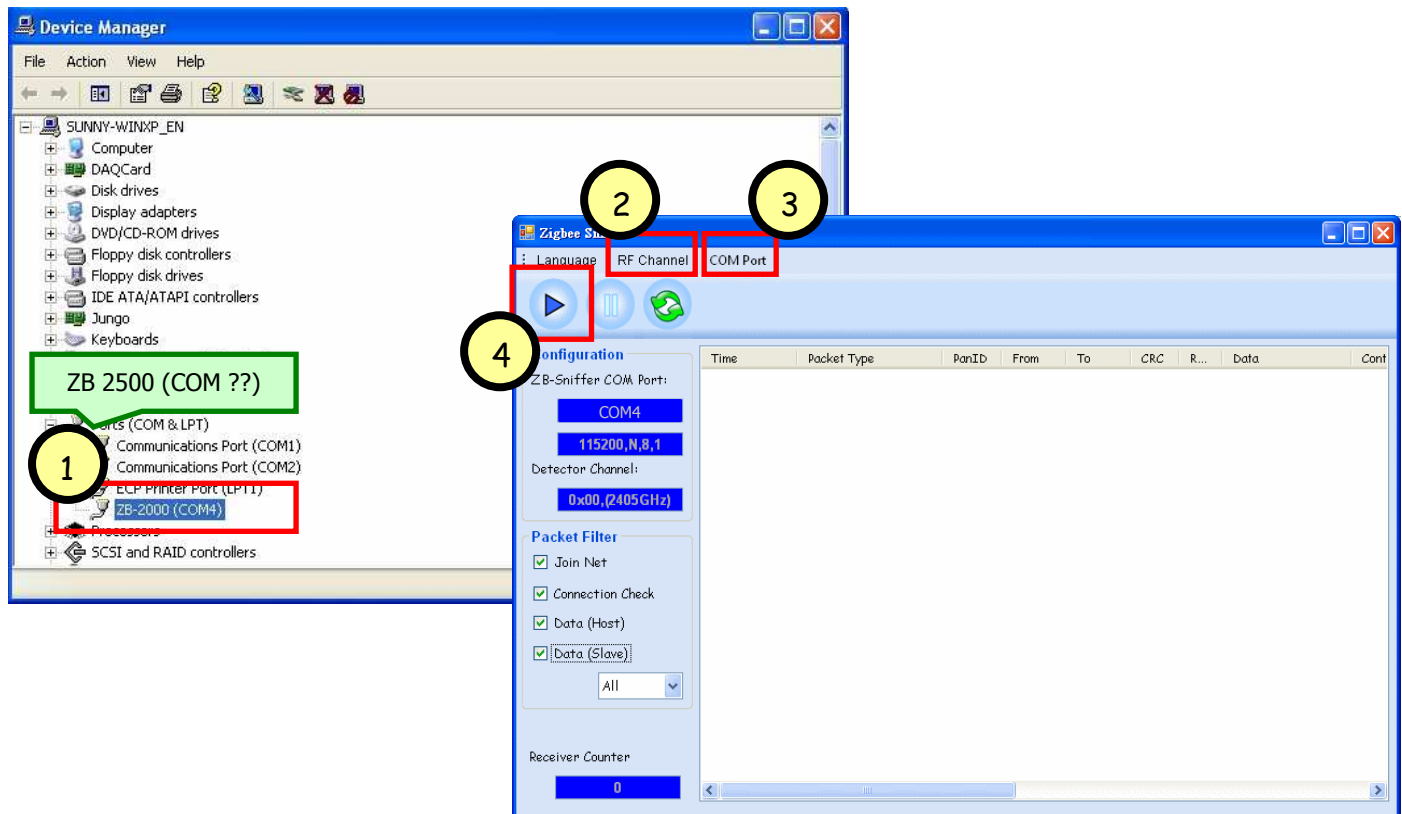
5.1 Start the ZB-2500

First, open the “**Device Manager**” by clicking on **Ports (COM & LPT)** and confirm the number of the COM Port allocated to the USB then launch the ZigBee Sniffer Utility.

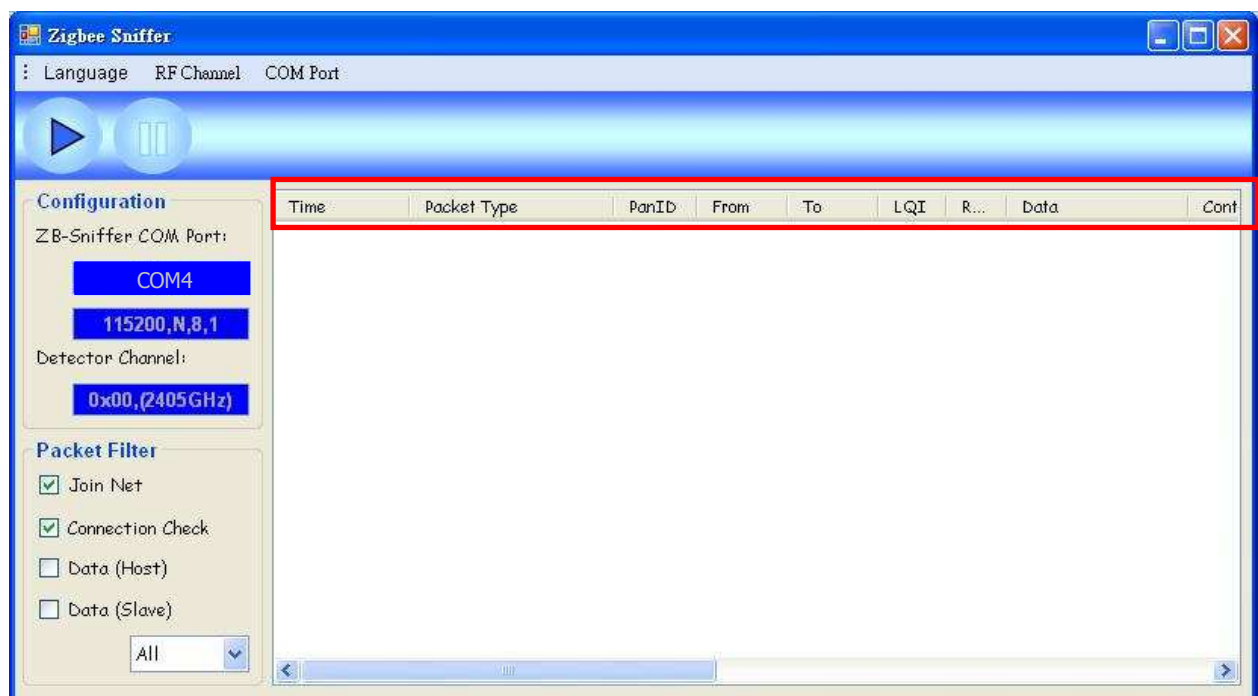
Next, click the menu to set the COM Port and open it.

The last, please choose a ‘RF channel’ that you want to detect and click the ‘Start button’ (▶).

The ZB-2500 will start to detect the ZigBee packets at selected RF frequency.



5.2 The field of ZigBee Sniffer Utility Introduction.



- 1. Time:** The actual time taken to receive a ZigBee packet.
- 2. Packet Type:** The packet header shows the packet type. Packet types are divided into either 'Join Network', 'Slave Connection Check' or 'Data transmission'.
- 3. Pan ID:** The logical ID. Only communication with the same Pan ID can be accepted.
- 4. From:** Shows which ZigBee module packet is derived from. The last 2 bytes of the address or the virtual address are shown in this column (also 2 bytes to represent).
- 5. To:** Shows the address that the packet being transmitted to. There is showing the last 2 bytes address or the virtual address (also 2 bytes to represent).
- 6. CRC Check:** The field shows the CRC check flag state. It usually shows "00" at most of time. When the transmission gets serious interference, the field may show "FF" and the background color will be red.
- 7. RSSI (Received Signal Strength Indication):** An important indicator to show the signal strength.
- 8. Data:** Shows the actual payload data in the packet.
- 9. Content:** Show the complete command type and data content.
- 10. From (64 bits):** This item is same as item (4). The effective address is the last 2 bytes, and the front 6 bytes should always be set to 0x000000000000.
- 11. To (64 bits):** This item is same as item (5). The effective address is the last 2 bytes, and the front 6 bytes should always be set to 0x000000000000.

4.3 Additional features in the ZigBee Sniffer Utility

1. Packet Filter:

Check or clear the checkbox in the 'Packet Filter' option to filter the packets you want to detect. Through packet filtering, the utility would only display useful information.

2. Multi-color at background:

Use different color backgrounds to distinguish between the sources of different ZigBee packet.

3. Warning indicator (!):

If the ZB-2500 receives a connection request packet from a slave to the host, an icon will be displayed in the utility to warn the user that a ZigBee device is requesting to join or rejoin the ZigBee network, allowing the user to determine whether the request is expected or not.

In addition, if the RF transceiver determines that the CRC check is illegal, a warning icon will also be displayed and background color will change to warn the user. If the CRC check error occurs too frequently, it may indicate that there is too much interference on the network.

6. Applications and Usage

When a ZigBee module is installed for the first time, the ZigBee Topology Utility Tool can be used to scan the state of the ZigBee network. If the connection to the ZigBee modules is lost or a timeout occurs frequently, the ZB-2500 can be used to detect the packet flow. With this details, a solution can be determined for improving the data transmission.

Some of the common problems are listed:

6.1 The ZigBee slave is not displayed in the Topology Tool

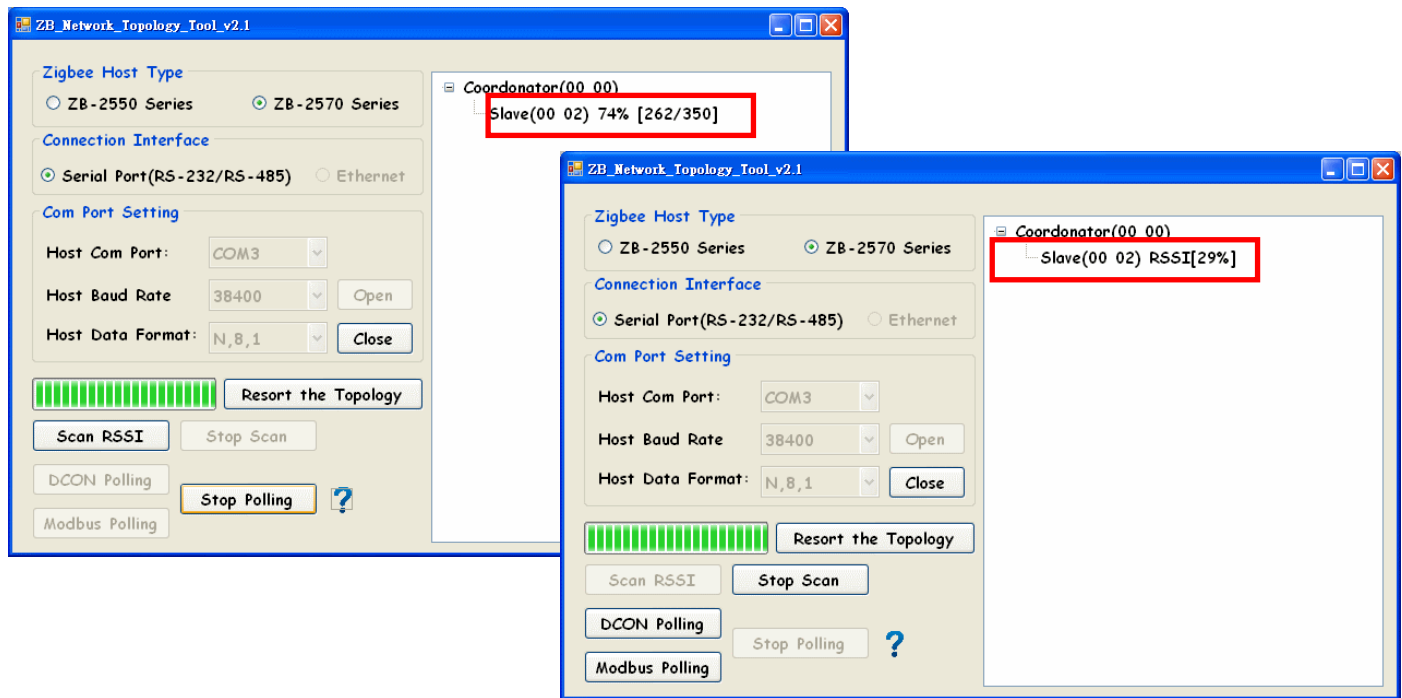
In this situation, confirm whether or not the target ZigBee slave module is continuing to send 0x30 (Init Net) packets.

- (1) If not, it indicates that the ZigBee slave is not working as expected. Confirm that the power supply is connected and that the RF channel settings are configured correctly.
- (2) If the ZB-2500 continue to receive 0x30 packets, confirm whether those value of 'Pan ID', 'To', and the 'RSSI' are correct or not.
 - A. Pan ID:** The 'Pan ID' must be set to same value as the Host.
 - B. To:** The 'To' field should show a value of '00 00' received during initialization. If a user-defined routing has been set for the ZigBee slave, confirm whether or not the connection to the target slave still exists.
 - C. RSSI:** If the RSSI value is less than 30 ~ 50%, it means that the signal strength is too weak to establish a connection. If the host is too far away from the ZigBee slave, a repeater can be added as a bridge to extend the transmission range. If the host is close to the ZigBee slave but the RSSI value is still low, it means that the hardware may be damaged.

The screenshot shows a table of ZigBee packet captures. A green box labeled 'Target ZigBee slave' points to the 'From' column. A red box highlights the 'PanID', 'From', 'To', and 'R...' columns. A red box labeled 'The signal strength is too weak.' points to the 'R...' column. Two red boxes at the bottom contain instructions: 'Confirm the Pan ID settings' and 'Confirm whether this node is still functioning.'.

Time	Packet Type	PanID	From	To	CRC	R...
1:50:53 PM	30 (Init_Net)	FF FF	00 01	Broadc...	00	99%
1:50:52 PM	30 (Init_Net)	FF FF	00 01	Broadc...	00	99%
1:50:52 PM	30 (Init_Net)	FF FF	00 01	Broadc...	00	99%
1:50:51 PM	30 (Init_Net)	FF FF	00 01	Broadc...	00	99%
1:50:51 PM	30 (Init_Net)	FF FF	00 01	Broadc...	00	99%
1:50:50 PM	30 (Init_Net)	FF FF	00 01	Broadc...	00	99%
1:50:50 PM	30 (Init_Net)	FF FF	00 01	Broadc...	00	99%
1:50:49 PM	30 (Init_Net)	FF FF	00 01	Broadc...	00	99%

6.2 The quality of the communication is not good.



In this situation, confirm the RSSI value first. If the RSSI value is not good enough to perform transmission, the ZB-2500 can be used to identify the location of the best signal in order to determine the ideal position for reinstalling the ZigBee module. Alternatively, a cable can be used to extend the length of the antenna.

If the RSSI value is higher than 90% but the PER (Packet Error Rate) is still not good enough, the ZB-2500 can also be used to confirm whether the signal is being affected by interference or not. If the ZigBee Sniffer Utility frequently shows CRC check error packets, it means that there is too much interference. An amplifier can be used to boost the signal strength so that the impact from the interference is minimized. An alternative solution is to use the ZB-2500 to determine the source of the interference and then use a ZB-repeater to by pass it. It should be noted that interference is usually related to high voltage power devices, so locating ZigBee modules near to the kind of high voltage devices or power supplies should be avoided.

The ZigBee is defined as low power transmission technology. Even if the RSSI value is adequate, interference from the power system may also occur.

Time	Packet Type	PanID	From	To	CRC	R...	Data
2:29:07 PM	46 (Mutil_Send)	FF FF	00 00	Broadc...	00	84%	01 01 01 05 00 05 ...
2:29:07 PM	46 (Mutil_Send)	FF FF	00 00	Broadc...	00	85%	01 01 01 05 00 05 ...
2:29:07 PM	46 (Mutil_Send)	FF FF	00 00	Broadc...	FF	85%	01 01 01 05 00 05 ...
2:29:07 PM	46 (Mutil_Send)	FF FF	00 00	Broadc...	FF	85%	01 01 01 05 00 05 ...
2:29:07 PM	46 (Mutil_Send)	FF FF	00 00	Broadc...	FF	84%	01 01 01 05 00 05 ...
2:29:07 PM	46 (Mutil_Send)	FF FF	00 00	Broadc...	00	85%	01 01 01 05 00 05 ...
2:29:06 PM	46 (Mutil_Send)	FF FF	00 00	Broadc...	00	84%	01 01 01 05 00 05 ...
29:06 PM	46 (Mutil_Send)	FF FF	00 00	Broadc...	00	85%	01 01 01 05 00 05 ...
29:06 PM	46 (Mutil_Send)	FF FF	00 00	Broadc...	00	84%	01 01 01 05 00 05 ...
29:06 PM	46 (Mutil_Send)	FF FF	00 00	Broadc...	00	85%	01 01 01 05 00 05 ...
29:06 PM	46 (Mutil_Send)	FF FF	00 00	Broadc...	FF	83%	01 01 01 05 00 05 ...
29:06 PM	46 (Mutil_Send)	FF FF	00 00	Broadc...	FF	84%	01 01 01 05 00 05 ...
29:06 PM	46 (Mutil_Send)	FF FF	00 00	Broadc...	FF	85%	01 01 01 05 00 05 ...
29:06 PM	46 (Mutil_Send)	FF FF	00 00	Broadc...	00	84%	01 01 01 05 00 05 ...
29:06 PM	46 (Mutil_Send)	FF FF	00 00	Broadc...	00	85%	01 01 01 05 00 05 ...
29:05 PM	46 (Mutil_Send)	FF FF	00 00	Broadc...	00	84%	01 01 01 05 00 05 ...
29:05 PM	46 (Mutil_Send)	FF FF	00 00	Broadc...	00	84%	01 01 01 05 00 05 ...
2:29:05 PM	46 (Mutil_Send)	FF FF	00 00	Broadc...	00	85%	01 01 01 05 00 05 ...
2:29:05 PM	46 (Mutil_Send)	FF FF	00 00	Broadc...	00	84%	01 01 01 05 00 05 ...
2:29:04 PM	46 (Mutil_Send)	FF FF	00 00	Broadc...	FF	83%	01 01 01 05 00 05 ...
2:29:04 PM	46 (Mutil_Send)	FF FF	00 00	Broadc...	FF	83%	01 01 01 05 00 05 ...
2:29:03 PM	46 (Mutil_Send)	FF FF	00 00	Broadc...	00	83%	01 01 01 05 00 05 ...

6.3 Transmission is unstable, and the Net LED indicator of ZigBee slave

sometimes begins blinking for a short time before returning to a steady state.

In this situation, check whether the ZB-2500 often receives "Request to Join Net" series packets (commands 0x30 ~ 0x33) or receives a number of the "Connection check" packets (command 0x50) within a short period, which means that the ZigBee slave is frequently disconnected.

Normal

The connection check interval is 20 seconds.

Time	Packet Type	PanID	From	To	CRC	RSSI
2:00:28 PM	51 (Connection Check ...	00 01	00 00	00 02	00	99%
2:00:28 PM	50 (Connection Check)	00 01	00 02	00 00	00	99%
2:00:08 PM	51 (Connection Check ...	00 01	00 00	00 02	00	99%
2:00:08 PM	50 (Connection Check)	00 01	00 02	00 00	00	99%
1:59:48 PM	51 (Connection Check ...	00 01	00 00	00 02	00	97%
1:59:48 PM	50 (Connection Check)	00 01	00 02	00 00	00	99%
1:59:28 PM	51 (Connection Check ...	00 01	00 00	00 02	00	95%
1:59:28 PM	50 (Connection Check)	00 01	00 02	00 00	00	99%
1:59:08 PM	51 (Connection Check ...	00 01	00 00	00 02	00	99%
1:59:08 PM	50 (Connection Check)	00 01	00 02	00 00	00	99%

Exception

The connection check request is very frequent, but a response is still received.

Time	Packet Type	PanID	From	To	CRC	RSSI
2:10:20 PM	51 (Connection Check ACK)	00 01	00 00	00 02	00	44%
2:10:20 PM	50 (Connection Check)	00 01	00 02	00 00	00	42%
2:10:19 PM	50 (Connection Check)	00 01	00 02	00 00	00	41%
2:10:19 PM	50 (Connection Check)	00 01	00 02	00 00	00	42%
2:10:19 PM	50 (Connection Check)	00 01	00 02	00 00	00	42%
2:10:19 PM	50 (Connection Check)	00 01	00 02	00 00	00	41%
2:10:19 PM	50 (Connection Check)	00 01	00 02	00 00	00	40%
2:10:19 PM	50 (Connection Check)	00 01	00 02	00 00	00	40%
2:10:18 PM	50 (Connection Check)	00 01	00 02	00 00	00	28%
2:10:18 PM	50 (Connection Check)	00 01	00 02	00 00	00	29%
2:10:18 PM	50 (Connection Check)	00 01	00 02	00 00	00	30%
2:10:18 PM	50 (Connection Check)	00 01	00 02	00 00	00	30%
2:10:18 PM	50 (Connection Check)	00 01	00 02	00 00	00	25%
2:10:18 PM	50 (Connection Check)	00 01	00 02	00 00	00	25%
2:10:18 PM	50 (Connection Check)	00 01	00 02	00 00	00	26%

This situation usually occurs when the signal strength is too weak or there is a lot of interference.

7. Appendix

7.1 Included Cables:

CA-USB18 (1.8 M Cable) x 1; USB Type A connector (Type A to Type B cable provided)

7.2 Document Download Location:

Website:

http://ftp.icpdas.com.tw/pub/cd/usbcd/napdos/zigbee/zigbee_sniffer/zb-2500/document/

CD path:

[Napdos\ZigBee\ZigBee_Sniffer\ZB-2500\Document\](#)

7.3 Utility Download Location:

Website:

http://ftp.icpdas.com.tw/pub/cd/usbcd/napdos/zigbee/zigbee_sniffer/zb-2500/utility/

CD path:

[Napdos\ZigBee\ZigBee_Sniffer\ZB-2500\Utility\](#)

7.4 Driver Download Location:

Website:

http://ftp.icpdas.com.tw/pub/cd/usbcd/napdos/zigbee/zigbee_sniffer/zb-2500/driver/

CD path:

[Napdos\ZigBee\ZigBee_Sniffer\ZB-2500\Driver](#)

7.5 ZigBee Products Website:

http://www.icpdas.com.tw/product/solutions/industrial_wireless_communication/wireless_solutions/wireless_selection.html#d

7.6 Technical Service:

If you have any questions about using the ZB-2500, please send a description of your problem to service@icpdas.com

8. Ordering Information

ZigBee Sniffer	
ZB-2500 CR	ZigBee Repeater (RoHS)
ZB-2500/S CR	ZigBee Repeater (RoHS) + GPSU06U-6 (Power Supply)

9. Accessories

ZigBee Converter	
ZB-2550	RS-485/RS-232 to ZigBee Converter (Host)
ZB-2550-T	RS-485/RS-232 to ZigBee Converter (Host) (CE/FCC/FCC ID)
ZB-2550-PA	RS-485/RS-232 to ZigBee Converter (Host) (long range)
ZB-2551	RS-485/RS-232 to ZigBee Converter (Slave)
ZB-2551-T	RS-485/RS-232 to ZigBee Converter (Slave) (CE/FCC/FCC ID)
ZB-2551-PA	RS-485/RS-232 to ZigBee Converter (Slave) (long range)
ZB-2570	Ethernet/RS-485/RS-232 to ZigBee Converter (Host)
ZB-2570-T	Ethernet/RS-485/RS-232 to ZigBee Converter (Host) (CE/FCC/FCC ID)
ZB-2570-PA	Ethernet/RS-485/RS-232 to ZigBee Converter (Host) (long range)
ZB-2571	Ethernet/RS-485/RS-232 to ZigBee Converter (Slave)
ZB-2571-T	Ethernet/RS-485/RS-232 to ZigBee Converter (Slave) (CE/FCC/FCC ID)
ZB-2571-PA	Ethernet/RS-485/RS-232 to ZigBee Converter (Slave) (long range)
ZB-Repeater	
ZB-2510	ZigBee Repeater
ZB-2510-T	ZigBee Repeater (CE/FCC/FCC ID)
ZB-2510-PA	ZigBee Repeater (long range)
ZigBee AIO	
ZB-2015-T	Wireless 6-ch RTD Input Module with 3-wire RTD Lead Resistance Elimination (CE/FCC/FCC ID)
ZB-2017-T	Wireless 8-ch Analog Input Module with High Voltage Protection (CE/FCC/FCC ID)
ZB-2017C-T	Wireless 8-ch Current Input Module with High Common Voltage Protection (CE/FCC/FCC ID)
ZB-2018-T	Wireless 8-ch Analog Input Module with High Voltage Protection (CE/FCC/FCC ID)
ZB-2024-T	Wireless 4-ch Voltage/Current Output Module (CE/FCC/FCC ID)
ZB-2026-T	Wireless 4-ch Voltage Input, 2-ch Voltage Output and 2-ch Digital Output Module (CE/FCC/FCC ID)
ZigBee DIO	
ZB-2042-T	Wireless 4-ch PhotoMOS Relay Output and 4-ch Open Collector Output Module (CE/FCC/FCC ID)
ZB-2043-T	Wireless 14-ch Isolated Digital Output Module (CE/FCC/FCC ID)
ZB-2052	Wireless 8-ch Isolated Digital Input Module with 16-bit Counters
ZB-2052-T	Wireless 8-ch Isolated Digital Input Module with 16-bit Counters (CE/FCC/FCC ID)
ZB-2053-T	Wireless 14-ch Isolated Digital Input Module (CE/FCC/FCC ID) (long range)
ZB-2060	Wireless 6-ch Isolated Digital Input and 4-ch Relay Output Module
ZB-2060-T	Wireless 6-ch Isolated Digital Input and 4-ch Relay Output Module (CE/FCC/FCC ID)
ZB-2060-PA	Wireless 6-ch Isolated Digital Input and 4-ch Relay Output Module (long range)