802.11b/g Wi-Fi Detector

User's Manual

Version: 1.0
(Dec 2005)

COPYRIGHT

This company makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution

This equipment must be installed and operated in accordance with provided instructions and a minimum 5 cm spacing must be provided between computer mounted antenna and person’s body (excluding extremities of hands, wrist and feet) during wireless modes of operation.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom.
The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not intended for use

None.

CONTENTS

1 Introduction

Thank you for purchasing this 802.11b/g Wi-Fi Detector. This convenient device instantly detects wireless hotspots anywhere. The backlightt LCM display tells the user detailed information about any detected hotspot. There's no need to purchase any battery because there is a rechargeable Li-Polymer battery which recharges whenever the detector is inserted into any USB port.

1.1 Features

- Complies with the IEEE 802.11b and IEEE 802.11g 2.4GHz standards.
- LCM displays: SSID, Signal Strength, Network type (802.11b/g), Network Mode (infrastructure, Adhoc), operating channel, number of AP's detected, battery strength, Link/Act indicator)
- Immediately indicates whether the environment has available wireless networks or equipment.
- Portable and mini-size design.
- Rechargeable Li-Polymer battery.

1.2 Specifications

- Standard: IEEE 802.11g/b
- LCM Size: 96x32 with EL backlight
- Battery: 4.2V Rechargeable Li-Polymer Battery
- USB Port: USB 2.0 Type A
- Frequency Band: 2.4000~2.4835GHz (Industrial Scientific Medical Band)
- Modulation: OFDM with BPSK, QPSK, 16QAM, 64QAM (11g)
  BPSK, QPSK, CCK (11b)
- Antenna: Internal Antenna
- Dimension: 14(H) x 28.5(W) x 91(D)
- Temperature: 32~131°F (0 ~55°C)
- Humidity: 0-85% (NonCondensing)
- Certification: FCC, CE

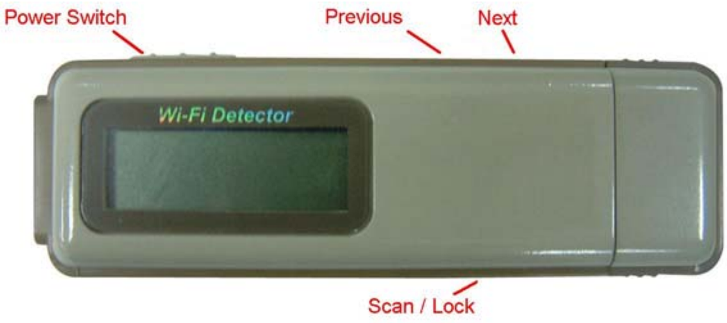
1.3 Package Contents

Before you begin the installation, please check the items of your package. The package should include the following items:

- One Wi-Fi Detector
- One User Manual

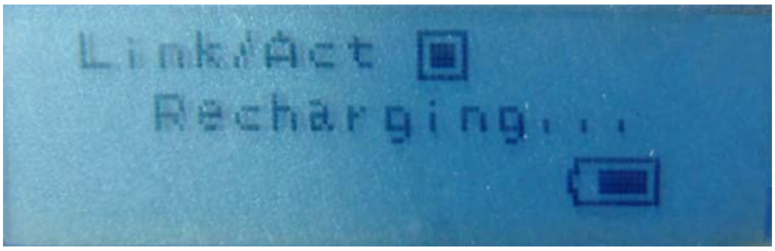
If any of the above items is missing, contact your supplier as soon as possible.

2 The Outward Appearance of the Wi-Fi Detector



3 How to charge the Wi-Fi Detector

1. Remove the cap from the Wi-Fi Detector and carefully insert the USB connector into any available USB port on your computer. You will see the recharging screen.

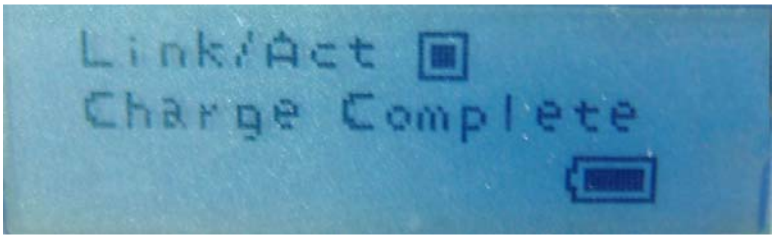


Link/Act

Recharging...

The battery strength indicator will be animated while the Wi-Fi detector is being recharged.

2. When the Wi-Fi detector is finished recharging it will automatically stop charging the battery. When it is finished recharging the battery you will see “charge complete” displayed on the LCM and the battery strength indicator will stop blinking.

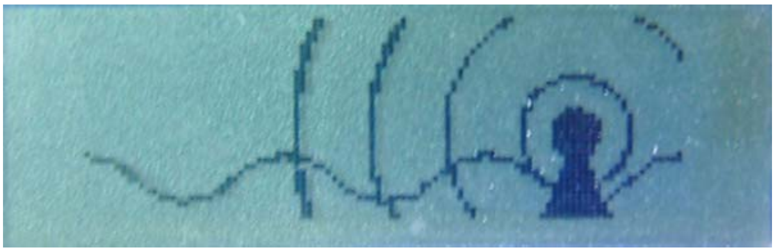


Link/Act

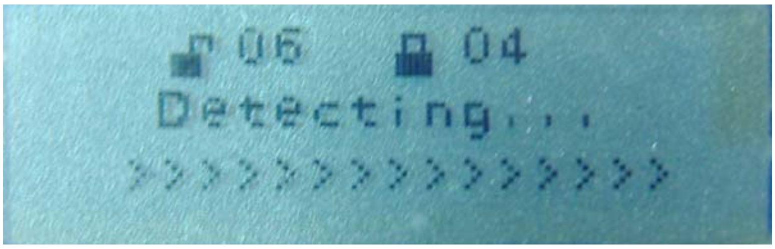
Charge Complete

4 How to use the Wi-Fi Detector

1. Slide the power switch to the “ON” position, and a welcome screen will greet the user.



2. After the welcome screen is displayed the Wi-Fi detector will automatically enter scanning mode to detect Wi-Fi signals.

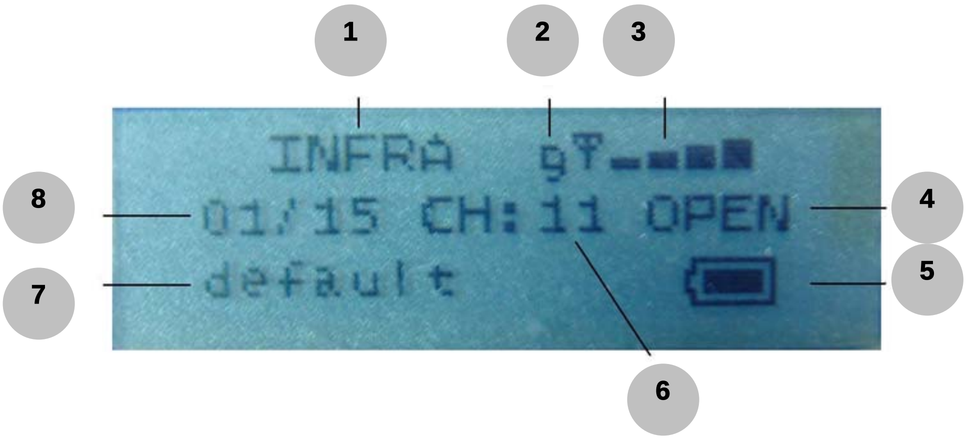


🔓06 🔒04
Detecting...
>>>>>>>>>>>>>>>

In scanning mode the display will display the total number of both non-encrypted and encrypted Wi-Fi signals detected.

3. Once scanning mode is complete, the detector will enter its standard display mode.

The detector automatically sorts the signals by the following criteria:
Non-encrypted AP’s according to signal strength followed by encrypted AP’s according to signal strength.

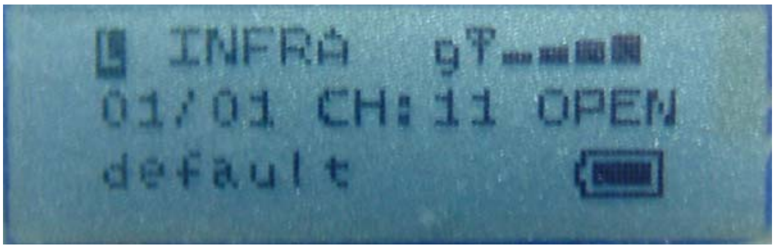


INFRA 9
01/15 CH:11 OPEN
default

The Icons on the LCM display are displayed as follows:

1. INFRA indicates the signal is an infrastructure mode signal, ADHOC indicates the signal is an Adhoc mode signal.
2. “g” indicates the signal is a 802.11g wireless signal. “b” indicates the signal is a 802.11b wireless signal.
3. Signal strength indicator with 5 bars indicating the signal strength.
4. Encryption indicator: “WEP” for WEP encryption, “WPA” for WPA encryption, and “WPA2” for WPA2 encryption, and “OPEN” indicates it is a non-encrypted signal.
5. Battery indicator with 3 bars indicating battery power. When the indicator is empty, please recharge the detector by inserting it into a USB port.
6. Operating Channel: Indicates the current operating channel of the detected Wi-Fi signal.
7. SSID Indicator: Displays the SSID of the detected Wi-Fi signal, if the SSID is too long the SSID indicator will scroll to display the complete SSID.
8. Number of AP’s Detected: the left digit indicates which detected Wi-Fi signal is currently displayed and the right digit indicates the total amount of Wi-Fi signals detected.

4. If the user wishes to determine where any detected signal strength is the strongest, the user simply has to hold down the “scan” button for 3 seconds to enter “lock mode”. When the detector is in “lock mode” an icon with a capitalized “L” appears in the upper left corner of the display.



```
L INFRA   g
01/01 CH:11 OPEN
default
```

In “lock mode” the detector constantly refreshes the signal strength so the user can move around to find where the detected signal strength is the strongest.

Just hold down the “scan” button for 3 seconds again to unlock the “lock mode”.

5 Appendix

This chapter provides some information about IEEE 802.11b/g standards.

1. **What is the IEEE 802.11g standard?**

   802.11g is the new IEEE standard for high-speed wireless LAN communications that provides for up to 54 Mbps data rate in the 2.4 GHz band. 802.11g is quickly becoming the next mainstream wireless LAN technology for the home, office and public networks. 802.11g defines the use of the same OFDM modulation technique specified in IEEE 802.11a for the 5 GHz frequency band and applies it in the same 2.4 GHz frequency band as IEEE 802.11b. The 802.11g standard requires backward compatibility with 802.11b.

   The standard specifically calls for:

   A. A new physical layer for the 802.11 Medium Access Control (MAC) in the 2.4 GHz frequency band, known as the extended rate PHY (ERP). The ERP adds OFDM as a mandatory new coding scheme for 6, 12 and 24 Mbps (mandatory speeds), and 18, 36, 48 and 54 Mbps (optional speeds). The ERP includes the modulation schemes found in 802.11b including CCK for 11 and 5.5 Mbps and Barker code modulation for 2 and 1 Mbps.

   B. A protection mechanism called RTS/CTS that governs how 802.11g devices and 802.11b devices interoperate.

2. **What is the IEEE 802.11b standard？**

   The IEEE 802.11b Wireless LAN standard subcommittee, which formulates the standard for the industry. The objective is to enable wireless LAN hardware from different manufactures to communicate.

3. **What does IEEE 802.11 feature support？**

   The product supports the following IEEE 802.11 functions:

   ●CSMA/CA plus Acknowledge Protocol
   ●Multi-Channel Roaming
   ●Automatic Rate Selection
   ●RTS/CTS Feature
   ●Fragmentation
   ●Power Management

4. **What is Ad-hoc？**

   An Ad-hoc integrated wireless LAN is a group of computers, each has a Wireless LAN adapter, Connected as an independent wireless LAN. Ad hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

5. **What is Infrastructure？**

   An integrated wireless and wireless and wired LAN is called an Infrastructure configuration. Infrastructure is applicable to enterprise scale for wireless access to central database, or wireless application for mobile workers.

6. **What is BSS ID？**

   A specific Ad hoc LAN is called a Basic Service Set (BSS). Computers in a BSS must be configured with the same BSS ID.

7. **What is WEP？**

   WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 40 bit shared key algorithm, as described in the IEEE 802 .11 standard.

8. **What is TKIP?**

   TKIP is a quick-fix method to quickly overcome the inherent weaknesses in WEP security, especially the reuse of encryption keys. TKIP is involved in the IEEE 802.11i WLAN security standard, and the specification might be officially released by early 2003.

9. **What is AES?**

   AES (Advanced Encryption Standard), a chip-based security, has been developed to ensure the highest degree of security and authenticity for digital information, wherever and however communicated or stored, while making more efficient use of hardware and/or software than previous encryption standards. It is also included in IEEE 802.11i standard. Compare with AES, TKIP is a temporary protocol for replacing WEP security until manufacturers implement AES at the hardware level.

10. **Can Wireless products support printer sharing？**

    Wireless products perform the same function as LAN products. Therefore, Wireless products can work with Netware, Windows 2000, or other LAN operating systems to support printer or file sharing.

11. **Would the information be intercepted while transmitting on air？**

    WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN series offer the encryption function (WEP) to enhance security and Access Control. Users can set it up depending upon their needs.

12. What is DSSS？What is FHSS？And what are their differences？

Frequency-hopping spread-spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-sequence spread-spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip is, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without-the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

13. What is Spread Spectrum？

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communication systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread –spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).