Instruction Manual

TYPHOON SPEEDNET WIRELESS ACCESS POINT

Art: 70062C

08/2002

HTTP://WWW.TYPHOONLINE.COM

DECLARATION OF CONFORMITY

We, the manufacturer / importer

Anubis Electronic GmbH
Am Langfeld 38
66130 Saarbrücken
Germany

Declare that the product

Type of product : Wireless Access Point
Type designation : Typhoon Speednet Wireless Access Point

Is herewith confirmed to comply with the requirements set in the Council Directive on the Approximation of the Laws of the Member States relating to

Electro Magnetic Compatibility Directive :
IEC60 950: 1991+A1: 1992+A2: 1993+A3: 1995+A4: 1996
EN60 950: 1992+A1:1993:A2:1993+A3:1995+A11:1997
EN300826:
-Measurement Stand:
   EN300328-2: 2000
   ETS 300826:1997
-Measurement Procedure:
   EN300328-1: 2000
   EN50081-1: 1992
   EN50082-1: 1997
EN55022: 1994
   EN61000-4-2: 1995
   EN61000-4-3: 1995
   EN61000-4-4: 1995
   EN61000-4-5: 1995
   EN61000-4-6: 1996
   EN61000-4-11: 1994
EN600826:
-Measurement Stand:
   ETSI EN300328-2:2000
-Measurement Procedure:
   EN300328-1:2000

FC CE0678①

Copyright

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 20 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.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

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 Not Intended for Use

The ETSI version of this device is intended for home and office use in Austria Belgium, Denmark, Finland, France, (with Frequency channel restrictions) 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.

Potential restrictive use
France: Only channels 10,11,12, and 13

Manual Contents

Chapter 1

Introduction

This chapter is your starting point for the rest of this manual.

Package Contents

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

● One Wireless Access Point

● One Power Adaptor

● One USB Cable

● One CD-Based Software (Including Wireless Access Point driver & utility and user manual.)

● One Quick Guide

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

Minimum System Requirements

Before you begin the installation, please check the following requirements with your equipment.

● Pentium Based (above) IBM-compatible PC system with an USB support

● CD-ROM driver

● One Available USB Connector

● One Available Ethernet port

● Windows 98/2000/ME/XP Operating System

● At least 500Kbytes of free disk space for utility and driver installation

Safety Precaution

Only use the accessories and connection cables attached with the device package. Otherwise, the device may not function. If you accidentally miss or damage the accessories and connection cables, please contact with your local dealer.

Installation Procedure

This chapter will walk you through the hardware and Device Manager

Installing the Hardware

Perform the following steps to install the Wireless Access Point (AP).

1. If applicable, insert the Ethernet cable into the RJ45 connector (labeled "WAN") on the AP to connect to a hub, router, cable or DSL modem.

2. Next, apply power to the AP by plugging in the power adapter supplied with the evaluation kit. This completes the hardware portion of the installation.

3. The next step is to add the AP into the wireless network. There are three configuration options of the AP:

● "Enroll" the AP in the network (Multimedia Mode only). Using the Network Management application on a wireless active PC node to enroll the AP into the network.

● The AP provides an SNMPv1 agent and the support for the standard IEEE 802.11 MIB and proprietary extensions (MIB files are included in the evaluation CD). These objects can be read and configured via a standard SNMP MIB Browser.

● Alternatively, read the below "Installing the AP Manager" to manually configure the AP Access.

● WAN / LAN Port Application

WAN Port	+ RJ45 Cross Over Cable	+ ADSL or Cable Modem
LAN Port	+ RJ45 Normal Cable	+ HUB

Or

WAN Port	+ RJ45 Normal Cable	+ HUB (uplink port) or PC
LAN Port	+ RJ45 Normal Cable	+ ADSL or Cable Modem or Intranet

Note: When the correct cables are connected to the "LAN" or "WAN" ports, the "LAN" or "WAN" LED indicators should be on. If you find the LED indicators still lightless, please check if the cables are loose or out of order.

7

Installing the AP Manager

The Access Point (AP) can be manually configured using the "AP Manager". Follow the below instructions to install this software.

1. Connect the AP to a computer using the included USB cable. The computer does not have to be a node in the network (any network or non-network PC can be used to run the AP Manager software).

2. Windows will notify you with a "New Hardware Found" dialog box. Following this, the Windows installation wizard will detect the AP.

3. Insert the installation CD into your CDROM drive and click "Next".

● **Windows 98**
   - Select "Search for the best driver for your device", and click "Next". Specify to search the CD Rom drives (check the box) and click "Next".

● **Windows ME/2000**
   - Select the "Automatic Search" option and click "Next".

4. Windows will find the drivers located on the CD and begin to install them. This may take several minutes.

5. When completed click "Finish". You will next be asked to reboot the computer. Click "Yes".

Note: If the system does not shut down (or restart) within 2 minutes, manually power down the computer and then power it back up.

6. After the restart, the software installation will continue automatically. Follow the instructions on the screen to install the software. You will be asked some basic questions including:

● Agreement to the (blank) license agreement

● Your name and company name

● SSID (This will be the SSID or network name immediately after installation, note that you can always change this after the installation).

7. After the software installation you may be asked to reboot once more, after which the installation is complete.

Important: On most systems it is necessary that you reset the AP after installation of the software. At this time, reset the AP using the reset button or by "power-cycling" the AP. You can now use the AP Device Manager.

Device & Network Management

This chapter will help you understand the device management, network management and device management applications.

To manage the various devices on the network and the network itself, three software applications are provided. Following is a short description of each application and its main purpose.

● **Device Manager**
- The Device Manager configures any client device located on the computer (i.e. PCMCIA).

● **Network Manager**
- Network Management provides network information and statistics regarding all devices on the network. This application is only available when the network is operating in Multimedia mode.

● **AP Device Manager**
- The AP Device Manager allows for configuring the AP through the USB cable.

The following sections describe these applications and their operation in greater detail.

Device Manager
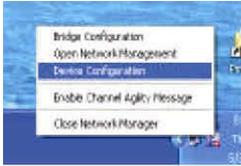
Start the Device Manager by right-clicking the icon on the system tray and selecting "Device Configuration".

The Device Manager uses the concept of "profiles." Profiles allow a user to store specific settings for a particular situation or environment. For example, a user may have an "Office" profile in which the node operates in Wi-Fi mode and a "Home" profile for Multimedia mode. Profiles will help the user manage the appropriate settings including network IDs, WEP, and operating mode.

Profiles can be created, managed (for editing) and activated from the Device Manager application by selecting the Profiles menu.

When creating a new profile from this menu, the software will ask the user to select either a Wi-Fi based or a Multimedia-based profile.

The screen (at left) displays the creation of a new Multimedia profile. Profile name, encryption settings, etc. can be set here. Settings that are unique to a Multimedia profile include the "Auto" setting for the channel selection and the "Channel Agility sensitivity" setting (both unique to the Channel Agility feature). Another Multimedia-only setting is the "Change to Master Node" option, which forces a particular node to be the network coordinator. A complete overview of all parameters is included at the end of this section.
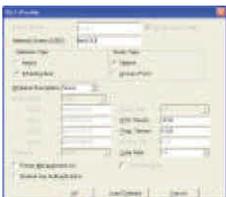
The screen (at left) shows the WiFi profile "create" screen. The WiFi-unique options that can be set on this screen are the Network and Node type settings in addition to Data Rate and Power Management settings.

Once two or more profiles are created, the user can switch between these profiles using the Profiles menu in the main device manager screen.

Previously created profiles can be edited, deleted, renamed and copied in the Manage Profiles screen. The Copy command is useful in creating multiple profiles that are similar without having to reset all options manually.

The list below defines all user-configurable settings within a profile.

Feature	Wi-Fi	MM	Description
Profile Name	X	X	Name to identify the profile, i.e. "Home", "Office", "Airport".
Network Name / SSID	X	X	Unique identifier for the network. All nodes on a network must have the same SSID/Network name to be able to communicate.
Set as active Profile	X	X	When checked, will activate the profile immediately upon clicking "OK".
Network Type	X		Defines if the network will be operating in "Infrastructure" or "Ad-Hoc" Mode. "Infrastructure" mode is used when a network includes an Access Point and all nodes communicate via the Access Point. "Ad-Hoc" is used when all nodes communicate directly with each other without an Access Point.
Node Type	X		Default is "Station" and should be used for standard operation. When "Access Point" is selected it will allow a node to act as an Access Point.
Change To Master Node		X	Forces a particular node to be the network coordinator.
Wireless Encryption	X	X	Disabled by default. 40 bit (=64 bit) WEP encryption can be selected. Up to 4 unique keys can be entered; one key must be selected to be the "active key". Keys must be 10 digits long and must be entered as HEX (0-9, A-F). Make sure all nodes in the network have the same key to establish connectivity.
Power Management	X		Disabled by default. Enabled "Protocol Power Save" allows part of the hardware to be shut-off when possible to conserve power.
Channel	X	X	Set to "Auto" by default. Forces the node to only operate on one particular channel. Not available in Wi-Fi Station mode. When set to "Auto" in Multimedia mode the "Channel Agility" feature is enabled.
Shared Key Authentication	X		Disabled by default. Allows for a more secure way of authenticating nodes onto the network. All nodes in the network must have Shared Key Authentication set to the same value.
Basic Rate	X		This value should not be changed during regular operation (For advanced users only).
RTS Threshold	X		This value should not be changed during regular operation (For advanced users only).
Frag. Threshold	X		This value should not be changed during regular operation (For advanced users only).
Beacon Interval	X		This value should not be changed during regular operation (For advanced users only).
Data rate	X		Set to 11 Mbps by default.
Load defaults	X	X	Sets the profile settings back the factory default.
Channel Agility Sensitivity		X	Determines the packet error rate the network will change channels to avoid the interference. The higher the sensitivity, the sooner it will change channels. 30% is the default and the recommended setting.

Network Management

Double-click on the system tray icon to start Network Management (or right-click and select "Open Network Management").

Note: The Network Management Application is ONLY available when the Network is in Multimedia mode.

The "Node Information" page in network management utility displays a diagram of the active Multimedia network. Additional information is also available by clicking on buttons to the left side of the page.

The Color legend on the lower left designates the quality of the connection and is indicated by the color of the lines between any two nodes.

The information on this page is obtained from the Master node for all nodes on the network. If the Master node is a non-functional node, this HTML page will not be available on the client nodes and a "trouble shooting page" will be displayed instead.

● **Adding nodes to the network** (Multimedia mode only)

- To add the AP node to the network, the designated Master node must allow the AP to be "enrolled" into its secured network group. This group is based on the network identification (or "Network ID") entered during installation. If the Network ID of a node matches the Master's Network ID, the node will be automatically enrolled into the group.

- To add a wireless AP to the network or add a new node which is configured to be in an open enrollment mode, click on the "Add A New Node" button in the Network Management page from any node in the system. The Master node will search for nodes that have not been added to the group. (those which are determined to be in open enrollment mode)

- To add (or enroll) this AP into the network, click on the "Add" button. The Master node will forward its Network ID to the AP node which as been detected to be in open enrollment mode.

Refer to the below section on the "AP Device Manager" for instructions on how to manually configure the AP. Manual configuration will give you more control over the AP settings including network names, SSID and WEP settings.

AP Device Manager

When the USB cable is connected, the AP will enter configuration mode. Double-clicking the icon on the desktop will start the AP Device Manager.

Note: While the AP is in "configuration mode" (when the USB cable is inserted), the AP will not function in the network. Upon removal of the USB cable, the AP will resume its normal operation.

After the application starts, it will display a general information screen which provides information for the current Multimedia and Wi-Fi settings.
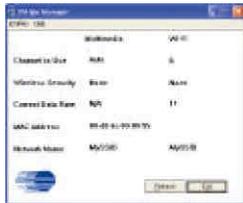
● **Setting up profiles**

- To edit these settings, select either the "Multimedia profile" or "Wi-Fi profile" from the Profile menu. All relevant settings for both Wi-Fi and Multimedia mode can be set or modified. Note that the separate profiles allow for unique settings (i.e. different SSID or network names) in each mode.

The list below outlines all user-configurable AP settings.

Feature	Wi-Fi	MM	Description
Network Name / SSID	X	X	Unique identifier for the network. All nodes on a network must have the same SSID/Network name to be able to communicate.
Wireless Encryption	X	X	Disabled by default. 40 bit (=64 bit) WEP encryption can be selected. Up to 4 unique keys can be entered; one key must be selected to be the "active key". Keys must be 10 digits long and must be entered as HEX (0-9, A-F). Make sure all nodes in the network have the same key to establish connectivity.
Power Management	X		Disabled by default. Enables "Protocol Power Save", which allows part of the hardware to be shut-off when possible to conserve power.
Channel	X	X	Forces the network to only operate on one particular channel. This selection is not available when Channel Agility is enabled in Wi-Fi mode.
Shared Key Authentication	X		Disabled by default. Allows for a more secure way of authenticating nodes onto the network. All nodes in the network must have Shared Key Authentication set to the same value.
Basic Rate	X		This value should not be changed during regular operation (For advanced users only).
RTS Threshold	X		This value should not be changed during regular operation (For advanced users only).
Frag. Treshold	X		This value should not be changed during regular operation (For advanced users only).
Beacon Interval	X		This value should not be changed during regular operation (For advanced users only).
Data rate	X		Set to 11 Mbps by default. Selecting a lower data rate MAY result in increased range.
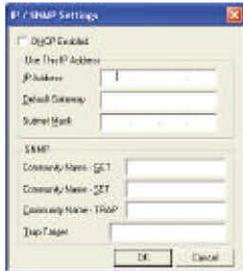
● **Setting up IP/SNMP settings**

- When operating in Wi-Fi mode, the AP runs an IP stack. The IP settings can be modified by selecting the "IP/SNMP" settings in the Profiles menu of the AP manager. The following parameters can be modified:

  ◆ **DHCP Enabled**

  - When enabled, the AP will attempt to obtain an IP address through DHCP.

  ◆ **IP Address**

  - Allows for manually assigning an IP address.

  ◆ **Default Gateway**

  - Allows for manually assigning a Gateway (enter Gateway's IP address).

  ◆ **Subnet Mask**

  - Allows for manually entering a subnet mask.

  - The AP provides an SNMPv1 agent and provides support for the standard IEEE 802.11 MIB and proprietary extensions. These objects can be read and configured via a standard SNMP MIB Browser. The following parameters can be set on the AP by selecting the "IP/SNMP Settings" from the Profiles menu in the AP Manager:

  ◆ **Community Name – GET**

  - The read password to monitor AP/Access Point statistics and configuration parameters. Default password is "public".

  ◆ **Community Name – SET**

  - The read / write password to monitor AP statistics and edit configuration parameters. Default password is "private".

  ◆ **Community Name – TRAP**

  - The password included in trap messages sent to the SNMP management tool. This password can be used to filter unwanted messages. Default password is "public".

  ◆ **Trap Target**

  - The IP address of the SNMP management station that will collect SNMP trap messages. Default address is "192.168.0.1".

Switches and Connectors

Nodes with a Cirrus wireless adapter installed can be switched from Wi-Fi to Multimedia mode (and vice versa) using the device manager software. As the Access Point (AP) does not have a user interface that can be used to switch between multimedia and Wi-Fi, it employs a manual mode switch. This switch can be found on the AP and is labeled accordingly.

Depending on the configuration of your evaluation kit you may have received one of three Access Points (AP). All APs offer similar functionality but vary in appearance. The below installation instructions apply to all available APs.

● **Mode Switch**
  - Used to switch between Multimedia (WhiteCap) and Wi-Fi mode.

● **Factory Default Reset**
  - Used to reset all parameters (i.e. SSID, WEP etc) to the factory default.

● **Reset**
  - Used to reset the AP. (similar to power cycling)

● **Power**
  - Connects to (included) power adapter.

● **WAN Port**
  - Connects to HUB, router, cable/DSL modem for LAN / Internet connectivity.

● **LAN Port (not available on all APs)**
  - Can be used to connect a wired client node to the network.

● **USB Port**
  - Connects to connector, use for configuration only. (AP Manager software required)

Uninstall Hardware & Software

This chapter will help with the Hardware & Software uninstall process.

1. To completely uninstall the wireless network adapter from your Windows operating system, use the Windows Add/Remove Programs Properties feature located in the Start /Settings/Control Panel menu.

2. Select the Wireless Network Adapter and click on the "Add/Remove…" button.

3. Follow the on-screen instructions to uninstall the software.

4. After the software uninstall, use the Windows Device Manager to uninstall/remove the wireless adapter.

● **Windows 98/ME**
 - Right-click on the "My Computer", select "properties", select the 'Wireless Networking Adapter' and click uninstall/remove.

● **Windows 2000/XP**
 - Right-click on the "My Computer", select "hardware", select "device manager", select the "Wireless Networking Adapter" and click uninstall/remove.

5. After uninstalling the device in the device manager, shut down the computer and remove the hardware.

Technical Specification

- Standard: Wi-Fi (IEEE 802.11b) and MM/QoS (IEEE 802.11e-type)

- Signal Type: DSSS (Direct Sequence Spread Spectrum)

- Frequency Band: 2.400 GHz ~2.4835GHz

- Modulation: QPSK / BPSK / CCK

- Ports Two RJ 45, One USB

- Ethernet Interface: IEEE 802.3; 10BaseT

- Antenna: Two External Dipole Antenna

- Channel: 11 Channels (US, Canada), 13 Channels (Europe), 14 Channels (Japan)

- Data Rate: Up to 11 Mbps (with automatic Fall Back)

- Transmit Power Output: Typically 20 dBm

- Receive Sensitively: Typically –83 dBm

- Compatibility: Windows 98/ME/2000/XP

- LED Indicators: LED1: Power, LED2: Radio Activity, LED3: Wi-Fi compliant or Multimedia, LED4: LAN, LED5: WAN

- Power Supply: Input: AC 100-240, 47-63Hz, 0.3A, Output: DC 5 V / 2A

- Certification: FCC, R&TTE

- Dimensions: 142x88x28mm

- Weight: 128g

**Chapter
6**

Troubleshooting

This section provides solutions to problems usually encountered during the installation and operation of this Wireless USB Adaptor. Read the description below to solve your problems.

✓ **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.

✓ **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

✓ **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.

✓ **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.

✓ **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.

✓ **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.

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

✓ **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.

✓ **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.

✓ **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).

✓ **Hotline and Service Information**

Land	Hotline Number	email
Deutschland	01805/8974666	Service_DE@anubisline.com
France	0033/387859602	Service_FR@anubisline.com
Italia	0039/067231 669	Service_IT@anubisline.com