NETGEAR

802.11b Wireless Access Point

Reference Guide

MODEL ME 102

Trademarks

NETGEAR is a registered trademark of NETGEAR, INC. Windows is a registered trademark of Microsoft Corporation. Other brand and product names are trademarks or registered trademarks of their respective holders. Information is subject to change without notice. All rights reserved. Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Certificate of the Manufacturer/Importer

It is hereby certified that the Model MA301 Wireless PCI Adapter has been suppressed in accordance with the conditions set out in the BMPT- AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

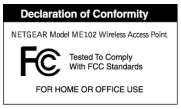
Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

VCCI Statement

This equipment is in the Class B category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas.

When used near a radio or TV receiver, it may become the cause of radio interference. Read instructions for correct handling.

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice



This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

This device may not cause harmful interference.

This device must accept any interference received, including interference that may cause undesired operation.

➲ Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the 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/TV technician for help.

Federal Communications Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits 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 20 cm (8 inches) during normal operation.

EN 55 022 Statement

This is to certify that the Model MA301 Wireless PCI Adapter is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class B (CISPR 22).

Compliance is dependent upon the use of shielded data cables.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (Model MA301 Wireless PCI Adapter) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

CONTENTS

CHAPTER 1: INTRODUCTION

The **ME102 802.11b wireless Access Point** is the basic building block of a wireless LAN infrastructure. It provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage, interacting with a wireless network interface card (NIC) via an antenna. Typically, individual in-building access point provides a maximum connectivity range of about 300 feet. The **ME102 wireless Access Point** can support a small group of users in a range of several hundred feet; most access points are rated between 30-70 users simultaneously.

The **ME102 wireless Access Point** converts airwave data into wired Ethernet data, acting as a bridge between the wired LAN and wireless clients. Connecting multiple ME102 Access Points via a wired Ethernet backbone can further lengthen the wireless network coverage. As a mobile computing device moves out of the range of one access point, it moves into the range of another. As a result, wireless clients can freely roam from one Access Point domain to another and still maintain seamless connection to the network.

The auto-sensing capability of the **ME102 wireless Access Point** allows packet transmission in 11Mbps for maximum throughput, or speed reduction to lower 1Mbps speed for distance or for operating in a noisy environment.

Features

The features supported by the ME102 Wireless Access Point are outlined below:

- Interfaces directly to 10Mbps IEEE 802.3 Ethernet networks
- Supports IEEE 802.11 HR WLAN functions.
- Firmware is stored in a flash memory and can be upgraded remotely.
- Configurable through USB and Ethernet ports.
- Power and wireless activity LED indicators.
- Dual External antennas supporting diversity.

Related NETGEAR products

- MA401 – 802.11b Wireless PC Card
- MA301 – 802.11b Wireless PCI Adapter (requires the MA401 wireless PC Card)
- MA101 – 802.11b Wireless USB Adapter
- MR314 – 802.11b Wireless Cable/DSL Router

CHAPTER 2: WIRELESS NETWORK FUNDAMENTALS

Wireless Network Configuration

Ad-hoc Mode (Peer-to-Peer Workgroup)

The Institute of Electrical and Electronics Engineers (IEEE) standard for wireless LANs (WLANs), 802.11, offers two methods for configuring a wireless network — ad hoc and infrastructure. In an ad hoc network, computers are brought together as needed; thus, there is no structure or fixed points to the network — each node can generally communicate with any other node. There is no access point involved in this configuration. It enables you to quickly set up a small wireless workgroup and allows workgroup members to exchange data or share printers as supported by Microsoft Networking in the various Windows operating systems. Some vendors also refer to ad hoc networking as Peer-to-Peer group networking.

In this configuration, network packets are directly sent and received by the intended transmitting and receiving stations. As long as the stations are within range of one another, this is the easiest and least expansive way to set up a wireless network.

To set up an ad hoc workgroup operating with standard protocols, do the following:

- Set all stations to connect in Ad-hoc mode (or Peer-to-Peer workgroup mode).
- Set all stations to use the same network name (or SS ID).
- Set all stations to use no WEP encryption key or an identical WEP encryption key.
- Set all stations to use the same wireless channel for communication.

Infrastructure Mode

With a wireless access point, you can put the wireless LAN into the infrastructure mode. It provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage, interacting with wireless nodes via an antenna.
In the infrastructure mode, the wireless access point converts airwave data into wired Ethernet data, acting as a bridge between the wired LAN and wireless clients. Connecting multiple ME102 Access Points via a wired Ethernet backbone can further extend the wireless network coverage. As a mobile computing device moves out of the range of one access point, it moves into the range of another. As a result, wireless clients can freely roam from one Access Point domain to another and still maintain seamless network connection.

To set up an infrastructure network operating with standard protocols, do the following:

- Set all wireless stations to connect in infrastructure mode
- Set all stations to use the same network name (or SS ID).
- Set all wireless access point to use the same network name (or ESS ID).
- Set all stations to use no WEP encryption key or an identical WEP encryption key.
- Set up wireless channels used by individual access point. (It is not necessary to set channels on the stations as the stations will automatically scan through all channels for the nearest access point.)

Service Set Identification (SS ID)

The Service Set Identification (SS ID) is a thirty-two alphanumeric character (maximum) string identifying the wireless local area network. Some vendors refer to the SS ID as network name. For stations to communicate with each other, all stations must be configured with the same SS ID.

A wireless LAN consisting of nodes operating in ad hoc configuration without an access point is called a Basic Service Set (BSS). All nodes in a BSS must use the same Basic Service Set ID (BSS ID).

In an infrastructure configuration with access points, multiple BSS can be configured to form an Extended Service Set (ESS). In this configuration, the access points are configured with the same Extended Service Set ID (ESS ID). Wireless clients configured with the same ESS ID can freely roam from one Access Point domain to another and still maintain seamless connection to the network

Authentication and WEP Encryption

The absence of a physical connection between nodes makes the wireless links vulnerable to information theft. To provide certain level of security, IEEE 802.11 standard has defined two types of authentication methods, Open System and Shared Key. Open System authentication is a null algorithm. Shared Key authentication is an algorithm where both the transmitting node and the receiving node share an authentication key to perform a checksum on the original message. By default, IEEE 802.11 wireless devices operate in an open system network.

Wired Equivalent Privacy (WEP) data encryption is utilized when the wireless nodes or access points are configured to operate in Shared Key authentication mode. There are two shared key methods implemented in most commercially available products, forty-bit WEP data encryption and 128-bit WEP data encryption.

The forty-bit WEP data encryption method, allows for a five-character (forty-bit) input. Additionally, 24 factory-set bits are added to the forty-bit input to generate a 64-bit encryption key. (The 24 factory-set bits are not user configurable.) This encryption key will be used to encrypt/decrypt all data transmitted via the wireless interface. Some vendors may refer to the forty-bit WEP data encryption as 64-bit WEP data encryption since the actual encryption key used in the encryption process is 64 bits wide.

The 128-bit WEP data encryption method consists of 104 configurable bits. Similar to the forty-bit WEP data encryption method, the remaining 24 bits are factory set and not user configurable. Some vendors allow passphrases to be entered instead of the cryptic hexadecimal characters to ease encryption key entry.

Wireless Channel Selection

IEEE 802.11 wireless nodes communicate with each other using radio frequency signals in the ISM (Industrial, Scientific, and Medical) band between 2.4Ghz and 2.5Ghz. Neighboring channels are 5Mhz apart. However, due to spread spectrum effect of the signals, a node sending signals using a particular channel will utilize frequency spectrum12.5Mhz above and below the center channel frequency. As a result, two separate wireless networks using neighboring channels (for example, channel 1 and channel 2) in the same general vicinity will interfere with each other. Applying two channels that allow the maximum channel separation will decrease the amount of channel cross-talk, and provide a noticeable performance increase over networks with minimal channel separation.

Channel	Center Frequency	Frequency Spread
1	2412Mhz	2399.5Mhz – 2424.5Mhz
2	2417Mhz	2404.5Mhz – 2429.5Mhz
3	2422Mhz	2409.5Mhz –2434.5Mhz
4	2427Mhz	2414.5Mhz –2439.5Mhz
5	2432Mhz	2419.5Mhz – 2444.5Mhz
6	2437Mhz	2424.5Mhz –2449.5Mhz
7	2442Mhz	2429.5Mhz –2454.5Mhz
8	2447Mhz	2434.5Mhz – 2459.5Mhz
9	2452Mhz	2439.5Mhz –2464.5Mhz
10	2457Mhz	2444.5Mhz –2469.5Mhz
11	2462Mhz	2449.5Mhz – 2474.5Mhz
12	2467Mhz	2454.5Mhz – 2479.5Mhz
13	2472Mhz	2459.5Mhz – 2484.5Mhz

Note: The available channels supported by the wireless products in various countries are different.

The preferred channel separation between the channels in neighboring wireless networks is 25 MHz (5 channels). This means that you can apply up to three different channels within your wireless network. There are only 11 usable wireless channels in the United States. It is recommended that you start using channel 1 and grow to use channel 6, and 11 when necessary.

CHAPTER 3: Hardware Installation

Package Contents

The product package should contain:

- Model ME102 802.11b Wireless Access Point
- Power adapter and cord (5Vdc, 1.0A)
- 10-ft Category 5 Ethernet Cable
- 5-ft USB cable
- MA401/MA301 Wireless Access Point Resource CD
- Installation Guide
- Support Information Card

Call your reseller or customer support in your area if there are any wrong, missing, or damaged parts. Refer to the Support Information Card for the telephone number of customer support in your area. Keep the Support Information Card, along with the original packing materials. Use the packing materials to repack the Model MA401 Wireless PC Card if you need to return it for repair.

To qualify for product updates and product warranty registrations, register online on the NETGEAR Web page at: http://www.NETGEAR.com.

Hardware Description

The ME102 802.11b Wireless Access Point provides a bridge between Ethernet wired LANs and 802.11b compatible wireless LAN networks. It provides connectivity between Ethernet wired networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices. The ME102 access point provides an 11Mbps data transfer rate on the radio network.

The ME102 access point supports the following hardware functions:

- Built-in dual antenna assembly to support antenna diversity on both transmit and receive
- Wired Equivalent Privacy (WEP) data encryption accomplished on the fly
- Access Point configuration through USB port or using the SNMP manager through Ethernet or wireless interface.
- Firmware stored in flash to allow easy firmware upgrade.

Additionally, the ME102 access point supports the following wireless features:

- Distributed coordinated function (CSMA/CA, Back off procedure, ACK procedure, retransmission of unacknowledged frames
- RTS/CTS handshake
- Duplicate detection and Recovery
- Beacon generation
- Fragmentation and reassembly
- Authentication Algorithm (Open System, Shared Key)
- Short or long preamble
- Roaming among access points on the same subnet

CHAPTER 4: Access Point Configuration

The ME102 Wireless Access Point is configurable through its USB interface or using the SNMP utility through the Ethernet or wireless interface. .

Using USB Port

The installation example below illustrates the wireless access point configuration through its USB interface from a connected PC. This PC must be running Windows 98, Windows 2000, or Windows Millennium.

Connecting the USB Cable

Plug in the power adapter for the ME102 access point to provide power to the unit. Using the provided USB cable, connect the access point to a PC. The USB interface of the ME102 Access point can be connected to the PC either powered on or shut down. The following procedure illustrates connecting the access point to a PC running Microsoft Windows while powered on.

Installing the Access Point USB driver

This section explains how to install the Windows 98 Network Driver. Microsoft Windows 2000 or Windows Millennium may respond with different dialog boxes, or the dialog boxes may open in a different sequence than those shown in this guide, but should prompt you for the same information.

- ➲ Note: You also need to have the Windows 98 CD and the ME102 Wireless Access Point Resource CD ready to use in the installation process.
- ➲ Note: If the "Insert Disk" dialog box opens and the "Please insert the disk labeled Windows 98..." message appears at any time during the installation process, insert the Windows 98 CD in drive F (or whichever letter represents the CD-ROM drive on you PC) and click "OK." Then follow the next step in the instructions.

1. Upon connecting the USB cable, Windows indicates that new hardware is found, and looks for the driver to load. Click "Next."
2. In the next Add New Hardware Wizard window, select "Search for the best driver for your device (Recommended)," and then click "Next."
3. Click on "Specify a location" and enter the drive letter for the CD-ROM drive. Insert the MA102 Wireless Access Point Resource CD. Click on "Browse".
4. Double-click on the CD-ROM drive letter to show the content of the CD. Click to select the *USBDRV* folder in the CD-ROM. Click on "OK" to continue.
5. When Windows returns back to the original Add New Hardware Wizard window, the Specify a location entry field should show "*D:\USBDRV*" assuming that D: is the drive letter for the CD-ROM drive. Click on "Next".
6. Windows indicates that the best driver for the device has been found. Click on "Next". Windows starts copying files into your system.
7. Windows indicates that it has finished installing the software. Click on "Finish".

The USB driver for the access point is now installed into your PC. You can check into the Device Manager to see if there is any error in activating the USB driver for the access point.

Installing USB Configuration Utility

The access point USB configuration utility enables you to modify the various configurable parameters of the access point.

1. Insert the ME102 Wireless Access Point Resource CD into the CD-ROM drive. From the Windows 98 desktop, double-click on *My Computer*. Double-click on the CD-ROM drive to look into the content of the CD. Double-click on the *USBMANG* folder. Windows displays all of the files in the *\USBMANG* directory of the CD.
2. Double-click on the *SETUP* application icon to start the installation procedure. The InstallShields Wizard opens. Click on "Next" to continue.
3. Click on "Browse" to change the destination location where the Access Point USB utility is installed. Otherwise, click on "Next" to continue.
4. Modify the "Program Folders" entry field if desired. Click on "Next" to continue. InstallShields starts copying files into your system.
5. Click on "Finish" to complete the installation of the access point USB utility.

Configuring Access Point

From the Windows desktop, select *Start ⇒ Program ⇒ NETGEAR ME102 AP ⇒ Access Point USB Manager*. The opening screen opens showing the firmware version of the access point and the access point USB utility software version. Click on "Configure" to go into the main USB management window. Click on the "Get Value" button to retrieve the current configurable settings from the access point.

To modify the access point parameters, first click on the intended parameter to select the parameter. And click on "Modify". A pop-up window appears inquiring for changes to the parameter. Enter any desired changes and click "OK" to accept the changes.

After making modification to all of the parameters, click on "Set" to send the changes to the access point. It is recommended to make all intended changes prior to clicking "Set" to configure the access point all at once.

When configuration is done. Click on "Exit" on the device window and click on "Exit" at the main window to quit the USB configuration utility.

Changing Wireless Parameters

The following table explains each of the configurable parameters of the ME102 Wireless Access Point.

General Specifications	Model ME102 Wireless Access Point
Access Point Name	Assign name to the access point.
IP Address	Assign Internet Protocol (IP) address to the access point.
Subnet Mask	Assign IP Subnet Mask to the access point.
MAC Address	Displays the six-byte MAC address of the access point. This parameter is not changeable by the user.
ESSID	Enter a 32-character (maximum) extended service set ID in this field. The characters are case sensitive. With an access point, the wireless network always functions in infrastructure mode. The ESS ID assigned to the wireless nodes in the same network is required to match the access point ESS ID. The default ESS ID is "Wireless".
Channel	Only valid in ad-hoc mode, this field defines the wireless channel to use. In infrastructure mode, the wireless node automatically searches through all available wireless channels for an access point to be associated with. It is not necessary to select the wireless channel when operating in infrastructure mode. The default wireless channel is 6.
WEP	The ME102 Wireless access point supports 40-bit WEP data encryption. (40-bit WEP data encryption is also called 64-bit WEP data encryption by some vendors.) This parameter enables/disables encryption and select the 40-bit WEP data encryption key to use. Up to four keys can be defined in the access point. The possible values for this parameter are Disable, Key1, Key2, Key3, and Key4. . For more explanation on data encryption, please refer to the wireless network fundamental chapter at the beginning of this reference guide. The WEP data encryption method and the key used must be the same for all wireless nodes and access points in the same network. Note: the present version of the USB Configuration Utility software does not support WEP Passphrase.
Key1	One of the four data encryption keys defined in the access point. Each data encryption key contains five hexadecimal numbers, making it 40 bits wide. Together with the twenty-four factory-set bits to make up a 64-bit encryption key.
Key2	One of the four data encryption keys defined in the access point.
Key3	One of the four data encryption keys defined in the access point.
Key4	One of the four data encryption keys defined in the access point.

Authentication	Configurable between Open System (WEP disabled), Shared Key (40-bit WEP data encryption), and both.
Preamble Mode	A long transmit preamble allows the receiver to lock into the received bit patterns more easily. A short transmit preamble provides better performance. The default value is Long Tx Preamble.
Auto Rate	Enables or disables automatic negotiation of wireless transmit data rate.
Fragment Threshold	This is the packet length used for fragmentation. Packets larger than the size programmed in this field will be fragmented. The Fragment Threshold value must be larger than RTS Threshold value. The default value for Fragment Threshold is 2346.
RTS Threshold	The packet size that the wireless node uses to determine if it should use the CSMA/CD mechanism or the CSMA/CA mechanism for packet transmission. With the CSMA/CD transmission mechanism, the transmitting station sends out the actual packet as soon as it has waited for the silence period. With the CSMA/CA transmission mechanism, the transmitting station sends out a RTS packet to the receiving station, waits for the receiving station to send back a CTS packet before sending the actual packet data. The default value for RTS Threshold is 2346.

Using Ethernet/Wireless Port

The installation below illustrates the wireless access point configuration through its Ethernet/Wireless interface from a connected PC.

Installing SNMP Configuration Utility

The access point SNMP configuration utility enables you to modify the various configurable parameters of the access point. This utility must be running Windows 98 or Windows Millennium. The following steps illustrate the installation of the utility in Windows 98.

1. Insert the ME102 Wireless Access Point Resource CD into the CD-ROM drive. From the Windows 98 desktop, double-click on *My Computer*. Double-click on the CD-ROM drive to look into the content of the CD. Double-click on the *SNMPMANG* folder. Windows displays all of the files in the *\SNMPMANG* directory of the CD.
2. Double-click on the *SETUP* application icon to start the installation procedure. The InstallShields Wizard opens. Click on "Next" to continue.
3. Click on "Browse" to change the destination location where the Access Point SNMP utility is installed. Otherwise, click on "Next" to continue.
4. Modify the "Program Folders" entry field if desired. Click on "Next" to continue. InstallShields starts copying files into your system.
5. Click on "Finish" to complete the installation of the access point SNMP utility.

Assigning IP Address

In order to set the access point IP address you need to know the access point MAC address. Follow the steps below to give the access point a temporary address at the beginning and save the IP address permanently through the SNMP Configuration Utility.

Assigning temporary IP address

1. Connect an Ethernet station and the access point on the same subnet. The simplest way to accomplish this is to connect the access point and the Ethernet station to the same hub. You need to make sure that the station IP address and the Subnet Mask are configured properly. Also the new IP address for the access point must correspond to the same Subnet Mask.
2. From the Ethernet station, open an MS-DOS prompt window and enter a static route in the ARP table for the new IP address you want to assign. Use the "arp –s" command to do that:

   - arp –s "new-ip-address" "AP-MAC-address"

   ➲ Note: The MAC address of the access point is indicated on the bottom label of the access point.

3. Ping the access point, using the new IP address, to confirm the IP address assignment.

Saving the temporary IP address

Select an Ethernet/wireless station on the same subnet to install the access point SNMP utility. From the windows desktop of the station, select *Start ⇒ Program ⇒ NETGEAR ME102 AP ⇒ Access Point SNMP Manager*. You should be able to see the device that is configured with the new IP address.

Connect to the access point by selecting the access point and click on "Configure". Click on the IP Address folder tab. You might see a different IP address setting. Modify the IP address and Subnet Mask. Click on "Upgrade" to permanently save the new setting into the access point.

Configuring Access Point

From the Windows desktop, select *Start* ⇒ *Program* ⇒ *NETGEAR ME102 AP* ⇒ *Access Point SNMP Manager*. All accessible access points from this system are shown in a table. Select the access point, and click on "Configure". The configurable parameters are categorized into folders and are accessible by clicking on the folder tabs. The definitions of the parameters are explained in the following table.

General	MODEL ME102 WIRELESS ACCESS POINT
ESS ID	Enter a 32-character (maximum) extended service set ID in this field. The characters are case sensitive. With an access point, the wireless network always functions in infrastructure mode. The ESS ID assigned to the wireless nodes in the same network is required to match the access point ESS ID. The default ESS ID is "Wireless".
Channel	Only valid in ad-hoc mode, this field defines the wireless channel to use. In infrastructure mode, the wireless node automatically searches through all available wireless channels for an access point to be associated with. It is not necessary to select the wireless channel when operating in infrastructure mode. The default wireless channel to use is 6.
Rate	The Rate field allows you to define the data transfer rate. The default value is Auto. In this case, the best transfer rate is negotiated between the wireless node and the device it is communicating with. The highest possible wireless data transfer rate is 11Mbps. The other possible value for this entry field is 1-2Mbps, which means that the access point will only negotiate up to the wireless data transfer rate of 2Mbps.

IP Address	
IP Address	Assign Internet Protocol (IP) address to the access point.
Netmask	Assign IP Subnet Mask to the access point.
MAC Address	Displays the six-byte MAC address of the access point. This parameter is not changeable by the user.

Encryption	
Default Key	The ME102 Wireless access point supports 40-bit WEP data encryption. (40-bit WEP data encryption is also called 64-bit WEP data encryption by some vendors.) This parameter enables/disables encryption and select the 40-bit WEP data encryption key to use. Up to four keys can be defined in the access point. The possible values for this parameter are Disable, Key1, Key2, Key3, and Key4. . For more explanation on data encryption, please refer to the wireless network fundamental chapter at the beginning of this reference guide. The WEP data encryption method and the key used must be the same for all wireless nodes and access points in the same network. Note: the present version of the USB Configuration Utility software does not support WEP Passphrase.
Key1	One of the four data encryption keys defined in the access point. Each data encryption key contains five hexadecimal numbers, making it 40 bits wide. Together with the twenty-four factory-set bits to make up a 64-bit encryption key.
Key2	One of the four data encryption keys defined in the access point.
Key3	One of the four data encryption keys defined in the access point.
Key4	One of the four data encryption keys defined in the access point.
Authentication	Configurable between Open System (WEP disabled), Shared Key (40-bit WEP data encryption), and Both.

Operational Setting	
Fragmentation Setting	This is the packet length used for fragmentation. Packets larger than the size programmed in this field will be fragmented. The Fragment Threshold value must be larger than RTS Threshold value. The default value for Fragment Threshold is 2346.
RTS Threshold	The packet size that the wireless node uses to determine if it should use the CSMA/CD mechanism or the CSMA/CA mechanism for packet transmission. With the CSMA/CD transmission mechanism, the transmitting station sends out the actual packet as soon as it has waited for the silence period. With the CSMA/CA transmission mechanism, the transmitting station sends out a RTS packet to the receiving station, waits for the receiving station to send back a CTS packet before sending the actual packet data. The default value for RTS Threshold is 2346.
Preamble Type	A long transmit preamble allows the receiver to lock into the received bit patterns more easily. A short transmit preamble provides better performance. The default value is Long Preamble.

Ethernet Statistics	
Received Packets	Reports the various receive packet statistics on the Ethernet interface of the access point.
Transmitted Packets	Reports the various transmit packet statistics on the Ethernet interface of the access point.

Wireless Statistics	
Received Packets	Reports the various receive packet statistics on the wireless interface of the access point.
Transmitted Packets	Reports the various transmit packet statistics on the wireless interface of the access point.

Version	
Version Information	The software version number of the access point SNMP configuration utility.

APPENDIX A: HARDWARE SPECIFICATION

General Specifications	Model ME102 802.11 Wireless Access Point
Radio Data Rate	1, 2, 5.5, 11Mbps (Auto Rate Sensing)
Frequency	2.4Ghz to 2.5Ghz Direct Sequence Spread Spectrum (DSSS)
Range	Outdoor environment 1Mbps - 1650 ft (503 m) 2Mbps - 1320 ft (402 m) 5.5Mbps - 1155 ft (352 m) 11Mbps – 835 ft (255 m) Indoor environment 1Mbps - 500 ft (152 m) 2Mbps - 400 ft (122 m) 5.5Mbps - 270 ft (82 m) 11Mbps – 175 ft (53 m)
Encryption	40-bit (also called 64-bit) WEP data encryption
Maximum computers per network	Limited by the amount of wireless network traffic generated by each node; typically 30 to 70 nodes.
Ethernet Interface	IEEE 802.3i 10Mbps
USB Driver/Utility Platform	Microsoft Windows 98, 2000, Millennium
SNMP Utility Platform	Microsoft Windows 98, Millennium
Dimensions	L: 6.4 in (163 mm) W: 5.6 in (143 mm) H: 1.1 in (27 mm)
Weight	0.171 kg (0.076 lb)
Status LED	Power, Wireless Link/Activity, Ethernet Link/Act.
Power Adapter	5Vdc, 1.0A (customized plug for individual countries)
Environment Specifications	Operating temperature: 0 to 55 degree C
Electromagnetic Compliance	FCC Part 15 class B
Warranty	Limited 5-year warranty
Provided drivers	Microsoft Windows 95/B, 98, NT, 2000, Millennium
Dimensions	L: 145 mm (5.7 in.) W: 97 mm (3.8 in.) H: 14 mm (0.56 in.)
Weight	44.5 g (1.5 oz)
Status LED	Wireless Link
Environment Specifications	Operating temperature: 0 to 55 degree C
Warranty	Limited 5-year warranty