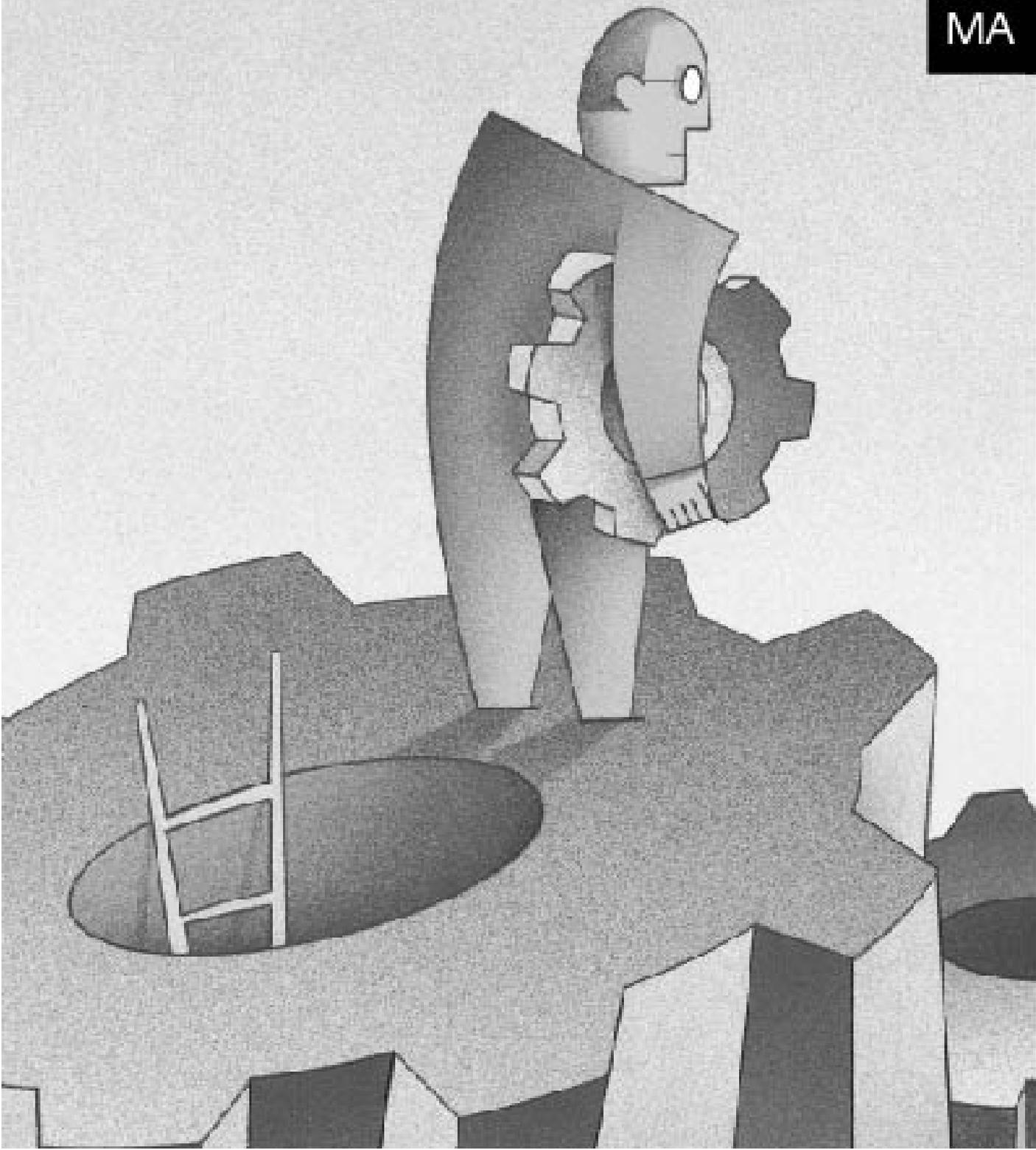


NETGEAR

802.11b Wireless USB Adapter Installation Guide

MODEL

MA 101



© 2001 by NETGEAR, Inc. All rights reserved.

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 MA101 Wireless USB 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:

1. This device may not cause harmful interference.
2. 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 MA101 Wireless USB 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 MA101 Wireless USB 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	1
BENEFITS	1
FEATURES	1
RELATED NETGEAR PRODUCTS	1
CHAPTER 2: WIRELESS NETWORK FUNDAMENTALS	2
WIRELESS NETWORK CONFIGURATION	2
SERVICE SET IDENTIFICATION (SS ID)	3
AUTHENTICATION AND WEP ENCRYPTION	3
WIRELESS CHANNEL SELECTION	4
CHAPTER 3: HARDWARE INSTALLATION	5
PACKAGE CONTENTS	5
HARDWARE DESCRIPTION	5
INSTALLING WIRELESS USB ADAPTER	5
CHAPTER 4: DRIVER INSTALLATION	6
WINDOWS 98 DRIVER SOFTWARE	6
WINDOWS MILLENNIUM DRIVER SOFTWARE	7
WINDOWS 2000 DRIVER SOFTWARE	8
CHAPTER 5: WIRELESS LAN CONFIGURATION	9
ADAPTER PROPERTIES CONFIGURATION	9
WLAN CONFIGURATION UTILITY	12
APPENDIX A: HARDWARE SPECIFICATION	16

CHAPTER 1: INTRODUCTION

The MA101 802.11b Wireless USB adapter enables you to effortlessly network avoiding the hassles of Ethernet wiring. It is designed for computers running Microsoft Windows 98, 2000, or Millennium. Its auto-sensing capability allows packet transfer at 11Mbps for maximum throughput, or speed reduction to the lower 1Mbps speed for distance or working in a noisy environment.

Benefits

- Quickly networks your employees without the time or expense of Ethernet cabling.
- Networks from any location in and around the home or office.
- Gives you constant access to corporate resources, e-mail and the intranet.
- Supports the vast majority of PCs and notebooks with USB interface.

Features

The key features of the MA101 Wireless USB adapter are:

- Reliable IEEE 802.11b standard-based wireless technology.
- 11Mbps high rate speed. Wireless nodes negotiate to operate in the optimal data transfer rate. In a noisy environment or when the distance between the wireless nodes is far, the wireless nodes automatically fall back to operate at the lower transfer rate of two or one Megabit per second.
- Highest level of data encryption using 128-bit Shared Key data encryption method. Lower level of data encryption or no data encryption is available to simplify your network setup or to improve data transfer rate.
- Supports multiple operating system platform including Microsoft Windows 98, Windows 2000, and Windows Millennium.

Related NETGEAR products

- MA401 802.11b Wireless PC Card
- ME102 802.11b Wireless Access Point
- MA301 802.11b Wireless PCI 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 a 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 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 spectrum 12.5Mhz 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 MA101 802.11b Wireless USB Adapter
- USB cable
- MA101 Wireless USB Adapter 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 MA101 Wireless USB Adapter 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 USB interface of the MA101 USB adapter allows the adapter to be connected with any USB Rev 1.1 compliant system by the USB cable. The USB LED on the MA101 adapter indicates the system status for operation. The RF LED on the MA101 card indicates the wireless link condition of the station with another wireless node or the associated access point.

Installing Wireless USB Adapter

Connect the MA101 802.11b wireless USB adapter with the PC or the notebook using an USB cable.

CHAPTER 4: Driver Installation

Windows 98 Driver Software

Installing Driver Software

1. To install the NETGEAR MA101 Wireless USB Adapter LAN driver for the first time in Windows 98:
2. Follow the procedure described in the hardware installation chapter to install the MA101 Wireless USB Adapter.
3. Upon connection, Windows 98 automatically detects the existence of the MA101 Wireless USB Adapter. An Add New Hardware Wizard window opens. Click on "Next" to continue.
4. In the next Add new Hardware Wizard window, select "Search for the best driver for your device (Recommended)." Click on "Next".
5. The next Add New Hardware Wizard window opens prompting for the location of the driver. Insert the MA101 USB adapter Resource CD into the CD-ROM drive. Click on "Browse".
6. Double-click on the CD-ROM drive letter to look into the content of the CD-ROM.
7. Double-click on the "WIN98" folder selection.
8. Click on "OK".
9. After returning to the original Add New Hardware Wizard window, make sure that the Specify a location:" entry field shows "D:\WIN98" assuming that D: is the driver letter for the CD-ROM drive. Click on "Next".
10. In the next window, Windows indicates that a Windows driver file is found and is ready to install the best driver for this device. Click on "Next".
11. Click on "Finish" when informed that the driver installation is complete.
12. Click on "Yes" when asked if you want to reboot the system.

The MA101 Wireless USB Adapter driver is now installed into your Windows 98 system.

Verifying Driver Installation

1. From the Windows 98 desktop, double-click on My Computer.
2. Double-click on Control Panel. Double-click on the System icon.
3. Click on the Device Manager folder tab.
4. Double-click on Network Adapter. There should be no yellow exclamation mark or red cross-sign on the MA101 Wireless USB Adapter selection.
5. Double-click on the MA101 Wireless USB Adapter. The Device Status windows should indicate that the MA101 USB adapter is working properly.

The installation of the MA101 Wireless USB Adapter driver in Windows 98 is now completed. Proceed to configuring the wireless parameters.

Windows Millennium Driver Software

Installing Driver Software

To install the NETGEAR MA101 Wireless USB Adapter LAN driver for the first time in Windows Millennium:

1. Follow the procedure described in the hardware installation chapter to install the MA101 Wireless USB Adapter.
2. Upon connection, Windows Millennium automatically detects the existence of the MA101 USB Adapter. An Add New Hardware Wizard window opens and indicates that new hardware has been found. Insert the MA101 USB adapter Resource CD into the CD-ROM drive. Make sure that "Automatic search for a better driver (Recommended)" is selected. Click on "Next" to continue.
3. Windows Millennium looks into the floppy disk drive and the CD-ROM drive for the appropriate driver. Windows Millennium automatically installs the appropriate driver from the CD for the MA101 USB Adapter. Click on "Finish".
4. Click on "Yes" when asked if you want to reboot the system.

The MA101 Wireless USB Adapter driver is now installed into your Windows Millennium system.

Verifying Driver Installation

1. From the Windows Millennium desktop, double-click on My Computer.
2. Double-click on Control Panel. Double-click on the System icon.
3. Click on the Device Manager folder tab.
4. Double-click on Network Adapter. There should be no yellow exclamation mark or red cross-sign on the NETGEAR MA101 Wireless USB Adapter selection.
5. Double-click on the MA101 Wireless USB Adapter. The Device Status windows should indicate that the MA101 USB adapter is working properly.

The installation of the MA101 Wireless USB Adapter driver in Windows Millennium is now completed. Proceed to configuring the wireless parameters.

Windows 2000 Driver Software

Installing Driver Software

1. Follow the procedure described in the hardware installation chapter to install the MA101 Wireless USB Adapter.
2. Upon connection, Windows 2000 automatically detects the existence of the MA101 Wireless USB Adapter. A Found New Hardware Wizard window opens and indicates that new hardware has been found. Click on Next.
3. In the next Found New Hardware Wizard window, click to select "Search for a suitable driver for my device (recommended)". Click on "Next" to continue.
4. The next Found New Hardware Wizard window opens prompting for the location of the driver. Insert the MA101 USB adapter Resource CD into the CD-ROM drive. Select "Specify a location" and click on "Next".
5. Type in "D:\WIN2000" assuming that D: is the driver letter for the CD-ROM drive.
6. Windows searches into the driver CD and locate the driver for the MA101 USB adapter. Verify that the Windows has found the driver in the "D:\WIN2000" directory. Click on "Next".
7. Click on "Yes" to continue when Windows indicates that the Digital Signature is not found.
8. Windows indicates that the software for the MA101 Wireless USB Adapter is now installed. Click on "Finish".

Verifying Driver Installation

1. From the Windows 2000 desktop, double-click on My Computer.
2. Double-click on Control Panel. Double-click on the System icon.
3. Click on the Hardware folder tab. Double-click on the Device Manager button.
4. Double-click on Network Adapter. There should be no yellow exclamation mark or red cross-sign on the MA101 Wireless USB Adapter selection.
5. Double-click on the MA101 Wireless USB Adapter. The Device Status windows should indicate that the MA101 USB adapter is working properly.

The installation of the MA101 Wireless USB Adapter driver in Windows 2000 is now completed. Proceed to configuring the wireless parameters.

CHAPTER 5: Wireless LAN Configuration

Adapter Properties Configuration

Device Properties Page

When running Windows 98 or Millennium

Wireless parameters for the MA101 Wireless USB Adapter can be modified from the Network control window.

1. From the Windows desktop, right-click on the Network Neighborhood icon. When a pop-up menu opens, move to select the Properties selection.
2. The Network window opens. Click on the "NETGEAR MA101 Wireless USB Adapter" selection in the component window. Click on the "Properties" button.
3. A window pops up displaying three folder tabs. Click on the *Advanced* folder tab. The property screen opens displaying a number of configurable parameters. These parameters are shown in the Wireless LAN Configuration Chapter.

When running Windows 2000

Configuring the network adapter properties for Windows 2000 is different from all other Windows operating systems.

1. From the Windows desktop, right-click on "My Computer". Click on the "Hardware" folder tab. Click on "Device Manager".
2. In the Device Manager window, double-click on "Network adapters" to show all network adapters. Double-click on "NETGEAR MA101 Wireless USB Adapter".
3. The NETGEAR MA101 Wireless USB Adapter Properties window opens. Click on the *Advanced* folder tab. The list of configurable parameters is shown.

Device Properties Modification

Table 5-1. Device Properties Parameters

General Specifications	Model MA101 Wireless USB Adapter
Authentication Type	Select between Open System and Shared Key authentication types
Channel	Only valid in 802.11 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.
Use WEP / Encryption Level	Set the data encryption level for the wireless node. The data encryption level must be the same between all wireless nodes and access points in the same network. The possible values for the data encryption level are Disable, 64 bits and 128 bits. 64-bit data encryption is also called 40-bit data encryption by some vendors. For more explanation on data encryption, please refer to the wireless network fundamental chapter at the beginning of this reference guide. Setting the data encryption level to Disable is to not use any encryption; this is also called Open System data encryption. Setting the data encryption level to 64-bit configures the wireless node to use the 40-bit (also called 64-bit) Shared Key data encryption method. 128-bit encryption is another possible Shared Key data encryption method.
SSID / ESSID	Enter a 32-character (maximum) service set ID in this field. The characters are case sensitive. When the wireless node is operating in 802.11 ad hoc mode, this field operates as the basic service set ID (BSS ID). All wireless nodes in the same network should use the same BSS ID. When in infrastructure mode, this field defines the extended service set ID (ESS ID). The ESS ID assigned to the wireless node is required to match the access point ESS ID for the wireless node to communicate with the access point. The default SS ID is "Wireless".
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.
Network Type / Operating Mode	Configurable between 802.11 ad hoc and infrastructure modes. In 802.11 ad hoc mode, the wireless nodes form their own local network where the end nodes communicate peer-to-peer without an access point. In infrastructure mode, the wireless searches all available wireless channels to associate with an access point. The default value for Network Type is Infrastructure.
Preamble Mode / 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 Tx Preamble.

Table 5-1. Device Properties Parameters (continued)

General Specifications	Model MA101 Wireless USB Adapter
Rate (Mbps)	The Rate field allows you to control the data transfer rate. The default value is Fully Automatic. In this case, the best transfer rate is negotiated between the wireless node and the device it is communicating with. This could be another wireless node or an access point. Other possible values for this field are 1, 2, 5.5, and 11.
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.
WEP Key #1 WEP Key #2 WEP Key #3 WEP Key #4	The encryption key used to encrypt/decrypt wireless data. When set to 64-bit (also called 40-bit by some vendors) data encryption mode, you may specify up to four different keys to encrypt wireless data. However, only one key is allowed in the 128-bit data encryption mode.
Key to Use	When the encryption level is set to 64-bit (also called 40-bit by some vendors) or 128-bit, the wireless LAN configuration utility allows you to specify up to four different keys to encrypt wireless data. The Default Tx field allows you to specify which one of the four keys to activate.
WEP Mode	Select between Mandatory and Optional

WLAN Configuration Utility

A wireless LAN configuration utility program is provided to give you information on your wireless network such as signal quality and link conditions, and to let you modify the various configurable wireless parameters.

WLAN Configuration Utility Installation

1. Insert the MA101 USB adapter Resource CD into the CD-ROM drive. From the Windows desktop, double-click on *My Computer*. Double-click on the CD-ROM drive letter to look into the content of the CD. Double-click on the *UTILITY* folder. The *\UTILITY* directory of the CD is now open.
2. Double-click on the *SETUP* application icon to start the installation procedure. The InstallShields Wizard opens. Click on "Next" to continue.
3. Click "Yes" on the Software License Agreement window to accept the agreement.
4. Click on "Browse" to change the destination location where the wireless LAN configuration utility is installed. Otherwise, click on "Next" to continue.
5. Modify the "Program Folders" field, if desired. Click on "Next" to continue. InstallShields starts copying files into your system.
6. Click on the "Yes, I want to restart my computer now." button selection to restart the computer. And click on "Finish" to complete the installation.

System Tray Applications

Note: The SysTray (System Tray) resides on one end of the taskbar in the Microsoft Windows desktop. It displays interface icons for memory-resident applications that execute in the background continuously, such as the clock, speaker volume, and virus detection.

The wireless LAN configuration utility installation for the MA101 Wireless USB Adapter adds a status reporting and configuration utility icon in the SysTray. Once you have completed the installation, the Windows SysTray should show the following icon in different colors. This icon indicates different status condition depending on the operating mode of the MA101 Wireless USB Adapter.



Icon color	Ad-hoc mode	Infrastructure mode
Red		The wireless adapter is not able to link to any access point or the link between the wireless adapter and the access point is lost.
Blue	The wireless adapter is ready to communicate or has successfully communicated with another wireless node.	The wireless adapter has established good communication with an access point and the signal quality is strong.

WLAN Parameter Modification

Double-clicking on the wireless SysTray icon activates the wireless LAN configuration utility for the MA101 Wireless USB adapter. You can click on any of the folder tab in the Wireless LAN configuration utility window to modify the operational parameters.

Status	
Network type / Operating Mode	Configurable between 802.11 ad-hoc and infrastructure modes. In 802.11 ad hoc mode, the wireless nodes form their own local network where the end nodes communicate peer-to-peer without an access point. In infrastructure mode, the wireless searches all available wireless channels to associate with an access point.
Channel	Only valid in 802.11 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.
SSID	Enter a 32-character (maximum) service set ID in this field. The characters are case sensitive. When the wireless node is operating in ad hoc mode, this field operates as the basic service set ID (BSS ID). All wireless nodes in the same network should use the same BSS ID. When in infrastructure mode, this field defines the extended service set ID (ESS ID). The ESS ID assigned to the wireless node is required to match the access point ESS ID for the wireless node to communicate with the access point.
Tx Rate	The Tx Rate field allows you to define the data transfer rate. The default value is Fully Automatic. In this case, the best transfer rate is negotiated between the wireless node and the device it is communicating with. This could be another wireless node or an access point. Other possible values for this field are 1Mbps, 2Mbps, 5.5Mbps, and 11Mbps.
MAC Address	The MAC Address field shows the MAC Address of the MA101 USB adapter.
Status	This field show the MAC address of the associated access point when the MA101 Wireless USB adapter is configured in infrastructure mode,
Signal Strength	Signal Strength indicates the signal strength of the radio frequency signal received by the wireless node.
Link Quality	Link Quality indicates how well that the wireless node is communicating with the associated access point or another wireless node.

Statistics	
Statistics	The Statistics screen shows the number of successfully Transmitted and Received packets. The packets are divided into Data, Mgmt and Rejected packets.

Site Survey	
Mac Address	The Mac Address of the Access Point.
SSID	The SSID of the Access Point.
Signal	The signal strength of the Access Point.
Channel	The channel used by the Access Point.
Encryption	The encryption of the Access Point is enable or disable.

Encryption	
Encryption	<p>Set the data encryption level for the wireless node. The data encryption level must be the same between all wireless nodes and access points in the same network. The possible values for the data encryption level are Disable, 64 bits and 128 bits. 64-bit data encryption is also called 40-bit data encryption by some vendors. For more explanation on data encryption, please refer to the wireless network fundamental chapter at the beginning of this reference guide.</p> <p>Setting the data encryption level to Disable is to not use any encryption; this is also called Open System data encryption. Setting the data encryption level to 64-bit configures the wireless node to use the 40-bit (also called 64-bit) Shared Key data encryption method. 128-bit encryption is another possible Shared Key data encryption method.</p>
Key #1 Key #2 Key #3 Key #4	The encryption key used to encrypt/decrypt wireless data. When set to 64-bit (also called 40-bit) data encryption mode, you may specify up to four different keys to encrypt wireless data. However, only one key is allowed in the 128-bit data encryption mode.
Default Key	When the encryption level is set to 64-bit (also called 40-bit by some other vendors) or 128-bit, the wireless LAN configuration utility allows you to specify up to four different keys to encrypt wireless data. The Default Tx field allows you to specify which one of the four keys to activate.
Mode	<p>The Mandatory mode: Not only the WEP of your USB adapter will be used, but also any other station needs to use WEP encryption in order to establish a communication with your station.</p> <p>The Optional mode: Your USB adapter can communicate with every other station regardless if they use WEP or not.</p>
Authentication Type	<p>The Open System mode is for any USB adapter.</p> <p>The Share Key mode allows the USB adapter to use a shared secret key.</p>

Advanced	
Preamble Mode	The Long mode is set for 144 bits. The Short mode is set for 72 bits.
Fragmentation 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/CTS 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.

Version	
Version	The Version screen shows the release information of the wireless LAN configuration utility software and the wireless nodes firmware.

APPENDIX A: HARDWARE SPECIFICATION

General Specifications		Model MA101 802.11b Wireless USB Adapter	
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	indoor environment	
	1Mbps - 1650 ft (503 m)	1Mbps - 500 ft (152 m)	
	2Mbps - 1320 ft (402 m)	2Mbps - 400 ft (122 m)	
	5.5Mbps - 1155 ft (352 m)	5.5Mbps - 270 ft (82 m)	
	11Mbps - 835 ft (255 m)	11Mbps - 175 ft (53 m)	
Encryption	64-bit (also called 40-bit) WEP data encryption 128-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.		
Bus interface	USB Rev 1.1 compatible.		
Provided drivers	Microsoft Windows 98, 2000, Me		
Dimensions	L: 4.2 in (107 mm) W: 3.4 in (87 mm) H: 0.95 in (24 mm)		
Weight	67 g (2.2 oz)		
RF LED	Wireless Link		
USB LED	System status		
Environment Specifications	Operating temperature: 0 to 55 degree C		
Warranty	Limited 5-year warranty		