Reference Manual for the Model ME102 802.11b Wireless Access Point

NETGEAR

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA
Phone 1-888-NETGEAR

M1-ME102NA-2
November 2002
© 2002 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 ME102 802.11b Wireless Access Point 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 ME102 802.11b Wireless Access Point 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 (ME102 802.11b Wireless Access Point) 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.
Preface - About This Guide

Chapter 1 - Introduction

About the Wireless Access Point .................................................................1-1
Key Features .................................................................................................1-2
   Related NETGEAR Products .................................................................1-2
   802.11b Standards-based Wireless Networking .....................................1-3
What’s in the Box? ..........................................................................................1-4
   The ME102 802.11b Wireless Access Point’s Front Panel .......................1-5
   The Wireless Access Point’s Rear Panel ..................................................1-6

Chapter 2 - Setting Up Basic Wireless Connectivity

What You Will Need Before You Begin .........................................................2-1
   Placement and Range Guidelines .............................................................2-2
   Cabling Requirements ..............................................................................2-2
   Computer Requirements .........................................................................2-2
   LAN Configuration Requirements ............................................................2-3
   Wireless Network Configuration Settings .................................................2-3
Setting Up the ME102 Wireless Access Point on Your LAN .........................2-4
Install the NETGEAR ME102 Wireless Access Point Manager .....................2-7

Chapter 3 - Protecting Your Wireless Network

Enabling Basic Wireless Access Security Features .......................................3-1

Chapter 4 - Advanced Configuration

Configuring Advanced Security .................................................................4-1
   Restricting Wireless Access by MAC Address .........................................4-1
   Protecting Access to Your ME102 Wireless Access Point ......................4-4
   Using the USB Configuration Manager .........................................................4-5
   When Should I Use the SNMP vs. the USB Configuration Manager Utilities? 4-6
Using Advanced Networking Features of the ME102 802.11b Wireless Access Point 4-7
   Viewing Status and Usage Statistics .........................................................4-7
   Configuring the ME102 LAN IP Settings .....................................................4-9
   Operational and Advanced Network Settings ............................................4-12
Configuring Wireless Network Bridging .......................................................4-14
Chapter 5 - Troubleshooting

Basic Functioning ........................................................................................................... 5-1
No lights are lit on the access point ........................................................................... 5-1
The Wireless Activity light is not lit ........................................................................... 5-2
The Ethernet Link/Act light is not lit .......................................................................... 5-2
I cannot access the Internet or the LAN with a wireless capable computer .......... 5-2

Appendix A - Technical Specifications

Appendix B - Wireless, Network, and Routing Basics

Related Publications ...................................................................................................... B-1
Wireless Networking ...................................................................................................... B-1
Wireless Network Configuration ................................................................................ B-2
Ad-hoc Mode (Peer-to-Peer Workgroup) ................................................................... B-2
Infrastructure Mode ................................................................................................. B-2
Extended Service Set Identification (ESSID) ............................................................ B-2
Authentication and WEP Encryption ....................................................................... B-3
Wireless Channel Selection .................................................................................... B-4
Ethernet Cabling ........................................................................................................ B-5
Cable Quality ........................................................................................................... B-5
Uplink Switches, Crossover Cables, and MDI/MDIX Switching .............................. B-6
Basic Router Concepts ............................................................................................. B-7
What is a Router? ....................................................................................................... B-7
Routing Information Protocol ................................................................................ B-7
IP Addresses and the Internet ................................................................................ B-7
Netmask .................................................................................................................. B-9
Subnet Addressing ................................................................................................ B-10
Private IP Addresses ............................................................................................... B-12
Single IP Address Operation Using NAT ............................................................... B-13
MAC Addresses and Address Resolution Protocol .............................................. B-14
Related Documents ............................................................................................... B-15
Domain Name Server ............................................................................................. B-15
IP Configuration by DHCP ................................................................................... B-16
Internet Security ..................................................................................................... B-16

Appendix C - Preparing Your Network

Preparing Your Computers for TCP/IP Networking ...................................................... C-1
Configuring Windows 95, 98, and ME for TCP/IP Networking .............................. C-2
Contents

Install or Verify Windows Networking Components ........................................... C-2
Enabling DHCP to Automatically Configure TCP/IP Settings .......................... C-4
Selecting Windows’ Internet Access Method ................................................... C-4
Verifying TCP/IP Properties ............................................................................. C-5
Configuring Windows NT, 2000 or XP for IP Networking ................................. C-5
Install or Verify Windows Networking Components ........................................... C-5
Verifying TCP/IP Properties ............................................................................. C-6
Configuring the Macintosh for TCP/IP Networking .......................................... C-6
  MacOS 8.6 or 9.x ........................................................................................... C-6
  MacOS X ........................................................................................................ C-7
  Verifying TCP/IP Properties for Macintosh Computers ...................................... C-8
Verifying the Readiness of Your Internet Account .............................................. C-9
  Are Login Protocols Used? ........................................................................... C-9
  What Is Your Configuration Information? ....................................................... C-9
  Obtaining ISP Configuration Information for Windows Computers ............... C-10
  Obtaining ISP Configuration Information for Macintosh Computers ............. C-11
Restarting the Network .................................................................................. C-12

Glossary

Index
List of Procedures

Procedure 2-1: Setting Up the Wireless Access Point ..................................................2-4
Procedure 2-2: Installing the ME102 Wireless Access Point Configuration Manager on a
Windows PC .............................................................................................................2-7
Procedure 3-1: Defining the ESSID and WEP Settings ..............................................3-2
Procedure 3-2: Changing the ESSID ............................................................................3-3
Procedure 3-3: Configuring WEP Encryption ...............................................................3-5
Procedure 4-1: Restricting Wireless Access by MAC Address ....................................4-2
Procedure 4-2: Changing the Built-In Password .........................................................4-4
Procedure 4-3: Using the USB Manager to Restore the ME102 Wireless Access Point
Default Factory Settings .........................................................................................4-6
Procedure 4-4: Configure the ME102 as a DHCP Client ............................................4-9
Procedure 4-5: Configuring Two ME102s for ‘Master-Slave’ Bridging .....................4-14
Procedure 4-6: Configuring Two ME102s for Point-to-Point Wireless Bridging ..........4-16
Procedure 4-7: Configuring Multi-Point Wireless Bridging .......................................4-17
Thank you for purchasing the NETGEAR™ ME102 802.11b Wireless Access Point.

The ME102 Wireless Access Point provides continuous, high-speed 11 Mbps access between your wireless and Ethernet devices.

**Note:** If you are unfamiliar with wireless communications, refer to Appendix B, “Wireless, Network, and Routing Basics,” to become more familiar with the terms and procedures used in this manual.

**Audience**

This reference manual assumes that the reader has basic to intermediate computer and Internet skills. However, basic computer network, Internet, and wireless technologies tutorial information is provided in the Appendices.

**Technical Support**

For help with any technical issues, contact Customer Support at 1-888-NETGEAR, or visit us on the Web at www.NETGEAR.com. The NETGEAR Web site includes an extensive knowledge base, answers to frequently asked questions, and a means for submitting technical questions online.

To get technical support, you register your product online at: www.NETGEAR.com/register
Typographical Conventions

This guide uses the following typographical conventions:

*italics*  Book titles and UNIX file, command, and directory names.

courier font  Screen text, user-typed command-line entries.

Initial Caps  Menu titles and window and button names.

[Enter]  Named keys in text are shown enclosed in square brackets. The notation [Enter] is used for the Enter key and the Return key.

[Ctrl]+C  Two or more keys that must be pressed simultaneously are shown in text linked with a plus (+) sign.

ALL CAPS  DOS file and directory names.

Special Message Formats

This guide uses the following formats to highlight special messages:

**Note:** This format is used to highlight information of importance or special interest.

**Procedure:** This format is used to let you know that you are following a sequence of steps required to complete a task.

**Warning:** This format is used to highlight information about the possibility of injury or equipment damage.

**Danger:** This format is used to alert you that there is the potential for incurring an electrical shock if you mishandle the equipment.
Chapter 1
Introduction

This chapter introduces the features, package contents, and appearance of the NETGEAR ME102 802.11b Wireless Access Point.

About the Wireless Access Point

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, an individual in-building access point provides a maximum connectivity range of about 300 feet. The ME102 802.11b 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 802.11b 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 802.11b Wireless Access Point allows packet transmission up to 11Mbps for maximum throughput, or reduced speed operation to compensate for distance or electromagnetic noise interference.
Key Features

The ME102 Wireless Access Point provides the following features:

- Interfaces directly to 10Mbps IEEE 802.3 Ethernet networks
- Supports IEEE 802.11 WLAN functions.
- Firmware is stored in flash memory and can be upgraded remotely.
- Configurable through USB and Ethernet ports.
- Power and wireless activity LED indicators.
- Dual External antennas supporting diversity.
- Secured Wired Equivalent Privacy (WEP) 128/104- and 64/40-bit encryption.
- Allow non-broadcasting System Service ID to prevent unauthorized connections.

Related NETGEAR Products

The following Netgear products can be configured to communicate with the ME102 Wireless Access Point.

- MA701 — 802.11b 11 Mbps Wireless Compact Flash Card.
- MA401 — 802.11b 11 Mbps Wireless PC Card.
- MA311 — 802.11b 11 Mbps Wireless PCI Adapter.
- MA101 — 802.11b 11 Mbps Wireless USB Adapter.
- MR814 — 802.11b 11 Mbps Wireless Cable/DSL Router with 4-port switch.
- FR114W — 802.11b 11 Mbps Wireless Ready Cable/DSL Router with 4-port switch.
- FM114P — 802.11b 11 Mbps Wireless Cable/DSL Router with Print Server and 4-port switch.
- POE101 — Power over Ethernet adapters.
802.11b Standards-based Wireless Networking

The ME102 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 Wireless Access Point provides an 11Mbps data transfer rate on the radio network.

The ME102 Wireless 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 Wireless 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
What’s in the Box?

The product package should contain the following items:

- ME102 802.11b Wireless Access Point
- AC power adapter (varies by region)
- A ten foot long Category 5 (Cat 5) Ethernet cable
- A five foot long USB Cable
- Wall mount kit
- Model ME102 Resource CD, including:
  - This guide
  - Warranty Card
  - Support Information Card

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the product for repair.
The ME102 802.11b Wireless Access Point’s Front Panel

The front of the ME102 contains wireless antennae on the left and right along with status LEDs.

![Figure 1-2: ME102 Front Panel](image)

You can use the LEDs to verify connections. Table 1-1 lists and describes each LED on the front of the wireless access point. These LEDs are yellow when lit.

<table>
<thead>
<tr>
<th>Label</th>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>Off</td>
<td>Power is not supplied to the wireless access point.</td>
</tr>
<tr>
<td></td>
<td>On -- Yellow</td>
<td>Power is supplied to the wireless access point.</td>
</tr>
<tr>
<td>Wireless</td>
<td>Off</td>
<td>Indicates no wireless link.</td>
</tr>
<tr>
<td></td>
<td>On -- Yellow</td>
<td>The wireless access point is ready and running.</td>
</tr>
<tr>
<td></td>
<td>Blinking</td>
<td>The wireless access point is transmitting or receiving data.</td>
</tr>
</tbody>
</table>
The Wireless Access Point’s Rear Panel

The rear panel of the ME102 802.11b Wireless Access Point contains port connections.

Viewed from left to right, the rear panel contains the following elements:

- AC power adapter outlet
- USB port
- Ethernet RJ-45 port for connecting the wireless access point to the local network.

**Figure 1-3: ME102 Rear Panel**

**Table 1-1. Back Panel Port Descriptions**

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>5 Volt 1 Amp power adapter socket.</td>
</tr>
<tr>
<td>Console</td>
<td>USB configuration console port.</td>
</tr>
</tbody>
</table>
| Ethernet Link/Activity | Off: Indicates no Ethernet link detected  
                        | Green On: Ethernet link detected but no activity  
                        | Green Blinking: Indicates Ethernet data traffic                               |
| Full/Half         | Indicates Full or Half duplex data traffic                                  |
Chapter 2
Setting Up Basic Wireless Connectivity

This chapter describes how to set up your ME102 802.11b Wireless Access Point for wireless connectivity on your Local Area Network (LAN). This basic configuration will enable computers with 802.11b compliant wireless adapters to do such things as connect to the Internet, or access printers and files on your LAN.

What You Will Need Before You Begin

You need to prepare these three things before you can establish a connection through your wireless access point:

1. A location for the ME102 that conforms to the placement and range guidelines below.
2. The wireless access point connected to your LAN through a device such as a hub, switch, router, or Cable/DSL gateway.
3. One or more computers with properly configured 802.11b compliant wireless adapters.

Note: Computers can connect over 802.11b wireless networks at a maximum range of 300 feet. This is a sufficient distance to allow for others outside your immediate area to access your network. Therefore, it is important to take appropriate steps to secure your network from unauthorized access. The ME102 802.11b Wireless Access Point provides highly effective security features which are covered in detail in the Securing Your Network chapter below. Netgear strongly recommends you deploy the security features appropriate to your needs.
Placement and Range Guidelines

Computers can connect over 802.11b wireless networks at a maximum range of 300 feet. However, the operating distance or range of your wireless connection can vary significantly based on the physical placement of the wireless access point.

For best results, identify a location for your wireless access point according to these guidelines:

- Away from potential sources of interference, such as PCs, large metal surfaces, microwaves, and cordless phones

Note: Warning: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the wireless access point.

- In an elevated location such as a high shelf, near the center of the area in which your PCs will operate.
  The best location is elevated, such as wall mounted or on the top of a cubicle, and at the center of your wireless coverage area for all the mobile devices.

Cabling Requirements

The ME102 Wireless Access Point connects to your LAN via twisted-pair a Category 3 or Category 5 Ethernet cable with RJ-45 connectors.

Computer Requirements

To access your network through the ME102 Wireless Access Point, a computer must have an installed a 802.11b wireless adapter.

To perform advanced configuration of the ME102 Wireless Access Point, you will need a computer that meets the following requirements:

- A CD-ROM drive.
- A USB and RJ-45 Ethernet ports
- Windows 98, Millennium, 2000, or XP
LAN Configuration Requirements

Your LAN will need to meet the following requirements.

- A 10 Mbps port on a device such as a hub, switch, or Cable/DSL router gateway.
- The ME102 802.11b Wireless Access Point defaults to getting its LAN TCP/IP settings automatically from the LAN via DHCP. If it does not find a DCHP server on the LAN, it then uses a static IP configuration of either the factory default of 192.168.0.5 with a subnet of 255.255.255.0, or the IP settings from the previous session before it was turned off.

Note: Most home and small office networking products use the Private Network Addressing network address of 192.168.0.0, which will work with the ME102 factory default settings, you will need to identify the TCP/IP network configuration of your organization, and then use the Advanced Configuration chapter procedures to configuring the ME102 Wireless Access Point for use with a public TCP/IP address. Please refer to Appendix C, “Preparing Your Network for assistance with TCP/IP configuration.

Wireless Network Configuration Settings

If this is a new wireless network installation, use the factory default settings to set up the network and verify wireless connectivity. If this is an addition to an existing wireless network, you will need to identify the wireless configuration and security parameters already defined. Please refer to Chapter 4, “Advanced Configuration” for advanced configuration and security settings.

Your ME102 802.11b Wireless Access Point factory default basic settings are as follows:

- SSID: Wireless

  Note: In order for the ME102 Wireless Access Point to communicate with a wireless adapter, both must be configured with the same SSID. For the access point and wireless nodes to communicate with each other, all must be configured with the same SSID.

- Mode (Infrastructure or Ad Hoc): Infrastructure

- For the 802.11b wireless adapters in your computers, configure them to match the settings listed above.

  Note: All NETGEAR, Inc. 802.11b wireless access products use the same factory settings as the ME102 and will work without requiring any configuration changes.
Setting Up the ME102 Wireless Access Point on Your LAN

This section provides instructions for setting up the ME102 802.11b Wireless Access Point.

Procedure 2-1: Setting Up the Wireless Access Point

Estimated setup time: 10 to 15 minutes

There are three steps to setting up your wireless access point:

1. Set up the wireless access point on your network.
2. Configure wireless access to your network.
3. Verify wireless connectivity to your network.

Follow the steps below to set up your wireless access point on your network.

1. Set up the ME102 Wireless Access Point.
   a. Unpack the box and verify the contents.
   b. Identify a flat surface where you will put the wireless access point. For best results, follow these guidelines:
      • Place it away from potential sources of interference, such as PCs, monitors, TVs, microwaves, cordless phones, or large metal surfaces.

      Warning: Failure to follow these guidelines can cause intermittent or complete failure of wireless connectivity.

      • Place it in an elevated location such as a high shelf or on a wall in the center of your wireless access area.
c. Connect the Ethernet cable (A) from your ME102 Wireless Access Point to a LAN port on your Cable/DSL router.

![Diagram showing the connection between ME102 and Cable/DSL router]

**Figure 2-1: Connect the ME102**

*Note:* This procedure explains how to connect to your network through a Cable/DSL router. For other configurations, please see the Advanced Configuration chapter below.

d. Lift the antennae on either side so that they are vertical.

e. Connect the power adapter to the wireless access point and plug the power adapter in to a power outlet. The Power Light and Wireless Activity lights should light up.

![Images of ME102's Power and Wireless Activity lights]

**Figure 2-2: ME102 lights**

Also, the Ethernet Link/Act light in the back will flash when there is network activity.
2. Configure wireless access.

   a. Any 802.11b compliant wireless device can communicate with the ME102 Wireless Access Point.

   b. Configure your wireless adapter to use the ME102 802.11b Wireless Access Point factory default settings as follows:
      - ESSID: **Wireless**
      - Mode (Infrastructure or Ad Hoc): **Infrastructure**

      *Note:* All NETGEAR, Inc. 802.11b wireless access products use the same factory settings as the ME102 and will work without requiring any configuration changes.

      - For other 802.11b wireless adapters, configure them to match the settings listed above.

3. Verify wireless connectivity to your network.

   Using a computer with an 802.11b wireless adapter, verify connectivity by using a browser such as Netscape or Internet Explorer to connect to the Internet, or check for file and printer access on your network.

   *Note:* If you are unable to connect, see to Troubleshooting Tips below or to the Reference Manual for the Model ME102 802.11b Wireless Access Point on the Model ME102 Resource CD.
Install the NETGEAR ME102 Wireless Access Point Manager

The NETGEAR ME102 802.11b Wireless Access Point includes a configuration utility for managing your wireless access point. For your convenience, the Model ME102 Resource CD contains the following two versions of this utility:

1. The NETGEAR ME102 Wireless Access Point SNMP Manager
   The SNMP version of the utility provides convenient wireless or Ethernet LAN access to your wireless access point even if it is located in another area or mounted high on a wall.

2. The NETGEAR ME102 Wireless Access Point USB Manager
   The USB version of the utility provides trouble-free access to your wireless access point directly through a USB cable attached to a PC, bypassing the wireless and LAN network, so that you can preconfigure or troubleshoot your wireless access point settings.

Both versions of the configuration utility provide essentially the same functions.

Procedure 2-2: Installing the ME102 Wireless Access Point Configuration Manager on a Windows PC

The access point SNMP configuration utility enables you to modify the various configurable parameters of the access point. This utility must be run on Windows 98, ME, 2000 or XP.

1. Insert the ME102 Wireless Access Point Resource CD into the CD-ROM drive.
2. Windows displays the splash screen with the Install Utility & Driver link.
3. Click on Install Utility & Driver link. The InstallShield Wizard opens.
4. Follow the InstallShield Wizard prompts to complete the installation.
Chapter 3
Protecting Your Wireless Network

The absence of a physical connection between nodes makes wireless links vulnerable to information theft. This chapter describes how to use the basic security features of the ME102 802.11b Wireless Access Point to protect your network.

Enabling Basic Wireless Access Security Features

There are several ways you can strengthen the security of access to your wireless network.

- Change the factory default SSID setting of the ME102 802.11b Wireless Access Point.
- Enable Wired Equivalent Privacy (WEP) encryption of the wireless data communications.
- Change the factory default private Administrator and public User passwords of the ME102 802.11b Wireless Access Point.
- Restrict wireless access based on MAC address.
- Place the ME102 802.11b Wireless Access Point in a location where it cannot be physically tampered with.

In addition to the ME102 wireless security features, you should also configure appropriate LAN network security features such as requiring a user name and password to access the shared resources in your network.

Netgear strongly recommends that, at a minimum, you change the SSID of your ME102. The procedures below identify how to change the SSID and WEP encryption settings of your ME102 802.11b Wireless Access Point. Stronger security options are covered in the Advanced Configuration chapter below.
Procedure 3-1: Defining the ESSID and WEP Settings

1. For a new wireless network, print this form and fill in the configuration parameters.

For an existing wireless network, print this form and fill in the configuration parameters. The person who set up or is responsible for the network will be able to provide this information.

- **ESSID**: The Extended Service Set Identification (ESSID) identifies the wireless local area network. Wireless is the default ME102 ESSID. However, you may customize it by using up to 32 alphanumeric characters. Netgear recommends that you write your customized SSID on the line below.

  **Note**: When configuring wireless adapter cards, the ESSID in the wireless access point is the SSID you configure in the wireless adapter card. In order for the ME102 802.11b Wireless Access Point to communicate with a wireless adapter, both must be configured with the same SSID. For the access point and wireless nodes to communicate with each other, all must be configured with the same SSID.

  ESSID: ______________________________

- **WEP Encryption key**: The default WEP encryption key number is 1, and the default key size is 64 bits.

  **Note**: The key number as well as the key value used by both the ME102 Wireless Access Point and wireless nodes must be the same.

  WEP Encryption Passphrase: ______________________________

  WEP Encryption Key Size, circle one: 64 or 128 bits

2. Use the procedures below to configure basic security settings in the ME102.

3. Store this information in a safe place.
Procedure 3-2:  Changing the ESSID

The ME102 Wireless Access Point allows you to restrict access to your wireless network based on the SSID and WEP keywords. Following the steps below to perform this procedure.

1. From the Windows desktop, select **Start => Program => NETGEAR ME102 AP => Access Point SNMP Manager**. The SNMP Manager main window displays the name and IP address of the accessible ME102 Wireless Access Points.

2. Select the access point you want to configure and click Login.

![NETGEAR ME102 Access Point SNMP Manager](image)

**Figure 3-1: NETGEAR ME102 Access Point SNMP Manager**
3. When prompted, enter **private** as the default Password.

The SNMP management dialog box opens. It is divided into seven tabs: General, IP Setting, Encryption, Operational Setting, Authorized MAC, Advanced, Statistics and About. The default tab is General.

![SNMP Manager General Tab Page](image)

**Figure 3-2: SNMP Manager General Tab Page**

4. To change the ESSID, enter a new ESSID.

   **Note:** The characters are case sensitive. An access point always functions in infrastructure mode. The SSID for any wireless device communicating with the access point must match the ESSID configured in the access point.

5. Click Apply or OK for the changes to take effect.
Procedure 3-3: Configuring WEP Encryption

The ME102 Wireless Access Point allows you to restrict access to your wireless network based on WEP keywords. Following the steps below to perform this procedure.

1. From the Windows desktop, select Start => Program => NETGEAR ME102 AP => Access Point SNMP Manager. The SNMP Manager main window displays the name and IP address of the accessible ME102 Wireless Access Points.

![Figure 3-3: NETGEAR ME102 Access Point SNMP Manager](image)

2. Select the access point you want to configure and click Login.

3. When prompted, enter private as the default Password.

The SNMP management dialog box opens. It is divided into seven tabs: General, IP Setting, Encryption, Operational Setting, Authorized MAC, Advanced, Statistics and About. The default tab is General.

Figure 3-3: NETGEAR ME102 Access Point SNMP Manager

Protecting Your Wireless Network
4. Click the Encryption Tab option from the ME102 Access Point SNMP Manager window.

![SNMP Manager Encryption Tab Page](image)

**Figure 3-4: SNMP Manager Encryption Tab Page**

5. Select the Authentication Type you will use. The choices are:
   - Open System -- WEP disabled
   - Shared Key -- 64 or 128-bit WEP data encryption enabled
   - Both

6. Check the Enable Encryption WEP Key box and choose 64 or 128-bit in the key length drop down both.

   **Note:** A larger encryption key requires more processing to encode/decode the messages. Larger encryption key lengths may slow the communications process response times.
7. Enter the Create with Passphrase radio button and enter the passphrase from the configuration worksheet your filled out in the procedure above. When you click the Apply button, the configuration manager utility will automatically generate the WEP keys.

**Note:** The characters are case sensitive. Be sure to use the same passphrase when configuring the other wireless devices that will communicate with this wireless access point.

8. Click Apply then OK for the changes to take effect.
This chapter describes how to configure the advanced security and networking features of your ME102 802.11b Wireless Access Point.

**Configuring Advanced Security**

The ME102 802.11b Wireless Access Point provides a variety of advanced features, such as:

- Restrict wireless access based on MAC address.
- Change the factory default **private** Administrator password and **public** User passwords of the ME102 802.11b Wireless Access Point.

These features are discussed below.

**Restricting Wireless Access by MAC Address**

Each device on Ethernet and wireless LAN networks have a media access control (MAC) address, which is a unique 48-bit number assigned to each device by the manufacturer. A highly secure way of protecting unauthorized access to your wireless network is to restrict access to only those devices whose MAC addresses you specify. To do so, you must configure your wireless access point to recognize and accept communications from the MAC address of only authorized wireless devices. Follow the steps in the procedure below to restrict access to your ME102 by MAC address.
Procedure 4-1: Restricting Wireless Access by MAC Address

**Note:** This procedure is only possible via the ME102 Wireless Access Point SNMP Manager. You cannot use the USB Manager to restrict wireless access by MAC address.

1. From the Windows desktop, select `Start => Program => NETGEAR ME102 AP => Access Point SNMP Manager`. The SNMP Manager main window displays the name and IP address of the accessible ME102 Wireless Access Points.

![NETGEAR ME102 Access Point SNMP Manager](image)

**Figure 4-1: NETGEAR ME102 Access Point SNMP Manager**

2. Select the access point you want to configure and click Login.

3. When prompted, enter `private` as the default Password.

   The SNMP management dialog box opens. It is divided into seven tabs: General, IP Setting, Encryption, Operational Setting, Authorized MAC, Advanced, Statistics and About. The default tab is General.
4. Click the Authorized MAC Tab option from the ME102 Access Point SNMP Manager window.

![Figure 4-2: SNMP Manager Authorized MAC Tab Page](image)

5. Click the Authorization Table Enable checkbox.

6. Enter the MAC addresses you want to allow to access your wireless network.
   - Load From File button -- Press this button to load a file with the MAC addresses that can be associated with the ME102 Wireless Access Point.
     
     **Note:** You must use a text file containing a list of the MAC addresses. Refer to the sample MAC.txt file on the *Model ME102 Resource CD* as an example.
   
   - Download to AP button -- Press this button to download the authorized MAC Addresses to the ME102 Wireless Access Point from the current PC.
   
   - Get From AP button -- Press this button to get the authorized of currently wirelessly connected MAC Addresses from the ME102 Wireless Access Point.

7. Click Apply or OK for the changes to take effect.
Protecting Access to Your ME102 Wireless Access Point

For security reasons, the wireless access point has its own user name and password. NETGEAR recommends that you change this password to a more secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of both upper and lower case letters, numbers, and symbols. Your password can be up to 30 characters.

Note: If you change the administrator password, you can always reset the ME102 to the factory default by using the Netgear ME102 Wireless Access Point USB Manager as explained below.

Procedure 4-2: Changing the Built-In Password

1. From the Windows desktop, select Start => Program => NETGEAR ME102 AP => Access Point SNMP Manager. The SNMP Manager main window displays the name and IP address of the accessible ME102 Wireless Access Points.

   ![NETGEAR ME102 Access Point SNMP Manager](image)

   Figure 4-3: NETGEAR ME102 Access Point SNMP Manager

2. Select the access point you want to configure and click Login.
3. When prompted, enter **private** as the default Password. The SNMP management dialog box opens. It is divided into seven tabs: General, IP Setting, Encryption, Operational Setting, Authorized MAC, Advanced, Statistics and About. The default tab is General.

4. Click the Encryption Tab option from the ME102 Access Point SNMP Manager window.

![Figure 4-4: SNMP Manager Operational Tab Page](image)

5. Select the Password Setting Administrator check box.

6. Enter a new administrator password.

7. Click Apply or OK for the changes to take effect. Be sure to record the new password on your configuration settings form from the procedure above and store it in a safe place.

**Using the USB Configuration Manager**

The installation example below illustrates the Wireless Access Point configuration through its USB interface of a connected PC. This PC must be running Windows 98, Windows 2000, Windows Millennium or Windows XP.
When Should I Use the SNMP vs. the USB Configuration Manager Utilities?

For most functions, the SNMP and USB configuration manager utilities are identical. However, there are several key differences.

- Only the SNMP Configuration Manager can configure the ME102 to restrict access by MAC address.
- The USB Configuration Manager does not need a password to access the configuration options.
- Because the SNMP Configuration Manager works over the wireless connection, it is more convenient to use, especially if the ME102 Wireless Access Point is placed on a high shelf or on a wall.
- Because the USB Configuration Manager works directly between a Windows PC and the ME102 Wireless Access Point over a USB cable, problems with an Ethernet LAN or wireless configuration will not interfere with using the USB Configuration Manager. Also, the USB connection allows you to preconfigure a ME102 Wireless Access Point for use in a different LAN setting.

The procedures for installing and using the USB Configuration Manager are presented below.

Procedure 4-3: Using the USB Manager to Restore the ME102 Wireless Access Point Default Factory Settings

1. From the Windows desktop, select Start => Programs => 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.
2. Click on Configure to go into the main USB manager window.
3. Click the Operational Setting to display the tab page below.
4. Click Restore to erase your configuration settings and restore the ME102 factory default settings for the SSID of Wireless, on Channel 6, no encryption, and the Administrator password of private. When you are done, click Apply or OK button for the changes to take effect.
Using Advanced Networking Features of the ME102 802.11b Wireless Access Point

The ME102 provides several advanced networking features such as:

- Status and usage statistics.
- Advanced network configuration settings.
- Advanced network to network configurations.

These features are presented below.

**Viewing Status and Usage Statistics**

Open the Statistics Tab of the configuration utility to view the ME102 usage statistics.
The Statistics Tab page provides status and usage information. This screen shows the following parameters:

**Table 4-1. Menu 3.2 - Statistics Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Received Packets</strong></td>
<td></td>
</tr>
<tr>
<td>Total Bytes</td>
<td>The number of bytes in the frames that have received</td>
</tr>
<tr>
<td>Total Packets</td>
<td>The number of packets received</td>
</tr>
<tr>
<td>CRC Errors</td>
<td>The number of packets received with CRC Errors</td>
</tr>
<tr>
<td><strong>Transmitted Packets</strong></td>
<td></td>
</tr>
<tr>
<td>Total Bytes</td>
<td>The number of bytes in the frames that have transmitted</td>
</tr>
<tr>
<td>Total Packets</td>
<td>The number of packets transmitted</td>
</tr>
<tr>
<td>CRC Errors</td>
<td>The number of packets transmitted with CRC Errors</td>
</tr>
<tr>
<td><strong>Received Packets</strong></td>
<td></td>
</tr>
<tr>
<td>Unicast Packets</td>
<td>The number of unicast packets that were successful received</td>
</tr>
<tr>
<td>Broadcast Packets</td>
<td>The number of broadcast packets that were successful received</td>
</tr>
<tr>
<td>Multicast Packets</td>
<td>The number of multicast packets that were successful received</td>
</tr>
<tr>
<td><strong>Transmitted Packets</strong></td>
<td></td>
</tr>
<tr>
<td>Unicast Packets</td>
<td>The number of unicast packets that were successful transmitted</td>
</tr>
<tr>
<td>Broadcast Packets</td>
<td>The number of broadcast packets transmitted</td>
</tr>
<tr>
<td>Multicast Packets</td>
<td>The number of multicast packets transmitted</td>
</tr>
</tbody>
</table>
Configuring the ME102 LAN IP Settings

You can configure the ME102 802.11b Wireless Access Point to obtain its IP configuration dynamically from your network via DHCP. Use the procedure below to change these settings.

Procedure 4-4: Configure the ME102 as a DHCP Client

The IP Setting tab page of the configuration utility lets you view and configure the following LAN IP settings for the ME102 802.11b Wireless Access Point:

- View IP Information.
  - MAC Address
  - IP Address
  - Subnet Mask
  - Gateway
- DHCP Setting -- Enable the ME102 to obtain its IP configuration automatically via DHCP.
- DHCP Primary Port -- Specify whether the ME102 should get its DHCP configuration from the Ethernet or Wireless connections.

Follow the steps below to perform this procedure.

**Note:** If you change the LAN IP address of the wireless access point while connected through the browser, you will be disconnected. Restart your computer to establish a new connection and log in again. Make sure the ME102 and your computer are in the same subnet.
1. From the Windows desktop, select **Start => Program => NETGEAR ME102 AP => Access Point SNMP Manager**. The SNMP Manager main window displays the name and IP address of the accessible ME102 Wireless Access Points.

![NETGEAR ME102 Access Point SNMP Manager](image)

Figure 4-5: NETGEAR ME102 Access Point SNMP Manager

2. Select the access point you want to configure and click Login.

3. When prompted, enter **private** as the default Password.

   The SNMP management dialog box opens. It is divided into seven tabs: General, IP Setting, Encryption, Operational Setting, Authorized MAC, Advanced, Statistics and About. The default tab is General.
4. Click the IP Setting Tab option from the ME102 Access Point SNMP Manager.

![Figure 4-6: SNMP Manager IP Setting Tab Page](image)

5. Check the DHCP Enable box, and choose the DHCP Primary Port you will use.
6. Click Apply or OK for the changes to take effect.
# Operational and Advanced Network Settings

The following table explains each of the configurable parameters of the ME102 Wireless Access Point in Operational Setting screen.

<table>
<thead>
<tr>
<th>CONFIGURATION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Setting</td>
<td>This option allows you to change a new password and confirm password in Administrator mode and User mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> private for Administrator, public for User</td>
</tr>
<tr>
<td>Preamble Type</td>
<td>A long transmit preamble allows the receiver to lock into the received bit patterns more easily and better backward compatibility with some older legacy wireless station.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> Long</td>
</tr>
<tr>
<td>Fragmentation Threshold</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 2346</td>
</tr>
<tr>
<td>RTS Threshold</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 2346</td>
</tr>
<tr>
<td>Restore</td>
<td>Click this button to restore the default settings of the ME102 Access Point.</td>
</tr>
</tbody>
</table>
The following table explains each of the configurable parameters of the ME102 Wireless Access Point in the Advanced Tab page. The following table explains each of the configurable parameters of the ME102 Wireless Access Point in Operational Setting screen.

<table>
<thead>
<tr>
<th>CONFIGURATION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SNMP trap messages</td>
<td>This option allows you to enable the SNMP trap broadcast messages sent in the wired Ethernet.</td>
</tr>
<tr>
<td></td>
<td>Default: Disable</td>
</tr>
<tr>
<td>Enable ESSID Broadcast</td>
<td>Disable ESSID broadcast allows you to prevent the unauthorized user from connecting to your access point if you will use Open System as the authentication type. Note that: if you need more secure wireless connection, consider using WEP encryption.</td>
</tr>
<tr>
<td></td>
<td>Default: Enable</td>
</tr>
</tbody>
</table>
Configuring Wireless Network Bridging

The ME102 802.11b Wireless Access Point provides a variety of advanced features which allow you to build large wireless networks which cover large areas and allow many Ethernet devices seamless access to the extensive network. Examples of wireless bridged configurations are:

- Client Access Point to Access Point.
- Point to point wireless bridging.
- Multi-point wireless bridging.

These features are discussed below.

Procedure 4-5: Configuring Two ME102s for ‘Master-Slave’ Bridging

1. Configure the ME102 labelled AP1 in the illustration in access point mode.

   ![Diagram showing ME102 in Access Point Mode]

   **Note:** To avoid problems, you may want to restore the factory default settings, and then proceed to the following setups.
a. From the Windows desktop, select Start => Program => NETGEAR ME102 AP => Access Point SNMP Manager. The SNMP Manager main window displays the name and IP address of the accessible ME102 Wireless Access Points.

b. Select the access point that corresponds to AP1 in the illustration above and click Login.

c. When prompted, enter private as the default Password. The SNMP management dialog box opens. It is divided into seven tabs: General, IP Setting, Encryption, Operational Setting, Authorized MAC, Advanced, Statistics and About. The default tab is General.

d. Click the IP Setting Tab option and verify that the IP Address conforms to the LAN network address of the router.

e. Click on the DHCP Setting DHCP Enable check box to let the ME102 get its TCP/IP configuration from the DHCP server in the router, and click the Ethernet radio button under DHCP Primary Port to tell the wireless access point to get its TCP/IP configuration from the router through the Ethernet connection that AP1 has with the router.

f. Click Apply or OK to apply the settings for AP1.

2. **Configure the ME102 labelled AP2 in the illustration to operate in Client Mode.**

a. Log in to AP2, click the Operational Setting Tab, and then click on the Operational Mode button to open the Operational Mode dialogue box.

b. Select the Access Point Client radio button to set AP2 in client mode.

c. Enter the MAC address of AP1.

d. Click OK to save your settings, and then OK again to save your configuration changes for AP2.

e. Be sure that the channel, SSID, and WEP authentication settings are the same for both AP1 and AP2.

3. **Verify connectivity across the LAN.**

Verify the following parameters for both access points:

- AP1 is in regular Access Point mode.
- AP2 is in Access point Client mode.
- Verify that the LAN network configuration the ME102 Wireless Access Points both are configured to operate in the same LAN network address range as the LAN devices.
- Both use the same ESSID, Channel, authentication mode, if any, and WEP keys if WEP encryption is in use.
• AP2 set in Access Point Client mode must have AP1’s MAC address in its Preferred BSSID field.

• A PC on the same hub or switch as the ME102 should be able to connect to the router and use the Internet or share files and printers of PCs connected to the router.

• Wireless stations will be able to connect to AP1, connect to the Internet, and share files and printers with PCs on the hub or router.

• A PC on the router should be able to connect to a PC on the hub.

• Wireless stations will not be able to connect to AP2.

**Procedure 4-6: Configuring Two ME102s for Point-to-Point Wireless Bridging**

**Note:** ME102s configured for Point-to-Point wireless bridging do not communicate with wireless clients.

1. Configure the ME102 (AP1) on LAN 1 in Wireless Bridging Point-to-Point Mode.

2. Configure the ME102 (AP2) on LAN 2 in Wireless Bridging Point-to-Point Mode.

3. Configure and verify the following parameters for both access points:

   • Verify that the LAN network configuration of the ME102 Wireless Access Points both are configured to operate in the same LAN network address range as the LAN devices

   • Both use the same ESSID, Channel, authentication mode, if any, and WEP keys if WEP encryption is in use.
If using DHCP, the ME102 on the same physical LAN as the router should be set to get with the DHCP Primary Port as Ethernet, and all the other APs should be set to get with the DHCP Primary Port as Wireless.

- AP1 must have AP2’s MAC address in its Remote AP MAC address field, and AP2 must have AP1’s MAC address in its Remote AP MAC address field.

4. Verify connectivity across the LAN 1 and LAN 2.
   - A PC on either LAN should be able to connect to the Internet or share files and printers of any other PCs or servers connected to the LAN 1 or LAN 2.
   - Wireless stations will not be able to connect to either APs.

**Procedure 4-7: Configuring Multi-Point Wireless Bridging**

1. Configure ME102 (AP1) on LAN 1 in Wireless Bridging Point-to-Point Mode.
2. Because it is in the central location, configure ME102 (AP2) on LAN 2 in Wireless Bridging Point-to-MultiPoint Mode.
3. Configure the ME102 (AP3) on LAN 3 in Wireless Bridging Point-to-Point Mode.
4. Configure and verify the following parameters for all access points:
Verify that the LAN network configuration the ME102 Wireless Access Points both are configured to operate in the same LAN network address range as the LAN devices.

Only one AP is configured in Multi-Point Mode, and all the others are in Point-to-Point wireless bridging mode.

All APs must be on the same LAN. That is, all the APs LAN IP address must be in the same network.

If using DHCP, the ME102 on the same physical LAN as the router should be set to get with the DHCP Primary Port as Ethernet, and all the other APs should be set to get with the DHCP Primary Port as Wireless.

Both use the same ESSID, Channel, authentication mode, if any, and WEP keys if WEP encryption is in use.

All Point-to-Point APs must have AP1’s MAC address in its Remote AP MAC address field.

Verify connectivity across the LANs.

A PC on any LAN should be able to connect to the Internet or share files and printers of any other PCs or servers connected to any of the three LANs.

Wireless stations will not be able to connect to either APs.

Note: You can extend this multi-point bridging to up to eight LANs by adding additional ME102s configured in Point-to-Point mode for each additional LAN.
Chapter 5
Troubleshooting

This chapter gives information about troubleshooting your ME102 802.11b Wireless Access Point. After each problem description, instructions are provided to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the wireless access point on?
- Have I connected the wireless access point correctly?
  Go to “Basic Functioning” on page 5-1.
- I can’t remember the wireless access point’s configuration password.
  Go to “Using the USB Configuration Manager” on page 4-5.

Basic Functioning

If you have trouble setting up your ME102, check the tips below.

No lights are lit on the access point

The access point has no power.

- Make sure the power cord is connected to the access point.
- Make sure the power adapter is connected to a functioning power outlet. If it is in a power strip, make sure the power strip is turned on. If it is plugged directly into the wall, verify that it is not a switched outlet.
- Make sure you are using the correct NETGEAR power adapter supplied with your access point.
The Wireless Activity light is not lit

The access point’s antennae are not working.

- If the Wireless Activity light is off, disconnect the adapter from its power source and then plug it in again. Contact NETGEAR if the Wireless Activity light remains off.

The Ethernet Link/Act light is not lit

There is a hardware connection problem.

- Make sure the cable connectors are securely plugged in at the access point and the network device (hub, switch, or router).
- Make sure the connected device is turned on.
- Be sure the correct cable is used. Use a standard Category 5 Ethernet patch cable. If the network device has Auto Uplink™ (MDI/MDIX) ports, you may use either a cross-over cable or a normal patch cable.

I cannot access the Internet or the LAN with a wireless capable computer

There is a configuration problem.

- You may not have restarted the computer with the wireless adapter to have TCP/IP changes take effect. Restart the computer.
- The computer with the wireless adapter may not have the correct TCP/IP settings to communicate with the network. Restart the computer and check that TCP/IP is set up properly for that network. The usual setting for Windows is the Network Properties are set to Obtain an IP address automatically.
- The access point’s default values may not work with your network. Install the ME102 configuration software and see the Reference Guide in the Doc folder on the Resource CD for details.
Appendix A
Technical Specifications

This appendix provides technical specifications for the ME102 802.11b Wireless Access Point

**ME102 802.11b Wireless Access Point**

**Power Adapter**
- North America: 120V, 60 Hz, input
- All regions (output): 5 V DC @ 1A output

**Physical Specifications**
- Dimensions: H: 0.56 in (14 mm)
- W: 3.8 in (97 mm)
- D: 5.7 in (145 mm)
- Weight: 0.076 lb. (171 g)
- LED Status Indicators: Power, Wireless Link/Activity, Ethernet Link/Act with full or half duplex indication

**Environmental Specifications**
- Operating temperature: 32°-122° F (0° to 50° C)
- Operating humidity: 90% maximum relative humidity, noncondensing

**Electromagnetic Emissions**
- Meets requirements of: FCC Part 15 Class B

**Interface Specifications**
- Local Ethernet: 10BASE-T, RJ-45
- Data, Routing, and Security Protocols:
  - IEEE 802.3i 10Mbps, IEEE 802.11b (Wi-Fi)
  - TCP/IP, DHCP, 64/128-bit WEP Data Encryption
## Wireless

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radio Data Rate</td>
<td>1, 2, 5.5, 11Mbps Auto Rate Sensing</td>
</tr>
<tr>
<td>Frequency</td>
<td>2.4-2.5Ghz</td>
</tr>
<tr>
<td>Data Encoding</td>
<td>Direct Sequence Spread Spectrum (DSSS)</td>
</tr>
<tr>
<td>Operating Range:</td>
<td><strong>Outdoor</strong></td>
</tr>
<tr>
<td></td>
<td>1Mbps - 1650 ft (503 m)</td>
</tr>
<tr>
<td></td>
<td>2Mbps - 1320 ft (402 m)</td>
</tr>
<tr>
<td></td>
<td>5.5Mbps - 1155 ft (352 m)</td>
</tr>
<tr>
<td></td>
<td>11Mbps - 835 ft (255 m)</td>
</tr>
<tr>
<td></td>
<td><strong>Indoor</strong></td>
</tr>
<tr>
<td></td>
<td>1Mbps - 500 ft (152 m)</td>
</tr>
<tr>
<td></td>
<td>2Mbps - 400 ft (122 m)</td>
</tr>
<tr>
<td></td>
<td>5.5Mbps - 270 ft (82 m)</td>
</tr>
<tr>
<td></td>
<td>11Mbps - 175 ft (53 m)</td>
</tr>
<tr>
<td>Maximum Computers Per Network:</td>
<td>Limited by the amount of wireless network traffic generated by each node. Typically 30-70 nodes.</td>
</tr>
</tbody>
</table>

## Software Requirements

- **USB Driver/Configuration Utility**: Microsoft Windows XP, 98/ME, 2000
- **SNMP Configuration Utility**: Microsoft Windows XP, 98/ME, 2000
This chapter provides an overview of IP networks, routing, and wireless networking.

Related Publications

As you read this document, you may be directed to various RFC documents for further information. An RFC is a Request For Comment (RFC) published by the Internet Engineering Task Force (IETF), an open organization that defines the architecture and operation of the Internet. The RFC documents outline and define the standard protocols and procedures for the Internet. The documents are listed on the World Wide Web at www.ietf.org and are mirrored and indexed at many other sites worldwide.

Wireless Networking

The ME102 Wireless Access Point conforms to the Institute of Electrical and Electronics Engineers (IEEE) 802.11b standard for wireless LANs (WLANs). On an 802.11b wireless link, data is encoded using direct-sequence spread-spectrum (DSSS) technology and is transmitted in the unlicensed radio spectrum at 2.5GHz. The maximum data rate for the wireless link is 11 Mbps, but it will automatically back down from 11 Mbps to 5.5, 2, and 1 Mbps when the radio signal is weak or when interference is detected.

The 802.11b standard is also called Wireless Ethernet or Wi-Fi by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standard group promoting interoperability among 802.11b devices.
Wireless Network Configuration

The 802.11b standard offers two methods for configuring a wireless network - ad hoc and infrastructure.

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

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. This mode 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 expensive way to set up a wireless network.

Infrastructure Mode

With a wireless Access Point, you can operate the wireless LAN in the infrastructure mode. This mode 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 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.

Extended Service Set Identification (ESSID)

The Extended Service Set Identification (ESSID) is one of two types of Service Set Identification (SSID). In an ad-hoc wireless network with no access points, the Basic Service Set Identification (BSSID) is used. In an infrastructure wireless network that includes an access point, the Extended Service Set Identification (ESSID) is used, but may still be referred to as SSID.
An SSID is a thirty-two character (maximum) alphanumeric key identifying the wireless local area network. Some vendors refer to the SSID as network name. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID.

The ESSID is usually broadcast in the air from an access point. The wireless station sometimes can be configured with the ESSID ANY. This means the wireless station will try to associate with whichever access point has the stronger radio frequency (RF) signal, providing that both the access point and wireless station use Open System authentication.

**Authentication and WEP Encryption**

The absence of a physical connection between nodes makes the wireless links vulnerable to eavesdropping and information theft. To provide certain level of security, the IEEE 802.11 standard defines two types of authentication methods:

- **Open System** – Open System authentication is a null algorithm which requires an system identifier but does not encrypt the wireless data. With Open System authentication, a wireless PC can join any network merely by providing the SSID and receive any messages that are not encrypted.

- **Shared Key** – 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. With Shared Key authentication, only those PCs that possess the correct authentication key can join the network.

By default, IEEE 802.11 wireless devices operate in open system network mode. That is, they do not encrypt the data being transmitted over the wireless network.

**Wired Equivalent Privacy (WEP)**

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, 64-bit and 128-bit WEP data encryption.

The 64-bit WEP data encryption method, allows for a five-character (40-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 refer to the 64-bit WEP data encryption as 40-bit WEP data encryption since the user-configurable portion of the encryption key is 40 bits wide.
The 128-bit WEP data encryption method consists of 104 user-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.

The radio frequency channels used are listed in Table 5-1:

**Table 5-1. 802.11 Radio Frequency Channels**

<table>
<thead>
<tr>
<th>Channel</th>
<th>Center Frequency</th>
<th>Frequency Spread</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2412Mhz</td>
<td>2399.5Mhz - 2424.5Mhz</td>
</tr>
<tr>
<td>2</td>
<td>2417Mhz</td>
<td>2404.5Mhz - 2429.5Mhz</td>
</tr>
<tr>
<td>3</td>
<td>2422Mhz</td>
<td>2409.5Mhz - 2434.5Mhz</td>
</tr>
<tr>
<td>4</td>
<td>2427Mhz</td>
<td>2414.5Mhz - 2439.5Mhz</td>
</tr>
<tr>
<td>5</td>
<td>2432Mhz</td>
<td>2419.5Mhz - 2444.5Mhz</td>
</tr>
<tr>
<td>6</td>
<td>2437Mhz</td>
<td>2424.5Mhz - 2449.5Mhz</td>
</tr>
<tr>
<td>7</td>
<td>2442Mhz</td>
<td>2429.5Mhz - 2454.5Mhz</td>
</tr>
<tr>
<td>8</td>
<td>2447Mhz</td>
<td>2434.5Mhz - 2459.5Mhz</td>
</tr>
<tr>
<td>9</td>
<td>2452Mhz</td>
<td>2439.5Mhz - 2464.5Mhz</td>
</tr>
<tr>
<td>10</td>
<td>2457Mhz</td>
<td>2444.5Mhz - 2469.5Mhz</td>
</tr>
<tr>
<td>11</td>
<td>2462Mhz</td>
<td>2449.5Mhz - 2474.5Mhz</td>
</tr>
<tr>
<td>12</td>
<td>2467Mhz</td>
<td>2454.5Mhz - 2479.5Mhz</td>
</tr>
<tr>
<td>13</td>
<td>2472Mhz</td>
<td>2459.5Mhz - 2484.5Mhz</td>
</tr>
</tbody>
</table>
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, as these three channels do not overlap.

Ethernet Cabling

Although Ethernet networks originally used thick or thin coaxial cable, most installations currently use unshielded twisted pair (UTP) cabling. The UTP cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector. A normal “straight-through” UTP Ethernet cable follows the EIA568B standard wiring and pinout as described in Table 5-2.

Table 5-2. UTP Ethernet cable wiring, straight-through

<table>
<thead>
<tr>
<th>Pin</th>
<th>Wire color</th>
<th>Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Orange/White</td>
<td>Transmit (Tx) +</td>
</tr>
<tr>
<td>2</td>
<td>Orange</td>
<td>Transmit (Tx) -</td>
</tr>
<tr>
<td>3</td>
<td>Green/White</td>
<td>Receive (Rx) +</td>
</tr>
<tr>
<td>4</td>
<td>Blue</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Blue/White</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Green</td>
<td>Receive (Rx) -</td>
</tr>
<tr>
<td>7</td>
<td>Brown/White</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Brown</td>
<td></td>
</tr>
</tbody>
</table>

Cable Quality

A twisted pair Ethernet network operating at 10 Mbits/second (10BASE-T) will often tolerate low quality cables, but at 100 Mbits/second (10BASE-Tx) the cable must be rated as Category 5, or "Cat 5" or "Cat V", by the Electronic Industry Association (EIA). This rating will be printed on the cable jacket. A Category 5 cable will meet specified requirements regarding loss and crosstalk. In addition, there are restrictions on maximum cable length for both 10 and 100 Mbits/second networks.
Uplink Switches, Crossover Cables, and MDI/MDIX Switching

In the wiring table above, the concept of transmit and receive are from the perspective of the PC, which is wired as Media Dependant Interface (MDI). In this wiring, the PC transmits on pins 1 and 2. At the hub, the perspective is reversed, and the hub receives on pins 1 and 2. This wiring is referred to as Media Dependant Interface - Crossover (MDI-X). When connecting a PC to a PC, or a hub port to another hub port, the transmit pair must be exchanged with the receive pair. This exchange is done by one of two mechanisms:

- Uplink switch
  Most hubs provide an Uplink switch which will exchange the pairs on one port, allowing that port to be connected to another hub using a normal Ethernet cable.

- Crossover cable
  A crossover cable is a special cable in which the transmit and receive pairs are exchanged at one of the two cable connectors. Crossover cables are often unmarked as such, and must be identified by comparing the two connectors. Since the cable connectors are clear plastic, it is easy to place them side by side and view the order of the wire colors on each. On a straight-through cable, the color order will be the same on both connectors. On a crossover cable, the orange and blue pairs will be exchanged from one connector to the other.
Basic Router Concepts

Large amounts of bandwidth can be provided easily and relatively inexpensively in a local area network (LAN). However, providing high bandwidth between a local network and the Internet can be very expensive. Because of this expense, Internet access is usually provided by a slower-speed wide-area network (WAN) link such as a cable or DSL modem. In order to make the best use of the slower WAN link, a mechanism must be in place for selecting and transmitting only the data traffic meant for the Internet. The function of selecting and forwarding this data is performed by a router.

What is a Router?

A router is a device that forwards traffic between networks based on network layer information in the data and on routing tables maintained by the router. In these routing tables, a router builds up a logical picture of the overall network by gathering and exchanging information with other routers in the network. Using this information, the router chooses the best path for forwarding network traffic.

Routers vary in performance and scale, number of routing protocols supported, and types of physical WAN connection they support. The ME102 802.11b Wireless Access Point is a small office router that routes the IP protocol over a single-user broadband connection.

Routing Information Protocol

One of the protocols used by a router to build and maintain a picture of the network is the Routing Information Protocol (RIP). Using RIP, routers periodically update one another and check for changes to add to the routing table.

The ME102 Wireless Access Point supports both the older RIP-1 and the newer RIP-2 protocols. Among other improvements, RIP-2 supports subnet and multicast protocols. RIP is not required for most home applications.

IP Addresses and the Internet

Because TCP/IP networks are interconnected across the world, every machine on the Internet must have a unique address to make sure that transmitted data reaches the correct destination. Blocks of addresses are assigned to organizations by the Internet Assigned Numbers Authority (IANA). Individual users and small organizations may obtain their addresses either from the IANA or from an Internet service provider (ISP). You can contact IANA at www.iana.org.
The Internet Protocol (IP) uses a 32-bit address structure. The address is usually written in dot notation (also called dotted-decimal notation), in which each group of eight bits is written in decimal form, separated by decimal points.

For example, the following binary address:

```
11000011  00100010  00001100  00000111
```

is normally written as:

```
195.34.12.7
```

The latter version is easier to remember and easier to enter into your computer.

In addition, the 32 bits of the address are subdivided into two parts. The first part of the address identifies the network, and the second part identifies the host node or station on the network. The dividing point may vary depending on the address range and the application.

There are five standard classes of IP addresses. These address classes have different ways of determining the network and host sections of the address, allowing for different numbers of hosts on a network. Each address type begins with a unique bit pattern, which is used by the TCP/IP software to identify the address class. After the address class has been determined, the software can correctly identify the host section of the address. The follow figure shows the three main address classes, including network and host sections of the address for each address type.

![Diagram of three main address classes](image)

**Figure 5-1: Three Main Address Classes**
The five address classes are:

- **Class A**
  Class A addresses can have up to 16,777,214 hosts on a single network. They use an eight-bit network number and a 24-bit node number. Class A addresses are in this range:
  
  1.x.x.x to 126.x.x.x.

- **Class B**
  Class B addresses can have up to 65,534 hosts on a network. A Class B address uses a 16-bit network number and a 16-bit node number. Class B addresses are in this range:
  
  128.1.x.x to 191.254.x.x.

- **Class C**
  Class C addresses can have 254 hosts on a network. Class C addresses use 24 bits for the network address and eight bits for the node. They are in this range:
  
  192.0.1.x to 223.255.254.x.

- **Class D**
  Class D addresses are used for multicasts (messages sent to many hosts). Class D addresses are in this range:
  
  224.0.0.0 to 239.255.255.255.

- **Class E**
  Class E addresses are for experimental use.

This addressing structure allows IP addresses to uniquely identify each physical network and each node on each physical network.

For each unique value of the network portion of the address, the base address of the range (host address of all zeros) is known as the network address and is not usually assigned to a host. Also, the top address of the range (host address of all ones) is not assigned, but is used as the broadcast address for simultaneously sending a packet to all hosts with the same network address.

**Netmask**

In each of the address classes previously described, the size of the two parts (network address and host address) is implied by the class. This partitioning scheme can also be expressed by a netmask associated with the IP address. A netmask is a 32-bit quantity that, when logically combined (using an AND operator) with an IP address, yields the network address. For instance, the netmasks for Class A, B, and C addresses are 255.0.0.0, 255.255.0.0, and 255.255.255.0, respectively.
For example, the address 192.168.170.237 is a Class C IP address whose network portion is the upper 24 bits. When combined (using an AND operator) with the Class C netmask, as shown here, only the network portion of the address remains:

\[
\begin{array}{cccc}
11000000 & 10101000 & 10101010 & 11101101 \quad (192.168.170.237) \\
\end{array}
\]

combined with:

\[
\begin{array}{cccc}
11111111 & 11111111 & 11111111 & 00000000 \quad (255.255.255.0) \\
\end{array}
\]

Equals:

\[
\begin{array}{cccc}
11000000 & 10101000 & 10101010 & 00000000 \quad (192.168.170.0) \\
\end{array}
\]

As a shorter alternative to dotted-decimal notation, the netmask may also be expressed in terms of the number of ones from the left. This number is appended to the IP address, following a backward slash (\(/\) ), as “/n.” In the example, the address could be written as 192.168.170.237/24, indicating that the netmask is 24 ones followed by 8 zeros.

**Subnet Addressing**

By looking at the addressing structures, you can see that even with a Class C address, there are a large number of hosts per network. Such a structure is an inefficient use of addresses if each end of a routed link requires a different network number. It is unlikely that the smaller office LANs would have that many devices. You can resolve this problem by using a technique known as subnet addressing.

Subnet addressing allows us to split one IP network address into smaller multiple physical networks known as subnetworks. Some of the node numbers are used as a subnet number instead. A Class B address gives us 16 bits of node numbers translating to 64,000 nodes. Most organizations do not use 64,000 nodes, so there are free bits that can be reassigned. Subnet addressing makes use of those bits that are free, as shown below.

![Figure 5-2: Example of Subnetting a Class B Address](image)
A Class B address can be effectively translated into multiple Class C addresses. For example, the IP address of 172.16.0.0 is assigned, but node addresses are limited to 255 maximum, allowing eight extra bits to use as a subnet address. The IP address of 172.16.97.235 would be interpreted as IP network address 172.16, subnet number 97, and node number 235. In addition to extending the number of addresses available, subnet addressing provides other benefits. Subnet addressing allows a network manager to construct an address scheme for the network by using different subnets for other geographical locations in the network or for other departments in the organization.

Although the preceding example uses the entire third octet for a subnet address, note that you are not restricted to octet boundaries in subnetting. To create more network numbers, you need only shift some bits from the host address to the network address. For instance, to partition a Class C network number (192.68.135.0) into two, you shift one bit from the host address to the network address. The new netmask (or subnet mask) is 255.255.255.128. The first subnet has network number 192.68.135.0 with hosts 192.68.135.1 to 129.68.135.126, and the second subnet has network number 192.68.135.128 with hosts 192.68.135.129 to 192.68.135.254.

The following table lists the additional subnet mask bits in dotted-decimal notation. To use the table, write down the original class netmask and replace the 0 value octets with the dotted-decimal value of the additional subnet bits. For example, to partition your Class C network with subnet mask 255.255.255.0 into 16 subnets (4 bits), the new subnet mask becomes 255.255.255.240.

<table>
<thead>
<tr>
<th>Number of Bits</th>
<th>Dotted-Decimal Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>128</td>
</tr>
<tr>
<td>2</td>
<td>192</td>
</tr>
<tr>
<td>3</td>
<td>224</td>
</tr>
<tr>
<td>4</td>
<td>240</td>
</tr>
<tr>
<td>5</td>
<td>248</td>
</tr>
<tr>
<td>6</td>
<td>252</td>
</tr>
<tr>
<td>7</td>
<td>254</td>
</tr>
<tr>
<td>8</td>
<td>255</td>
</tr>
</tbody>
</table>

Note: The number 192.68.135.127 is not assigned because it is the broadcast address of the first subnet. The number 192.68.135.128 is not assigned because it is the network address of the second subnet.
The following table displays several common netmask values in both the dotted-decimal and the masklength formats.

Table 5-2. Netmask Formats

<table>
<thead>
<tr>
<th>Dotted-Decimal</th>
<th>Masklength</th>
</tr>
</thead>
<tbody>
<tr>
<td>255.0.0.0</td>
<td>/8</td>
</tr>
<tr>
<td>255.255.0.0</td>
<td>/16</td>
</tr>
<tr>
<td>255.255.255.0</td>
<td>/24</td>
</tr>
<tr>
<td>255.255.255.128</td>
<td>/25</td>
</tr>
<tr>
<td>255.255.255.192</td>
<td>/26</td>
</tr>
<tr>
<td>255.255.255.224</td>
<td>/27</td>
</tr>
<tr>
<td>255.255.255.240</td>
<td>/28</td>
</tr>
<tr>
<td>255.255.255.248</td>
<td>/29</td>
</tr>
<tr>
<td>255.255.255.252</td>
<td>/30</td>
</tr>
<tr>
<td>255.255.255.254</td>
<td>/31</td>
</tr>
<tr>
<td>255.255.255.255</td>
<td>/32</td>
</tr>
</tbody>
</table>

NETGEAR strongly recommends that you configure all hosts on a LAN segment to use the same netmask for the following reasons:

- So that hosts recognize local IP broadcast packets
  
  When a device broadcasts to its segment neighbors, it uses a destination address of the local network address with all ones for the host address. In order for this scheme to work, all devices on the segment must agree on which bits comprise the host address.

- So that a local router or bridge recognizes which addresses are local and which are remote

Private IP Addresses

If your local network is isolated from the Internet by a router, you can assign any IP addresses to the local host computers without problems. However, the IANA has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255
NETGEAR recommends that you choose your private network number from this range. The DHCP server of the ME102 Wireless Access Point is preconfigured to automatically use a private address.


**Single IP Address Operation Using NAT**

In the past, if multiple PCs on a LAN needed to access the Internet simultaneously, you had to obtain a range of IP addresses from the ISP. This type of Internet account is more costly than a single-address account typically used by a single user with a modem, rather than a router. The ME102 Wireless Access Point employs an address-sharing method called Network Address Translation (NAT). This method allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your ISP.

The router accomplishes this address sharing by translating the internal LAN IP addresses to a single address that is globally unique on the Internet. The internal LAN IP addresses can be either private addresses or registered addresses. For more information about IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

The following figure illustrates a single IP address operation.
This scheme offers the additional benefit of firewall-like protection because the internal LAN addresses are not available to the Internet through the translated connection. All incoming inquiries are filtered out by the router. This filtering can prevent intruders from probing your system. However, using port forwarding, you can allow one PC (for example, a Web server) on your local network to be accessible to outside users.

**MAC Addresses and Address Resolution Protocol**

An IP address alone cannot be used to deliver data from one LAN device to another. To send data between LAN devices, you must convert the IP address of the destination device to its media access control (MAC) address. Each device on an Ethernet network has a unique MAC address, which is a 48-bit number assigned to each device by the manufacturer. The technique that associates the IP address with a MAC address is known as address resolution. Internet Protocol uses the Address Resolution Protocol (ARP) to resolve MAC addresses.
If a device sends data to another station on the network and the destination MAC address is not yet recorded, ARP is used. An ARP request is broadcast onto the network. All stations on the network receive and read the request. The destination IP address for the chosen station is included as part of the message so that only the station with this IP address responds to the ARP request. All other stations discard the request.

**Related Documents**

The station with the correct IP address responds with its own MAC address directly to the sending device. The receiving station provides the transmitting station with the required destination MAC address. The IP address data and MAC address data for each station are held in an ARP table. The next time data is sent, the address can be obtained from the address information in the table.

For more information about address assignment, refer to the IETF documents RFC 1597, *Address Allocation for Private Internets*, and RFC 1466, *Guidelines for Management of IP Address Space*.

For more information about IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

**Domain Name Server**

Many of the resources on the Internet can be addressed by simple descriptive names such as [www.NETGEAR.com](http://www.NETGEAR.com). This addressing is very helpful at the application level, but the descriptive name must be translated to an IP address in order for a user to actually contact the resource. Just as a telephone directory maps names to phone numbers, or as an ARP table maps IP addresses to MAC addresses, a domain name system (DNS) server maps descriptive names of network resources to IP addresses.

When a PC accesses a resource by its descriptive name, it first contacts a DNS server to obtain the IP address of the resource. The PC sends the desired message using the IP address. Many large organizations, such as ISPs, maintain their own DNS servers and allow their customers to use the servers to look up addresses.
IP Configuration by DHCP

When an IP-based local area network is installed, each PC must be configured with an IP address. If the PCs need to access the Internet, they should also be configured with a gateway address and one or more DNS server addresses. As an alternative to manual configuration, there is a method by which each PC on the network can automatically obtain this configuration information. A device on the network may act as a Dynamic Host Configuration Protocol (DHCP) server. The DHCP server stores a list or pool of IP addresses, along with other information (such as gateway and DNS addresses) that it may assign to the other devices on the network. The ME102 Wireless Access Point has the capacity to act as a DHCP server.

The ME102 Wireless Access Point also functions as a DHCP client when connecting to the ISP. The wireless access point can automatically obtain an IP address, subnet mask, DNS server addresses, and a gateway address if the ISP provides this information by DHCP.

Internet Security

When your LAN connects to the Internet through a router, an opportunity is created for outsiders to access or disrupt your network. A NAT router provides some protection because by the very nature of the Network Address Translation (NAT) process, the network behind the NAT router is shielded from access by outsiders on the Internet. However, there are methods by which a determined hacker can possibly obtain information about your network or at the least can disrupt your Internet access.
This appendix describes how to prepare your network to connect to the Internet through the ME102 802.11b Wireless Access Point and how to verify the readiness of broadband Internet service from an Internet service provider (ISP).

**Note:** If an ISP technician configured your computer during the installation of a broadband modem, or if you configured it using instructions provided by your ISP, you may need to copy the current configuration information for use in the configuration of your wireless access point. Write down this information before reconfiguring your computers.

### Preparing Your Computers for TCP/IP Networking

Computers access the Internet using a protocol called TCP/IP (Transmission Control Protocol/Internet Protocol). Each computer on your network must have TCP/IP installed and selected as its networking protocol. If a Network Interface Card (NIC) is already installed in your PC, then TCP/IP is probably already installed as well.

Most operating systems include the software components you need for networking with TCP/IP:

- Windows® 95 or later includes the software components for establishing a TCP/IP network.
- Windows 3.1 does not include a TCP/IP component. You need to purchase a third-party TCP/IP application package such as NetManage Chameleon.
- Macintosh Operating System 7 or later includes the software components for establishing a TCP/IP network.
- All versions of UNIX or Linux include TCP/IP components. Follow the instructions provided with your operating system or networking software to install TCP/IP on your computer.
In your IP network, each PC and the wireless access point must be assigned a unique IP addresses. Each PC must also have certain other IP configuration information such as a subnet mask (netmask), a domain name server (DNS) address, and a default gateway address. In most cases, you should install TCP/IP so that the PC obtains its specific network configuration information automatically from a DHCP server during bootup.

The ME102 Wireless Access Point is shipped preconfigured as a DHCP server. The wireless access point assigns the following TCP/IP configuration information automatically when the PCs are rebooted:

- PC or workstation IP addresses—192.168.0.2 through 192.168.0.254
- Subnet mask—255.255.255.0
- Gateway address (the wireless access point)—192.168.0.1

These addresses are part of the IETF-designated private address range for use in private networks.

**Configuring Windows 95, 98, and ME for TCP/IP Networking**

As part of the PC preparation process, you need to manually install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

**Install or Verify Windows Networking Components**

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network icon.
   - The Network window opens, which displays a list of installed components:
You must have an Ethernet adapter, the TCP/IP protocol, and Client for Microsoft Networks.

**Note:** It is not necessary to remove any other network components shown in the Network window in order to install the adapter, TCP/IP, or Client for Microsoft Networks.

If you need to install a new adapter, follow these steps:

a. Click the Add button.

b. Select Adapter, and then click Add.

c. Select the manufacturer and model of your Ethernet adapter, and then click OK.

If you need TCP/IP:

a. Click the Add button.

b. Select Protocol, and then click Add.

c. Select Microsoft.

d. Select TCP/IP, and then click OK.
If you need Client for Microsoft Networks:

a. Click the Add button.
b. Select Client, and then click Add.
c. Select Microsoft.
d. Select Client for Microsoft Networks, and then click OK.

3. Restart your PC for the changes to take effect.

Enabling DHCP to Automatically Configure TCP/IP Settings

After the TCP/IP protocol components are installed, each PC must be assigned specific information about itself and resources that are available on its network. The simplest way to configure this information is to allow the PC to obtain the information from the internal DHCP server of the ME102 Wireless Access Point. To use DHCP with the recommended default addresses, follow these steps:

1. Connect all PCs to the wireless access point, then restart the wireless access point and allow it to boot.
2. On each attached PC, open the Network control panel (refer to the previous section) and select the Configuration tab.
3. From the components list, select TCP/IP->(your Ethernet adapter) and click Properties.
4. In the IP Address tab, select “Obtain an IP address automatically”.
5. Select the Gateway tab.
6. If any gateways are shown, remove them.
7. Click OK.
8. Restart the PC.

Repeat steps 2 through 8 for each PC on your network.

Selecting Windows' Internet Access Method

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Internet Options icon.
3. Select “I want to set up my Internet connection manually” or “I want to connect through a Local Area Network” and click Next.
4. Select “I want to connect through a Local Area Network” and click Next.
5. Uncheck all boxes in the LAN Internet Configuration screen and click Next.
6. Proceed to the end of the Wizard.

Verifying TCP/IP Properties

After your PC is configured and has rebooted, you can check the TCP/IP configuration using the utility `winipcfg.exe`:

1. On the Windows taskbar, click the Start button, and then click Run.
2. Type `winipcfg`, and then click OK.
   The IP Configuration window opens, which lists (among other things), your IP address, subnet mask, and default gateway.
3. From the drop-down box, select your Ethernet adapter.
   The window is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends:
   - The IP address is between 192.168.0.2 and 192.168.0.254
   - The subnet mask is 255.255.255.0
   - The default gateway is 192.168.0.1

Configuring Windows NT, 2000 or XP for IP Networking

As part of the PC preparation process, you need to manually install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

Install or Verify Windows Networking Components

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network and Dialup Connections icon.
3. If an Ethernet adapter is present in your PC, you should see an entry for Local Area Connection. Double-click that entry.
4. Select Properties.
5. Verify that ‘Client for Microsoft Networks’ and ‘Internet Protocol (TCP/IP)’ are present. If not, select Install and add them.

6. Select ‘Internet Protocol (TCP/IP)’, click Properties, and verify that “Obtain an IP address automatically is selected.

7. Click OK and close all Network and Dialup Connections windows.

8. Make sure your PC is connected to the wireless access point, then reboot your PC.

Verifying TCP/IP Properties

To check your PC’s TCP/IP configuration:

1. On the Windows taskbar, click the Start button, and then click Run.
   The Run window opens.

2. Type cmd and then click OK.
   A command window opens

3. Type ipconfig /all
   Your IP Configuration information will be listed, and should match the values below if you are using the default TCP/IP settings that NETGEAR recommends:
   • The IP address is between 192.168.0.2 and 192.168.0.254
   • The subnet mask is 255.255.255.0
   • The default gateway is 192.168.0.1

4. Type exit

Configuring the Macintosh for TCP/IP Networking

Beginning with Macintosh Operating System 7, TCP/IP is already installed on the Macintosh. On each networked Macintosh, you will need to configure TCP/IP to use DHCP.

MacOS 8.6 or 9.x

1. From the Apple menu, select Control Panels, then TCP/IP.
The TCP/IP Control Panel opens:

2. From the “Connect via” box, select your Macintosh’s Ethernet interface.
3. From the “Configure” box, select Using DHCP Server. You can leave the DHCP Client ID box empty.
4. Close the TCP/IP Control Panel.
5. Repeat this for each Macintosh on your network.

**MacOS X**

1. From the Apple menu, choose System Preferences, then Network.
2. If not already selected, select Built-in Ethernet in the Configure list.
3. If not already selected, Select Using DHCP in the TCP/IP tab.
4. Click Save.
Verifying TCP/IP Properties for Macintosh Computers

After your Macintosh is configured and has rebooted, you can check the TCP/IP configuration by returning to the TCP/IP Control Panel. From the Apple menu, select Control Panels, then TCP/IP.

![TCP/IP Control Panel](image)

The panel is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends:

- The IP Address is between 192.168.0.2 and 192.168.0.254
- The Subnet mask is 255.255.255.0
- The Router address is 192.168.0.1

If you do not see these values, you may need to restart your Macintosh or you may need to switch the “Configure” setting to a different option, then back again to “Using DHCP Server”.

---

*Reference Manual for the Model ME102 802.11b Wireless Access Point*

**C-8 Preparing Your Network**
**Verifying the Readiness of Your Internet Account**

For broadband access to the Internet, you need to contract with an Internet service provider (ISP) for a single-user Internet access account using a cable modem or DSL modem. This modem must be a separate physical box (not a card) and must provide an Ethernet port intended for connection to a Network Interface Card (NIC) in a computer. Your wireless access point does not support a USB-connected broadband modem.

For a single-user Internet account, your ISP supplies TCP/IP configuration information for one computer. With a typical account, much of the configuration information is dynamically assigned when your PC is first booted up while connected to the ISP, and you will not need to know that dynamic information.

In order to share the Internet connection among several computers, your wireless access point takes the place of the single PC, and you need to configure it with the TCP/IP information that the single PC would normally use. When the wireless access point’s Internet port is connected to the broadband modem, the wireless access point appears to be a single PC to the ISP. The wireless access point then allows the PCs on the local network to masquerade as the single PC to access the Internet through the broadband modem. The method used by the wireless access point to accomplish this is called Network Address Translation (NAT) or IP masquerading.

**Are Login Protocols Used?**

Some ISPs require a special login protocol, in which you must enter a login name and password in order to access the Internet. If you normally log in to your Internet account by running a program such as WinPOET or EnterNet, then your account uses PPP over Ethernet (PPPoE).

When you configure your router, you will need to enter your login name and password in the router’s configuration menus. After your network and wireless access point are configured, the wireless access point will perform the login task when needed, and you will no longer need to run the login program from your PC. It is not necessary to uninstall the login program.

**What Is Your Configuration Information?**

More and more, ISPs are dynamically assigning configuration information. However, if your ISP does not dynamically assign configuration information but instead used fixed configurations, your ISP should have given you the following basic information for your account:
An IP address and subnet mask
A gateway IP address, which is the address of the ISP’s router
One or more domain name server (DNS) IP addresses
Host name and domain suffix

For example, your account’s full server names may look like this:

mail.xxx.yyy.com

In this example, the domain suffix is xxx.yyy.com.

If any of these items are dynamically supplied by the ISP, your wireless access point automatically acquires them.

If an ISP technician configured your PC during the installation of the broadband modem, or if you configured it using instructions provided by your ISP, you need to copy the configuration information from your PC’s Network TCP/IP Properties window or Macintosh TCP/IP Control Panel before reconfiguring your PC for use with the wireless access point. These procedures are described next.

**Obtaining ISP Configuration Information for Windows Computers**

As mentioned above, you may need to collect configuration information from your PC so that you can use this information when you configure the ME102 Wireless Access Point. Following this procedure is only necessary when your ISP does not dynamically supply the account information.

To get the information you need to configure the wireless access point for Internet access:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network icon.
   
   The Network window opens, which displays a list of installed components.
3. Select TCP/IP, and then click Properties.
   
   The TCP/IP Properties dialog box opens.
4. Select the IP Address tab.
   
   If an IP address and subnet mask are shown, write down the information. If an address is present, your account uses a fixed (static) IP address. If no address is present, your account uses a dynamically-assigned IP address. Click “Obtain an IP address automatically”.
5. Select the Gateway tab.
If an IP address appears under Installed Gateways, write down the address. This is the ISP’s gateway address. Select the address and then click Remove to remove the gateway address.

6. Select the DNS Configuration tab.
   If any DNS server addresses are shown, write down the addresses. If any information appears in the Host or Domain information box, write it down. Click Disable DNS.

7. Click OK to save your changes and close the TCP/IP Properties dialog box.
   You are returned to the Network window.

8. Click OK.

9. Reboot your PC at the prompt. You may also be prompted to insert your Windows CD.

**Obtaining ISP Configuration Information for Macintosh Computers**

As mentioned above, you may need to collect configuration information from your Macintosh so that you can use this information when you configure the ME102 Wireless Access Point. Following this procedure is only necessary when your ISP does not dynamically supply the account information.

To get the information you need to configure the wireless access point for Internet access:

1. From the Apple menu, select Control Panels, then TCP/IP.
   The TCP/IP Control Panel opens, which displays a list of configuration settings. If the “Configure” setting is “Using DHCP Server”, your account uses a dynamically-assigned IP address. In this case, close the Control Panel and skip the rest of this section.

2. If an IP address and subnet mask are shown, write down the information.

3. If an IP address appears under Router address, write down the address. This is the ISP’s gateway address.

4. If any Name Server addresses are shown, write down the addresses. These are your ISP’s DNS addresses.

5. If any information appears in the Search domains information box, write it down.

6. Change the “Configure” setting to “Using DHCP Server”.

7. Close the TCP/IP Control Panel.
Restarting the Network

Once you’ve set up your computers to work with the wireless access point, you must reset the network for the devices to be able to communicate correctly. Restart any computer that is connected to the firewall.

After configuring all of your computers for TCP/IP networking and restarting them, and connecting them to the local network of your ME102 Wireless Access Point, you are ready to access and configure the wireless access point.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>10BASE-T</strong></td>
<td>IEEE 802.3 specification for 10 Mbps Ethernet over twisted pair wiring.</td>
</tr>
<tr>
<td><strong>100BASE-Tx</strong></td>
<td>IEEE 802.3 specification for 100 Mbps Ethernet over twisted pair wiring.</td>
</tr>
<tr>
<td><strong>802.11b</strong></td>
<td>IEEE specification for wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.5GHz.</td>
</tr>
<tr>
<td><strong>ADSL</strong></td>
<td>See Asymmetric Digital Subscriber Line</td>
</tr>
<tr>
<td><strong>Asymmetric Digital Subscriber Line</strong></td>
<td>A technology for sending data over regular telephone lines. ADSL allows data rates up to 8 Mbps downstream and 640 Kbps upstream.</td>
</tr>
<tr>
<td><strong>Denial of Service attack</strong></td>
<td>DoS. A hacker attack designed to prevent your computer or network from operating or communicating.</td>
</tr>
<tr>
<td><strong>DHCP</strong></td>
<td>See Dynamic Host Configuration Protocol.</td>
</tr>
<tr>
<td><strong>DNS</strong></td>
<td>See Domain Name Server.</td>
</tr>
<tr>
<td><strong>Domain Name</strong></td>
<td>A descriptive name for an address or group of addresses on the Internet.</td>
</tr>
<tr>
<td></td>
<td>Domain names are of the form of a registered entity name plus one of a number of predefined top level suffixes such as .com, .edu, .uk, etc. For example, in the address mail.NETGEAR.com, mail is a server name and NETGEAR.com is the domain.</td>
</tr>
<tr>
<td><strong>Domain Name Server</strong></td>
<td>A Domain Name Server (DNS) resolves descriptive names of network resources (such as <a href="http://www.NETGEAR.com">www.NETGEAR.com</a>) to numeric IP addresses.</td>
</tr>
<tr>
<td><strong>DSLAM</strong></td>
<td>DSL Access Multiplexor. The piece of equipment at the telephone company central office that provides the ADSL signal.</td>
</tr>
</tbody>
</table>
### Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic Host Configuration Protocol</td>
<td>DHCP. An Ethernet protocol specifying how a centralized DHCP server can assign network configuration information to multiple DHCP clients. The assigned information includes IP addresses, DNS addresses, and gateway (router) addresses.</td>
</tr>
<tr>
<td>ESSID</td>
<td>The Extended Service Set Identification (ESS ID) is a thirty-two character (maximum) alphanumeric key identifying the wireless local area network.</td>
</tr>
<tr>
<td>Gateway</td>
<td>A local device, usually a router, that connects hosts on a local network to other networks.</td>
</tr>
<tr>
<td>IP</td>
<td>See Internet Protocol.</td>
</tr>
<tr>
<td>IP Address</td>
<td>A four-byte number uniquely defining each host on the Internet. Ranges of addresses are assigned by Internic, an organization formed for this purpose. Usually written in dotted-decimal notation with periods separating the bytes (for example, 134.177.244.57).</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security. IPSec is a series of guidelines for securing private information transmitted over public networks. IPSec is a VPN method providing a higher level of security than PPTP.</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet service provider.</td>
</tr>
<tr>
<td>Internet Protocol</td>
<td>The main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.</td>
</tr>
<tr>
<td>LAN</td>
<td>See local area network.</td>
</tr>
<tr>
<td>local area network</td>
<td>LAN. A communications network serving users within a limited area, such as one floor of a building. A LAN typically connects multiple personal computers and shared network devices such as storage and printers. Although many technologies exist to implement a LAN, Ethernet is the most common for connecting personal computers.</td>
</tr>
<tr>
<td>MAC address</td>
<td>Media Access Control address. A unique 48-bit hardware address assigned to every Ethernet node. Usually written in the form 01:23:45:67:89:ab.</td>
</tr>
<tr>
<td>Mbps</td>
<td>Megabits per second.</td>
</tr>
<tr>
<td>MSB</td>
<td>See Most Significant Bit or Most Significant Byte.</td>
</tr>
<tr>
<td>MTU</td>
<td>See Maximum Transmission Unit.</td>
</tr>
<tr>
<td>Maximum Transmit Unit</td>
<td>The size in bytes of the largest packet that can be sent or received.</td>
</tr>
<tr>
<td><strong>Most Significant Bit or Most Significant Byte</strong></td>
<td>The portion of a number, address, or field that is farthest left when written as a single number in conventional hexadecimal ordinary notation. The part of the number having the most value.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>NAT</strong></td>
<td>See Network Address Translation.</td>
</tr>
<tr>
<td><strong>Netmask</strong></td>
<td>A number that explains which part of an IP address comprises the network address and which part is the host address on that network. It can be expressed in dotted-decimal notation or as a number appended to the IP address. For example, a 28-bit mask starting from the MSB can be shown as 255.255.255.192 or as /28 appended to the IP address.</td>
</tr>
<tr>
<td><strong>Network Address Translation</strong></td>
<td>A technique by which several hosts share a single IP address for access to the Internet.</td>
</tr>
<tr>
<td><strong>packet</strong></td>
<td>A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.</td>
</tr>
<tr>
<td><strong>PPP</strong></td>
<td>See Point-to-Point Protocol.</td>
</tr>
<tr>
<td><strong>PPPoA</strong></td>
<td>See PPP over ATM</td>
</tr>
<tr>
<td><strong>PPPoE</strong></td>
<td>See PPP over Ethernet</td>
</tr>
<tr>
<td><strong>PPP over ATM</strong></td>
<td>PPPoA. PPP over ATM is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.</td>
</tr>
<tr>
<td><strong>PPP over Ethernet</strong></td>
<td>PPPoE. PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.</td>
</tr>
<tr>
<td><strong>PPTP</strong></td>
<td>Point-To-Point Tunneling Protocol. A method for establishing a virtual private network (VPN) by embedding Microsoft’s network protocol into Internet packets.</td>
</tr>
<tr>
<td><strong>PSTN</strong></td>
<td>Public Switched Telephone Network.</td>
</tr>
<tr>
<td><strong>Point-to-Point Protocol</strong></td>
<td>PPP. A protocol allowing a computer using TCP/IP to connect directly to the Internet.</td>
</tr>
<tr>
<td><strong>RFC</strong></td>
<td>Request For Comment. Refers to documents published by the Internet Engineering Task Force (IETF) proposing standard protocols and procedures for the Internet. RFCs can be found at <a href="http://www.ietf.org">www.ietf.org</a>.</td>
</tr>
<tr>
<td><strong>RIP</strong></td>
<td>See Routing Information Protocol.</td>
</tr>
<tr>
<td><strong>router</strong></td>
<td>A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.</td>
</tr>
<tr>
<td><strong>Routing Information</strong></td>
<td>A protocol in which routers periodically exchange information with one another so that they can determine minimum distance paths between sources and destinations.</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td></td>
</tr>
<tr>
<td><strong>SSID</strong></td>
<td>Service Set Identification. A thirty-two character (maximum) alphanumeric key identifying the wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID.</td>
</tr>
<tr>
<td><strong>subnet mask</strong></td>
<td><em>See</em> netmask.</td>
</tr>
<tr>
<td><strong>UTP</strong></td>
<td>Unshielded twisted pair. The cable used by 10BASE-T and 100BASE-Tx Ethernet networks.</td>
</tr>
<tr>
<td><strong>VCI</strong></td>
<td>Virtual Channel Identifier. Together with the VPI, defines a Virtual Channel through an ATM network. Used by ATM switching equipment to route data through the network.</td>
</tr>
<tr>
<td><strong>VPI</strong></td>
<td>Virtual Path Identifier. Together with the VCI, defines a Virtual Channel through an ATM network. Used by ATM switching equipment to route data through the network.</td>
</tr>
<tr>
<td><strong>VPN</strong></td>
<td>Virtual Private Network. A method for securely transporting data between two private networks by using a public network such as the Internet as a connection.</td>
</tr>
<tr>
<td><strong>WAN</strong></td>
<td><em>See</em> wide area network.</td>
</tr>
<tr>
<td><strong>WEP</strong></td>
<td>Wired Equivalent Privacy. WEP is a data encryption protocol for 802.11b wireless networks. All wireless nodes and access points on the network are configured with a 64-bit or 128-bit Shared Key for data encryption.</td>
</tr>
<tr>
<td><strong>wide area network</strong></td>
<td>WAN. A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.</td>
</tr>
<tr>
<td><strong>Wi-Fi</strong></td>
<td><em>See</em> 802.11b. A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see <a href="http://www.wi-fi.net">http://www.wi-fi.net</a>), an industry standard group promoting interoperability among 802.11b devices.</td>
</tr>
<tr>
<td><strong>Windows Internet Naming Service</strong></td>
<td>WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses. If a remote network contains a WINS server, your Windows PCs can gather information from that WINS server about its local hosts. This allows your PCs to browse that remote network using Network Neighborhood.</td>
</tr>
<tr>
<td><strong>WINS</strong></td>
<td><em>See</em> Windows Internet Naming Service.</td>
</tr>
</tbody>
</table>
Index
N
NAT  C-9
NETGEAR
  contacting  1-xi
netmask
  translation table  B-11, B-12
Network Address Translation  B-13, C-9

O
Open System authentication  B-3

P
PC, using to configure  C-12
pinout, Ethernet cable  B-5
Placement  2-2
port forwarding behind NAT  B-14
PPP over Ethernet  C-9
PPPoE  C-9
protocols
  Address Resolution  B-14
  DHCP  B-16
  Routing Information  B-7
publications, related  B-1

R
Range  2-2
range  2-2
rear panel  1-6
requirements
  hardware  2-2
RFC
  1466  B-13, B-15
  1597  B-13, B-15
  1631  B-13, B-15
  finding  B-13
router concepts  B-7
Routing Information Protocol  B-7

S
Shared Key authentication  B-3
SSID  2-3, B-2
subnet addressing  B-10
subnet mask  B-11, C-10, C-11

T
TCP/IP
  configuring  C-1
TCP/IP properties
  verifying for Macintosh  C-8
  verifying for Windows  C-5, C-6
technical support  1-xi
troubleshooting  5-1
typographical conventions  1-xii

U
uplink switch  B-6
USB  C-9

W
WEP  3-1, B-3
Wi-Fi  B-1
Windows, configuring for IP routing  C-2, C-5
winipcfg utility  C-5
WinPOET  C-9
Wired Equivalent Privacy. See WEP
Wireless Ethernet  B-1