

# WaveMANAGER

## User's Guide



---

### **About this Book:**

The product described in this book is a licensed product of Lucent Technologies Inc.

- WaveLAN and WavePOINT are trademarks of Lucent Technologies.
- Microsoft, Windows 95, Windows NT, Windows for Workgroups and MS-DOS are registered trademarks of Microsoft Corporation.
- Adobe Acrobat is a registered trademark of Adobe Systems Inc.

All other brand and product names are trademarks or registered trademarks of their respective holders.

### **September, 1998**

It is the policy of Lucent Technologies to improve products as new technology, components, software, and firmware become available. Lucent Technologies, therefore, reserves the right to change specifications without prior notice.

All features, functions, and operations described herein may not be marketed by Lucent Technologies in all parts of the world. In some instances, drawings are of equipment prototypes. Therefore, before using this document, consult your Lucent Technologies representative or Lucent Technologies office for information that is applicable and current.

Copyright ©1998 Lucent Technologies  
All Rights Reserved

---

# Contents

---

<b>Contents</b>	i
WaveLAN Technical Support	vii
Regulatory Information	viii
Exposure to Radio Frequency Radiation	viii
<hr/>	
<b>1 Introduction</b>	1-1
About WaveLAN	1-1
About WaveMANAGER	1-2
WaveMANAGER/CLIENT	1-2
WaveMANAGER/AP	1-2
About This User's Guide	1-3
About Icons Used In This Document	1-4
On-line Help Documentation	1-5
Additional Files on Your Diskettes	1-5
Other Sources of Information	1-5
Sample Network Scenarios	1-6
Basic Access Network	1-6
Enterprise-Wide Network	1-8
Wireless Outdoor Connections	1-10
<hr/>	
<b>2 Setting up your WaveMANAGER Station</b>	2-1
Introduction	2-1
Assigning a WaveMANAGER Station	2-2
Wireless WaveMANAGER Station	2-2

## Contents

---

Wired WaveMANAGER Station	2-4
Installing the WaveMANAGER software	2-7
WaveMANAGER/CLIENT	2-7
WaveMANAGER/AP	2-8
Uninstalling WaveMANAGER Software	2-10

---

<b>3</b>	<b>Configuring your Network</b>	3-1
	Introduction	3-1
	Configuring a Basic Access Network	3-2
	Step 1 - Installing the WavePOINT-II	3-3
	Step 2 - Connecting to a WavePOINT-II	3-3
	Step 3 - Setting the WaveLAN Parameters	3-5
	Step 4 - Saving the Configuration to a File	3-7
	Step 5 - Upload the Configuration	3-8
	Configuring an Enterprise-wide Network	3-9
	Step 1 - The Paperwork	3-10
	Step 2 - Creating a Template File	3-13
	Step 3 - Configuring WavePOINT-II	3-24
	Step 4 - Mounting the WavePOINT-II Units	3-29
	Modifying the Configuration	3-30
	Changing Common Parameters	3-30
	Configuring Outdoor Antenna Links	3-31
	Point-to-Point Link Configuration	3-33
	Multiple Point-to-Point Link Configuration	3-37

---

<b>4</b>	<b>Monitoring your WaveLAN Network</b>	4-1
	Introduction	4-1
	WaveMANAGER Utilities	4-1

## Contents

---

	WaveMANAGER/CLIENT	4-4
	Monitoring Methods	4-4
	Running WaveMANAGER/CLIENT	4-6
	Link Test	4-8
	Site Monitor	4-12
	Logging Measurement Data	4-17
	Frequency	4-19
	Access Control	4-20
	WaveMANAGER/AP	4-21
	Monitoring Methods	4-21
	Running WaveMANAGER/AP	4-22
<hr/>		
<b>5</b>	<b>Optimizing Performance</b>	5-1
	Introduction	5-1
	Areas of Activity	5-2
	Eliminating Redundant Traffic	5-2
	Optimizing Wireless Connections	5-9
	Dual Band Configuration	5-13
	Avoiding Channel Crosstalk	5-20
<hr/>		
<b>6</b>	<b>Security</b>	6-1
	Introduction	6-1
	Securing Access to Wireless Data	6-2
	Connecting to the Network	6-2
	Data Encryption	6-3
	Access Control	6-6
	Securing WavePOINT-II Configuration	6-11
	Read and Read/Write passwords	6-11

## Contents

---

	SNMP IP Access	6-12
	Trap Host Alerts	6-13
<hr/>		
<b>A</b>	<b>Troubleshooting</b>	A-1
	Problem Determination	A-1
	Problem-solving Approach	A-1
	Where do I start?	A-2
	LED Error Table	A-12
	Miscellaneous problems	A-14
	Time-Out Error	A-14
	WavePOINT-II Resets Continuously	A-14
<hr/>		
<b>B</b>	<b>Forced Reload Procedure</b>	B-1
	Introduction	B-1
	Performing a Forced Reload	B-3
	1 - Preparations	B-3
	2 - Set the Unit to 'Forced Reload' Mode	B-5
	3 - Open The WavePOINT-II Software File	B-6
	4 - Modify WavePOINT-II parameters	B-8
	5 - Upload the Software and Configuration	B-8
	6 - Finishing the Forced Reload	B-10
<hr/>		
<b>C</b>	<b>WavePOINT-II Configuration Record</b>	C-1
	Start-Up Configuration	C-1

## Contents

---

---

**GL**   **Glossary** GL-1

---

**LOF**   **List of Figures** LOF-1

---

**IX**   **Index** IX-1



---

## WaveLAN Technical Support

You can find the most recent software and user documentation for all WaveLAN products on our internet site.

---

### Software and Documentation

World Wide Web	<a href="http://www.wavelan.com">http://www.wavelan.com</a>
FTP Server	<a href="ftp://ftp.wavelan.com/pub">ftp://ftp.wavelan.com/pub</a>

If you encounter problems when installing or using this product, or would like information about our other WaveLAN products, please contact your local Authorized WaveLAN Reseller or regional Lucent Technologies Sales Office. Addresses of Resellers and Sales Offices can be found on the WaveLAN website.

In case no local or regional support is available, you can reach us at the addresses or telephone numbers listed below.

---

### WaveLAN Regional Support

U.S.A	<a href="mailto:usasupport@wavelan.com">usasupport@wavelan.com</a>
Caribbean/ Latin America / Canada	<a href="mailto:calasupport@wavelan.com">calasupport@wavelan.com</a>
Europe/ Middle-East/ Africa	<a href="mailto:emeasupport@wavelan.com">emeasupport@wavelan.com</a>
Asia/ Pacific	<a href="mailto:apasupport@wavelan.com">apasupport@wavelan.com</a>

---

### WaveLAN Global Support

U.S.A	Voice:	+1 800 WAVELAN
		+1 937 445 7256
	Fax:	+1 937 445 5552

When contacting WaveLAN Support, please complete the WaveLAN Problem Report form and include it with your email or fax. The form (report.txt) is available on the WaveLAN software diskette, or you can go to the Feedback section of the WaveLAN website and fill out the Problem Report form on-line.

---

## **Regulatory Information**

The devices described within this manual must be installed and used in strict accordance with the manufacturer's instructions, as described in the user documentation that came with the device. Lucent Technologies is not responsible for any radio or television interference caused by unauthorized modification of WaveLAN equipment or the substitution or attachment of connecting cables and equipment other than specified by Lucent Technologies. The correction of interference caused by such unauthorized modification, substitution or attachment will be the responsibility of the user.

In situations where the devices are used in combination with other wireless products and/or antennas, the user should consult the documentation that came with each device for additional Regulatory Information and/or Safety and Installation Requirements that might apply to the wireless installation.

## **Exposure to Radio Frequency Radiation**

The radiated output power of WaveLAN devices are far below the FCC radio frequency exposure limits. Nevertheless, all WaveLAN devices should be mounted in such a manner as to minimize the potential for human contact during normal operation. Antennas should not be contacted during operation to avoid the possibility of exceeding the FCC radio frequency exposure limits. When installing any WaveLAN device, please refer to the regulatory statements in the documentation that comes with those products for additional information.

---

# Introduction

# 1

---

**About WaveLAN** **1-1**

---

**About WaveMANAGER** **1-2**

WaveMANAGER/CLIENT 1-2

WaveMANAGER/AP 1-2

---

**About This User's Guide** **1-3**

About Icons Used In This Document 1-4

On-line Help Documentation 1-5

Additional Files on Your Diskettes 1-5

Other Sources of Information 1-5

---

**Sample Network Scenarios** **1-6**

Basic Access Network 1-6

Enterprise-Wide Network 1-8

Wireless Outdoor Connections 1-10



---

# Introduction

# 1

---

## About WaveLAN

---

The WaveLAN product family is a comprehensive set of network equipment that enables you to build any type of network configuration, from an ad-hoc wireless workgroup to a completely wireless infra-structure. The WaveLAN product family consists of:

- WaveLAN/ISA network adapter cards, for (desktop) computers with AT/ISA compatible expansion slots.
- WaveLAN/PCMCIA network adapter cards, for (mobile) computers that support a PC Card Type II slot.
- WavePOINT-II access points are transparent WaveLAN to Ethernet bridges that enable you to connect WaveLAN wireless stations to existing Ethernet LAN infrastructures.

The WaveLAN network adapter cards are not much different than any other type of adapter card for wired LANs. The operating system of your host devices will not even notice the difference.

WaveLAN cards support any protocol that is supported by regular Ethernet adapter cards. Like wired network adapter cards, WaveLAN adapter cards are installed with a dedicated WaveLAN driver, but unlike wired adapter cards, WaveLAN adapters do not need a cable to connect them to the network. Only WaveLAN cards allow you to relocate workstations without need to change network cabling or connections on patch panels or hubs.

## Introduction

### About WaveMANAGER

---

## About WaveMANAGER

---

The WaveMANAGER software suite consists of a set of management tools that enable you to:

- Configure network components such as WavePOINT-II access points.
- Diagnose the network performance and, if necessary, analyze and solve network errors.
- Manage and optimize network performance.

WaveMANAGER consists of two major tools:

- **WaveMANAGER/CLIENT**
- **WaveMANAGER/AP**

### WaveMANAGER/CLIENT

---

The WaveMANAGER/CLIENT is a diagnostic utility designed for WaveLAN client stations. You can use this tool to monitor wireless communication between a WaveLAN client station and its WavePOINT access point, or between a WaveLAN station and other wireless stations in its vicinity.

WaveMANAGER/CLIENT can be installed on any WaveLAN client station or (mobile) Administrator Station that runs the Microsoft Windows 95 or Windows NT (v.4.0) operating system.

### WaveMANAGER/AP

---

WaveMANAGER Access Point (WaveMANAGER/AP) is primarily a tool for LAN administrators or system supervisors. You can use the WaveMANAGER/AP program to configure WavePOINT-II access points and to monitor the performance of your wireless network.

WaveMANAGER/AP can be installed on both wired and wireless (mobile) WaveLAN Administrator Stations that run the Microsoft Windows 95 or Windows NT (v. 4.0) operating system.

## About This User's Guide

---

This guide was intended for use with WaveMANAGER on WaveLAN-I installations only. If you are using WaveLAN/IEEE, you should check the website for more information.

Within this manual, you will find the following:

- Chapter 1 "Introduction" describes the various WaveMANAGER tools and three WaveLAN Network scenarios that will be used throughout this document.
- Chapter 2 "Setting up your WaveMANAGER Station", describes how to assign a WaveMANAGER station and how to install the necessary software.
- Chapter 3 "Configuring your Network" explains how to configure your particular network, using three network scenarios, from simple to complicated.
- Chapter 4 "Monitoring your WaveLAN Network", describes how to monitor and optimize wireless performance, and how to enhance security for your WaveLAN network.
- Chapter 5 "Optimizing Performance" The performance of your LAN is usually determined by a complex combination of different factors. This section will present a number of considerations that may help you.
- Chapter 6 "Security" To minimize unauthorized use of your WaveLAN network, you will need to secure your network.
- Appendix A "Troubleshooting", describes various scenarios for troubleshooting and solving networking problems.

This document does not describe every possible option as supported by the WaveMANAGER/CLIENT and WaveMANAGER/AP program. It serves as a general guideline to help you to decide which tool can help you to accomplish a specific task. For more information about specific WaveMANAGER screens or options you are advised to consult the On-line Help Documentation.

## Introduction

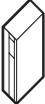
### About This User's Guide

---

## About Icons Used In This Document

---

Throughout this document we use the icons listed below to picture the following network devices:

<b>Icon</b>	<b>Description</b>
	Wireless (mobile) Client Station equipped with WaveLAN/PCMCIA
	Wireless Client Station equipped with WaveLAN/ISA
	WavePOINT-II access point optionally equipped with WaveLAN/PCMCIA or WaveLAN/ EAM
	Server Station
	Router
	Outdoor (Directional) Antenna

## Introduction

### About This User's Guide

---

## On-line Help Documentation

---

Information about specific WaveMANAGER screens or options, that is displayed on the screen of your WaveMANAGER/AP or WaveMANAGER/Client program, is covered in the on-line help of the program.

- To access context-sensitive help on a specific screen for the WaveMANAGER programs, click the Help button or press the **F1** function key.
- You can click the Help Contents tab to get an overview of the on-line information, or click the Index tab to open an alphabetical list of specific topics.

Product Specifications are listed in the 'User's Guide' that came with your WaveLAN products.

## Additional Files on Your Diskettes

---

All software diskettes that are shipped with your WaveLAN products include a file called 'README.TXT'. This file contains information about the version of the software and/or drivers on the diskette.

You are advised to print and read this file prior to installing your WaveLAN products, as it may contain additional information that was not available when this document was printed. You can also download or view the readme.txt file on the WaveLAN web site.

## Other Sources of Information

---

For information on updates and other WaveLAN news, see the WaveLAN web site: <http://www.wavelan.com>

For WaveLAN Technical Support, please consult the information printed on page vii of this document.

## Sample Network Scenarios

---

You can use WaveLAN networking products to set up a wide range of different network configurations. To make this document as relevant as possible to your situation, we have selected three network scenarios:

- Basic Access Network
- Enterprise-Wide Network.
- Wireless Outdoor Connections.

According to your networking requirements, you can select one of these scenarios to set up an initial installation. When your situation differs from the scenarios described, the information and instructions provided in this guide should be sufficient to cover almost all technical variations on the scenarios provided.

For a description of the icons used in the following illustrations, see “About Icons Used In This Document” on page 1-4.

### Basic Access Network

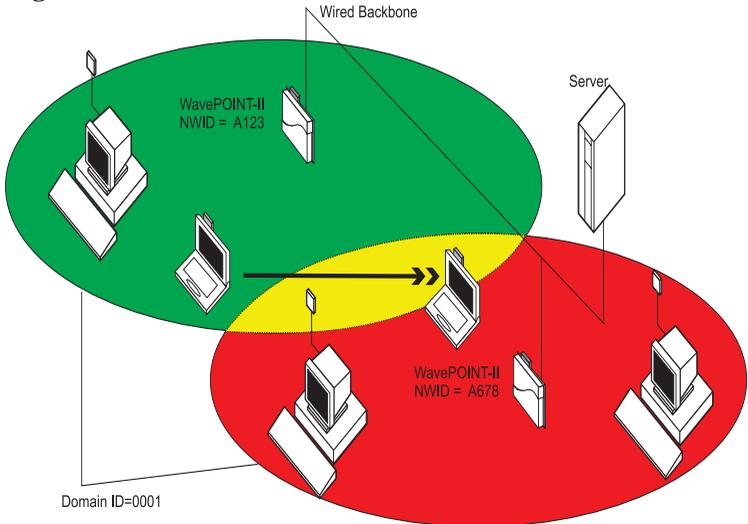
---

A basic access network as pictured in Figure 1-1 on page 1-7, consists of a small to medium size wireless LAN, where WavePOINT access points provide access to a wired LAN or backbone that interconnects multiple wireless cells. A Basic Access Network does not include any routers or gateways that connect the wireless network to enterprise LANs, leased lines or outdoor connections.

The number of WavePOINT-II access points in this network typically varies from 1 to 5.

In a Basic Access Network, mobile users can use laptop or notebook computers (mobile stations) equipped with a WaveLAN/ PCMCIA card.

**Figure 1-1 Basic Access Network**



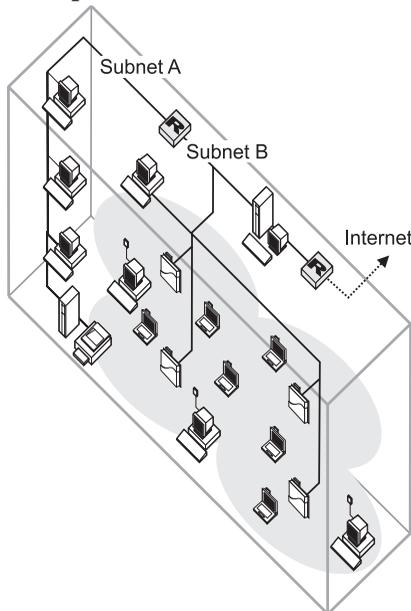
The roaming functionality of the WaveLAN/PCMCIA card will provide seamless connectivity when moving between different wireless cells. Roaming throughout the building, the station will dynamically connect to other WavePOINT access points when needed to maintain the wireless connection without interruption.

## **Enterprise-Wide Network**

---

This network scenario has the scale of a corporate LAN which may include network segments in different departments, interconnected by means of routers or gateways.

**Figure 1-2 Enterprise-wide network**



The network may extend to wireless networking in different buildings, where the buildings are connected by a wired link, e.g. a leased line. Furthermore, enterprise-wide networks may be part of a global network.

All wireless computing devices that are equipped with WaveLAN cards will be able to connect to servers or other stations anywhere in the network environment via the WavePOINT-II access points.

The access points are interconnected via a wired backbone to provide inter-cell communication.

Enterprise-wide networks will typically use a TCP/IP protocol and IP addressing for network equipment. A LAN Administrator may address this type of equipment from a central location.

Each WavePOINT unit and WaveMANAGER Station, as well as all network devices such as routers and gateways, must have a unique IP address. However, IP addressing is not required for client stations.

Naturally, this network also allows roaming of mobile stations.



**NOTE:**

WaveLAN stations can not roam over routers. To allow roaming between different cells, all WaveLAN stations and WavePOINT-II access points must be connected to the same subnet.

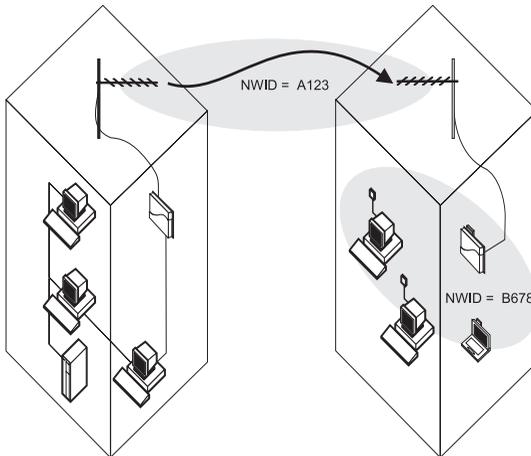
**Wireless Outdoor Connections**

---

This scenario may be a specific application of a WaveLAN within an “Enterprise-Wide Network” as described on page 1-8.

This scenario covers a corporate network which may extend to multiple buildings. As an alternative to leased lines, the buildings are connected by wireless links, thus providing optimum flexibility.

**Figure 1-3 Wireless Outdoor Connection**



To set up a WaveLAN Outdoor Connection, you can use WavePOINT-II access points in combination with the WaveLAN/EAM Module and outdoor antennas.

**⇒ NOTE:**  
Outdoor wireless communication may be subject to local or national regulations.

## **Introduction**

### **Sample Network Scenarios**

---

The maximum range of a WaveLAN Outdoor installation is determined by the type of antenna equipment used. For more detailed information, refer to the WaveLAN Outdoor 'Getting Started' document that is available on our WaveLAN web site.

To comply with local regulations the antenna type offerings in the various regions may differ. You are advised to consult your local WaveLAN reseller for information about outdoor antenna solutions that are available in your country.



---

# Setting up your WaveMANAGER Station

# 2

---

<b>Introduction</b>	<b>2-1</b>
<hr/>	
<b>Assigning a WaveMANAGER Station</b>	<b>2-2</b>
Wireless WaveMANAGER Station	2-2
• Configuration	2-3
• Monitoring	2-4
Wired WaveMANAGER Station	2-4
• Configuration	2-5
• Monitoring	2-6
<hr/>	
<b>Installing the WaveMANAGER software</b>	<b>2-7</b>
WaveMANAGER/CLIENT	2-7
WaveMANAGER/AP	2-8
<hr/>	
<b>Uninstalling WaveMANAGER Software</b>	<b>2-10</b>



---

# Setting up your WaveMANAGER Station

# 2

---

## Introduction

---

The configuration and management of WaveLAN infrastructures is managed from a WaveMANAGER station. The WaveMANAGER station is typically a computer used by the LAN administrator to administer the network. A WaveMANAGER station is required to:

- Configure and manage all WavePOINT-II access points.
- Determine the optimal placement of WavePOINT-II access points and antennas.
- Diagnose the performance of the network.

To set up a WaveMANAGER Station you will need to:

- Assign a WaveMANAGER Station.
- Install the WaveMANAGER software.

The WaveMANAGER software suite is comprised of two software tools that are described later in this chapter:

- WaveMANAGER/CLIENT and
- WaveMANAGER/AP

You can assign as many WaveMANAGER stations as you like. Depending on how you would like to manage your WaveLAN network, you can select both wired and wireless stations to function as a WaveMANAGER station.

## Setting up your WaveMANAGER Station

### Assigning a WaveMANAGER Station

---

## Assigning a WaveMANAGER Station

---

To set up a WaveMANAGER Station, you can use any wired or wireless desktop computer or laptop that meets the following requirements:

- A 80486 or faster processor.
- Free disk space of 4 Mb.
- 8 Mb RAM (16 Mb or more recommended).
- Microsoft Windows 95 or Windows NT (v.4.0).
- An Ethernet or WaveLAN network adapter card.
- A loaded TCP/IP stack that provides a Windows Sockets (winsock) interface. The TCP/IP protocol can be found on the Microsoft Windows installation disks or CD-ROM.

The choice for a wireless or wired WaveMANAGER Station will depend on your preferences and abilities to administer your WaveLAN network. Of course you can assign multiple stations to serve as WaveMANAGER Stations, allowing for a combination of wired and wireless stations.

## Wireless WaveMANAGER Station

---

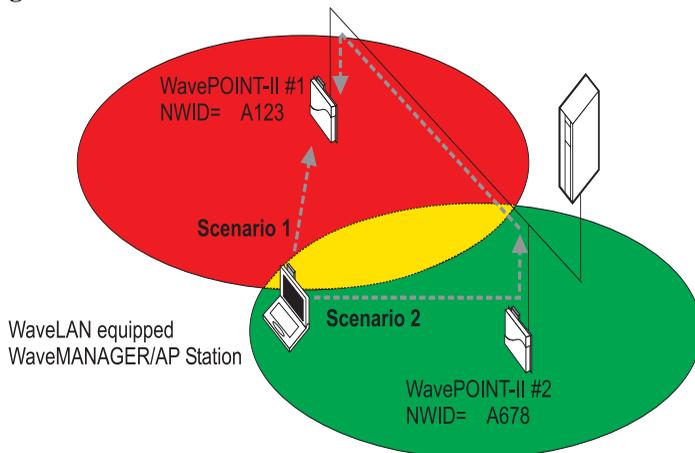
A wireless WaveMANAGER Station is recommended when:

- Your network is relatively small, e.g. a Basic Access Network.
- LAN Administrators require easy access to wireless areas, e.g. for on-site troubleshooting.
- You need to perform a site verification to determine optimal placement of WavePOINT-II access points.

A wireless, mobile WaveMANAGER Station allows you to use WaveMANAGER/CLIENT as well as WaveMANAGER/AP.

- ⇒ NOTE:**  
When you use a wireless station, please note that stations equipped with ISA cards do not support the Site Monitor option as described in “Site Monitor Options” on page 4-5.

**Figure 2-1 Wireless WaveMANAGER Station**



## Configuration

As shown in Figure 2-1, the wireless WaveMANAGER Station can use the WaveMANAGER/AP program to configure the WavePOINT-II access points. WavePOINT units are addressed by their unique IP address. Access to the configuration of the WavePOINT units can either be:

- Direct, by means of a wireless point-to-point connection (scenario 1). In this scenario, the WaveLAN parameters of the WaveMANAGER Station should match the settings of WavePOINT #1 (NWID A123).

## Setting up your WaveMANAGER Station

### Assigning a WaveMANAGER Station

---

- Indirect, via a wireless point-to-point connection between the WaveMANAGER Station and the nearest WavePOINT access point and a backbone that interconnects all WavePOINT access points (scenario 2). In this scenario, the parameters of the WaveMANAGER Station should match the settings of WavePOINT #2 (NWID A678).

## Monitoring

Looking at Figure 2-1 again, a wireless WaveMANAGER Station can use the WaveMANAGER/CLIENT program to diagnose the Radio Frequency link with:

- Both WavePOINTs simultaneously (Site Monitor), for example to perform a site verification.
- A single WaveLAN station or WavePOINT-II access point within range or a remote WaveLAN device using WaveMANAGER/AP's Remote Link Test.

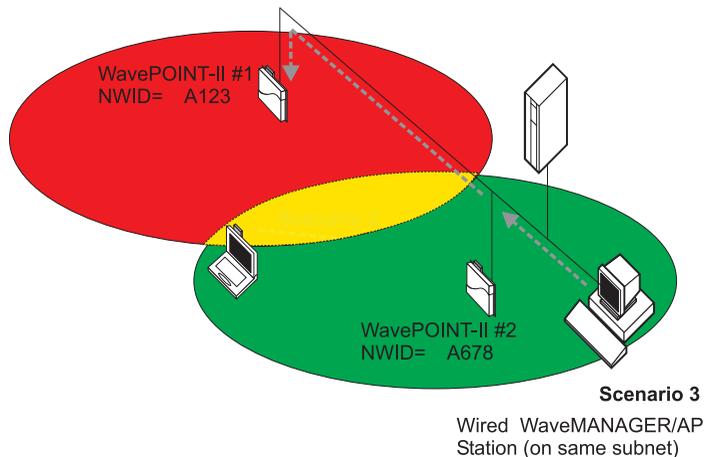
## Wired WaveMANAGER Station

---

A wired WaveMANAGER Station allows you to configure WavePOINT-II access points through a wired backbone.

The WaveMANAGER/AP enables you as well to validate Radio Frequency links between a remote WavePOINT-II access point and WaveLAN stations connected to the WavePOINT-II.

**Figure 2-2**    **Wired WaveMANAGER Station**



## Configuration

As shown in Figure 2-2, the wired WaveMANAGER Station has access to both WavePOINTs A and B via the wired backbone. The WavePOINT units are identified by means of their unique IP address.

When your LAN architecture comprises multiple subnets separated by gateways or routers, please note that the WaveMANAGER Station which you intend to use for the initial configuration, must be on the same subnet as the WavePOINT-II access points. Once the WavePOINT-II access points have been configured and their IP addresses have been registered, you can use any station that can access the WavePOINT units via the TCP/IP protocol.

## **Setting up your WaveMANAGER Station**

### Assigning a WaveMANAGER Station

---

#### **Monitoring**

When you use a wired WaveMANAGER Station you will not be able to move around different physical locations of the network to determine or optimize the placement of stations, WavePOINT-II access points or antennas.

To perform monitoring tasks, however, a wired WaveMANAGER Station can use WaveMANAGER/AP's Remote Link Test and Remote Statistics.

## **Installing the WaveMANAGER software**

---

The WaveMANAGER software suite includes the following tools:

- WaveMANAGER/CLIENT.
- WaveMANAGER/AP.

### **WaveMANAGER/CLIENT**

---

WaveMANAGER/CLIENT is a WaveLAN diagnostics tool that runs on wireless stations only. To setup a WaveMANAGER station that is capable of running the WaveMANAGER/CLIENT program, the station must be equipped with a WaveLAN/PCMCIA or WaveLAN/ISA card in the assigned station.

To install the WaveMANAGER/CLIENT software, proceed as follows:

1. Insert the WaveMANAGER/CLIENT for Windows diskette in the station that you want to designate as the WaveMANAGER Station.
2. Select 'Run' from the Windows 95 or Windows/NT Start menu.
3. Browse to select the diskette drive.
4. Select the folder Util.
5. Select **Setup.exe** from the list of files in the Util folder; subsequently, this file name should be displayed in your Run window.
6. Click OK. (Older versions of the software will be overwritten).
7. Follow the instructions of the setup program that are displayed on the screen.

## Setting up your WaveMANAGER Station

### Installing the WaveMANAGER software

---

#### WaveMANAGER/AP

---

WaveMANAGER/AP can be installed on both wireless and wired stations.

For a wireless station, the network interface card would typically be a WaveLAN/ISA or WaveLAN PCMCIA card.

For a wired station, this would typically be an Ethernet card, but could also be a Token ring card, modem or ISDN adapter.

To use the WaveMANAGER/AP program, the station must also have the TCP/IP protocol installed. To determine if the TCP/IP protocol has been installed on your WaveMANAGER station, display the Network Neighborhood properties for your WaveMANAGER station:

1. From the Windows Taskbar, click the 'Start' button.
2. Point to settings and click on 'Control Panel'
3. In the Control Panel window, double-click the Network Neighborhood icon.
4. On a Windows 95 station, scroll down the list of 'network components installed' to verify if this list includes the item 'TCP/IP -> xxxxxxxx', where xxxxxx identifies the name of your network adapter (e.g. WaveLAN PCMCIA Adapter).

On a Windows NT station, select the tab 'Protocols' and verify if the list of protocols includes the item 'TCP/IP Protocol'.

5. If the list includes the TCP/IP protocol, click Cancel to close the window and proceed with the installation of your WaveMANAGER/AP software.

If the list does not include the TCP/IP protocol, click the Add button and follow the instructions that appear on the screen prior to proceeding with the software installation for WaveMANAGER/AP.

## Setting up your WaveMANAGER Station

### Installing the WaveMANAGER software

---

To install the WaveMANAGER/AP software, proceed as follows:

1. Insert WavePOINT-II Management Software disk 1 in your WaveMANAGER Station.
2. From the Start menu, select 'Run'.
3. Use the Browse button to select the diskette drive.
4. Select **Setup.exe** from the list of files on the diskette.
5. Click OK to return to the 'Run' menu.
6. Click OK to start the 'Setup' program.
7. Follow the instructions of the setup program that are displayed on the screen.



#### **NOTE:**

The first dialog box of the installation is a reminder to remove all older versions of WaveMANAGER/AP. You can follow the screen prompts to remove older versions, or you can use the method described in the section "Uninstalling WaveMANAGER Software" on page 2-10.

During the installation, you will be prompted for a directory to install the WaveLAN program files. The default directory for WaveLAN programs is:

C:\Program Files\WaveLAN\WaveMANAGER\AP

We recommend that you use the default directory suggested by the installation program because other WaveLAN programs may refer to this default directory.

## **Uninstalling WaveMANAGER Software**

To uninstall WaveMANAGER software, proceed as follows.

1. Click the Start button and select Settings, Control Panel.
2. On the Control Panel, click the icon 'Add/Remove Programs'.
3. Select WaveMANAGER/AP or WaveMANAGER/CLIENT and click the 'Add/Remove' button.

The Uninstall option will remove program files only. If you have stored logfiles in the Program directory, these files will not be removed.

---

# Configuring your Network

# 3

---

**Introduction** **3-1**

---

**Configuring a Basic Access Network** **3-2**

- Step 1 - Installing the WavePOINT-II 3-3
- Step 2 - Connecting to a WavePOINT-II 3-3
- Step 3 - Setting the WaveLAN Parameters 3-5
- Step 4 - Saving the Configuration to a File 3-7
- Step 5 - Upload the Configuration 3-8

---

**Configuring an Enterprise-wide Network** **3-9**

- Step 1 - The Paperwork 3-10
  - About IP Addresses and Subnets 3-11
  - About NWIDs 3-11
- Step 2 - Creating a Template File 3-12
  - Open the Default Configuration File 3-13
  - Set the Common Parameters 3-13
  - Save the Template File 3-23

---

Step 3 - Configuring WavePOINT-II	3-23
• Connecting to the WavePOINT-II	3-24
• Import the Template File	3-26
• Setting the Unique Identifiers	3-26
• Create a Back-up File of the Configuration	3-27
• Upload the Configuration	3-27
• Complete the Paperwork	3-27
Step 4 - Mounting the WavePOINT-II Units	3-28

---

<b>Modifying the Configuration</b>	<b>3-29</b>
------------------------------------	-------------

Changing Common Parameters	3-29
----------------------------	------

---

<b>Configuring Outdoor Antenna Links</b>	<b>3-30</b>
--	-------------

Point-to-Point Link Configuration	3-32
• Setting the Required Parameters	3-33
Multiple Point-to-Point Link Configuration	3-36

---

# Configuring your Network

# 3

---

## Introduction

---

Within this chapter, we describe how to configure a network using WaveLAN products. Because the number of possible network configurations is unlimited, we have defined three possible scenarios, from simple to complicated:

- Basic Access Network
- Enterprise-wide Network
- Outdoor Connections

Naturally, your particular situation may differ from these scenarios, so you should select the scenario that best suits your particular network environment.

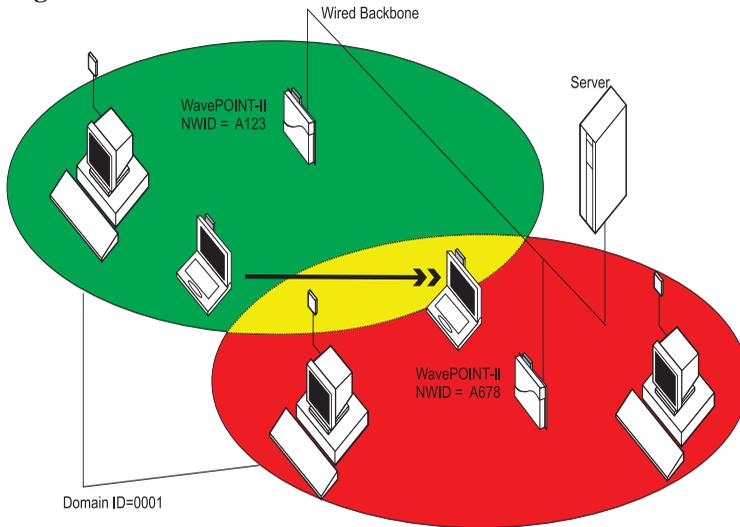
To manage your WavePOINT-II access points, you must assign a unique IP address for each WavePOINT-II unit within your network. Furthermore, your WaveMANAGER Station needs to have an IP address. The TCP/IP connection of your WaveMANAGER Station should be either:

- on the same subnet as the WavePOINT-II access points, as described in “Basic Access Network” on page 1-6, or
- provide access to the subnet of the WavePOINT-II access points via routers, gateways or another type of LAN connection that supports the TCP/IP protocol.

## **Configuring a Basic Access Network**

---

**Figure 3-1 Basic Access Network**



In Figure 3-1, all devices have the same Domain ID. However, each area, or cell, is identified by its own unique network ID (NWID). For each cell, the unique NWID is assigned to the WavePOINT-II interface and each WaveLAN card within the cell.

Because the coverage area and the number of devices in this network are relatively small, it is most practical to start by installing the WavePOINT-II units in their various locations in the department or building and then to configure them one by one.

The easiest way to configure the WavePOINT-II units is to move around the network with a mobile WaveMANAGER Station and to make a direct, wireless connection with each WavePOINT-II unit.

To install and configure the WavePOINT-II units, you need to carry out the following activities:

1. Install the WavePOINT-II units in their various locations.
2. Connect to the WavePOINT-II unit from your WaveMANAGER Station and register the IP address (required).
3. Modify the factory-set default WaveLAN parameters
  - NWID (optional)
  - Roaming enabled (optional)
  - Domain ID (required if you have roaming stations).
4. Save the configuration parameters to a back-up file.
5. Upload the configuration to the WavePOINT-II unit.
6. Repeat steps 2 to 5 for each of the WavePOINT-II units to be configured.

#### **Step 1 - Installing the WavePOINT-II**

---

For installation instructions of the WavePOINT-II units, please refer to the 'WavePOINT-II Getting Started' manual.

#### **Step 2 - Connecting to a WavePOINT-II**

---

To connect to a WavePOINT, you need to assign a unique IP address. Because each new WavePOINT-II unit has the same, factory-set default IP address (153.69.254.254), this address needs to be changed to an address that falls within the range of IP addresses allocated to your organization. If your network includes a DHCP or BOOTP server, see "BOOTP and DHCP" on page 3-11.

If your organization does not use IP addressing, you will need to assign a user-defined IP address (see "About IP Addresses and Subnets" on page 3-11).

## Configuring your Network

### Configuring a Basic Access Network

---

To make a direct connection with a WavePOINT-II unit and to change the default IP address, proceed as follows:

1. Move the WaveMANAGER Station to a location in the vicinity of the WavePOINT-II unit to be configured.
2. Start WaveMANAGER/AP by clicking its icon in the WaveLAN program folder.
3. Select 'Open Remote Configuration' from the 'File' menu.
4. Click the 'Scan' button to display a list of WavePOINT-II units within range of your WaveMANAGER Station and then select the WavePOINT-II unit to be configured.

**Figure 3-2 Scan IP address dialog box**



5. Click the 'Change IP' button. (This button is only active if the IP address still has its default value; it becomes inactive once the default IP address has been changed).
6. Assign a unique IP address to the WavePOINT-II unit.
  - If you select an address from a range of assigned IP addresses, make sure that the selected IP address belongs to the same subnet as the other WavePOINT-II units.
  - If you use user-defined IP addresses, it may be possible to simply change the last three digits of the default IP address.

## Configuring your Network

### Configuring a Basic Access Network

---

7. Record the IP address on the "WavePOINT-II Configuration Record" located in Appendix C.
8. Click OK to save the new IP address to the target WavePOINT-II unit (Please note that the IP address is now stored in the volatile memory of the WavePOINT-II unit. It will remain active until the WavePOINT-II unit is reset or switched off and on again).
9. Click OK again to return to the WaveMANAGER's opening window.

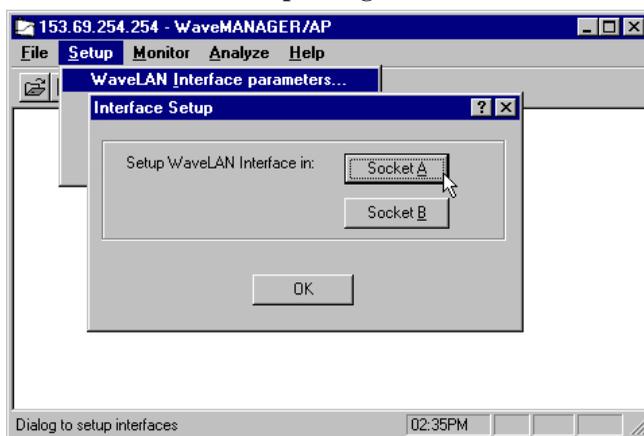
### Step 3 - Setting the WaveLAN Parameters

---

To change the default values of the WaveLAN parameters (Network ID (NWID), Domain ID and roaming), proceed as follows:

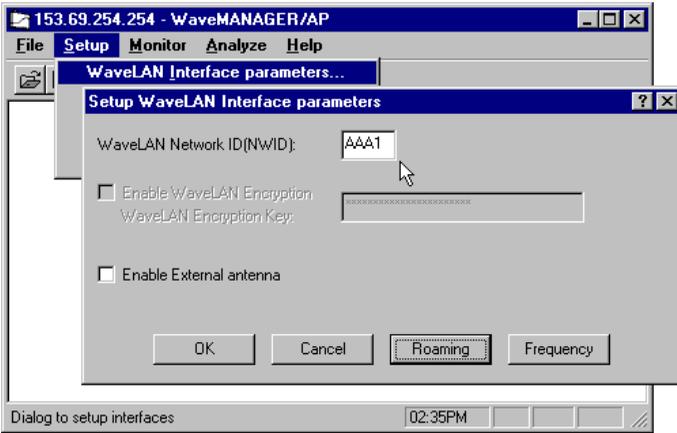
1. Select 'WaveLAN Interface parameters' from the 'Setup' menu.

**Figure 3-3 Interface setup dialog box**



2. Select the socket (A or B) of the WavePOINT-II unit which you want to configure. After clicking the OK button, the following dialog box is displayed:

**Figure 3-4 Setup WaveLAN Interface Parameters**



3. Change the default value of the Network ID (NWID) to the value you wish to use for this interface of the WavePOINT-II unit. The NWID of sockets A and B must be different. The default value of the NWID is Sxxx, in which S indicates the socket (either A or B) and xxx represents the last three digits of the WavePOINT-II unit's serial number.

- Click the 'Roaming' button. The following dialog box will be displayed:

**Figure 3-5 Setup WaveLAN Roaming Parameters**



- Click the 'Enable Roaming' check box to enable roaming.
- Change the value of the Domain ID to the value you wish to use for all WavePOINT-II units in your network.
- Click OK to return to the WaveMANAGER/AP opening window.

#### **Step 4 - Saving the Configuration to a File**

---

- Select 'Save Config File as' from the 'File' menu to make a backup file of the configuration data on a local disk. We recommend that you use a name that allows you to easily recognize the relationship between the file name and the WavePOINT-II unit.
- We also suggest that you record the filename and the location where the WavePOINT-II unit will be installed on the "WavePOINT-II Configuration Record".

### **Step 5 - Upload the Configuration**

---

To upload the configuration data to the WavePOINT-II unit, select 'Save Config' from the 'File' menu.

The entire set of common and unique parameters are now saved permanently into the non-volatile Flash ROM of your WavePOINT-II unit. They will remain stored in the WavePOINT-II unit, even if the unit is reset or switched off and on again.

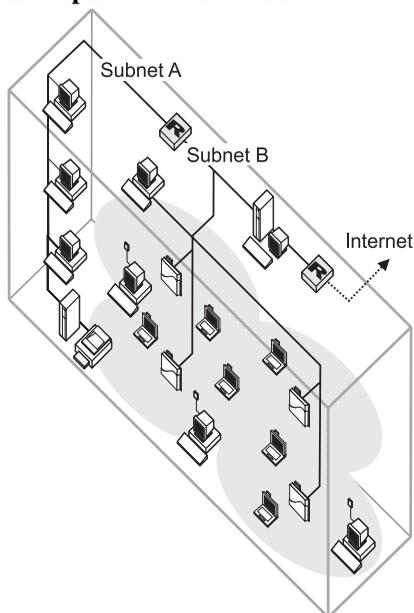
To install and configure more WavePOINT-II units, refer back to "Step 1 - Installing the WavePOINT-II" on page 3-3.

## **Configuring an Enterprise-wide Network**

---

As explained in the introduction, the second network scenario represents a network that may be composed of several departments or buildings.

**Figure 3-6 Enterprise-wide network**



Because this network is likely to involve a large number of WavePOINT-II units, the most efficient way to configure this network is to configure all WavePOINT-II units in one location before they are installed throughout the building(s) in which the network is to be installed.

To perform the configuration, all common configuration parameters are set one time, saved in a template file and subsequently loaded into each of the WavePOINT-II units. Values that are unique for each WavePOINT-II unit are then set or adjusted.

## Configuring your Network

### Configuring an Enterprise-wide Network

---

To configure the WavePOINT-II units, you need to carry out the following activities:

Step 1 - The Paperwork.

Step 2 - Creating a Template File to identify and set the parameters that must be the same for all WavePOINT-II units within the network.

Step 3 - Configuring WavePOINT-II, to identify and set the parameters that must be unique for each WavePOINT-II unit within the network.

Step 4 - Mounting the WavePOINT-II Units.

Each phase will consist of a series of numbered steps.

#### **Step 1 - The Paperwork**

---

To prepare the configuration, you need to carry out the following activities:

- Unpack the WavePOINT-II units and record their serial number and MAC address on the "WavePOINT-II Configuration Record" as printed in Appendix C of this document.
- Make a list of IP addresses available in your network, you will need one IP Address for each WavePOINT-II unit.
- Use the "WavePOINT-II Configuration Record" to assign one IP address to each of your WavePOINT-II units.
- Mark which socket(s) of the WavePOINT-II unit will contain a WaveLAN adapter and assign a unique four-digit NWID to each adapter interface (see "About NWIDs" on page 3-12').
- Record the intended system location of each WavePOINT-II unit on the "WavePOINT-II Configuration Record".

#### About IP Addresses and Subnets

In larger organizations that make use of IP addressing for communications, the network architecture may include different network segments (subnets), typically separated by a router or gateway.

When installing WaveLAN into this type of network architecture, please note that all WavePOINT-II devices and wireless stations must be installed on the same subnet, i.e. on the same side of the router or gateway, in order to support seamless connectivity for mobile users that 'roam' between various areas.

When assigning IP addresses to WaveLAN stations and WavePOINT-II access points, make sure that:

- Each WaveLAN device has a unique IP address
- All WaveLAN devices use the same subnet mask

The WaveLAN Roaming Functionality does not work over routers. When WavePOINT-II units are connected to different subnets, a mobile station may lose its network connection when it physically enters an area where the WavePOINT-II units are connected to a different subnet.

#### BOOTP and DHCP

When powered-up for the very first time, (i.e. the WavePOINT-II still uses its factory-set IP Address) the WavePOINT-II will broadcast a request for an IP Address. When your network includes a DHCP or BOOTP server, the server will automatically assign an available IP Address to the WavePOINT-II unit.

Depending on the exact settings of your BOOTP/DHCP services, you may need to add the MAC Address of the WavePOINT-II to the MAC Address table of the BOOTP/DHCP server. For more information about BOOTP/DHCP configuration, consult the

## Configuring your Network

### Configuring an Enterprise-wide Network

---

documentation that came with your BOOTP/DHCP server software.

The instructions in this chapter describe in detail how to assign the IP addresses and NWIDs to WavePOINT-II units in a network *without* a BOOTP/DHCP server.

### About NWIDs

The WaveLAN Network Identification Designator (NWID) distinguishes the wireless data traffic in one cell from all traffic in other cells in the vicinity, each WavePOINT-II unit in a wireless cell must have a different NWID.

New WavePOINT-II units have a factory-set default NWID that matches the last three digits of the unit's serial number, preceded by the letter A or B. The letter A or B identifies the PC Card slot of the WavePOINT-II device.

In other words, when you insert the WaveLAN adapter in slot A, the WavePOINT-II will start bridging operation with a NWID value of the format Axxx, where xxx identifies the last three digits of the units' serial number (that you wrote down on the WavePOINT-II Configuration Record). For xxx, you can use any character in the range of 0-9 and A-F, for example A09F, or BC34.



**NOTE:**

The factory-set default NWID differs from the NWID after you perform a 'Forced Reload'. For more information on 'Forced Reload' and the associated default parameters, please see "Introduction" on page B-1.

#### **Step 2 - Creating a Template File**

---

In larger networking organizations, it may become quite cumbersome to copy the common parameters to each of the WavePOINT-II units. When the number of access points increases, the risk of errors increases, usually as a result of typos when entering the common parameters.

Therefore, in larger networking environments, you are advised to create a template file that contains all common parameter settings that apply to all units within the network.

To create a template file with the common parameters that apply to all WavePOINTS, you need to carry out the following activities:

- Import a set of default configuration values from a file.
- Set the parameters that are common to all wavePOINT-II units of your network.
- Save these settings to a template configuration file.

#### **Open the Default Configuration File**

Before you start setting the common parameters, it is easiest if you import the default configuration values from a file. To do so, proceed as follows:

1. Start WaveMANAGER/AP by clicking its icon in the WaveLAN program folder.
2. Select 'Open Config File' from the 'File' menu and open the file 'default.cnf' from the following directory:

c:\program files\WaveLAN\WaveMANAGER\AP

## Configuring your Network

### Configuring an Enterprise-wide Network

---

#### Set the Common Parameters

The following common parameters should be set and stored in the template file:

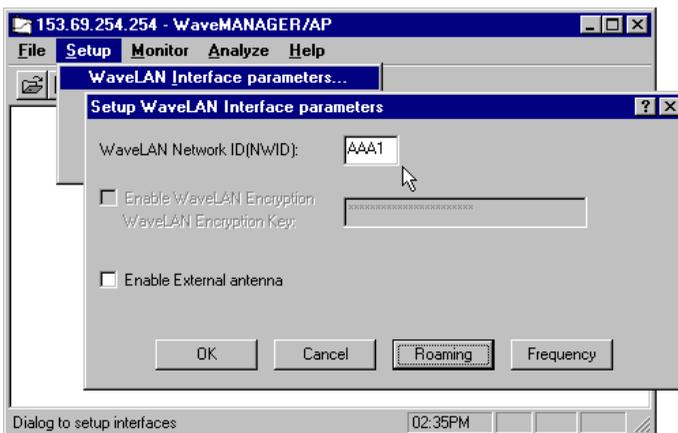
- WaveLAN interface parameters which include settings for Roaming, Domain ID, Responsiveness and Sensitivity levels (see “WaveLAN Interface Parameters” on page 3-14);
- Bridge parameters which include settings for Network protocol and static MAC address filtering, spanning tree and storm thresholds (see “Bridge Parameters” on page 3-17);
- Common IP parameters such as the default router and TTL (see “WavePOINT IP Parameters” on page 3-20);
- SNMP parameters such as passwords, system contact and SNMP traps (see “SNMP Parameters” on page 3-21).

#### WaveLAN Interface Parameters

To set the WaveLAN Interface Parameters:

1. Select the ‘WaveLAN Interface Parameters...’ option from the ‘Setup’ menu.
2. Select the socket (A or B) of the WavePOINT-II unit which you want to configure, then click OK. The following dialog box will be displayed:

**Figure 3-7 Setup WaveLAN Interface Parameters**



3. Change the default value of the Network ID (NWID) into a common value that will later be changed into a unique value. We suggest using A111 for socket A and B111 for socket B. Please note that the NWID of socket A and B must be different.
4. Click the Roaming button to display the following dialog box:

## Configuring your Network

### Configuring an Enterprise-wide Network

---

**Figure 3-8**     **Roaming setup dialog box**



5. Click the 'Enable Roaming' check box to enable roaming.
6. Change the value of the Domain ID to the value you wish to use for all WavePOINT-II units. If you wish, you can use the default value for all WavePOINT-II units.
7. (Optional) Enter a value for the Beacon Key to add security to your messages. The value of the Beacon Key is used to encode the NWID information included in beacon messages.
8. Use the default value (Normal) for the Responsiveness and Sensitivity levels. The Responsiveness level defines the frequency and time-out value of beacons issued by the WavePOINT-II unit. The Sensitivity level defines threshold values related to the Signal to Noise ratio of the WavePOINT-II.
9. Click OK to return to the WaveMANAGER/AP opening window.

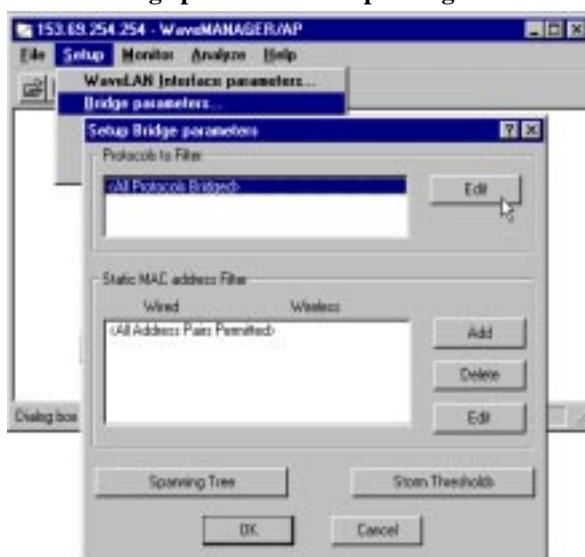
#### Bridge Parameters

To set the common bridge parameters:

1. Select 'Bridge parameters' from the 'Setup' menu to display the 'Setup Bridge Parameters' dialog box. The top section of this dialog box shows the 'Protocols to Filter' field which initially contains only one line: All Protocols Bridged.

---

**Figure 3-9** Bridge parameters setup dialog box



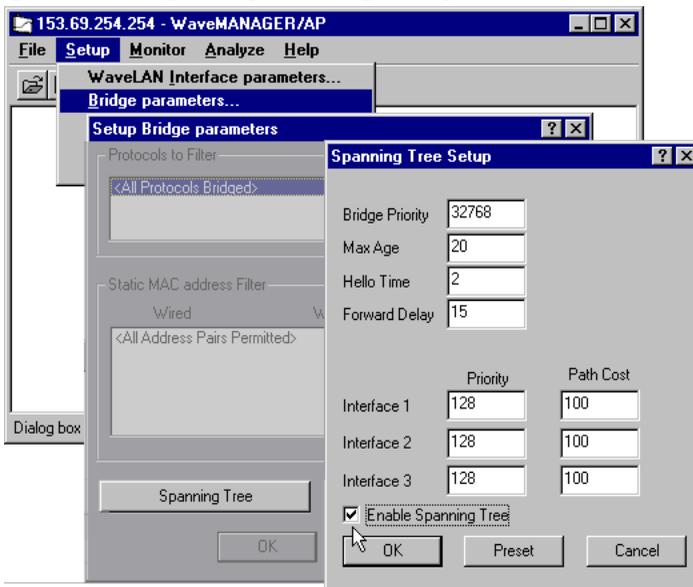
If you don't require specific networking protocols to be filtered, you can use the default setting for this parameter, which means that all protocols will be bridged by the WavePOINT-II unit. If you do require specific protocols to be filtered, e.g. if you want to optimize the performance of your network, see "Protocol Filtering" on page 5-3.

## Configuring your Network

### Configuring an Enterprise-wide Network

2. The bottom half of this dialog box shows the 'Static MAC Address Filter' field which is used to filter out stations that are not to send or receive any network traffic from the WavePOINT-II unit. For the common parameters, the default value can be left in this field. For more information on this field, please refer to Chapter 5 "Optimizing Performance".
3. The Spanning Tree button allows you to set parameters that are used in determining the optimum path for network traffic to travel, in a network that has been designed to include loops. To enable Spanning Tree and set the common parameters.
  - Click 'Enable Spanning Tree' check box;
  - Use default values (see Figure 3-10);
  - Click OK to return to the Bridge Parameters window.

**Figure 3-10 Spanning tree setup dialog box**



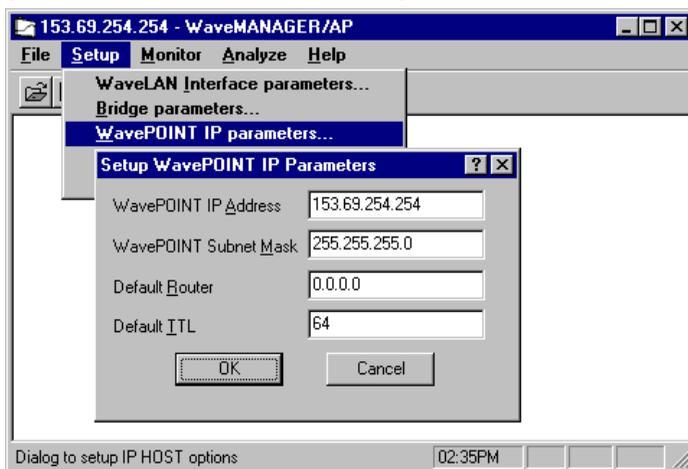
## Configuring your Network

### Configuring an Enterprise-wide Network

---

4. The Storm Threshold button allows you to set parameters that are used in protecting the network against overload from one station.

**Figure 3-11 Storm threshold dialog box**



5. To set the common parameters, press the Preset button. This will disable all threshold protection. Click OK to return to the 'Bridge Parameter' dialog box.
6. Click OK to return to the WaveMANAGER/AP opening window.

## Configuring your Network

### Configuring an Enterprise-wide Network

---

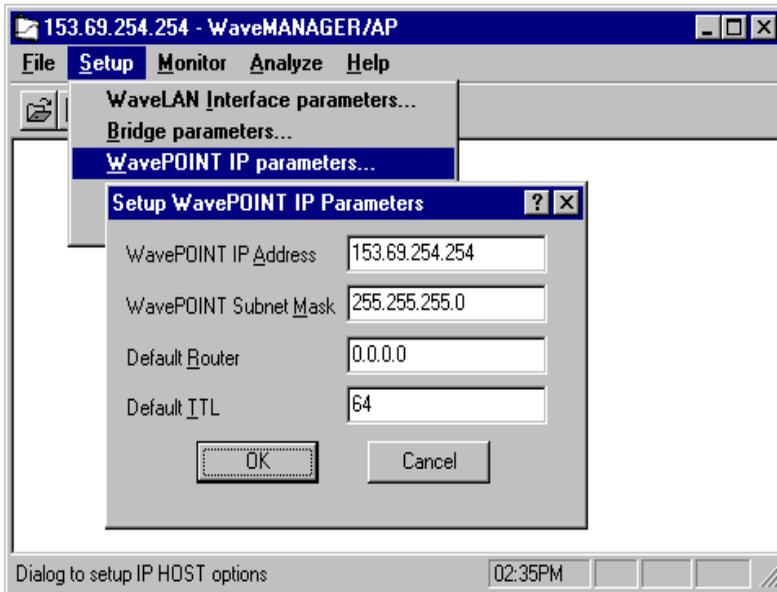
#### WavePOINT IP Parameters

To set the common IP parameters:

1. Select 'WavePOINT IP parameters' from the 'Setup' menu to display the 'IP Host Setup' dialog box (Figure 3-12).

---

**Figure 3-12** WavePOINT IP parameters setup dialog box



2. Use the default value of the IP address, since this value will be changed later when you set the values that are unique for each WavePOINT-II unit.
3. You can use either the default value (255.255.0.0) or change the value of the subnet mask for use with all units in your subnet.

## Configuring your Network

### Configuring an Enterprise-wide Network

---

4. The Default Router field is only relevant when you intend to use the WavePOINT-II support for TRAP messages (see also SNMP parameters).

You can use this (optional) field to identify the IP address of the router which the WavePOINT-II unit should use to find the Trap Host IP Address (identified in the SNMP Setup window).

The Default Router and the Trap Host IP Address are only used for TRAP messages generated by the WavePOINT-II unit upon a reset, modification of the configuration, or forced reload procedure.

If the value of this field is set to 0.0.0.0 (default), the WavePOINT-II unit will ignore the TRAP messages.

5. The default value of the TTL (Time To Live) field identifies the maximum number of hops for an IP message generated by the WavePOINT-II unit (typically used for the Trap Host messages).

The value in this field will be decreased each time the message passes a router. When the TTL value becomes 0, the message will be rejected by the next router it meets.

6. Click OK to return to the WaveMANAGER/AP opening window.

### **SNMP Parameters**

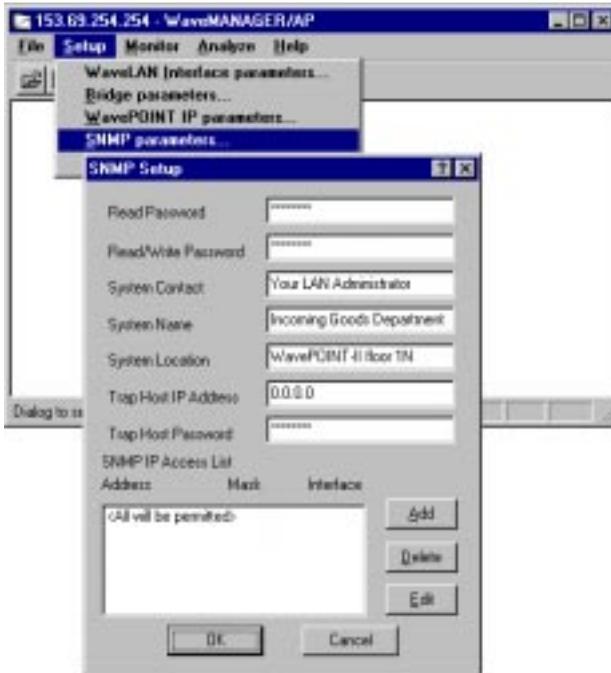
To set the common SNMP parameters, proceed as follows:

1. Select 'SNMP parameters' from the 'Setup' menu. Now the following dialog box is displayed:

## Configuring your Network

### Configuring an Enterprise-wide Network

Figure 3-13 SNMP setup dialog box



2. Change the Read Password in order to protect access to the SNMP parameters. The Read Password is used in the 'Select another device' option from the Monitor and Analyze menus.

With the correct Read Password, a local LAN administrator can only view monitor windows, but not view or modify the SNMP parameters.

3. Change the Read/Write Password in order to protect access to the SNMP parameters. The Read/Write password is used in the 'Open remote configuration' option from File menu.

With the correct Read/Write password, a network supervisor can view and modify the SNMP parameters.

## Configuring your Network

### Configuring an Enterprise-wide Network

---

4. Use the System Contact field to enter a generic name for the network supervisor or department, (e.g. 'Your LAN Administrator' as pictured in Figure 3-13). Alternatively, leave the default value, since you may change it later when you set the values that are unique for each WavePOINT-II unit.
5. Use the System Name field to enter a generic logical location of a WavePOINT-II unit, (e.g. Incoming Goods Department as in Figure 3-13). Alternatively, use the default value, since you can change it later when you set the values that are unique for each WavePOINT-II unit.
6. Use the System Location field to enter a generic physical location of a WavePOINT-II unit, (e.g. WavePOINT-II floor 1N as in Figure 3-13). Alternatively, use the default value, since you may change it later when you set the values that are unique for each WavePOINT-II unit.
7. Use the Trap Host IP Address field to enter the address of the network management station that should collect the SNMP Trap messages. You can use the "trap alert" system to receive a warning message when a WavePOINT-II unit is reset or rebooted. For more detailed information, see "Trap Host Alerts" on page 6-13.
8. Use the Trap Host Password field to enter a password that will be included in the SNMP trap messages. You can use this password at the Trap Host station to filter out Trap messages that may have been sent to the Trap Host station erroneously.
9. Use the SNMP IP Access List to determine which stations are authorized to modify the SNMP setup of the WavePOINT-II units. In many cases this would only be your WaveMANAGER Station.
  - To add lines to the list, you need to enter the IP address of the station that is allowed to modify SNMP settings, and the interface through which the WavePOINT-II unit will be accessed.

## Configuring your Network

### Configuring an Enterprise-wide Network

---

- To indicate the interface, use '0' for Ethernet, '1' for the WaveLAN interface in socket A, '2' for the WaveLAN interface in socket B, or 'x' for any available interface.
  - If you want to assign a range of IP addresses, enter a subnet mask value that indicates the subnet from which all stations are authorized to modify the SNMP setup.
10. Click OK to return to the WaveMANAGER/AP opening window.

### Save the Template File

From the File menu, select 'Save Config File as' to save the settings of the common parameters to a template file on the hard disk of the WaveMANAGER Station.

Use a name that allows you to easily recognize the template file, such as template.cnf.

### Step 3 - Configuring WavePOINT-II

---

In the configuration scenario suggested here, the WavePOINT-II units have not been installed yet. Before they are installed, they will first be configured in a batch-mode approach.

To configure each of the WavePOINT-II units, you need to carry out the following activities:

- Make a wireless or wired connection between a WavePOINT-II unit and WaveMANAGER/AP.
- Open the remote configuration to import the current values of the WavePOINT-II unit.
- Import the values that are common for all WavePOINT-II units from a template file.
- Set the unique parameters for each WavePOINT-II unit.
- Save the values to an individual configuration file on disk.
- Upload the values to the WavePOINT-II unit.

#### Connecting to the WavePOINT-II

The easiest and most flexible setup to configure the WavePOINT-II units is to use a wireless WaveMANAGER/AP station that provides direct access to the WavePOINT-II units. In this case, there is only one point-to-point connection and there are no complications caused by IP addressing requirements.

Alternatively, you can use a WaveMANAGER/AP station that is connected directly to the WavePOINT-II unit (i.e. no router between the WaveMANAGER/AP station and the WavePOINT-II unit). The direct connection is required because a WavePOINT-II unit with a default, factory-set IP address may cause problems in the address recognition of a router.

To make a wired connection between a WaveMANAGER Station and a WavePOINT-II unit, you can use either a 10Base-T cable with RJ45 connectors or a 10Base2 cable with BNC connectors.

- If you use 10Base-T cabling, you will need a hub or cross-cable to make the proper connection.
- If you use 10Base2 cabling, you will need to place a terminator on the unused side of the T-connectors attached to the WavePOINT-II unit and the WaveMANAGER Station.

## Configuring your Network

### Configuring an Enterprise-wide Network

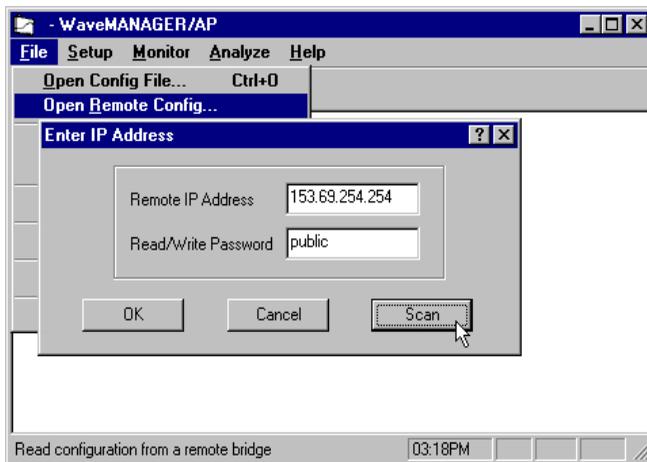
---

To connect to the WavePOINT-II unit and import the WavePOINT-II unit's current values into WaveMANAGER/AP, proceed as follows:

1. Start WaveMANAGER/AP by clicking its icon in the WaveLAN program folder.
2. Select 'Open Remote Configuration' from the 'File' menu.
3. Click the 'Scan' button to display the WavePOINT-II unit to be configured.

---

**Figure 3-14** Scan IP address dialog box



4. Select the name of the WavePOINT-II unit that you want to configure. If you select a WavePOINT-II unit with a default IP address, you need to change the default value. To do so, click the 'Change IP' button, change the IP address and click OK to return to the 'Scan' window.
5. Click OK twice to return to the opening window of the WaveMANAGER/AP program.

#### Import the Template File

To import the common parameters from a template file, select 'Import Config file' from the 'File' menu and select the template configuration file (e.g. template.cnf).



**NOTE:**

The IP address which you entered in the 'Open Remote Configuration' dialog box will be changed into the IP address which was set in the common parameters. When you set the unique parameters for the WavePOINT-II units, you need to change the IP address again into its unique value for each WavePOINT-II unit.

#### Setting the Unique Identifiers

After you have imported the common parameters from a template file, the parameters that are unique to each WavePOINT-II unit need to be set.

---

**Table 3-1**      **Where to set WaveLAN Parameter Settings**

Parameter	WaveMANAGER/AP 'Setup' Menu Option
NWID	WaveLAN Interface parameters...
Roaming Enabled/Disabled	WaveLAN Interface parameters...
IP Address	WavePOINT IP parameters...
Read/Write Password	SNMP parameters...
System Name and Location	SNMP parameters...

## Configuring your Network

### Configuring an Enterprise-wide Network

---

#### Create a Back-up File of the Configuration

To save the values to an individual configuration file on a local disk, select 'Save Config File as' from the 'File' menu. Use a name that allows you to easily recognize the relationship between the file name and the target WavePOINT-II unit.

#### Upload the Configuration

To upload the configuration data to the WavePOINT-II unit, select 'Save Config' from the 'File' menu.

The entire set of common and unique parameters are now saved permanently into the (non-volatile) Flash ROM of the WavePOINT-II unit. They will remain stored in the WavePOINT-II unit, even if the unit is reset or switched off and on again.

#### Complete the Paperwork

Now that you have completed the configuration of a WavePOINT-II unit, proceed as follows:

1. Record the intended location of the WavePOINT-II unit on a label and attach the label to the WavePOINT-II unit.
2. Record the name of the file with the WavePOINT-II unit's configuration data and the location where you will install the WavePOINT-II unit on the "WavePOINT-II Configuration Record".
3. To set the common and unique parameters for the other WavePOINT-II devices, start from "Connecting to the WavePOINT-II" on page 3-25.
4. Save the configuration record form, together with the disk containing the configuration back-up file, in a safe place.

## **Configuring your Network**

### **Configuring an Enterprise-wide Network**

---

#### **Step 4 - Mounting the WavePOINT-II Units**

---

When finished configuring all WavePOINT-II units, you are ready to install the units in their physical locations within your network.

If you completed the WavePOINT-II Configuration Record according to the instructions in the previous sections, you will have a detailed list of intended locations for each WavePOINT-II unit.

Refer to the 'WavePOINT-II Getting Started' manual for mounting instructions for your WavePOINT-II access points.

## **Modifying the Configuration**

---

You can modify the WavePOINT-II configuration parameters any time you wish, using the 'Open Remote Config...' option from the file menu.

Keep in mind that you will need to address the unit using its new IP address and the new Read/Write password (if you changed the Read/Write password) to open the configuration file. If your WaveMANAGER station is a wireless station, you may need to modify the station's WaveLAN Interface Parameters to match the values as that were stored in the WavePOINT-II unit.

Alternatively, if you have forgotten the Read/Write password, or any other setting required to access the unit, you may need to perform a 'Forced Reload', as described on page B-3 in Chapter B "Performing a Forced Reload".



**NOTE:**

When you make changes to the configuration of a particular WavePOINT-II device, you should update the WavePOINT-II Configuration Record to reflect these changes.

## **Changing Common Parameters**

---

If at any stage changes need to be made to the common parameters for all WavePOINT-II units, the most efficient way to do so is as follows:

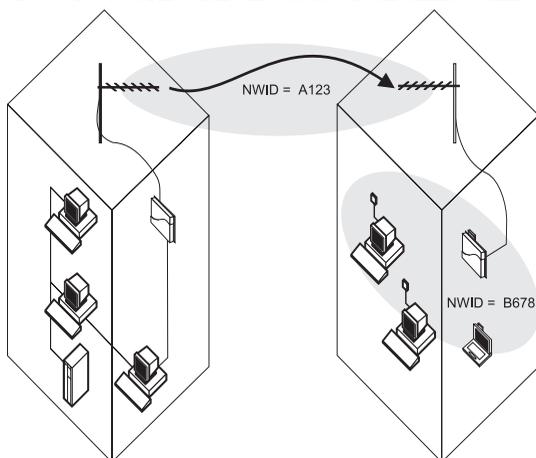
1. Change the required parameters for one particular WavePOINT-II unit.
2. Save the changes to a new template file.
3. Upload the template file to all WavePOINT-II units.
4. Set the unique parameters for your WavePOINT-II units. See "Connecting to the WavePOINT-II" on page 3-25.

## **Configuring Outdoor Antenna Links**

---

Where regulations permit wireless outdoor communication, you can use WaveLAN to connect multiple LAN segments located in different buildings.

**Figure 3-15 Network with an outdoor antenna connection**



To connect to a building within a line-of-sight distance of up to 100 meters, you can use standard omni-directional antennas.

To bridge distances of up to 2 kilometers, you can use the WavePOINT-II units in combination with a special outdoor antenna.

To create a wireless point-to-point bridge between two buildings as shown in Figure 3-15, you will need two WavePOINT-II units, i.e. one WavePOINT-II unit in each building.

To create a wireless bridge between three buildings, two situations are possible:

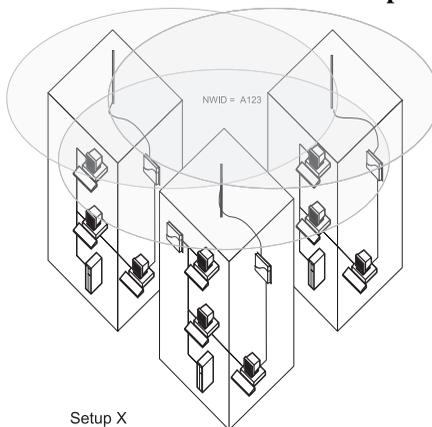
- Setup X (Figure 3-16), buildings A, B and C have an omni-directional (point-to-multipoint) connection. Building A can therefore transmit directly to building B and C; building B directly to A and C, and so on.
- Setup Y (Figure 3-17 on page 3-33), buildings A and C have a point-to-point connection with building B. All transmissions therefore go via building B.

To configure each of these bridges, you need to set the following parameters:

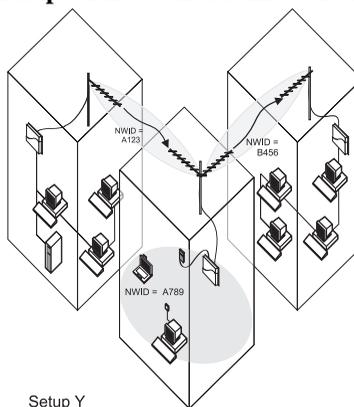
- NWID (required)
- disable roaming (recommended)
- network protocol filters (optional)
- Static MAC address list (optional)

---

**Figure 3-16 Omni-directional Point-to-Multipoint**



**Figure 3-17 Multiple Directional Point-to-Point**



### Point-to-Point Link Configuration

---

To configure a point-to-point bridge using two WavePOINT-II units, the WaveLAN interface of the WavePOINT-II units on both sides of the bridge must have the same network ID.

You can also optimize the data traffic by filtering out particular network protocols. Furthermore, the Static MAC address list of each of the bridge WavePOINT-II units can be used to enter the MAC addresses of stations which are not to receive any traffic from the WavePOINT-II unit (see "Protocol Filtering" on page 5-3).

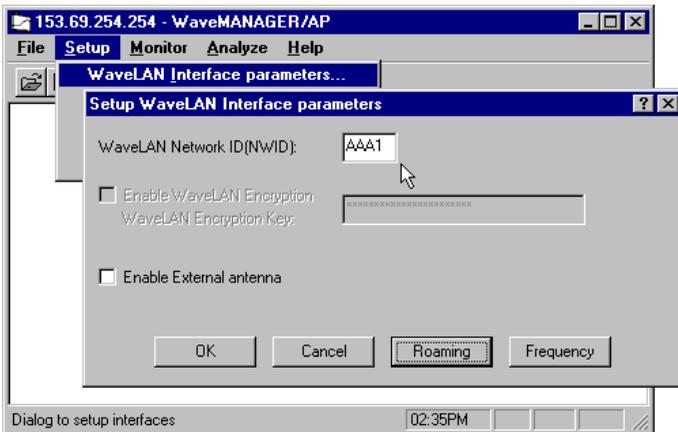
## Setting the Required Parameters

### NWID, External Antenna and Roaming Parameters

To set the NWID, External antenna and Roaming parameters, proceed as follows:

1. Select 'WaveLAN Interface Parameters...' from the 'Setup' menu.
2. Select the interface which is to be used for the point-to-point bridge. The following dialog box will be displayed:

**Figure 3-18 Setup WaveLAN Interface Parameters**



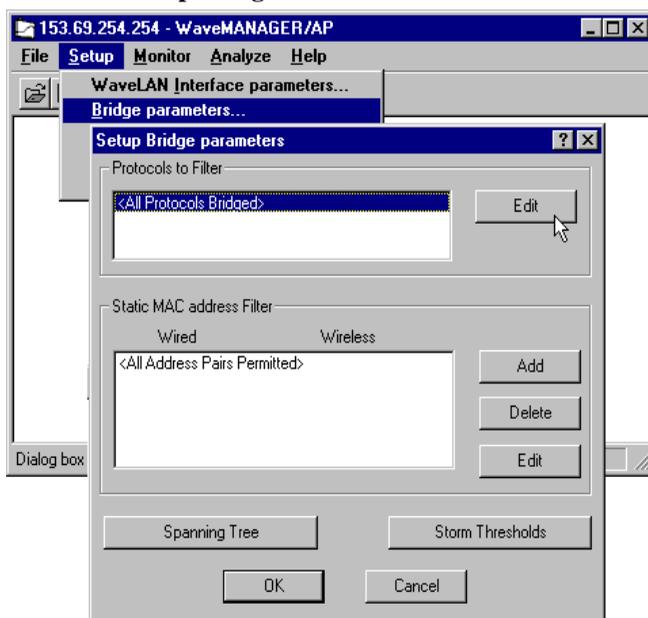
3. Enter the NWID for the socket.
4. Click the 'Enable External Antenna' field to enable the external antenna connector of the EAM and enable diversity. This will not harm a non-diversity antenna.
5. Click the Roaming button and then clear the Enable Roaming checkbox to disable roaming and optimize data traffic.

### Protocol Filters

To set the network protocol filters:

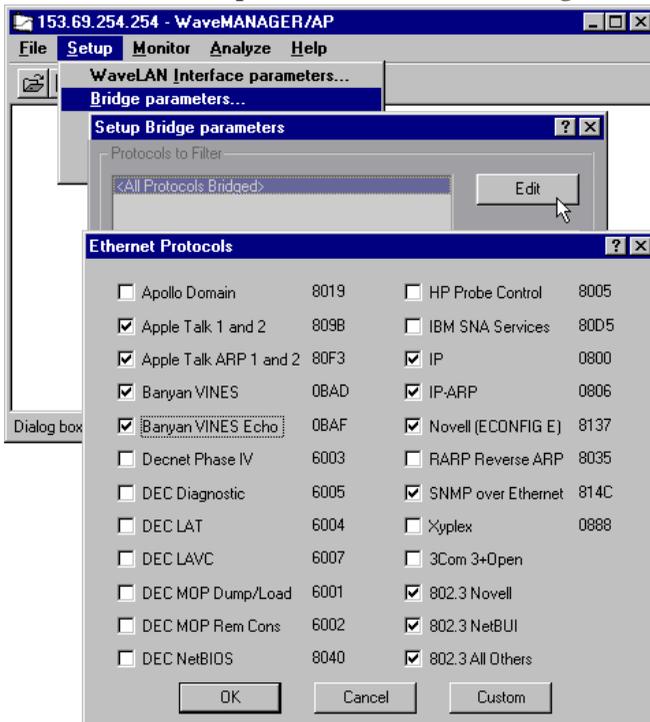
1. Determine the minimum set of protocols that must be bridged.
2. To filter all other protocols, select 'Bridge parameters' from the 'Setup' menu to display the 'Setup Bridge Parameters' window. The top section of this dialog box shows the 'Protocols to Filter' field which initially contains only one line: All Protocols Bridged. For more information, see "Protocol Filtering" on page 5-3.

**Figure 3-19 Setup Bridge Parameters**



3. Press the Edit button to display the following window with Ethernet Protocols.

**Figure 3-20 Ethernet protocol filter selection dialog box**



4. Click the check boxes (see Figure 3-20) in front of the protocols that you would like to filter. Each protocol marked with a check mark will be listed in the 'Protocols to Filter' field of the Bridge Parameters window.

To cancel the filtering of a specific protocol, clear the check box.

To add a non-listed protocol to the list, click the 'Custom' button.

### Static MAC Address List

When you are using WaveLAN as a wireless outdoor link, the WavePOINT-II interface connected to the outdoor antenna will typically communicate to a single or limited set of stations. You can use the Static MAC address list to deny traffic between two specific stations over the WavePOINT-II interface. Besides limiting the traffic over the WavePOINT-II unit, you will also increase the efficiency of the bridge.

To set the Static MAC address list on your WavePOINT-II unit:

1. Select 'Bridge Parameters...' from the 'Setup' menu
2. In the 'Static MAC address Filter' field, click the 'Add' button
3. Enter the MAC addresses of the two stations that will be denied network traffic privileges on the WavePOINT-II unit. Make sure that you enter the correct MAC addresses into the appropriate fields (either wired or wireless as viewed from the WavePOINT-II unit you are configuring).
4. Click OK to return to the 'Setup Bridge Parameters' window.

If you are looking to restrict access to your wireless network, rather than simply deny access between specific stations on the network, see "Access Control" on page 6-6.

### Multiple Point-to-Point Link Configuration

---

Bridges between more than two buildings can be accomplished by using either a point-to-multipoint bridge or several point-to-point bridges.

- If the buildings are linked by means of a point-to-multipoint bridge, each building can transmit directly to each of the other buildings (see Setup X in Figure 3-16 on page 3-32).
- In a series of point-to-point bridges, all transmissions go via one building (see Setup Y in Figure 3-17 on page 3-33).

To configure a point-to-multipoint bridge (see setup X in Figure 3-16 on page 3-32), follow the same instructions as given on page 3-33 for a point-to-point bridge between two buildings, while observing the following guidelines:

- all WavePOINT-II wireless interfaces in a Point-to-Multipoint link (Figure 3-16 on page 3-32) must share the same NWID;
- roaming must be disabled in each of the WavePOINT-II units;
- each WavePOINT-II involved in the link must use the same settings for protocol filtering;
- when using Static MAC address filtering, all WavePOINT-II units involved must contain the addresses of all other WavePOINT-II units that participate in the wireless link.

To configure a series of point-to-point bridges (see setup Y in Figure 3-17 on page 3-33), follow the same instructions as given on page 3-33 for a point-to-point bridge between two buildings, while observing the following guidelines:

- each wireless link should be identified by a unique NWID. WavePOINT-II units on both ends of a specific link must share the same NWID;
- roaming must be disabled in each of the WavePOINT-II units;
- each bridge WavePOINT must filter the same network protocols;
- the Static MAC address list in each WavePOINT-II unit must contain the addresses of all stations to be filtered.
- if possible, set different links on two, non-overlapping channels to increase performance.

---

# Monitoring your WaveLAN Network

# 4

---

<b>Introduction</b>	<b>4-1</b>
WaveMANAGER Utilities	4-1
. WaveMANAGER/CLIENT	4-2
. WaveMANAGER/AP	4-2
. Which utility should you use?	4-3
<hr/>	
<b>WaveMANAGER/CLIENT</b>	<b>4-4</b>
Monitoring Methods	4-4
. Link Test Options	4-4
. Site Monitor Options	4-5
. Logging Measurement Data Options	4-5
Running WaveMANAGER/CLIENT	4-6
. Main Window	4-6
Link Test	4-8
. Analyzing Link Quality	4-9
. Resetting the diagnostic counters	4-10
. Selecting another Link Test Partner	4-11

---

Site Monitor	4-12
. Starting Site Monitor	4-13
. Selecting another Domain ID	4-15
. Resetting the diagnostic counters	4-16
. Sorting the list of WavePOINT units	4-16
Logging Measurement Data	4-17
. Manual Logging	4-17
. Automatic Logging	4-18
. Setting the Logging Options	4-18
. Starting/Stopping the Logging Function	4-19
Frequency	4-19
Access Control	4-20

---

**WaveMANAGER/AP** **4-21**

Monitoring Methods	4-21
. Remote Statistics	4-21
. Remote Link Test	4-22
Running WaveMANAGER/AP	4-22
. Using Remote Statistics	4-22
. Important indicators to monitor	4-24
. Adjusting Remote Statistics Time Interval	4-28
. Using Remote Link Test	4-28

---

# Monitoring your WaveLAN Network

# 4

---

## Introduction

---

Once your network has been configured and installed, you can use WaveMANAGER utilities to:

- Monitor the performance of your network;
- Verify optimal placement of your WavePOINT-II access points and wireless stations.

You are advised to verify the performance of your network on a regular basis, as performance may change when wireless computing devices are relocated, or office environments add or rearrange cube walls, or when new equipment is installed that might interfere with WaveLAN wireless communication.

## WaveMANAGER Utilities

---

The WaveMANAGER Software Suite offers two utilities that enable you to monitor your WaveLAN network:

- WaveMANAGER/CLIENT
- WaveMANAGER/AP

### WaveMANAGER/CLIENT

WaveMANAGER/CLIENT has been designed to monitor the radio performance of your network on-site.

- You can use WaveMANAGER/CLIENT to run dynamic Radio Communication Diagnostics with all WavePOINT-II units within range of your monitoring station.
- Alternatively you can display detailed Link Test measurements with a single WaveLAN station or WavePOINT-II unit.

WaveMANAGER/CLIENT is a 'mobile' wireless utility that can only run on a WaveLAN equipped station, typically a portable device such as a notebook computer.

### WaveMANAGER/AP

WaveMANAGER/AP has been designed to monitor your network from a central location, e.g. the LAN Administrators office.

- You can use this utility to display measurements for areas in remote networks.
- Alternatively you can use this utility to display measurements for areas in your network that can not easily be reached, (e.g. building-to-building links, where antennas are placed on rooftops).

WaveMANAGER/AP allows you to display Link Test measurements between a (remote) WavePOINT-II unit of your choice and a WaveLAN device connected to the selected WavePOINT-II unit.

The WaveMANAGER/AP utility can run on both wired stations (Ethernet) and wireless (WaveLAN) stations. To run diagnostic measurements the WaveMANAGER/AP station must be

connected to the network. Furthermore, the WaveMANAGER/AP station must be connected to a network infrastructure that allows the WaveMANAGER/AP station to access the WavePOINT-II unit using the TCP/IP protocol.

### **Which utility should you use?**

The decision whether to use WaveMANAGER/CLIENT or WaveMANAGER/AP largely depends on your capabilities or desire to perform diagnostic measurements on-site, or from one central location.

Both WaveMANAGER/CLIENT and WaveMANAGER/AP offer logging functions that can save all measurement data for later evaluation or comparison with previous measurements.

You can view saved logfiles with any ASCII editor, or import the data into standard spreadsheet or database applications. The logfiles are saved in Comma Separated Value (CSV) file format.

## WaveMANAGER/CLIENT

---

### Monitoring Methods

---

WaveMANAGER/CLIENT offers three monitoring methods:

- Link Test (page 4-8)
- Site Monitor (page 4-12)
- Logging Measurement Data (page 4-17)



**NOTE:**

For on-line help, press the F1 Function Key on your keyboard or click the 'Help' button on the WaveMANAGER window.

### Link Test Options

You can use the Link Test option to investigate a specific link between two wireless stations. In Link Test mode, the Link Test partners exchange data packets to determine the link quality.

You can use the measurement results to analyze the radio frequency path between the two partners in more detail.

Link Test monitors a specific link between two stations and can therefore be used to analyze the Link Test quality of the communications path with the Link Test Partner.

### Site Monitor Options

The Site Monitor option enables you to display the communications quality of multiple WavePOINT-II units simultaneously. You can use the Site Monitor to:

- Determine the overall wireless coverage of your WaveLAN network.
- Determine or optimize the placement of your WavePOINT access points, in order to provide seamless connectivity to mobile stations.

In Site Monitor mode, the WaveMANAGER/CLIENT station will listen for beacons transmitted by all WavePOINT access points to determine the communications quality for each WavePOINT.

Roaming throughout the wireless network environment with your WaveMANAGER/CLIENT station, you will be able to identify areas that may not have adequate coverage, or that suffer from in-band interference by other (wireless) equipment such as security gates, microwave ovens or photo copiers.

This will help you to verify and optimize the placement of your WavePOINT-II units.



**NOTE:**

Every location where wireless stations will be used must be covered by at least one WavePOINT that provides a communications quality that is acceptable or better.

### Logging Measurement Data Options

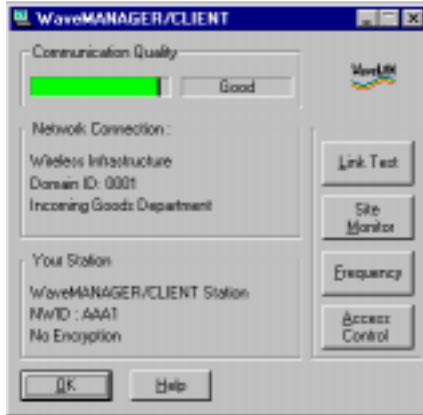
Both Site Monitor and Link Test enable you to log measurement results. The measurement data can be logged manually or at regular intervals automatically.

## **Running WaveMANAGER/CLIENT**

---

To start WaveMANAGER/CLIENT, click its icon in the WaveLAN software folder. This will display the following window:

**Figure 4-1 WaveMANAGER/CLIENT Main Window**



### **Main Window**

The opening window of WaveMANAGER/CLIENT will provide you information about your station, the network station you are connected to (if connected) and a visual indication of the quality of the connection.

The Communications Quality indicator displays the quality of the link between your WaveMANAGER/CLIENT station (Your Station) and the nearest WavePOINT-II unit (Network Connection), if one is available.

## Monitoring your WaveLAN Network

### WaveMANAGER/CLIENT

---

The Communications Quality is displayed as one of the following colors:

<b>Color</b>	<b>Description</b>
Green	Communication Quality is good, no intervention is required.
Yellow	Communication Quality is acceptable, no intervention is required.
Red	Communication Quality is poor, intervention is required (see Appendix A “Troubleshooting”)
Blank	No connection

If the Communications Quality indicator is fully red and displays ‘No connection’, no access point found’, your WaveMANAGER Station has been configured for operation in a wireless infrastructure, such as the Basic Access Network described in Chapter 2.

If your WaveMANAGER/CLIENT Station is not able to find a WavePOINT-II (network Connection), it may be:

- out of range of the WavePOINT units or,
- the Domain ID value does not match the value of the network (see “Selecting another Domain ID” on page 4-15)

If you are still having problems connecting to the network, please refer to Appendix A “Troubleshooting” for possible solutions.

When the communications quality indicator is blank and displays ‘Not available’, your WaveMANAGER Station is configured for operation in an ad-hoc wireless workgroup; i.e. roaming is disabled. See “Selecting another Link Test Partner” on page 4-11 for more detailed information.

## **Link Test**

---

You can use the Link Test to monitor one specific link between:

- two stations in a point-to-point link
- two WaveLAN computers in an ‘ad-hoc wireless workgroup’
- A WaveLAN computer and a WavePOINT-II unit.

The communications quality of the link is expressed in terms of a general quality indication, the SNR value of the link and the number of packets received and lost. Each of the values shown is the result of several measurements over a specific interval.

The Link Test can be performed from stations with either a WaveLAN/PCMCIA card or an ISA card. This station could be a WaveMANAGER Station or an ordinary workstation.

In Link Test mode, your WaveMANAGER Station will stick to the Link Test partner, i.e., roaming between WavePOINTS will be disabled for the run-time session of the Link Test.

To display the Link Test window (Figure 4-2), click the ‘Link Test’ button in the opening window of WaveMANAGER/CLIENT.

---

**Figure 4-2 Link Test Window**



The Link Quality indicator shown in the top section of the window (in Figure 4-2) gives a first impression of the communications quality of the current link, which is the link between the local and the remote stations shown below the link quality indicator.

The link quality is displayed as one of the following colors:

<b>Color</b>	<b>Description</b>
Green	Communication Quality is good, no intervention is required.
Yellow	Communication Quality is acceptable, no intervention is required.
Red	Communication Quality is poor, intervention is required (see Appendix A "Troubleshooting")
Blank	No connection

The 'Advice' button will provide more information about the Link Quality qualification and, if applicable, provide suggestions to improve the Link Quality.

### Analyzing Link Quality

When you want to investigate the Link Quality in more detail, the fields in the middle of the window show the communications quality in terms of the SNR value of the link. The bottom field shows the percentage of packets received compared to the number of packets sent.

To investigate Link Quality results in more detail, you can use one of the following options:

- Freeze the display by clicking the 'Freeze' button
- Display details by clicking the 'Details' button

For example, when the Signal to Noise (SNR) indicator displays a value that is less than expected, the Details view will show whether this is due to a low signal level (stations are too far apart) or a high noise level (a source of interference that is located in the communications path between the two Link Test partners).

You can use the Local/Remote indicators to identify whether the cause of reduced performance is in the area of the Link Test partner (Remote) or in the vicinity of the WaveMANAGER Station (Local).

Signal Quality is a measure of the clarity of the signal. This indicator needs special attention only when performing Link Tests to diagnose the impact of signal reflections caused by high ceilings or reflecting surfaces such as steel structural components.

### **Resetting the diagnostic counters**

You may wish to reset the diagnostic counters in order to restart the Link Test measurements.

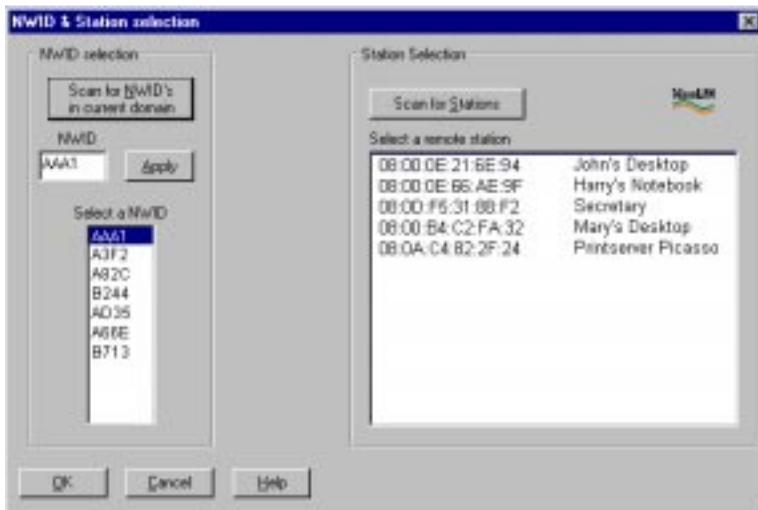
A situation in which this may be useful is when you would like to validate and remedy a case of poor performance.

For example, you switch off a photocopier, which you assumed to be the source of the interference. Clicking the 'Reset' button after you remove the suspected source of interference will analyze the Link Quality, ignoring previous results that were possibly influenced by the source of interference.

### Selecting another Link Test Partner

To investigate the link with another station or access point, click the 'Other' button from the 'Link Test' window. This will display the following window in Figure 4-3:

**Figure 4-3** NWID & Station selection dialog box



- To select another Link Test partner, select a station from the remote station list in the right half of the window.
- To scan for other stations within the same wireless cell, click the 'Scan for Stations' button. This will display all stations within range of your WaveMANAGER Station that use the same NWID, as shown in the NWID field in the left half of the window. Click OK to start the Link Test within the selected station.

## Monitoring your WaveLAN Network

### WaveMANAGER/CLIENT

---

To set up a Link Test with a station in another wireless cell:

1. From the 'NWID & Station selection' window, enter the NWID of the wireless cell in which you intend to run a Link Test.
2. Click the 'Apply' button.
3. Click the 'Scan for Stations' button. Your screen will display all stations within range of your WaveMANAGER Station, that use the new NWID value.
4. Select a remote station.
5. Click OK to start the Link Test with the selected station.

If you do not know the NWID's of the wireless cells in your network:

1. Click the 'Scan for NWIDs in current domain' button. When you scan for NWID's, your screen will only display those wireless cells that are within range of your station.
2. Select a NWID from the displayed list.
3. Click the 'Apply' button.

### Site Monitor

---

You can use the Site Monitor to display the quality of communications with multiple WavePOINT units simultaneously. It shows which WavePOINT units are available, and of the available WavePOINT units, it shows the communications quality.

The Site Monitor option is available only to WaveMANAGER/CLIENT Stations equipped with a WaveLAN PCMCIA card. To use the Site Monitor, the WaveMANAGER/CLIENT Station must have the roaming options enabled.



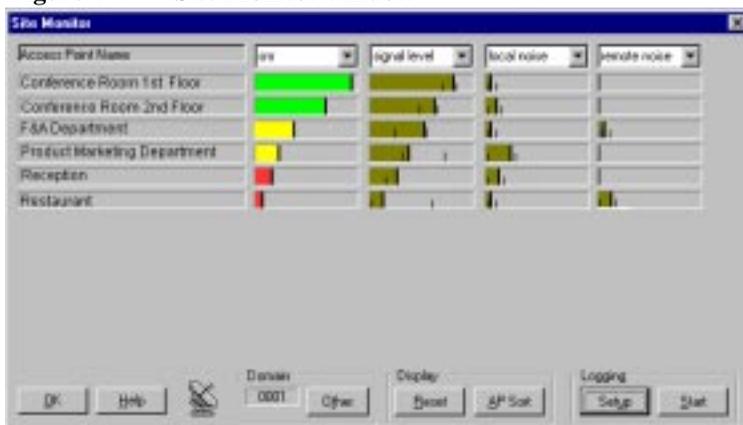
**NOTE:**

Site Monitor is recommended for monitoring the communications quality between WavePOINT units within a building. To monitor the communications quality between outdoor building-to-building links, you should use the Remote Link Test available in WaveMANAGER/AP program.

### Starting Site Monitor

To start the Site Monitor, click the 'Site Monitor' button in the main window of WaveMANAGER/CLIENT. This will display the following window:

**Figure 4-4 Site Monitor window**



Each row displays the communications quality with the WavePOINT units identified in the first column. When this column does not display all WavePOINTS, some of the units may be out of range of your WaveMANAGER Station.

You can use the pull-down menus of the other columns to display a variety of diagnostic tallies in the format and arrangement that you prefer. The recommended set of tallies for most monitoring tests is as follows:

- SNR (Signal to Noise Ratio)
- Signal level
- Local Noise level
- Remote Noise level

## Monitoring your WaveLAN Network

### WaveMANAGER/CLIENT

---

The Signal to Noise (SNR) ratio is calculated as the sum of Signal Level minus Noise Level, where Noise Level represents the highest value of either Local or Remote Noise at the time of measurement.

You will need the Signal Quality indicator only in exceptional circumstances, for example when you are performing a site survey in environments with high ceilings or with reflecting surfaces, such as steel structural components, cause excessive signal reflections.

The colors used to express the various parameters are the same as those used on WaveMANAGER/CLIENT's opening window (see page 4-7 for color/parameter table).

When walking through your wireless LAN environment, each location should be covered by at least one WavePOINT that provides an SNR that is acceptable or better.

If the Signal to Noise Ratio is of poor quality, use the information in the other columns to obtain additional information. If this does not sufficiently clarify the reasons for the poor quality, please refer to Appendix A "Troubleshooting".

Use the buttons along the bottom of the window to change the list of information displayed for the WavePOINT units, or to log the measurement data.

- **Domain**
  - **Other** - select another Domain ID or other WavePOINT units
- **Display**
  - **Reset** - to reset the diagnostic counters
  - **AP Sort** - to sort the list of WavePOINT units
- **Logging**
  - **Setup** - to set parameters for the logging function
  - **Once** or **Start/Stop** - to start or stop logging

### Selecting another Domain ID

If the Site Monitor did not list the WavePOINT units you expected, you may need to select another Domain ID. This may happen in situations where your WaveMANAGER/CLIENT station has been configured with a Domain ID which is different from the Domain ID used by the network under investigation.

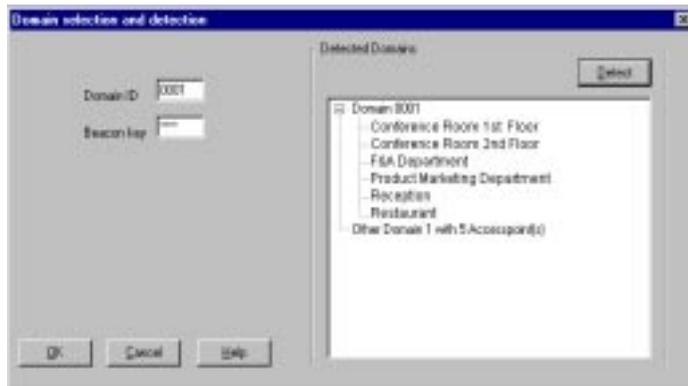
The 'Select another Domain ID' option enables you to:

- temporarily change the Domain ID used by your WaveMANAGER/CLIENT station, or
- scan for the presence of other wireless domains in the vicinity.

To do so, click the 'Other' button in the domain section at the bottom of the window. This will display the following dialog box:

---

**Figure 4-5 Domain Selection Window**



To change the Domain ID of your WaveMANAGER/CLIENT station, enter a new Domain ID in the 'Domain ID' field. In addition to the Domain ID, you may need to enter a correct beacon key value in order to decode the network IDs of the WavePOINT units shown. Click OK to confirm the new Domain ID.

## Monitoring your WaveLAN Network

### WaveMANAGER/CLIENT

---

The new Domain ID value will be valid only for the run-time session of the WaveMANAGER/CLIENT program. When you exit the program, your wireless station will revert to its usual Domain ID value, as identified for the WaveLAN adapter in the “Network Neighborhood” properties of your station.

To scan for the presence of other wireless domains, click the ‘Detect’ button. If there are other wireless domains in the vicinity of your WaveLAN network, the ‘Detect’ option will show all other Domains with the number of access points that belong to it.



#### **NOTE:**

You cannot retrieve the Domain ID or NWIDs of the neighboring WaveLAN networks.

### Resetting the diagnostic counters

You may wish to reset the diagnostic counters in order to return all values of the parameters to their initial values and to restart all measurements. To do so, click the ‘Reset’ button in the ‘Display’ field of the Site Monitor window. A reset will also clear the WavePOINTS that are no longer within range.

### Sorting the list of WavePOINT units

The list of WavePOINT units is sorted in descending order of the SNR values as they were registered when you opened the Site Monitor screen.

When you have moved along through the area covered by the network, you may wish to sort the list of WavePOINT units in order to show the WavePOINT units with the best communications quality at the top of the list.

## Monitoring your WaveLAN Network

### WaveMANAGER/CLIENT

---

To sort the list of access points again in its new order of SNR values, click the 'AP Sort' button.



#### **NOTE:**

When using the logging option, note that sorting the list of access points may affect the listings in your logfiles as well.

### Logging Measurement Data

---

Both Site Monitor and Link Test enable you to log measurement results. The measurement data can be logged manually or at regular intervals automatically.

WaveMANAGER/CLIENT saves the data to Comma Separated Value (CSV) logfiles that can be imported into standard spreadsheet or database applications for further analysis.

Comparison of measurement data with previous measurements may help you investigate the performance of your wireless LAN over a period of time, for example to analyze the consequences of relocated network equipment. To perform the comparison, use the functionality of your spreadsheet or database applications into which you import the data from the logfiles.

### Manual Logging

The manual logging function allows you to log the measurement data at specific locations and moments, e.g., when you are running Site Monitor to perform a site survey or when you are investigating a particular source of interference.

When you choose the manual mode, you may wish to enable the 'Add extra info' option to allow you to add comments to your logging information, e.g. a description of the location or event. If you enable this option, a dialog box will appear each time you press the 'Log Once' button.

The Manual Logging option is typically used on WaveMANAGER/CLIENT stations that roaming the network running Site Monitor.

## Automatic Logging

The automatic logging function allows you to log the network performance over a longer period of time. This may be useful if you wish to monitor recurring events or variation in values.

When you choose the automatic mode, you need to set the measurement interval to the required number of seconds.

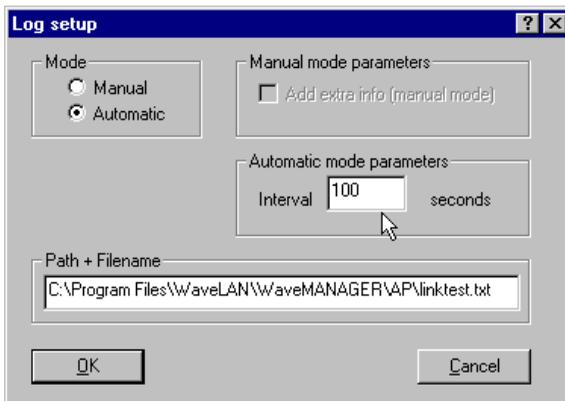
Automatic logging is typically used when the WaveMANAGER/CLIENT station is running a Link Test at a particular location.

## Setting the Logging Options

To set the logging options, click the 'Setup' button in the 'Logging' field. This will display the following window.

---

**Figure 4-6 Log setup dialog box**



In both modes, the measurement data is saved in the file entered in the 'Path and filename' field. Each time new data is saved, this information is appended to the existing file. If you wish to save the data in a new file, use this field to enter a new filename.

## **Starting/Stopping the Logging Function**

Depending on your choice of logging option, the button to the right of the 'Setup' button on the diagnostics window will be labeled 'Once' (manual option) or 'Start' (automatic option).

- For manual logging, click the 'Once' button each time you wish to log data. WaveMANAGER/CLIENT will record a 'snapshot' of the data in the log file.
- For automatic logging, click the 'Start' button. Click this button again to stop the logging function.

To change the logging option, proceed as described in "Setting the Logging Options" on page 4-18.

## **Frequency**

---

To communicate, all WaveLAN stations and WavePOINT access points in the wireless network environment must use the same operating frequency. You can change the operating frequency of your WaveLAN product by clicking on the 'Frequency' button on the main WaveMANAGER/CLIENT window.

WaveLAN 2.4 GHz products support multiple sub-channels in the 2.4 GHz band. Multiple channels can be configured to:

- avoid interference that may be affecting specific sub-channels.
- optimize performance, by allowing two, non-overlapping channels within the same frequency.

The WaveLAN 915 MHz cards have a fixed frequency that can not be modified.



**NOTE:**

Operating frequencies are subject to local radio regulations. Please consult local authorities before operating any product that uses radio frequencies.

#### Access Control

---

You can restrict wireless access to the WavePOINT-II units by means of the Access Control Table. When Access Control is enabled, your WavePOINT-II access points will ignore all requests to forward data to/from WaveLAN devices that are not identified in the Access Control Table.

For more information on Access Control, see “Enabling Access Control” on page 6-6.

## **WaveMANAGER/AP**

---

### **Monitoring Methods**

---

You can use WaveMANAGER/AP to perform remote tests of the communications quality of a WavePOINT unit. WaveMANAGER/AP offers a set of diagnostic options of which the following two are the most important for most users:

- Remote Statistics, and
- Remote Link Test

All other diagnostic options are standard SNMP tallies that are not described in this manual.



**NOTE:**

Each diagnostic option is also described in the on-line help information that you can access by pressing the F1 Function Key or clicking the 'Help' button in your WaveMANAGER/AP window.

### **Remote Statistics**

The Remote Statistics option allows you to monitor a set of SNMP variables for each of the WavePOINT interfaces (both Ethernet and WaveLAN).

Remote Statistics can be viewed for both WavePOINT-II and previous generation WavePOINT access points.

## Remote Link Test

The Remote Link Test option allows you to analyze the communications path between a remote WavePOINT-II unit and a station connected to the selected WavePOINT-II unit.

The user-interface of the WaveMANAGER/AP Remote Link Test is very similar to the Link Test offered by WaveMANAGER/CLIENT. The Remote Link Test feature is not supported for previous generation WavePOINT access points.

## Running WaveMANAGER/AP

---

### Using Remote Statistics

To display the Remote Statistics for a WavePOINT-II unit, you must first connect to the target WavePOINT-II unit.

1. From the 'Monitor' menu, click the 'Select another device' option.
2. Enter the IP address and the 'Read' password of the WavePOINT-II unit which you want to monitor. Alternatively you can click the 'Scan' button to display the WavePOINT-II units available in your subnet.



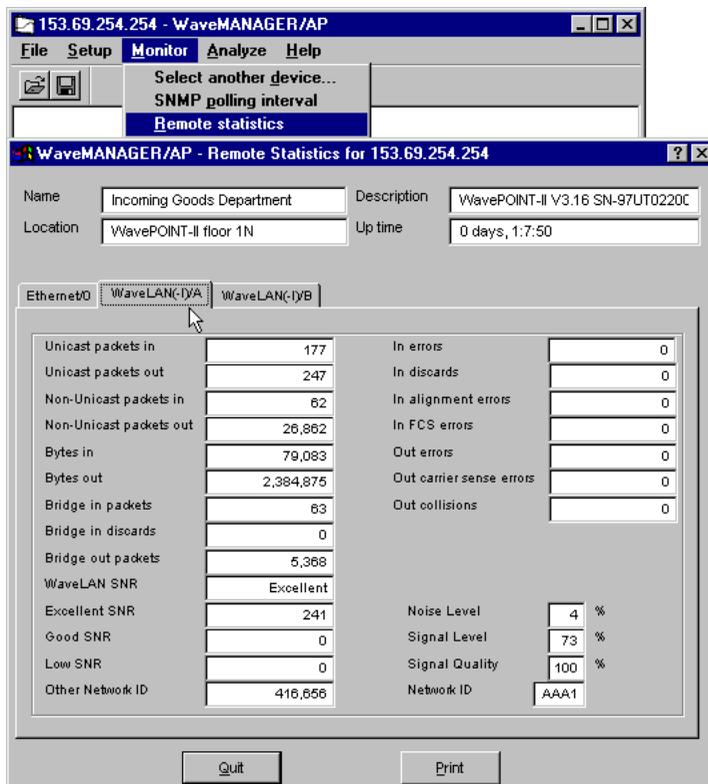
**NOTE:**

The 'Scan' button will only display WavePOINT-II units in the same subnet as the management station. To investigate a link outside of the subnet, enter the IP address and the 'Read' password in the initial dialog box.

When the addressed WavePOINT-II unit has been found, the WaveMANAGER/AP program will acknowledge the connection by stating 'Device Located'.

To start the remote statistics monitor, select 'Remote Statistics' from the 'Monitor' menu. This will display the following window:

**Figure 4-7 Remote Statistics Window**



The performance for each of the interfaces of the selected WavePOINT unit is displayed on separate tab sheets. Use the corresponding 'tabs' just below the top section of the window to select the interface of your choice.

If you prefer to read the remote statistics information from paper, click the 'Print' button to print the remote statistics window.

### Important indicators to monitor

The WaveMANAGER/AP Remote Statistics display a wide range of variables that provide information about the performance of the selected WavePOINT-II unit.

The indicators which provide the main monitoring information are:

- Up Time
- The ratio of 'Errors' to 'Bridge Packets'

### Up Time

The first performance indicator of your WavePOINT-II unit is the 'Up Time' field which is displayed in the top section of the Remote Statistics window. The 'Up Time' field displays the time interval measured from the last time the WavePOINT-II unit was reset. If the up time is lower than expected, the WavePOINT-II unit may have been reset or reloaded.

### Ratio of 'Errors' to 'Bridge Packets'

The following ratios are of particular diagnostic value:

- 'In errors' / 'Bridge packets in';
- 'Out errors' / 'Bridge packets out';
- 'Out collisions' / 'Bridge packets out'

The following table provides diagnostic information relating to each of the three ratios.

**Table 4-1 Ratio of Errors to Bridge Packets**

<b>Ratio Errors to Bridge Packets</b>	<b>Conclusion</b>	
0.1% or less	Status	Performance is Good.
	Impact:	None.
	Action:	None.
0.1% and 1%	Status	Performance is acceptable.
	Impact:	Network performance is OK, but your network might not perform as well as you expected.
	Action:	Refer to the Optimization section to determine the cause of the problem and optimize your network performance.
1% or more	Status	Performance is poor.
	Impact:	The performance problem may be caused by your network cabling or connections.
	Action:	Refer to the Optimization section to solve the problem.
2% or more	Status	Performance is very poor.
	Impact:	Your network operating system is likely to face severe performance problems.
	Action:	Refer to the Optimization section to investigate the problem in more detail. You may need to consult an external expert.

### WaveLAN Parameter Tallies

When you choose to monitor the Remote Statistics of the WaveLAN interface(s), WaveMANAGER/AP will display an additional set of WaveLAN specific parameters:

- SNR Packets ratio - Low SNR / (Good SNR + Excellent SNR)
- 'Noise Level' ratio
- 'Other Network ID'
- the level of variation in the values shown for all indicators.

The tallies for these parameters are derived from the packets which the WavePOINT-II unit receives from all stations in its range.



#### **NOTE:**

The specific tallies displayed for the WaveLAN interfaces do not represent a running average for the wireless environment. These tallies only reflect the information about individual packets that may have been sent by different stations within range of the WavePOINT-II unit

In Table 4-2, you will find diagnostic ratios for the WaveLAN parameter tallies. If dynamic changes occur in the values of the WaveLAN tallies, the most probable cause is that the links with one or more stations are of poor quality.

**Table 4-2 WaveLAN Parameter Ratios**

<b>Ratio</b>	<b>Value</b>	<b>Result</b>	
SNR Packets Ratio Low / (Good + Excellent)	< 0.1	Status	Performance is Good.
		Impact:	None.
		Action:	None.
SNR Packets Ratio Low / (Good + Excellent)	> 1	Status	The WavePOINT-II unit has been receiving more packets with a low SNR level than packets with a good SNR level.
		Impact:	A number of stations is located at the periphery of the coverage area of this WavePOINT-II unit.
		Action:	Refer to the Optimization section to identify the trouble stations, and optimize antenna/station placement to optimize wireless performance.
Noise level ratio	> 15%	Status	The WaveLAN interface of the WavePOINT suffers from interference.
		Impact:	Your network operating systems may suffer from poor performance as lost packets need to be retransmitted.
		Action:	Refer to the Optimization section to identify the trouble stations, and optimize antenna/station placement, or eliminate the source of interference.

If any of the above situations occur, use the WaveMANAGER/AP Remote Link Test option to find the poorly linked station(s).

### Adjusting Remote Statistics Time Interval

The 'Remote Statistics' monitor refreshes the data in its window at regular intervals that can vary between 1 second and 5 minutes.

Use an interval of 1 second when you want to monitor remote statistics on-line, e.g., in case of troubleshooting and/or when you have full bandwidth access to the WavePOINT unit via the local network.

Use an interval of 5 minutes when you run remote statistics only for background display purposes, on in cases when you access the network of the selected WavePOINT unit via a low-speed connection (e.g. a dial-up connection).

To change the setting of this interval, select the 'SNMP Polling Interval' option from the 'Monitor' menu. This will display a dialog box with a time bar, which allows you to adjust the time interval.

### Using Remote Link Test

The WaveMANAGER/AP Remote Link Test enables you to investigate the link between a remote WavePOINT-II unit and a wireless station connected to the selected WavePOINT-II unit.



**NOTE:**

The Remote Link Test works only in combination with WavePOINT-II units.

To run a Remote Link Test:

1. Connect to a remote WavePOINT-II unit (called the initiator station)
2. From the 'Analyze' menu, click the 'Select another device' option.

3. Enter the IP address or click the 'Scan' button to select the WavePOINT-II unit which you want to act as the initiator station.

**NOTE:**

The 'Scan' button only displays WavePOINT-II units that are connected to the same subnet as the management station. You must enter the IP address and Read password of a WavePOINT-II unit outside of the subnet.

To show the devices connected to the selected WavePOINT-II unit, select the 'Link Test' option from the 'Analyze' menu. This will display the window shown below.

---

**Figure 4-8 Select a Link Test Partner**



# Monitoring your WaveLAN Network

## WaveMANAGER/AP

The fields in the top section of the 'Link Test' window (Figure 4-8 on page 4-29) identify the 'Initiator Station'.

The list of devices in the middle section of Figure 4-8 on page 4-29 show all wireless devices connected to the 'Initiator Station'. These devices are identified by their station name and MAC address. The 'Interface' field identifies the WaveLAN interface that connects the device to the 'Initiator Station' (2=socket A, 3=socket B).

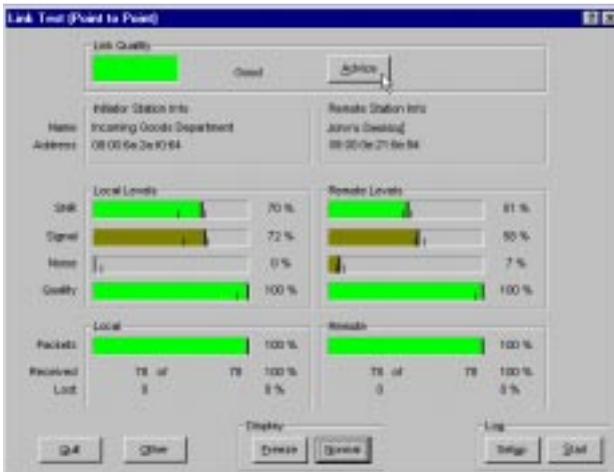


### NOTE:

The list of wireless devices connected to the WavePOINT-II unit may change as roaming mobile stations may enter or exit the coverage area of the selected WavePOINT-II unit. To refresh the list of devices, click the 'Explore' button.

To investigate the link between the initiator station and a particular station, select a station from the list and click the 'Link Test' button. This will display the 'Link Test' window as shown in Figure 4-9:

**Figure 4-9 Link Test Window**



For more information on this window, please refer to the section "Link Test" on page 4-8.

### **Adjusting the time Interval for the Link Test**

The Link Test data refreshes at regular intervals, which can vary from 1 to 15 seconds.

- Use a time interval of 1 second for on-line monitoring, e.g., when troubleshooting or when you have full bandwidth access via the local network.
- Use a time interval of 15 seconds when you run a Remote Link Test only for background information purposes, or in cases when you access the Initiator Station's network via a low-speed connection (e.g., a dial-up connection).

To change the setting of this interval, select the 'Analysis Interval' option from the 'Analyze' menu. A dialog box will appear, allowing you to adjust the time interval.



---

# Optimizing Performance

# 5

---

**Introduction** **5-1**

---

**Areas of Activity** **5-2**

Eliminating Redundant Traffic	5-2
. Protocol Filtering	5-3
. User-Defined Multicast Delay	5-4
. Optimizing Wired Connections	5-6
. Checking the Cable System	5-7
. Checking the Length of Your LAN Segments	5-8
Optimizing Wireless Connections	5-9
. Diagnosing Link Quality	5-10
Dual Band Configuration	5-13
. Setting Frequency for WavePOINT-II	5-16
. Setting Frequency for WaveLAN Stations	5-18
Avoiding Channel Crosstalk	5-20
. Frequency Mismatch	5-20
. Diagnosing Frequency Mismatch	5-21
. Verifying Operating Frequency	5-22
. Other Causes of Frequency Mismatch	5-22



---

# Optimizing Performance

# 5

---

## Introduction

---

You might consider optimizing network performance in situations where:

- You are troubleshooting a reported problem
- LAN performance is less than expected, or
- Routine checks at regular intervals show a performance degradation.

The performance of your LAN is usually determined by a complex combination of different factors. This section will present a number of considerations that may help you to:

- Determine whether optimization is really needed,
- Tailor your WaveLAN network to optimize its performance.

The benefit of each of the proposed solutions will largely depend on the actual situation that caused the current performance.



### **CAUTION:**

*Create separate backup files of the configuration data for each WavePOINT-II unit, before you start changing the configuration(s). Doing so will enable you to restore the initial setup of your network in case corrective actions did not result in the desired effect.*

## Areas of Activity

---

Optimization can be achieved in a number of ways that may include:

- Eliminating Redundant Traffic
- Optimizing Wired Connections
- Optimizing Wireless Connections
- Dual Band Configuration

### Eliminating Redundant Traffic

---

Data transmitted via your network can be divided in two major types of data:

- **True Data** - is data communicated between network stations, such as file-transfer or e-mail. This 'true data' is also referred to as payload. In the WaveMANAGER/AP Monitoring Windows, the 'true data' is displayed as Unicast Packets.
- **Network Overhead Data** - is data exchanged between network services to control the dataflow, such as protocol messages. This data is also referred to as traffic load. In the WaveMANAGER/AP Monitoring Windows, the 'Network Overhead Data' is displayed as Non-Unicast Packets.

The ratio of network overhead in relation to 'true data' differs from one networking service to another. When the ratio of network overhead is more than actually required, this may affect the performance of your wireless LAN, i.e. your 'true data' has to share the maximum bandwidth capacity with the network overhead. Eliminating Redundant Traffic will usually result in a significant performance improvement.

To eliminate redundant traffic, use the following options:

- Protocol Filtering
- User-Defined Multicast Delay

### Protocol Filtering

Some network protocols send large volumes of broadcasts to all stations. In many cases, these protocols may not be required by your wireless (client) stations. In these cases, protocol filtering may prevent the transmission of unnecessary data, saving more bandwidth for the actual communication within your network.

Use the 'Remote Statistics' function of the WaveMANAGER/AP to diagnose whether or not the protocol broadcasts degrade the performance of a wireless network (see Figure 4-7 on page 4-23).

1. Click either one of the WaveLAN tabs on the 'Remote Statistics' window to display the WaveLAN interface statistics.
2. Compare the number of Packets 'Out Collisions' with the number of 'Bridge out Packets'.
  - When the number of 'Out Collisions' is 1% of the 'Bridge out Packets' or more, this indicates that the wireless medium is very busy.
3. Compare the number of 'Unicast Packets In' to the number of 'Non-Unicast Packets In'.
  - When the number of 'Non-Unicast Packets In' is relatively high when compared to the number of 'Unicast Packets In', this might indicate your network generates a large amount of network traffic.

This does not necessarily mean that the traffic load is caused by the protocols, but it might be worth investigating whether protocol filtering will improve your network performance.



#### **CAUTION:**

*It may require advanced networking expertise to identify which protocols are used within your network, and to decide which protocols can be filtered without affecting the proper operation of your Network Operating System.*

## Optimizing Performance

### Areas of Activity

---

To filter network protocols:

1. Investigate what type of network stations and services are located in the WaveLAN environment of your network.
2. Consult the documentation that came with your network operating system to investigate which protocols are required for the network servers and services, and for the (wireless) clients.
3. Using the WaveMANAGER/AP program, click the 'Edit' button in the 'Protocols to Filter' section of the 'Setup Bridge Parameters' window (see Figure 3-9 on page 3-17). Check the protocols that you wish to filter, or click the 'Custom' button to 'Add' a protocol not on this list.

If this does not solve your problem, consider one of the following options:

- User-Defined Multicast Delay on page 5-4
- Optimizing Wired Connections on page 5-6
- Optimizing Wireless Connections on page 5-9

### User-Defined Multicast Delay

Many servers send broadcast messages to all stations in the network on a regular basis. When all WavePOINT-II units transmit these messages simultaneously over your wireless LAN, a large number of collisions will occur. As the 'addressed' stations will never receive the collided messages anymore, it is likely that your network system will encounter severe problems.

To avoid this problem the WavePOINT-II access points use a 'Random Multicast Delay'.

When the WavePOINT-II receives a Multicast message that is to be transmitted over the wireless LAN, the WavePOINT-II unit will apply a random delay before transmitting the message.

## Optimizing Performance

### Areas of Activity

---

This random delay is different for each of the WaveLAN interfaces, based on the last digit of the MAC address of the WaveLAN Card(s) in the WavePOINT-II unit.

The factory-set 'Random Multicast Delay' will provide sufficient networking performance. In some cases, you may wish to select a 'User-Defined Multicast Delay'.

This may be useful in situations where neighboring WavePOINT access points or interfaces have been equipped with WaveLAN/PCMCIA cards or WaveLAN/EAM modules that have an identical last digit in their MAC Address.

To verify whether this is the case in your situation, you may need to record the MAC addresses of all WaveLAN/PCMCIA Cards and/or WaveLAN/EAM modules that are used in your WavePOINT-II access points. You can do so using either the WaveMANAGER/CLIENT Link Test function, or the WaveMANAGER/AP Remote Link Test function. In the Link Test window, click the 'Details' button to display the MAC address of the stations.

When neighboring WavePOINT-II interfaces use cards of which the last digit of the MAC address match one another you will need to either:

- Swap cards to eliminate the matching digit problem, or
- Specify a unique 'User Defined Multicast Sequence' number (in the range from 1 to 10) for each of the WavePOINT-II units concerned.

## Optimizing Performance

### Areas of Activity

---

#### Setting User-Defined Multicast Delay

You can set the Multicast Delay option in the 'Roaming Setup Dialog box', which can be accessed from the WaveLAN Interface Parameters screen.

If the 'Random Multicast Delay' is enabled, click the check box to disable the random delay. Then:

1. Enter the number of access points (in a range of 1 to 10).
2. Enter the access point sequence.



**NOTE:**

When using User-Defined Multicast Delay on WavePOINT-II devices with two WaveLAN interfaces, you will need to specify separate Multicast Delay settings for each of the WaveLAN interfaces.

#### Roaming

In most cases, there will not be any stations roaming along the wireless outdoor link, therefore you can disable the roaming functionality. Roaming support does not cause a lot of overhead, but by disabling roaming, you may save some bandwidth, thus optimizing your data traffic.

#### Optimizing Wired Connections

Sometimes performance degradation of your (wireless) is caused by a failure in the cabling system that connects WaveLAN network to the wired infrastructure.

Such failures may be caused by one of the following situations:

- A faulty cable or connector in the wired infrastructure
- A LAN Segment that has been stretched over a distance that is too long.

## Optimizing Performance

### Areas of Activity

---

Usually what will happen in this kind of situation is that:

- The system does not work at all, or
- Your network system will generate a large number of error messages as a result of the faulty connection(s). As these messages are taking up bandwidth, the performance of your network may become very slow.

### Checking the Cable System

The occurrence of a problem in the cabling system can be diagnosed with the 'Remote Statistics' function of the WaveMANAGER/AP tool (see Figure 4-7 on page 4-23).

1. Click the Ethernet/0 tab to display the statistics for the Ethernet interface.
2. Compare the number of Packets 'In Errors' with the number of 'Bridge in Packets'.
  - When the number of 'In Errors' is 1% or more of the 'Bridge in Packets', this may indicate that there is a cabling problem.
3. Compare the number of packets 'Out Errors' with the number of 'Bridge out Packets'.
  - When the number of 'Out Errors' is 1% or more of the 'Bridge out Packets', it is likely that there is a cabling problem.
4. Compare the number of 'Out Carrier Sense Errors' with the number of 'Bridge out Packets'.
  - When the number of 'Out Carrier Sense Errors' is 1% of the 'Bridge out Packets' or the value of the 'Out Carrier Sense Errors' increases too rapidly, this indicates insufficient space on the network due to a backbone overload, or faulty cabling.

## Optimizing Performance

### Areas of Activity

---

5. Check whether the problem occurs only with the selected WavePOINT-II device, or with multiple WavePOINT-II devices.
  - If the problem is observed on only one unit, the problem may lie in the connectors or cable(s) that connect the WavePOINT-II to the hub or wired backbone.
  - When the problem exists with multiple units, it is likely to be caused by the cables or connectors of the wired backbone, hub or the bridge/router device that connects this network segment to your LAN.
6. Check the cabling system to verify whether all connectors are properly seated at the WavePOINT-II units, bridges, routers and hubs.
7. If your network uses coax cable (10Base2), make sure that terminators are placed on both ends.

### Checking the Length of Your LAN Segments

In exceptional cases, networking problems may be caused by LAN Segments that have been stretched over (too) large distances.

In these situations, frequent collisions might occur because stations can no longer detect the carriers transmitted by distant stations. Collided frames will no longer be received by the addressed station.

The occurrence of a LAN Segment system that is too long can be diagnosed with the 'Remote Statistics' function of the WaveMANAGER/AP tool (see Figure 4-7 on page 4-23).

1. Click the Ethernet/0 tab to display the statistics for the Ethernet interface.
2. Compare the number of Packets 'In Errors' with the number of 'Bridge in Packets'.
  - When the number of 'In Errors' is 1% of the 'Bridge in Packets' or more, there may be a cabling problem.

## Optimizing Performance

### Areas of Activity

---

3. Monitor the value increase of the parameter 'Bytes in' over a longer period of time.
  - When this number increases constantly with more than 600,000 bytes per second, this may indicate a problem with the length of your LAN Segment.

You may need to consult a network expert to verify or adjust the length of your cable segments.



#### **NOTE:**

If you decide to split the LAN (segment) into multiple (sub)segments, make sure that all WaveLAN devices will be grouped into the same LAN segment. WaveLAN stations will not be able to roam between LAN segments that are separated by Routers and/or Gateways.

If this does not solve your problem, consider one of the following options as described in this chapter:

- Eliminating Redundant Traffic on page 5-2
- Optimizing Wireless Connections on page 5-9
- Dual Band Configuration on page 5-13

## Optimizing Wireless Connections

---

When the Link Quality of communications between a wireless station and its WavePOINT-II unit are poor, packets communicated between this station and the access point may get lost. Waiting in vain for an acknowledgment of the receiving station, the sending station will re-transmit the lost packet.

Upon receipt of the same packet for the second time, the receiving station might decide to discard all packets received so-far, which would require that the sending station will have to retransmit all packets once again.

## Optimizing Performance

### Areas of Activity

---

Please note that:

- Many retransmissions may affect your effective data throughput as the 'True Data' has to share the WaveLAN bandwidth with the re-transmitted frames.
- The retransmissions will also degrade the performance of your wireless stations, for example, saving a file will take longer than without retransmissions.

A poor Link Quality can be caused by one or more of the following problems:

- The station is almost 'out of range' of the WavePOINT-II access point
- There is a source of interference in the WaveLAN signal path between the station and the WavePOINT-II unit
- The station and/or WavePOINT use WaveLAN operating frequencies that do not match (see also "Avoiding Channel Crosstalk" on page 5-20).

### Diagnosing Link Quality

The occurrence of a poor Link Quality on the wireless network can be diagnosed with the 'Remote Statistics' function of the WaveMANAGER/AP tool (see Figure 4-7 on page 4-23).

From the 'Remote Statistics' window, click either one of the WaveLAN tabs to display the statistics for the WaveLAN interface(s). Then, use the following to diagnose Link Quality:

1. Compare the number of Packets 'In Errors' with the number of 'Bridge In Packets'.
  - When the number of 'In Errors' is 1% or more of the 'Bridge in packets', this may indicate that the WaveLAN medium is very busy.

## Optimizing Performance

### Areas of Activity

---

2. Monitor the value increase of the parameter 'Bytes in' over a longer period of time.
  - When this number increases constantly with more than 150,000 bytes per second, this indicates that the problem is caused by one or more stations that send many re-transmissions as a result of a 'poor radio connection'.
3. To verify this assumption, also compare the number of packets 'Out Errors' with the number of 'Bridge out packets'.
  - When the number of 'Out Errors' is 1% or more of the 'Bridge out packets', it is likely that one or more stations suffer form a poor Link Quality.
4. Compare the number of packets 'Out Collisions' with the number of 'Bridge out packets'.
  - If the number of 'Out Collisions' is 1% or more of the 'Bridge Out Packets', it is likely that the WaveLAN medium is very busy. This might be caused by many retransmitted frames, but it could also refer to many stations trying to communicate at the same time.

Usually, in this situation, you will be able to witness similar behavior looking at the Signal to Noise Ratio (SNR) tallies.
5. The Signal-to-Noise Ratio (SNR) tallies count the number of packets that were received. SNR is measured as either 'Excellent', 'Good', or 'Low'.
  - If the number of 'Low SNR' is relatively high when compared to the sum of 'Good SNR + Excellent SNR', this indicates that the WavePOINT-II receives many frames from stations with a poor Link Quality. This large number of frames, probably includes numerous retransmissions.
  - If the number of 'Low SNR' remains relatively low when compared to the sum of 'Good SNR + Excellent SNR', then the wireless medium is busy due to extensive wireless traffic. Most likely, you will also see that the number of 'Bridge In Packets' increases as well.

## Optimizing Performance

### Areas of Activity

---

- When no stations suffer from a poor Signal Level or high Noise level, take a closer look at the 'Packets Sent/Received' indicators. (You may need to click the 'Details' button to display the Signal Level and Noise Level indicators.)

In most situations where packets are lost, and the Signal Level and Noise Level are normal, the medium may simply be too busy. Consider one of the other options described in this chapter to remedy the busy medium.

6. You can also use the WaveMANAGER/AP Remote Link Test to analyze whether one or more stations show a poor 'Link Quality':

- When the poor 'Link Quality' is caused by a low Signal Level, the station is almost out of range of the WavePOINT-II unit.
- When the poor 'Link Quality' is caused by a high Noise Level, there is a source of interference in the signal path between the station and the WavePOINT-II unit.

7. When one or more stations show a poor Link Quality, re-transmissions of frames will disturb overall statistics and performance.

- You may be able to solve the problem by either moving the station(s) or eliminating the source of interference.
- If the problem is caused by a poor Signal Level, add an extra WavePOINT-II unit, or adjust the placement of your WavePOINT-II units to provide coverage for all wireless stations.



#### **NOTE:**

You can also use the WaveMANAGER/CLIENT tool to analyze the link quality between a remote station and the WavePOINT-II unit. In that case, you will need to be on-site to run the WaveMANAGER/CLIENT tool on the suspect station(s).

## Optimizing Performance

### Areas of Activity

---

If these options do not resolve your problem, consider one of the following options:

- Optimizing Wireless Connections on page 5-9
- Optimizing Wired Connections on page 5-6
- Eliminating Redundant Traffic on page 5-2

## Dual Band Configuration

---

When your wireless network is very busy and none of the previous options solved your problem, you may consider the installation of a WaveLAN Dual Band Configuration.

A Dual Band Configuration is a wireless networking environment, where you use two, non-overlapping radio frequency channels to increase the WaveLAN bandwidth.



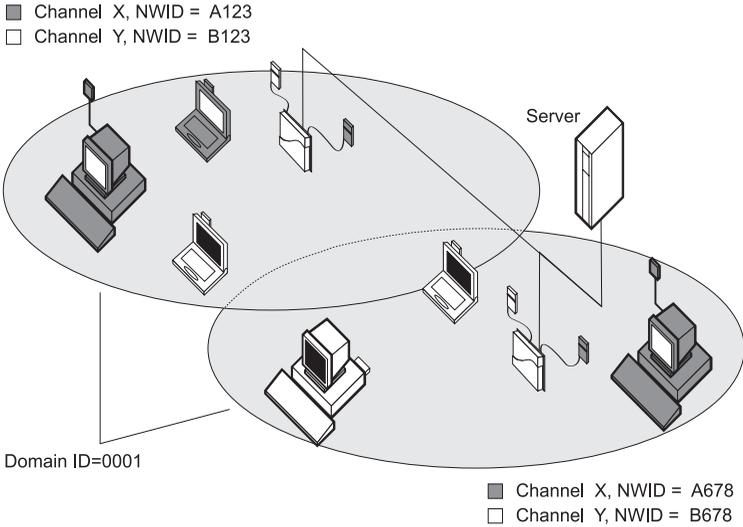
### **NOTE:**

To comply with local radio regulations WaveLAN products are sold with a country-specific channel-sets (ETS, FCC, JP or FR). The number of selectable channels for each set will differ according to the local radio certifications. Therefore, in some countries, Dual Band Configurations may not be a suitable solution to expand the WaveLAN bandwidth.

To setup a Dual Band Configuration, you will need to:

1. Equip all your WavePOINT-II access points with two WaveLAN/PCMCIA cards.
2. Configure each of the WaveLAN interfaces to operate at a different frequency channel.
3. Configure your wireless stations to operate at one of the dedicated channels as supported by the WavePOINT-II access points.

**Figure 5-1 Dual Band Configuration**



In Figure 5-1, the WavePOINT-II access points have been equipped with two WaveLAN/PCMCIA cards:

- Socket A operating at a channel identified as Channel X
- Socket B operating at a channel identified as Channel Y

In fact each wireless cell is now covered twice (both Channel X and Y). The WaveLAN stations do not roam over multiple channels, but will use either Channel X or Channel Y to communicate with the WavePOINT-II units and/or stations that use the same frequency channel.

Communication between stations that operate at different channels will be bridged by the WavePOINT-II access points that support both frequency channels.

## Optimizing Performance

### Areas of Activity

---

To setup a Dual Band Configuration, you can:

- Use a combination of WaveLAN 915 MHz and WaveLAN 2.4 GHz products, or
- Use WaveLAN 2.4 GHz products only, where you select two different sub-channels from the country-specific channel set.

To avoid cross-talk between the two WaveLAN channels, you are advised to:

- Mount the two WaveLAN interfaces for the WavePOINT-II access point separated from one another as pictured in Figure 5-1 (minimum separation is 1,5 m./5 ft.)
- Select WaveLAN sub-channels that allow for a maximum channel separation (minimum separation is 30 MHz).

The standard cable length of WaveLAN/PCMCIA is 45 cm(17.5"). To separate the WaveLAN interfaces at the WavePOINT-II access point, WaveLAN/PCMCIA adapters are available with a cable length of 100 cm(40") cables.



**NOTE:**

If you need further information on cables or other WaveLAN products, please contact your local Lucent Sales Office or Authorized WaveLAN Reseller. You can also find more information on our website at [www.wavelan.com](http://www.wavelan.com).

## Optimizing Performance

### Areas of Activity

---

Table 5-1 lists a number of successful channel combinations that you can use to setup a Dual Band Configuration.

**Table 5-1 Recommended Dual Band Combinations**

<b>WavePOINT-II</b>	<b>Socket A</b>	<b>Socket B</b>
	915 MHz	any 2.4 GHz Channel
	2412 MHz	2442 / 2452 / 2462 MHz or 915 MHz
	2422 MHz	2452 / 2462 MHz or 915 MHz
	2425 MHz	2462 MHz or 915 MHz
	2430.5 MHz	2462 MHz or 915 MHz
	2432 MHz	2462 MHz or 915 MHz
	2442 MHz	2412 MHz or 915 MHz
	2452 MHz	2412 / 2422 MHz or 915 MHz
	2462 MHz	2412 / 2422 / 2425 / 2430.5 MHz 2432 MHz or 915 MHz



**NOTE:**

The availability of each of the listed channels in Table 5-1 is subject to local radio regulations that apply in your country.

### Setting Frequency for WavePOINT-II

The frequency for WavePOINT-II access points is managed via the WaveLAN card that you inserted into the PC-Card slot(s).

To configure the frequencies for your WavePOINT-II access points proceed as follows:

1. Start the WaveMANAGER/AP program and connect to the WavePOINT-II unit.
2. From the Setup menu, select WaveLAN Interface Parameters.

## Optimizing Performance

### Areas of Activity

---

3. Select the socket for the WaveLAN interface that you would like to configure.
4. In the WaveLAN Interface Parameters, click the 'Frequency' button.
  - When the WaveLAN card supports only a single frequency, a pop-up box will appear stating that you have selected a 'Fixed Frequency Card' that can not be changed.
  - When the WaveLAN card supports multiple sub-channels, a pull-down box will appear, allowing you to select a different operating frequency.
5. In the Frequency Setup dialog box, use the pull-down menu to select a frequency of your choice.
6. Click OK to confirm the selected frequency and close the Frequency Select window.
7. Click OK to close the WaveLAN Interface Parameters window.
8. Repeat steps 3-7 to verify and/or change the frequency for the second WaveLAN interface.
9. When finished click OK to close the Socket Selection window.
10. From the File menu select 'Save' to upload the new settings to the WavePOINT-II access points.
11. Next select 'Save as' from the File menu to save the modified configuration to a back-up file.
12. Update the WavePOINT-II Configuration Record to reflect these changes.
13. (Optionally) Modify the configurations of all your other WavePOINT-II access points accordingly.
14. Modify the configuration of all your wireless workstations to set the frequency to one of the supported frequencies as described in "Setting Frequency for WaveLAN Stations" on page 5-18.

## Optimizing Performance

### Areas of Activity

---

#### Setting Frequency for WaveLAN Stations

In Dual Band Configurations you will need to configure the wireless workstations to operate at either one of the frequencies you selected for the WavePOINT-II access points.

The purpose of Dual Band Configurations in most cases will be to distribute the wireless traffic load equally over both frequencies. In order to allocate frequencies correctly, you are advised to:

- map all wireless stations that are present in the network
- identify the specific data-traffic requirements for the wireless stations
- identify the roaming paths of mobile stations

Doing so will help you to determine which stations should be set to operate at the same WaveLAN sub-channel, or be set to different channels.

For example when one WaveLAN cell includes a wireless database server that generates/receives a lot of traffic, you may decide to set all other WaveLAN (work)stations in that area to operate at another channel, in order to leave maximum bandwidth to the server.

To modify the operating frequency of your WaveLAN workstation(s), you can use one of the following WaveLAN programs:

- WaveMANAGER/CLIENT tool for stations that run either Microsoft Windows 95 or Windows NT Operating System.
- WaveLAN Frequency Select Utility (wfreqsel.exe) for stations that run on different operating systems.



**NOTE:**

The MS-DOS-based WaveLAN Frequency Select Utility is not described in this document. For more information on how to use this utility, please refer to the User's Guide that came with your WaveLAN/PCMCIA and WaveLAN/ISA card.

## Optimizing Performance

### Areas of Activity

---

To change a station's frequency using WaveMANAGER/CLIENT, proceed as follows:

1. Make sure that the WaveLAN station has the WaveMANAGER/CLIENT program installed.
2. From the Windows taskbar click 'Start', 'Program Files', 'WaveLAN'.
3. From the WaveLAN menu or window, select WaveMANAGER/CLIENT.
4. In the main window, select the 'Frequency' button.
  - When the WaveLAN card supports only a single frequency, a pop-up box will appear stating that you have selected a 'Fixed Frequency Card' that can not be changed.
  - When the WaveLAN card supports multiple sub-channels, a list of supported frequencies will appear, allowing you to select another operating frequency.
5. In the Frequency Setup window, use the radio buttons to select the frequency of your choice.
6. Click OK to confirm the selected frequency and close the Frequency Select window.
7. Click OK to close the WaveMANAGER/CLIENT program.
8. Repeat steps 1-7 for all other WaveLAN workstations to verify and/or change the frequency of these WaveLAN stations.
9. (Optional) Create a maintenance report to identify which stations have been set to operate at a specific channel.

#### Avoiding Channel Crosstalk

---

In most network configurations you are advised to remain within one operating frequency. WaveLAN stations that have a frequency mismatch may cause unpredictable behavior on your WaveLAN network, such as:

- When the mismatched frequencies are close to one another, packets may sometimes be received, but in most cases will be received in error.
- The medium looks busy, because your WaveLAN stations are deferring for carriers sensed on an adjacent (mismatched) 2.4 GHz sub-channel.
- Stations that operate at a mismatched frequency are perceived as in-band interferers that affect the quality of wireless communications between other WaveLAN stations.

#### Frequency Mismatch

The occurrence of a frequency mismatch can be difficult to diagnose. The existence of a frequency mismatch should be suspected when monitoring WaveLAN Remote Statistics, you detect a busy WaveLAN medium, but are unable to trace any evidence of extensive LAN traffic.

Typical examples of situations where you might encounter a network suffering from a frequency mismatch are WaveLAN installations that include 2.4 GHz products, and where:

- In a “Dual Band Configuration”, as described on page 5-13, the selected sub-bands are too close to one another. The recommended minimum channel separation is 40 MHz or more (see Table 5-1 on page 5-16).
- Your installation includes both multiple channel and single channel 2.4 GHz products. The first releases of WaveLAN 2.4 GHz products supported only a single (country-specific)

operating frequency. Later models supported a country specific channel-set that allowed for 2.4 GHz sub-channel selection. The factory-set default channels of these units might not match the operating frequency of the fixed channel models.

### Diagnosing Frequency Mismatch

The occurrence of a frequency mismatch can be diagnosed with the 'Remote Statistics' function of the WaveMANAGER/AP tool (see Figure 4-7 on page 4-23).

1. From the WaveLAN Interface Parameters screen, click either one of the WaveLAN tabs to display the statistics for the WaveLAN interface(s).
2. Compare the number of Packets 'In errors' with the number of 'Bridge in packets'.
  - If the number of 'In Errors' is 1% or more of the 'Bridge in packets', this indicates the medium is very busy.  
Usually in this situation, you will be able to witness similar behavior looking at the Signal to Noise Ratio (SNR).
3. The Signal to Noise Ratio (SNR) tallies count the number of packets that were received with a SNR qualified as either 'Excellent', 'Good', or 'Low'.
  - If the number of 'Low SNR' remains relatively low when compared to the sum of 'Good SNR + Excellent SNR', this indicates that the wireless medium is just busy, as a result of extensive wireless traffic.
  - Most likely, you will also see that the number of 'Bridge in Packets' increases constantly as well.

In most cases, this would refer to a 'busy medium' that you should remedy using one of the other options described in this chapter. However when you are certain that there is not that much traffic on your LAN, you are advised to check the operating frequency of all your WaveLAN cards and access points.

## Optimizing Performance

### Areas of Activity

---

#### Verifying Operating Frequency

Use one of the following methods to verify (correct) the operating frequency of your WaveLAN product.

##### **WavePOINT Access Points**

For WavePOINT-II units, use the WaveMANAGER/AP program, as described in “Setting Frequency for WavePOINT-II” on page 5-16

For other WavePOINT products, use the ‘Configuration’ program as described in the ‘Installation and Operation Guide’ that came with the unit.

##### **WaveLAN Stations**

For stations that use the Microsoft Windows 95, or Windows NT operating system, use the WaveMANAGER/CLIENT program as described in “Setting Frequency for WaveLAN Stations” on page 5-18.

For stations that use Microsoft Windows 3.x or another operating system, use the WaveLAN Frequency Select Utility as described in the ‘User’s Guide’ that came with your WaveLAN adapter card.

#### Other Causes of Frequency Mismatch

If you are still having troubles identifying a single station that is operating on a mismatched channel, yet you still suspect a mismatch, it could be one of the following:

##### **Station Shut Down**

Restart the station, and then re-verify the operating frequency.

#### **Busy Medium**

The diagnosed problem was not caused by a frequency mismatch, but the network indicates that the medium is 'too busy'

Consider one of the other options described in this Chapter to remedy the busy medium:

- Eliminating Redundant Traffic on page 5-2
- Optimizing Wired Connections on page 5-6
- Optimizing Wireless Connections on page 5-9

#### **Interference from Neighboring Network**

There may be a neighboring WaveLAN network that is interfering with your wireless LAN. You should use the WaveMANAGER/CLIENT program, to scan the wireless medium for the existence of neighboring WaveLAN Domains.

If there is a neighboring WaveLAN network that might interfere with your wireless LAN, you may consider to:

- Set your network to operate at a different sub-channel, or
- Move your WavePOINT access points out of range of the neighboring network.

If you are running WaveMANAGER/CLIENT with 'Domain Detect Mode' as an option on the 'Site Monitor' window, you can display the number of neighboring domains that are up and running, and the number of access points associated with these domains that are within range of your wireless LAN.



**NOTE:**

The 'Domain Detect Mode' will only display the existence of a Domain. It will not reveal the Domain ID of the other WaveLAN networks.



---

<b>Introduction</b>	<b>6-1</b>
<hr/>	
<b>Securing Access to Wireless Data</b>	<b>6-2</b>
Connecting to the Network	6-2
Data Encryption	6-3
Access Control	6-6
• Enabling Access Control	6-6
• Creating/Editing an Access Control Table	6-7
• Disabling Access Control	6-10
<hr/>	
<b>Securing WavePOINT-II Configuration</b>	<b>6-11</b>
Read and Read/Write passwords	6-11
SNMP IP Access	6-12
Trap Host Alerts	6-13



---

## Introduction

---

A distinct advantage of WaveLAN offers quick, easy, wireless access to your network.

To minimize unauthorized use of your WaveLAN network, you will need to secure your network in two ways:

- Securing Access to Wireless Data
- Securing WavePOINT Configuration

Of course WaveLAN supports standard security mechanisms, such as User Names and Passwords as implemented by Network Operating Systems.

## Securing Access to Wireless Data

---

To prevent unauthorized WaveLAN stations from accessing data that is transmitted over the network, WaveLAN supports the following levels of security:

- Control of the ability to 'connect' to the WaveLAN network by means of the standard WaveLAN interface parameters such as NWID, Domain ID and beacon keys.
- Data encryption to encrypt all data transmitted via the wireless medium.
- Access control to restrict wireless access to authorized MAC addresses only from certain WavePOINT-II units using the Access Control Table feature.

## Connecting to the Network

---

Access protection to the network is arranged as follows:

- In a WaveLAN network the 'Network Identification Designator' (NWID) logically connects stations in a wireless cell, like a cable physically connects stations in a wired network. In ad-hoc workgroups, it is not possible to connect to the wireless group without the correct NWID (i.e. cable). The Domain ID and the NWID secure the wireless medium (connections to the wireless traffic), not the stations.
- In multiple-cell environments, like those described in Chapter 2, wireless stations may roam between multiple cells, where each cell is identified by a unique NWID. In these environments (domains), stations can only retrieve the required NWID information when they have been configured with the correct Domain ID. You can use the Domain ID in combination with a Beacon Key. The Beacon Key will encode the NWID information that

## Security

### Securing Access to Wireless Data

---

is sent to the wireless stations. Without a matching Beacon Key the wireless station will not be able to decode the NWID required to connect to a local cell.

- In addition to the two protection mechanisms mentioned above, you can use network passwords as implemented by Standard Network Operating Systems. These network passwords secure access to the network at the level of the networking software.

## Data Encryption

---

To encrypt the data that is sent via the wireless medium of your network, you can use WaveLAN devices equipped with a factory-installed encryption chip.

The encryption chip enables you to define an encryption key of 16 alphanumeric characters in the range of 0 to 9 and A to F.



### **NOTE:**

To use data encryption, all WaveLAN devices must be equipped with an encryption chip.

To allow communication, all WaveLAN stations and WavePOINT-II units on your network must use the same encryption key.

### **Enabling Data Encryption**

1. To enable encryption for your WavePOINT-II units, first open the configuration of your WavePOINT-II unit(s) (see “Step 2 - Connecting to a WavePOINT-II” on page 3-3).
2. From the ‘Setup’ menu, select WaveLAN Interface Parameters.
3. Select the socket of the WaveLAN interface for which you would like to enable encryption.

## Security

### Securing Access to Wireless Data

---

4. In the WaveLAN interface parameters window, select the 'Enable WaveLAN Encryption' box.

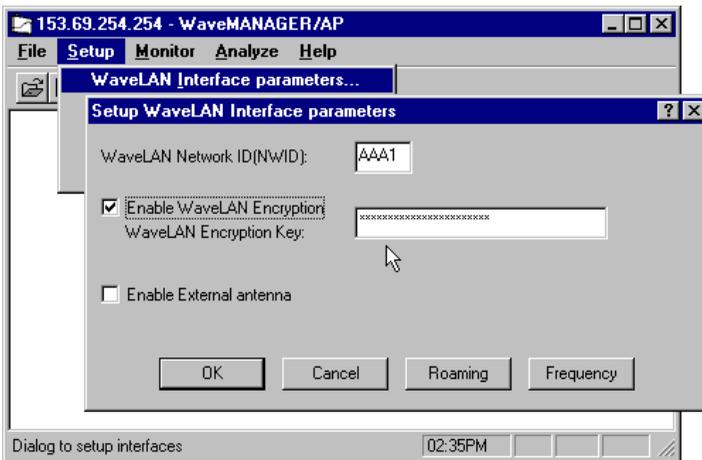


**NOTE:**

If the 'Enable WaveLAN Encryption' box is grayed out, the WaveLAN card inserted into the corresponding socket of your WavePOINT-II unit does not support encryption. Replace the WaveLAN card for this WavePOINT-II interface with a WaveLAN/PCMCIA card that supports encryption.

---

**Figure 6-1 WaveLAN Interface parameters**



**NOTE:**

Enter a 16-digit hexadecimal encryption key. Make sure that all WaveLAN stations and WavePOINT-II units use the identical encryption key.

## Security

### Securing Access to Wireless Data

---

5. Click OK to confirm the encryption key and close the WaveLAN interface parameters window.
6. (Optional) Repeat steps 3-6 for the second WaveLAN interface.
7. Click OK to return to the main menu.
8. From the 'File' menu, select 'Save Config file' to load the new configuration into the WavePOINT-II unit.
9. (Optional) From the 'File' menu, select 'Save Config file as' to save the parameter settings to a local back-up file (\*.cnf).
10. Update the WavePOINT-II Configuration record to reflect this modification.
11. (Optional) Configure the encryption settings for all other WaveLAN devices in your network to match the settings of your WavePOINT-II unit(s). Refer to the User's Guide that came with your WaveLAN product for information about how to modify the WaveLAN parameters.

### Disabling Data Encryption

1. To disable encryption for your WavePOINT-II units, first open the configuration of your WavePOINT-II unit(s) (see "Step 2 - Connecting to a WavePOINT-II" on page 3-3).
2. From the 'Setup' menu, select WaveLAN Interface Parameters.
3. Select the socket of the WaveLAN interface for which you want to disable encryption.
4. In the WaveLAN interface parameters window, deselect the 'Enable WaveLAN Encryption' box.
5. Click OK to confirm and close the WaveLAN interface parameters window.
6. (Optional) Repeat steps 3-6 for the second WaveLAN interface.
7. Click OK to return to the main menu.
8. From the 'File' menu, select 'Save Config file' to load the new configuration into the WavePOINT-II unit.

## Security

### Securing Access to Wireless Data

---

9. (Optional) From the 'File' menu, select 'Save Config file as' to save the parameter settings to a local back-up file (\*.cnf).
10. Update the WavePOINT-II Configuration record to reflect this modification.
11. (Optional) Modify the encryption settings for all other WaveLAN devices in your network to match the settings of your WavePOINT-II unit. Refer to the User's Guide that came with your WaveLAN product for information about how to modify the WaveLAN parameters.

## Access Control

---

You can restrict Wireless Access to the WavePOINT-II units by means of the Access Control Table. When Access Control is enabled, your WavePOINT-II access points will ignore all requests to forward data to/from WaveLAN devices that are not identified in the Access Control Table.

### Enabling Access Control

To authorize a WaveLAN device to access the WavePOINT-II unit, you must identify the MAC address of the WaveLAN device in the Access Control Table. The Access Control Table is a separate file (\*.tbl) that is loaded into the WavePOINT-II access points as part of the configuration.



**NOTE:**

All WavePOINTs should use the identical Access Control Table.

## Security

### Securing Access to Wireless Data

---

#### Creating/Editing an Access Control Table

There are two ways to create or edit the Access Control Table:

- add the MAC addresses manually, using the WaveMANAGER/AP program;
- add the MAC address automatically, using the WaveMANAGER/CLIENT program.

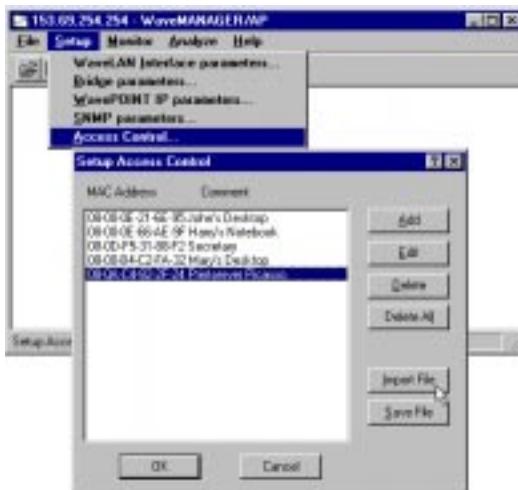
The manual option is the most efficient choice when you know all MAC addresses. If you do not know the MAC addresses, you can run WaveMANAGER/CLIENT on each WaveLAN station to retrieve its MAC address and add it to the Access Control Table.

#### Setting up the Access Control Table Manually

1. Open the configuration of your WavePOINT-II unit(s) (see “Step 2 - Connecting to a WavePOINT-II” on page 3-3).
2. Select the ‘Access Control’ option from the ‘Setup’ menu to display all MAC addresses that are currently authorized (the default is ‘all will be permitted’).

---

**Figure 6-2 Access Control Setup Dialog Box**



## Security

### Securing Access to Wireless Data

---

3. To modify the current list of MAC addresses:
  - click the 'Add' button to enter the MAC addresses, one at a time, to be listed in the table;
  - use the 'Edit' button to change entries in the list or use the 'Delete' buttons to remove items from the list;
  - click the 'Import File' button to import an existing Access Control Table and, if required, edit the table.
4. (Optional) Use the 'Input Ethernet Address' dialog box to enter a name or comment for the listed MAC addresses.
5. Repeat steps 1-4 for all stations you want to authorize to send/receive data via this WavePOINT-II unit.
6. In the 'Input Ethernet Address' dialog box, click the 'Save file' button to make a back-up copy of the Access Control Table you just created. You can use this file later to import the file (\*.tbl) into the configuration of the other WavePOINT-II units.
7. Click OK to return to the main menu.
8. From the 'File' menu, select 'Save Config file' to load the new configuration file and the access control table into the WavePOINT-II unit.
9. (Optional) From the 'File' menu, select 'Save Config file as' to save the parameter settings to a local back-up file (\*.cnf).

To save the table to all WavePOINT-II units, please refer to the information on common parameters in "Set the Common Parameters" on page 3-14.

#### **Setting up the Access Control Table Automatically**

To set up the Access Control Table automatically, you will need to run WaveMANAGER/CLIENT on every WaveLAN station of which you want to add the MAC address to the Access Control Table.

To run WaveMANAGER/CLIENT, the client station must have the latest Miniport driver installed.

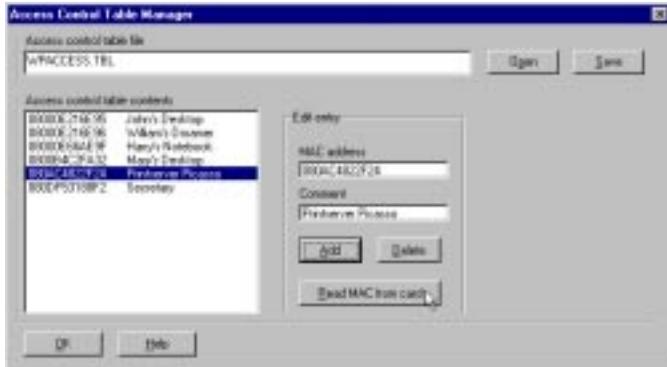
1. Start WaveMANAGER/CLIENT.

## Security

### Securing Access to Wireless Data

2. On the Opening window of WaveMANAGER/CLIENT, click the 'Access Control' button to display the following window:

**Figure 6-3 Access Control Table Manager**



To fill in the table, you can either open an existing table and add/edit MAC addresses, or you can compose a new table.

- To open an existing Access Control Table file, type the path and filename in the field in the top of the window.
- To create a new table, enter a new path and filename (e.g. A:\Myaccess.tbl) in the field in the top of the window and click the 'Save' button.



**NOTE:**

save the file to a diskette, as you will need to add subsequent addresses on multiple stations.

3. To add the MAC address of the current WaveLAN station, click the 'Read MAC from card' button.
4. (Optional) Add a comment for the MAC address.
5. (Optional) If you know the MAC addresses of other WaveLAN stations, you can also use this menu in the WaveMANAGER/CLIENT program to add them manually.

## Security

### Securing Access to Wireless Data

---

6. Save the Access Control Table to diskette again.
7. Exit the WaveMANAGER/CLIENT program.
8. Take out the diskette and move to the next WaveLAN station.
9. At the next WaveLAN station, start the WaveMANAGER/CLIENT program again.
10. In the 'Access Control Table Manager' window, use the 'Open Access Control Table file' option to import the table file from diskette.
11. Repeat steps 3 through 11 for all other WaveLAN stations.

When all addresses have been added to the table, use WaveMANAGER/AP to upload your WavePOINT-II units with the new Access Control Table information.

For more information on how to upload the table to all WavePOINT-II units, refer to "Step 5 - Upload the Configuration" on page 3-8.

### Disabling Access Control

To disable Access Control for your WavePOINT-II units:

1. Open the configuration of your WavePOINT-II unit(s) (see "Step 2 - Connecting to a WavePOINT-II" on page 3-3).
2. Select the 'Access Control' option from the 'Setup' menu to display all MAC addresses that are currently authorized.
3. To disable Access Control, click the 'Delete All' button. The MAC address window will read <All will be permitted>.
4. Click OK to return to the main menu.
5. From the 'File' menu, select 'Save Config file' to load the new configuration file and access control table into the unit.
6. (Optional) From the 'File' menu, select 'Save Config file as' to save the parameter settings to a local back-up file (\*.cnf).
7. Update the WavePOINT-II Configuration Record to reflect this change.
8. (Optional) Modify the Access Control Settings for all other WavePOINT-II units.

## **Securing WavePOINT-II Configuration**

---

All security measures such as Domain ID, Encryption Key or Access Control become useless when unauthorized persons can view and modify the configuration of your WavePOINT access points.

To protect your network configuration from undesired modifications, you are advised to implement the following measures:

- Read and Read/Write Passwords
- the SNMP IP Address Access List
- Trap Host Alert Mechanisms (optional)

### **Read and Read/Write passwords**

---

To restrict access to WavePOINT configuration information, you can create two authority levels for passwords:

- Read password
- Read/Write password

#### **Read password**

A Read password will only provide access to the WavePOINT to display diagnostic information listed under the 'Monitor' and 'Analyze' pull-down menus in the WaveMANAGER/AP program. Entering an incorrect password will result in a time-out error.

You can only enter Read passwords using the 'Select another Device' option of the 'Monitor' and 'Analyze' pull-down menus. Entering a Read password in the 'Open Remote Config' dialog box will result in a time-out error.

You can define a Read password in the 'SNMP parameters' window from the 'Setup' menu (the default value is 'public').

#### **Read/Write password**

A Read/Write password will provide full access to display WavePOINT diagnostic information listed under the 'Monitor' and 'Analyze' menus, and the configuration settings listed under the Setup menu.

Entering an incorrect password will result in a time-out error.

You can define a Read/Write password in the 'SNMP Parameters' window from the 'Setup' menu (the default value is 'public').

#### **SNMP IP Access**

---

In addition to the Read and Read/Write passwords, you can restrict access to the WavePOINT configuration to a limited number of authorized stations. Authorized stations are identified by:

- the unique IP address of the management station
- the WavePOINT interface via which this station will access the configuration

When the IP address or interface does not match the listing in the SNMP Access List, the requester will receive a time-out error.

To authorize a management station, enter its IP address into the SNMP IP Access List. The SNMP IP Access List is registered in the 'SNMP Parameters' window from the 'Setup' menu (the default value is 'all will be permitted').

When using the SNMP IP Access List, the list should include the IP address of all stations that might need to retrieve configuration or diagnostic information of the access point, i.e., stations of administrators who use either Read or Read/Write passwords.

## **Trap Host Alerts**

---

You can use the Trap Host mechanism to inform a network administrator when somebody resets a WavePOINT-II unit or performs a forced reload procedure. The Trap Host alert will enable the network administrator to verify whether the Reset or Forced Reload action was an authorized action or not.

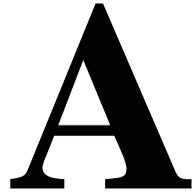
To activate the Trap Host mechanism, enter an IP address and a password in the appropriate fields of the 'SNMP parameters' window from the 'Setup' menu.

The IP address should identify the Trap Host station, i.e. the network management station that will be used to receive the Trap messages. The Trap Host password is included in the Trap messages and will help the Trap Host station to identify whether a received Trap Host message came from its own domain or not.



---

# Troubleshooting



---

## Problem Determination

---

Problems experienced in wireless LAN operation can be related to:

- Configuration mismatch
- Component failure
- Wired or wireless network problems.

The WaveMANAGER product suite offers a variety of tools to assist you in diagnosing, investigating and solving the problem.

## Problem-solving Approach

---

Depending on the location and the nature of the problem, you will need to decide whether you can solve the problem from a remote location, or whether you need to go 'on-site' to investigate and solve the problem.

The information in this chapter offers a set of guidelines for solving a problem both 'on-site' and 'remote' ('off-site'). To decide which solution will provide the best result in your situation, use the flowcharts as described on the following page.

When troubleshooting 'on-site', you can use the "LED Error Table" on page A-12 to determine if the problem is hardware related (component failure) or an operational problem.

## Troubleshooting

### Problem Determination

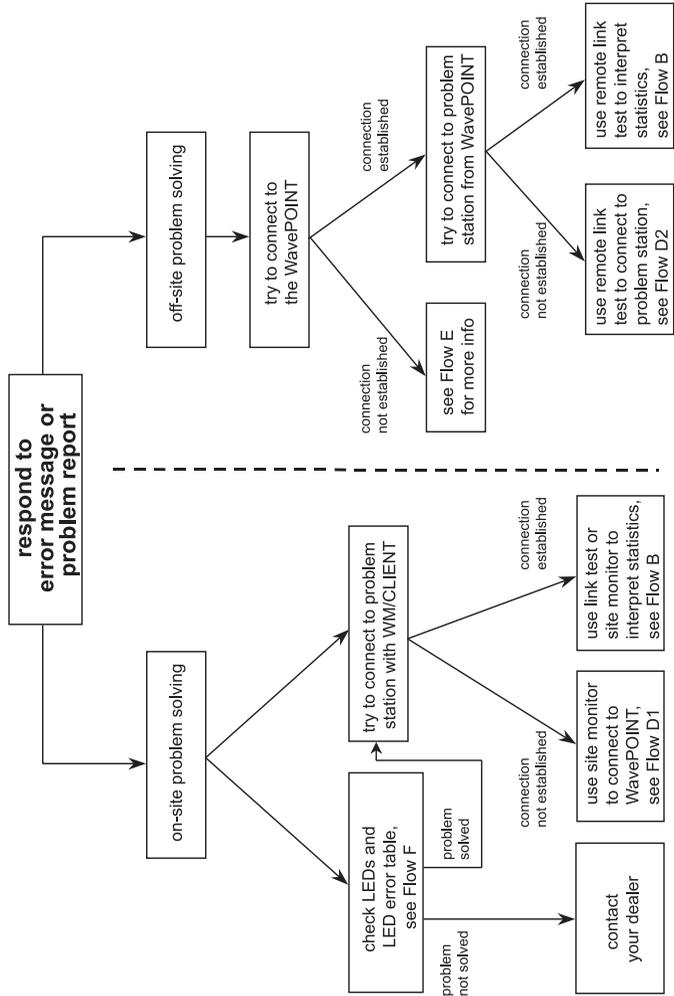
---

#### Where do I start?

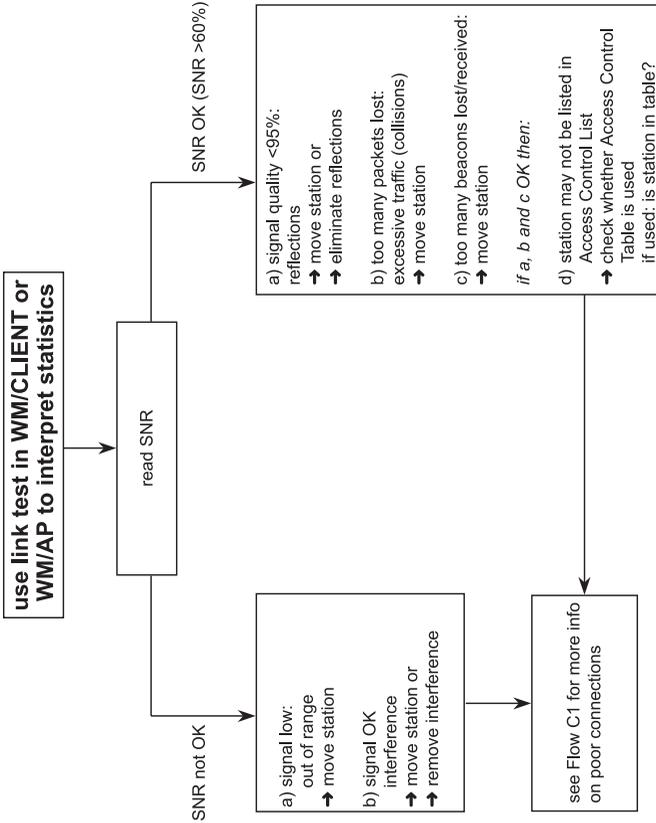
---

Flow	Trigger	Action
A	Error message displayed on screen or problem reported to network manager	Solve problem on-site at the location of the problem or off-site from the WaveMANAGER station
B	Information from problem station needs to be diagnosed	Use link test (in WM/CLIENT or WM/AP) to interpret statistics
C1/2	Network is showing poor performance	Choose WM/CLIENT or WM/AP to diagnose cause of poor performance
D1	Problem station cannot connect to WavePOINT-II unit	Use site monitor (in WM/CLIENT) to investigate network
D2	(Remote) WavePOINT-II unit cannot connect to problem station	Use remote link test (in WM/AP) to investigate network
E1/2	Management station cannot connect to WavePOINT-II unit	Check network parameters and connections
F	LEDs of WavePOINT-II unit need to be interpreted	Use LED Error table to diagnose LEDs

**Flow A, Error message displayed or problem reported**



## Flow B, interpret statistics

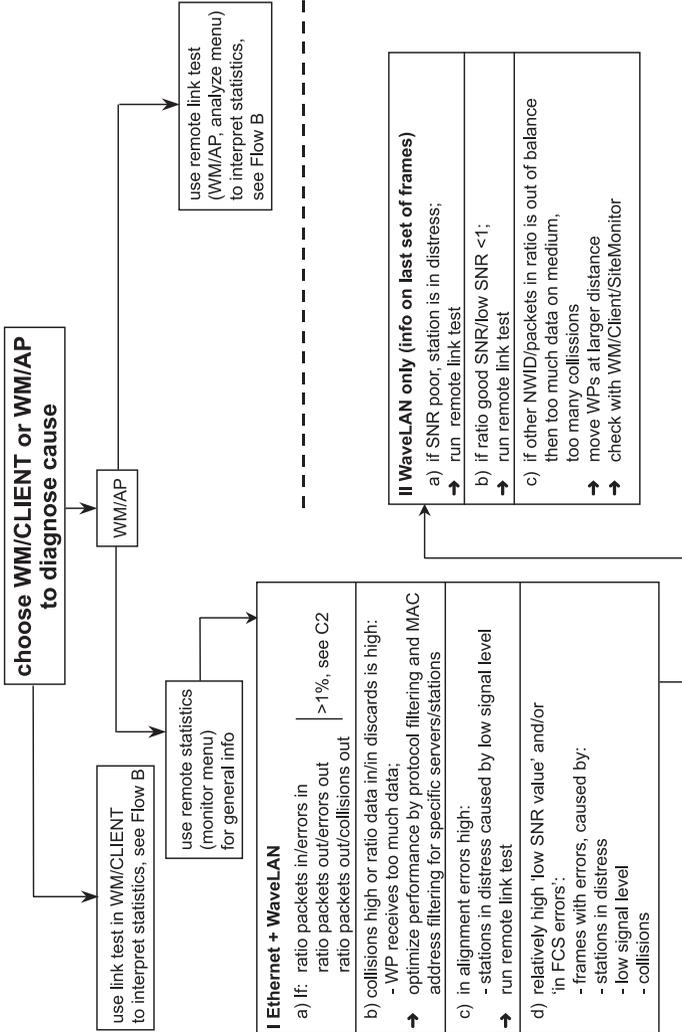


# Troubleshooting

## Problem Determination

---

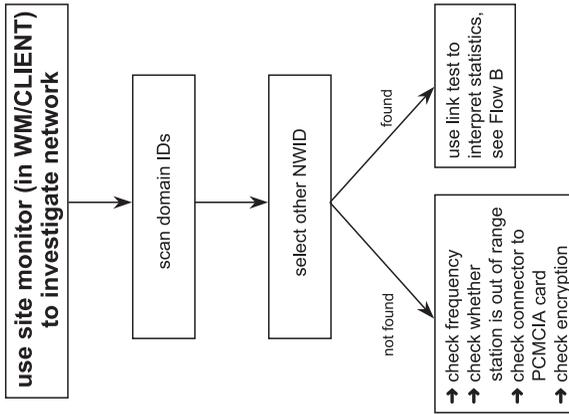
## Flow C1, poor performance reported



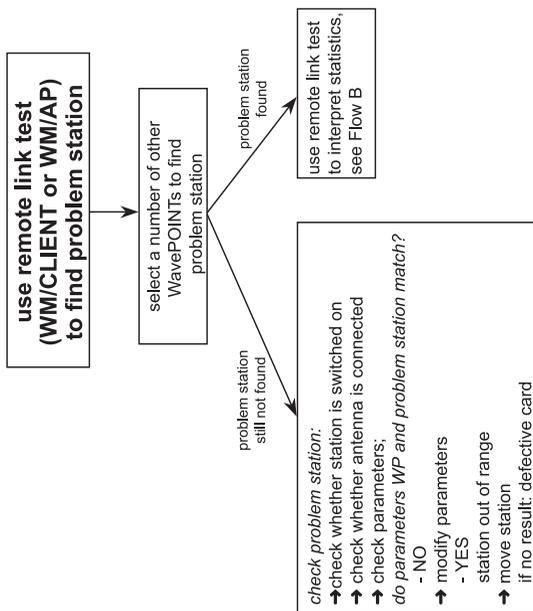
### Flow C2, poor performance reported (cont.)

ratio >1%	
a) Ethernet interference	<ul style="list-style-type: none"> <li>- check cables and connectors</li> <li>if problem with only 1 WP;</li> <li>&gt; problem in connection between WP and backbone</li> <li>if problem with several WPs;</li> <li>&gt; problem on backbone, bridge or router</li> </ul>
b) WaveLAN interface	<ul style="list-style-type: none"> <li>- check for 1 or more stations (almost) out of range which disturbs overall statistics</li> <li>&gt; run remote link test to identify station, and troubleshoot station</li> </ul>

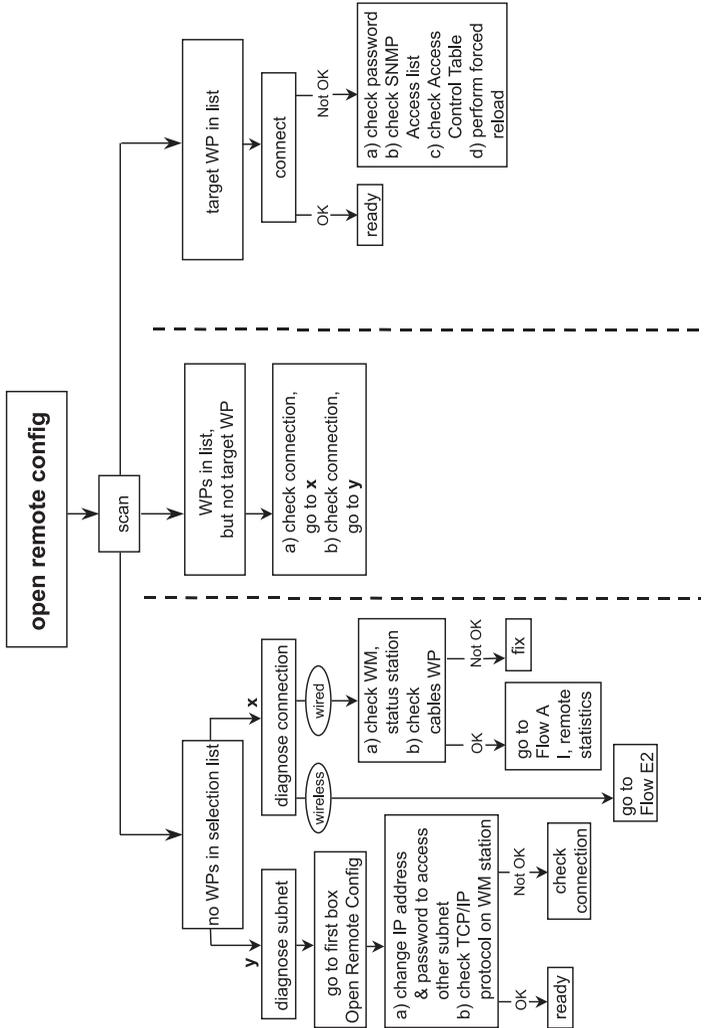
**Flow D1, problem station cannot connect to WavePOINT**



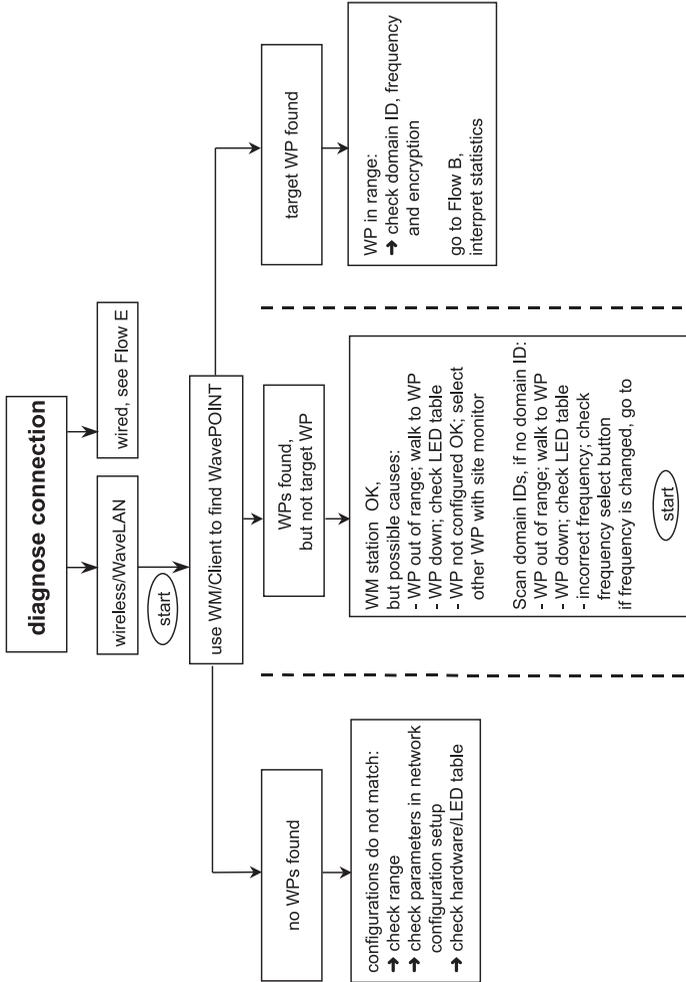
**Flow D2, remote WavePOINT cannot connect to problem station**



**Flow E1, WM management station tries to access WavePOINT**



**Flow E2, diagnose wireless connection**



## LED Error Table

Power	Ethernet	WaveLAN A	WaveLAN B	Error Description	Action:
Continuous Green	Flicker Green	Flicker Green	Flicker Green	none, normal operation where flickering indicates interface activity	none
Continuous Green	Off	Off	Off	none, no LAN activity	none
Off	Off	Off	Off	no power	Check power cord connection, check power supply
Continuous Green	Flicker Green	Amber		network overload, ethernet sends more traffic to	Check network, (see WaveMANAGER/AP
Continuous Green	Flicker Green		Amber	wireless stations than the wavepoint bridge can forward to the wireless	Remote Statistics performance:
Continuous Green	Green	Amber	Amber	side (>2mb/s). Normally wavepoint will buffer such requests, in this situation the buffer is full, packets ignored	Watch the Unicast/Non-Unicast tallies (multicast, broadcast), redundant protocols, set storm threshold, eliminate defect ethernet station

Continuous Green	Red	Don't Care	Don't Care	frames are rejected because of unknown cause	Check WaveMANAGER/AP Remote Statistics for packet errors. If Packets Lost is relatively high, run a Link Test to determine the problem station. and investigate the cause.
Continuous Green	Don't Care	Flash Red	Don't Care		
Continuous Green	Don't Care	Don't Care	Flash Red		
Amber	Off	Off	Off	Forced Reload, state	Proceed with forced reload as described in user documentation
Amber	Flicker Green	Off	Off	Forced Reload, state activity sensed on LAN interface, probably the WaveMANAGER/AP	
Amber	Off	Flicker Green	Off	station that is performing the forced reload.	
Amber	Off	Off	Flicker Green		
Amber	Amber	Amber	Amber	Forced Reload, state	
Red	Don't Care	Don't Care	Don't Care	Hardware Failure	Reset, if problem persists contact support
Don't Care	Red	Don't Care	Don't Care	Ethernet Failure	Reset, if problem persists contact support
Don't Care	Don't Care	Red	Don't Care	Wavelan Failure	Reset, if problem persists contact support
Don't Care	Don't Care	Don't Care	Red	Wavelan Failure	Reset, if problem persists contact support

## Miscellaneous problems

---

### Time-Out Error

---

The message 'Time out error' may be displayed when you try to connect to a WavePOINT from the 'File' menu or the 'Monitor' menu. This message is displayed when:

- You have entered an incorrect IP address.
- You have entered an incorrect password, or entered a 'Read' password where a 'Read/Write' password was required.
- The WavePOINT is switched off or out of order.
- Your Management Station is not listed in the SNMP IP Access List.
- When WaveLAN parameters are incorrectly set.

### WavePOINT-II Resets Continuously

---

A reset of your WavePOINT-II access points can be observed in two ways:

- Noticing strange LED activity at the location where the WavePOINT-II was installed.
- Using the WaveMANAGER/AP program, where the 'Uptime' field in the monitoring windows shows a date and time that is much shorter than expected (e.g. 1 hour instead of 5 days).

In exceptional cases, such as a cable problem on the wired infrastructure, the network may generate an excessive amount of error messages. The WavePOINT-II memory buffer may not be able to handle this excessive traffic, causing your WavePOINT-II unit to:

## Troubleshooting

### Miscellaneous problems

---

1. Reset spontaneously to clear the memory buffers.
2. Perform start-up diagnostics characterized by a LED sequence (LEDs will change color in the range Amber, Red and Green).
3. And, when finished (after approximately 60 seconds), the WavePOINT-II will start a bridging operation using your last configured settings.

When the WavePOINT-II unit remains in spontaneous reset mode, you may need to first solve the network cable problem.

- When the WavePOINT-II device is not connected to a wired cabling system (i.e. you use the bridge with two WaveLAN interfaces only) place a terminator on the 10Base2 connector of the WavePOINT-II device. A terminator is included with each WavePOINT-II kit.
- When the WavePOINT-II device is connected to a 10Base2 cabling system (i.e. a thin coax with BNC connectors) make sure that terminators are placed on both ends of the Ethernet cable.



---

# Forced Reload Procedure

# B

---

## Introduction

---

A Forced Reload allows you to recover from a situation where:

- The WavePOINT-II has stopped responding to the system
- You have mislaid the unique identifiers such as IP Address, SNMP Read/Write password, or other parameters that prevent communication with the WavePOINT-II device.
- The WavePOINT-II has been configured with an incorrect NWID, Beacon Key or Encryption Key or other WaveLAN(-I) parameter, preventing you to access the unit via the WaveLAN(-I) interface.

Upon a Forced Reload, the unit will clear the Flash ROM that contains all configurations settings and switch to a 'Forced Reload' mode. The unit will stop bridging operation and program the FlashROM to use the parameter settings of the Forced Reload Configuration (see Table B-1 on page B-7).



### **NOTE:**

The parameter settings of the Forced Reload configuration are not identical to the 'out-of-the-box' configuration. To access a WavePOINT-II unit in 'Forced Reload' mode, you may need to reconfigure your WaveMANAGER/AP station to match the Forced Reload Configuration Settings as listed in Table B-1 on page B-7.

## Forced Reload Procedure

### Introduction

---

For example when your WaveMANAGER station is a WaveLAN station, modify the NWID, and Operating Frequency of your WaveMANAGER station according to the settings in Table B-1 on page B-7.



#### **CAUTION:**

*When you need to perform a Forced Reload, please keep in mind the following:*

- a. *WavePOINT-II access points equipped with IEEE 802.11 WaveLAN interfaces that are set to 'Forced Reload' mode can not be accessed via the IEEE 802.11 WaveLAN interface.*
- b. *Do not perform a 'Forced Reload' procedure for more than one WavePOINT unit simultaneously. You risk unexpected administrative problems due to configuring multiple units with an identical configuration image and IP Address.*

When your WavePOINT-II access points are equipped with IEEE 802.11 WaveLAN cards only, you may either wish to:

- Insert a WaveLAN(-I) card into the unit, prior to starting the Forced Reload procedure, or
- Perform the 'Forced Reload' procedure using one of the configuration scenario's described in your "WavePOINT-II Getting Started" manual.

## **Performing a Forced Reload**

---

### **1 - Preparations**

---

A Forced Reload procedure can only be performed when you have physical access to the WavePOINT-II unit.

- Familiarize yourself with the location of the WavePOINT-II unit. Do you need special equipment to access the unit, such as a ladder or keys to get into the room where the unit is located?
- Do you have a back-up copy of the unit's current configuration file (\*.cnf)?
  - If Yes, you can use the back-up copy to restore the original configuration.
  - If No, you will need to set all the user-defined parameters for the WavePOINT-II that apply in your network again.

Back-up copies may have been created upon initial installation using the 'Save Config File As' option using the WaveMANAGER/AP program.

- If you have access to the WaveLAN website, you can download the latest software (\*.bin) available for your WavePOINT-II unit. Did you check the WaveLAN website?
- Does the configuration of your WaveMANAGER/AP station enable you to logically access the WavePOINT-II?
  - If your WaveMANAGER/AP is a WaveLAN station, see "WaveMANAGER/AP is a WaveLAN Station" on page B-4.
  - If your WaveMANAGER/AP is a wired (Ethernet) station, see "WaveMANAGER/AP is a Wired Station" on page B-5.

**WaveMANAGER/AP is a WaveLAN Station**

Access to a WavePOINT-II unit in 'Forced Reload' mode is not possible using the IEEE 802.11 WaveLAN interface.

- Direct wireless access is possible only via a WaveLAN(-I) interface, i.e. both WavePOINT-II and the WaveMANAGER station should be equipped with a WaveLAN(-I) adapter card.
- Alternatively you can access the WavePOINT-II unit via an indirect, wireless access option. Consult your "WavePOINT-II Getting Started" manual for further information.

Subject to the type of configuration scenario you prefer, make sure that your WaveMANAGER station matches the settings of the WavePOINT-II access point that you will use to establish the connection.

- Make sure the WaveMANAGER/AP station is within range of the WavePOINT-II unit.
- When using a WaveLAN(-I) interface, adjust the operating frequency and NWID parameters of your WaveMANAGER/AP station to match the WavePOINT-II unit.
- Familiarize yourself with the Forced Reload configuration parameter settings as listed in Table B-1 on page B-7.
- When using IP addressing, write down the (new) IP Address that you would like to assign to the WavePOINT-II unit in Forced Reload mode.

## Forced Reload Procedure

### Performing a Forced Reload

---

#### WaveMANAGER/AP is a Wired Station

If your station is connected to the WavePOINT-II unit via the Ethernet interface of the WavePOINT-II unit.

- Make sure the WaveMANAGER/AP station and the WavePOINT-II unit are connected to the same LAN segment (subnet).  
To communicate with a WavePOINT-II unit in 'Forced Reload' mode, no routers are allowed between the target WavePOINT-II unit and the WaveMANAGER/AP station.
- Familiarize yourself with the other forced reload configuration parameter settings of WavePOINT-II (see Table B-1 on page B-7).
- When using IP addressing, write down the IP Address that the WavePOINT-II unit should use.

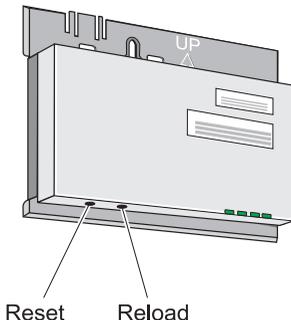
#### 2 - Set the Unit to 'Forced Reload' Mode

---

1. Remove the cover of the WavePOINT-II unit.
2. Locate the two small holes on the long-edge side of the processor module, marked 'Reset' and 'Reload'.

---

**Figure B-1** Reset and Forced Reload Buttons



## **Forced Reload Procedure**

### **Performing a Forced Reload**

---

3. Use a small pointed object, such as the tip of a ball-point, to press the 'Reset' button.
4. Release the 'Reset' button and wait 5 seconds. The WavePOINT-II unit will perform start-up diagnostics, characterized by a LED sequence, where the LEDs will change color in the range Amber, Red and Green'
5. After approximately 5 seconds, use the small pointed object again to press the 'Reload' button for approximately 30 seconds. You will see the LEDs changing color in the range Amber, Red and Green again.
6. When all LEDs turn Amber, release the Reload button. The Power LED turns to Amber. Other LEDs will be off, or may flicker Green to indicate LAN activity on the associated interface.

### **3 - Open The WavePOINT-II Software File**

---

1. Start the WaveMANAGER/AP program.
2. Select 'Open Config File...' from the 'File' menu.
3. Move to the directory where you have installed the WaveMANAGER/AP program.  

If you downloaded the latest WavePOINT-II software from the WaveLAN website, select the directory where you saved the downloaded file.\*).
4. Select the file wpntxxx.bin, (where 'xxx' identifies the version of the WavePOINT-II software).
5. Click the 'Open' button to open the WavePOINT-II software.
6. Proceed with "4 - Modify WavePOINT-II parameters" on page B-8.

**Table B-1 WavePOINT-II Forced Reload Configuration**

**WavePOINT-II Identifiers**

IP address	153.69.254.254 <sup>1</sup>
Read Password	'public'
Read/Write Password	'public'

**WaveLAN(-I) Interface**

RF-Channel	2.4 GHz <sup>2</sup>	2.460 MHz	France
		2.484 MHz	Japan
		2.422 GHz	All other countries
	915 MHz	915 MHz	Americas only
WaveLAN Network Name	Domain ID	0000	Roaming disabled <sup>3</sup>
	Beacon Key	0000	Key disabled
Wireless Cell ID	NWID	AAAA	For WaveLAN(-I) card in slot 'A'
		BBBB	For WaveLAN(-I) card in slot 'B'
Encryption key	0 <sup>4</sup>	Encryption disabled	

**IEEE 802.11 WaveLAN Interface**

The WavePOINT-II device does not support a 'Forced Reload' configuration for IEEE PC Cards inserted into your WavePOINT-II

- 1 When using IP networks, change the initial IP address to a unique address in the range assigned to your organization.
- 2 These values apply to new WaveLAN/PCMCIA Kits. When you use a previously installed kit, verify or correct the current operating frequency using the WaveMANAGER/AP program.
- 3 This parameter deviates from the factory set configuration, to avoid other roaming stations from unintentionally connecting to a WavePOINT-II unit in Forced Reload mode.
- 4 Only when the WaveLAN/PCMCIA Kit has a factory installed Security Feature.

## **4 - Modify WavePOINT-II parameters**

---

When performing a Forced Reload, you will need to set the configuration parameters for the WavePOINT-II unit again:

- When you have a previously saved back-up file of the unit's configuration file (\*.cnf), you can use the 'Import Config File' option from the 'File' menu, to copy all the parameter settings of the unit into the WavePOINT-II software file (\*.bin).
- If you do not have such a file, you will need to configure the WavePOINT-II unit manually as you would do upon initial installation, i.e. assign a unique IP Address, setup the WaveLAN parameters and, (if applicable) the other WavePOINT-II identifiers such as the IP Address and SNMP Access List (see "SNMP IP Access" on page 6-12).



**NOTE:**

Always check the parameter settings when you import a configuration file to verify that you have imported the correct file for the target WavePOINT-II unit.

Configuring a WavePOINT-II unit with a configuration file that is identical to the configuration of another unit may lead to unpredictable behavior of your WaveLAN network.

## **5 - Upload the Software and Configuration**

---

Once you have restored the configuration parameters for the WavePOINT-II unit, you can upload the WavePOINT-II software file and the configuration file to the WavePOINT-II unit that is in 'Forced Reload' mode.

1. From the 'File' menu, select 'Upload Software...'

## Forced Reload Procedure

### Performing a Forced Reload

---

2. When prompted for the IP Address, click the 'Scan' button, to look for the target WavePOINT-II unit, that can be identified by the factory set IP Address.



#### **NOTE:**

The Scan option does not work over routers. Make sure your WaveMANAGER/AP station is on the same subnet as the WavePOINT-II unit that is in 'Forced Reload' mode.

3. Select the target WavePOINT-II unit from the list displayed.
4. Click the 'Change IP Address' button to modify the factory set IP Address into a (new) IP Address for this unit. This should be a unique IP Address in your network.

The WaveMANAGER/AP will assign the IP Address to the WavePOINT-II unit that is in 'Forced Reload Mode'.

5. Click OK. The WaveMANAGER/AP program will return to the 'Scan' menu and refresh the list of WavePOINT-II access points. Your WavePOINT-II should now be listed with the new IP Address that you assigned to the unit.
6. Select the WavePOINT-II again, and click OK to return to 'Enter IP Address' dialog box.
7. Verify that the IP Address displayed in the 'Remote IP Address' field is correct. Failing to do so may adversely affect the configuration of another WavePOINT-II unit.
  - If the IP Address displayed is not the IP Address you assigned to the unit in 'Forced Reload' mode, return to the 'Scan' menu to select the correct WavePOINT-II unit.
  - When the IP Address is correct, click OK again.
8. When prompted to confirm the 'Reload of the Remote System', check the list of parameters displayed once again.
  - If the pop-up window does not display the correct IP Address and/or SNMP passwords click 'No' to cancel.
  - If the IP Address and/or SNMP passwords are correct, click 'Yes' to proceed.

## **Forced Reload Procedure**

### **Performing a Forced Reload**

---

9. The WaveMANAGER/AP program will upload the new (restored) configuration to your WavePOINT-II access point. The WavePOINT-II unit will reboot and start bridging operation in approximately 60 seconds.

## **6 - Finishing the Forced Reload**

---

(Optional) Use the 'Save Config File as...' option, to save the configuration parameters of the WavePOINT-II unit to a back-up file (\*.cnf). Save the back-up file under a name that allows for easy identification in the future.

You are advised to do so now, to anticipate future network errors that might force you to perform a Forced Reload procedure in the future.

## **Start-up Diagnostics**

When powered on, the WavePOINT-II unit will perform start-up diagnostics characterized by a LED sequence, where the LEDs will change color in the range of Amber, Red and Green.

The start-up diagnostics take approximately 60 seconds. When finished, the WavePOINT-II unit will start bridging operation characterized by the LED activity. For more information on the start-up sequence of the WavePOINT-II, see your "WavePOINT-II Getting Started" manual.

---

# WavePOINT-II Configuration Record



---

## Start-Up Configuration

---

When unpacking your WavePOINT-II access points, you are advised to register the unit's Serial Number and MAC address, printed on a small label at the unit's processor module.

You will need these numbers to identify the unit when running the WaveMANAGER/AP program or in situations where you need to consult WaveLAN Technical Support.

---

**Figure C-1 WavePOINT-II Identification Label**



When you power-up your WavePOINT-II unit for the first time, the unit will start bridging operation using the parameter settings as listed in Table C-1 on page C-2.

If you decide to change the factory-set configuration, always register the modified configuration parameters in the 'WavePOINT-II Configuration Record' printed.

# WavePOINT-II Configuration Record

## Start-Up Configuration

---

**Table C-1 Factory-set Configuration for WavePOINT-II**

RF-Channel	2.4 GHz	France	2.460 GHz
		Japan	2.484 GHz
		All other countries (including Americas)	2.422 GHz
	915 MHz	Americas only	915 MHz
Domain ID	0001	(Roaming enabled)	
Beacon Key	0000	(No encoding of NWID information)	
NWID	<b>Sxxx</b>	<b>S</b> identifies the PCMCIA Socket of the WavePOINT unit (A or B), you selected to insert the WaveLAN/PCMCIA Card.  <b>xxx</b> represent the last three digits of the unit's Serial number (see Figure C-1 on page C-1).	
Encryption key	0 <sup>1</sup>	(no encryption)	
IP address	153.69.254.254 <sup>2</sup>		

- 1 Only when the WaveLAN/EAM Kit has a factory installed Security Feature
- 2 When using IP networks, change the initial IP address to a unique address in the range assigned to your organization.





---

# Glossary

---

## A

### **Access Control**

A security feature for WavePOINT access points that enables you to restrict wireless access to a WavePOINT-II to authorized stations only.

Authorized stations are identified by the MAC address of their WaveLAN card in a so-called 'Access Control Table' file that is loaded into the WavePOINT access points as part of the configuration

When Access Control is enabled, the WavePOINT will ignore all requests to forward data to/from WaveLAN devices that are not identified in the Access Control Table. You can create or edit Access Control Table files using either the WaveMANAGER/AP or the WaveMANAGER/CLIENT program.

*See also: Chapter 4 Security*

### **Ad-hoc Workgroup**

A stand-alone workgroup of wireless stations which participate in a small (peer-to-peer) network. This is typically a WaveLAN network configuration without WavePOINT access points that could connect the stations into a network infrastructure.

The workgroup is identified by a unique NWID that is agreed upon by the workgroup participants. To connect to the workgroup each station must be configured with the agreed NWID. As the workgroup does not include WavePOINT access points, the stations can disable roaming (i.e. a Domain ID is not required).

### **AES (Advanced Encryption Scheme)**

A Lucent Technologies proprietary data encryption scheme to encrypt data that is transmitted via the wireless medium. The AES encryption scheme is similar to the DES encryption scheme. WaveLAN products are available with factory-installed AES security features for export to all countries.

*See also: Chapter 4, Security*

### **Analysis Polling interval**

A parameter that enables you to control the responsiveness of the WaveMANAGER/AP Remote Link Test. The Analysis Polling Interval determines how often WaveMANAGER/AP will read the diagnostic tallies of the bridge unit. Valid values: 1-15 seconds.

*See also: Chapter 4, Monitoring*

### **Antenna (external)**

You can use WavePOINT-II in combination with an external antenna to connect two or more buildings. To connect the external antenna to the WavePOINT-II access point, the WavePOINT-II unit must be equipped with the WaveLAN External Antenna Module (WaveLAN/EAM).

---

## **B**

### **Basic Access Network**

A basic access network consists of a small sized wireless LAN, with no connections via gateways or routers. The number of WavePOINT-II access points in this network typically varies between 1 and 5. The administrator stations need to have the TCP/IP protocol stack loaded and use IP addressing to configure and monitor the WavePOINT access points. IP addressing and the TCP/IP protocol are not strictly necessary for client stations.

### **Glossary**

A message that is transmitted at regular intervals by the WavePOINT access points to all wireless stations in the domain. Beacon messages are used to maintain and optimize communications by helping mobile WaveLAN stations to automatically connect to the WavePOINT that provides the best communications quality.

A beacon message contains the Domain ID, the NWID of the transmitting WavePOINT, information about the communications quality at the WavePOINT and communications quality threshold values.

### **Beacon Key**

A four-digit code that provides extra protection against eavesdropping of NWID information included in the beacon messages. You can set the beacon key in the WavePOINT configuration. To allow WaveLAN stations to decode the NWID information, you will need to configure the stations with the same beacon key.

A beacon key consists of four hexadecimal numbers in the range 0-9, A-F.

*See also: Chapter 4, Security*

### **BOOTP (Bootstrap Protocol)**

The standard protocol that is used to configure systems across internetworks.

### **Bridge in**

The total number of data packets arriving at the WavePOINT from the LAN segment served by the selected WavePOINT interface.

This number reflects the sum of Unicast and Non-Unicast packets.

*See also: WaveMANAGER/AP, Monitoring, Remote Statistics*

### **Bridge in discards**

The number of data packets not accepted by the WavePOINT.

*See also: WaveMANAGER/AP, Monitoring, Remote Statistics*

### **Bridge out**

The number of data packets that have been forwarded by the WavePOINT to the LAN segment served by the selected interface.

*See also: WaveMANAGER/AP, Monitoring, Remote Statistics*

### **Bridge Priority**

A Bridge setup parameter that enables you to influence the choice of the 'Root Bridge' and the 'Designated Bridge' as calculated by the Spanning Tree Algorithm. A low numerical value of the Bridge Priority Parameter makes the bridge more likely to become the designated bridge or Root Bridge (typically '0'). The recommended value is '32768'. Valid values: 0-65000, Initial value: '32768'.

*See also: WaveMANAGER/AP, Setup Bridge Parameters*

### **Broadcast**

Messages transmitted by a single station (typically a server) to all stations on the network. This type of traffic is also referred to as Non-Unicast messages.

### **Bytes in**

The number of bytes (octets) received at the WavePOINT from the LAN segment served by the selected WavePOINT interface, including framing characters.

*See also: WaveMANAGER/AP, Monitoring, Remote Statistics*

### Bytes out

The number of frames requested by higher level protocols that are to be transmitted to a Non-Unicast address (i.e. a subnetwork broadcast or subnetwork Multicast address). This number includes the frames that were discarded or not sent.

*See also: WaveMANAGER/AP, Monitoring, Remote Statistics*

---

## C

### Collisions

The number of packets that were not received properly as a result of a collision, due to multiple stations trying to send packets over the medium simultaneously.

*See also: WaveMANAGER/AP, Monitoring, Remote Statistics*

---

## D

### DES (Data Encryption Standard)

A data encryption scheme to encrypt data that is transmitted via the wireless medium. DES has been defined by the US department of Commerce, National Institute of Standards and Technology (NIST), formerly called the National Bureau of Standards (NBS).

The use of DES encryption is limited to usage within the USA only. Export outside the USA is limited by the Department of Commerce to financial institutions.

WaveLAN products are available with factory-installed DES security features. For other countries Lucent Technologies

offers WaveLAN products with factory-installed AES Encryption.

*See also: Chapter 4, Security*

### **DHCP (Dynamic Host Configuration Protocol)**

DHCP is a Microsoft proprietary extension to the existing bootstrap protocol (BOOTP). DHCP enables a LAN administrator to have a network server configure workstations with an IP address dynamically without further intervention.

A dynamically assigned IP address is referred to as an 'Active Lease'. The Active Lease usually has an expiry date, which allows re-allocation of IP addresses that are no longer used.

For WavePOINT access points you are advised to use a specific IP address for which there is no expiry date. To do so, you can use your DHCP management program to reserve the IP address or a range of IP addresses.

For network devices that require a specific IP address, or for which you do not want the 'IP address lease' to expire, you can use a DHCP Management program to reserve their IP addresses. This is the case with your WavePOINT-II access points.

Once a range of IP addresses has been reserved, you can use the values in this range to assign to your WavePOINT-II system.

The Unique Identifier is the Media Access Control (MAC) address for the DHCP Client. The Client Name should be the computer name for the DHCP Client. However, this name is used for identification purposes in the DHCP Manager interface and, therefore, does not have to be and will not affect the actual computer name.

To see which IP addresses are still available, your DHCP Management program will usually include a 'Scope Active

Leases' option. This option allows you to see which DHCP Clients have leased an IP address from the DHCP Server.

### **Domain**

A logical group of wireless cells that belong to the same network. This group of cells is identified by a common identification designator called 'Domain ID'. Within a domain WaveLAN devices can roam between different wireless cells, connecting automatically to the WavePOINT that provides the best communication quality.

### **Domain ID**

A four-digit code that 'logically' connects multiple wireless cells into one wireless coverage area, the Domain.

Where each cell is identified by the unique NWID of the WavePOINT, the Domain ID determines which cells belong to the group of cells.

A Domain ID consists of four hexadecimal numbers in the range 0-9, A-F.

---

## **E**

### **Encryption**

A security feature for WavePOINT access points and WaveLAN stations that enables you to encrypt data that is transmitted via the wireless medium.

WaveLAN products are optionally available with a factory-installed encryption chip that is based on either the AES or DES encryption algorithm.

To use encryption in your wireless network, all WaveLAN stations and access points must have the encryption feature installed and set to 'Enable'. All WavePOINTS and

WaveLAN devices in the network environment must use the same encryption key.

The encryption key consists of 16 hexadecimal numbers in the range 0-9, A-F. The second digit of each pair must be even (0,2,4,6,8,A,C,E).

### **Enterprise-wide Network**

A network configuration that has the scale of a corporate LAN. This type of network may include network segments in different departments, interconnected by means of bridges and routers. When the network comprises gateways, routers or bridges, each network device must be identified by a unique IP address. The network may extend to wireless networking in different buildings, where the buildings are connected by a wired link, e.g. a leased line.

---

## **F**

### **Filter Aging Time**

WavePOINT-II access points maintain dynamic lists to identify the interface where they last spotted a WaveLAN station (either the Ethernet interface, or WaveLAN interface A or B).

When the WavePOINT receives a packet addressed to a specific station, this list will help to determine to which interface the packet should be bridged.

When mobile stations roam between multiple cells this table will be updated automatically.

When there is no traffic from or to a specific station for a longer period of time (for example when a station was shut down), the Filter Aging Time determines how long the WavePOINT will 'remember' the location of this WaveLAN device.

### **Firmware**

The Firmware (also referred to as 'Bridge Kernel') is the factory-installed basic operating software for your WavePOINT-II access points.

Firmware upgrades may become available when new functions or features are developed for the WavePOINT-II access point.

The firmware is stored in a binary file of the format 'wp2\_vxxx.bin', (where 'xxx' identifies the version of the firmware).

You can use the 'Upload Firmware' option of your WaveMANAGER/AP program (File Menu) to load the new firmware into the FlashROM of your WavePOINT-II access points.

### **Forward Delay**

A timer for the 'Spanning Tree Algorithm' that prevents a bridge to forward data packets when:

- \* the bridge receives information that the active Spanning Tree topology must be updated (for example when a bridge breaks down or when somebody modified the 'Bridge Priority' or 'Path Cost' value of a particular bridge);
- \* the bridge registers that the protocol information exceeds the specified 'Max. Age' value.

Changes in the Spanning Tree topology must be communicated to all bridges in the bridged network. The Forward Delay timer will compensate for the propagation delays that occur in passing the protocol information, allowing all bridges to close the old data paths, before the new data paths are activated.

Recommended value: 15 seconds

---

### H

#### Hello Time

A Spanning Tree parameter that identifies the time interval between Configuration BPDU messages as transmitted by a root bridge or a bridge that is attempting to become the root bridge.

Recommended value: 2 seconds.

---

### I

#### Initiator Station

The (remote) WavePOINT-II device that you selected to initiate a Remote Link Test with a wireless station connected to the selected WavePOINT-II access point.

The Remote Link Test Partner can either be a WaveLAN station, or (in case of an outdoor antenna link) another WavePOINT unit.

#### IP Address

The Internet Protocol (IP) address is a unique addressing code for computing devices. When your network already uses IP addressing, you must change the factory-set IP address to a value selected from the range of IP addresses assigned to your organization.

---

### K

#### Kernel

*See 'Firmware'*

### L

#### **LAN Segment**

A logical area within a network that is connected with other areas via a bridge.

For WavePOINT access points, these areas can either be an Ethernet or a WaveLAN segment. For WavePOINT-II access points there could even be two WaveLAN segments (A and B). Each WaveLAN segment is identified by a unique NWID.

#### **Link Test**

A WaveLAN Diagnostics option that enables you to investigate a specific link between two wireless stations.

You can use the Link Test to analyze the quality of the wireless communication, and to determine or optimize the placement of stations and antennas.

---

### M

#### **MAC Address Filter**

An advanced Bridge Setup parameter for WavePOINT-II that enables you to deny data traffic between two specific devices via the WaveLAN interface(s) of the WavePOINT bridge.

You can use the Static MAC Address filter to optimize the performance of a wireless (and wired) network.

For example, to prevent redundant traffic from being transmitted over the wireless network, you could deny traffic between two particular servers, identified by their MAC

Address and their location as perceived by the WavePOINT (on the 'wired' or wireless' port of the bridge).

In most situations, however, it will be easier to control redundant traffic via other filtering options, such as 'Protocol Filtering.

### **Max Age**

An advanced Bridge Setup parameter for WavePOINT-II that identifies the maximum age of received Spanning Tree protocol information.

When the bridge receives protocol information that exceeds the Max Age value, the bridge will discard the information and start the Forward Delay timer to allow other bridges to forward updated topology information, e.g. that another bridge has become the Root Bridge.

Recommended value: 20 seconds.

### **Multicast**

Messages transmitted by a single station (typically a server) to multiple stations on the network. This type of traffic is also referred to as Non-Unicast messages.

### **Multicast Mechanism**

In network environments that include several WavePOINTS, the Multicast Mechanism avoids frame collisions when several WavePOINTS try to access the wireless medium at the same time, for example in case of messages that are transmitted from one station to multiple stations (Multicast) or all stations (Broadcast) on the network.

The default Multicast Mechanism generates a random delay for each WaveLAN Interface of a WavePOINT. The random

delay is based on the last digits of the MAC address of the inserted WaveLAN Card.

Optionally you can define a 'User-defined' Multicast delay in the range of 1-10.

*See also: WaveMANAGER/AP Setup WaveLAN Parameters*

---

## N

### **Network ID**

*See NWID*

### **Noise Level**

The Noise level is the level of local background noise as measured at the WaveLAN interface of a WavePOINT. The Noise level counter reflects only the Noise Level value (in %) of the latest frame that was received on the interface.

*See also: WaveMANAGER/CLIENT Link Test*

### **Non-Unicast packets in**

The number of Non-Unicast packets delivered to a higher protocol, typically Multicast or Broadcast messages.

*See also: WaveMANAGER/AP Remote Statistics*

### **Non-Unicast packets out**

The number of packets requested by higher level protocols, to be transmitted to a subnetwork-unicast address, typically Multicast or Broadcast messages. This number includes the frames that were discarded or not sent.

*See also: WaveMANAGER/AP Remote Statistics*

### NWID

A Network Identification Designator, also referred to as Network ID.

The NWID is a four-digit code, which is used to logically group and connect WaveLAN devices in a wireless group (cell), like cabling physically connects stations, in a wired network.

Each cell is identified by a unique NWID. Within the cell, all WaveLAN devices must use the same NWID, to distinguish the data traffic in their cell from wireless traffic in other cells in the vicinity.

In ad-hoc configurations the NWID is a random value as agreed upon by the workgroup participants.

In WaveLAN infrastructures the NWID of the cell is determined by the NWID of the WavePOINT that connects the wireless cell to the rest of the network.

The NWID code consists of four hexadecimal numbers in the range 0-9, A-F.

---

## O

### Out Collisions

The number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one or more collisions plus the number of collisions detected on a particular interface later than 512 bit-times into the transmission of a packet.

*See also: WaveMANAGER/AP Remote Statistics*

### P

#### **Packets received/lost**

The 'Packets received/lost' counter displays the percentage of packets received relative to the number of packets expected. The 'packets received/lost' counter is only displayed when you select the View Details option.

*See also: WaveMANAGER/CLIENT Link Test*

#### **Path cost**

An advanced Bridge Setup parameter for WavePOINT-II that is used to determine the preferred data paths between bridges throughout the network and the root bridge as calculated by the 'Spanning Tree Algorithm.

The 'Root Bridge' transmits BPDU messages throughout the Local Area Network. When a bridge unit receives a BPDU message at one of its ports, it will add the value in the 'Path Cost' field for that port to the value in the 'root path cost field' of the BPDU message prior to forwarding the message again. This will help the other bridges to determine the 'Total Path Cost' to the Root Bridge via this port.

A lower 'Path Cost' value would typically be used for ports to LAN segments closer to the Root Bridge. A higher 'Path Cost' value would typically be used for ports to LAN segments that are 'the leaves' of the Spanning Tree.

For example, when you use the WavePOINT-II as an access point for wireless stations to the Ethernet, a high 'Path Cost' for the WaveLAN port will minimize unnecessary use of the bandwidth for the wireless medium (recommended value 500).

When you use WavePOINT-II units in a wireless point-to-point link to interconnect two LAN segments, a low 'Path Cost' for the WaveLAN port will prioritize this link as

compared to other physical links, such as a leased line or low-bandwidth connections.

Valid values: 0-255. Initial value: '100'

### **Point-to-Point Link**

A wireless connection between two or more remote locations, such as multiple buildings on a campus location.

In (outdoor) point-to-point link configurations, you will typically use two or more WavePOINT units that have been equipped with WaveLAN/EAM and external antennas.

The wireless interfaces on both ends of the antenna link must be configured with an identical NWID.

### **Point-to-Point Diagnostics**

An MS-DOS based WaveLAN Diagnostics utility, similar to the WaveMANAGER/CLIENT Link Test.

### **Port Priority**

An advanced Bridge Setup parameter for WavePOINT-II that enables you to influence which port should be included in the Spanning Tree, when concurrent bridge ports of a single bridge unit are connected in a loop.

A lower value makes a port more likely to become selected in the Spanning Tree than the concurrent one that has a higher numerical value. Valid values: 0-255. Initial value: '128'

---

## **R**

### **Read Password**

A security option that enables you to create a network management level by means of a password.

For example, the 'Read Password' in combination with the correct IP address will authorize a local LAN Administrator to display only the WaveMANAGER/AP Monitor/Analyze

windows for a specific WavePOINT-II, but not to view or modify the WavePOINT-II Configuration.

You can set the 'Read Password' using the SNMP Setup window in the WaveMANAGER/AP program.

### **Read/Write Password**

A security option that enables you to create a network management level, by means of a password.

For example, the 'Read/Write' password in combination with the correct IP address will authorize a Corporate LAN Administrator to display all WaveMANAGER/AP Monitor/Analyze windows and to display or modify the WavePOINT-II configuration.

You can set the 'Read/Write' password using the SNMP Setup window in the WaveMANAGER/AP program.

### **Remote Link Test**

A WaveLAN diagnostics option of the WaveMANAGER/AP program. You can use the Remote Link Test to analyze the Link Quality between a remote WavePOINT-II and a station connected to the selected WavePOINT-II device.

This option is often used to investigate wireless outdoor links, or to analyze the Link Quality of wireless stations in a remote network.

### **Remote Point-to-Point Diagnostics**

An MS-DOS based diagnostic utility similar to the 'Remote Link Test' of the WaveMANAGER/AP program.

### **Responsiveness**

This advanced WaveLAN interface parameter for roaming defines the beacon interval time and time-out value of beacons transmitted by WavePOINT access points. The

time-out value is communicated to all stations in the wireless domain.

When the interval time between received beacons exceeds the time-out value, the WaveLAN station will presume an 'out of range' situation.

In case of a presumed 'out of range' situation, the WaveLAN station will automatically switch to a Fast Cell Search Mode and try to connect to the first available WavePOINT.

All WavePOINT access points must be configured with the same level of Responsiveness. Using different settings throughout the same domain can have unpredictable results.

### Roaming

In a WaveLAN network, each cell is identified by the unique NWID of the WavePOINT. To communicate within that cell, all wireless stations must use the same NWID.

When the wireless network consists of multiple cells, all cells will be grouped into a group of cells that is called the Domain. The Domain ID determines which cells belong to the group of cells.

Roaming is a function that enables mobile WaveLAN devices to migrate between different cells.

The roaming functionality will monitor the communications quality with the WavePOINT access points and, if required, automatically connect to another WavePOINT to maintain the network connection; the WaveLAN driver will automatically change its NWID setting to connect to the new WavePOINT.

Roaming is only possible within one domain, i.e., as long as the mobile station is within range of WavePOINT access points that are identified by the same Domain ID as the WaveLAN station.

### S

#### **Sensitivity**

This advanced WaveLAN interface parameter for roaming defines a set of threshold values that are related to different levels of the Signal to Noise Ratio (SNR). A roaming station will use these thresholds to determine when to hand over to another WavePOINT if the level of SNR decreases.

All WavePOINTS must be configured with the same level of Sensitivity. Using different settings throughout the same domain can have unpredictable results.

#### **Signal Level**

The signal level indicates the strength of the WaveLAN signal as received at the WaveLAN interface.

#### **Signal Quality**

The signal quality indicates the clarity of a received signal. A low value may indicate interference due to signal reflections in special environments, such as buildings with high ceilings and exposed steel structural components.

#### **Site Monitor**

A WaveLAN diagnostics option of the WaveMANAGER/CLIENT program that enables you to display the communications quality of multiple WavePOINT-II units simultaneously. You can use the Site Monitor to investigate the overall coverage of your WaveLAN network, and to perform site verifications.

#### **Site Verification**

A procedure to determine or optimize the placement of your WavePOINT access points.

*See also: Site Monitor, WaveMONITOR*

### **SNMP (Simple Network Management Protocol)**

A standard network protocol that can be used to manage networks locally, or worldwide via the Internet.

### **SNMP IP Access List**

An advanced Security option that enables you to authorize SNMP management to a restricted group of SNMP Management stations.

To authorize a station to access the WavePOINT-II configuration or diagnostic information, you will need to add the IP address of that station to the so-called SNMP IP Access List.

When you enable the SNMP IP access option, the WavePOINT-II will deny all requests to read the configuration data or diagnostic tallies when the IP address of the requesting station is not registered in the SNMP IP access list.

You can use the SNMP IP Access List in combination with other security options such as the 'Read' and 'Read/Write' passwords.

To create or edit the SNMP IP Access List, use the SNMP Setup menu of the WaveMANAGER/AP program.

### **SNMP Polling Interval**

A parameter that enables you to control the responsiveness of the WaveMANAGER/AP Monitor options. Valid values: 1 second - 5 minutes.

### **SNMP Trap Messages**

SNMP trap messages are part of the trap host mechanism which can be used to inform a network administrator when somebody resets a WavePOINT-II unit, loads a new

configuration into the WavePOINT-II, or performs a forced reload procedure.

The trap host alert message will enable the network administrator to verify whether this was an authorized action or not.

To receive the Trap Alert messages, the management station needs to have a standard Trap Host Agent installed to handle the trap messages.

### **SNR (Signal to Noise Ratio)**

The Signal-to-Noise Ratio (SNR) is the primary diagnostic counter to diagnose wireless performance. The SNR indicates the relative strength of the received Signal Level compared to The Local Noise Level.

### **Spanning Tree**

An advanced Bridge Setup option for complex network topologies that enables you to enhance data traffic efficiency and eliminate the possibility of data loops.

With the spanning tree algorithm, all bridges on the LAN exchange special configuration messages that allow them to:

- \* Elect a single bridge among all bridges in the connected LAN segments to be the root bridge.
- \* Calculate the distance of the shortest path to the Root Bridge.
- \* Elect a 'Designated Bridge' in each LAN segment that will forward packets between that LAN segment and the Root Bridge.
- \* Select a 'Root Port' among all ports of the bridge unit.

The spanning tree algorithm enables bridges to calculate a loop-free subset of the LAN topology (a tree) that provides

the most efficient level of connectivity between every pair of physically connected Local Area Network segments.

If the 'shortest data path' fails, (for example as a result of a physical breakdown), the Spanning Tree will automatically rebuild the topology within the confines of the available bridged LAN components.

### **Station address**

The station address is a unique identification designator stored in each WaveLAN card and WavePOINT. The addressing system used for station addresses conforms to the universal MAC addressing convention. The station address is a 12 digit, alphanumeric code, arranged as 6 digit pairs of hexadecimal numbers.

### **Station Name**

The station name is an optional parameter that may be used to designate WaveLAN devices in the network. The name can help to identify a device in one of the WaveLAN diagnostic utilities. A station name can consist of up to 31 alphanumeric characters.

### **Storm Threshold**

An advanced Bridge Setup option that you can use to protect the network against data overload by:

- \* Specifying a maximum number of frames per second as received from a single network device (identified by its MAC address).
- \* Specifying an absolute maximum number of messages per port.

The 'Storm Threshold' parameters allow you to specify a set of thresholds for each port of the WavePOINT-II access point, identifying separate values for the number of

broadcast messages/second and Multicast messages/second.

When the number of frames for a port or identified station exceeds the maximum value per second, the WavePOINT will ignore all subsequent messages issued by the particular network device, or ignore all messages of that type.

### **Subnet**

A subnet is a logical sub-division of a Local Area Network that has been divided by means of routers or gateways. A subnet may include multiple LAN segments.

Each subnet is identified by the Subnet Mask.

Note:

WaveLAN roaming does not work over routers. To allow mobile stations to roam between different wireless cells, all WaveLAN stations and access points must be connected to the same LAN subnet.

---

## **T**

### **TTL (Time-To-Live)**

An advanced IP Parameter Setup counter that you can use to maintain network efficiency. The purpose of the Time To Live counter (TTL) is to avoid endless forwarding of message frames with an incorrect address that pollute the network medium.

The TTL defines a maximum number of passes per hop. Each time the frame is forwarded by a router, the TTL counter decreases by one. When the TTL = 0, the frame is rejected.

### U

#### **Unicast packets in**

The number of subnetwork-frames delivered to a higher protocol. This is 'true data' from station to station.

#### **Unicast packets out**

The number of bytes (octets) transmitted out to the interface.

This is 'true data' from station to station.

#### **Up Time**

The amount of time elapsed since the last time the WavePOINT-II unit was powered up, reset, or uploaded with a new configuration.

---

### W

#### **WaveLAN workgroup**

A group of WaveLAN stations located in the same area, that use the same NWID to communicate with one another or the WavePOINT access point that connects the stations to the network infrastructure. The workgroup participants do not need to be functionally related (e.g. belong to the same department).

#### **WaveMONITOR**

An MS-DOS based WaveLAN diagnostics utility, similar to the WaveMANAGER/CLIENT Site Monitor option.

#### **Windows workgroup**

A Windows workgroup can consist of either wireless or wired network connections or a combination of the two. Usually a Windows workgroup consists of members who are related because of a shared function, e.g. members of

## Glossary

---

the same department. For a Windows workgroup it is not relevant where the workgroup participants are located, since the members of a Windows workgroup are identified by their workgroup name only.



---

## List of Figures

Figure 1-1	Basic Access Network	1-7
Figure 1-2	Enterprise-wide network	1-8
Figure 1-3	Wireless Outdoor Connection	1-10
Figure 2-1	Wireless WaveMANAGER Station	2-3
Figure 2-2	Wired WaveMANAGER Station	2-5
Figure 3-1	Basic Access Network	3-2
Figure 3-2	Scan IP address dialog box	3-4
Figure 3-3	Interface setup dialog box	3-5
Figure 3-4	Setup WaveLAN Interface Parameters	3-6
Figure 3-5	Setup WaveLAN Roaming Parameters	3-7
Figure 3-6	Enterprise-wide network	3-9
Figure 3-7	Setup WaveLAN Interface Parameters	3-15
Figure 3-8	Roaming setup dialog box	3-16
Figure 3-9	Bridge parameters setup dialog box	3-17
Figure 3-10	Spanning tree setup dialog box	3-18
Figure 3-11	Storm threshold dialog box	3-19
Figure 3-12	WavePOINT IP parameters setup dialog box	3-20
Figure 3-13	SNMP setup dialog box	3-22
Figure 3-14	Scan IP address dialog box	3-26
Figure 3-15	Network with an outdoor antenna connection	3-31
Figure 3-16	Omni-directional Point-to-Multipoint	3-32
Figure 3-17	Multiple Directional Point-to-Point	3-33
Figure 3-18	Setup WaveLAN Interface Parameters	3-34
Figure 3-19	Setup Bridge Parameters	3-35
Figure 3-20	Ethernet protocol filter selection dialog box	3-36
Figure 4-1	WaveMANAGER/CLIENT Main Window	4-6
Figure 4-2	Link Test Window	4-8
Figure 4-3	NWID & Station selection dialog box	4-11
Figure 4-4	Site Monitor window	4-13

## List of Figures

---

Figure 4-5	Domain Selection Window	4-15
Figure 4-6	Log setup dialog box	4-18
Figure 4-7	Remote Statistics Window	4-23
Figure 4-8	Select a Link Test Partner	4-29
Figure 4-9	Link Test Window	4-30
Figure 5-1	Dual Band Configuration	5-14
Figure 6-1	WaveLAN Interface parameters	6-4
Figure 6-2	Access Control Setup Dialog Box	6-7
Figure 6-3	Access Control Table Manager	6-9
Figure B-1	Reset and Forced Reload Buttons	B-5
Figure C-1	WavePOINT-II Identification Label	C-1

---

# Index

---

## A

- Access Control 6-6
  - disable 6-10
- Access Control Table 6-7
  - automatic setup 6-8
  - manual setup 6-7, 6-10
- Analysis Interval 4-31
- Analyze Menu 4-28

---

## B

- Back-up
  - configuration files B-3, B-10
  - create file 3-28
- Backup File 3-7
- Beacon Key 3-16
- Bridge Packets in 4-24
- Bridge Packets out 4-24
- Bridge Parameters 3-17
  - protocols 3-17

---

## C

- Change IP Button 3-4, 3-26
- Channel Crosstalk 5-20
- Common Parameters 3-14
  - saving 3-24
- Communications Quality 4-6
- Component Failure A-1
- Configuration
  - back-up 3-28

- common parameters 3-14
- default values 3-13
- unique parameters 3-27
- upload 3-28

- Configuration Mismatch A-1
- Configuration Scenarios
  - basic access network 1-6
  - enterprise-wide network 1-8
  - outdoor connections 1-10
- Connections
  - wireless outdoor 1-10

---

## D

- Default Router 3-21
  - SNMP 3-21
- Detect Button 4-16
- Diagnostic Counters 4-16
- Diskettes
  - files on 1-5
- Documentation Updates vii
- Domain ID 3-5, 3-7, 6-2
  - select another 4-15

---

## E

- Encryption
  - disable 6-5
  - enable 6-3
- Enterprise-wide Network
  - setting up 3-9
- Explore Button 4-30

## Index

---

External Antenna  
enable 3-34

---

### F

Forced Reload  
mode B-1  
procedure B-1  
Forced Reload Mode  
IEEE 802.11 B-2  
Frequency 5-16, 5-18

---

### H

Help  
on-line 1-5

---

### I

Icons  
used in this document 1-4  
In Errors 4-24  
Information  
World Wide Web vii  
Initiator Station 4-30  
Interface 3-14  
Interface Parameters 3-5  
WaveLAN Setup 3-14  
IP Access List, SNMP 3-23  
IP Address 3-12  
assigned address range 3-4  
change button 3-4  
user-defined 3-4  
WavePOINT-II 3-20  
IP Addresses  
about 3-11

---

### L

Link Quality Indicator 4-9  
Link Test 4-4, 4-8  
link quality indicator 4-9  
logging measurement data 4-5,  
4-17  
resetting diagnostic counters 4-10  
selecting another link test partner  
4-11  
Local Noise Level 4-13  
Logging  
automatic 4-18  
manual 4-17  
Logging Measurement Data  
stop 4-19

---

### M

MAC Address  
access control 3-37  
static filter 6-6  
Manual Logging 4-17  
Measurement Data  
automatic Logging 4-18  
automatic logging 4-18  
logging 4-5, 4-17  
logging options 4-18  
manual logging 4-17  
Monitoring 5-1, 6-1  
introduction 4-1  
utilities 4-1  
WaveMANAGER/AP 4-2, 4-21  
WaveMANAGER/CLIENT 4-2  
Monitoring Methods 4-4  
Link Test 4-4

## Index

---

Site Monitor 4-4

---

### N

#### Network

- basic access 3-1, 3-2
- basic scenario 1-6
- enterprise-wide 3-1, 3-9
- enterprise-wide scenario 1-8
- managing 4-1
- performance 4-1

#### Network ID 3-6

- outdoor connections 3-32
- see NWID 3-5

#### Network Problems A-1

#### Network Scenarios 1-6

#### Noise Level 4-26

#### NWID 3-5

- about 3-12

---

### O

#### Optimization

- dual band configuration 5-2
- redundant traffic 5-2
- wired connections 5-2
- wireless connections 5-2

#### Other Button 4-15

#### Other Network ID 4-26

#### Out Collisions 4-24

#### Out Errors 4-24

#### Outdoor Antenna Links

- setup 3-31

#### Outdoor Connections 1-10, 3-1

#### Outdoor Links

- multiple connections 3-37

multiple point-to-point connection  
3-33

omni-directional connection 3-32

---

### P

#### Paperwork 3-10, 3-28

#### Parameters

changing common 3-30

#### Performance 4-1

#### Point-to-multipoint Connection 3-32

#### Point-to-point Connection 3-33

#### Polling Interval

WaveMANAGER A/P 4-31

#### Protocols

filtering 3-17

---

### R

#### Read Password 6-11

#### Read/Write Password 6-11

SNMP 3-22

#### Redundant Traffic 5-2

#### Remote Link Test 4-22, 4-28

WaveMANAGER/AP 4-22

#### Remote Noise 4-13

#### Remote Statistics 4-21

WaveMANAGER A/P 4-21

#### Responsiveness 3-16

#### Roaming 3-7, 3-11

enable 3-16

outdoor connections 3-32, 3-34

setup 3-7

## Index

---

### S

Save Config File as 3-7, 3-24

Scan Button 3-4

open remote configuration 3-26

Securing Access to (Wireless) Data  
6-2

Security 6-1

access control 4-20, 6-6

access control table 6-8

data encryption 6-3

read password 6-11

SNMP IP access 6-12

trap host alerts 6-13

write password 6-12

Select Another Domain ID 4-15

Setup

basic access network 3-2

bridge parameters 3-17

enterprise-wide network 3-9

menu 3-5

Signal Level 4-13

Site 4-12

Site Monitor 4-5

logging measurement data 4-5,  
4-17

selecting another domain ID 4-15

sorting list WavePOINTS 4-16

SNMP

IP access list 3-23

IP address access list 6-11

parameters 3-21

polling interval 4-28

read password 3-22

read/write password 3-22

SNR (Signal to Noise Ratio) 4-13,

4-26

link test 4-9

Socket

WavePOINT-II 3-6

Software Updates vii

Spanning Tree 3-18

Static MAC Address Filter 3-18

Static Mac Address List 3-37

Storm Threshold 3-19

Subnet Mask 3-20

Subnets

about 3-11

Support

WaveLAN vii

System Contact, SNMP 3-23

System Location, SNMP 3-23

System Name, SNMP 3-23

---

### T

Technical Support vii

Time Interval 4-28, 4-31

WaveMANAGER A/P 4-31

Time To Live 3-21

Tools

WaveMANAGER/AP 1-2

Trap Host 3-21

alerts 6-13

IP address 3-23

mechanism 6-13

password 3-23

Trap Messages 3-21

Troubleshooting A-1

problem determination A-1

problem-solving approach A-1

TTL. See Time To Live

## Index

---

### U

- Unicast Packets 4-24
- Up Time 4-24
  - WaveMANAGER/AP 4-24
- Updates vii

### W

- WaveLAN
  - setting parameters 3-5
- WaveLAN Interface Parameters 3-5, 3-14
- WaveLAN Technical Support vii
- WaveMANAGER
  - utilities 4-1
- WaveMANAGER Software
  - install 2-7
  - uninstall 2-10
- WaveMANAGER Station
  - introduction 2-1
  - wired station 2-4
  - wireless station 2-2
- WaveMANAGER/AP 4-2, 4-3
  - About 1-2
- WaveMANAGER/CLIENT 4-3, 4-6
  - About 1-2
  - installing 2-7
  - Link Test 4-4
  - Site Monitor 4-5
  - software installation 2-7
- WavePOINT IP Parameters 3-20
- Wireless Bridge 3-32



---

**This book was created by:**

Lucent Technologies Nederland B.V.  
Wireless Communications & Networking Division (WCND)  
Zadelstede 1-10  
3431 JZ Nieuwegein  
The Netherlands

An electronic copy of this document can be downloaded  
from the WaveLAN Library on the World Wide Web:

**<http://www.wavelan.com>.**

To view or print the electronic document, in Adobe's Portable  
Document Format (PDF), you will need the freeware 'Acrobat'  
viewer from Adobe Inc. (available at

**<http://www.adobe.com/acrobat>).**

Dear reader,

We value your feedback. If you find errors or omissions in  
this book, or if you can suggest ways to improve its  
usefulness, I would like to hear from you.

Please contact me at:

Telephone: + 31 30 609 7471  
Fax: + 31 30 609 7556  
E-Mail: [moolen@lucent.com](mailto:moolen@lucent.com)

Sincerely,

William van der Moolen

008-0127385/B  
September 1998

Copyright © 1998 Lucent Technologies Inc.  
All Rights Reserved

