High Rate Wireless LAN Manager Suite

User's Guide

OPTIONS
by IBM

High Rate Wireless LAN Manager Suite

User's Guide

Note: Before using this information and the product it supports, be sure to read the information under Appendix F "Product warranties and notices".

Second edition April 2001

Contents

Part 1: Introduction

About IBM High Rate Wireless LAN

The IBM High Rate Wireless LAN product family is a comprehensive set of network equipment that enables you to build any type of network configuration, from a small independent wireless network to a large, completely wireless infrastructure. The IBM High Rate Wireless LAN product family consists of:

- PC Card, for (mobile) computers that support the PC Card Type II slot.
- High Rate Wireless LAN adapters, to install PC Cards into desktop computers.
- High Rate Wireless LAN Access Points, that enable you to connect wireless stations to existing Ethernet LAN infrastructures.

The wireless network interface is not much different from the interface for wired LANs. The operating system will not even notice the difference.

The wireless network interface supports all protocols that are supported by standard Ethernet adapter cards. Like wired network interfaces, wireless network interfaces are installed with a dedicated High Rate Wireless LAN driver, but unlike wired network interfaces, wireless network interfaces do not need a cable to connect them to the network. Only wireless network interfaces allow you to relocate workstations without the need to change network cabling or connections to patch panels or hubs.

About IBM High Rate Wireless LAN Tools

The IBM High Rate Wireless LAN software suite consists of a set of management tools that enables you to:

- Display and modify the configuration of (remote) network components.
- Configure network components such as Access Points.
- Diagnose the network performance and, if necessary, identify and solve network errors.
- Manage and optimize network performance.

The IBM High Rate Wireless LAN software suite consists of the following tools:

- Client Manager
- AP Manager

The IBM High Rate Wireless LAN tools can be installed on stations that run the Microsoft Windows 95, 98, ME, NT 4.0 or 2000 operating systems.

Note: The IBM High Rate Wireless LAN products have been designed for interoperability with all other wireless LAN products that use the direct sequence radio technology, as identified in the IEEE 802.11 standard for wireless LANs.

In addition, the High Rate Wireless LAN products are certified with the Wi-Fi logo for proven interoperability with the major other 802.11 products.

This means that your High Rate Wireless LAN hardware will communicate with other vendors' IEEE 802.11 compliant wireless LAN products.

However, you may not always be able to use the High Rate Wireless LAN software suite in combination with other vendors' products, due to the following reasons:

- The IEEE 802.11 standard for wireless LANs does not identify standards for diagnostic or management tools; i.e. each vendor may have designed a customized tool to configure and/or manage the IEEE 802.11 wireless network.
- The IBM High Rate Wireless LAN software suite has been designed to offer an enhanced set of tools to monitor and analyze a wide range of diagnostic tallies.

  Some of these tools require additional functions in the hardware that (by default) is supported by all IBM High Rate Wireless LAN products, but may not be supported by the other vendors' products.

If other vendors' products do not allow you to display communications quality or configuration parameters using the High Rate Wireless LAN software suite, please refer to the documentation that was shipped with the other vendors' product.

Client Manager

The Client Manager is a diagnostic tool to monitor wireless radio communication between a wireless station and its Access Point, or to monitor the link between two wireless stations in an independent network.

Furthermore it can be used as a site monitor to show the coverage of the installed Access Point in a certain area.

AP Manager

The AP Manager is primarily a tool for LAN administrators or system supervisors. You can use the AP Manager program to configure Access Points and to monitor the performance of your wireless network. It can be run on any station in the network, either wired or wireless.

About High Rate Wireless LAN Access Points

The Access Points are identified by either one of the following MAC addresses:

- The universal MAC address of the Wireless Network Interface(s) used by the Access Point, or
- The universal MAC address of the Ethernet Interface.

Access Point-500

The AP-500 is a transparent bridge device equipped with:

- An integrated Wireless Network Interface to connect Wireless Stations to a (wired) network.

Note: The integrated Wireless Network Interface of the Access Point-500 is called interface ‘A’ in this guide.

- A 10Base-T Ethernet Interface, that can be used to connect Wireless Stations to an Ethernet network.

For information concerning all IBM products, please refer to the documentation that was included with your product, or visit our website at: **http://www.ibm.com/pc/support**

About This User’s Guide

This guide describes how to use the High Rate Wireless LAN tools to configure and monitor wireless LANs built with High Rate Wireless LAN products.

In this manual, you will find the following:

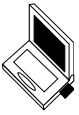
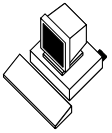
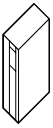
- Part 1 “Introduction” describes the High Rate Wireless LAN tools and the sources for finding more information.
- Part 2 “Wireless Configurations” describes network scenarios that will be used throughout this document.
- Part 3 “Setting Up your LAN Administrator Station” describes how to select a station to manage your High Rate Wireless LAN network, and how to install the necessary software.
- Part 4 “Basic Network Configuration” explains how to configure your particular network, using three network scenarios, from simple to sophisticated.
- Part 5 “Monitoring your High Rate Wireless LAN Network”, describes how to monitor and diagnose communications quality.
- Part 6 “Optimizing Performance” presents a number of considerations to help you sort through the complex factors that determine the performance of your wireless LAN.
- Part 7 “Security” describes how to enhance security and minimize unauthorized use of your High Rate Wireless LAN network.
- Part 8 “Advanced Network Configurations” describes how to customize your High Rate Wireless LAN network to support advanced networking scenarios.

This document does not describe every possible option supported by the High Rate Wireless LAN software suite. It should serve as a general guideline to help you to decide which tool can help you to accomplish a specific task.

For more information about specific software screens or options, you are advised to consult the on-line help documentation.

About Icons used in this Document

Throughout this document we use the following icons to represent the various networking devices:

Icon	Description
	Wireless computer Equipped with: ■ PC Card ■ ISA Adapter
	
	Access Point
	Server station
	Router
	Range Extender Antenna
	Network Hub

On-line Help Documentation

Information about specific software screens or options in your AP Manager or Client Manager program is covered in the on-line help of the programs.

- To access context-sensitive help on a specific screen for the High Rate Wireless LAN programs, click the **Help** button or press the F1 function key.
- In the on-line help you can click the **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 High Rate Wireless LAN products.

Additional Files on your CD-ROM

The CD-ROM that is shipped with your High Rate Wireless LAN products include a file called “readme.txt”. This file contains information about the version of the software and/or drivers on the CD-ROM.

You are advised to read this file prior to installing your High Rate Wireless LAN products, as it may contain additional information that was not available when this document was produced. You can also download or view the “readme.txt” file on the IBM High Rate Wireless LAN website.

Other Sources of Information

For information on updates and other IBM news, see the website at: **http://www.ibm.com/pc/support**.

For technical support, please consult the information at the back of this document.

Part 2: Wireless Configurations

Introduction

This document describes a number of network scenarios that may serve as an example for building your wireless system.
Wireless systems typically apply to indoor network environments that require connectivity for devices roaming throughout the network environment.

Wireless systems are wireless networks that service wireless (mobile) devices. Wireless devices may roam freely throughout the network, with the only restrictions being the size and distance of the wireless device.

Subject to the size and requirements of your LAN, a wireless system can be identified by either one of the following type of configurations:

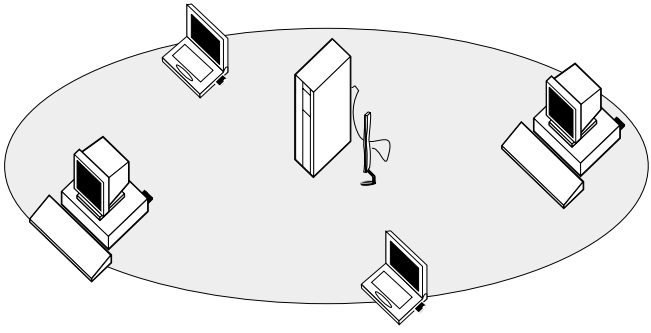
- Independent network
- Basic infrastructure
  - — Stand alone configuration
  - — Wireless access to ethernet networks
- Advanced infrastructures
  - — Multiple channel configuration

Peer-to-Peer Workgroup

A Peer-to-Peer workgroup, as pictured in Figure 2-1, is a group of wireless devices that do not bridge their data via the Access Point. All machines within a Peer-to-Peer network are configured to “Peer- to-Peer” mode.

The most simple independent network is one without a server, where stations communicate Peer-to-Peer, e.g. by sharing a disk or printer via Microsoft Networking or Novell personal NetWare.

Figure 2-1. Peer-to-Peer Workgroup



Peer-to-Peer networks are typically used for small networks where:

- All wireless stations participate in workgroup computing, for example using the disk-sharing option of Microsoft Networking and Printers.
- All stations are within range of a wireless server.

Peer-to-Peer networks are a quick and easy solution to set up a wireless network at trade-shows, business visits or other (off-site) locations.

Basic Infrastructure

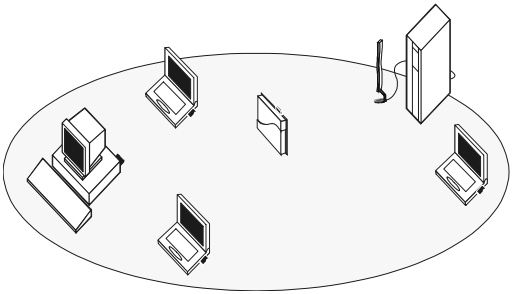
Stand Alone Configuration

In a stand alone configuration (Figure 2-2), the Access Point will function as a relay base station, that will forward the data communication from one computer to another within the same wireless cell.

This is the quickest and easiest way to set up a small wireless LAN infrastructure. This configuration is ideal for temporary installations (e.g. tradeshows) environments that do not allow the installation of a wired infrastructure.

A server is not required in a stand alone wireless configuration; equipped devices can communicate Peer-to-Peer, as described in “Peer-to-Peer Workgroup” on page 2-1.

Figure 2-2. Stand Alone Configuration



The wireless infrastructure is identified by a unique network name. All equipped devices that wish to connect to this network, must be configured with an identical network name.

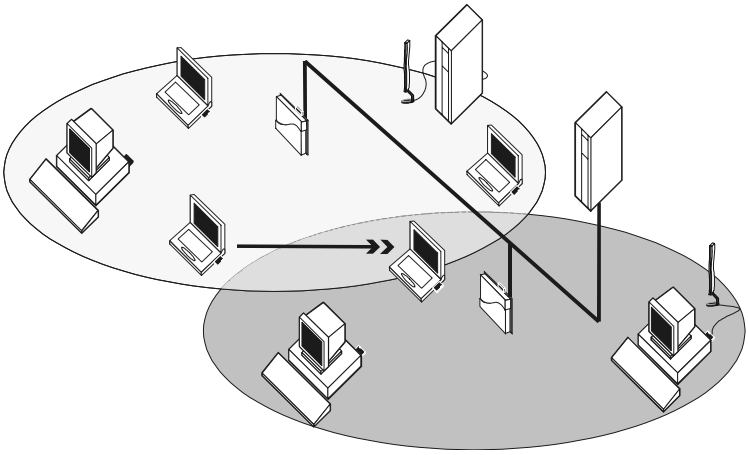
Mobile wireless stations will maintain communication with the infrastructure as long as they remain within range of the Access Point in their High Rate Wireless LAN network.

Wireless Access to Ethernet Networks

Connecting Access Points to an Ethernet network, as pictured in Figure 2-3, allows you to:

- create a wireless environment for mobile computers, or
- connect a number of stations (mobile and/or desktop) to an existing ethernet infrastructure, creating a larger coverage area.

Figure 2-3. Wireless to Ethernet Access Configuration



All wireless stations within this coverage area that wish to connect to the network must be configured with the same network name as the Access Points.

Roaming wireless stations will automatically switch between Access Points, when required, thus maintaining the wireless connection to the network.

Advanced Infrastructures

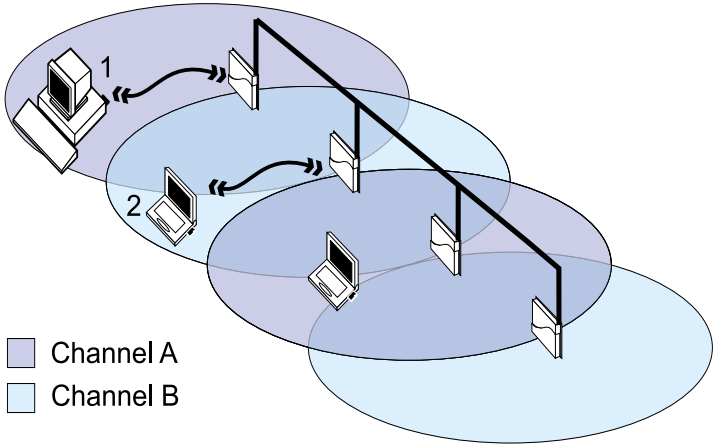
Multiple Channel Configuration

The stations are capable of switching their operating frequency channel dynamically when roaming between Access Points that have been configured to use different radio channels.

Using different channels enables you to optimize wireless performance, assigning different frequency channels to neighboring Access Points. Multiple frequency configurations may prove very useful in environments where:

- A high concentration of wireless stations are operational.
- The stations experience a performance decrease in terms of network response times as a result of the collision avoidance protocol (for more information, see “RTS/CTS Medium Reservation” on page 6-8.

Figure 2-4. Dual Channel Configuration



- By configuring neighboring Access Points with different frequencies, you create separate mediums for each wireless cell. Operating at different channels, the stations can no longer “hear” one another, and therefore no longer need to defer communications.
- When the configuration pictured in Figure 2-4 represents a single channel system, both station 1 and station 2 share the same medium. Station 1 might need to defer communication with the Access Point when it senses that station 2 is already communicating with the Access Point in the neighboring cell.

As is the case in any roaming environment, you must configure all Access Points in multiple channel configurations with an identical network name.

The preferred channel separation between the channels in neighboring cells is 25 MHz (5 channels). Subject to the number of channels supported by the wireless client adapters available in your country, this means that you can apply up to three different channels within your wireless network (see Table 6-1 on page 6-14 for recommended channel configurations).

Applying two channels that allow the maximum channel separation will decrease the amount of channel cross-talk, and provide a noticeable performance increase over networks with minimal channel separation.

To configure networks with multiple channels, refer to “Frequency Channel Management” on page 6-12.

Part 3: Setting Up your LAN Administrator Station

Introduction

High Rate Wireless LAN infrastructures are managed from the LAN administrator station. Within this chapter decision points are described which are necessary to help you set up LAN administrator station(s) to properly manage your network.

Typically, the LAN administrator station is a computer used by the LAN administrator to configure, manage and monitor the network. You can assign as many LAN administrator stations as you like, depending on how you would like to manage your network.

The LAN administrator station uses the tools available in the High Rate Wireless LAN software suite to configure and monitor your network. The following programs are included within the High Rate Wireless LAN software suite:

- Client Manager
- AP Manager

In this chapter, we describe how to set up the LAN administrator station in the following network configurations:

- **Peer-to-Peer workgroup** - all stations within the network directly communicate with all other stations. No Access Points are necessary to bridge the data.
- **Infrastructure network** - all stations communicate to each other and the Ethernet backbone via Access Point interfaces.

For an overview of the High Rate Wireless LAN software tools, please refer to “About IBM High Rate Wireless LAN Tools” on page 1-1.

Assigning an LAN Administrator Station

Minimum Requirements

To set up the LAN administrator station, you can use any desktop or portable computer 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, 98, ME, 2000 or NT 4.0.

For the **Client Manager** you will also need:

- The wireless client adapters

For the **AP Manager** you will need the following:

- Access to the LAN, via

- Wireless client adapter
- Ethernet card
- dial-up connection

- High Rate Wireless LAN Access Points.
- A loaded TCP/IP protocol that provides a Windows sockets (winsock) interface. The TCP/IP drivers can be found on the Microsoft Windows installation disks or CD-ROM.

Managing Peer-to-Peer Workgroups

A Peer-to-Peer workgroup consists of several stations communicating directly to each other without bridging data via the Access Point.

Peer-to-Peer workgroups do not need the IBM High Rate Wireless LAN tools. For more information refer to the documentation that comes with your product.

Managing Infrastructure Networks

In an infrastructure network, you will primarily use the LAN administrator station that has the AP Manager installed to configure your Access Points and monitor the radio traffic between selected Access Points and stations within the network.

You may also install the Client Manager on all stations within the network, or on selected mobile stations with the PCCard, to monitor the link between the mobile station and the nearest Access Points.

Wired or Wireless?

The choice for a wireless or wired LAN administrator station will depend on your preferences and abilities to administer your network.

You should first determine how you would like to manage your network. If you like to configure and monitor stations from:

- **on-site**, to troubleshoot problems at the physical location of the station, you may choose to have a mobile, wireless LAN administrator station.
  Tool: AP Manager and Client Manager
- **a central location**, such as the LAN administrator station, you may prefer a wired LAN administrator station.
  Tool: AP Manager
- **a remote location**, via modem, calling into a RAS or PPP entry point to your network.
  Tool: AP Manager

Your next consideration for wired or wireless station should be the size of your network. For instance:

- in larger networks, it may be more convenient to manage the stations from a central location, so a wired station would be more appropriate.

- in smaller network configurations, in which there are only few Access Points, a mobile, wireless station may be the most efficient way to configure and manage your network.

For wireless stations the following has to be considered:

- 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 Access Points.
- It is also possible remote configure and monitor the Access Point via a dial-up connection. This feature is only possible when the network is externally accessible.

Of course you can assign multiple stations as LAN administrator stations, allowing for a combination of wired and wireless stations and allowing you the freedom to choose the most appropriate tool for the situation.

Wired Stations

A wired LAN administrator station allows you to configure and monitor Access Points through a wired backbone by using the AP Manager tool.

Configuration

A wired LAN administrator station has access to all Access Points via a wired backbone. The Access Points are identified by means of their unique IP address.

When your LAN architecture is comprised of multiple subnets, separated by gateways or routers, please note that the LAN administrator station which you intend to use for the initial configuration, must be on the same subnet as the Access Points.

Once the Access Points have been configured and their IP addresses have been registered, you can use any station to access the Access Points via the TCP/IP protocol.

For more information on configuring your Access Point, please refer to “Configuration Scenarios” on page 3-7.

Monitoring

When you use a wired LAN administrator station you will not be able to move around to different physical locations of the network to determine or optimize the placement of stations, Access Points or antennas.

However, a wired LAN administrator station can use the AP Manager remote link test and remote statistics features to perform monitoring tasks.

With the AP Manager you can validate radio frequency links between a remote Access Point and stations connected to that Access Point. For more information on monitoring, refer to “Monitoring Options” on page 5-17.

Wireless Stations

A wireless, mobile LAN administrator station allows you to use the Client Manager as well as the AP Manager.

Monitoring

You can use the following tools to monitor your infrastructure network:

- Client Manager
  - — Wireless client adapter diagnostics
  - — Logging measurements data
  - — Site monitor
  - — Link test
- AP Manager
  - — System information
  - — Remote link test
  - — Remote statistics

For more information on monitoring your network, refer to Part 5 “Monitoring your High Rate Wireless LAN Network”.

Installing High Rate Wireless LAN Software

Client Manager

The Client Manager is a diagnostics tool that runs on wireless stations only. To setup the LAN administrator station that is capable of running the Client Manager program, the station must be equipped with the wireless client adapter.

To install the Client Manager software, proceed as follows:

1. Insert the software CD-ROM that came with your Access Point station that you have designated as the LAN administrator station.
   If you downloaded the software from the web, please refer to the installation instructions found on the web.
2. When the CD Browser automatically starts you can proceed with the next step. If not:
   - Click the **Start** button on the Windows task bar, then select **Run**.
   - Click the **Browse** button in the Run window.
   - Select the drive letter of your CD-ROM player in the Browse window, then select the file “setup.exe”, and click the **Open** button.
   - Click the **OK** button in the Run window. The CD Browser will start-up.
3. From the CD Browser main menu select the **Install Software** button.
4. Click on **Install Client Manager**.
5. Follow the instructions on your screen. If not available yet, a special IBM group in the Windows Programs menu will be created. This group will provide access to the Client Manager.

Note: Previously installed versions of the Client Manager program will automatically be replaced.

During the installation, you will be prompted for a directory to install the program files. The default directory for the Client Manager program is: "C:\Program Files\IBM Wireless LAN\Client Manager"

Throughout this manual, we make references to a variety of files. Unless otherwise specified, you will find these files in this default directory.

AP Manager

The AP Manager can be installed on both wireless and wired stations. To install the program, you will need to select a station that is configured with:

- Network Interface Card (NIC) to connect this station to the network. The NIC cards can be of any type, including:
  - — Wireless client adapter (for wireless stations)
  - — Ethernet card
- TCP/IP protocol stack (see "Verifying the TCP/IP Protocol Settings" on page 3-6).

Installing AP Manager

To install the AP Manager software, proceed as follows:

1. Insert the software CD-ROM that came with your product in the CD-ROM drive of the computer that you have designated as the LAN administrator station.
   If you downloaded the software from the web, please refer to the installation instructions found on the web.
2. When the CD Browser automatically starts you can proceed with the next step. If not:
   - Click the **Start** button on the Windows task bar, then select **Run**.
   - Click the **Browse** button in the Run window.
   - Select the drive letter of your CD-ROM player in the Browse window, then select the file "setup.exe", and click the **Open** button.
   - Click the **OK** button in the Run window. The CD Browser will start-up.
3. From the CD Browser main menu select the **Install Software** button
4. Click on **Install AP Manager**.
5. Follow the instructions on your screen. If not available yet, a special IBM group in the Windows Programs menu will be created. This group will provide access to the AP Manager software to configure your Access Point.

Note: Previously installed versions of the Client Manager program will automatically be replaced, without affecting any other file that you might have saved into the program's directory. For example if you saved back-ups of Access Point configuration files which you created with the previous version in the Access Point program folders, these files will not be deleted or overwritten.

During the installation, you will be prompted for a directory to install the program files. The default directory for the AP Manager program is: "C:\Program Files\IBM Wireless LAN\AP Manager"

Throughout this manual, we make references to a variety of files. Unless otherwise specified, you will find these files in this default directory.

Verifying the TCP/IP Protocol Settings

The AP Manager program requires a TCP/IP networking protocol to communicate with the Access Point. When setting up the Access Points for the first time you will need to verify the TCP/IP settings of the LAN administrator station.

- When the network operating system in your network does not use the TCP/IP protocol, you will need to install it onto the LAN administrator station and assign a user-defined IP address to each LAN administrator station.
- When your network operating system uses the TCP/IP protocol, your station will already have an IP address assigned to it. This could either be a user-defined value, or a value assigned by for example a DHCP server. You do not need to modify this IP address.

To verify whether the TCP/IP protocol is properly installed, proceed as follows:

On the Windows task bar, click the Start button.
Point to **Settings** and then click on **Control Panel**.
In the Control Panel window, double-click the **Network** icon.
Verify that the list of network components includes the **TCP/IP Protocol** for the wireless network interface that you will use to access the Access Point (e.g. your ethernet or adapter).

- If **Yes**, close all windows using the **Cancel** button and proceed with "Configuration Scenarios" on page 3-7.
- If **No**, proceed as follows:
  a. Click the **Add** button.
  b. From the list of component types, select **Protocol** and click the **Add** button.
  c. Select a TCP/IP protocol from the list displayed.

     In most network environments, the Microsoft TCP/IP protocol will work just fine. Alternatively, select a TCP/IP protocol that matches your network operating system.
  d. When your network does not use IP addressing, enable the option **Specify an IP Address**.

     This will disable the DHCP mechanism that would assign an IP address to your LAN administrator station automatically in networks that include a DHCP server.
  e. Enter a user-defined value in the **IP Address** field of the format **153.69.254.xxx**, where xxx may be any numerical value in the range of 1-253.

     When configuring multiple LAN administrator stations, make sure to assign different values to each station.
  f. In the Subnet Mask field enter the value **255.255.255.0**
  g. Click the **OK** button to confirm and follow the instructions as displayed on your screen.

5. When prompted to restart your computer, select **Yes**.

Once your computer has restarted, you will be ready to configure the Access Point via any of the configuration scenarios as described on “Configuration Scenarios” on page 3-7.

Configuration Scenarios

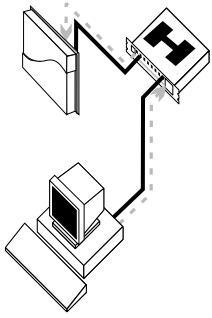
In the previous section you may have selected either a wired, or a wireless LAN administrator station. This section will describe some of the characteristics and features of each type and identify whether further modifications to the setup of your computer or “desktop workplace” are required.

Wired LAN Administrator Station

Using a wired LAN administrator station allows you to configure Access Points via:

- A “desktop workplace” setup, connecting your computer to the Access Point via a hub as pictured in Figure 3-1.
- A regular wired ethernet connection as pictured in Figure 3-2.

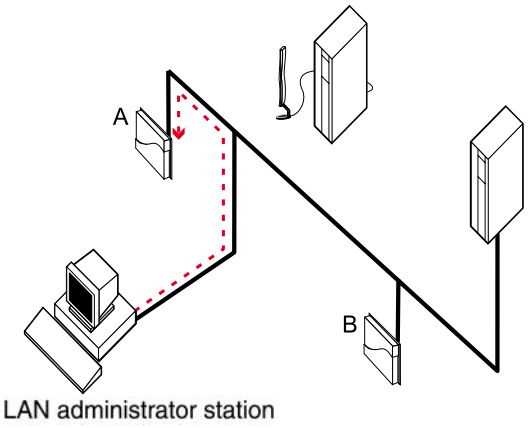
Figure 3-1. Wired Access via a Direct Cable Connection



Selecting a wired LAN administrator station is recommended in one of the following situations:

- You prefer to manage your Access Points from a fixed central location.
- The Access Points will be installed on remote locations, that are accessible via TCP/IP networking.

Figure 3-2. Wired Access via a Network Connection



Looking at Figure 3-2, the LAN administrator station has access to both Access Points **A** and **B** via the wired backbone.

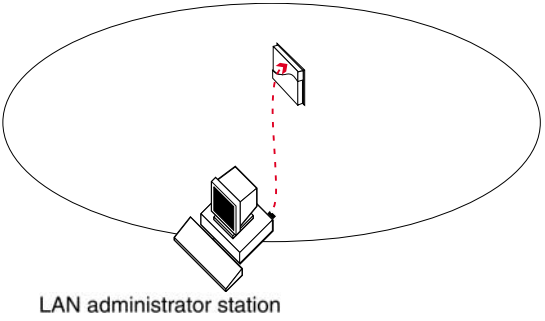
- When these Access Points are still using the “out-of-the-box” configuration, the Access Points can be identified by means of their ethernet MAC Address, provided that the Access Points are on the same subnet as your LAN administrator station (i.e. there are no routers between your LAN administrator station and the Access Point).
- When you have assigned a unique IP address value to each Access Point, you should be able to access each Access Point from anywhere within the network by using its unique IP address.

When installing new Access Points “out-of-the-box”, you are advised to configure the Access Points one-by-one using the “desktop workplace” scenario as pictured in Figure 3-1 on page 3-7. This will allow you to assign a unique IP address value to each unit prior to connecting the units to the network infrastructure.

Wireless LAN Administrator Station

A wireless, mobile LAN administrator station allows you to use the AP Manager in combination with the Client Manager tool.

Figure 3-3. Wireless Access via a Direct Connection



Using a wireless LAN administrator station allows you to configure Access Points:

- Directly by means of a wireless point-to-point connection as pictured in Figure 3-3, or
- Indirectly by means of a wireless point-to-point connection with another Access Point that provides access to the “target” Access Point via a network backbone as pictured in Figure 3-4 on page 3-9.

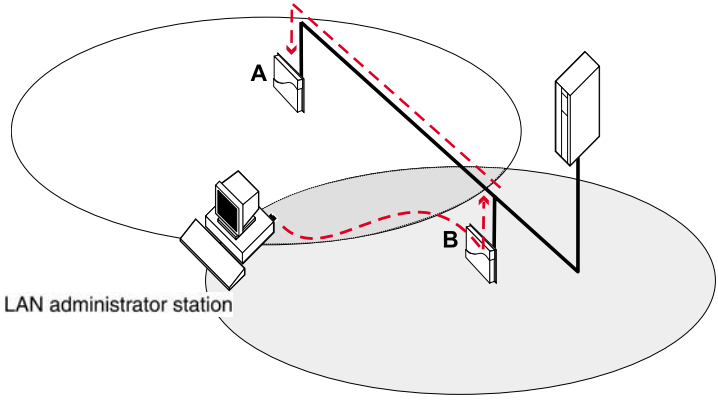
Note: In the same manner in which wired networks require you to verify that all cables are connected properly to establish connection, wireless networks require you to verify that:

— the LAN administrator station is within range of the “target” Access Point, and

— the wireless network interface setup matches the parameter values of the Access Point(s).

When using the configuration setup as pictured in Figure 3-3, the wireless network interface of the LAN administrator station should be configured to match the settings of the “target” Access Point.

Figure 3-4. Wireless Access via an Indirect Connection



When looking at the scenario pictured in Figure 3-4 on page 3-9, the wireless network interface of the LAN administrator station should be configured to match the settings of Access Point **B**.

- The scenario pictured in Figure 3-3 will be most convenient when configuring multiple “out-of-the-box” Access Points sequentially.
- The scenario pictured in Figure 3-4 will be most efficient when adding new Access Points to an existing network or when you are not within range of the “target” Access Point.

In both scenarios the Access Points are identified by means of their unique IP address.

Uninstalling High Rate Wireless LAN Software

If you wish to remove the High Rate Wireless LAN software from the LAN administrator station you can use the “Add/Remove” function of your Windows operating system.

To uninstall High Rate Wireless LAN software:

1. On the Windows taskbar, click the **Start** button.
2. Click on **Settings** and then **Control Panel**.
3. On the Control Panel window, double-click the **Add/Remove Programs** icon.
4. Select the program that you wish to uninstall, and click the **Add/Remove** button.

The **Add/Remove** option will remove program files only. If you have stored log files in the program files directory, these files will not be removed.

Part 4: Basic Network Configuration

Introduction

This chapter will describe how to configure the High Rate Wireless LAN network for:

- Peer-to-Peer workgroups, and
- Infrastructure networks

Peer-to-Peer Workgroups

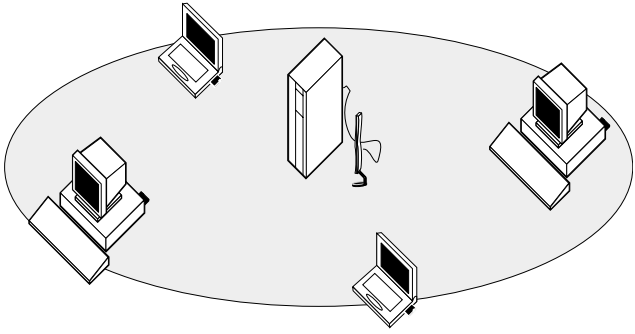
A Peer-to-Peer workgroup consists of several wireless stations communicating directly with each other without bridging data via the Access Point (see Figure 4-1).

To set up a Peer-to-Peer workgroup operating with the standard protocols, do the following:

- Set all stations to connect to a Peer-to-Peer workgroup.
- Set all stations to use the same Network Name.
- Set all stations to use an identical encryption key.

For more information to “Peer-to-Peer Workgroup” on page 2-1.

Figure 4-1. Peer-to-Peer workgroup



Infrastructure Networks

The number of network configurations that you could create using Access Points and High Rate Wireless LAN products is unlimited. Therefore, we have divided the rest of this chapter into three sections that should help you get your network up and running.

- The instructions for “Configuring Infrastructure Networks” on page 4-2 will work fine in most networking environments.
- More advanced configurations settings are described in Part 8 “Advanced Network Configurations”.

— The Advanced Parameters (page 8-1) may help you with tailoring the Access Point configuration to meet your networking requirements.

— Configuring Large Networks (page 8-13) provides a procedure to manage Access Point devices more efficiently.

What you Need

To manage your Access Points, you must assign a unique IP address to each Access Point within your network.

Furthermore, your management station must also have an IP address. The TCP/IP connection of your station should either:

- Be connected to the same subnet as the Access Points, as described in Basic Infrastructure (page 2-2), or
- Provide access to the subnet of the Access Points via routers, gateways or another type of LAN connection that supports the TCP/IP protocol.

Configuring Infrastructure Networks

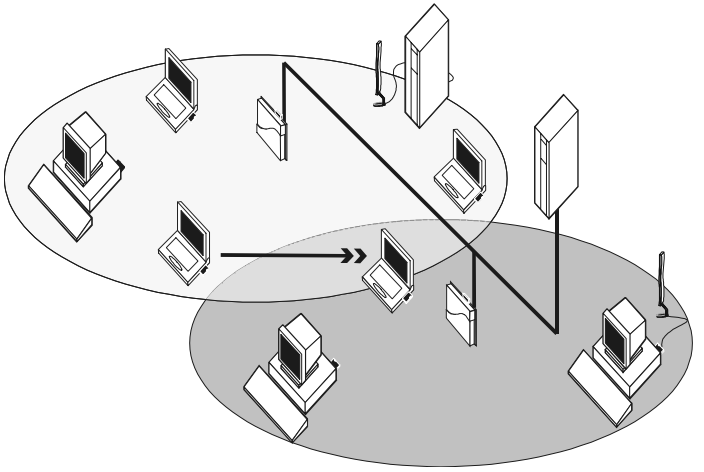
Basic Configuration

Introduction

This section will describe a 4-step installation approach to configure your Access Points to service a roaming network environment for (mobile) wireless stations.

Looking at the example pictured in Figure 4-2, each wireless cell is serviced by one Access Point that has been set to “Access Point Services”. All Access Points share the same Network Name.

Figure 4-2. Basic Access Network



To connect a wireless station to the High Rate Wireless LAN network, each station must be configured with the same Network Name as the Access Point.

To configure the wireless stations, follow the instructions as described in the documentation that comes with your wireless client adapter.

To install and configure the Access Point perform the following steps:

1. Install the Access Point hardware[1].
2. Connect to the Access Point with the AP Manager program.
3. Set the Network Name and save configuration to the Access Point.
4. Create a back-up file of the new configuration settings (optional but recommended).

Repeat steps 2 to 4 for each of the Access Points that you wish to install.

Step 1 - Installing the Access Point

For installation instructions of the Access Point hardware, please refer to the Getting Started Guide that was shipped with the Access Point.

Step 2 - Connecting to the Access Point

To connect to the Access Point, you need to address each Access Point via its IP address.

- If your network includes a BOOTP or DHCP server, the IP address will be assigned automatically (refer to for more information about BOOTP/DHCP.
- In situations where no IP addresses are assigned automatically, the IP address will be 153.69.254.254.

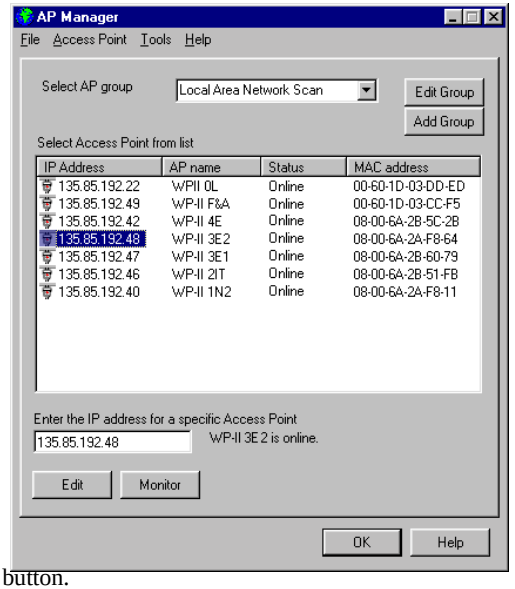
  You must change this factory-set IP address (153.69.254.254) upon first configuration.

To connect to the Access Point proceed as follows:

1. Start the AP Manager program.
2. Select the Access Point that you wish to configure from the list or enter the IP address in the field **Enter the IP address for a specific Access Point** (see Figure 4-3).
   - A new Access Point is marked with a special icon.
   - This list will display all Access Points located on the same IP subnet as your management station (see also “Modifying the Configuration” on page 8-17).
   - To gain access to Access Points on a different subnet or via a dial-up connection, enter a specific IP address in the field **Enter the IP address for a specific Access Point**.

1. Subject to the decisions you made in Part 3 “Setting Up your LAN Administrator Station”, you may either install the Access Points at your desk and configure them one by one, or have the Access Points mounted directly in their various locations prior to configuring them via a network connection.

Figure 4-3. Main AP Manager window



3. Click the **Edit** button.

   - If the Access Point that you select is identified by the factory-set IP address 153.69.254.254, you will be prompted to change this IP address.
     a. Enter a unique IP address for the Access Point in the field Access Point **IP Address**.
     b. Record the IP address on the “Access Point Configuration Record” located in Appendix A “Start-up Configuration”.

4. Enter the Read Write password and click **OK** (default password is “public”).

   - If the Access Point is found and if you entered the right passwords, a new window appears with parameter tabs to change the configuration (see Figure 4-4).
   - If the Access Point is not found in the network and/or the configuration is not read, or if the wrong password is entered, the message “Invalid password” appears.
     Click **OK** to return to the main AP Manager window and try again.

You are now ready to change the Access Point configuration settings.

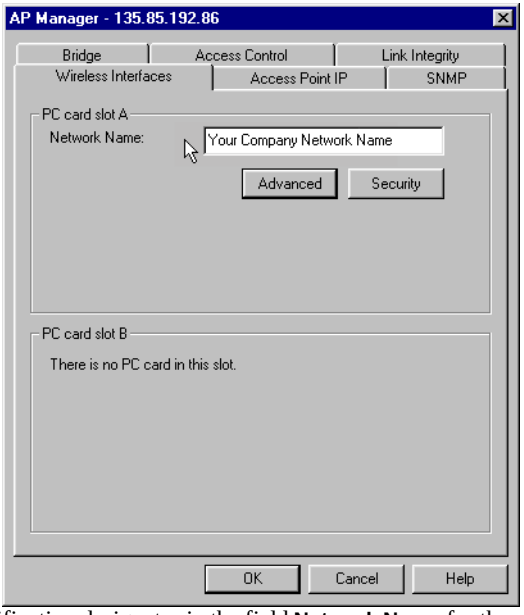
Step 3 - Set Network Name and Save Configuration

When installing the High Rate Wireless LAN network, you are advised to modify the default settings of the wireless network interfaces. Although the Access Point will work fine with its factory-set values, changing the High Rate Wireless LAN parameters to unique values will differentiate your network from possible neighboring networks.

1. Select the tab **Wireless Interfaces** (see Figure 4-4).

Note: The integrated Wireless Network Interface of the AP-500 is called Interface ‘A’ in this guide.

Figure 4-4. AP Manager Wireless Interfaces tab



2. Enter the identification designator in the field **Network Name** for the service type that this interface should use:

   The network name can be any alphanumeric string from 1 to 32 characters in the range of “a” to “z”, “A” to “Z” and “0” to “9”.

   The network name should be the same for all wireless network interfaces that will service wireless stations that belong to the network.

   The network name distinguishes your Access Points from Access Points that belong to a neighboring network.

   For information on other Interface parameters (like the **Advanced** and **Security** button), see Part 8 “Advanced Network Configurations”.

3. When finished changing parameters, click **OK** to save the configuration to the Access Point and to return to the main AP Manager window (as pictured in Figure 4-3 on page 4-4).

   At this stage, the IP address and other settings are stored in the volatile memory of the Access Point.

Note: If you save the configuration to the Access Point (by clicking the **OK** button), the Access Point reboots automatically.

This will complete the basic configuration of your Access Point. This basic configuration will work efficiently in most networking situations. You are advised to make a back-up file of this configuration as described in “Step 4 - Create a Back-up of the Configuration”.

More advanced parameter settings are discussed in Part 8 “Advanced Network Configurations”.

Step 4 - Create a Back-up of the Configuration

At all times when you change the configuration of the Access Point, we recommend that you create a back-up file of the configuration. You can use this back-up to quickly restore the Access Point configuration in situations where:

- Your Access Point goes out of service.
- You would like to recreate the original configuration of the Access Point that you had to replace (for example following a repair).
- When you need to perform a forced reload as described in Appendix C “Forced Reload Procedure”.

To create a back-up file proceed as follows:

1. Start the AP Manager program.
2. Select the Access Point you want to create a backup of.
3. From the Access Point menu select **Download Config File**.
4. When prompted for a name, enter a name that allows you to easily recognize the relationship between the file name and the Access Point.
5. Record the filename and the location where the Access Point will be installed on the “Access Point Configuration Record” in Start-up Configuration (page A-1).

To install and configure other Access Points, refer back to “Step 1 - Installing the Access Point” on page 4-3.

Part 5: Monitoring your High Rate Wireless LAN Network

Introduction

Once your network has been configured and installed, you can use High Rate Wireless LAN software tools to:

- Monitor the performance of your network;
- Verify optimal placement of your 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 stations are relocated, or office environments add or re-arrange cube walls, or when new equipment is installed that might interfere with the wireless communication.

High Rate Wireless LAN Tools

The High Rate Wireless LAN software suite offers two tools that enable you to monitor your network:

- Client Manager
- AP Manager

Client Manager

The Client Manager has been designed to monitor the radio performance of your network on-site. You can use this program to:

- Run dynamic radio communication diagnostics with the Access Point within range of your monitoring station.
- Display detailed link test measurement results with the Access Point nearest your Client Manager station.

The Client Manager is a mobile wireless tool that can only run on a wireless station (typically a portable device such as a notebook computer).

AP Manager

The AP Manager has been designed to monitor your network from a central location, e.g. the LAN administrator station.
You can use this tool to display link test measurements between a (remote) Access Point of your choice and a station connected to the selected Access Point.

The AP Manager tool can run on both wired stations (Ethernet) and wireless stations. To run diagnostic measurements, the LAN administrator station must be connected to the network infrastructure that allows the station to access the Access Point using the TCP/IP protocol.

Which Tool Should You Use?

The decision whether to use the Client Manager or AP Manager largely depends on your capabilities or desire to perform diagnostic measurements on-site, or from a central location.

Both the Client Manager and the AP Manager offer logging functions that can save measurement data for later evaluation or comparison with previous measurements. You can view saved log files with any ASCII editor, or import the data into standard spreadsheet or database applications.

Note: Alternatively you may use the AP Manager program to monitor wireless performance of both wireless systems via Access Points (see “Remote Link Test Window” on page 5-19).

The High Rate Wireless LAN products have been designed for interoperability with all other wireless LAN products that use the direct sequence radio technology, as identified in the IEEE 802.11 standard for wireless LANs. Operating in the unlicensed 2.4 GHz band, the High Rate Wireless LAN system can transmit through walls and floors, giving you the freedom to roam throughout the network while maintaining your network connection.

This means that your High Rate Wireless LAN hardware will communicate with other vendors’ IEEE 802.11 compliant wireless LAN products.

However, you may not always be able to use the High Rate Wireless LAN software suite in combination with other vendors’ products, due to the following reasons:

- The IEEE 802.11 standard for wireless LANs does not identify standards for diagnostic or management tools; i.e. each vendor may have designed a customized tool to configure and/or manage the IEEE 802.11 wireless network.
- The IBM High Rate Wireless LAN software suite has been designed to offer an enhanced set of tools to monitor and analyze a wide range of diagnostic tallies.

  Some of these tools require additional functions in the hardware that (by default) is supported by all IBM High Rate Wireless LAN products, but may not be supported by the other vendors’ products.

If other vendors’ products do not allow you to display communications quality or configuration parameters using the High Rate Wireless LAN software suite, please refer to the documentation that was shipped with the other vendors’ product.

Using the Client Manager

Monitoring Methods

The Client Manager offers four monitoring methods:

- Wireless Client diagnostics (see “Diagnose Card” on page 5-16)

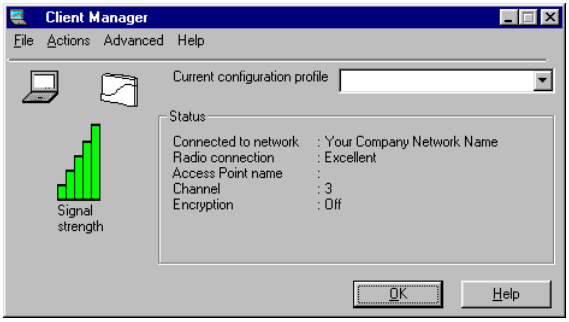
- Link test (see “Link Test Window” on page 5-4)
- Site monitor (see “Site Monitor Window” on page 5-8)
- Logging measurement data (see “Logging Measurement Data” on page 5-14)

The site monitor, link test and logging measurement data options are only available when the Client Manager is installed in “Advanced” mode (see “Client Manager” on page 1-2” for more information).

To start the Client Manager tool:

1. The Client Manager program starts automatically when Windows is started. The Client Manager icon is displayed on the windows task bar. If the program is not running:
   - Select the **Start** button on the windows task bar.
   - Select **Programs**, and then select the **IBM** program group.
   - Next select **Client Manager** to start the Client Manager program.
2. Click on the Client Manager icon  in the taskbar to open the main Client Manager window pictured in Figure 5-1.

Figure 5-1. Main Client Manager Window



The main Client Manager window will display the key information required to validate the current network connection of your High Rate Wireless LAN station:

- The name of the network to which your station is connected (“Peer-to-Peer” in case of a Peer-to-Peer workgroup, or the network name of your Access Point infrastructure, e.g. “Your company network name”).
- The quality of the radio connection to this network:
  - — Excellent
  - — Good
  - — Marginal
  - — Poor, or
  - — Out of range

The quality of the radio connection is also displayed with a colored icon. The color indicates the quality of the connection

- Green: Excellent or good connection
- Yellow: Marginal connection
- Red: Poor connection
- Red with error sign: No connection

- The name of the Access Point to which the mobile wireless computer is connected at that moment.
- The channel used for the connection.
- Encryption: on / off

If your Client Manager could not establish a network connection, this screen will display either:

- **No wireless network card driver present** - your station was unable to detect the High Rate Wireless LAN driver. Check to make sure that the wireless client adapter is properly connected and that you have configured your station correctly.
- **Out of range** - you are out of range of the network for which your station has been configured.
- **Searching for initial connection to network: Network Name.** - the network named Network Name can not be found.

For more detailed information use the monitoring methods as described in “Monitoring Methods” on page 5-2.

From the main Client Manager window (as pictured in Figure 5-1 on page 5-3) you will also have access to a number of menu items. These menus are described in the next paragraphs.

If you are having problems connecting to the network:

- Click the **Help** button or press F1 for troubleshooting hints
- Refer to Appendix B “Troubleshooting” for possible solutions.

Link Test Window

You can use the link test mode to perform detailed diagnostic measurements in indoor wireless environments between your Client Manager station and one specific test partner. Subject to the type of network to which your Client Manager station is connected, the test partner may be either one of the following:

- The Access Point, when your Client Manager station is connected to an “Infrastructure Network” (see Part 2 “Wireless Configurations”).
  In this type of network you will not be able to select another link test partner; when roaming throughout the wireless network environment, the link test partner may change dynamically whenever another Access Point provides better communications quality.
- The station, when your Client Manager station is connected to a Peer-to-Peer workgroup (see Part 2 “Wireless Configurations”).

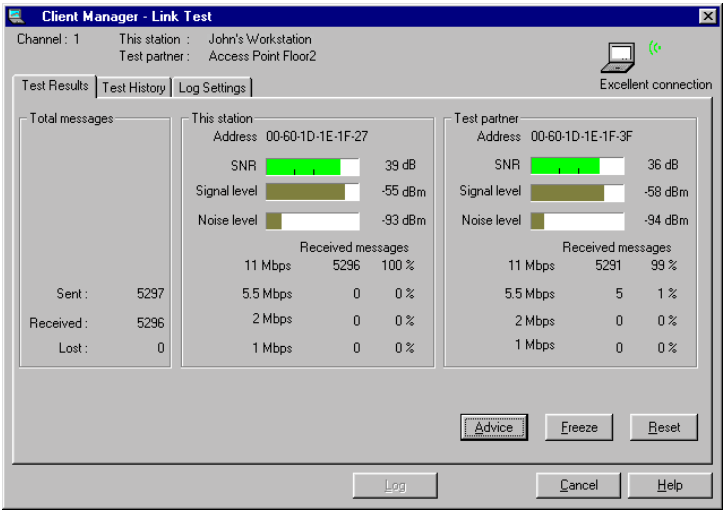
In this type of network you will be able to select your link test partner from a list of stations available in the independent network identified by the same network name as your Client Manager station.

To start the link test, select **Link Test** in the **Advanced** menu of the main Client Manager window. This will display the window pictured in Figure 5-2.

Across the top of the Link Test window, you can see:

- The radio channel on which both devices are communicating.
- The name of your computer (This Station),
- The name of the link test partner (Test Partner), and
- The quality of the connection.

Figure 5-2. Link Test Window



The “Link Test” window provides you with three link test options to assist you in analyzing the link test data:

- **Test results** - provides measurement results of the link test.
- **Test history** - provides graphical results of the link quality.
- **Log Settings** - set the measurement parameters to record test results for future analysis.

Test Results Tab

The Test Results tab is your primary screen to analyze link test results using the following indicators:

- Signal to noise radio (SNR)
- Received messages

Signal to Noise Ratio (SNR)

The signal to noise ratio (SNR) identifies the communications quality of radio path between your station and the link test partner. This indicator is updated dynamically according to the actual status of the radio link.

The color of SNR indicator relates to the following levels of communications quality

Color	Description
■ Green	Communication quality is “Excellent” or “Good”, no intervention is required.
■ Yellow	Communication quality is “Marginal”, no intervention is required.
■ Red	Communication quality is “Poor”, intervention required. (see Appendix B “Troubleshooting”)

If the level of SNR is lower than expected the signal level and noise level indicators may help you investigate the cause:

- A low signal level indicates that the “strength” of the radio signal is fairly low: i.e. your Client Manager station is almost ‘out-of-range’ of its link test partner.
- A high noise level indicates a source of radio interference in the radio path between the two link test partners.
  Comparing the values for your station and the link test partner will help you to identify the location where the interference occurs, and investigate whether any actions to eliminate or remedy the source interference resulted in a better performance.

Received Messages

The indicator “Received Messages” provides a way to determine the efficiency of the radio path between your Client Manager station and the link test partner.

When running a link test, your Client Manager station will exchange messages with its test partner. The test partner will confirm proper receipt by returning an acknowledgment response.

Both your wireless station and the link test partner will use these messages to:

- Measure the signal to noise ratio (SNR).
- Compare the total number of messages sent to the number of messages received.
  - — When the communications quality is rated as “Excellent” or “Good”, the total number of lost messages should be zero.
  - — When communications quality is “Marginal”, the total number of lost messages may be in the range of 1% to 3%
  - — When the total number of messages is >5% your network environment will most likely suffer from performance problems.

In most situations you will see that the number of lost messages will increase whenever the level of SNR decreases.

The different fields for messages received at the different transmit rates (e.g. “11 Mbit/s”, “5.5 Mbit/s”, “2 Mbit/s” and “1 Mbit/s”) may serve as an indicator for network throughput efficiency.

It is normal behavior for High Rate Wireless LAN stations to retransmit messages that were lost (either as a result of a frame-collision, or because the test partner was “out-of-range”):

- If a message transmission fails, your station will retransmit the “lost” frame.
- If a retransmission fails repeatedly, the station will switch to a lower data speed[1] and try to transmit the message again.

The higher the number of messages received with the highest transmit rate, the better your throughput efficiency. A relatively high number of messages received at lower transmit rates may indicate:

- Inadequate radio performance, which can typically be related to the level of SNR, or
- Network congestion. This may typically be the case when the SNR was rated “Good”.

In situations where you see a lot of (re)transmissions at lower data rates, the lower data speed might be the result of:

- A link test partner that is almost “out-of-range” of your Client Manager station. This is easily recognized by a low level of SNR.
- One of the test partners is using a wireless card that does not support the high rates.

To investigate link quality results in more detail, you can use one of the following buttons:

- **Advice** - to display more detailed information related to the current link quality and troubleshooting hints to increase performance.
- **Freeze** - to momentarily stop the dynamic indicators and updating of numerical values, for example to analyze the results on your screen in more detail.
- **Reset** - to reset all of the diagnostic counters back to zero.
  You can use this option to investigate the results of an action to remedy a cause of poor performance. For example after you switched off a microwave oven that you suspect is causing interference. Clicking the **Reset** button will analyze the link quality again, ignoring previous results that may have adversely influenced the statistics.
- **Help** - to display general information about the Client Manager link test.
  To access the on-line help system you can also press the F1 function key on your keyboard.

Test History Tab

You can use the Test History tab to display link test results as a line-chart. You can change the display to include the diagnostic parameters of your choice, and a user-defined time window. You can set the time window to display the information of the last minute, last hour or last 24 hours.

1. The range of wireless data is related to the data speed. Radio messages transmitted at lower data speeds will travel longer distances than messages at maximum data speed. In most network environments, the “Auto Fall-back” transmit rate will yield the best performance results.

For example, if you have an Access Point that shows mysterious performance problems at regular intervals, you can run the test history mode for 24 hours to:

- Determine the exact time the problem occurs in the selected Time window
- Analyze what was causing the performance problem without having to watch the dynamic indicators continuously.

Log Settings Tab

You can record the link test measurements to a log file, and use this log file to more fully analyze the link quality. The measurement data can be logged automatically at regular intervals or manually upon user-command.

For more information on log files, see “Logging Measurement Data” on page 5-14.

Site Monitor Window

The Site Monitor option enables you to display the communications quality between your Client Manager station and all Access Points within its range.

The site monitor has been designed for indoor roaming environments to:

- Determine the overall wireless coverage of your network.
- Verify or optimize the placement of your Access Points, in order to provide seamless roaming connectivity to mobile stations.

When roaming throughout a wireless network environment with your Client Manager station, you will be able to identify areas that may not have adequate coverage, or that suffer from in-band interference from other (wireless) equipment such as security gates, microwave ovens or photo copiers.

To start the site monitor, select **Site Monitor** in the **Advanced** menu in the main Client Manager window. This will display the window pictured in Figure 5-3 on page 5-9.

Options in the Site Monitor Window

- **Site Monitor** tab - the primary tab to monitor the performance of your wireless network (see “Site Monitor Tab” on page 5-8).
- **Selection** tab - enables you to scan for neighboring networks and select such networks for monitoring (see “Selection Tab” on page 5-10).
- **Log Settings** tab - allows you to enable, disable or configure the site monitor logging options (see “Logging Measurement Data” on page 5-14).
- **AP names** tab - allows you to create user-defined Access Point names for easy identification of Access Points in the Site Monitor window (see “AP Names Tab” on page 5-13).

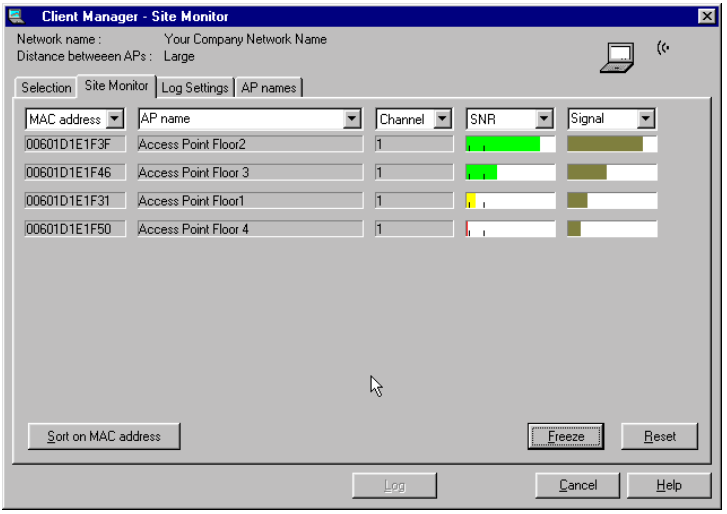
Note: The Site Monitor option only works in combination with Access Points. When you select this option in a Peer-to-Peer workgroup environment[1], the Site Monitor window will not start with the Site Monitor tab but will start with the Selection tab described on “Selection Tab” on page 5-10.

Site Monitor Tab

1. Independent networks never include Access Points (see also Part 2 “Wireless Configurations”)

When you open the Site Monitor window, this will display the window pictured in Figure 5-3.

Figure 5-3. Site Monitor window



Displayed across the top of the Site Monitor window are the following fields:

- **Current Network (SSID)** - which identifies the name of the network to which you are currently connected.
- **Distance between APs** - describes the Access Point density setting of the network to which you are currently connected.

These fields will remain visible when selecting any of the other options in the Site Monitor window.

Also displayed in the Site Monitor window are all Access Points that:

- Belong to the same Infrastructure as the one to which you are currently connected, and
- Are within range of your Client Manager station.

In the site monitor mode you can customize the selection of site monitor parameters to satisfy your personal preferences as described on “Customizing the Site Monitor Display” on page 5-10. The recommended selection for standard site survey procedures is as follows:

- **AP name** (Access Point name) - to identify devices by the name of the Access Point: This name is identified either in:
  - — The **System Name** field of the Access Point’s configuration (see “SNMP Parameters” on page 8-10).
  - — A user-defined Access Point **Name List**, that you can create using the Client Manager tool (see “AP Names Tab” on page 5-13).

- **SNR** - the signal to noise ratio which indicates the communications quality with the various Access Points.
- **Channel** - to identify which radio channel is used by each of the Access Points.

To perform a standard site survey:

1. Arrange the site monitor display as described above.
2. Determine which locations in your network environment require wireless connectivity.
3. Use a mobile computing device to walk through your wireless LAN environment.
4. Roaming throughout the network environment, verify that each location is covered by at least one Access Point that provides a level of SNR that is at least “Marginal” (Yellow) or better.
5. (optional) Use the **Sort on** button to re-arrange the display of Access Points by the data displayed in the first column.

   The first time you open the Site Monitor window, the Access Points are sorted in descending order of the SNR values.
6. (optional) To sort Access Points in a different way, simply select another display item in column one.

Customizing the Site Monitor Display

For specific purposes, you may wish to select one or more of the other parameters as well, for example:

- Display the signal level (**Signal**) and noise level (**Noise**) to determine the cause of a poor level of SNR.
  - — A low signal level would indicate a “weak” radio signal, i.e. the Access Point is almost ‘out-of-range’.
  - — A high noise level would indicate a source of interference in the radio path between your Client Manager station and the Access Point.

  The SNR, signal level and noise level can be displayed as dynamic indicators and/or numerical values in dBm.

Selection Tab

The **Selection** tab enables you to select another network, in situations where you wish to:

- Verify the presence of neighboring networks.
- Determine whether such network might interfere with your network.

Which Access Points will be displayed when you start the site monitor tool is actually determined by the configuration of the network name parameter on your Client Manager station (**Edit/Add Configuration Profile** in the **Actions** menu of the main Client Manager window). For example when the network name of your Client Manager station is set to:

- **A specific Network Name** - the station will:
  - — only connect to an infrastructure network identified by the same network name when the station is powered up.
  - — display only the Access Points belonging to that network that are within range of your Client Manager station.

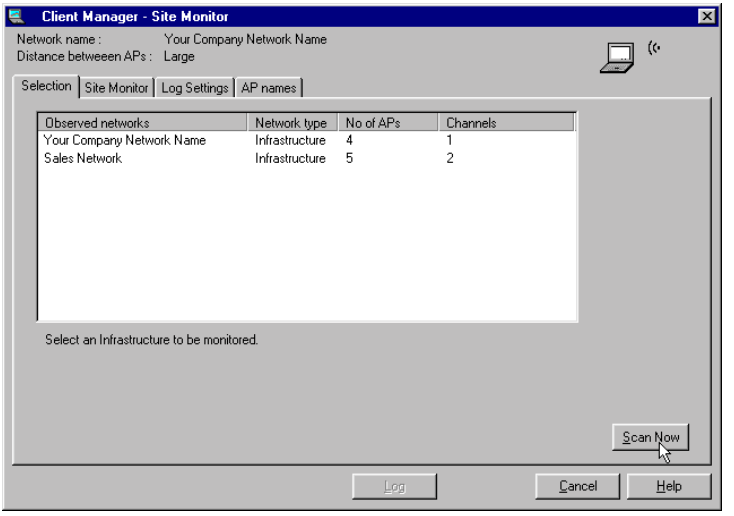
- "**ANY**" network - the monitoring station will:
  - connect to the first "open" network it sees when the station is powered up.
  - display all Access Points belonging to that network that are within range of your Client Manager station.

- **Peer-to-Peer** workgroup:
  — a workgroup is created between stations with the setting Peer-to-Peer.

Selecting another Wireless Network:

1. Click the **Selection** tab on the Site Monitor window to display the window pictured in Figure 5-4.

Figure 5-4. Select another Network to Monitor



The list of **Observed Networks** on this tab will show:

- All networks that are operational within the range of your Client Manager station.
- The type of network that might either be an:
  — Infrastructure network
  — Peer-to-Peer workgroup
- The number of Access Points in the observed infrastructure network(s).
- The different radio channels used by the Access Points.

2. (Optional) Click the **Scan Now** button to refresh the list of observed networks.
3. Click the network of your choice to return to the Site Monitor tab and display the diagnostic indicators[1].

Note: For reasons of security, the site monitor will not display the network name, and the MAC address or Access Point names of the neighboring network. You can display these values only for the infrastructure network to which you are actually connected.

1. Although the Site Monitor Selection tab will allow you to determine the presence of a neighboring Independent (Ad-Hoc) network, you can not select this type of networks for Site Monitor statistics. This is because this feature requires the presence of Access Points, that are typically not available in Independent networks (see also Part 2 “Wireless Configurations”).

When the list of **Observed Networks** does not show other networks, this means that:

- Your Client Manager station has been configured with a specific Network Name.
- This setting will not allow you to scan for/monitor other network infrastructures. To do so, you will need to reconfigure your station to use the Network Name “ANY”.
- There are no other networks operational in the vicinity of your Client Manager station, or
- The neighboring networks have been “closed” to deny wireless compliant devices to establish a radio connection when these devices have been configured with:
  - — The network name “ANY”, or
  - — A zero-string SSID (the equivalent of the network name “ANY”).

  For more information about “open” and “closed” networks, please consult Part 7 “Security”.

Log Settings Tab

You can record the Site Monitor measurement results to a log file, and use this log file to more fully analyze the overall wireless coverage of your network. The measurement data can be logged automatically at regular intervals or manually upon user-command.

For more information on log files, see “Logging Measurement Data” on page 5-14.

AP Names Tab

The **AP names** tab enables you to create a user-defined list of Access Point names associated with the MAC address of the wireless network interface(s) of your Access Points.

The field **AP name** in the Site Monitor window will display the value of the **System Name** parameter that has been assigned to the Access Point upon configuration[1].

To display this name it is required that your computer first establishes true data connections with such Access Points. This means your computer did not yet:

- Walk around
- Use the **AP Names** tab

When you are running the Client Manager tool in site monitor mode, you can use the **AP Names** tab to assign the Access Point name “on-the-fly” to any Access Point MAC address that you spot.

When you spot Access Points identified as “unknown” proceed as follows:

1. Open the tab **AP names**.
2. Enter a MAC address or double-click on one of the MAC addresses in the list.
3. Enter a name that allows for easy identification of this Access Point in the Access Point **Name** field.
4. Next click the **Add to Table** button to associate the name with this MAC address.
5. Repeat steps 2 through 4 for all other MAC addresses.
6. When finished return to the **Site Monitor** tab to proceed with the site monitor survey.

1. To assign a system name to the Access Point, you will need the AP Manager program specify this name in the “SNMP Parameters” window as pictured in Figure 8-6 on page 8-11.

When walking throughout the wireless networking environment, you may see new MAC addresses appear when approaching other Access Points. If that is the case, repeat the steps described above to complete your Access Point **Name** table.

The Access Point names you assign to a spotted MAC address will be saved into an ASCII file that you can use to:

- Share the file with other LAN Administrators that use the Client Manager tool to monitor performance of the wireless network. This file ("APlist.txt") is stored in "C:\Program Files\IBM Wireless LAN\Client Manager", or
- Edit the names later on, using an ASCII editor, such as the MS-Windows Notepad.

Logging Measurement Data

Both link test and site monitor enable you to log measurement results. The measurement data can be logged manually or at regular intervals automatically.

The Client Manager saves the data to a Comma Separated Value (*.csv) file 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.

Both the Link Test window and the Site Monitor window have almost the same log settings parameters. The only difference is that the Link Test window supports continuous data logging, which the Site Monitor window does not support.

Manual Data Logging

The manual data logging function allows you to take a snapshot of the measurement data at specific moment in time, 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 also wish to enable the **Add comments to log** 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 data logging option is typically used on Client Manager stations roaming the network running site monitor.

Automatic Data Logging

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

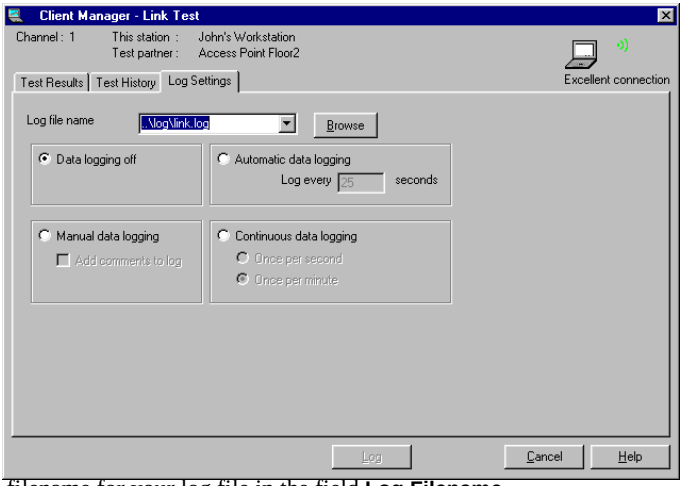
When you choose the automatic mode, you need to set the measurement interval to a specific number of seconds.

Automatic data logging is typically used when the Client Manager station is running a link test at a particular location.

Setting the Logging Options

1. Click the **Log Settings** tab in the Link Test window or in the Site Monitor window to display the window pictured in Figure 5-5.

Figure 5-5. Log Settings



2. Enter a filename for your log file in the field **Log Filename**.
   If you:
   - Enter a new filename - a new file is created.
   - Enter the same filename - the data will be appended
   - Use the default filename - the data will be appended.
3. Select the mode of logging:
   - **Data logging off** - no data is logged.
   - **Manual data logging** - to manually record your link measurements. Optionally, you can add comments each time you log data by clicking the “Add comments” check box.
   - **Automatic data logging** - to automatically log data. You must enter a time interval between measurements.
   - **Continuous data logging** (only available in Link Test window) - Automatically log data with the following interval:
     — **Once per second**, or
     — **Once per minute**

In all modes, the measurement data is saved in the file entered in the **Log 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 logging button will read either **Log Once** (manual option) or **Start Log** (automatic options).

- For manual logging, click the “Log Once” button each time you wish to log data. Logging stops automatically after the data is recorded to the log file.
- For automatic logging, click the **Start Log** button. Click the **Stop Log** button to stop the logging function.

Diagnose Card

If you suspect that your wireless client adapter may not be functioning properly, you can select **Diagnostics** in the **Advanced** menu of the main Client Manager window to investigate the functionality of the hardware and software of the card.

The Diagnose Card window allows you to check the software and firmware information, configuration information as well as communication statistics.

To test the wireless client adapter, click the **Test Card Now** button on the **Card Check** tab.

Note: Running the card test will disrupt the normal operation of your wireless client adapter, which may result in a temporary loss of your connection to the network.

If the wireless client adapter passes all tests, the test status will read “OK” in all fields, and the Error Code field will remain blank. If an error occurs, click the **Advice** button for more information on how to handle the error.

Troubleshooting Site Monitor

When the Site Monitor does not display (all of) the Access Points that you expected, this may be due to one or more of the following reasons:

- Your Client Manager station is “out-of-range” of the Access Points that you wish to monitor. Typically the values for signal level and SNR are ‘0’ (zero).
- A configuration mismatch of your Client Manager station, for example:
  - — Your Client Manager station uses a specific network name that does not match the name of the infrastructure that you wish to monitor.
  - — Your Client Manager station uses the network name “ANY”, and when it was powered up, the station erroneously connected to the Access Point of a neighboring network because that Access Point provided the best level of SNR.
- The infrastructure that you wish to monitor has been “Closed” to wireless IEEE 802.11 compliant devices that try to establish a radio connection using:
  - — The network name “ANY”, or
  - — A zero-string SSID (the equivalent of the network name “ANY”).

When your Client Manager station uses the network name “ANY”, you can use the **Selection** tab to see other networks as described on “Selection Tab” on page 5-10.

For more information on “open” and “closed” infrastructure networks, please consult Part 7 “Security”.

Using the AP Manager

You can use the AP Manager to:

- Display a standard set of SNMP variables to monitor general LAN traffic performance in your network (see “Remote Statistics Tab” on page 5-22).
- Display remote link test measurements (see “Remote Link Test Window” on page 5-19) between a (remote) Access Point of your choice and a wireless station connected to the selected Access Point.

The AP Manager has been designed to monitor your network from a central location (e.g. the LAN administrator station) enabling you to monitor wireless performance in areas that can not easily be reached. For example: wireless networks in remote locations.

Monitoring Options

The AP Manager program offers a variety of diagnostic options of which the following two are the most relevant for standard users:

- System information (see “System Information” on page 5-18)
- Remote link test (see “Remote Link Test Window” on page 5-19)
- Remote statistics (see “Remote Statistics Tab” on page 5-22)

All other diagnostic options are standard SNMP tallies that are not described in this manual, but documented in the on-line help system of your AP Manager program.

Note: All diagnostic options are described in the on-line help information of the AP Manager. To access that you can access by pressing the F1 function key or clicking the **Help** button in your AP Manager window.

Connecting to Access Points

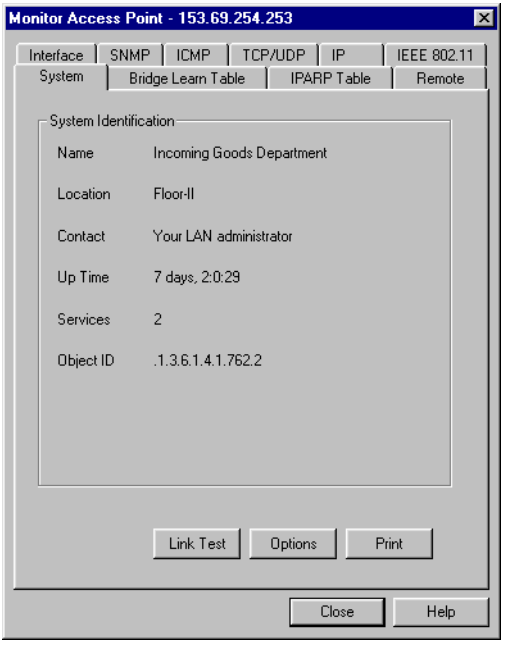
To start monitoring the Access Point, you must first connect to the target Access Point.

1. Start the AP Manager program.
2. Select the target Access Point from the local list or enter the IP address of the Access Point that you wish to monitor.
   Alternatively, you can select **Refresh Access Point List** from the Access Point menu to display all Access Points available in your subnet.

Note: Only Access Points in the same subnet as the management station are displayed in the list. To investigate a link outside of the subnet, enter the specific IP address in the **Enter the IP address of a specific** Access Point field.

3. Click **Monitor** to connect to the target Access Point.
4. The monitor mode of the AP Manager window is displayed as pictured in Figure 5-6. You can now monitor your network.

Figure 5-6. System Information Window



System Information

The system information does not provide on-line statistics, but is primarily used to verify the version level of the embedded software that is loaded into the Access Point.

To display the system information for the Access Point, you must first connect to the target Access Point (see “Connecting to Access Points” on page 5-17).

Select the **System** tab to view the system information.

- The fields **Name**, **Location** and **Contact** represent the values that have been entered in the corresponding fields of the **SNMP** tab in de edit mode when the Access Point was configured.

  If you would like to change these names, please consult the section about configuring SNMP parameters as described in “SNMP Parameters” on page 8-10.

- The **Up Time** field displays the time interval measured from the last time the Access Point was reset. If the up time is lower than expected, the Access Point may have been reset manually or rebooted automatically.

- The fields **Services** and **Object ID** do not display relevant information to end-users. You will need these values and the contents of the **Description** field only when contacting Technical Support to report a problem.

  Providing this information to your Technical Support representative will help to determine the cause of the problem.

  To do so, you can either:

— Use the **Print** button to print the information to paper that you will fax to your authorized reseller together, or

— Press the keys ALT and Print Scrn simultaneously to copy the contents of this screen to the Windows clipboard, and paste the screen capture into the e-mail that you will send to your authorized reseller.

- The field **Description** is the most important field of this screen. It allows you to quickly determine whether the Access Point is running with the latest embedded software, or might require an upgrade to support all the High Rate Wireless LAN functionalities required.

  The **Description** field of contains a set of strings to identify:

  — The type of networking device (typically High Rate Wireless LAN Access Point)

  — The type and version of the embedded software that is loaded into this Access Point. The value can be:

    - **VX.xx**[1] to identify software that supports Access Point services only

  — The character string of the format **SN-xxUTxxxxxxxx** represents the unique serial number of the Access Point.

  — The last string of characters of the format **VX.xx** identify the version of the Access Point hardware in its “processor module”.

  When reporting a problem to your Technical support representative, always include a completed problem report form. You can find this form in ASCII text format (report.txt) on the Access Point software diskettes and the IBM High Rate Wireless LAN website.

Note: Updates for the embedded software of the Access Points are usually released via the IBM website at: **http://www.ibm.com/pc/support**, and with new releases on the software CDs.

You are advised to consult the IBM website at regular intervals to find out whether newer software is available for your Access Points.

Remote Link Test Window

The AP Manager remote link test enables you to investigate the radio link between the Access Point of your choice (the “initiator station”) and a station connected to the selected Access Point.

This station can be a wireless station connected to the selected Access Point.

Note: The remote link test works only in combination with Access Points.

The user-interface of the AP Manager Remote Link Test is very similar to the Link Test of the Client Manager.

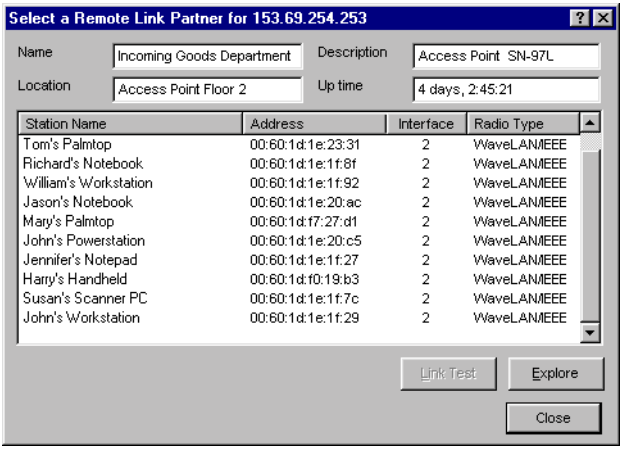
Starting the Remote Link Test

To display the remote statistics for the Access Point, you must first connect to the target Access Point as described in “Connecting to Access Points” on page 5-17.

1. To support Access Point services for PC Cards this value must read V3.57 or higher.

1. Select the **System** tab and click the **Link Test** button to display the window pictured in Figure 5-7.
   The fields in the top section of this window identify the “initiator station” you selected when connecting to the Access Point.

Figure 5-7. Select a Link Test Partner



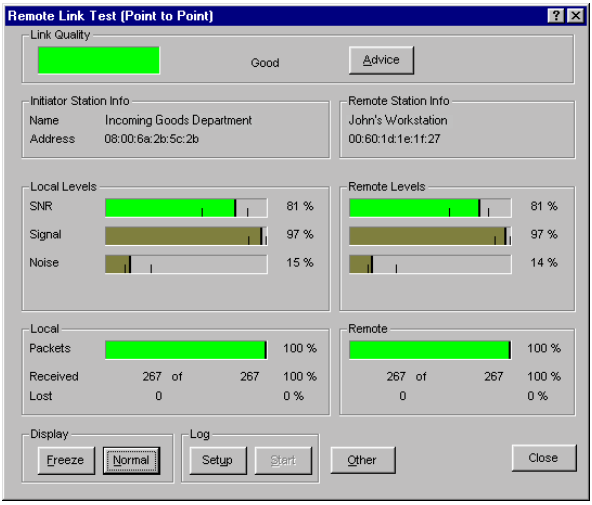
The middle section of the “Select Remote Link Partner for ..." window displays all wireless devices connected to the “initiator station”. The following fields are visible:

- The fields **Station Name** and **Address** these wireless devices are identified by their station name and MAC address respectively.
  This list may change as roaming mobile stations enter or exit the coverage area of the selected Access Point.
- The **Interface** field identifies the slots of the Access Point into which the PCCard has been inserted.
  — 2 = PC Card slot A
- The **Radio Type** field identifies the type of PC Card (in the corresponding slots):
  — IEEE 802.11 for PCCards

2. (Optional) To refresh the list, click the **Refresh** button.
3. Select a station from the list and click the **Link Test** button to display the Remote Link Test window as pictured in Figure 5-8 on page 5-21.

Note: Subject to the “Radio Type” of the wireless network interface that you selected, the lay-out of the Remote Link Test windows may differ. The window pictured in Figure 5-8 represents the window for the wireless network interface.

Figure 5-8. Remote Link Test window



Important Indicators to Monitor

The Signal to Noise Ratio (SNR) identifies the communication quality of the radio path between the initiator station (i.e. the Access Point) and its remote link test partner.

The color of the SNR indicator, the link quality indicator, and the remote levels indicators relate to the following levels of communications quality:

Color	Description
■ Green	Communication quality is “Good”, no intervention is required.
■ Yellow	Communication quality is “Marginal”, no intervention is required.
■ Red	Communication quality is “Poor”, intervention required. (see Appendix B “Troubleshooting”)
■ Blank	No connection

If the level of SNR is lower than expected the signal and noise level indicators may help you investigate the cause.

Click the **Details** button to show the signal and noise level indicators.

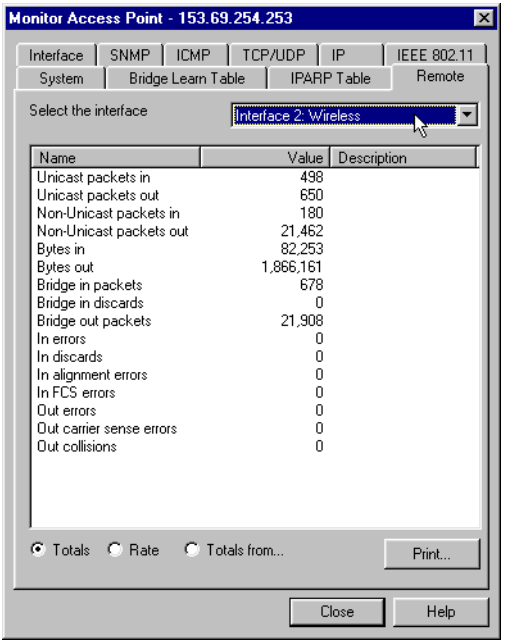
- A low signal level indicates that the “strength” of the radio signal is fairly low, i.e. the Access Point selected link test partner has moved “out-of-range”.
- A high noise level indicates a source of radio interference in the radio path between the Access Point and its link test partners.
  Comparing the values for the Access Point and its link test partner will help you to identify the location where the interference occurs, and investigate whether any actions to eliminate or remedy the source interference resulted in a better performance.

For more information about the Remote Link Test window please consult the AP Manager on-line help documentation by clicking the **Help** button or pressing the F1 function key on your keyboard.

Remote Statistics Tab

The remote statistics option allows you to monitor a set of SNMP variables for each of the Access Point interfaces (both Ethernet and wireless).

Figure 5-9. Remote Statistics information



Starting Remote Statistics

To display remote statistics for the Access Point, you must first connect to the target Access Point as described in “Connecting to Access Points” on page 5-17.

1. To view the remote statistics, select the **Remote** tab from the AP Manager window in the monitor mode (see Figure 5-9).

The performance for each of the interfaces of the selected Access Point can be displayed. Selecting the interface of your choice from the **Select the interface** pull down menu.

Note: When one of the items in the pull down menu displays “WaveLAN(-I)”, the corresponding socket of the Access Point contains a WaveLAN Legacy card. To interpret network interface tallies for this type of WaveLAN PC cards, please consult the AP Manager on-line help documentation, or visit the IBM website at: **http://www.ibm.com/pc/support**.

Important Indicators to Monitor

The AP Manager **Remote** tab statistics display a wide range of variables that provide information about the performance of the selected Access Point.

The indicators which provide the main monitoring information is called the **ratio of Errors to Bridge Packets**. There are three ratios which are of particular diagnostic value:

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

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

Table 5-1. Ratio of Errors to Bridge Packets

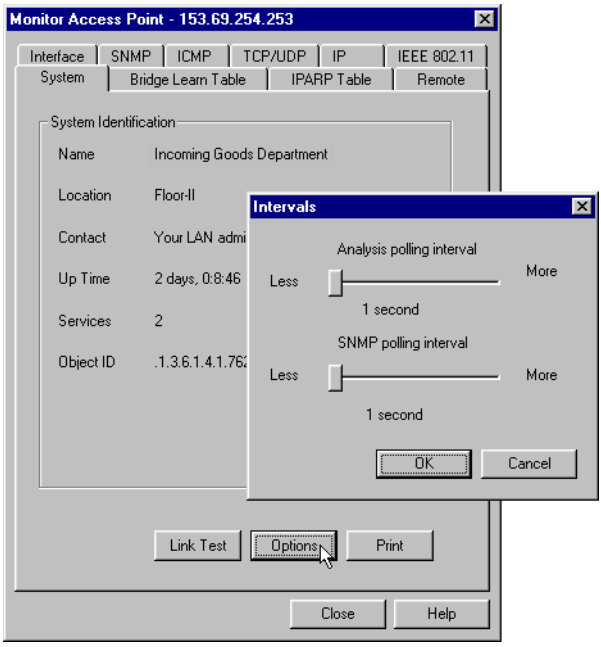
Ratio Errors to Bridge Packets	**Conclusion**	
0.1% or less	Status:	Performance is Good.
	Impact:	None.
	Action:	None.
0.1% and 1%	Status:	Performance is acceptable.
	Impact:	Network performance is OK, but your network might not perform as well as you expected.
	Action:	Refer to Part 6 “Optimizing Performance” 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 Part 6 “Optimizing Performance” 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 Part 6 “Optimizing Performance” to investigate the problem in more detail. You may need to consult an external expert.

System Intervals

To display the system interval parameters to monitor the Access Point, you must first connect to the target Access Point as described in “Connecting to Access Points” on page 5-17.

Select the **System** tab and click the **Options** button to display the window pictured in Figure 5-10.

Figure 5-10. Intervals window



In the Intervals window two different time interval parameters can be set to change to monitor interval settings:

- Analysis polling interval (used for remote link test)
- SNMP polling interval (used for SNMP statistics)

Adjusting Analysis Polling Interval

Subject to the type of connection, you can adjust the refresh rate of the remote link test results, also identified as the analysis polling interval.

While the remote link test will proceed to continuously collect measurement results, the selected Access Point (initiator station) will transfer the results to the LAN administrator station at regular intervals, which can vary from 1 to 15 seconds.

- Use a short time interval (e.g.1 second) for on-line monitoring, e.g., when troubleshooting or when you have full bandwidth access via the local network.
- Use a longer time interval (e.g. 15 seconds) when you run a remote link test only for background information purposes, or in cases when you access the initiator stations network via a low-speed connection (e.g. a dial-up modem connection).

Adjusting SNMP Polling Interval

The data displayed in the **Remote** tab refreshes at regular intervals that can vary between 1 second and 5 minutes. Adjust the refresh rate by changing the SNMP polling interval.

- Use a short interval (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 Access Point via the local network.
- Use a long interval (5 minutes) when you run remote statistics only for background display purposes, in cases when you access the network of the selected Access Point via a low-speed connection (for example a dial-up modem connection).

Part 6: Optimizing Performance

Introduction

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 High Rate Wireless LAN network to optimize its performance.

Consider optimizing network performance in these situations:

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

In this chapter, we recommend various solutions to some of the most commonly reported problems. 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 Access Point, 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.**

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”, usually referred to as “payload”, also includes messages that were retransmitted one or multiple times as a result of a collision, malfunctioning cable connection or poor radio link.

  In the AP Manager Remote tab in the monitoring mode, the “True Data” is displayed as Unicast Packets.

- **Network Overhead Data -** is data exchanged between network services to control the dataflow. This overhead data that usually referred to as “traffic load”, includes protocol and broadcast messages and/or error messages that result from a configuration mismatch.

  In the High Rate Wireless LAN AP Manager Remote tab in the monitoring mode, 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. However when the ratio of network overhead is more than actually

required, this may affect the performance of your wireless LAN, because your “True Data” has to share the bandwidth capacity with the network overhead.

Eliminating redundant traffic can significantly improve the performance of your network. Using the AP Manager you can choose from one or more of the following options:

- Protocol Filtering (page 6-2): to filter protocols that are not relevant to wireless stations.
- Optimizing Wired Connections (page 6-3): to eliminate redundant error messages due to failing connections.
- Optimizing Wireless Connections (page 6-5): to avoid retransmission of lost or collided frames.

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 stations. In these cases, protocol filtering may prevent the transmission of unnecessary data, saving more bandwidth for the communication of “true data” in your network.

Do You Need Protocol Filtering?

To diagnose whether or not the protocol broadcasts degrade the performance of a wireless network, you can use the Remote Statistics tab as described on “Remote Statistics Tab” on page 5-22.

1. Start the AP Manager and select the Access Point and click the **Monitor** button.
2. From the **Monitor** menu, select **Remote Statistics**.
3. Select the **Remote** tab to display the interface statistics.
4. Compare the number of **Out collisions** with the number of **Bridge out packets**.
    - When the number of “Out collisions” is less than 1% of the “Bridge out packets”, this indicates that the wireless medium is performing fine, i.e. protocol filtering is not required, but might still be considered.
    - When the number of “Out collisions” is more than 1% of the “Bridge out packets”, this indicates that the wireless medium is very busy.
      If the wireless medium is busy, and you do not see many users or excessive traffic on the network, it might be worth investigating whether protocol filtering will improve your network performance.
5. Compare the number of **Unicast packets out** to the number of **Non-Unicast packets out**.
    - When the number of “Non-Unicast packets out” is relatively high when compared to the number of “Unicast packets out”, 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.

Filtering Network Protocols

When you suspect that network protocols are adversely affecting the performance of your network, use the following procedure to filter out unnecessary or unwanted network protocols.

1. Investigate what type of network stations and services are located in the environment of your network.
2. Consult the documentation that came with your network operating system to investigate which protocols are required for network servers and services, and for the (wireless) stations.
3. Start the AP Manager program.
4. Select the Access Point of your choice and click the **Edit** button.
5. Select the **Bridge** tab to show the protocol filtering information.
6. On the top-right side of the protocol filtering section, click the **Edit** button to open the Protocols to Filter window (pictured in Figure 8-2 on page 8-6).
7. Place a check mark for all protocols that you wish to filter.
8. (Optional) To add a non-listed protocol to the list, click the **Custom** button to enter the protocol manually.
9. When finished click **OK** to return to the **Bridge** tab.

   All of the protocols that you have selected, and/or all of the custom protocols that you have added manually, will be listed in the **Protocol Filtering** field.
10. Click **OK** again to save the changes to the Access Point and to return to the main window of the AP Manager.
11. Download a backup file as described in "Step 4 - Create a Back-up of the Configuration" on page 4-5.

    When prompted to enter a name for the back-up file, you are advised to select a name that is different from the original configuration file.

    Do not overwrite the previous version of the back-up file, since this might jeopardize your ability to restore the original configuration if this change did not result in the expected performance increase.

Repeat the steps as described under "Do You Need Protocol Filtering?" on page 6-2 to see whether this change resolved your problem. If this does not solve your problem, consider one of the following options:

- Optimizing wired connections
- Optimizing wireless connections

Optimizing Wired Connections

Sometimes performance degradation of your (wireless) connection is caused by a failure in the cabling system that connects the 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.

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 found on “Remote” tab in the monitor mode of the AP Manager.

1. Select **Interface 1: Ethernet** from the pull-down menu to display the statistics for the ethernet interface.
2. Compare the number of **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 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.
5. Check whether the problem occurs only with the selected Access Point, or with multiple Access Points.
    - If the problem is observed on only one Access Point, the problem may lie in the connectors or cable(s) that connect the Access Point to the hub or wired backbone.
    - When the problem exists with multiple Access Points, 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.

Troubleshooting Cabling Problems

Using the procedure described above, you may have determined the area where a cabling error might be suspected. To resolve the problem, carefully check the cabling system in this area to verify whether all connectors are properly seated at the:

- Access Points
- Bridges, routers and hubs
- Wired stations connected to the cabling system.

If your network uses BNC 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 found on the **Remote** tab in the monitor mode of the AP Manager.

1. Select **Interface 1: Ethernet** from the pull-down menu to display the statistics for the Ethernet interface.
2. Compare the number of **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.
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 and/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 High Rate Wireless LAN equipped devices will be grouped into the same LAN segment. High Rate Wireless LAN 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:

- Protocol Filtering (page 6-2)
- Optimizing Wireless Connections (page 6-5)

Optimizing Wireless Connections

When the link quality of communications between a wireless station and its Access Point is 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.

Please note that:

- Many retransmissions may affect your effective data throughput efficiency as the “true data” has to share the wireless bandwidth with the re-transmitted frames.
- The retransmissions will also degrade the performance as perceived by the end-user of a wireless stations: e.g. saving a file will take longer if many retransmissions are required.

A poor link quality can be caused by one or more of the following problems:

- The station is almost out of range of the Access Point.
- There is a source of interference in the signal path between the station and the Access Point.
- A station may be "hidden" from another station within the same coverage area (for more information on hidden stations, see the section "RTS/CTS Medium Reservation" on page 6-8).

Diagnosing Link Quality

The occurrence of a poor link quality on the wireless network can be diagnosed in different ways.

- You can use the AP Manager tool to diagnose the quality of radio communications on-site as described in Part 5 "Monitoring your High Rate Wireless LAN Network", or
- Use the AP Manager tool to investigate from your current location whether a specific remote area is suffering from poor radio performance.

  The AP Manager provides the following options to diagnose radio link quality:

  — The remote link test

  — The IEEE information

  — The Remote Statistics tab

These tallies can be useful in determining whether or not the performance of your network is caused by interference.

Remote Link Test

For instructions about the Remote Link Test window that displays communications as dynamic indicators, please refer to the information about this window as described on "Remote Link Test Window" on page 5-19.

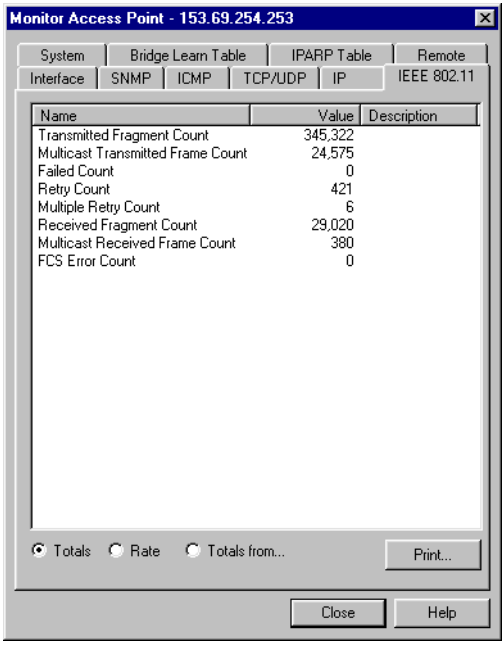
Important indicators to monitor on the Remote Link Test window are:

- Signal to noise ratio (SNR) for an overview of the radio link quality.
- Signal level to determine whether a poor SNR is related to a weak radio signal (i.e. a station is "out-of-range").
- Noise level to determine whether a poor SNR is related to a source of interference.

IEEE Information

The IEEE information on the **IEEE 802.11** tab in the monitor mode allows you to track frame activity on the IEEE interface of the Access Point.

Figure 6-1. IEEE information tab



The three indicators that you should pay particular attention to are:

- **Retry Count** - counts the number of frames that are lost (due to collisions) during the initial transmission. During normal operation, the **Retry Count** should be less than 3% of the **Transmitted Fragment Count**.
- **Multiple Retry Count** - counts the number of frames that are lost after the initial transmission. During normal operation, the **Multiple Retry Count** will be less than 3% of the **Retry Count**.
- **Failed Count** - counts the number of frames that have reached the **Retry Limit**. Failed frames will no longer attempt to re-transmit.

  If the **Failed Count** is 1% or more of the **Multiple Retry Count**, your network may be suffering from interference. Use the AP Manager Remote Link Test Window (page 5-19) to look for either suddenly high noise figures, or low SNR values, to find the cause of the interference.

Remote Statistics Tallies

Select the **Remote** tab in the monitor mode. Select either one of the interfaces from the pull-down menu to display the statistics for the wireless network interface(s). Then, use the following to diagnose link quality:

1. Compare the number of **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 wireless medium is very busy.
2. 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.

3. 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 wireless 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.

4. You can also use the AP Manager 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 Access Point.

   - 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 Access Point.

5. 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 a poor signal you may consider:
     — Connecting the Range Extender Antenna to the station or Access Point that suffers from poor radio performance.
     — Adding an extra Access Point to the network, or
     — Adjusting the placement of your Access Points and/or antennas to provide coverage for all wireless stations.

   - If you suspect a “hidden” station, see “RTS/CTS Medium Reservation” on page 6-8.

Note: You can also use the Client Manager to analyze the link quality between a remote station and the Access Point. In that case, you will need to have access to the “problem location” to perform on-site diagnostics.

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

- Protocol Filtering (page 6-2)
- Optimizing Wired Connections (page 6-3)
- Designing High Capacity Networks (page 6-16)

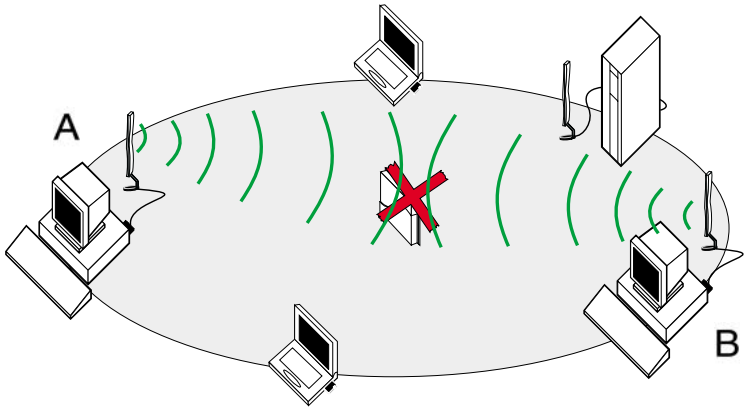
RTS/CTS Medium Reservation

It is normal behavior for High Rate Wireless LAN stations to defer transmissions automatically when they sense that another wireless device is using the wireless medium.

This behavior also referred to as the Carrier Sense Multiple Access/Collision Avoidance protocol (CSMA/CA) will avoid that wireless messages would collide in situations where two or more stations would start transmissions at the same time.

The RTS/CTS medium reservation mechanism enables you to improve wireless performance in network environments where the CSMA/CA protocol would fail due to the “hidden station” problem as pictured in Figure 6-2.

Figure 6-2. The Hidden Station Problem



RTS/CTS medium reservation may provide a solution for networks where:

- The density of stations and Access Points is very low.
- You witness poor network performance due to excessive frame collisions at the Access Points.

About the Hidden Station Problem

A hidden station is a situation in which two wireless stations are within range of the same Access Point, but are not within range of each other.

Figure 6-2 on page 6-9 illustrates an example of the “hidden station” problem. Both station A and station B are within range of the Access Point however, station B cannot “hear” station A, therefore station A is a “hidden station” for station B.

When station B starts to communicate with the Access Point, it might not notice that station A is already using the wireless medium. When station A and station B send messages at the same time, they might collide when arriving simultaneously at the Access Point. The collision will most certainly result in a loss of messages for both stations.

In situations as pictured Figure 6-2, RTS/CTS medium reservation may provide a solution to prevent message collisions by handing over transmission control to the Access Point.

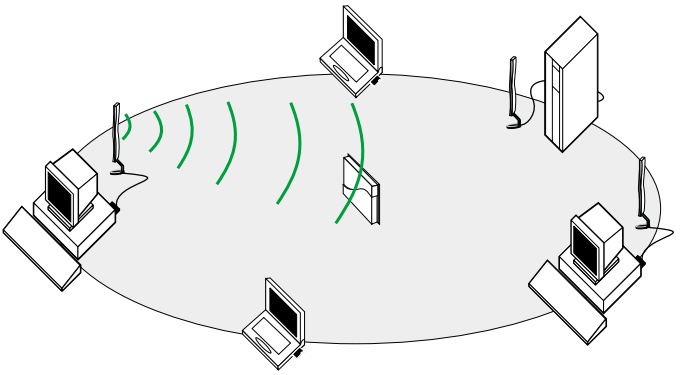
Troubleshooting a “hidden station” problem usually provides the best results when it is performed on the suspected stations that suffer from errors as a result of the “hidden station” problem.

When configuring the PCCard parameters of an individual station you can enable the RTS/CTS Medium Reservation parameter:

- To enable RTS/CTS Medium Reservation parameter, choose **Add/Edit configuration profile** in the Client Manager, select the **Advanced** tab and enable **RTS/CTS Medium Reservation**.

You can enable RTS/CTS Medium Reservation on individual stations, i.e. the setting of this parameter does not have to be the same for all High Rate Wireless LAN equipped devices in your network.

Figure 6-3. Medium Reservation "Request to Send"



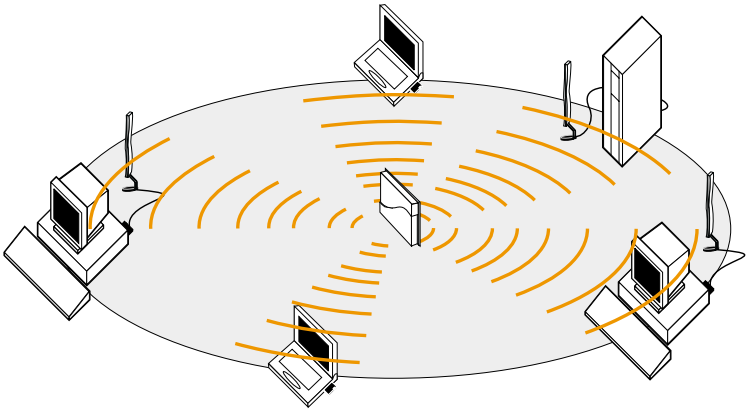
About the Medium Reservation Mechanism

When you enable RTS/CTS medium reservation on a suspect "hidden station", this station and its Access Point will use a Request to Send/Clear to Send protocol (RTS/CTS).

- The station will send an RTS to the Access Point, that will include information about the length of the frame that the station would like to transmit (see Figure 6-3).
- Upon receipt, the Access Point will respond with a CTS message to all stations within its range to:
  - — notify all other stations to defer transmissions for the time-frame of the requested transmission.
  - — confirm the requestor station that the Access Point has checked the medium for availability, and has reserved it for the time-frame of the requested transmission.

  The CTS process is shown in Figure 6-4 on page 6-11.

Figure 6-4. Medium Reservation "Clear to Send"



Note: In most networking environments it is very unlikely that you will need to enable RTS/CTS medium reservation on the Access Point to prevent collisions.

Since all stations connected to the Access Point are typically within range of that Access Point, they should be able to sense whenever the Access Point is using the medium to transmit messages via the wireless medium.

Enabling RTS/CTS medium reservation on the Access Point would require the Access Point to ask for a CTS for every message that it wishes to forward to stations within its range, even if it is forwarding traffic between stations that belong to the same wireless cell.

This might cause redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

If you insist on enabling RTS/CTS medium reservation on the Access Point, you will notice that the configuration of this option for Access Points is slightly different from that of stations.

The Access Points allow you to customize the sensitivity of the RTS/CTS mechanism. By entering a user-defined frame length value in the **RTS/CTS Medium Reservation Threshold** field (in the edit mode, select **Interface** tab, then click the **Advanced** button), you can influence when the Access Point should apply the RTS/CTS mechanism. For example:

- When a message is shorter than the RTS/CTS medium reservation threshold, the Access Point will not initiate an RTS to the addressed station, but use the CSMA/CA protocol: i.e. it will immediately transmit the message when it senses that the medium is free.
- When the length of a message exceeds the RTS/CTS medium reservation threshold, the Access Point will first send an RTS to the addressed station and defer transmission until the addressed station has responded with a CTS message.
  All other stations will defer their transmissions for the duration of the "radio-silence time" identified in the CTS message.

Enabling RTS/CTS Medium Reservation

1. Start the AP Manager program, select the Access Point that services the wireless cell where you suspect poor performance caused by a hidden station problem and click the **Edit** button.
2. Select the **Wireless Interfaces** tab.
3. Choose the socket that contains the network interface that suffers from a hidden station.
4. Click the **Advanced** button.
5. Click the **RTS/CTS Medium Reservation** check box.
6. In the **Threshold** field, enter a value in the range of 0 to 2347.

   By default, the RTS/CTS medium reservation threshold is 2347 (disabled) which means that RTS/CTS will not be used.

   - In a network using RTS/CTS medium reservation, a typical setting for the medium reservation threshold is 500.
   - Alternatively enter a value of your choice.

   The value you enter here will determine when the Access Point will issue a Request to Send (RTS). For example, if the value you select is 500:

   - The Access Point will send use the RTS/CTS protocol for each message that exceeds the length of 500.
   - Messages with a length that is shorter than 500, will be transmitted according to the standard CSMA/CA protocol.
7. Click **OK** to return to the Interface tab.
8. Click **OK** again to save the new configuration to the Access Point and to return to the main AP Manager window.
9. Next create a backup-file of the new configuration (see “Step 4 - Create a Back-up of the Configuration” on page 4-5).

Frequency Channel Management

When your network consists of more than one Access Point, we recommend that you alternate sub-channel frequencies between adjacent Access Points to provide more bandwidth to the wireless stations in each cell.

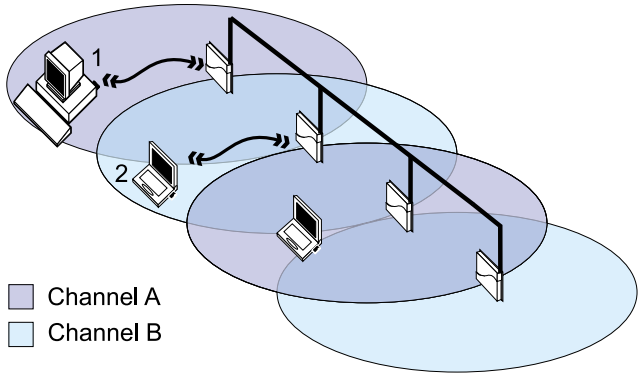
The number of available channels is subject to local radio regulations that apply in your country. A list of supported channels for your country can be found in the online documentation of the Wireless Client Adapter.

Dual Channel Configuration

A Dual Channel system could look as follows (see Figure 6-4):

- All Access Points identified as operating on channel A would use channel 1 (2412 MHz).
- All Access Points identified as operating on channel B would use channel 11 (2462 MHz).

Figure 6-5. Dual Channel Configuration



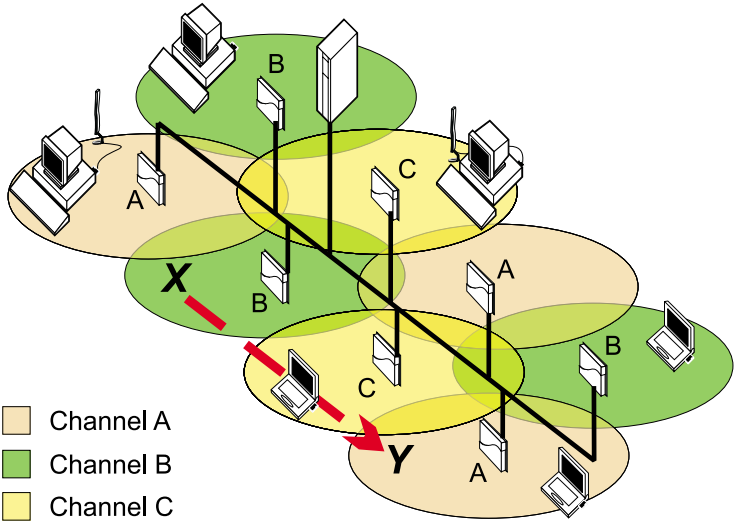
This way you can apply a maximum channel separation for neighboring Access Points that will easily satisfy the requirements recommended for optimal operation.

Station 1 would use channel A to communicate with its Access Point without bothering station 2 to defer its transmissions to the neighboring Access Point. When either one of the stations would roam to another location, it will automatically switch its radio to any other operating channel required to remain connected to the network.

Multiple-Channel Configuration

You can alternate the frequency channels of your Access Points between three or more sub-channels (depending on local radio regulations that apply in your country).

Figure 6-6. Multiple Channel Configuration



For example, looking at Figure 6-5, to set up a three channel system you could configure the Access Points as follows:

- All Access Points identified as operating on channel A would use channel 1 (2412 MHz)
- All Access Points identified as operating on channel B would use channel 6 (2437 MHz),
- All Access Points identified as operating on channel C would use channel 11 (2462 MHz)

This would just meet the minimum channel separation of 25 MHz for neighboring Access Points that is recommended for optimal operation.

A station roaming from location ***X*** to location ***Y*** would automatically switch its radio consecutively from channel A, B to C to remain connected to the network.

In that case, you must assign different frequency channels to each card (with a separation of 25 MHz or more) to avoid cross-talk between the two cards.

Configuring Channel Frequency

To change the frequency of your Access Point, proceed as follows:

1. Connect to the Access Point by opening the AP Manager, selecting the target Access Point, and click the **Edit** button.
2. Select the **Wireless Interfaces** tab.
3. Choose the socket (A or B) for the network interface that you would like to configure.
4. Click the **Advanced** button. A pull-down box will appear. Select the frequency of your choice. The number of channels is subject to local regulations.
5. In the Wireless Advanced Setup window, use the **Channel** pull-down menu to select a sub-channel that allows for maximum channel separation from neighboring Access Points (minimum channel separation: 25 MHz).

   Table 6-1 lists a number of successful channel combinations that you can use to configure High Rate Wireless LAN networks with multiple Access Points.

   - For Dual Channel Configuration (page 6-12), alternate between channels A and B.
   - For Dual Channel Configuration (page 6-12), alternate between channels A, B and C

Note: The availability of the listed channels in Table 6-1 is subject to local radio regulations that apply in your country. A complete list of supported channels for your country can be found in the online documentation of the Wireless Client Adapters.

Table 6-1. Recommended Sub-Channel Configurations

Channel A	Channel B	Channel C
2412 MHz (1)	2437 MHz (6)	2462 MHz (11)
2417 MHz (2)	2442 MHz (7)	2467 MHz (10)
2422 MHz (3)	2447 MHz (8)	

For wireless networks where wireless cells only have a slight overlap, you may also experiment with multiple channel configuration using a channel separation of less than 25 MHz, for example using the channels as listed in Table 6-2.

Table 6-2. Optional Sub-Channel Configurations

Channel A	Channel B	Channel C	Channel D
2412 MHz (1)	2427 MHz (4)	2442 MHz (7)	2457 MHz (10)

6. Click **OK** to close the Wireless Advanced Setup window and return to the **Wireless Interfaces** tab.
7. (Optional) Repeat steps 3-6 to verify and/or change the frequency for the second network interface in this Access Point.
8. Click **OK** again to save the new configuration to the Access Point and to return to the main AP Manager window.
9. Next create a backup-file of the new configuration (see “Step 4 - Create a Back-up of the Configuration” on page 4-5).
10. Update the “Access Point Configuration Record” in Appendix A “Start-up Configuration” to reflect these changes.
11. (Optionally) Modify the configurations of all your other Access Points accordingly. We recommend that you use different frequencies for neighboring Access Points, as described in Dual Channel Configuration (page 6-12) or Multiple-Channel Configuration (page 6-13).

Link Integrity

In situations where the connection of the Access Point to the rest of the Ethernet network fails, typically as a result of a broken cable connection or network error, the Ethernet failure might disrupt regular network communication for (roaming) wireless stations.

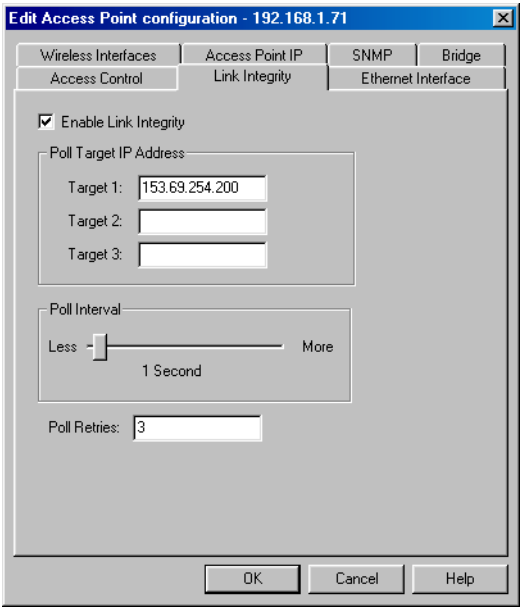
> **CAUTION:**
> **This feature is only used if your network provides duplicate ethernet connections.**

If the wireless connection however is still intact, the wireless station would not roam to another Access Point, since its radio might still interpret its “physical” connection to the Access Point as “good” or “acceptable”.

The Ethernet link integrity feature is a high-end solution that enables you to resolve this type of network failures, as it allows Access Points to:

- Detect any disruption in its connection to network services by testing the link between the Access Point and a maximum of three IP hosts.
- Reconnect automatically to another Access Point in situations where disruptions occur that are not related to poor radio communications.

Figure 6-7. Link Integrity Window



For more information about link integrity refer to the help-file of the AP Manager program.

Designing High Capacity Networks

In networking environments where you have either data intensive users, or a large number of users in a small area, you may wish to improve the throughput efficiency and/or load balancing of your Access Points.

This solution described in this section allows you to balance “maximum range for minimum hardware investments” versus “maximum throughput performance for higher hardware investments”.

About the CSMA/CA Protocol

In normal network configurations, all equipped devices apply a standard mechanism to avoid collision of wireless messages. When a station intends transmitting a message, it will first sense whether no other station is already transmitting (“using the wireless medium”).

- If no other transmissions are sensed, the station will start its transmission.
- If it does sense another transmission carrier, the station will apply a random defer timer. After the timer has expired it will start sensing the medium again to see if it can start transmitting.

This protocol, also referred to as the “Carrier Sense Multiple Access/Collision Avoidance” (CSMA/CA) protocol works fine in most networking environments. The user of a wireless computing device will hardly notice the deferral behavior of the wireless radio.

In network environments with many wireless users in the vicinity of one another and/or wireless stations that are engaged in heavy data traffic, you may perceive that wireless stations show a degrading performance, perceived as long network response times when communicating via the network.

Where poor performance is typically caused by poor radio link quality (identified by a poor a signal to noise ratio (SNR)), the scenario described above may also be perceived in areas where:

- Site monitor measurements show an excellent wireless coverage by at least two Access Points or more on every location.
- Link test measurements at such locations may show:
  - An excellent SNR for communications between wireless stations and the Access Point.
  - A large number of messages transmitted at lower rates.

In this type of situations the disappointing network performance might be caused by the busy wireless traffic in that area, where the CSMA/CA protocol causes the wireless stations to defer transmissions to often for either:

- Heavy data traffic by other stations in the same wireless cell
- Traffic from stations in neighboring cells, where stations in a location where wireless cells overlap one another seem to suffer more than the other stations.

The last example would typically occur only in networks where all Access Points have been configured to operate at the same frequency, or at frequencies with an insufficient channel separation (see “Frequency Channel Management” on page 6-12).

Influencing the Deferral Behavior

To overcome the performance issue described on previous pages, you can choose to design a high performance network based on the following principles:

- Add more Access Points to your network.
- Configure Access Points in neighboring cells to operate at different frequency channels with a maximum channel separation (see “Frequency Channel Management” on page 6-12).
- Adjust the **Distance Between APs** parameter to optimize the load balance of the number of wireless stations per Access Point (see “Distance Between APs” on page 8-2).

> **CAUTION:**
> **Distance between APs is a parameter that must be set on both the wireless stations and the Access Point. The values that you select must be the same for ALL High Rate Wireless LAN equipped devices in your network to avoid unpredictable behavior of your network and the roaming connectivity of wireless devices.**

By changing the **Distance between APs** parameter from **Large** to **Medium** or **Small**, you can virtually reduce the receiver sensitivity of the wireless radios, that will show the following behavior:

- The stations will show a more active roaming behavior and connect to one of the added Access Points more quickly.
- Considering the fact that you have added more Access Points, the deferral behavior does no longer need to be as strict in environments where the density of installed Access Points was fairly low:
  - The stations will only defer transmissions when the signal level of a message sensed on the wireless medium equals or exceeds a specific level.
  - Messages with a low signal level are not likely to be addressed at the Access Point that services the local cell, since the more active roaming behavior should have caused the station to connect to another Access Point.

To support the more active roaming behavior of the wireless stations and to compensate the lower receiver sensitivity, changing the Distance between APs parameter should correspond with the actual increase of and more dense placement of your Access Points.

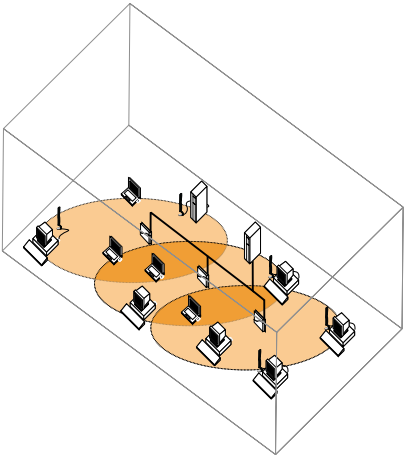
The examples listed on the following pages will illustrate the effect of the various Distance between APs configurations.

In Figure 6-8 you see the standard configuration of networks, where **Distance between APs** parameter has been set to **Large**.

- The receiver sensitivity in this mode causes the wireless radio device to defer transmissions for all messages that it senses within its range (identified by the colored circles).
- Roaming stations in a specific cell will remain connected to the servicing Access Point until they exit the wireless cell.

This setting provides you with the maximum radio range possible with the minimum number of Access Points to cover the wireless network area.

Figure 6-8. Large Distance between APs



The examples in Figure 6-9 and Figure 6-10 show you the effect of changing the Distance between APs parameter. Although the absolute range of the wireless radio is still the same,

the Distance between APs setting has virtually reduced the range of the wireless cell by applying different levels of receiver sensitivity:

- The absolute range of the radio signal from the Access Points is identified by the gray-dotted circles
- The reduced virtual range is identified by the colored areas.

With the new settings for the Distance between APs parameter, stations will only defer for radio signals that are received at a level that is equal or higher to the average signal as applicable in the colored areas. Messages with a lower signal level are considered to be traffic belonging to another cell, so will be ignored when the station determines whether it can start transmitting.

Roaming stations will start looking for/connect to another Access Point as soon as they leave the colored area belonging to a specific Access Point.

Figure 6-9. Medium Distance between APs

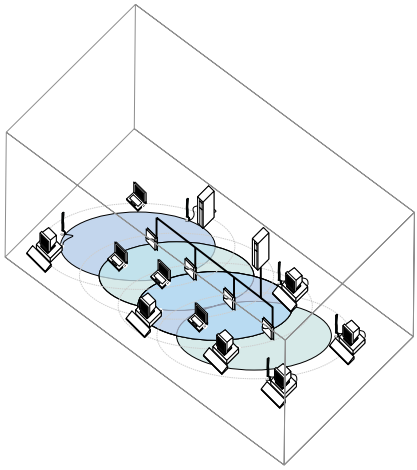
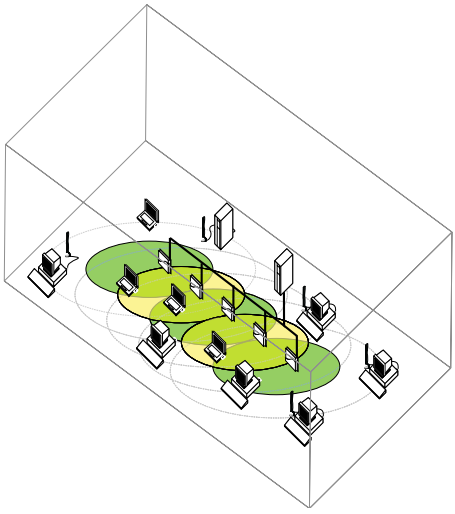


Figure 6-10. Small Distance between APs



Part 7: Security

Introduction

A distinct advantage of the IEEE 802.11 standard for wireless networks is that it provides a quick and easy way to connect your wireless station to a network. For instance, High Rate Wireless LAN stations that have been configured with the network name “ANY” will connect to the first IEEE 802.11 compatible Access Point it can find within range.

The drawback of this “quick & easy connectivity” is the vulnerability of the LAN to unauthorized access. Does this mean that Wireless LANs are not secure? The answer is no:

- Access to network resources is controlled via standard security mechanisms, such as user names and passwords, as implemented by all network operating systems.
- The IBM High Rate Wireless LAN products allow you to apply additional security measures to restrict access to your wireless medium and/or network resources.

Subject to the level of security required in your network environment, these measures may include:

Securing Access to Wireless Data

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

- “Restrict Wireless Access to the Network”
- Data encryption to encrypt all data transmitted via the wireless medium (see “Wireless Data Encryption” on page 7-7).

These security measures that apply to communications at the “physical layer” complement the “user name/password” validation at the “network layer” as implemented by standard network operating systems.

Restrict Wireless Access to the Network

To exclude unknown and unauthorized computing devices from establishing a wireless connection to the network, you can use the following options:

- Closing your network to all stations that have not been programmed with the correct network name (see “Closing the Wireless Network” on page 7-2).
- Use access control tables to build a list of authorized stations allowed to establish a wireless connection with the network (see “Access Control” on page 7-3).

Closing the Wireless Network

Closing the wireless network prevents unauthorized users from accessing the Access Point within a specified High Rate Wireless LAN network. If a user tries to access the network, without configuring their station with the correct network name, the station will not be able to bridge data on the Access Point.

There are two options for this type of access security: **Open** and **Closed**.

- The **Open** configuration is the standard IEEE 802.11 mode that will allow access to the Access Point for:
  - — all stations with the correct network name.
  - — all stations with the network name set to “ANY”.
- The **Closed** configuration is the IBM High Rate Wireless LAN proprietary mode that closes your network to all stations that have not been programmed with the correct network name.

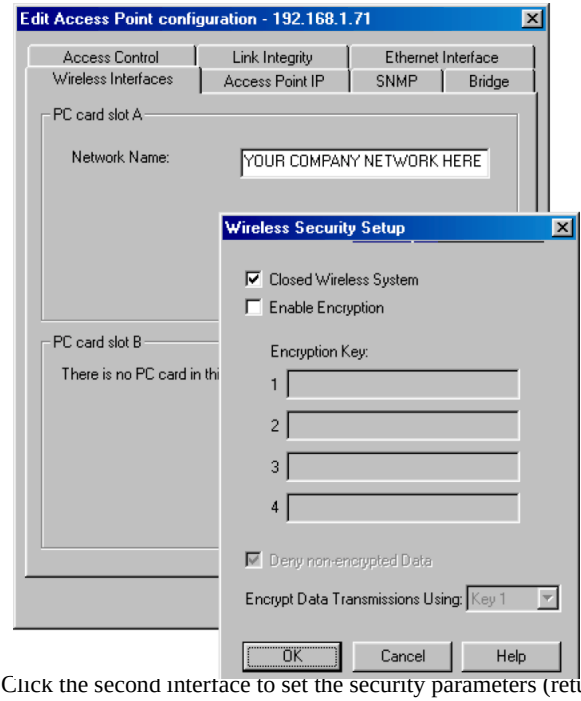
  This option will deny access to:
  - — all wireless stations with the network name set to “ANY” and,
  - — all non-High Rate Wireless LAN stations with a “zero string ESSID” or “ANY” as network name.

Note: The **Closed** option is not compliant with the IEEE 802.11 standard for wireless LANs.

To close your network proceed as described below:

1. Start the AP Manager and select the Access Point.
2. Click **Edit** to connect the Access Point.
3. Select the **Wireless Interfaces** tab (see Figure 7-1).
4. PC CardClick the **Security** button to display the security properties.
5. Click the check box next to **Closed Wireless System**.
6. Click **OK** to confirm and close the Wireless Security Setup window.

Figure 7-1. Close the Wireless System



7. (Optional) Click the second interface to set the security parameters (return to step 4).
8. Click **OK** to save the new configuration to the Access Point and to return to the main AP Manager window.

Your Access Point will automatically reboot and start bridging operation again allowing access only to those users that have been configured with exactly the same network name as identified in the setup of your Access Point(s).

Repeat steps 1 through 9 for all other Access Points.

Access Control

Another method to restrict wireless access to the Access Points is to use the access control table feature and/or the RADIUS Server Access Control feature.

If you decide to enable the access control table feature your Access Points will:

- only bridge messages to/from authorized stations, that have been identified in the access control table.
- ignore all requests to forward data to/from non-listed High Rate Wireless LAN stations.

Enabling access control is a more rigid security mechanism than “Closing the Wireless Network”, as it requires the LAN administrators to authorize each individual Wireless LAN station.

To authorize wireless stations to access the network, the LAN administrator(s) must:

- append the unique universal MAC address of the Wireless LAN station to the access control table file (*.tbl), and
- upload the access control table file to all Access Points.

Note: The access control feature does not work in network environments that require local MAC addressing.

If you decide to enable RADIUS Access Control, you can:

- Specify the lifetime of a granted authorization
- Set the authorization password
- Assign up to two RADIUS servers for validating the MAC address of wireless stations.

To enable RADIUS Server Access Control refer to “Enabling RADIUS Server Access Control” on page 7-6

Enabling Access Control

To enable access control you will first need to create an access control table file (*.tbl) using the AP Manager program.

You can upload the access control table file into all Access Points in your network as part of a (new) configuration (see “Importing an Access Control Table” on page 7-5 for more information).

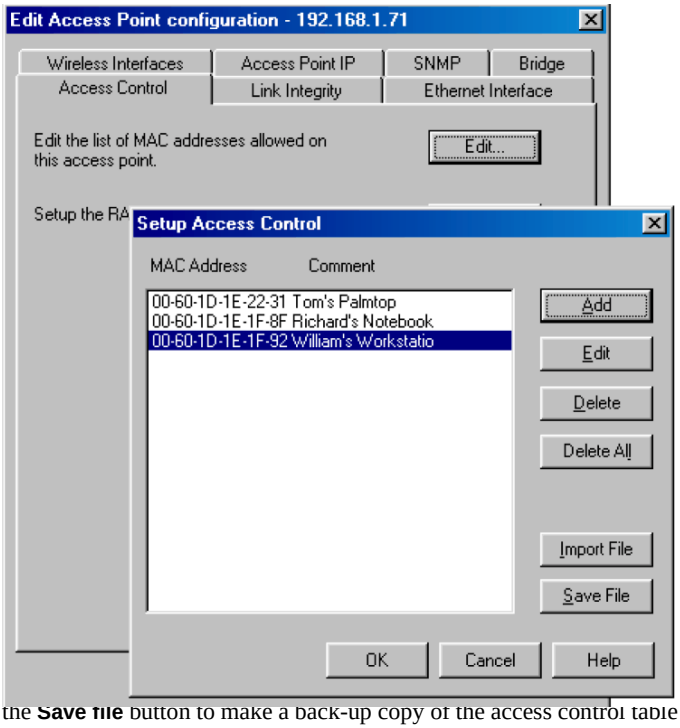
Creating/Editing an Access Control Table

To create or edit the access control table:

1. Start the AP Manager and select the Access Point.
2. Click the **Edit** button.
3. Select the **Access Control** tab.
4. Click the **Edit** button to display all MAC addresses that are currently authorized as pictured in Figure 7-2.

   By default, access control is set to **<All will be permitted>**, i.e. there are currently no access restrictions defined.
5. Use the following buttons to modify the MAC address table:
   - **Add** - to add MAC addresses one at a time. You can also use the **Comments** field to enter a name or add a comment about the listed MAC address.
   - **Edit** - to change entries in the table.
   - **Delete** - to remove MAC addresses one at a time.
   - **Delete All** - to remove all MAC addresses and disable access control.
   - **Import File** - to import an existing access control table.
   - **Save File** - to save the current access control to a file.
6. Repeat step 5 for all stations you want to authorize to send/receive data via this Access Point.

Figure 7-2. Setup Access Control



7. Click the **Save file** button to make a back-up copy of the access control table file you just created (*.tbl).

   You can use this file later to import the configuration into other Access Points.
8. Click **OK** to return to the Access Control tab.
9. Click **OK** again to save the new configuration to the Access Point and to return to the main AP Manager window.
10. (Optional) Save the configuration to a local back-up file (*.cnf) as described in “Step 4 - Create a Back-up of the Configuration” on page 4-5.

To save the table to all Access Points, please refer to “Importing an Access Control Table”[1].

Importing an Access Control Table

To import an access control table file (*.tbl) to your Access Points:

1. Start the AP Manager and connect to the Access Point in the edit mode.
2. Select the **Access Control** tab and click the **Edit** button to display all MAC addresses that are currently authorized.
3. Click the **Import File** button and select the access control table file (*.tbl) that you wish to import.
4. Click the **Open** button to import the selected file.
5. Click **OK** to return to the **Access Control** tab.
6. Click **OK** again to save the new configuration to the Access Point and to return to the main AP Manager window.

1. Also refer to information on “Common Parameters” on page 8-14.

7. (Optional) Save the configuration to a local back-up file (*.cnf) as described in "Step 4 - Create a Back-up of the Configuration" on page 4-5.

Disabling Access Control

To disable access control for your Access Points:

1. Start the AP Manager and connect to the Access Point in the edit mode.
2. Select the **Access Control** tab and click the **Edit** button 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 **Access Control** tab.
5. Click **OK** again to save the new configuration to the Access Point and to return to the main AP Manager window.
6. (Optional) Save the configuration to a local back-up file (*.cnf) as described in "Step 4 - Create a Back-up of the Configuration" on page 4-5.
7. Update the "Access Point Configuration Record" to reflect this change.
8. (Optional) Modify the access control settings for all other Access Points.

Enabling RADIUS Server Access Control

RADIUS Server Access Control is a method where you use Access Points in combination with a third-party RADIUS server.

To use RADIUS Server Access Control, you will need to:

1. Setup a RADIUS server
2. To configure a RADIUS server:
   - — The list of MAC addresses should be entered in the server's "users" file/database along with the password (=authorization password).
   - — It is also necessary to build a list of IP addresses of all Access Points that will use the RADIUS server. This list should be entered in the server's station file/ database along with the authorization password.
3. Build a list of MAC addresses of all (wireless) stations that you wish to authorize to establish a wireless connection with your Access Point infrastructure.
4. Configure all Access Points to:
   - — Enable RADIUS MAC Address authentication
   - — Set the RADIUS Authorization Lifetime
   - — Set the Authorization Password
   - — Identify the IP Address of the RADIUS server(s)
   - — Verify the Authentication Port of the RADIUS server(s)

RADIUS Server Access Control

RADIUS Access Control enables you to:

- Specify the lifetime of a granted authorization
- Set the authorization password
- Assign up to two RADIUS servers for validating the MAC address of wireless stations.

For each RADIUS server you will need to specify:

- The unique IP address of the RADIUS server
- The Authentication port as used by the selected server.

To restrict access to your network using MAC address control via a RADIUS server:

1. Start the AP Manager and select the Access Point.
2. Click the **Edit** button.
3. Select the **Access Control** tab.
4. Click the lower **Edit** button to display the RADIUS server name and secret parameter.
5. Enable the check box **Enable RADIUS Server**.
    - Default value is: RADIUS Access Control Disabled

For more information refer the help-file (press F1) of the AP Manager.

Wireless Data Encryption

To provide the highest level of security to wireless data transmitted via your network, you can use the Wired Equivalent Privacy (WEP) data encryption.

WEP data encryption uses 5-character encryption keys, based on the RC4 encryption algorithm, that will be used to encrypt/decrypt all data transmitted via the wireless interface.

You can specify up to 4 different keys to *decrypt* wireless data, and select one of the specified decryption key values to *encrypt* wireless data.

The option to use 4 different keys for decrypting wireless data, allows you to change your WEP keys at regular intervals without affecting regular network performance (see also “Maintaining WEP Encryption Keys” on page 7-15).

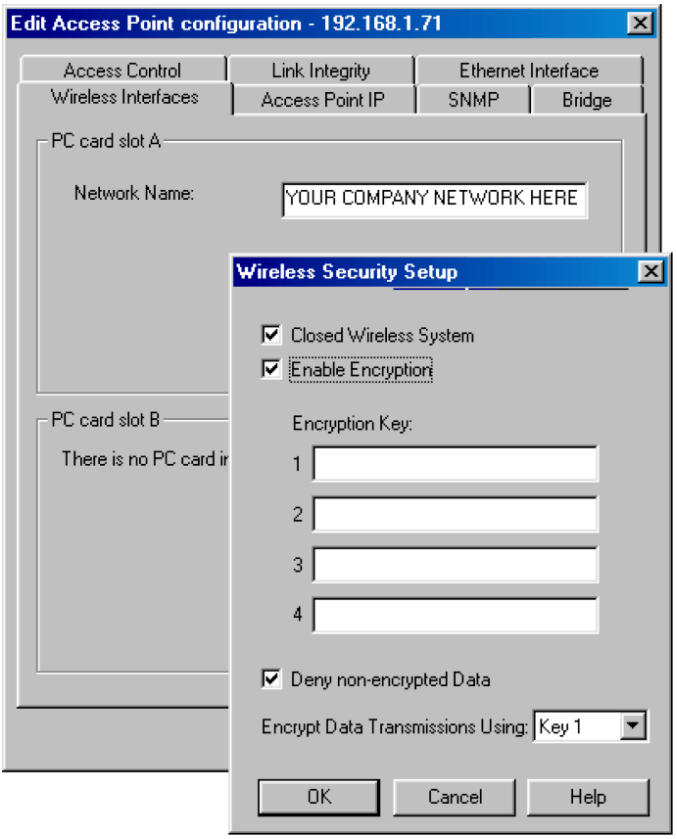
Enabling WEP Encryption

To enable WEP encryption you will need to ensure that:

- All wireless devices will be configured with matching encryption key values.

You are advised to use the Access Point configuration log to write down the proposed WEP key values, and store the information in a safe place.

Figure 7-3. Enabling WEP Encryption



Wired Equivalent Privacy (WEP) data encryption enables you to encrypt all data that will be transmitted via the wireless LAN medium.

To enable encryption:

1. Start the AP Manager and select the Access Point.
2. Click the **Edit** button.
3. Select the **Wireless Interfaces** tab.
4. Click the **Security** button to view the Wireless Security Setup window (see Figure 7-3).
5. Select the option **Enable Encryption** to enable encryption, and:
   - Enter up to 4 different keys to decrypt data received via the wireless interface
   - Select one of these keys to encrypt wireless data that is to be transmitted via the wireless interface.
6. Click **OK** to return to the **Wireless Interfaces** tab.
7. Click **OK** again to save the configuration to the Access Point and to return to the main AP Manager window.
   The Access Point will now reboot.

Optionally you can choose to configure your Access Point to allow or deny non-encrypted data.

WEP Encryption Key Values

If you select to enable encryption you may choose to enter up to the following encryption keys.

For the 128-bit RC4 encryption that supports 64-bit WEP based on RC4 encryption algorithm are either:

- 5-digit alphanumerical value in the range of “a-z” and “0-9”
  Example: SECU1
- A 10-digit hexadecimal value, preceded by the characters “0x” (zero x).
  Example: 0xABCD1234FE

For the 128-bit encryption based on the RC4 encryption algorithm are either:

- 13-digit alphanumerical value in the range of “a-z” and “0-9”
  Example: SECURE1234567
- A 26 -digit hexadecimal value, preceded by the characters “0x” (zero x).
  Example: 0x1234567890ABCDEF1234567890

Hexadecimal strings that are not preceded by the leading “0x” will be interpreted as alphanumerical string.

Note: The WEP key values you enter will remain visible only when you enter the character strings. As soon as you close the Security Setup window, the values will be stored in hidden characters: i.e. a next time the Security Setup window will be displayed, you will not be able to read the WEP key values anymore. You are advised to write down the values you enter, prior to closing the window.

WEP Transmit Key value

If you enable WEP encryption, you can select one key for wireless data transmissions from the list of WEP encryption key values. You can only select a transmit key that has a correct WEP encryption key value assigned. In case you specified no more than 2 key values, you can only select the transmit key from these two values.

CAUTION:

If you cleared the “Deny non-encrypted Data” tick box, your Access Point may also transmit in “non-encrypting mode”.

Deny non-encrypted Data

If you decide to use wireless data encryption, you are advised to encrypt all data that will be transmitted via the wireless medium.

In some cases however you may wish to choose to allow the Access Point also to process non-encrypted data as well.

Examples of such situations could be:

- Network environments that include .

- Network environments where you are about to install a large number of wireless stations, using “out-of-the-box” configurations, which by default will have encryption disabled.

If you would start-up such stations with their default configuration, these stations would not be able to establish an initial connection to the network, since they wouldn't be able to interpret the encrypted beacon messages.

For optimal security against unauthorized access to your network, you are advised always to leave the **Deny non-encrypted data** option enabled (=default).

> **CAUTION:**
>
> **Only when you would have good reasons to decide otherwise, you could clear this check-box, to allow the Access Point to communicate with wireless stations that either support WEP encryption or not, or have the WEP encryption enabled or disabled.**
> **Please read the information described in the following section prior to clearing the Deny non-encrypted Data tick box.**

How WEP Encryption works

The IEEE 802.11 standard on wireless LANs was designed to provide an easy to use, and easy to install wireless network, that would allow users to combine wireless LAN products from different vendors.

The drawback of easy access and interoperability is the vulnerability to unauthorized access to and/or use of your network. Although WEP encryption provides a good way to secure access to your wireless data, there are a few things you need to know to ensure your network provides the right level of security.

When you enable WEP encryption there are two modes of WEP operation:

- Enable encryption & deny non-encrypted data
- Enable encryption & allow non-encrypted data

For optimal security, you are advised always to use the **Deny non-encrypted data** option (=default).

Enable Encryption & Deny non-encrypted Data

When you select to enable encryption and deny non-encrypted data, your Access Point will:

- Only process messages received at its wireless interface, when the messages have been encrypted with either one of the four identified keys.
- Always transmit wireless data using the selected WEP key.
- Also encrypt all its multicast and broadcast traffic that it will transmit to the wireless medium.

If your network includes wireless stations configured with a non-matching WEP key, such stations will not be able to establish a wireless connection because they will not be able to understand (decrypt) crucial network information.

Enable Encryption & Allow non-encrypted Data

When you select to enable encryption, but you cleared the **deny non-encrypted data** check box, the Access Point will:

- Process all messages received at its wireless interface, regardless whether the messages have been encrypted with one of the identified keys or not.
- Encrypt wireless transmissions based on the encryption settings of the addressed station.
- If the addressed station does use WEP encryption, the Access Point will send the message in encrypted format, using the selected transmit key value.
- If the addressed station does not use WEP encryption, the Access Point will send the message in non-encrypted format.
- If the data message is a multicast or broadcast message, typically addressed to “all stations”, the Access Point will send the message in non-encrypted format.

This behavior of the Access Point is not related to the way the wireless message was received at the Access Point. If for example a wireless station that uses WEP encryption wishes to send data to another station in the same wireless cell, the data transmission will:

- Go encrypted from the WEP station to the Access Point
- Go un-encrypted from the Access Point to its final destination, if the addressed station does not support WEP encryption, or does not have the WEP option enabled.

> **CAUTION:**
>
> **For most network environments that require a higher level of security than the standard security mechanisms supported by High Rate Wireless LAN and most of today’s network operating systems (e.g. user names and passwords), IBM advises against using this option, unless you want to provide easy access for any client station and/or migration is more critical to your data network than top-level security.**

Good Practice Administering Encryption Keys

Like with other properties, your WEP lock is as safe as locking the door to your house: i.e. if you don't stick to secure policies on who will be allowed to use the key, or will know where to find it, even the strongest lock can be opened by an intruder.

That's why, for example you wouldn't “hide” the key to your house underneath the doormat. Similar good practice should be applied to the keys you will use to encrypt wireless communications.

To minimize the risk that intruders might be able to retrieve the WEP key values you are advised to:

- Lock away any paper registration sheet that you use to define/remember the defined WEP key values.
- Change the WEP encryption key values at regular intervals on both stations and Access Points.

The option to enter up to 4 different keys to decrypt data received via the wireless interface, enables you to define a WEP key roll-over scheme.

For example you could choose to select another transmit key every x weeks, until you reach the fourth key. At that point in time you could enter 3 new WEP key values for the first three WEP key entries, prior to the expiration period of the fourth key value. Once all stations and Access Points have been set to use the first new key again, you can replace the fourth key value with a new WEP key value.

Securing Access Point Setup

Security measures, such as access control, become ineffective when unauthorized persons can view and modify the configuration of your Access Points.

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

- Read and read/write passwords
- SNMP IP address access list
- Trap host alert mechanisms (optional)

Read and Read/Write passwords

To restrict access to the Access Point 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 Access Point to monitor diagnostic information found under **Monitor** button in the main AP Manager window.

You can define a read password in the field **Read Password** on the **SNMP** tab (Select Access Point from list, click **Edit** and select **SNMP** tab). The default value is “public”.

Read/Write password

A read/write password will provide you with full access to display Access Point diagnostic information found under the **Monitor** button, as well as the configuration settings found under the **Edit** button.

Entering an incorrect password will result in a time-out error, or “SNMP error no such name”.

To define a read/write password:

1. Start the AP Manager and select the target Access Point from the list or enter a specific IP address.
2. Click the **Edit** button to connect to the Access Point.
3. Select the **SNMP** tab.
4. In the field **Read/Write Password**, enter the new password. The default value is “public”.

5. Click **OK** to save the configuration to the Access Point. The Access Point will now reboot.

SNMP IP Access List

In addition to the read and read/write passwords, you can restrict access to the Access Point configuration to a limited number of authorized stations.

To authorize the High Rate Wireless LAN management station to access your Access Points, you must identify:

- the unique IP address of the management station, and
- the Access Point interface (port) via which this station will access the configuration

If you wish to authorize multiple stations, you can identify a range of IP addresses that you will reserve for authorized LAN administrator stations.

Note: When using the SNMP IP access list, you should include the IP address of all stations that will need to retrieve configuration or diagnostic information of the Access Point, i.e. stations of administrators who use either read or read/write passwords.

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

To authorize a management station via the SNMP IP access list:

1. Start the AP Manager and select the Access Point.
2. Click the **Edit** button to connect to the Access Point.
3. Select the **SNMP** tab to display the SNMP parameters. The **SNMP IP Access List** is visible at the bottom of the **SNMP** tab as pictured in Figure 8-6 on page 8-11
4. Use the following buttons to modify the SNMP IP access list:
   - **Add** - to add IP addresses to the list. (Press the F1 key for on-line Help for possible values for these fields).
   - **Delete** - to remove IP addresses from the list.
   - **Edit** - to change entries in the list.

   The default value is **<All will be permitted>**.

Trap Host Alerts

You can use the Trap Host mechanism to inform a network administrator when somebody resets the Access Point, performs the forced reload procedure or if there is an authentication failure or a link up or down is detected. The trap host alert will enable the network administrator to verify whether the reset or forced reload action was an authorized action or not.

Enable Trap Host Alerts

To activate the trap host mechanism:

1. Start the AP Manager and select the Access Point.
2. Click the **Edit** button to connect to the Access Point.
3. Select the **SNMP** tab to display the SNMP parameters.
4. In the field **Trap Host IP Address** enter:

- **Any valid IP address** - To this IP address a message is send if the Access Point is reset.
- **0.0.0.0 - (Initial value)** - To disable SNMP Trap Agent.

5. Enter a password in the field **Trap Host Password**.
   Choose a password that corresponds to the password set at the Trap Host to filter unsolicited or unauthorized SNMP Trap messages at the Trap Host.
   The Trap Host IP Password will be embedded in the SNMP Trap messages sent by this Access Point. If the Trap Host receives a message without or with an unknown password, the Trap message will be ignored.
   - **Valid Values**: Any alphanumeric value in the range of a-z, 0-9 with a minimum of 2 and a maximum of 31 characters.
   - **Initial Value**: public
6. Press **OK** to return save the new configuration to the Access Point and to return to the main AP Manager window.

When you activate the trap host alerts, be aware of the following:

- 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.

Trap Host Messages

The following message types can be distinguished:

- Call boot trap messages
- Authentication failure messages
- Link up or down messages

Call Boot Trap Messages

A Call boot trap message can occur in one of the following situations:

- Access Point is reset
- Power down
- Access Point configuration has been changed

Authentication Failure Messages

This message type is sent to the LAN administrator station once a wrong password has been entered on a (mobile) station. However, the Access Point itself does not respond, a time out error occurs.

Link Up or Down Messages

This type of message can be used to signal a problem with link integrity. If an ethernet link is broken, a Trap message “link down” is sent. As a result of this message, the AP-1000 disables it’s wireless interface to allow client stations to disconnect from the AP-1000 and

re-connect to another Access Point that provides a correct link to the Ethernet network. Once the link is restored, the original AP-1000 will send a “link up” message. The original Access Point can be used again.

Advanced Security Maintenance

Maintaining Access Control Tables

It is best to create a single access control table and store it on the harddisk of the LAN administrator station and/or share it with other LAN administrator stations. You are advised to use only one table for all Access Points.

For more information refer to “Creating/Editing an Access Control Table” on page 7-4.

Maintaining WEP Encryption Keys

The WEP Encryption functionality allows the wireless system to support up to four different keys simultaneously. This is in accordance with the 802.11 standard, which defines four so-called “default keys”.

These keys can be used to smooth the transition from the usage of one key to usage of a next key. The general requirement for two cards to transmit encrypted between each other is that they share a common key value at the same key-index number in the 4-key area at the moment of transmission. The key-index of the key that was used for encryption is transmitted in clear-text in the header of the message, and will be used at the receiving side to determine which of the 4 keys to use for decryption.

It is not mandatory that both sides (typically Access Point and High Rate Wireless LAN station) have the same active set of 4 keys. As long as there is one key in common, they can communicate, provided they both use that common key.

Note: The 802.11 standard also defines the possibility for having a unique key per Station, tied to the station’s MAC Address. High Rate Wireless LAN currently does not support that feature of the standard WEP function.

When planning the usage of different keys over time a number of aspects have to be considered:

- the length of time one key stays in use;
  this is a direct trade-off between security level (= the chance of someone finding out what the key value is) and operational overhead (= the efforts to reconfigure Access Point and stations)
- the requirements for smooth transition from one key to another
- the minimization of end user exposure to key values

The key roll-over possibilities built in the 802.11 standard and offered by High Rate Wireless LAN allow for a number of scenarios, each with different values for the above aspects.

The sequence of key configuration settings at Access Point (shown as AP=Access Point) and Station (shown as STA) over time is shown in a number of tables below. Each table reflects a certain key roll-over strategy. Notice that the column “Outward Key” shows which key is used to encrypt traffic from AP to STA and the column “Inward Key(s)” indicates the key(s) that are allowed and possibly used to encrypt traffic from STA to AP.

The WEP Keys that are configured are shown in order of index number 1-2-3-4; the column “Tx” is the index number configured for transmission. The key values are shown by capital letters to indicate a real key or by zero to indicate a non-configured index.

The column “Keys 1-2-3-4” shows an equal sign (=) when the value does not change from the previous period. This is particularly relevant when it concerns the stations keys, since it is envisaged that knowledge of the key values is typically not transferred to the end users, so they have to return their station equipment to an IT department to get the key values changed. It is envisaged that changing the Txkey Index is an action that can be done by end users, since it does not reveal secret information.

Three key roll-over strategies are distinguished:

- Single Key – No Transition (page 7-16),
- Single Key – Transition Period (page 7-16), and
- Alternative Schemes (page 7-17).

Single Key – No Transition

Table 7-1 shows a system, where at each point in time only one single key is used. The key to be used is dictated by the AP settings, showing only one valid key at each period. This requires a change over of keys at all stations more or less synchronous with the Access Point configuration changes. This is not practical and hence there are four keys.

Table 7-1. Single Key - No Transition

Period		AP Configuration		Out-ward	STA Configuration(s)		In-ward
#	Description	Keys 1-2-3-4	Tx	Key	Keys 1-2-3-4	Tx	Key
0	Main life key A	A-0-0-0	1	A	A-B-C-D	1	A
1	Main life key B	0-B-0-0	2	B	=	2	B
2	Main life key C	0-0-C-0	3	C	=	3	C
3	Main life key D	0-0-0-D	4	D	=	4	D
4	Main life key E	E-0-0-0	1	E	E-F-G-H	1	E
5	Main life key F	0-F-0-0	2	F	=	2	F

By initially configuring all stations with the keys for the first 4 periods, only the Txkey index needs to be changed at all stations for the first three steps. At the step from period 3 to period 4, the keys have to be changed at all STAs as well.

Single Key – Transition Period

To introduce a transition period between the main life of the successive keys, the scheme has to be changed as shown in Table 7-2.

Table 7-2. Single Key - Transition Period

Period		AP Configuration		Out-ward	STA Configuration(s)		In-ward
#	Description	Keys 1-2-3-4	Tx	Key	Keys 1-2-3-4	Tx	Key
0	Main life key A	A-0-0-0	1	A	A-B-C-D	1	A
1	Transition A-B	A-B-0-0	2	B	=	1|2	A | B
2	Main life key B	0-B-0-0	2	B	=	2	B
3	Transition B-C	0-B-C-0	3	C	=	2|3	B | C
4	Main life key C	0-0-C-0	3	C	=	3	C
5	Transition C-D	0-0-C-D	4	D	=	3|4	C | D
6	Main life key D	0-0-0-D	4	D	=	4	D
7	Transition D-E	E-0-0-D	1	E	A-B-C-D E-F-G-H	4 1	D E
8	Main life key E	E-0-0-0	1	E	E-F-G-H	1	E
9	Transition E-F	E-F-0-0	2	F	=	1|2	E | F

Notice that in the transition periods 1, 3 and 5 the end users can switch over from one Txkey index to the next. At the end of this period, all stations must be over to the new key index. Transition period 7 includes the transition to a new set of keys as well. The total length of time a key is used consists here of the main life time period and two transition periods. Assuming the main life is much bigger than the transition, this can still be considered to be a single key scheme, because most of the time only a single key is in use.

Alternative Schemes

Alternative schemes can be envisaged, which have main life periods in which two or more keys are active. An example is given in Table 7-3

Table 7-3. Alternative Schemes

Period		AP Configuration		Out-ward	STA Configuration(s)		In-ward
#	Description	Keys 1-2-3-4	Tx	Key	Keys 1-2-3-4	Tx	Key
0	Main life key A	A-0-0-0	1	A	A-B-C-D	1	A
1	Main life A+B	A-B-0-0	2	B	=	1|2	A | B
2	Main life B+C	0-B-C-0	3	C	=	2|3	B | C
3	Main life C+D	0-0-C-D	4	D	=	3|4	C | D
4	Main life D+E	E-0-0-D	1	E	A-B-C-D E-F-G-H	4 1	D E
5	Main life E+F	E-F-0-0	2	F	E-F-G-H	1|2	E | F

Table 7-3 gives a scheme where at each period two keys are in use; at the end of each period, the oldest key is no longer valid and needs to be replaced at all stations. Advantage of this scheme versus the scheme in Table 7-2 is that it requires less frequent configuration changes at all Access Points.

Part 8: Advanced Network Configurations

Introduction

To configure your High Rate Wireless LAN network beyond the basic configuration a number of advanced aspect will be discussed:

- “Advanced Parameters”,
- “Configuring Large Networks”,
- “Modifying the Configuration”,
- “Restoring a Back-up Configuration”,
- “About IP Addresses and Subnets”.

Advanced Parameters

You may wish to explore the “Advanced Parameters” options as supported by your Access Points, especially when administering larger networks that encompass more than 10 Access Points.

Advanced parameter options include:

- Advanced parameters, such as, RTS/CTS Medium Reservation, Distance between Access Points.
- Bridge parameters that enable you to filter specific networking protocols and/or traffic between specific stations.
- Access Point parameters, or
- SNMP parameters

For most networks, the default settings for the advanced parameters will provide more than reliable network connectivity. You are advised to change these parameters only when you are familiar to the type of parameters, for example based upon your experience and expertise with similar parameters in wired and/or High Rate Wireless LAN networking environments.

Note: A number of the advanced parameters described below may be marked as “common” parameters. This means that they should be the same for all Access Points in your network (see also “Configuring Large Networks” on page 8-13).

To set the advanced parameters, simply follow the instructions as described in the previous section, “Configuring Infrastructure Networks” on page 4-2, to connect to the Access Point that you wish to configure.

Advanced Parameters

If you created a basic Access Point configuration, as described in the previous section, you may have already noticed the additional buttons in the setup window, as pictured in Figure 4-4 on page 4-5.

Frequency

The Frequency setup menu gives you the ability to select an operating frequency from a range of sub-channels within the 2.4 GHz frequency band.
The number of selectable channels is determined by the radio regulations that apply in your country.

Click the **Advanced** button on the **Wireless Interfaces** tab of the edit mode to change the frequency parameters.

To optimize network traffic, we recommend that you assign different operating frequencies to Access Points that service neighboring wireless cells. Doing so, stations in each of the cells will be able to use the maximum bandwidth available to their cell.

Wireless stations equipped with Wireless Client Adapters can dynamically change the operating channel when roaming between Access Points that operate at different sub-channels.

RTS/CTS Medium Reservation

RTS/CTS medium reservation may provide a solution for networks where:

- Density of stations and Access Points is very low.
- You witness poor network performance due to excessive frame collisions at the Access Points.

However in most networking environments it is very unlikely that you will need to enable RTS/CTS medium reservation on the Access Point to prevent collisions. You are advised to read the information about “Optimizing Wired Connections” on page 6-3 prior to changing this setting for the Access Point.

To enable RTS/CTS medium reservation click the **Advanced** button on the **Wireless Interfaces** tab.

Interference Robustness

The Interference Robustness can be activated in exceptional cases when troubleshooting slow performance of your network that could be related to in-band interference from e.g. microwave ovens. Interference will usually show a poor Signal to Noise Ratio (SNR) that is based upon a good signal level and a high noise level. This behavior is often perceived when:

— the “trouble” station or Access Point is close to a interference source, or

— an interference source is located in the signal path between the “trouble” stations and the Access Point.

To enable Interference Robustness click the **Advanced** button on the **Wireless Interfaces** tab in the edit mode to display the Advanced Setup window, then select the option **Interference Robustness**.

Distance Between APs

In networking environments where you have either data intensive users, or a large number of users in a small area, you may wish to consider increasing the number of Access Points (making the distance between Access Points smaller), and then adjusting the Distance

Between APs parameter to optimize the load balance of the number of wireless stations per Access Point.

To change the Distance Between APs parameter display the **Wireless Interfaces** tab in the edit mode and click the **Advanced** button. In the field **Distance Between APs** choose one of the three density options:

- Large - (default)
- Medium
- Small

The default setting **Large** provides a maximum wireless coverage with a minimum number of Access Points. This option which is typically used for single-cell networks, but will also provide an efficient and cost effective solution for most networks that include multiple wireless cells.

> **CAUTION:**
> **The setting for distance between Access Points must be the same for all High Rate Wireless LAN equipped devices in your wireless network. A mismatch in the configuration setting for this parameter may have unpredictable performance results for wireless (mobile) stations in your network.**

Medium distance between Access Points can be selected for environments where stations experience slow network response times even though the quality of radio communications is rated as excellent. The slow response times might be experienced in areas where:

- A high number of wireless stations is located close to one another, causing other stations to defer data transmissions.
- A number of wireless stations engaged in heavy network traffic is causing other stations to defer data transmissions.
- The setting **Large** creates overlapping radio cells, which may cause stations in one cell to defer data transmission for stations located in the neighboring cell.

You should only select **Small** distance between Access Points when you are designing a wireless infrastructure that will include a high concentration of Access Points: i.e. the total cost of hardware investments is less critical than the maximum data throughput per cell.

Note: The settings **Medium** or **Small** distance between Access Points require a excellent quality of radio communications throughout the entire wireless coverage area. In environments where the actual placement of Access Points was designed to obtain maximum wireless coverage with a minimum number of Access Points, changing the distance between Access Points from **Large** to **Medium** or **Small** will not yield better results. Adversely, doing so might seriously affect the roaming performance of your wireless stations, risking network communication errors caused by “out-of-range” situations.

If you consider using the option **Medium** or **Small** distance between Access Points to create a high performance network, you are advised to read the section “Frequency Channel Management” on page 6-12 as well.

For more information about Access Point density, please consult Part 6 “Optimizing Performance”.

Multicast Rate

The Multicast Rate identifies the preferred transmission speed for your Access Point broadcast traffic as forwarded by the Access Point. Where transmissions at lower data rates are usually more reliable, you may prefer higher throughput performance over greater coverage for your wireless radio signal.

For more information about multicast rate refer to the help-file of the AP Manager program.

Bridge Parameters

One of the ways to optimize the performance of your wireless networks is to prevent “redundant” traffic from being transmitted over the wireless network. Redundant traffic may include:

- Specific network protocols exchanged by networking devices such as servers, that are not relevant to the wireless stations.
- Broadcast and/or multicast messages exchanged by specific networking devices such as servers that are not specifically addressed to the wireless stations.
- “Junk traffic” like for example error messages that are generated by malfunctioning devices, or as the result of incorrect network configurations that could have been avoided (for example closed network loops).

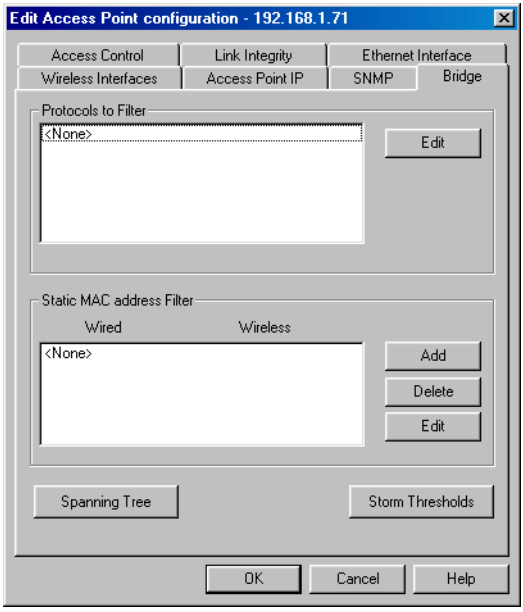
Filtering redundant traffic will save the bandwidth of the wireless medium for the wireless stations, optimizing throughput efficiency for these stations.

Optimizing wireless performance via the **Bridge** tab can be achieved in the following ways:

- Protocol filtering to deny specific networking protocols from being bridged to the wireless network interface (see “Protocol Filtering” on page 8-5).
- Filtering traffic exchanged between two specific stations that are identified by their static MAC address (see “Static MAC Address Filter” on page 8-6).
- Enabling the spanning tree mechanism to resolve the closed network loops errors (see “Spanning Tree” on page 8-7).
- Storm threshold filtering to limit the number of messages per port and/or station from being bridged (see “Storm Threshold” on page 8-8).

> **CAUTION:**
> **The Bridge parameter settings are typical “common” parameters, i.e. the Bridge parameter settings should be the same for all Access Points.**

Figure 8-1. Bridge Tab in the Edit Mode



To set the Bridge parameters, connect to the Access Point and select the **Bridge** tab to display the bridge parameters as pictured in Figure 8-1.

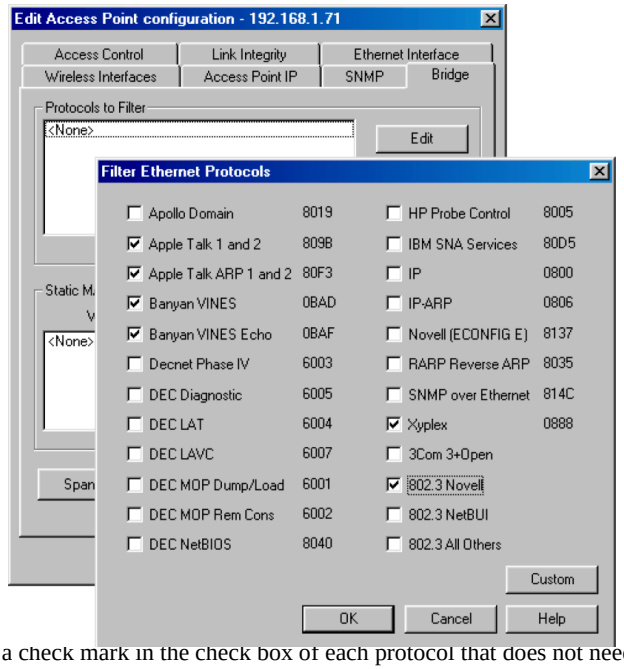
Protocol Filtering

The filtered protocols are listed in the top section of the **Bridge** tab. The factory-set default of the Access Point is **<None>** which will allow all protocols to be transmitted to the wireless medium. This is the recommended setting when you do not require specific protocols to be filtered.

To filter specific protocols, proceed as follows:

1. Determine the minimum set of protocols that must be bridged.
2. Click the **Edit** button to display the Filter Ethernet Protocols window pictured in Figure 8-2.

Figure 8-2. Select Ethernet Protocols to be Filtered



3. Place a check mark in the check box of each protocol that does not need to be transmitted to the wireless medium.

   To stop filtering a specific protocol, clear the check box.

4. (Optional) To add a non-listed protocol to the list, click the **Custom** button to enter the protocol manually.
5. When finished click **OK** to return to the **Bridge** tab as pictured in Figure 8-1.

   All of the protocols that you have selected, and/or all of the custom protocols that you have added manually, will be listed in the **Protocols to Filter** field.

6. You can now select one of the other Bridge parameter options, change other parameters or click **OK** to save your changes and return to the main AP Manager window.

Static MAC Address Filter

To filter out traffic exchanged between stations that is not required to be sent or received via the wireless interface, you can set the **Static MAC address Filter** in the bottom section of the **Bridge** tab. The default value, **<None>** will be acceptable for most networking environments (see Figure 8-1 on page 8-5).

You can use the MAC filtering option for example to filter broadcast or multicast messages exchanged between wired servers that can receive each others messages also via the wired network.

To filter out traffic between such devices add the MAC addresses of both devices as a pair in the **Static MAC address Filter** list.

The way the filter works is that when one of the listed stations sends a message to a MAC address that has been identified as a pair, the Access Point will not forward it via the

wireless station. All traffic that one of the stations wishes to send to any other (non-paired) MAC address will be forwarded.

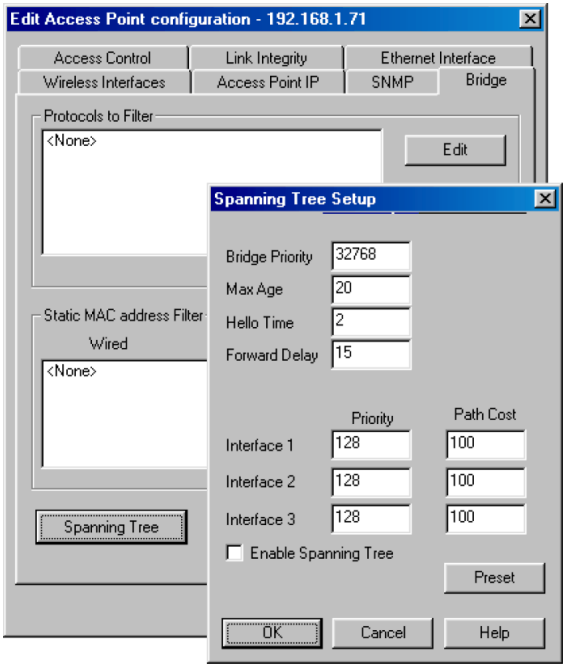
For more information about static MAC address filtering, please refer to Part 6 “Optimizing Performance”.

Spanning Tree

The **Spanning Tree** button allows you to set parameters that are used in determining the optimum path for network traffic to travel.

You can use spanning tree in a network that has been designed to include loops, such as a redundant wired link used as a back-up to the main wireless link.

Figure 8-3. Spanning Tree Setup window



To enable spanning tree:

1. Click the **Spanning Tree** button to open the Spanning Tree Setup window (see Figure 8-3).
2. Click the **Enable Spanning Tree** check box;
3. Use default values (see Figure 8-3);
4. Click **OK** to return to the **Bridge** tab.
5. Click **OK** again if you want to save this configuration and return to the main AP Manager window. Otherwise continue changing other parameters.

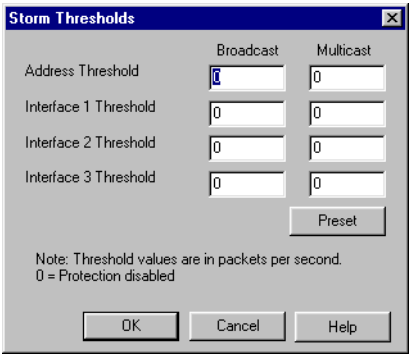
At this point, we recommend that you create a backup file, as described in “Step 4 - Create a Back-up of the Configuration” on page 4-5.

Storm Threshold

The **Storm Thresholds** button allows you to set parameters that are used in protecting the network against message overload as received from a single station or via a specific port.

The **Storm Thresholds** window allows you to determine the maximum number of multicast and broadcast messages that will be forwarded from one port (or address) per second.

Figure 8-4. Storm Thresholds Protection Disabled



The factory-set configuration for storm threshold protection is disabled (all values are set to zero).

1. If you need storm threshold protection, and are unsure of the proper broadcast and multicast values to input, click the **Preset** button for values that will provide adequate levels for most networking environments.
2. Click **OK** to keep these settings and return to the **Bridge** tab.

Click **OK** again if you want to save this configuration and return to the main AP Manager window. Otherwise continue changing other parameters.

Access point IP Parameters

The Access Point IP tab enables you to set the common IP parameters and to change the unique IP address of your Access Points.

To change the IP parameters proceed as follows:

1. Make sure you are connected to the right Access Point in the edit mode and select the Access Point **IP** tab to display the IP parameters (see Figure 8-5 on page 8-9).
2. Verify and/or modify the parameters of your choice.

   The mandatory parameters that you must specify are:

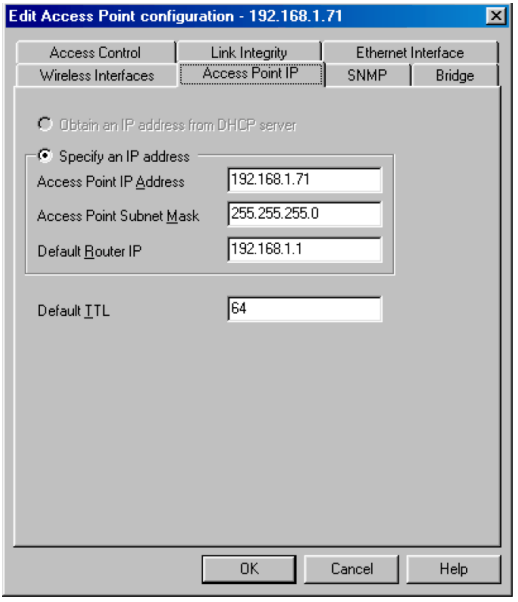
   - Access Point **"IP address"** (unique for each Access Point, in case of a BOOTP or DHCP server, this IP address is entered automatically).
   - Access Point **"Subnet Mask"** (the same for all Access Points, in case of a BOOTP or DHCP server, this IP address is entered automatically).
   - (optional) **Default router** (usually the same for all Access Points).

- (optional) **Default TTL** (Time To Live) (usually the same for all Access Points).

All parameters are explained in the next paragraphs.

3. When finished, proceed with configuring other parameters or click **OK** to save the configuration and return to the main AP Manager window.

Figure 8-5. Setup Access Point IP Parameters



IP address

Each Access Point needs an unique IP address. Use either:

- DHCP, to obtain an IP address automatically, or
- manually enter an IP address

Note: All Access Points must have a unique IP address value to allow you to address each Access Point specifically. Duplicate IP address values may cause unexpected behavior of the network and/or negative impact on network performance.

Manually assign an IP address

In case of manually assigning an IP address, use the field Access Point **IP Address** to enter a value from the range of IP addresses assigned to your organization.

The IP address is primarily used to address this Access Point when you use the AP Manager program to configure and/or monitor this device.

When your organization does not use IP addressing, you can enter a user-defined value. For example a value of the same pattern as the factory-set IP address 153.69.254.254, where you replace the last three digits with a numerical value in the range of “1” to “253”.

Automatically assign an IP address

In case when a DHCP server is available on the network, an IP address will be automatically assigned to the Access Point by the DHCP server. To enable automatically obtaining an IP address form the DHCP server, select the field **Obtain an IP address from DHCP server** on the Access Point **IP** tab.

For more information about DHCP refer to “BOOTP and DHCP” on page 8-19.

Subnet Mask

The field Access Point **Subnet Mask** is a common parameter and must be the same for ALL network devices within your IP subnet.

You can use either the default value (255.255.0.0) or change the subnet mask to a value that applies in your network.

If **Obtain an IP address from DHCP server** is enabled, the subnet is also automatically entered.

Default Router

The field **Default Router IP** is an optional field that is relevant when you intend to use the Access Point support for TRAP messages (see also “SNMP Parameters” on page 8-10).

You can use the Default Router IP field to identify the IP address of the router which the Access Point will use to find the Trap Host IP Address (identified in the SNMP Parameters).

The default router and the trap host IP address described later in this chapter are only used for TRAP messages generated by the Access Point upon a reset, modification of the configuration, or forced reload procedure.

If the value of the field **Default Router IP** is set to 0.0.0.0 (default), then no TRAP messages are initiated by this Access Point.

The Default Router is also relevant if you want to manage (or just ping) the Access Point from an other subnet.

Time To Live (TTL)

The field **Default TTL** (Time To Live) identifies the maximum number of hops for an IP message generated by the Access Point (typically used for the trap host messages).

The value 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. By default, the value is 64.

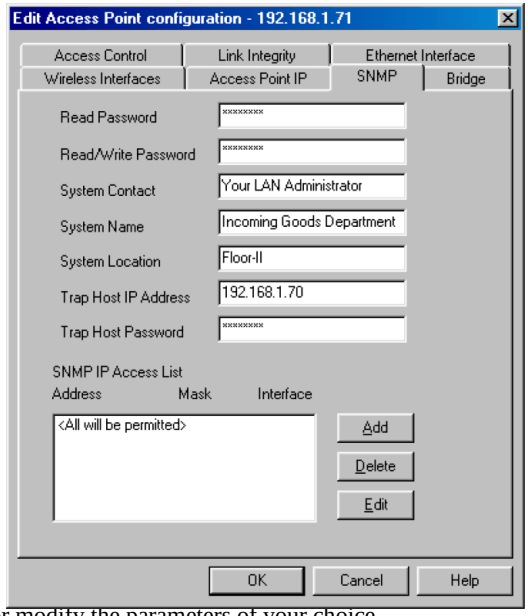
SNMP Parameters

Most SNMP parameters (except for the System Location and System Name) are common parameters, i.e. they should be the same for ALL Access Points in your network.

To set the SNMP parameters proceed as follows:

1. Make sure you are connected to the right Access Point and select the **SNMP** tab to display the SNMP parameters pictured in Figure 8-6.

Figure 8-6. Setup SNMP parameters



2. Verify and/or modify the parameters of your choice.
   The recommended parameters that you should specify are:

   - **Read/Write Password** to restrict access to the configuration of your Access Points, and
   - **System Name** to allow easy identification of the Access Point when using the diagnostic options of your software tools.

   These and all other SNMP parameters are explained in the following paragraphs.
3. When finished, proceed with configuring other parameters or click **OK** to save the configuration and return to the main AP Manager window.

Read Password

Change the **Read Password** parameter in order to prevent unauthorized access to the Access Points.

A read password is requested when you connect to Access Points with the **Monitor** option. The default value is “public”.

With the correct read password, a local LAN administrator can only monitor Access Point statistics and tables, but not view or change any of the parameters.

Read/Write Password

Change the **Read/Write Password** parameter in order to prevent unauthorized access to the Access Points to make changes to its configuration settings.

A read/write password is requested when using the **Edit** button to connect to the Access Point. The default value is “public”.

With the correct read/write password, a network supervisor can monitor Access Point statistics and view or change any of the parameters of the configuration. Using different values for the Read and Read/Write Password parameters you can create different levels of authority for your LAN Administrators to configure and/or monitor the Access Points.

System Contact

Use the field **System Contact** to enter a generic name for the network supervisor or department, (e.g. “Your LAN Administrator” as pictured in Figure 8-6).

System Name

Use the field **System Name** field to enter a generic logical location of the Access Point, (e.g. “Incoming Goods Department” as in Figure 8-6).

System Location

Use the field **System Location** to enter a generic physical location of the Access Point, (e.g. Access Point floor 1N as in Figure 8-6).

Trap Host IP Address

If you plan to use the trap alert system as described on “Trap Host Alerts” on page 7-13, you can use the **Trap Host IP Address** field to enter the address of the network management station that should collect the SNMP trap messages. If you do not intend to use trap host alerts, the value is set to “Don’t care”.

For more detailed information about trap host messages, see “Trap Host Alerts” on page 7-13.

Trap Host Password

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.

SNMP IP Access List

You can use the **SNMP IP Access List** to create an extra level of security in addition to the read an read/write passwords. This will allow you to authorize a limited number of LAN administrator stations to view and/or modify the configuration of the Access Points, based upon the IP address of these stations.

The field **SNMP IP Access List** should typically include the IP address of all LAN administrator stations that will use the AP Manager to configure and/or monitor your Access Points.

To authorize the LAN administrator station you must enter:

- The IP address of the station(s), and
- The Access Point network interface through which they will access the Access Point.

To indicate the interface, use either:

- “1” for ethernet

- “2” for the wireless network interface in socket A, or

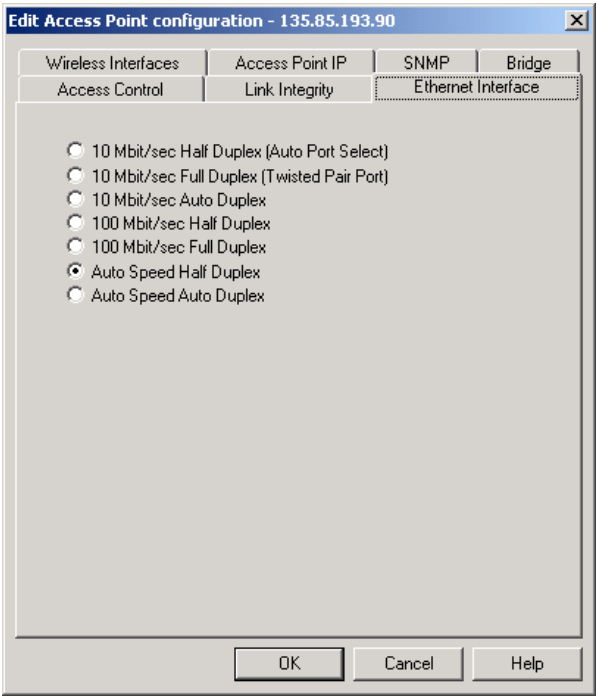
Alternatively you can use the value “x” to allow the identified IP address to access the Access Point via any of the available interfaces.

To allow multiple LAN administrator stations to access the Access Point configuration and/or monitor parameters, you can also assign a range of IP addresses. Doing so, enter a subnet mask value that will indicate the subnet from which all stations are authorized to modify the SNMP setup.

Ethernet Interface

Subject to the type of interface offered by your Access Point, you can select one of the options (see Figure).

Figure 8-7. Select Ethernet Interface



For more information about selecting the Ethernet Interface refer to the help-file of the AP Manager program.

Configuring Large Networks

Each Access Point configuration is characterized by two types of parameters:

- Common parameters that must be the same for ALL Access Points in your network, and
- Unique parameters that must be unique for each Access Point in your network.

In larger networking organizations, it may become quite cumbersome to copy the common parameters to each of the Access Points in the network in order to provide consistency throughout the entire network. As the number of Access Points increases, the risk of errors (e.g. as a result of typos) may increase as well.

Inconsistent values for common parameters, or duplicate values for the unique parameters may have unpredictable effects on the performance of your network. Document the configuration settings of your network in detail to avoid configuration mismatches.

Therefore, we recommend that you create a template file that contains all of the common parameter settings that apply to every Access Point within the network.

Common Parameters

Common parameters, such as the network name or SNMP Read/Write Password, are used to identify which Access Points belong to the same network environment. They differentiate your group of Access Points from other (neighboring) network environments.

A list of common parameters is shown in Table 8-1 below, together with the AP Manager tabs where you can view or modify the parameters.

Table 8-1. Common Access Point Parameters

Parameter	AP Manager tab
■ Network Name	Wireless Interfaces
■ Protocols to Filter ■ MAC Filtering	Bridge
■ Access Point Subnet Mask ■ Default Router IP ■ Default TTL	Access Point IP
■ Read Password ■ Read/Write Password ■ SNMP IP Access List ■ (optional) Trap Host IP Address and Password	SNMP

Unique Parameters

Unique parameters such as the IP Address or System Name, are used to differentiate a single Access Point from the group of Access Points that are operated within your network. The most important unique parameters are listed in Table 8-2.

Table 8-2. Unique Access Point Parameters

Parameter	AP Manager Setup Menu
■ Access Point IP Address	Access Point IP
■ System Name ■ System Location	SNMP

Managing Configuration Consistency

The most convenient way to manage the configuration of a large number of Access Points is to configure the first Access Point and save its configuration to file. Use this file as a template that you can upload to the other Access Points.

After loading the template file on each Access Point, you will modify the parameters identified as the unique parameters, to differentiate the Access Point from the other Access Points in this network.

In other words, the easiest way to manage a large number of Access Points is as follows:

1. **Preparation**
   Identify and record all information related to each of the Access Points to be configured.
2. **Creating a template file**
   Identify and set the common parameters that should apply to all Access Points within your network.
3. **Configuring all Access Points**
   Import the template file and modify all the unique identifiers to differentiate the Access Point from the other Access Points.

> **CAUTION:**
> **We recommend that you create a backup file for each unique Access Point configuration, using the Download Config File item from the Access Point menu in the main AP Manager window. Use a file name that allows you to easily recognize the relationship between a file name and the specific Access Point.**

Preparing Large-Scale Networks

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

- Unpack the Access Points and record their serial number and MAC address on the “Access Point Configuration Record” as printed in Appendix A “Start-up Configuration” of this document.
- Make a list of IP addresses available in your network, you will need one IP address for each Access Point.
- Use the “Access Point Configuration Record” to assign one IP address to each of your Access Points.
- Record the intended system location of each Access Point on the “Access Point Configuration Record”.

Creating a Template File

1. To create a template file, configure the first Access Point as described earlier under "Configuring Infrastructure Networks" on page 4-2.
2. Save the configuration of this Access Point to disk as described in "Step 4 - Create a Back-up of the Configuration" on page 4-5.
3. Create a copy of the back-up file with the name "common.cnf" or any other name that will allow you to easily recognize the file as the actual template file that we will use as the basis to configure the other Access Points in your network.

> **CAUTION:**
> **Do not start using your original back-up file as template file. Any changes you make to the file might impair your ability to fully restore the original configuration of your first Access Point, if the unit goes out of service. Always store back-up copies on a separate disk and/or location.**

Configuring other Access Points

Having created the template file, we can now start (re-)configuring the other Access Points in batch-mode. For each Access Point, the procedure will be as follows:

- Run AP Manager and connect to the target Access Point.
- Upload the template file that contains the values that are common for all Access Points from a template file.
- Set the unique parameters for each Access Point.
- Save the values to an individual configuration file on disk.

The detailed procedure is as follows:

1. Start the AP Manager program.
2. Select the target Access Point from the list or enter a specific Access Point IP address. If the target Access Point is not displayed in the list, choose **Refresh** Access Point **List** from the Access Point menu.
   If the selected Access Point is still using the factory-set IP address, for example when you are configuring a new "out-of-the-box" Access Point, you will be prompted to change the default IP address as described earlier in this chapter on Step 2 - Connecting to the Access Point (page 4-3).
3. When asked navigate to the disk and/or folder where you stored the template file.
4. Select the template configuration file (e.g. **"**common.cnf") and click the **Open** button.

> **WARNING:**
> *The IP address that was displayed in the list in the main AP Manager window has been overwritten with the IP address which was specified in the template file. Follow the procedures described below to change it to the desired IP address value. Failing to do so may lead to multiple Access Points being configured with the same IP address, resulting in unpredictable network behavior.*

The AP Manager program has now loaded the settings as identified in the template file. Now you must change all the parameters that should be unique to this Access Point (see “Unique Parameters” on page 8-14) prior to saving the configuration and returning to the main Access Point window by clicking **OK**.

5. Set the unique parameters that apply to this Access Point.
   The minimum set of unique parameters that you must set are listed in Table 8-2 on page 8-15.
6. Now save the configuration to the Access Point, by clicking the **OK** button. You return to the main Access Point window.
7. Create a back-up file of the configuration for this Access Point, using the **Download Config File** command from the Access Point menu.
   Use a file name that allows you to easily recognize the relationship between the file name and this Access Point.

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

Repeat step 2 - 7 for every other Access Point that you wish to configure.

Completing the Installation

When you configured the Access Points at your desk, i.e. the Access Points were not yet installed into their intended location, label each Access Point with clear instructions for your installation technicians.

1. Record the intended location of the Access Point on a label and attach the label to the Access Point.
2. Record the name of the file with the Access Point’s configuration data and the location where you will install the Access Point on the “Access Point Configuration Record”.
3. When finished, store the back-up files (*.cnf), your template file (“common.cnf”) and your “Access Point Configuration Record” in a safe place.

Modifying the Configuration

You can modify the Access Point configuration parameters using the **Edit** button from the main AP Manager window.

Keep in mind that you will need to address the Access Point using its new IP address and the new read/write password (if you changed the Read/Write Password parameter) to open the configuration file. If your High Rate Wireless LAN management station is a wireless station, you may need to modify the station’s interface parameters to match the values that were originally stored in the Access Point.

Alternatively, if you have forgotten the read/write password, or any other setting required to access the Access Point, you may need to perform a forced reload, as described in Appendix C “Forced Reload Procedure”.

Note: When you make changes to the configuration of a particular Access Point, you should update the “Access Point Configuration Record” to reflect these changes.

Changing Common Parameters

If you need to make changes to the common parameters, i.e. the parameters that apply to all Access Points, the most efficient way to do so is as follows:

1. Change the common parameters for one Access Point.
2. Save the changes to a new template file (e.g. “common.cnf”)
3. Follow the procedure as described in “Configuring other Access Points” on page 8-16.

Restoring a Back-up Configuration

To restore previously saved back-up configuration files to your Access Point proceed as follows:

1. Start the AP Manager program.
2. Select the Access Point you want to upload the configuration file to.
3. From the Access Point menu select **Upload Config File**.
4. Select the configuration file you want to upload, and click **Open**.
5. When prompted to confirm the upload, verify whether the pop-up message reflects the correct IP address.
    - When the IP address value is correct, click **Yes** to proceed. The Access Point will now reset automatically.
    - If the IP address in not correct, click **No** to return to cancel the upload procedure

The new parameter settings will now be loaded into the FlashROM of the Access Point. This means that the parameters will remain intact whenever the Access Point is reset or switched off and on again. To change the parameters again, simply repeat the procedure as described in this section to reconfigure your Access Points.

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 the High Rate Wireless LAN infrastructure into this type of network architecture, please note that all Access Points and wireless stations must be installed on the same subnet, i.e. on the same side of the router or gateway.

The roaming functionality does not work over routers. When Access Points are connected to different subnets, a mobile station may lose its network connection when it physically enters an area where the Access Points are connected to a different subnet.

The configuration and management of your Access Points is managed via the TCP/IP protocol stack. This means that each Access Point and computer that you wish to use to configure the Access Points must have a unique IP address.

You are advised to assign “static” IP addresses to the Access Points as described earlier in this chapter. This ensures that the Access Points at specific locations will always have the same IP address. For the LAN administrator stations you may either use a “static” IP address or a dynamic IP address that is assigned by a BOOTP or DHCP server.

When assigning IP addresses to LAN administrator stations and Access Points, make sure that:

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

Note: The wireless networking system does not need IP addressing to connect normal wireless stations to the network. The infrastructure is just the “physical” medium to connect a computer to an Access Point, like you could use wire to connect it to an ethernet infrastructure.

However in environments where the network operating system uses the TCP/IP protocol, stations may need to have an IP address as well to use specific networking services, like for example access to the internet.

BOOTP and DHCP

When powered-up for the very first time, the Access Point will broadcast a request for an IP address. If your network includes a BOOTP or DHCP server, this server will automatically assign an available IP address to the Access Point.

Subject to the settings of your BOOTP or DHCP services, you may need to introduce the Access Point MAC address to the BOOTP or DHCP server. Consult the documentation of your BOOTP/DHCP software for more information.

An IP address that is assigned by a DHCP server will be stored in the volatile memory of the Access Point: i.e. if the Access Point is reset, the DHCP server may assign another IP address. To obtain consistency in the IP address, it is advised to assign a permanent IP address to the Access Point, using the Access Point **IP Address** field on the Access Point **IP** tab.

An IP address that is assigned by a BOOTP server is stored in the configuration file of the BOOTP server. This configuration file has a one-to-one (static/fixed) mapping from MAC address to IP address. If a BOOTP server is used and the Access Point is reset, the IP address of the Access Point is the same as before the reset.

Appendix A: Start-up Configuration

Introduction

Your Access Point comes with installed operating software factory. Together with this software, the Access Point has also been loaded with a factory set configuration, that allows for “out-of-the box” operation.

Note: The factory-set configuration should not be confused with a “default” configuration. For example when performing a “Reboot” or “Forced Reload” (described later in this book) the unit will NOT return to the “factory-set” configuration.

To connect to the Access Point, the network parameters of each wireless station should be configured to match the values as identified for the Access Point unit.

- When powering up the Access Point for the very first time, these values should match the values listed in Table A-1.
- For normal operation these values should match the ones you identified when configuring the Access Point unit. You are advised to record this information on the Access Point Configuration Record in this appendix.

Factory-set Configuration

Table A-1. Start-up Configuration - Access Point

Access Point Parameters		
Access Point IP tab	Obtain an IP address from DHCP server	Enabled
	Default TTL	64
SNMP tab	Read Password	public
	Read/Write Password	public
	System Name	xx-xx-xx-xx-xx-xx [1]
	Trap Host IP address	0.0.0.0 [2]
	Trap Host Password	public
	SNMP IP Access List	<All will be permitted>
Bridge tab	Protocols to Filter	<none>
	Static MAC address Filter	<none>
	Spanning Tree	disabled
	Storm Thresholds	disabled
Access Control tab	(Static) Access Control	<All will be permitted>
	RADIUS Server Access Control	Disabled
Link Integrity tab	Link Integrity	Disabled

1. Ethernet MAC address of the device (printed on a small label on the processor module).
2. No SNMP traps are sent with this IP address.

Table A-2. Start-up Configuration - Interface

Wireless Interface		
	Network Name	WaveLAN Network
	RF-Channel	2.462 MHz
	Closed wireless system	Disabled
	Encryption	Disabled
	Medium reservation	Disabled
	Microwave oven robustness support	Disabled
	DTIM period	1
	Distance between APs	Large
	Multicast rate	2 Mbit/s

Access Point Configuration Record

Common Parameters

Wireless Network

Network Name: _____

Access Control

Access Control ❑ Enabled

Table File Name: _____

RADIUS server ❑ Enabled

SNMP

System Location: _____

IP Subnet Mask: _____

Read Password: _____

Read/Write Password: _____

Access Point Unique Identifiers

Serial Number	MAC Address	IP Address	IF	Frequency	Device Location	Date Installed	Configuration File
			❑E ❑A ❑B				
			❑E ❑A ❑B				
			❑E ❑A ❑B				
			❑E ❑A ❑B				
			❑E ❑A ❑B				
			❑E ❑A ❑B				
			❑E ❑A ❑B				
			❑E ❑A ❑B				
			❑E ❑A ❑B				

Appendix B: Troubleshooting

Introduction

Problems experienced in wireless LAN operation can be related to:

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

Problem-solving Approach

To resolve a configuration mismatch you will need to compare the configuration parameter settings of both Access Points and all stations involved.

To determine a component failure, check the LED activity of the Access Point. You can use the "LED Error Table" on page B-2 to determine if a problem has a hardware-related cause (component failure). This table may also provide help in diagnosing and solving operational problems that might have other possible causes.

When your Access Point appears to have stopped responding to normal bridging requests, you may try to reboot the device as described under "Rebooting Access Points" on page B-3.
In exceptional cases you may consider to perform a forced reload procedure as described in Appendix C "Forced Reload Procedure".

Table B-1. LED Error Table

Power	**Ethernet**	**Wireless interface A**		**Description/Action:**
⏻	⟷	~A		
Continuous Green	Flicker Green	Flicker Green		Normal operation where flickering indicates interface activity. No action required.
	Off	Off		Normal operation that indicates there is no LAN activity ■ No action required ■ (Optional) Check if all ethernet connections are properly installed
Off	Off	Off		No power. ■ Check the power cord, ■ Check the power supply
Continuous Green	Flicker Green	Amber		Network overload. The ethernet connection sends more traffic to wireless stations than the Access Point Bridge can forward to the interface[1]. Run the AP Manager Remote Statistics to investigate network performance. If possible try to eliminate redundant traffic by: ■ Filtering protocols ■ Setting storm threshold, or ■ Shut down defect ethernet stations that transmit excessive data
		-		
	Green	Amber		
Continuous Green	Flash Red	-		Frames are rejected because of an unknown cause. ■ Run the AP Manager Remote Statistics to investigate the number of packets in error. ■ If this number is relatively high, run a remote link test to determine which station is causing the packet loss.
	-	Flash Red		
		-		

1. When traffic load exceeds the wireless throughput capacity (>11MB/s), the Access Point will buffer such requests. In this situation however the buffer is full, and packets are ignored.

Power	Ethernet	Wireless interface A		Description/Action:
⏻	⟷	~A		
Amber	Off	Off		Forced reload state. ■ Proceed with the forced reload procedure as described in Appendix C “Forced Reload Procedure” of this user’s guide.
	Amber	Amber		
Amber	Flicker Green	Off		Forced reload state. The flickering LED indicate LAN activity on the specific LAN interface. This activity is typically caused by the LAN administrator station that is performing the forced reload. ■ Proceed with the forced reload procedure as described in Appendix C “Forced Reload Procedure” of this user’s guide.
	Off	Flicker Green		
		Off		
Red	-	-		General hardware failure ■ Reboot the Access Point as described in this Appendix. ■ If the problem persists, contact IBM technical support.
-	Amber	-		Ethernet hardware failure ■ Reboot the Access Point as described in this Appendix. ■ If the problem persists, contact IBM technical support.
	-	Amber		High Rate Wireless LAN hardware failure ■ Reboot the Access Point as described in this Appendix. ■ If the problem persists, contact IBM technical support.
		-		
				If the PC Card is broken, which can be tested by inserting the card into the High Rate Wireless LAN computer, return the card to your authorized reseller.

Rebooting Access Points

If a particular Access Point has stopped responding to normal bridging requests, you can reboot (reset) the Access Point. You can reboot Access Points either manually on-the-spot or remotely.

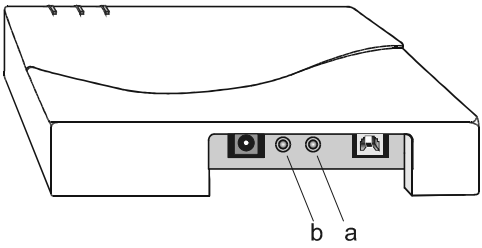
Upon reboot, the Access Point will run the start-up diagnostics and start bridging operation using the configuration parameters as they were stored in the Access Point prior to the reboot. For “out-of-the-box” Access Points, these parameters will be as identified in Table A-1 on page A-2.

Manual Reboot

To reboot the Access Point manually on-the-spot proceed as follows:

1. Remove the cover of the Access Point (see the Getting Started guide that came with your Access Point, for assistance if needed).
2. Locate the two small holes on the bottom of the processor module, marked “Reset” (A) and “Reload” (B) as pictured in Figure B-1.

Figure B-1. Reset Button



3. Use a small pointed object, such as the tip of a ball-point, to press the **Reset** button. The Access Point will restart and run the start-up diagnostics, characterized by a LED sequence where the LEDs change color in the range Red, Amber, Green.
4. When the Power LED is green, and other LEDs are off or flickering (indicating LAN activity), you can mount the cover of the Access Point.

After approximately 15 seconds, the unit will start bridging operation using the configuration parameters as they were stored in the Access Point prior to the reboot.

Remote Reboot

To reboot the Access Point from a remote location:

1. Start the AP Manager program.
2. Select the target Access Point from the list or enter the IP address for a specific Access Point.
3. Open the Access Point menu.
4. Select **Reboot** Access Point.
   The AP Manager program will now prompt you to enter the password required to reboot the device.
5. Enter the Read/Write password and click **OK**.
6. The Access Point will restart and run the start-up diagnostics.

After approximately 15 seconds, the Access Point will start bridging operation using the configuration parameters as they were stored in the Access Point prior to the reboot.

If you would like to display the configuration file or monitor the Access Point's performance after a reboot, you may have to wait until the unit completes the start-up diagnostics before you can access the Access Point again.

Appendix C: Forced Reload Procedure

Introduction

A forced reload allows you to recover from a situation where:

- The Access Point 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 Access Point.
- The Access Point has been configured with incorrect parameters, preventing you to access the Access Point via the network interface.

CAUTION:

When you need to perform a forced reload, please keep in mind the following:

a. *The Access Points equipped with network interfaces that are set to Forced Reload" mode can not be accessed via the wired network interface.*

b. *Do not perform a "Forced Reload" procedure for more than one Access Point simultaneously.*

You might risk unexpected administrative problems due to configuring multiple units with an identical configuration image and IP address.

When in"Forced Reload Mode" the Access Point will stop bridging operation. The Access Point is only capable of accepting a new software image to be programmed into the FlashROM.

To access the Access Point in forced reload mode you may need to reconfigure your LAN administrator station.

When using AP-500s you may wish to perform the forced reload using a configuration scenario as described in Part 3 "Setting Up your LAN Administrator Station" (see either Figure 3-2 on page 3-8 or Figure 3-4 on page 3-9).

Performing a Forced Reload

A forced reload procedure consists of three steps:

1. Step 1 - Preparations.
2. Step 2 - Set to “Forced Reload” Mode.
3. Step 3 - Configuring and Uploading Files.

One additional step is optional, but recommended:

- Creating a Back-up File

Step 1 - Preparations

A forced reload procedure can only be performed when you have physical access to the Access Point.

- Familiarize yourself with the location of the Access Point:
  Do you need special equipment to access the Access Point, such as a ladder or keys to get into the room where the Access Point is located?
- Do you have a back-up copy of the Access Point’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 Access Point that apply in your network again.

  Back-up copies may have been created upon initial installation using the **Download Config File** option of the AP Manager program.
- If you have access to the IBM High Rate Wireless LAN website, you can download the latest software (*.bin) available for your Access Point.
- It is advised to specify a temporary IP address for the Access Point. To enter this temporary IP address:
  - — Open the AP Manager program.
  - — Select from the **Tools** menu the option **Options**.
  - — Enter the temporary IP address in the **Local IP address** field.

  The temporary IP address is assigned to the Access Point in forced reload mode. This is done to enable configuring and uploading the software file, before the Access Point has its definite IP address.

Two configurations of your LAN administrator station are possible to enable you to logically access the Access Point:

- Your LAN administrator station is the High Rate Wireless LAN station.
- Your LAN administrator station is a wired (Ethernet) station.

Your LAN administrator station is a Wired Station

Your LAN administrator station is connected to the Access Point via the Ethernet interface of the Access Point.

- Make sure the LAN administrator station and the Access Point are connected to the same LAN segment (subnet).

To communicate with the Access Point in “Forced Reload” state, no routers are allowed between the target Access Point and the LAN administrator station.

- When using IP addressing, write down the IP address that the Access Point should use.

Your LAN administrator station is a Wireless Station

You can use a wireless LAN administrator station to access the Access Point in force reload mode **ONLY IF** the station has indirect access to the Access Point, as described on “Wireless Access via an Indirect Connection” on page 3-9.

Make sure that your LAN administrator station matches the settings of the Access Point that you will use to establish the connection to in forced reload mode.

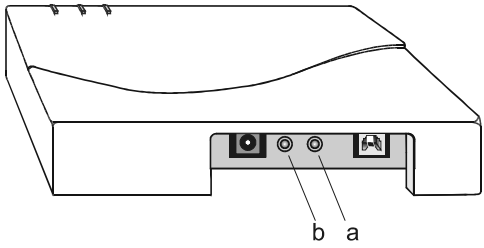
- Make sure the LAN administrator station is within range of the Access Point.

When using IP addressing, write down the (new) IP address that you would like to assign to the Access Point in forced reload mode.

Step 2 - Set to “Forced Reload” Mode

1. Remove the cover of the Access Point.
2. Locate the two small holes on the long-edge side of the processor module, marked “Reset” (A) and “Reload” (B) (see Figure C-1).

Figure C-1. Reset and Reload Buttons

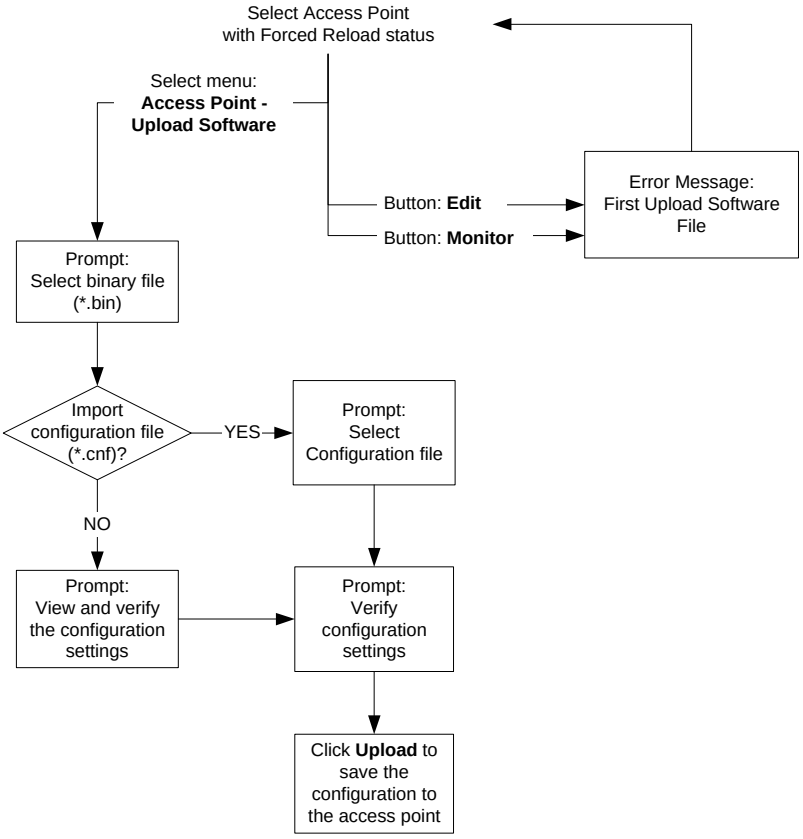


3. Use a small pointed object, such as the tip of a ball-point, to press the **Reset** button.
4. Release the **Reset** button and wait 5 seconds.
   The Access Point will perform start-up diagnostics, characterized by LED activity, where the LEDs will change color in the range Amber, Red and Green.
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.
7. Start the AP Manager program and proceed with “Step 3 - Configuring and Uploading Files”

Step 3 - Configuring and Uploading Files

The complete configuration and upload procedure of the forced reload procedure is pictured in Figure C-2.

Figure C-2. Configuration an upload in forced reload mode

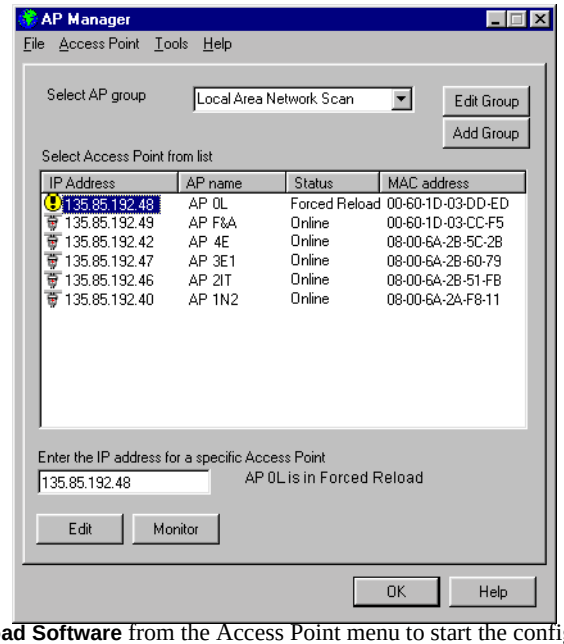


To configure the Access Point in forced reload status and to upload the configuration perform the following steps:

1. Select the Access Point which is in Forced Reload.
   The Access Point in Forced Reload status is displayed in the main AP Manager at the top of the list and can be recognized window as follows (see Figure C-3):

   - the Access Point is marked with the Forced Reload icon,
   - the Access Point is marked with the status “Forced Reload”, and
   - the Access Point has the IP address 153.69.254.254.

Figure C-3. The Access Point in Forced Reload



2. Select **Upload Software** from the Access Point menu to start the configuration and upload procedure.

   - If you click the **Edit** or **Monitor** button before uploading the software, you will be prompted to upload the software first.

3. In the Open window, move to the directory where you have installed the AP Manager program. If you downloaded the latest Access Point software from the IBM High Rate Wireless LAN website, select the directory where you saved the downloaded file.
4. From the list of displayed files, select the file "wpnt*xxx*.bin" or "ap05xxx.bin", (where "*xxx*" identifies the version of the Access Point software).
5. Click the **Open** button to open the software file.
6. You now have the possibility to upload a back-up configuration file to the Access Point.

Note: When importing a configuration file, make sure you import the correct back-up file. Configuring the Access Point with a configuration file that is identical to the configuration of another Access Point may lead to unpredictable behavior of your network.

- If you **do** have a back-up configuration file and if you **do** wish to use this file to configure the Access Point, click **Yes**.

  Select the back-up configuration file (*.cnf) and click **Open** to open the back-up configuration settings.

  You are advised to check the configuration settings. Click **Ok** to continue.

- If you **do not** have a back-up configuration file, or if you do have a file but **do not** want to use this file to configure the Access Point click **No**.

You are now advised to manually modify/verify the configuration settings of the Access Point (i.e. assign a unique IP address, setup the High Rate Wireless LAN parameters and, (if applicable) the other Access Point identifiers such as the IP Address and SNMP passwords).

7. The Edit Configuration window is displayed. Note that the Edit Configuration window does not contain an **OK** button but an **Upload** button to upload the configuration settings to the Access Point.This means that you are editing a local configuration file and that you are not yet connected to the Access Point.
8. View (and modify) the configuration settings in all tabs.
   Refer to Part 4 “Basic Network Configuration” for changing the configuration settings.
9. Click the **Upload** button to upload the new configuration settings to the Access Point in force reload mode.
   The message “Please wait while trying to connect to the Access Point” appears. While trying to connect to the Access Point, the IP address in the configuration settings is pinged.
   - Only if the IP address specified in the configuration already exists, you are prompted to enter a new IP address. If the IP address does not yet exists the uploading continues.
   - Because the password of the Access Point in forced reload mode is always “public”, you do not have to enter this password before uploading information to the Access Point.
10. When prompted to confirm the “Reload of the Remote System”, click **Yes** to continue.
    The local software file (“wpntxxx.bin” or “ap05xxx.bin”) will now import the configuration settings and save these to the software (binary) file. The software file will now be overwritten by the new software file. This does not influence the functionality of the software file. For more information see “Upload Software, a Look under the Hood” on page D-2.
    When you want to preserve the original software file, make a back-up copy of this file.
11. You are again prompted to confirm the “Reload of the Remote System”. Check the list of parameters displayed thoroughly to make sure all settings are right.
    - 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.
12. The AP Manager program will upload the new (restored) configuration to your Access Point and load it into the FlashROM. The Access Point will reboot and start bridging operation in approximately 60 seconds.

Creating a Back-up File

You are advised to save the configuration parameters of the Access Point to a back-up file (*.cnf). To create a back-up file, use the **Download Config File** option from the Access Point menu.

You are advised to create a back-up file, to anticipate future network errors that might force you to perform a forced reload in the future.

Save the back-up file under a name that allows for easy identification in the future.

Start-up Diagnostics

On reboot, the Access Point will perform start-up diagnostics characterized by a LED sequence, where the LEDs will change color in the range Amber, Red and Green.

The start-up diagnostics take approximately 15 seconds. When finished the Access Point will start bridge operation characterized by the LED activity. See Appendix B “Troubleshooting” for more information.

Appendix D: Upgrading Access Point Software

About the Access Point Software

The Access Point runs on embedded software, that is also referred to as “firmware” or “Bridge Kernel”. This software is already factory installed, so in normal situations, you do not need to worry about the software of the Access Point.

In exceptional cases however, you may choose to load new Access Point software into the FlashROM of your Access Points, for example in situations where:

- You wish to upgrade your Access Point to support new functionalities.
- You were advised to do so by IBM support
- You need to perform a forced reload procedure.

The Access Point software is a binary file of the format “wpntxxx.bin”, where *xxx* identifies the version of the Access Point software.

You can find a copy of this file in the program directory where you installed the AP Manager program. For the latest version of the Access Point software versions you are advised to consult the IBM High Rate Wireless LAN website.

Upload Software

When uploading Access Point software (or firmware) no changes are made to the configuration of the Access Point. However, it is recommended to create a back-up file using the **Download Config File** from the **Access Point** menu in case no backup-file exist of the current configuration setting.

1. Select the target Access Point from the list or enter an IP address for a specific Access Point.
2. From the **Access Point** menu, select **Upload Software**.
   The AP Manager program will prompt you to open an Access Point software file (*.bin).
3. Move to the directory where you have installed the AP Manager program file, or the directory where you saved the Access Point software file you downloaded from the IBM High Rate Wireless LAN website.
4. From the list of displayed files, select the file “wpntxxx.bin”, where “xxx” identifies the version of the Access Point software.
5. Click the **Open** button to open the Access Point software file.
6. Enter the password for the Access Point if you are prompted to and click **OK** to continue.
7. When prompted to confirm the Access Point software upload, click **Yes**.
   The Access Point will now reboot and start bridging operation using the parameters as set in the software file.

Confirm Upload Access Point Software

When you try to upload the Access Point software file (*.bin) to your Access Point, a message box will pop-up asking you to confirm:

- The upload to the Access Point, and
- Overwriting the Access Point software file (*.bin) that you selected for upload to the Access Point.

You do not need to be concerned that the Access Point software file will be overwritten, as this will affect neither its functionality nor its features.

Yes, Upload Access Point Software

When you select “Yes, Upload Access Point Software”, the AP Manager program will:

1. First save the Access Point software file back to disk, using the same filename, i.e. the software file you opened will be overwritten.
2. Next use the saved file to upload the target Access Point.

When the Access Point software file is saved to disk, the “Configuration Parameter Area” of the software file is updated with the settings that were retrieved from the Access Point or imported from the back-up file (*.cnf). The “Software Area” of the Access Point software file remains unchanged (see for more information “Upload Software, a Look under the Hood” on page D-2.

As the “Software Area” remains unchanged, overwriting the software file does not affect the functionality or the features of this software file.

No, do not Upload Access Point Software

When you select “No, do not Upload Access Point Software”, the AP Manager program will abort the upload operation.

If you would still like to upload the Access Point software, but hesitate to overwrite the original software file, you are advised to make a back-up copy of the original software file (*.bin) and save it to a separate (floppy) disk drive.

Upload Software, a Look under the Hood

Actually the Access Point software file consists of two information areas that are both stored in the FlashROM of the Access Point Bridge:

1. The actual software program area. The data in this area can not be configured by the end-user.
2. The Configuration Parameters area that contains user-defined settings of the Access Point. The data in this area can be modified at any moment when you use the AP Manager program to open and save a remote config file.

What actually happens in the procedure to upload Access Point software, is that the AP Manager program will merge the configuration parameters retrieved from the Access Point with the software information from the Access Point software file (*.bin). These will be saved to disk first, prior to uploading the information into the Access Point.

Appendix E: Help and service information

This section contains information on how to obtain online and telephone technical support.

Technical support

Technical support is available during the life of your product. Assistance can be obtained through the Personal Computing Support Web site and the IBM Automated Fax System. During the warranty period, assistance for replacement or exchange of defective components is available. In addition, if your IBM option is installed in an IBM computer, you might be entitled to service at your location. Your technical support representative can help you determine the best alternative.

Technical support	
IBM Personal Computing Support Web Site	http://www.ibm.com/pc/support
IBM Automated Fax System	1-800-426-3395 1-800-465-3299 (in Canada)

Marketing, installation, and configuration support through the HelpCenter will be withdrawn or made available for a fee, at IBM's discretion, 90 days after the option has been withdrawn from marketing. Additional support offerings, including step-by-step installation assistance, are available for a nominal fee.

Telephone technical support

To assist the technical support representative, have available as much of the following information as possible:

1. Option name
2. Option number
3. Proof of purchase
4. Computer manufacturer, model, serial number (if IBM), and manual
5. Exact wording of the error message (if any)
6. Description of the problem
7. Hardware and software configuration information for your system

If possible, be at your computer. Your technical support representative might want to walk you through the problem during the call.

For the support telephone number and support hours by country, refer to the following table or to the enclosed technical support insert. If the number is not provided, contact your IBM reseller or IBM marketing representative. Response time may vary depending on the number and nature of the calls received.

Support 24 hours a day, 7 days a week	
Canada (Toronto only)	1-416-333-3344
Canada (all others)	1-800-565-3344
U.S.A. / Puerto Rico	1-800-772-2227

Power supply FRU part numbers

IBM High Rate Wireless LAN Access Point Power Supply	
Region/country	**Part Number**
US & Japan FRU	22P4935
Euro FRU	22P4936
UK FRU	22P4937
ANZ FRU	22P4939

Appendix F: Product warranties and notices

The following section provides product warranty information and legal notices.

Warranty Statements

The warranty statements consist of two parts: Part 1 and Part 2. Part 1 varies by country. Part 2 is the same for both statements. Be sure to read both the Part 1 that applies to your country and Part 2.

- **United States, Puerto Rico, and Canada (Z125-4753-05 11/97)** "IBM Statement of Limited Warranty for United States, Puerto Rico, and Canada (Part 1 - General Terms)"
- **Worldwide except Canada, Puerto Rico, Turkey, and United States (Z125-5697-01 11/97)** "IBM Statement of Warranty Worldwide except Canada, Puerto Rico, Turkey, United States (Part 1 - General Terms)" on page D-4
- **Worldwide Country-Unique Terms**"Part 2 - Worldwide Country-Unique Terms" on page D-7

IBM Statement of Limited Warranty for United States, Puerto Rico, and Canada (Part 1 - General Terms)

This Statement of Warranty includes Part 1 - General Terms and Part 2 - Country-unique Terms. **The terms of Part 2 may replace or modify those of Part 1.** *The warranties provided by IBM in this Statement of Warranty apply only to Machines you purchase for your use, and not for resale, from IBM or your reseller. The term "Machine" means an IBM machine, its features, conversions, upgrades, elements, or accessories, or any combination of them. The term "Machine" does not include any software programs, whether pre-loaded with the Machine, installed subsequently or otherwise. Unless IBM specifies otherwise, the following warranties apply only in the country where you acquire the Machine. Nothing in this Statement of Warranty affects any statutory rights of consumers that cannot be waived or limited by contract. If you have any questions, contact IBM or your reseller.*

The IBM Warranty for Machines

Machine - IBM High-Rate Wireless Access Point

Warranty period* - 3 Years

** Contact your place of purchase for warranty service information. Some IBM Machines are eligible for on-site warranty service depending on the country where service is performed.*

IBM warrants that each Machine 1) is free from defects in materials and workmanship and 2) conforms to IBM's Official Published Specifications. The warranty period for a Machine is a specified, fixed period commencing on its Date of Installation. The date on your sales receipt is the Date of Installation, unless IBM or your reseller informs you otherwise.

During the warranty period IBM or your reseller, if approved by IBM to provide warranty service, will provide repair and exchange service for the Machine, without charge, under the type of service designated for the Machine and will manage and install engineering changes that apply to the Machine.

If a Machine does not function as warranted during the warranty period, and IBM or your reseller are unable to either 1) make it do so or 2) replace it with one that is at least functionally equivalent, you may return it to your place of purchase and your money will be refunded. The replacement may not be new, but will be in good working order.

Extent of Warranty

The warranty does not cover the repair or exchange of a Machine resulting from misuse, accident, modification, unsuitable physical or operating environment, improper maintenance by you, or failure caused by a product for which IBM is not responsible. The warranty is voided by removal or alteration of Machine or parts identification labels.

THESE WARRANTIES ARE YOUR EXCLUSIVE WARRANTIES AND REPLACE ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THESE WARRANTIES GIVE YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF EXPRESS OR IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION OR LIMITATION MAY NOT APPLY TO YOU. IN THAT EVENT, SUCH WARRANTIES ARE LIMITED IN DURATION TO THE WARRANTY PERIOD. NO WARRANTIES APPLY AFTER THAT PERIOD.

Items Not Covered by Warranty

IBM does not warrant uninterrupted or error-free operation of a Machine.

Unless specified otherwise, IBM provides non-IBM machines **WITHOUT WARRANTIES OF ANY KIND.**

Any technical or other support provided for a Machine under warranty, such as assistance via telephone with "how-to" questions and those regarding Machine set-up and installation, will be provided **WITHOUT WARRANTIES OF ANY KIND.**

Warranty Service

To obtain warranty service for the Machine, contact your reseller or IBM. In the United States, call IBM at 1-800-565-3344. In Canada, call IBM at 1-800-565-3344. You may be required to present proof of purchase.

IBM or your reseller provides certain types of repair and exchange service, either at your location or at a service center, to keep Machines in, or restore them to, conformance with their Specifications. IBM or your reseller will inform you of the available types of service for a Machine based on its country of installation. IBM may repair the failing Machine or exchange it at its discretion.

When warranty service involves the exchange of a Machine or part, the item IBM or your reseller replaces becomes its property and the replacement becomes yours. You represent that all removed items are genuine and unaltered. The replacement may not be new, but

will be in good working order and at least functionally equivalent to the item replaced. The replacement assumes the warranty service status of the replaced item.

Any feature, conversion, or upgrade IBM or your reseller services must be installed on a Machine which is 1) for certain Machines, the designated, serial-numbered Machine and 2) at an engineering-change level compatible with the feature, conversion, or upgrade. Many features, conversions, or upgrades involve the removal of parts and their return to IBM. A part that replaces a removed part will assume the warranty service status of the removed part.

Before IBM or your reseller exchanges a Machine or part, you agree to remove all features, parts, options, alterations, and attachments not under warranty service.

You also agree to

1. ensure that the Machine is free of any legal obligations or restrictions that prevent its exchange;
2. obtain authorization from the owner to have IBM or your reseller service a Machine that you do not own; and
3. where applicable, before service is provided

    a. follow the problem determination, problem analysis, and service request procedures that IBM or your reseller provides,

    b. secure all programs, data, and funds contained in a Machine,

    c. provide IBM or your reseller with sufficient, free, and safe access to your facilities to permit them to fulfill their obligations, and

    d. inform IBM or your reseller of changes in a Machine's location.

IBM is responsible for loss of, or damage to, your Machine while it is 1) in IBM's possession or 2) in transit in those cases where IBM is responsible for the transportation charges.

Neither IBM nor your reseller is responsible for any of your confidential, proprietary or personal information contained in a Machine which you return to IBM or your reseller for any reason. You should remove all such information from the Machine prior to its return.

Production Status

Each IBM Machine is manufactured from new parts, or new and used parts. In some cases, the Machine may not be new and may have been previously installed. Regardless of the Machine's production status, IBM's appropriate warranty terms apply.

Limitation of Liability

Circumstances may arise where, because of a default on IBM's part or other liability, you are entitled to recover damages from IBM. In each such instance, regardless of the basis on which you are entitled to claim damages from IBM (including fundamental breach, negligence, misrepresentation, or other contract or tort claim), IBM is liable for no more than

damages for bodily injury (including death) and damage to real property and tangible personal property; and

the amount of any other actual direct damages, up to the greater of U.S. $100,000 (or equivalent in local currency) or the charges (if recurring, 12 months' charges apply) for the Machine that is the subject of the claim.

This limit also applies to IBM's suppliers and your reseller. It is the maximum for which IBM, its suppliers, and your reseller are collectively responsible.

UNDER NO CIRCUMSTANCES IS IBM LIABLE FOR ANY OF THE FOLLOWING: 1) THIRD-PARTY CLAIMS AGAINST YOU FOR DAMAGES (OTHER THAN THOSE UNDER THE FIRST ITEM LISTED ABOVE); 2) LOSS OF, OR DAMAGE TO, YOUR RECORDS OR DATA; OR 3) SPECIAL, INCIDENTAL, OR INDIRECT DAMAGES OR FOR ANY ECONOMIC CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), EVEN IF IBM, ITS SUPPLIERS OR YOUR RESELLER IS INFORMED OF THEIR POSSIBILITY. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

IBM Statement of Warranty Worldwide except Canada, Puerto Rico, Turkey, United States (Part 1 - General Terms)

This Statement of Warranty includes Part 1 - General Terms and Part 2 - Country-unique Terms. **The terms of Part 2 may replace or modify those of Part 1.** *The warranties provided by IBM in this Statement of Warranty apply only to Machines you purchase for your use, and not for resale, from IBM or your reseller. The term "Machine" means an IBM machine, its features, conversions, upgrades, elements, or accessories, or any combination of them. The term "Machine" does not include any software programs, whether pre-loaded with the Machine, installed subsequently or otherwise. Unless IBM specifies otherwise, the following warranties apply only in the country where you acquire the Machine. Nothing in this Statement of Warranty affects any statutory rights of consumers that cannot be waived or limited by contract. If you have any questions, contact IBM or your reseller.*

Machine - IBM High-Rate Wireless Access Point

Warranty period* - 3 Years

** Contact your place of purchase for warranty service information. Some IBM Machines are eligible for on-site warranty service depending on the country where service is performed.*

The IBM Warranty for Machines

IBM warrants that each Machine 1) is free from defects in materials and workmanship and 2) conforms to IBM's Official Published Specifications. The warranty period for a Machine is a specified, fixed period commencing on its Date of Installation. The date on your sales receipt is the Date of Installation, unless IBM or your reseller informs you otherwise.

During the warranty period IBM or your reseller, if approved by IBM to provide warranty service, will provide repair and exchange service for the Machine, without charge, under

the type of service designated for the Machine and will manage and install engineering changes that apply to the Machine.

If a Machine does not function as warranted during the warranty period, and IBM or your reseller are unable to either 1) make it do so or 2) replace it with one that is at least functionally equivalent, you may return it to your place of purchase and your money will be refunded. The replacement may not be new, but will be in good working order.

Extent of Warranty

The warranty does not cover the repair or exchange of a Machine resulting from misuse, accident, modification, unsuitable physical or operating environment, improper maintenance by you, or failure caused by a product for which IBM is not responsible. The warranty is voided by removal or alteration of Machine or parts identification labels.

THESE WARRANTIES ARE YOUR EXCLUSIVE WARRANTIES AND REPLACE ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THESE WARRANTIES GIVE YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF EXPRESS OR IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION OR LIMITATION MAY NOT APPLY TO YOU. IN THAT EVENT, SUCH WARRANTIES ARE LIMITED IN DURATION TO THE WARRANTY PERIOD. NO WARRANTIES APPLY AFTER THAT PERIOD.

Items Not Covered by Warranty

IBM does not warrant uninterrupted or error-free operation of a Machine.

Unless specified otherwise, IBM provides non-IBM machines **WITHOUT WARRANTIES OF ANY KIND.**

Any technical or other support provided for a Machine under warranty, such as assistance via telephone with "how-to" questions and those regarding Machine set-up and installation, will be provided **WITHOUT WARRANTIES OF ANY KIND.**

Warranty Service

To obtain warranty service for the Machine, contact your reseller or IBM. You may be required to present proof of purchase.

IBM or your reseller provides certain types of repair and exchange service, either at your location or at a service center, to keep Machines in, or restore them to, conformance with their Specifications. IBM or your reseller will inform you of the available types of service for a Machine based on its country of installation. IBM may repair the failing Machine or exchange it at its discretion.

When warranty service involves the exchange of a Machine or part, the item IBM or your reseller replaces becomes its property and the replacement becomes yours. You represent that all removed items are genuine and unaltered. The replacement may not be new, but will be in good working order and at least functionally equivalent to the item replaced. The replacement assumes the warranty service status of the replaced item.

Any feature, conversion, or upgrade IBM or your reseller services must be installed on a Machine which is 1) for certain Machines, the designated, serial-numbered Machine and 2) at an engineering-change level compatible with the feature, conversion, or upgrade. Many features, conversions, or upgrades involve the removal of parts and their return to IBM. A part that replaces a removed part will assume the warranty service status of the removed part.

Before IBM or your reseller exchanges a Machine or part, you agree to remove all features, parts, options, alterations, and attachments not under warranty service.

You also agree to

1. ensure that the Machine is free of any legal obligations or restrictions that prevent its exchange;
2. obtain authorization from the owner to have IBM or your reseller service a Machine that you do not own; and
3. where applicable, before service is provided

    a. follow the problem determination, problem analysis, and service request procedures that IBM or your reseller provides,

    b. secure all programs, data, and funds contained in a Machine,

    c. provide IBM or your reseller with sufficient, free, and safe access to your facilities to permit them to fulfill their obligations, and

    d. inform IBM or your reseller of changes in a Machine's location.

IBM is responsible for loss of, or damage to, your Machine while it is 1) in IBM's possession or 2) in transit in those cases where IBM is responsible for the transportation charges.

Neither IBM nor your reseller is responsible for any of your confidential, proprietary or personal information contained in a Machine which you return to IBM or your reseller for any reason. You should remove all such information from the Machine prior to its return.

Production Status

Each IBM Machine is manufactured from new parts, or new and used parts. In some cases, the Machine may not be new and may have been previously installed. Regardless of the Machine's production status, IBM's appropriate warranty terms apply.

Limitation of Liability

Circumstances may arise where, because of a default on IBM's part or other liability, you are entitled to recover damages from IBM. In each such instance, regardless of the basis on which you are entitled to claim damages from IBM (including fundamental breach, negligence, misrepresentation, or other contract or tort claim), IBM is liable for no more than

1. damages for bodily injury (including death) and damage to real property and tangible personal property; and
2. the amount of any other actual direct damages, up to the greater of U.S. $100,000 (or equivalent in local currency) or the charges (if recurring, 12 months' charges apply) for the Machine that is the subject of the claim.

This limit also applies to IBM's suppliers and your reseller. It is the maximum for which IBM, its suppliers, and your reseller are collectively responsible.

UNDER NO CIRCUMSTANCES IS IBM LIABLE FOR ANY OF THE FOLLOWING: 1) THIRD-PARTY CLAIMS AGAINST YOU FOR DAMAGES (OTHER THAN THOSE UNDER THE FIRST ITEM LISTED ABOVE); 2) LOSS OF, OR DAMAGE TO, YOUR RECORDS OR DATA; OR 3) SPECIAL, INCIDENTAL, OR INDIRECT DAMAGES OR FOR ANY ECONOMIC CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), EVEN IF IBM, ITS SUPPLIERS OR YOUR RESELLER IS INFORMED OF THEIR POSSIBILITY. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

Part 2 - Worldwide Country-Unique Terms

ASIA PACIFIC

AUSTRALIA: The IBM Warranty for Machines: The following paragraph is added to this Section:
The warranties specified in this Section are in addition to any rights you may have under the Trade Practices Act 1974 or other legislation and are only limited to the extent permitted by the applicable legislation.

Extent of Warranty: The following replaces the first and second sentences of this Section:
The warranty does not cover the repair or exchange of a Machine resulting from misuse, accident, modification, unsuitable physical or operating environment, operation in other than the Specified Operating Environment, improper maintenance by you, or failure caused by a product for which IBM is not responsible.

Limitation of Liability: The following is added to this Section:
Where IBM is in breach of a condition or warranty implied by the Trade Practices Act 1974, IBM's liability is limited to the repair or replacement of the goods or the supply of equivalent goods. Where that condition or warranty relates to right to sell, quiet possession or clear title, or the goods are of a kind ordinarily acquired for personal, domestic or household use or consumption, then none of the limitations in this paragraph apply.

PEOPLE'S REPUBLIC OF CHINA: Governing Law: The following is added to this Statement:
The laws of the State of New York govern this Statement.

INDIA: Limitation of Liability: The following replaces items 1 and 2 of this Section:

liability for bodily injury (including death) or damage to real property and tangible personal property will be limited to that caused by IBM's negligence;

as to any other actual damage arising in any situation involving nonperformance by IBM pursuant to, or in any way related to the subject of this Statement of Warranty, IBM's liability will be limited to the charge paid by you for the individual Machine that is the subject of the claim.

NEW ZEALAND: The IBM Warranty for Machines: The following paragraph is added to this Section:
The warranties specified in this Section are in addition to any rights you may have under the Consumer Guarantees Act 1993 or other legislation which cannot be excluded or

limited. The Consumer Guarantees Act 1993 will not apply in respect of any goods which IBM provides, if you require the goods for the purposes of a business as defined in that Act.

Limitation of Liability: The following is added to this Section:
Where Machines are not acquired for the purposes of a business as defined in the Consumer Guarantees Act 1993, the limitations in this Section are subject to the limitations in that Act.

EUROPE, MIDDLE EAST, AFRICA (EMEA)

The following terms apply to all EMEA countries.

The terms of this Statement of Warranty apply to Machines purchased from an IBM reseller. If you purchased this Machine from IBM, the terms and conditions of the applicable IBM agreement prevail over this warranty statement.

Warranty Service

If you purchased an IBM Machine in Austria, Belgium, Denmark, Estonia, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland or United Kingdom, you may obtain warranty service for that Machine in any of those countries from either (1) an IBM reseller approved to perform warranty service or (2) from IBM.

If you purchased an IBM Personal Computer Machine in Albania, Armenia, Belarus, Bosnia and Herzegovina, Bulgaria, Croatia, Czech Republic, Georgia, Hungary, Kazakhstan, Kirghizia, Federal Republic of Yugoslavia, Former Yugoslav Republic of Macedonia (FYROM), Moldova, Poland, Romania, Russia, Slovak Republic, Slovenia, or Ukraine, you may obtain warranty service for that Machine in any of those countries from either (1) an IBM reseller approved to perform warranty service or (2) from IBM.

The applicable laws, Country-unique terms and competent court for this Statement are those of the country in which the warranty service is being provided. However, the laws of Austria govern this Statement if the warranty service is provided in Albania, Armenia, Belarus, Bosnia and Herzegovina, Bulgaria, Croatia, Czech Republic, Federal Republic of Yugoslavia, Georgia, Hungary, Kazakhstan, Kirghizia, Former Yugoslav Republic of Macedonia (FYROM), Moldova, Poland, Romania, Russia, Slovak Republic, Slovenia, and Ukraine.

The following terms apply to the country specified:

EGYPT: Limitation of Liability: The following replaces item 2 in this Section:
2. as to any other actual direct damages, IBM's liability will be limited to the total amount you paid for the Machine that is the subject of the claim.

Applicability of suppliers and resellers (unchanged).

FRANCE: Limitation of Liability: The following replaces the second sentence of the first paragraph of this Section:
In such instances, regardless of the basis on which you are entitled to claim damages from IBM, IBM is liable for no more than: (items 1 and 2 unchanged).

GERMANY: The IBM Warranty for Machines: The following replaces the first sentence of the first paragraph of this Section:
The warranty for an IBM Machine covers the functionality of the Machine for its normal use and the Machine's conformity to its Specifications.

The following paragraphs are added to this Section:
The minimum warranty period for Machines is six months.

In case IBM or your reseller are unable to repair an IBM Machine, you can alternatively ask for a partial refund as far as justified by the reduced value of the unrepaired Machine or ask for a cancellation of the respective agreement for such Machine and get your money refunded.

Extent of Warranty: The second paragraph does not apply.

Warranty Service: The following is added to this Section:
During the warranty period, transportation for delivery of the failing Machine to IBM will be at IBM's expense.

Production Status: The following paragraph replaces this Section:
Each Machine is newly manufactured. It may incorporate in addition to new parts, re-used parts as well.

Limitation of Liability: The following is added to this Section:
The limitations and exclusions specified in the Statement of Warranty will not apply to damages caused by IBM with fraud or gross negligence and for express warranty.

In item 2, replace "U.S. $100,000" with "1.000.000 DEM."

The following sentence is added to the end of the first paragraph of item 2:
IBM's liability under this item is limited to the violation of essential contractual terms in cases of ordinary negligence.

IRELAND: Extent of Warranty: The following is added to this Section:
Except as expressly provided in these terms and conditions, all statutory conditions, including all warranties implied, but without prejudice to the generality of the foregoing all warranties implied by the Sale of Goods Act 1893 or the Sale of Goods and Supply of Services Act 1980 are hereby excluded.

Limitation of Liability: The following replaces items one and two of the first paragraph of this Section:
1. death or personal injury or physical damage to your real property solely caused by IBM's negligence; and 2. the amount of any other actual direct damages, up to the greater of Irish Pounds 75,000 or 125 percent of the charges (if recurring, the 12 months' charges apply) for the Machine that is the subject of the claim or which otherwise gives rise to the claim.

Applicability of suppliers and resellers (unchanged).

The following paragraph is added at the end of this Section:
IBM's entire liability and your sole remedy, whether in contract or in tort, in respect of any default shall be limited to damages.

ITALY: Limitation of Liability: The following replaces the second sentence in the first paragraph:
In each such instance unless otherwise provided by mandatory law, IBM is liable for no more than: (item 1 unchanged) 2) as to any other actual damage arising in all situations involving non-performance by IBM pursuant to, or in any way related to the subject matter of this Statement of Warranty, IBM's liability, will be limited to the total amount you paid for the Machine that is the subject of the claim.

Applicability of suppliers and resellers (unchanged).

The following replaces the second paragraph of this Section:
Unless otherwise provided by mandatory law, IBM and your reseller are not liable for any of the following: (items 1 and 2 unchanged) 3) indirect damages, even if IBM or your reseller is informed of their possibility.

SOUTH AFRICA, NAMIBIA, BOTSWANA, LESOTHO AND SWAZILAND: Limitation of Liability: The following is added to this Section:
IBM's entire liability to you for actual damages arising in all situations involving nonperformance by IBM in respect of the subject matter of this Statement of Warranty will be limited to the charge paid by you for the individual Machine that is the subject of your claim from IBM.

TURKIYE: Production Status: The following replaces this Section:
IBM fulfills customer orders for IBM Machines as newly manufactured in accordance with IBM's production standards.

UNITED KINGDOM: Limitation of Liability: The following replaces items 1 and 2 of the first paragraph of this Section:

death or personal injury or physical damage to your real property solely caused by IBM's negligence;

the amount of any other actual direct damages or loss, up to the greater of Pounds Sterling 150,000 or 125 percent of the charges (if recurring, the 12 months' charges apply) for the Machine that is the subject of the claim or which otherwise gives rise to the claim.

The following item is added to this paragraph:
3. breach of IBM's obligations implied by Section 12 of the Sale of Goods Act 1979 or Section 2 of the Supply of Goods and Services Act 1982.

Applicability of suppliers and resellers (unchanged).

The following is added to the end of this Section:
IBM's entire liability and your sole remedy, whether in contract or in tort, in respect of any default will be limited to damages.

NORTH AMERICA

CANADA: Warranty Service: The following is added to this section:
To obtain warranty service from IBM, call **1-800-565-3344**. In Toronto, call **416-383-3344**.

UNITED STATES OF AMERICA: Warranty Service: The following is added to this section:
To obtain warranty service from IBM, call **1-800-772-2227**.

Notices

This publication was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's

responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

- IBM

Microsoft, Windows, and Windows NT, are trademarks of the Microsoft Corporation in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Electronic emission notices

High-Rate Wireless LAN Access Point

Federal Communications Commission (FCC) Statement

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult an IBM authorized dealer or service representative for help.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Proper cables and connectors are available from IBM authorized dealers. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Responsible party:

International Business Machines Corporation
New Orchard Road
Armonk, NY 10504
Telephone: 1-919-543-2193

Tested To Comply
With FCC Standards
FOR HOME OR OFFICE USE

Industry Canada Class B emission compliance statement

This Class B digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de classe B est conforme à la norme NMB-003 du Canada.

Deutsche EMV-Direktive (electromagnetische Verträglichkeit)

Dieses Gerät ist berechtigt in Übereinstimmung mit dem deutschen EMVG vom 9.Nov.92 das EG-Konformitätszeichen zu führen.

Der Aussteller der Konformitätserklärung ist die IBM UK, Greenock.

Dieses Gerät erfüllt die Bedingungen der EN 55022 Klasse B.

European Union EMC Directive conformance statement

This product is in conformity with the protection requirements of EU Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a nonrecommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class B Information Technology Equipment according to CISPR 22/European Standard EN 55022. The limits for Class B equipment were derived for typical residential environments to provide reasonable protection against interference with licensed communication devices.

Union Européenne - Directive Conformité électromagnétique

Ce produit est conforme aux exigences de protection de la Directive 89/336/EEC du Conseil de l'UE sur le rapprochement des lois des États membres en matière de compatibilité électromagnétique.

IBM ne peut accepter aucune responsabilité pour le manquement aux exigences de protection résultant d'une modification non recommandée du produit, y compris l'installation de cartes autres que les cartes IBM.

Ce produit a été testé et il satisfait les conditions de l'équipement informatique de Classe B en vertu de CISPR22 / Standard européen EN 55022. Les conditions pour l'équipement de Classe B ont été définies en fonction d'un contexte résidentiel ordinaire afin de fournir une protection raisonnable contre l'interférence d'appareils de communication autorisés.

Unione Europea - Directiva EMC (Conformidad électromagnética)

Este producto satisface los requisitos de protección del Consejo de la UE, Directiva 89/336/CEE en lo que a la legislatura de los Estados Miembros sobre compatibilidad electromagnética se refiere.

IBM no puede aceptar responsabilidad alguna si este producto deja de satisfacer dichos requisitos de protección como resultado de una modificación no recomendada del producto, incluyendo el ajuste de tarjetas de opción que no sean IBM.

Este producto ha sido probado y satisface los límites para Equipos Informáticos Clase B de conformidad con el Estándar CISPR22 y el Estándar Europeo EN 55022. Los límites para los equipos de Clase B se han establecido para entornos residenciales típicos a fin de proporcionar una protección razonable contra las interferencias con dispositivos de comunicación licenciados.

Part Number:

Printed in Taiwan R.O.C. on recycled paper
containing 10% recovered post-consumer fiber.

Union Europea - Normativa EMC

Questo prodotto è conforme alle normative di protezione ai sensi della Direttiva del Consiglio dell'Unione Europea 89/336/CEE sull'armonizzazione legislativa degli stati membri in materia di compatibilità elettromagnetica.

IBM non accetta responsabilità alcuna per la mancata conformità alle normative di protezione dovuta a modifiche non consigliate al prodotto, compresa l'installazione di schede e componenti di marca diversa da IBM.

Le prove effettuate sul presente prodotto hanno accertato che esso rientra nei limiti stabiliti per le le apparecchiature di informatica Classe B ai sensi del CISPR 22 / Norma Europea EN 55022. I limiti delle apparecchiature della Classe B sono stati stabiliti al fine di fornire ragionevole protezione da interferenze mediante dispositivi di comunicazione in concessione in ambienti residenziali tipici.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。