IBM

High-Rate Wireless LAN Access Point

User's Guide

OPTIONS
by IBM

IBM

High-Rate Wireless LAN Access Point

User's Guide

Note:

Before using this manual and the product it supports, see Appendix D: Product warranties and notices, on page D-1 of the *High-Rate Wireless LAN Access Point Quick Start Guide* **included in your option package.**

First Edition (June 2000)

Contents

Safety Information

Before installing this product, read the Safety Information book.

مج، يجب قراءة   دات السلامة

Antes de instalar este produto, leia o Manual de Informações sobre Segurança.

安装本产品前请先阅读《安全信息》手册。

Prije instalacije ovog proizvoda pročitajte priručnik sa sigurnosnim uputama.

Před instalací tohoto produktu si přečtěte příručku bezpečnostních instrukcí.

Læs hæftet med sikkerhedsforskrifter, før du installerer dette produkt.

Lue Safety Information -kirjanen, ennen kuin asennat tämän tuotteen.

Avant de procéder à l'installation de ce produit, lisez le manuel Safety Information.

Vor Beginn der Installation die Broschüre mit Sicherheitshinweisen lesen.

Πριν εγκαταστήσετε αυτό το προϊόν, διαβάστε το εγχειρίδιο Safety Information.

לפני שתתקינו מוצר זה, קראו את הוראות הבטיחות.

Installálás el tt olvassa el a Biztonsági el írások kézikönyvét !

Prima di installare questo prodotto, leggere l’opuscolo contenente le informazioni sulla sicurezza.

本製品を導入する前に、安全情報資料を御読みください。

이 제품을 설치하기 전에, 안전 정보 책자를 읽어보십시오.

Пред да го инсталирате овој производ прочитајте ја книгата со безбедносни информации.

Lees voordat u dit product installeert eerst het boekje met veiligheidsvoorschriften.

Les heftet om sikkerhetsinformasjon (Safety Information) før du installerer dette produktet.

Przed zainstalowaniem tego produktu należy przeczytać broszurę Informacje Dotyczące Bezpieczeństwa.

Antes de instalar este produto, leia o folheto Informações sobre Segurança.

Перед установкой продукта прочтите брошюру по технике безопасности (Safety Information).

Pred inštaláciou tohto produktu si pre ítajte Informa nú brožúrku o bezpe nosti.

Preden namestite ta izdelek, preberite knjižico Varnostne informacije.

Antes de instalar este producto, lea la Información de Seguridad.

Läs säkerhetsinformationen innan du installerar den här produkten.

在安裝本產品之前，也請先閱讀「安全性資訊」小冊子。

About this book

This manual contains instructions for installing and using the IBM® High-Rate WIreless LAN Access Point. The manual is divided into two parts:

Part 1: Installation and user's guide

This guide contains the product description, hardware and software installation instructions, and product use and maintenance information.

Part 2: Appendixes

The appendixes contain help and service information, the product warranties, and notices.

Note: The illustrations in this manual might be slightly different from your hardware.

Installation and user's guide

This section provides the product and software descriptions, and the installation and user's guide.

For help and service information, and product warranties and notices, see the *High-Rate Wireless LAN Access Point Quick Start Guide* included in your package.

Product description

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

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

The High-Rate Wireless LAN network interface is not much different than the interface for wired LANs. The operating system will not even notice the difference.

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

The High-Rate Wireless LAN tools can be installed on stations that run the Microsoft® Windows® 95, Windows 98, or Microsoft Windows NT® 4.0 operating system. The High-Rate Wireless LAN Client Manager also works with Microsoft Windows 2000 Professional.

The High-Rate Wireless LAN products have been designed for compatibility with all other wireless LAN products that use the direct sequence radio technology, as identified in the IEEE 802.11 standard for wireless LANs. Based on market-leading WaveLAN IEEE 802.11b technology, High-Rate Wireless LAN provides mobile broadband connection to IP/Internet for businesses, homes, and public areas.

However, you might not always be able to use the High-Rate Wireless LAN software suite 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. Each vendor might 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 might not be supported by the other vendors' products.

If other vendors' products do not work with the High-Rate Wireless LAN software suite, refer to the documentation that comes with the other vendors' product.

Software description

The High-Rate Wireless LAN software suite consists of the High-Rate Wireless LAN Client Manager and the High-Rate Wireless LAN AP Manager. These tools enable you to:

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

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

For more information about specific High-Rate Wireless LAN software screens or options, consult the online help.

High-Rate Wireless LAN Client Manager

The High-Rate Wireless LAN Client Manager is a diagnostic tool that you can use to monitor wireless radio communication between a wireless station and its High-Rate Wireless LAN Access Point, or to monitor the link between two wireless stations in an independent network.

It can also be used as a site monitor to show the coverage of the installed High-Rate Wireless LAN Access Point in a certain area.

High-Rate Wireless LAN AP Manager

The High-Rate Wireless LAN Access Point Manager (High-Rate Wireless LAN AP Manager) is primarily a tool for LAN administrators or system supervisors. You can use the High-Rate Wireless LAN AP Manager program to configure High-Rate Wireless LAN Access Points and to monitor the performance of your wireless network. It can be run on wired or wireless stations in the network.

Online help

Information about specific High-Rate Wireless LAN software screens or options in your High-Rate Wireless LAN AP Manager or High-Rate Wireless LAN Client Manager program is included in the online help of the programs.

To access context-sensitive help on a specific screen for the High-Rate Wireless LAN programs, click **Help** or press F1.

In the online help, you can click the **Contents** tab to get an overview of the online information, or click the **Index** tab to open an alphabetical list of specific topics.

Product specifications are listed in the *User's guide* of your High-Rate Wireless LAN products.

Additional files

The CD that comes with your High-Rate Wireless LAN products include a README.TXT file. This file contains information about the version of the software and the device drivers on the CD.

Read this file prior to installing your High-Rate Wireless LAN products; it might contain additional information that was not available when this document was produced. You can also download or view the README.TXT file on the High-Rate Wireless LAN Web site.

Other sources of information

For information on updates and other High-Rate Wireless LAN news, go to the Web site at http:www.ibm.com/pc. For technical support, consult the information in the appendixes.

Wireless configurations

This section describes a number of network scenarios that can 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. The wireless devices can roam freely throughout the network, with the only restrictions being the size and cabling of the wireless device.

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

- Independent network
  - Peer-to-Peer workgroup
- Basic infrastructure
  - Standalone configuration
  - Wireless access to ethernet networks
- Advanced infrastructures
  - Multiple channel configuration

Peer-to-Peer workgroup

A Peer-to-Peer workgroup is a group of High-Rate Wireless LAN wireless devices that do not bridge their data through a High-Rate Wireless LAN 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, that is, by sharing a disk or printer through Microsoft Network Neighborhood.

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

- All wireless stations participate in workgroup computing, that is, they use the disk-sharing option of Microsoft Network Neighborhood and Printers.
- All High-Rate Wireless LAN 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

This section describes the two types of basic infrastructure configurations: standalone configuration and wireless access to Ethernet networks.

Standalone configuration

In a standalone configuration, the High-Rate Wireless LAN Access Point functions as a relay base station that forwards 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 (for example, trade shows) and environments where the installation of a wired infrastructure is not possible.

A server is not required in a standalone wireless configuration; equipped devices can communicate Peer-to-Peer, as described on “Peer-to-Peer workgroup” on page 1-4.

The wireless infrastructure is identified by a unique High-Rate Wireless LAN network name. All equipped devices must be configured with an identical High-Rate Wireless LAN network name before connecting to the network.

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

Wireless access to Ethernet networks

Connecting High-Rate Wireless LAN Access Points to an Ethernet network enables you to create a wireless environment for notebook computers or connect a number of High-Rate Wireless LAN stations (notebook or desktop) to an existing Ethernet infrastructure, creating a larger coverage area.

All wireless stations within this coverage area that are to be connected to the network must be configured with the same High-Rate Wireless LAN network name as the High-Rate Wireless LAN Access Points.

Roaming wireless stations automatically switch between High-Rate Wireless LAN Access Points, when required, maintaining the wireless connection to the network.

Advanced infrastructures

This section describes the multiple channel configuration infrastructure.

Multiple channel configuration

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

By using different channels, you can optimize wireless performance, assigning different frequency channels to neighboring High-Rate Wireless LAN Access Points. Multiple frequency configurations might prove very useful in environments where:

- A high concentration of wireless stations are operational in the same vicinity of one another.
- The High-Rate Wireless LAN stations experience a performance decrease in terms of network response times as a result of the High-Rate Wireless LAN collision avoidance protocol (for more information, see “RTS/CTS protocol” on page 1-41).

By configuring neighboring High-Rate Wireless LAN 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.

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

The preferred channel separation between the channels in neighboring cells is 25 MHz (five channels). Subject to the number of channels supported by the High-Rate Wireless LAN PC Cards available in your country, this means that you can apply up to three different channels within your High-Rate Wireless LAN network.

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, see “Frequency channel management” on page 1-42.

Setting up the LAN administrator’s station

High-Rate Wireless LAN infrastructures are managed from a High-Rate Wireless LAN administrator’s station. This section describes how to set up High-Rate Wireless LAN administrator’s stations to properly manage your network.

Typically, a High-Rate Wireless LAN administrator’s station is a computer used by the LAN administrator to configure, manage, and monitor the High-Rate Wireless LAN network. You can assign as many administrator’s stations as you like, depending on how you want to manage your High-Rate Wireless LAN network.

A High-Rate Wireless LAN administrator’s 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:

- High-Rate Wireless LAN Client Manager
- High-Rate Wireless LAN AP Manager

This section describes how to set up a High-Rate Wireless LAN administrator’s station in the following network configurations:

- Peer-to-Peer workgroups: All stations within the network directly communicate with all other stations. No High-Rate Wireless LAN Access Points are necessary to bridge the data.
- Infrastructure network: All stations communicate to each other and the Ethernet backbone through High-Rate Wireless LAN Access Point interfaces.

For an overview of the High-Rate Wireless LAN software tools, refer to“High-Rate Wireless LAN tools” on page 1-2.

Assigning a LAN administrator’s station

To set up a High-Rate Wireless LAN administrator’s station, you can use any desktop or notebook computer that meets the following requirements:

- An 80486 or faster processor
- 4 MB of free disk space
- 16 MB RAM
- Windows 95, Windows 98, Windows 2000, or Windows NT 4.0

For the High-Rate Wireless LAN Client Manager, you also need a High-Rate Wireless LAN PC Card.

For the High-Rate Wireless LAN AP Manager you will need the following:

- Access to the LAN, through:
  - — a High-Rate Wireless LAN PC Card
  - — an Ethernet card
  - — a 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.

Managing Peer-to-Peer workgroups

A Peer-to-Peer workgroup consists of several stations communicating directly to each other without bridging data through an access point.

Peer-to-Peer workgroups do not need the High-Rate Wireless LAN tools. For more information, refer to the *High-Rate Wireless LAN PC Card User’s Guide*.

Managing infrastructure networks

In an infrastructure network, you will primarily use an High-Rate Wireless LAN administrator’s station that has the High-Rate Wireless LAN AP Manager installed to configure your access points and monitor the radio traffic between selected access points and stations within the network.

You can also install the High-Rate Wireless LAN Client Manager on all stations within the network, or on selected mobile stations with a High-Rate Wireless LAN PC Card, to monitor the link between the mobile station and the nearest High-Rate Wireless LAN Access Points.

Choosing wired or wireless
The choice for a wireless or wired High-Rate Wireless LAN administrator’s station will depend on your preferences and abilities to administer your High-Rate Wireless LAN network.

First, determine how you would like to manage your network:

- If you prefer to configure and monitor stations from on-site and to troubleshoot problems at the physical location of the station, you can choose to have a mobile, wireless High-Rate Wireless LAN administrator’s station. Use the High-Rate Wireless LAN AP Manager and High-Rate Wireless LAN Client Manager.
- If you prefer to configure and monitor stations from a central location, such as a administrator’s station, you may prefer a wired High-Rate Wireless LAN administrator’s station. Use the High-Rate Wireless LAN AP Manager.
- If you prefer to configure and monitor stations from a remote location, through a modem and calling into an RAS or PPP entry point to your network, use the High-Rate Wireless LAN AP Manager.

Your next consideration for wired or wireless station is the size of your network. In larger networks, it might 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 High-Rate Wireless LAN Access Points, a mobile, wireless station might be the most efficient way to configure and manage your network.

For wireless stations, note the following information:

- LAN administrators require easy access to wireless areas.
- You need to perform a site verification to determine optimal placement of High-Rate Wireless LAN Access Points.
- It is also possible to remotely configure and monitor an access point through a dial-up connection. This feature is only possible when the network is externally accessible.

You can assign multiple stations as High-Rate Wireless LAN administrator’s stations, enabling a combination of wired and wireless stations and giving you the freedom to choose the most appropriate tool for the situation.

Wired stations: A wired High-Rate Wireless LAN administrator’s station enables you to configure and monitor access points through a wired backbone by using the High-Rate Wireless LAN AP Manager tool.

Configuration: A wired High-Rate Wireless LAN administrator’s station has access to all High-Rate Wireless LAN Access Points through a wired backbone. The access points are identified by means of their unique IP address.

Note: When your LAN architecture is comprised of multiple subnets, separated by gateways or routers, note that the administrator’s station that you intend to use for the initial configuration must be on the same subnet as the High-Rate Wireless LAN Access Points.

When the High-Rate Wireless LAN Access Points have been configured and their IP addresses have been registered, you can use any station to access the access points through the TCP/IP protocol.

For more information on configuring your High-Rate Wireless LAN Access Point, see “Configuration scenarios” on page 1-11.

Monitoring: When you use a wired High-Rate Wireless LAN administrator’s station you will not be able to move around to different physical locations of the network to determine or optimize the placement of stations, High-Rate Wireless LAN Access Points, or antennas. However, a wired High-Rate Wireless LAN administrator’s station can use the High-Rate Wireless LAN AP Manager remote link test and remote statistics features to perform monitoring tasks.

With the High-Rate Wireless LAN AP Manager, you can validate radio frequency links between a remote High-Rate Wireless LAN Access Point and High-Rate Wireless LAN stations connected to that access point. For more information on monitoring, see “Monitoring” on page 1-8.

Wireless stations: With a wireless High-Rate Wireless LAN administrator’s station, you can use the High-Rate Wireless LAN Client Manager as well as the High-Rate Wireless LAN AP Manager.

Monitoring: You can use the following High-Rate Wireless LAN tools to monitor your infrastructure network:

- High-Rate Wireless LAN Client Manager
- PC Card diagnostics
- Logging measurements data
- Site monitor
- Link test
- High-Rate Wireless LAN AP Manager
- System information
- Remote link test
- Remote statistics

For more information on monitoring your High-Rate Wireless LAN network, see “Monitoring” on page 1-8.

Installing High-Rate Wireless LAN Software

This section provides information on installing the High-Rate Wireless LAN Client Manager and the High-Rate Wireless LAN AP Manager.

Installing the High-Rate Wireless LAN Client Manager

To install the Client Manager software, do the following:

1. Insert the High-Rate Wireless LAN software CD into the CD-ROM drive of your computer. If Autorun is enabled on your computer, the Wireless Networking Client Software window opens.

   Note: If you downloaded the software from the Web, please refer to the installation instructions found on the Web site.

2. Click **Install Client Manager**; then follow the on-screen instructions.

   Note: If Autorun is not enabled on your computer, you can start Client Manager by running the .EXE file located in the root directory of the High-Rate Wireless LAN software CD; then following the on-screen instructions.

During the installation, you will be prompted for a directory to install the High-Rate Wireless LAN program files. The default directory for the High-Rate Wireless LAN Client Manager program is C:\PROGRAM FILES\IBM\WIRELESS LAN\CLIENT MANAGER.

Installing the High-Rate Wireless LAN AP Manager

The High-Rate Wireless LAN 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:

- A network interface card (NIC) to connect this station to the network. The NIC card can be of any type, including the High-Rate Wireless LAN PC Card (for wireless stations) or an Ethernet card.
- A TCP/IP protocol stack

To install the AP Manager software, do the following:

1. Insert the High-Rate Wireless LAN software CD into the CD-ROM drive of your computer. If Autorun is enabled on your computer, the Wireless Networking Client Software window opens.

   Note: If you downloaded the software from the Web, please refer to the installation instructions found on the Web site.

2. Click **Install AP Manager**; then follow the on-screen instructions.

   Note: If Autorun is not enabled on your computer, you can start AP Manager by running the .EXE file located in the root directory of the High-Rate Wireless LAN software CD; then following the on-screen instructions.

During the installation, you will be prompted for a directory in which to install the High-Rate Wireless LAN program files. The default directory for the High-Rate Wireless LAN AP Manager program is C:\PROGRAM FILES\IBM\WIRELESS LAN\AP MANAGER.

Verifying the TCP/IP protocol settings

The High-Rate Wireless LAN AP Manager program requires a TCP/IP networking protocol to communicate with the High-Rate Wireless LAN Access Point. When setting up the access points for the first time you need to verify the TCP/IP settings of the administrator's station.

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

To verify whether the TCP/IP protocol is properly installed, do the following:

1. Click **Start** → **Settings** → **Control Panel**.
2. Double-click **Network**.
3. Verify that the list of network components includes the TCP/IP Protocol for the High-Rate Wireless LAN network interface that you want to use to access the High-Rate Wireless LAN Access Point (your Ethernet or High-Rate Wireless LAN adapter, for example).
    - If the list is correct, close all windows by clicking **Cancel**; then go to "Configuration scenarios" on page 1-11.
    - If the list is incorrect, do the following:
        a. Click **Add**.

        b. From the list of component types, select **Protocol**; then click **Add**.

        c. Select a TCP/IP protocol from the displayed list. In most network environments, the Microsoft TCP/IP protocol will work just fine. If not, select a TCP/IP protocol that matches your network operating system.

        d. If your network does not use IP addressing, select **Specify an IP Address**. This will disable the DHCP mechanism that would assign an IP address to your High-Rate Wireless LAN administrator's station automatically in networks that include a DHCP server.

        e. Enter a user-defined value in the IP Address field in the `153.69.254.`*`xxx`* *format*, where *xxx* is any numerical value in the range of 1-253.

        When configuring multiple High-Rate Wireless LAN administrator's stations, be sure to assign different values to each station.

        f. In the Subnet Mask field enter the value `255.255.255.0`

        g. Click **OK**; then follow the onscreen instructions.
4. Click **Yes** to restart your computer

When your computer has restarted, you will be ready to configure the High-Rate Wireless LAN Access Point through any of the configuration scenarios as described in "Configuration scenarios" on page 1-11.

Configuration scenarios

In the previous section you selected a wired or a wireless High-Rate Wireless LAN administrator’s station. This section describes some of the characteristics and features of each type of administrator’s station, and identifies whether further modifications to the setup of your computer or “desktop workplace” are required.

Configuring a wired LAN administrator’s station

If you are using a wired High-Rate Wireless LAN administrator’s station, you can configure High-Rate Wireless LAN Access Points through:

- A “desktop workplace” setup, connecting your computer to the Access Point through a hub
- A regular wired Ethernet connection

Select a wired High-Rate Wireless LAN administrator’s station if one of the following conditions exist:

- You prefer to manage your High-Rate Wireless LAN Access Points from a fixed central location
- The High-Rate Wireless LAN Access Points will be installed on remote locations that are accessible through TCP/IP networking

When these High-Rate Wireless LAN 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 High-Rate Wireless LAN administrator’s station (if there are no routers between your High-Rate Wireless LAN administrator’s station and the High-Rate Wireless LAN Access Point).

When you have assigned a unique IP address value to each High-Rate Wireless LAN Access Point, you will be able to access each access point from anywhere within the network by using its unique IP address.

When installing new High-Rate Wireless LAN Access Points “out-of-the-box”, configure the access points one-by-one using the “desktop workplace” scenario. You can assign a unique IP address value to each unit prior to connecting the units to the network infrastructure.

Configuring a wireless LAN administrator’s station

With a wireless High-Rate Wireless LAN administrator station, you can use the High-Rate Wireless LAN AP Manager in combination with the High-Rate Wireless LAN Client Manager tool.

Using a wireless High-Rate Wireless LAN administrator’s station, you can configure access points directly through a wireless point-to-point connection, or indirectly through a wireless point-to-point connection with another High-Rate Wireless LAN Access Point that provides access to the “target” access point through a network backbone.

In the same way in which wired networks require you to verify that all cables are connected properly to establish connection, High-Rate Wireless LAN networks require you to verify that the High-Rate Wireless LAN administrator’s station is within range of the “target” access point, and that the High-Rate Wireless LAN network interface setup matches the parameter values of the access point(s).

When using the configuration setup directly through of a wireless point-to-point connection, the High-Rate Wireless LAN network interface of the administrator’s station should be configured to match the settings of the “target” High-Rate Wireless LAN Access Point.

The direct connection scenario is most convenient when configuring multiple out-of-the-box access points sequentially.

The indirect connection scenario is most efficient when adding new High-Rate Wireless LAN Access Points to an existing network, or when you are not within range of the “target” access point.

Note: In both scenarios, the High-Rate Wireless LAN Access Points are identified by their unique IP address.

Removing High-Rate Wireless LAN software

To remove the High-Rate Wireless LAN software from a High-Rate Wireless LAN administrator’s station, do the following:

1. Click **Start** → **Settings**→ **Control Panel**.
2. Double-click **Add/Remove Programs**.
3. Select the High-Rate Wireless LAN management program that you want to remove; then click **Add/Remove**.

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

Basic network configuration

This section describes how to configure a 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 to each other without bridging data through an access point.

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 about Peer-to-Peer workgroups refer to the *High-Rate Wireless LAN PC Card Quick Start Guide*.

Infrastructure networks

This section describes how to configure infrastructure networks for most networking environments. For more advanced configuration settings, see “Advanced Network Configurations” on page 1-60.

Managing your High-Rate Wireless LAN Access Points

To manage your High-Rate Wireless LAN Access Points, you must assign a unique IP address to each access point within your network. Your High-Rate Wireless LAN management station must also have an IP address. The TCP/IP connection of your station needs to do one of the following:

- The TCP/IP connection needs to be connected to the same subnet as the High-Rate Wireless LAN Access Points, as described in “Basic infrastructure” on page 1-4.
- The TCP/IP connection needs to provide access to the subnet of the High-Rate Wireless LAN Access Points through routers, gateways or another type of LAN connection that supports the TCP/IP protocol.

Configuring infrastructure networks

This section gives instructions on basic configuration of a High-Rate Wireless LAN infrastructure network.

The following requirements must be met before configuring the 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 High-Rate Wireless LAN Access Point.
- To configure the wireless stations, follow the instructions in the *High-Rate Wireless LAN PC Card Quick Start Guide*.

To install and configure the High-Rate Wireless LAN Access Point, do the following:

Note: Repeat steps 2 to 4 for each of the access points that you wish to install.

Step 1: Installing an access point: For installation instructions of the High-Rate Wireless LAN Access Point hardware, refer to the *High-Rate Wireless LAN Access Point Quick Start Guide* included with the access point.

Step 2: Connecting to an access point: To connect to a High-Rate Wireless LAN Access Point, you need to address each access point through its IP address.

If your network includes a BOOTP or DHCP server, the IP address will be assigned automatically refer to “BOOTP and DHCP” on page 1-73 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 your first configuration.

To connect to a High-Rate Wireless LAN Access Point, do the following:

1. Start the High-Rate Wireless LAN AP Manager program.
2. Select the access point that you want to configure from the list, or enter the IP address in the **Enter the IP address for a specific Access Point** field.
   - A new access point is marked with a special icon.
   - A list will display all access points located on the same IP subnet as your High-Rate Wireless LAN management station. See modifying the configuration “Modifying the configuration” on page 1-71.

- To gain access to an access point on a different subnet or through a dial-up connection, enter a specific IP address in the field Enter the IP address for a specific Access Point.

3. Click **Edit**.

    - 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 High-Rate Wireless LAN Access Point in the field Access Point IP Address.

        b. Record the IP address on the “Configuration record” on page A-3.

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

You are now ready to change the High-Rate Wireless LAN Access Point configuration settings.

Step 3: Setting the network name and saving the configuration: When installing a High-Rate Wireless LAN network, modify the default settings of the High-Rate Wireless LAN 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 High-Rate Wireless LAN network from possible neighboring networks.

To set the network name and save your configuration, do the following:

1. Open the High-Rate Wireless LAN AP Manager.

2. Select the **Wireless Interfaces** tab.

3. Choose the slot of the High-Rate Wireless LAN Access Point (PC card Slot A or B) that contains the High-Rate Wireless LAN PC Card that you want to configure.

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

    - The High-Rate Wireless LAN 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 High-Rate Wireless LAN network name must be the same for all High-Rate Wireless LAN network interfaces that service wireless stations that belong to the network.

    - The network name distinguishes your High-Rate Wireless LAN Access Points from access points that belong to a neighboring network.

    Note: For information on other High-Rate Wireless LAN Interface parameters (like the Advanced and Security button), see “Advanced Network Configurations” on page 1-60.

5. Click **OK** to save the configuration to the Access Point and to return to the main AP Manager window.

    Note: The access point restarts automatically when you save your configuration.

Step 4: Creating a backup file of your configuration: When you change the configuration of a High-Rate Wireless LAN Access Point, create a backup file of the configuration. You can use this backup file to quickly restore a High-Rate Wireless LAN Access Point configuration in situations where:

- An access point goes out of service
- You want to recreate the original configuration of an access point that you had to replace (following a repair, for example)
- You need to perform a forced reload as described in Appendix C, “Forced reload procedure” on page C-1.

To create a backup file, do the following:

1. Open the High-Rate Wireless LAN AP Manager.
2. Select the access point you want to create a backup of.
3. 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 Configuration record, found under “Configuration record” on page A-3.

To install and configure other access points, see the *High-Rate Wireless LAN PC Card Quick Start Guide*.

Monitoring your High-Rate Wireless LAN network

When your network has been configured and installed, you can use High-Rate Wireless LAN software tools to monitor the performance of your network, and to verify optimal placement of your High-Rate Wireless LAN Access Points and wireless stations.

Verify the performance of your network on a regular basis, as performance may change when wireless stations are relocated, office environments change, 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 High-Rate Wireless LAN network:

- High-Rate Wireless LAN Client Manager
- High-Rate Wireless LAN AP Manager

For basic information on High-Rate Wireless LAN tools, see “Software description” on page 1-2.

High-Rate Wireless LAN Client Manager

High-Rate Wireless LAN Client Manager is designed to monitor the radio performance of your network on-site. You can use this program to:

- Run dynamic radio communication diagnostics with the High-Rate Wireless LAN Access Point within range of your monitoring station
- Display detailed link test measurement results with the access point nearest your High-Rate Wireless LAN Client Manager station

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

High-Rate Wireless LAN AP Manager

The High-Rate Wireless LAN AP Manager is designed to monitor your network from a central location, such as the administrator’s station.

You can use this tool to display link test measurements between a remote High-Rate Wireless LAN Access Point of your choice and a station connected to the selected access point.

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

Selecting a High-Rate Wireless LAN tool

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

Both the High-Rate Wireless LAN Client Manager and the High-Rate Wireless LAN 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.

You can also use the High-Rate Wireless LAN AP Manager program to monitor wireless performance of both wireless systems through High-Rate Wireless LAN Access Points. see “Remote Link Test window” on page 1-30.

Monitoring a network with the High-Rate Wireless LAN Client Manager

The High-Rate Wireless LAN Client Manager offers four monitoring methods:

- PC card diagnostics
- Link test
- Site monitor
- Logging measurement data

Note: The site monitor, link test and logging measurement data options are only available when the High-Rate Wireless LAN Client Manager is installed in “Advanced” mode. See “High-Rate Wireless LAN Client Manager” on page 1-2 for more information.

The Client Manager starts automatically when Windows is started. The Client Manager icon is displayed on the windows task bar. If the program is not running, do the following:

1. Click **Start** → **Programs** → **IBM Wireless LAN**
2. Click **Client Manager**.
3. Click **Client Manager** on the task bar to open the 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 High-Rate Wireless LAN network to which your station is connected (“Peer-to-Peer” in the case of a Peer-to-Peer workgroup, or the network name of your High-Rate Wireless LAN Access Point infrastructure).
- The quality of the radio connection to this network, displayed with a colored icon. The values are Excellent (green), Good (green), Marginal (yellow), Poor (red), or Out of range (red with an error sign).
- The name of the access point to which the mobile wireless computer is connected at that moment.
- The channel used for the connection.
- Encryption status (on or off)

If your High-Rate Wireless LAN Client Manager cannot establish a network connection, this screen will display one of the following:

- `No wireless network card driver present`: Your station was unable to detect an High-Rate Wireless LAN device driver in your High-Rate Wireless LAN station. Check to make sure that the card is properly inserted and that you have configured your station correctly.
- `Out of range`: You are out of range of the High-Rate Wireless LAN network for which your station has been configured.
- `Searching for initial connection to network:` *`XXX`*: The network cannot be found, where *XXX* is the name of your network.

For more detailed information use the monitoring methods as described in “Monitoring your High-Rate Wireless LAN network” on page 1-15.

From the main Client Manager window, you 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, see Appendix B, “Troubleshooting the access point” on page B-1.

Link test

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

- A High-Rate Wireless LAN Access Point, when your High-Rate Wireless LAN Client Manager station is connected to an infrastructure network. 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 might change dynamically whenever another access point provides better communications quality. See "Wireless configurations" on page 1-3 for more information on infrastructure networking.
- A High-Rate Wireless LAN station, when your High-Rate Wireless LAN Client Manager station is connected to an Peer-to-Peer workgroup. 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 High-Rate Wireless LAN network name as your High-Rate Wireless LAN Client Manager station. See "Wireless configurations" on page 1-3 for more information on Peer-to-Peer workgroups.

To start the link test, select **Link Test** in the Advanced menu of the main Client Manager window.

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

- 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)
- The quality of the connection

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

- Signal-to-noise ratio (SNR)
- Received messages

Signal-to-noise ratio (SNR): The signal-to-noise ratio identifies the communications quality of the 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 actions are necessary
Yellow	Communication quality is marginal; no actions are necessary
Red	Communication quality is poor. See Appendix B, “Troubleshooting the access point” on page B-1.

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.
- 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 helps you to identify the location where the interference occurs, and to determine whether any actions to eliminate or remedy the source interference result in a better performance.

Received messages: The Received Messages indicator provides a way to determine the efficiency of the radio path between your High-Rate Wireless LAN Client Manager station and the link test partner.

When you run a link test, your High-Rate Wireless LAN Client Manager station exchanges messages with the test partner. The test partner confirms 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 is zero.
    - When communications quality is marginal, the total number of lost messages is in the range of 1% to 3%.
    - When the total number of messages is >5% your network environment is suffering from performance problems.

In most situations, the number of lost messages increases whenever the level of SNR decreases.

The different fields for messages received at the different transmit rates (for example, 11 MBps, 5.5 MBps, 2 MBps, and 1 MBps) can 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 High-Rate Wireless LAN station retransmits the lost frame.
- If a retransmission fails repeatedly, the station switches to a lower data speed[1] and tries 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
- Network congestion. This is typically the case when the SNR is rated good.

In situations where there are a lot of retransmissions at lower data rates, the lower data speed might be the result of one of the following:

- A link test partner is almost out-of-range of your High-Rate Wireless LAN 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, use one of the following buttons:

- **Advice**: to display more detailed information related to the current link quality and to display troubleshooting hints.
- **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. Click **Reset** to analyze the link quality again, ignoring previous results that might have adversely influenced the statistics.
- **Help**: to display general information about the High-Rate Wireless LAN Client Manager link test.

  To access the online help system, you can also press F1 on your keyboard.

[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 yields the best performance results.

Test history: 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.

For example, if you have an High-Rate Wireless LAN 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: 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 1-26.

Site monitor

With the Site Monitor option, you can display the communications quality between your High-Rate Wireless LAN Client Manager station and all High-Rate Wireless LAN Access Points within the range of the station.

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

- Determine the overall wireless coverage of your High-Rate Wireless LAN network
- Verify or optimize the placement of your access points, to provide seamless roaming connectivity to mobile stations

When roaming throughout a wireless network environment with your High-Rate Wireless LAN Client Manager station, you are able to identify areas that might not have adequate coverage, or that suffer from in-band interference from other wireless equipment such as security gates, microwave ovens or photocopiers.

To start the site monitor, select **Site Monitor** in the Advanced menu in the main Client Manager window. The Site Monitor provides the following options:

- **Site Monitor** tab: the primary tab to monitor the performance of your wireless network
- **Selection** tab: enables you to scan for neighboring High-Rate Wireless LAN networks and select such networks for monitoring
- **Log Settings** tab: allows you to enable, disable, or configure the site monitor logging options
- **AP names** tab: allows you to create user-defined access point names for easy identification of High-Rate Wireless LAN Access Points in the Site Monitor window

Note: The Site Monitor option only works in combination with High-Rate Wireless LAN Access Points. When you select this option in a Peer-to-Peer workgroup environment, the Site Monitor window starts with the **Selection** tab instead of the **Site Monitor** tab.

Site Monitor tab: Displayed across the top of the **Site Monitor** tab are the following fields:

- Current Network (SSID): identifies the name of the High-Rate Wireless LAN network to which you are currently connected
- Distance between APs: describes the access point density setting of the High-Rate Wireless LAN network to which you are currently connected.

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

Also displayed in the Site Monitor window are all High-Rate Wireless LAN Access Points that belong to the same infrastructure as the one to which you are currently connected, and are within range of your High-Rate Wireless LAN Client Manager station.

In the site monitor mode, you can customize the selection of site monitor parameters. The standard selection for site survey procedures is as follows:

- AP name (access point name): to identify devices by the name of the High-Rate Wireless LAN Access Point. This name is identified either in:
  - — The System Name field of the configuration of the access point
  - — A user-defined Access Point Name List, which you can create using the High-Rate Wireless LAN Client Manager tool
- 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, arrange the site monitor display as described above; then do the following:

1. Determine which locations in your network environment require wireless connectivity.
2. Use a mobile computing device to walk through your wireless LAN environment.
3. Roaming throughout the network environment, verify that each location is covered by at least one High-Rate Wireless LAN Access Point that provides a level of SNR that is at least “Marginal” (Yellow) or better.
4. (Optional) Click **Sort on** 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.
5. (Optional) To sort access points in a different way, simply select another display item in column one.

Customizing the Site Monitor display: You might want to select one or more of the other parameters, as well. For example:

- To display the signal level and noise level to determine the cause of a poor level of SNR
  - A low signal level indicates a weak radio signal.
  - A high noise level indicates a source of interference in the radio path between your High-Rate Wireless LAN Client Manager station and the access point.

    The SNR, signal level, and noise level are displayed as dynamic indicators or as numerical values in dBm.
- To display the MAC address of the wireless cards in the High-Rate Wireless LAN Access Point. This option is useful if:
  - You are building an access point name list as described in “AP Names tab” on page 1-25
  - Your network includes access points that are equipped with multiple High-Rate Wireless LAN PC Cards, and you want to distinguish the cards

Selection tab: WIth the **Selection** tab, you can select another High-Rate Wireless LAN network. This is helpful in situations where you want to:

- Verify the presence of neighboring High-Rate Wireless LAN networks
- Determine whether such network might interfere with your High-Rate Wireless LAN network

The High-Rate Wireless LAN Access Points that are displayed when you start the site monitor tool is determined by the configuration of the High-Rate Wireless LAN network name parameter on your High-Rate Wireless LAN Client Manager station (Edit/Add Configuration Profile in the Actions menu of the main Client Manager window). For example, when the High-Rate Wireless LAN network name of your High-Rate Wireless LAN Client Manager station is set to:

- A specific High-Rate Wireless LAN network name: The station will:
  - only connect to an infrastructure network identified by the same High-Rate Wireless LAN network name when the station is turned on
  - display only the access points belonging to that network that are within range of your High-Rate Wireless LAN Client Manager station
- “ANY” network: The monitoring station will:
  - connect to the first open network it detects when the station is turned on
  - display all access points belonging to that network that are within range of your High-Rate Wireless LAN Client Manager station
- Peer-to-Peer workgroup:
  - a workgroup is created between stations with the Peer-to-Peer setting.

Selecting another wireless network: To select another wireless network, do the following:

1. Click the **Selection** tab on the Site Monitor window.

   The list of Observed Networks on this tab will show:

   - All networks that are operational within the range of your High-Rate Wireless LAN Client Manager station
   - The type of network:
     - 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 **Scan Now** 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[2]

Note: For reasons of security, the site monitor will not display the High-Rate Wireless LAN network name, 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.

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

- Your High-Rate Wireless LAN Client Manager station has been configured with a specific High-Rate Wireless LAN Network Name
- With this setting, you cannot scan for/monitor other network infrastructures. To do so, you will need to reconfigure your station to use the High-Rate Wireless LAN Network Name “ANY”
- There are no other working networks near your High-Rate Wireless LAN Client Manager station
- The neighboring networks have been closed to deny wireless High-Rate Wireless LAN compliant devices, and to establish a radio connection when these devices have been configured with:
  - The High-Rate Wireless LAN network name “ANY”
  - A zero-string SSID (the equivalent of the High-Rate Wireless LAN network name “ANY”)

For more information about “open” and “closed” networks, see “Securing your High-Rate Wireless LAN network” on page 1-46.

[2] Although the **Site Monitor Selection** tab will enable you to determine the presence of a neighboring Independent (Ad-Hoc) network, you cannot select this type of network for Site Monitor statistics. This feature requires the presence of High-Rate Wireless LAN Access Points, which are typically not available in independent networks.

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 1-26.

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 High-Rate Wireless LAN network interface(s) of your access points.

The AP name field in the Site Monitor window displays the value of the System Name parameter that has been assigned to the access point upon configuration.[3] To display this name your computer must first establish true data connections with such access points. This means your computer did not yet walk around or use the **AP Names** tab.

When you are running the High-Rate Wireless LAN Client Manager tool in site monitor mode, you can use the **AP Names** tab to assign an access point name immediately to any access point MAC address that you spot.

When you spot an High-Rate Wireless LAN Access Point identified as “unknown” do the following:

1. Click the **AP Names** tab.
2. Enter a MAC address, or double-click one of the **MAC addresses** in the list.
3. In the Access Point Name field, enter a name that allows for easy identification of this access point.
4. Click **Add to Table** to associate the name with this MAC address.
5. Repeat steps 2 through 4 for all other MAC addresses.
6. When you are finished, click the **Site Monitor** tab to continue the site monitor survey.

When walking throughout the wireless networking environment, you might see new MAC addresses appear when approaching other access points. If that is the case, repeat the steps 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 a file with other LAN Administrators that use the High-Rate Wireless LAN Client Manager tool to monitor performance of the wireless network. This file (APLIST.TXT) is stored in C:\PRGRAM FILES\IBM\WIRELESS LAN\CLIENT MANAGER.
- Edit the names later on, using an ASCII editor such as Notepad

[3] To assign a system name to an High-Rate Wireless LAN Access Point, you will need the High-Rate Wireless LAN AP Manager program specify this name in the SNMP Parameters window.

Logging measurement data

With both link test and site monitor, you can log measurement results. The measurement data can be manually or automatically logged at regular intervals.

The High-Rate Wireless LAN 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 might be helpful to gauge the performance of your wireless LAN over a period of time.

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

Logging data manually: With the manual data logging function, you can view the measurement data at a specific moment (for example, when you are running the site monitor to perform a site survey, or when you are investigating a particular source of interference).

When you choose the manual mode, you can enable the Add comments to log option to add comments to your logging information. If you enable this option, a window opens every time you press the Log Once button.

The manual data logging option is typically used on High-Rate Wireless LAN Client Manager stations roaming the network running site monitor.

Logging data automatically: The automatic data logging function allows you to log the network performance automatically at preset intervals. This is useful in situations where you want to monitor recurring events or variation in values over a long period of time.

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

Automatic data logging is typically used when the High-Rate Wireless LAN Client Manager station is running a link test at a particular location.

Setting the logging options: To set the logging options, do the following:

1. Click the **Log Settings** tab in the Link Test window or in the Site Monitor window.
2. Enter a filename for your log file in the field Log Filename.

    - IF you enter a new filename, a new file is created.
    - If you enter the same filename or use the default filename, the data will be appended.

3. Select the mode of logging to one of the following:
   - Data logging off: No data is logged
   - Manual data logging: Manually records your log measurements.
   - Automatic data logging: Automatically logs data at user-defined intervals.
   - Continuous data logging (only available in the Link Test window): Automatically logs data in the following intervals:
     - — Once per second
     - — Once per minute

In each mode, 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 want to save the data in a new file, enter a new filename in the Log Filename field

Starting and stopping the logging function: Depending on your choice of logging option, the logging button will read `Log Once` for manual logging, or `Start Log` for automatic logging).

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

Diagnosing the PC Card

If you suspect that your High-Rate Wireless LAN PC Card is not functioning properly, select **Diagnostics** in the Advanced menu of the main Client Manager window to explore the functionality of the hardware and software of the card.

In the Diagnose Card window, you can check the software and firmware information, configuration information, and communication statistics.

To test the High-Rate Wireless LAN PC Card, click the **Card Check** tab in the Diagnose Card window; then click **Test Card Now**.

Attention: Running the card diagnostics disrupts the normal operation of your High-Rate Wireless LAN PC Card, which can result in a temporary loss of your connection to the network.

If the High-Rate Wireless LAN PC Card passes all tests, the test status displays `OK` in all fields, and the Error Code field remains blank. If an error occurs, click **Advice** for more information on how to handle the error.

Troubleshooting Site Monitor

When the Site Monitor does not display all of the High-Rate Wireless LAN Access Points that you expected, this can be for one or more of the following reasons:

- Your High-Rate Wireless LAN Client Manager station is out-of-range of the access points that you want to monitor. Typically, the values for signal level and SNR are zero in this situation.

- There is a configuration mismatch of your High-Rate Wireless LAN Client Manager station. For example:
    - Your High-Rate Wireless LAN Client Manager station uses a specific High-Rate Wireless LAN network name that does not match the name of the infrastructure that you want to monitor.
    - Your High-Rate Wireless LAN Client Manager station uses the High-Rate Wireless LAN network name “ANY”, and when it was turned on, the station connected to an access point of a neighboring network instead, because that access point provided the best level of SNR.
- The infrastructure that you want to monitor has been closed to wireless IEEE 802.11-compliant devices that attempt to establish a radio connection using:
    - The High-Rate Wireless LAN network name “ANY”
    - A zero-string SSID (the equivalent of the High-Rate Wireless LAN network name “ANY”)

When your High-Rate Wireless LAN Client Manager station uses the High-Rate Wireless LAN network name “ANY”, you can use the **Selection** tab to select another network name. See “Selection tab” on page 1-23 for more information.

For more information on "open" and "closed" infrastructure networks, see “Securing your High-Rate Wireless LAN network” on page 1-46.

Using the High-Rate Wireless LAN AP Manager

You can use the High-Rate Wireless LAN AP Manager to:

- Display a standard set of SNMP variables to monitor general LAN traffic performance in your network
- Display remote link test measurements between a remote High-Rate Wireless LAN Access Point and a wireless station connected to the selected access point

The High-Rate Wireless LAN AP Manager is designed to monitor your network from a central location (for example, the administrator’s station), enabling you to monitor wireless performance in areas that cannot easily be reached (for example, wireless networks in remote locations).

Monitoring options

The High-Rate Wireless LAN AP Manager program offers a variety of diagnostic options:

- System information
- Remote link test
- Remote statistics

All other diagnostic options are standard SNMP tallies that are not described in this manual, but are documented in the online help information of your High-Rate Wireless LAN AP Manager program. Press F1 or click **Help** in your AP Manager window.

Monitoring an access point

To monitor a High-Rate Wireless LAN Access Point, do the following:

1. Start the High-Rate Wireless LAN AP Manager program.
2. Select the target access point form the local list, or enter the IP address of the access point that you want to monitor.

   You can also 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 High-Rate Wireless LAN 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. The monitor mode of the AP Manager window opens.

You can now monitor your network.

System information

The system information verifies the version level of the embedded software that is loaded into the High-Rate Wireless LAN Access Point.

To display the system information for an access point, you must first connect to the target access point. See "Monitoring an access point" on page 1-29.

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

- The Name, Location, and Contact fields represent the values that have been entered in the corresponding fields of the **SNMP** tab in the edit mode when the access point was configured.
- 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 might have been reset manually or rebooted automatically.
- The Services and Object ID fields do not display relevant information to end-users. You need these values only when contacting High-Rate Wireless LAN Technical support to report a problem.

  Providing this information to your High-Rate Wireless LAN Technical support representative can help to solve the problem.

  To provide this information, do one of the following:

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

  — Press ALT + Print Scrn to copy the contents of this screen to the Windows clipboard. Paste the screen capture into the e-mail that you will send to your authorized reseller.

- In the Description field, you can quickly determine whether a High-Rate Wireless LAN Access Point is running with the latest embedded software, or if the access point requires an upgrade to support all the required High-Rate Wireless LAN functions.

  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, in the format V*X.xx*, where *X.xx* represents the software version. To support access point services for High-Rate WIreless LAN PC Cards, you must have version 3.57 or higher.

  — The unique serial number of the access point, in the format SN-*xx*UT*xxxxxxxx*, where each *x* represents a number in the serial number.

  — The version of the access point software in the processor module of the access point, in the format V*X.xx*, where *X.xx* represents the version number of the software.

  When reporting a problem to your High-Rate Wireless LAN Technical support representative, you must include a completed High-Rate Wireless LAN problem report form. You can find this form in ASCII text format (REPORT.TXT) on the High-Rate Wireless LAN Access Point software diskettes and the IBM High-Rate Wireless LAN Web site at

  http://www.ibm.com/pc/

  Software updates are usually released through the High-Rate Wireless LAN Web site, with new releases of the software diskettes. Visit the High-Rate Wireless LAN Web site at regular intervals to find out whether newer software is available for your access points.

Remote Link Test window

In the High-Rate Wireless LAN AP Manager Remote Link Test window, you can investigate the radio link between an 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 High-Rate Wireless LAN Access Points.

The High-Rate Wireless LAN AP Manager Remote Link Test window is similar to the Link Test window of the High-Rate Wireless LAN Client Manager.

Starting the remote link test: To display the remote statistics for a High-Rate Wireless LAN Access Point, you must connect to the target access point as described in "Monitoring an access point" on page 1-29; then do the following:

1. Click the **System** tab; then click **Link Test** to open the Select a remote Link Partner for *xxx.xx.xxx.xxx*, where *xxx.xx.xxx.xxx* represents the IP address of the access point.

   The fields in the top section of this window identify the initiator station you selected when connecting to the High-Rate Wireless LAN Access Point.

   The middle section of the window displays all wireless devices connected to the initiator station. The following fields are visible:

   - The Station Name and Address fields identify the High-Rate Wireless LAN devices.

     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 High-Rate Wireless LAN PC Card has been inserted.

     — 2 = PC Card slot A

     — 3 = PC Card slot B

   - The Radio Type field identifies the type of High-Rate Wireless LAN PC Card in the corresponding slots.

2. (Optional) To refresh the list, click **Refresh**.

3. Select a station from the list; then click **Link Test** to open the Remote Link Test window.

   Note: Subject to the Radio Type of the High-Rate Wireless LAN network interface that you selected, the layout of the Remote Link Test windows might differ.

Important indicators to monitor: The Signal to Noise Ratio (SNR) identifies the communications quality of radio path between the initiator station (the High-Rate Wireless LAN Access Point) and the remote link test partner.

The color of SNR indicator, as well of the link quality and remote levels indicators, relates to the following levels of communications quality. See "Signal-to-noise ratio (SNR)" on page 1-18 for details on SNR indicators.

For more information about the Remote Link Test window, see the High-Rate Wireless LAN AP Manager online help information by pressing F1 or by clicking **Help**.

Remote Statistics window

In the remote statistics window, you can monitor a set of SNMP variables for each of the High-Rate Wireless LAN Access Point interfaces (both Ethernet and wireless).

Starting remote statistics: To display remote statistics for a High-Rate Wireless LAN Access Point, you must first connect to the target access point as described in "Monitoring an access point" on page 1-29; then click the **Remote** tab from the Monitor Access Point window. The performance for each of the interfaces of the selected access point is displayed. Select the interface of your choice from the pull down menu.

Important indicators to monitor: The High-Rate Wireless LAN AP Manager **Remote statistics** tab displays a wide range of variables that provide information about the performance of the selected access point.

The indicator that provides 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 for the three ratios.

Ratio errors to Bridge packets	**Conclusion**
0.1% or less	Performance is good. No action is necessary.
0.1% to 1%	Performance is acceptable. See “Optimizing performance” on page 1-33.
1% to 2%	Performance is poor. There might be a problem with network cabling or connections. See “Optimizing performance” on page 1-33.
2% or more	Performance is very poor. Your network might face severe performance problems. See “Optimizing performance” on page 1-33.

System intervals

To display the system interval parameters to monitor a High-Rate Wireless LAN Access Point, you must first connect to the target access point as described in “Monitoring an access point” on page 1-29.

Click the **System** tab; then click **Options** to open the 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 the 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 continuously collect measurement results, the selected High-Rate Wireless LAN Access Point (initiator station) will transfer the results to the LAN administrator’s station at regular intervals, which can vary from one to 15 seconds.

- Use a short time interval for online monitoring (for example, when troubleshooting, or when you have full bandwidth access through the local network).
- Use a longer time interval when you run a remote link test only for background information purposes, or when you access the initiator stations network through a low-speed connection, such as a dial-up modem connection.

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

- Use a short interval when you want to monitor remote statistics online (for example, for troubleshooting, or when you have full bandwidth access to the High-Rate Wireless LAN Access Point through the local network).
- Use a long interval when you run remote statistics only for background display purposes, in cases when you access the network of the selected access point through a low-speed connection, such as a dial-up modem connection.

Optimizing performance

A combination of factors usually determines Wireless LAN performance. This section presents a number of considerations that might help you to:

- Determine causes of poor Wireless LAN performance
- Provide remedies for poor Wireless LAN performance
- Tailor your High-Rate Wireless LAN network for optimal performance

Look for ways to optimize network performance in the following situations:

- Troubleshooting a suspected problem
- Wireless LAN performance is less then expected
- Routine checks show a performance degradation

This section provides solutions to some of the most commonly reported High-Rate Wireless LAN problems. The degree of benefit in these solutions largely depends on the actual conditions for your LAN.

Attention: This section describes changing Wireless LAN configurations. Before you change any configuration, create separate backup files of the configuration data for each High-Rate Wireless LAN Access Point. Backups will allow you to restore the initial setup.

Eliminating traffic

Data transmitted over a network can be divided in two types:

- True data: Data communicated between network stations, such as file-transfer or e-mail. True data, also called “payload”, includes retransmitted messages for a collision, malfunctioning cable connection, or poor radio link.

  In the High-Rate Wireless LAN AP Manager **Remote** tab, True data is displayed as Unicast Packets.

- Network overhead data: Data exchanged between network services to control the dataflow. Overhead data, also called “traffic load”, includes protocol and broadcast messages, and configuration error messages.

  In the High-Rate Wireless LAN AP Manager **Remote** tab, Network Overhead Data is displayed as Non-Unicast Packets.

The ratio of network overhead to true data differs from one networking service to another. When the ratio of network overhead is more than actually required, this might affect the performance of your wireless LAN, because the true data has to share the bandwidth capacity with the network overhead.

Eliminating redundant traffic can significantly improve the performance of your network. Following are some options from the High-Rate Wireless LAN AP Manager:

- Protocol filtering: Eliminating unnecessary protocols to wireless stations
- Optimizing wired connections: Eliminating redundant error messages
- Optimizing wireless connections: Avoiding retransmission of lost or collided frames

Protocol filtering

Some network protocols send large volumes of protocol broadcasts to all stations. Not all protocols might be required by your wireless stations. Using protocol filters can prevent the transmission of unnecessary data, saving more bandwidth for the communication of true data.

Assessing the need for protocol filtering

To determine if too many protocol broadcasts degrade the performance of a wireless network, use the **Remote Statistics** tab of the High-Rate Wireless LAN AP Manager. For more information on the **Remote Statistics** tab, see “Remote Statistics window” on page 1-31; then do the following:

1. Start the High-Rate Wireless LAN AP Manager; then click **Monitor**.
2. From the Monitor menu, select **Remote Statistics**.
3. Click the **Remote** tab to display the High-Rate Wireless LAN interface statistics.

4. Compare the number in the Out collisions field with the number in the Bridge out packets field.

   - If Out collisions is less than 1% of Bridge out packets, the wireless network is performing fine. Protocol filtering is optional.

   - If Out collisions is more than 1% of Bridge out packets, the wireless network is very busy.

     If the wireless network is busy, and you do not see many users on the network, protocol filtering might improve network performance.

5. Compare the number of Unicast packets out to the number of Non-Unicast packets out.

   - A high number of Non-Unicast packets out relative to the number of Unicast packets out might indicate a large amount of network traffic. You do not need to filter the protocols, but it might be worth investigating whether protocol filtering might improve network performance.

Note: Identifying and deciding which protocols can be filtered without affecting the proper operation of your network operating system might require advanced networking expertise.

Filtering network protocols: To filter out unnecessary or unwanted network protocols, do the following:

1. Know what type of network stations and services are on the High-Rate Wireless LAN environment of your network.

2. Use the documentation that came with your network operating system to determine which protocols are required for the equipment on your network.

3. Start the High-Rate Wireless LAN AP Manager program.

4. Select an access point; then click **Edit**.

5. Click the **Bridge** tab to display the protocol filtering information.

6. On the top-right side of the protocol filtering section, click **Edit** to open the Protocols to Filter window. Look for all protocols that you wish to filter.

7. To add a new protocol to the list, click **Custom** to enter the protocol manually.

8. Click **OK** to return to the **Bridge** tab. All of the protocols that you have selected or added manually will be listed in the Protocol Filtering field.

9. Click **OK** again to save the changes to the access point and to return to the main window of the High-Rate Wireless LAN AP Manager.

10. Download a backup file. See “Step 4: Creating a backup file of your configuration” on page 1-15 for further information.

    When you are prompted to enter a name for the back-up file, select a name that is different from the original configuration file. Do not overwrite the original backup file. Keep your ability to restore the original configuration if your changes did not result in a performance increase.

Repeat the steps under "Assessing the need for protocol filtering" on page 1-34 to see the results of your changes. If problems continue, consider one of the following options:

- Optimizing wired connections
- Optimizing wireless connections

Optimizing wired connections

Sometimes a failure in the cabling system that connects the High-Rate Wireless LAN network to the wired infrastructure causes a performance degradation. The following are symptoms of cable failure:

- The system does not work at all
- The network generates a high volume of error messages, resulting in slowed network performance

The following are examples of cabling system failures:

- A faulty cable or connector in the wired infrastructure
- A LAN segment might be too long

Checking the cables: The cabling system can be diagnosed with the remote statistics found on the **Remote** tab in the monitor mode of the High-Rate Wireless LAN AP Manager. To diagnose cabling problems, do the following:

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 number of Bridge in packets, this might 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 number of Bridge out packets, this might indicate 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 numbers of 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. Verify that the problem occurs only with the selected High-Rate Wireless LAN Access Point or with multiple access points.

   If the problem is observed on only one access point, the problem might be with the connectors or cables that connect the access point to the hub or wired backbone.

   If 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.

To resolve a cabling problem, carefully check the cabling system in these areas to verify whether all connectors are properly seated:

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

For BNC coaxial cable (10BASE2), make sure that terminators are placed on both ends.

Checking the length of LAN segments: In exceptional cases, networking problems might 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.

Use the remote statistics found on the **Remote** tab in the monitor mode of the High-Rate Wireless LAN AP Manager to determine if A LAN segment is too long:

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. If the number of In errors is 1% of the Bridge in packets or more, there might be a cabling problem.
3. Monitor the value increase of the Bytes in parameter over a longer period of time. If this number constantly displays more than 600,000 bytes per second, this might indicate a problem with the length of the LAN segment.

Always consult a network expert to verify or adjust the length of cable segments.

Note: If you decide to split the LAN segment into multiple sub-segments, group all High-Rate Wireless LAN-equipped devices into the same LAN segment. High-Rate Wireless LAN stations will not be able to roam between LAN segments that are separated by routers or gateways.

If checking and adjusting the length of LAN segments does not solve your problem, consider one of the following options:

- Protocol filtering (see page 1-34)
- Optimizing wireless connections

Optimizing wireless connections

When the link quality between a wireless station and its High-Rate Wireless LAN Access Point is poor, packets communicated between this station and the access point might get lost. Stations and access points will simply resend information, resulting in unnecessarily increased traffic.

Many retransmissions might affect data transmission efficiency. The true data must share the wireless bandwidth with the retransmitted frames. Retransmissions also degrade the performance of the network as perceived by the wireless station user. For example, saving a file will take longer if many retransmissions are required.

One or more of the following can cause poor link quality:

- The station is almost out of range of the access point.
- A source of interference is in the signal path between the station and the access point.
- A station might be “hidden” from another station within the same coverage area. For more information on hidden stations, see “RTS/CTS protocol” on page 1-41.

Diagnosing link quality: The link quality on the wireless network can be diagnosed with the following tools. Use the High-Rate Wireless LAN AP Manager to:

- Diagnose the quality of radio communications
- Investigate on-site whether a specific remote area is suffering from poor radio performance.

  The High-Rate Wireless LAN AP Manager provides the following tools to diagnose radio link quality:

  — Remote link test

  — IEEE information

  — Remote statistics

These readings can be usefulto determine if the performance of your High-Rate Wireless LAN network is caused by interference.

Remote link test: For instructions about the Remote Link Test window that displays communications indicators, see “Remote Link Test window” on page 1-30.

Use the following indicators to monitor in the Remote Link Test window:

- 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 (if 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 High-Rate Wireless LAN Access Point.

Pay attention to the following indicators:

- 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, a source of interference might be present. Use the Remote Link Test window to look for high noise figures or low SNR values, to find the cause of the interference.

Remote statistics: To diagnose link quality using the **Remote** tab, do the following:

1. Click the **Remote** tab in the monitor mode.
2. Select one of the interfaces from the pull-down menu to display the statistics for the High-Rate Wireless LAN wireless network interfaces; then use the following to diagnose link quality:
   - Compare the number of In errors with the number of Bridge in packets.

     If the number of In errors is 1% or more of the Bridge in packets, this might indicate that the wireless medium is very busy.
   - Compare the number of packets Out errors with the number of Bridge out packets.

     If the number of Out errors is 1% or more of the Bridge out packets, one or more stations might have poor link quality.
   - Compare the number of packets in the Out collisions field 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. Possible reasons for this include many retransmitted frames, and many stations communicating at the same time.
3. Use the AP Manager remote link test to analyze whether one or more stations show a poor link quality.
   - A low signal level indicates that the station is almost out of range of the access point.
   - A high noise level indicates a source of interference in the signal path between the station and the access point.
4. If a station shows a poor link quality, retransmissions of frames will disturb overall statistics and performance. You can solve the problem by moving the stations or eliminating the source of interference.
5. If the problem is a poor signal, consider the following:
   - Connect a High-Rate Wireless LAN Range Extender Antenna to the station or access point that has poor radio performance.
   - Add an extra access point to the network.
   - Adjust the placement of your access points or antennas to provide coverage for all wireless stations.

   The network may have "hidden stations." For more information on hidden stations, see “Hidden stations” on page 1-41.

Note: You can also use the High-Rate Wireless LAN Client Manager to analyze the link quality between a remote station and the access point. You must have access to the problem location to perform on-site diagnostics.

If the problem recurs, consider one of the following options:

- Protocol filtering (see page 1-34)
- Optimizing wired connections (see page 1-36)

Protocols

In most networks, two types of protocols are used:

- Carrier sense multiple access/collision advance (CSMA/CA)
- Request to send/clear to send (RTS/CTS)

CSMA/CA and RTS/CTS. The following sections describe each of the protocols and the conditions in which each is used.

CSMA/CA protocol: In normal High-Rate Wireless LAN network configurations, all equipped devices apply a standard protocol to avoid collision of wireless messages. When a station intends to transmit a message, it will first detect if no other station is already transmitting (using the wireless medium). If no other transmissions are detected, the High-Rate Wireless LAN station will start its transmission. If the station does detect another transmission carrier, the High-Rate Wireless LAN station will apply a random defer timer. After the timer has expired, the station will detect the medium again to see if transmitting is properly working.

This protocol works fine in most networking environments. The user of a wireless computing device will probably not notice the deferral behavior of the wireless radio.

In network environments where many wireless users are close to one another, or wireless stations must carry heavy data traffic, the network might show a degradation in performance. This degradation in performance will be evident as long network response times.

Poor performance can typically be caused by poor radio link quality. Radio link quality is measured as the signal to noise ratio, SNR. Further evidence of poor link quality might consist of the following:

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

In this situation, the CSMA/CA protocol itself might be the source of the problems. Busy wireless traffic in the area can cause the CSMA/CA protocol to defer transmissions too often for either:

- Heavy data traffic by other stations in the same wireless cell
- Traffic from stations in neighboring cells in a location where wireless cells overlap one another

The last example usually occurs only in networks where all access points have been configured to operate at the same frequency, or at frequencies with an insufficient channel separation. You will need to change the frequency of some of these stations to improve network performance. See “Frequency channel management” on page 1-42.

The CSMA/CA protocol has the following drawbacks:

- The protocol fails due to hidden stations.
- The protocol fails when the density of High-Rate Wireless LAN stations and access points is very low.
- The protocol fails with excessive frame collisions at the access point.

RTS/CTS protocol: The Request to Send/Clear to Send protocol (RTS/CTS) provides some benefits over CSMA/CA. The RTS/CTS medium reservation mechanism provides enhanced wireless network performance, and solves the problem of hidden stations.

Hidden stations: A "hidden station" occurs when two wireless stations are within range of the same access point, but are not within range of each other. Troubleshooting a hidden station problem provides the best results when performed from the suspected station. When the wireless stations send messages at the same time, they might collide when arriving simultaneously at the access point. The collision results in a loss of messages for both stations. RTS/CTS medium reservation will prevent message collisions by handing over transmission control to the access point.

The RTS/CTS Medium Reservation can be set on individual stations, that is, the setting of this parameter does not have to be the same for all High-Rate Wireless LAN equipped devices in your network. To enable the High-Rate Wireless LAN PC Card parameters of an individual station, start the High-Rate Wireless LAN Client Manager; then select **Add/Edit configuration profile**. Click the **Advanced** tab; then click **RTS/CTS Medium Reservation**.

Enabling RTS/CTS on hidden stations: When you enable the RTS/CTS protocol on a suspect hidden station, the following occurs:

- The station will send an RTS to the access point, which will include information about the length of the frame that the station would like to transmit.
- 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 requesting station that the access point has checked the medium for availability, and has reserved it for the time-frame of the requested transmission.

Note: RTS/CTS requires the access point to ask for a CTS for every message that it sends, even if it is forwarding traffic between stations that belong to the same wireless cell. Using RTS/CTS when using CSMA/CA is sufficient might cause increased network overhead, negatively affecting network performance.

Enabling RTS/CTS for access points: RTS/CTS medium reservation configuration for access points is slightly different from that of stations. With the RTS/CTS configuration for access points, you can customize the sensitivity of the RTS/CTS mechanism and determine when RTS/CTS controls data flow. To customize when RTS/CTS works, do the following:

1. In the edit mode, click the **Interface** tab; then click **Advanced**.
2. Enter a frame length value in the **RTS/CTS Medium Reservation Threshold** field.

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, but uses the CSMA/CA protocol.
- When the length of a message exceeds the RTS/CTS medium reservation threshold, the access point first sends an RTS to the station. The access point will 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.

To enable RTS/CTS for access points, do the following:

1. Start the High-Rate Wireless LAN AP Manager program
2. Select the access point that services the wireless cell where you suspect poor performance is caused by a hidden station problem; then click **Edit**.
3. Click the **Wireless Interfaces** tab.
4. Choose the socket that contains the High-Rate Wireless LAN network interface that suffers from a hidden station.
5. Click **Advanced**.
6. Click the check box next to **RTS/CTS Medium Reservation**.
7. 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. You can enter any value you like.

   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 High-Rate Wireless LAN Access Point will 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.
8. Click **OK** to return to the **Interface** tab.
9. Click **OK** again to save the new configuration to the access point and to return to the main AP Manager window.
10. Create a backup file of the new configuration using instructions in “Step 4: Creating a backup file of your configuration” on page 1-15.

Frequency channel management

When your network consists of more than one High-Rate Wireless LAN Access Point, you must alternate 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 High-Rate Wireless LAN PC Card *User’s Guide*.

Dual channel configuration: Apply a maximum channel separation for neighboring access points so that one station uses a particular channel to communicate with an access point without interfering with the transmissions of another station. When either one of the stations roams to another location, the station will automatically switch its radio to any other operating channel required to maintain the network connection.

Multiple channel configuration: Alternating the frequency channels of your High-Rate Wireless LAN Access Points between three or more channels, is called multiple-channel configuration. This configuration complies with the minimum channel separation (25 MHz) 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.

When your access point is equipped with two High-Rate Wireless LAN PC Cards or the High-Rate Wireless LAN PC Card supports multiple sub-channels, you must use two different frequency channels, with the maximum channel separation, to avoid as much channel cross-talk as possible.

Configuring channel frequency: To change the frequency of your High-Rate Wireless LAN Access Point, do the following:

1. Connect to an access point by opening the High-Rate Wireless LAN AP Manager.
2. Select the target access point; then click **Edit**.
3. Select the **Wireless Interfaces** tab.
4. Choose the socket (A or B) for the High-Rate Wireless LAN network interface that you would like to configure.
5. Click **Advanced**.
    - If the High-Rate Wireless LAN PC Card supports multiple sub-channels, you can select a different operation frequency from a pull-down menu.
    - If the High-Rate Wireless LAN PC Card supports only a single frequency, a window opens stating that you have selected a Fixed Frequency Card that cannot be changed.
6. In the Wireless Advanced Setup window, select a sub-channel from the **Channel** pull-down menu. Select a sub-channel that is most separated from neighboring access points (with a minimum channel separation of 25 MHz).

    The following table lists channel combinations to configure a network with multiple access points.

    - For dual channel configuration, alternate between channels A and B.
    - For three-channel configurations, alternate between channels A, B and C

Channel A	Channel B	Channel C
2412 MHz (1)	2472 MHz (13)	2442 MHz (7)
2417 MHz (2)	2472 MHz (13)	2442 MHz (7)
2422 MHz (3)	2472 MHz (13)	2447 MHz (8)
2427 MHz (4)	2472 MHz (13)	n/a
2432 MHz (5)	2472 MHz (13)	n/a
2437 MHz (6)	2472 MHz (13)	2412 MHz (1)
2442 MHz (7)	2412 MHz (1)	2472 MHz (13)
2447 MHz (8)	2412 MHz (1)	2472 MHz 13()
2452 MHz (9)	2412 MHz (1)	n/a
2457 MHz (10)	2412 MHz (1)	n/a
2462 MHz (11)	2412 MHz (1)	2437 MHz (6)
2467 MHz (12)	2412 MHz (1)	2442 MHz (7)
2472 MHz (13)	2412 MHz (1)	2442 MHz (7)

Note: The availability of channels listed in the table is subject to local radio regulations in your country. A complete list of supported channels for your country can be found in the online High-Rate Wireless LAN PC Card *User's Guide*.

7. Click **OK** to close the Wireless Advanced Setup window and return to the **Wireless Interfaces** tab.
8. (Optional) Repeat steps 4-7 to verify or change the frequency for the second High-Rate Wireless LAN network interface in this access point.
9. Click **OK** again to save the new configuration to the Access Point and to return to the main AP Manager window.
10. Create a backup-file of the new configuration. See "Step 4: Creating a backup file of your configuration" on page 1-15 for more information on creating backup files.
11. Update the Configuration record, found under "Configuration record" on page A-3.
12. (Optional) Modify the configurations of all your other access points accordingly. Use different frequencies for neighboring access points, as described in "Dual channel configuration" on page 1-43, or "Multiple channel configuration" on page 1-43.

Link integrity

Where the High-Rate Wireless LAN Access Point connection 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.

Note: Only use this feature if your network provides duplicate Ethernet connections.

If the wireless connection is still intact, the wireless station will not roam to another access point, since the radio will interpret its physical connection to the access point as at least acceptable.

The Ethernet link integrity feature is a high-end solution that enables you to resolve network failures. The Ethernet link integrity feature 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

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

Optimizing network capacity

In networking environments where you have data intensive users or a large number of users in a small area, you might want to improve the throughput efficiency or load balancing of your High-Rate Wireless LAN Access Points. This section describes how to balance maximum range for a minimum amount of hardware investments versus maximum throughput performance for a higher amount of hardware investment.

Changing deferral behavior

You can design a high performance network based on the following principles:

- Adding more High-Rate Wireless LAN Access Points to your network
- Configuring access points in neighboring cells to operate at different frequency channels with a maximum channel separation. See “Configuring channel frequency” on page 1-43.
- Adjusting the Distance Between APs parameter to optimize the load balance of the number of wireless stations per access point. See “Distance between access points” on page 1-62

Attention: The Distance Between APs parameter must be set on both the wireless stations and the High-Rate Wireless LAN Access Point. The values that you select must be the same for all High-Rate Wireless LAN equipped devices in your network. If you do not set the same distance value for all devices, the roaming quality of wireless devices will not function properly.

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

- The High-Rate Wireless LAN stations will show a more active roaming behavior and connect to one of the added access points more quickly.

- Adding more access points means the deferral behavior no longer needs to be as strict in environments where the density of access points was fairly low:
  - 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 High-Rate Wireless LAN Access Point that services the local cell, since the more active roaming behavior normally causes 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 corresponds with the actual density in placement of the access points.

When the Distance Between APs parameter is set to Large, the receiver sensitivity causes the wireless radio device to defer transmissions for all messages that it senses within its range.

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.

Changing the Distance Between APs parameter virtually reduces the range of the wireless cell by applying different levels of receiver sensitivity.

With the Distance Between APs parameter set to Medium or Small, 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 reduced virtual range. Messages with a lower signal level are considered to be traffic belonging to another cell, so will be ignored. Roaming stations will connect to another access point as soon as they leave the area belonging to a specific access point.

Securing your High-Rate Wireless LAN network

This chapter provides information IBM High-Rate Wireless LAN security options.

A distinct advantage of the IEEE 802.11 standard for wireless networks is that it provides a quick and convenient way to connect a 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. Access to the network is controlled via standard security mechanisms, such as user names and passwords.

The drawback of quick and easy connectivity is the vulnerability of the LAN to unauthorized access.

IBM High-Rate Wireless LAN products enable you to apply additional security measures to restrict access to your wireless medium and network resources. Subject to the level of security required in your network environment, these measures might include:

- Securing access to wireless data
- Wireless data encryption
- Securing access point setup
- Advanced security maintenance

Restricting access to data

To prevent unauthorized wireless stations from accessing data over the network, IBM High-Rate Wireless LAN products support the following levels of security:

- Restricting access to the network
- Data encryption to encrypt all data transmitted through the wireless medium

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.

Restricting wireless access to the network

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

- Programming authorized stations with the correct network name.
- Building and using access control tables of authorized stations

Closing the wireless network

Closing the wireless network prevents unauthorized users from using a network access point. If a user tries to access the network without configuring their station with the correct High-Rate Wireless LAN network name, the user will not be able to use an access point.

There are two options for network access security: open and closed.

- The **Open** configuration is IEEE 802.11-compliant and the standard mode that enables access to the High-Rate Wireless LAN Access Point for:
  - All stations with the correct High-Rate Wireless LAN network name.
  - All stations with the network name field set to “ANY”
- The **Closed** configuration is an IBM High-Rate Wireless LAN proprietary mode that closes your network to all stations that have not been programmed with the correct High-Rate Wireless LAN network name. This option denies access to:
  - All High-Rate Wireless LAN stations with the High-Rate Wireless LAN network name set to “ANY”
  - All non-High-Rate Wireless LAN stations

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

To close your High-Rate Wireless LAN network, do the following

1. Start the High-Rate Wireless LAN AP Manager; then select the Access Point.
2. Click **Edit** to connect the access point.
3. Select **Wireless Interfaces**.
4. Select the interface (**PC card Slot A** or **B**) of the network.
5. Click **Security** to display the security properties.
6. Click the check box next to **Closed Wireless System**.
7. Click **OK** to confirm and close the Wireless Security Setup window.

8. If necessary, return to step 4 to set the Closed parameter for a second High-Rate Wireless LAN.
9. 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 the bridging operation again, allowing access only to those users that have been configured with exactly the same High-Rate Wireless LAN network name as identified in the setup of your access points.

Repeat steps 1 through 9 for all other access points.

Access control

Another method to restrict wireless access to the High-Rate Wireless LAN Access Points is to use the access control table feature or the RADIUS Server Access Control feature. Enabling the access control table feature provides these benefits:

- The access point only bridges messages to or from authorized High-Rate Wireless LAN stations identified in the access control table.
- The access point ignores all requests to forward data to or from non-listed High-Rate Wireless LAN stations.

Enabling access control is a more rigid security mechanism than closing the wireless network, because the LAN administrators must authorize each individual High-Rate Wireless LAN PC Card for each wireless device.

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, see “RADIUS server access control” on page 1-50.

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

- Append the unique universal MAC address of the High-Rate Wireless LAN PC Cards 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.

Enabling access control

To enable access control, create an access control table file (.TBL) using the AP Manager program.

Copy 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 1-49).

Creating/Editing an access control table

To create or edit the access control table:

1. Start the High-Rate Wireless LAN AP Manager and select an access point.
2. Click the **Access Control** tab
3. Click **Edit** to display all MAC addresses that are currently authorized. The default address is `All will be permitted`.
4. Use the following buttons to change the MAC address table:
   - **Add**: To add MAC addresses one at a time. 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.
5. Repeat step 4 for all stations you want to authorize to send and receive data by this access point.
6. Click **Save file** to create a file of the access control table. Use this file to import the configuration to other access points.
7. Click **OK** to return to the **Access Control** tab.
8. Click **OK** again to save the new configuration to the Access Point and to return to the main AP Manager window.
9. (Optional) Save the configuration to a local backup file (.CNF).

To save the table to all High-Rate Wireless LAN Access Points, see “Importing an Access Control Table” on page 1-49.

Importing an Access Control Table

To import an access control table file to your access points, do the following:

1. Start the High-Rate Wireless LAN AP Manager and connect to an access point in the edit mode.
2. Click the **Access Control** tab; then click **Edit** to display all currently authorized MAC addresses.
3. Click **Import File** and select the access control table file that you want to import.
4. Click **Open** 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.
7. (Optional) Save the configuration to a local backup file.

Disabling access control

To disable access control for your High-Rate Wireless LAN Access Points, do the following:

1. Start the High-Rate Wireless LAN AP Manager and connect to an access point in edit mode.
2. Click the **Access Control** tab; then click **Edit** to display all currently authorized MAC addresses.
3. To disable access control, click **Delete All**. The MAC address window displays `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. Update the Configuration record, found under "Configuration record" on page A-3 to reflect your changes.
7. (Optional) Save the configuration to a local backup file (.CNF).

Using a RADIUS server

You can use an IBM High-Rate Wireless LAN with a third-party RADIUS server. To use RADIUS server access control, do the following:

1. Set up a RADIUS server
2. Configure the RADIUS server:
   - Create a list of server users with their authorization passwords in the users file or database file of the RADIUS server.
   - Build a list of IP addresses of all access points on the RADIUS server in the station file or database along with the authorization password.
   - Build a list of all wireless stations and their MAC addresses that will be using the RADIUS server.
3. Configure all access points to:
   - Enable RADIUS MAC address authentication
   - Set the RADIUS authorization lifetime
   - Identify the RADIUS server IP address
   - Verify the RADIUS server authentication port

RADIUS server access control

With RADIUS server access control, you can do the following:

- Specify the lifetime of a granted authorization
- Set the authorization password
- Assign up to two RADIUS servers to validate wireless station MAC addresses.

For each RADIUS server you need to specify:

- the RADIUS server IP address
- the RADIUS server authentication port

WEP encryption

To provide the highest level of security to data transmitted over the network, use wired equivalent privacy (WEP) data encryption.

To use WEP data encryption in your network, all devices must be configured with matching WEP encryption key values.

WEP data encryption uses five-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 four different keys to decrypt wireless data, and select one of the specified decryption key values to encrypt wireless data.

With the option to use four different keys for decrypting wireless data, you can change your WEP keys at regular intervals without affecting regular network performance.

Enabling WEP encryption

Note: Use the Configuration record, found under “Configuration record” on page A-3 to record the WEP key values. Store the information in a safe place.

To enable encryption, do the following:

1. Start the High-Rate Wireless LAN AP Manager and select an access point.
2. Click **Edit**.
3. Click the **Wireless Interfaces** tab.
4. Click **Security** to view the Wireless Security Setup window.
5. Select **Enable Encryption** to enable encryption.
    a. Enter up to four different keys to decrypt data received through the wireless interface.
    b. Select one of these keys to encrypt wireless data that is to be transmitted through 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 reset.
8. (Optional) You can choose to configure your High-Rate Wireless LAN Access Point to allow or deny non-encrypted data.

WEP encryption key values

If you select to enable encryption, you can choose to enter up to four encryption keys.

For the High-Rate Wireless LAN PC Card, valid values are either:

- Five-digit alphanumerical value in the range of a-z and 0-9
- A 10-digit hexadecimal value, preceded by the characters "0x" (zero x).

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, that is, the next time the Security Setup window opens, you will not be able to read the WEP key values anymore. Write down the values you enter on the Configuration record, found under “Configuration record” on page A-3.

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. If you specified no more than two key values, you can only select the transmit key from these two values.

If you cleared the Deny non-encrypted Data check box, your High-Rate Wireless LAN Access Point might also transmit in non-encrypting mode.

Deny non-encrypted data

If you use wireless data encryption, encrypt all data that will be transmitted through the wireless medium.

In some cases you might want to choose to enable the access point to also process non-encrypted data. Examples of such situations might be:

- Network environments that include both wireless stations equipped with High-Rate Wireless LAN Silver cards that support WEP encryption and High-Rate Wireless LAN PC Cards that do not support encryption.
- Network environments where you are about to install a large number of wireless stations, using out-of-the-box configurations, which by default have encryption disabled.

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

For optimal security against unauthorized access to your network, leave the Deny non-encrypted data option enabled.

If you must enable the High-Rate Wireless LAN Access Point to communicate with wireless stations that support or do not support WEP encryption, or have the WEP encryption enabled or disabled, first go to “How WEP encryption works” on page 1-52.

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 for users to combine wireless LAN products from different vendors.

The drawback of easy access and compatibility is the vulnerability to unauthorized access to 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

  Note: For optimal security, use the Deny non-encrypted data option.

Enable encryption and deny non-encrypted data

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

- Only process messages received at its wireless interface, when the messages have been encrypted with 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, or is equipped with High-Rate Wireless LAN PC Cards that do not support WEP encryption, those stations will not be able to establish a wireless connection, because they will not be able to understand (decrypt) crucial network information.

Enable encryption and allow non-encrypted data

If you select to enable encryption, but you clear the deny non-encrypted data check box, the High-Rate Wireless LAN Access Point will:

- Process all messages received at its wireless interface, regardless of whether the messages have been encrypted with one of the identified keys.
- Encrypt wireless transmissions based on the encryption settings of the addressed station.
- Send the message in encrypted format, using the selected transmit key value, if the addressed station uses WEP encryption
- Send the message in non-encrypted format, if the addressed station does not use WEP encryption.
- Send the message in non-encrypted format, if the data message is a multicast or broadcast message

This performance of the High-Rate Wireless LAN 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

Attention: 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 (for example, user names and passwords) do not use this option, unless easy access or migration is more critical to your data network than top-level security.

Good practice administering encryption keys

To minimize the risk that intruders might be able to retrieve the WEP key values. do the following:

- Lock away any paper registration sheet that you use to define or 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 four different keys to decrypt data received through the wireless interface enables you to define a WEP key roll-over scheme.

For example, you can select another transmit key every x number of weeks, until you reach the fourth key. At that point in time you can enter three new WEP key values for the first three WEP key entries, prior to the expiration period of the fourth key value. When 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 the access point setup

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

To protect your network configuration from undesired modifications, take the following measures:

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

Read and Read/Write passwords

To restrict access to the High-Rate Wireless LAN 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 by clicking **Monitor** in the main High-Rate Wireless LAN AP Manager window.

You can define a read password in the Read Password field on the **SNMP** tab (Select **access point** from the list, click **Edit** ; then click the **SNMP** tab). The default value is "public".

Read/Write password: A read/write password will provide you with full access to display High-Rate Wireless LAN Access Point diagnostic information found by clicking **Monitor**, as well as the configuration settings found by clicking **Edit**.

Entering an incorrect password will result in a time-out error, or an error that displays `SNMP error no such name`.

To define a read/write password, do the following:

1. Start the High-Rate Wireless LAN AP Manager; then select the target access point from the list, or enter a specific IP address.
2. Click **Edit** to connect to the access point.
3. Click 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 resets.

SNMP IP access list

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

To authorize a High-Rate Wireless LAN management station to access an access point, you must identify:

- The unique IP address of the management station
- The access point interface (port) through which this station will access the configuration

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

Note: When using the SNMP IP access list, include the IP address of all stations that need to retrieve configuration or diagnostic information of the access point, that is, 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, do the following:

1. Start the High-Rate Wireless LAN AP Manager and select an access point.
2. Click **Edit** to connect to the access point.
3. Click the **SNMP** tab to display the SNMP parameters. The SNMP IP Access List is visible at the bottom of the SNMP window.
4. Use the following buttons to modify the SNMP IP access list:
    - **Add**: To add IP addresses to the list. (Press F1 for online 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 someone resets a High-Rate Wireless LAN Access Point, someone performs the forced reload procedure, if there is an authentication failure, or a link up or down is detected. The trap host alert enables the network administrator to verify whether the reset or forced reload action was an authorized action.

Enable trap host alerts

To activate the trap host mechanism, do the following:

1. Start the High-Rate Wireless LAN AP Manager and select an access point.
2. Click **Edit** to connect to the access point.
3. Click the **SNMP** tab to display the SNMP parameters.
4. In the field Trap Host IP Address enter:
    - Any valid IP address: A message is sent to this IP address if the Access Point is reset.
    - `0.0.0.0`: (Initial value) To disable SNMP Trap Agent.
5. Enter a password in the **Trap Host Password** field.

    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 is 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 is ignored.

    - Valid Values: Any alphanumeric value in the range of a-z or 0-9 with a minimum of 2 and a maximum of 31 characters.
    - Initial Value: public
6. Press **OK** to 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, that is, the network management station that will be used to receive the trap messages.
- The trap host password is included in the trap messages and helps 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 the following situations:

- The access point is reset
- The power to the access point is cut off
- Access point configuration has been changed

Authentication failure messages

This type of message is sent to the administrator’s station once a wrong password has been entered on a (mobile) station. However, the access point itself does not respond, and a time out error occurs.

Link up or down messages

This kind of message can be used in case of link integrity. If, for example, in a duplicate Ethernet connection an Ethernet link is broken automatically, a link down message can be generated. As a result of this message, the other Ethernet connection will be used. When the link is restored to the original connection, a link up message will be generated. The original connection will be used again.

Advanced security maintenance

This section provides information on the more advanced security measures for your Hihg-Rate Wireless LAN Access Point

Maintaining access control tables

Create a single access control table and store it on the hard disk drive of the administrator’s station, or share it with other administrator’s stations. Use only one table for all access points.

For more information, see “Creating/Editing an access control table” on page 1-49.

Maintaining WEP encryption keys

The WEP Encryption function enables the High-Rate Wireless LAN system to support up to four different keys simultaneously. This is in accordance with the 802.11 standard that defines four 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 information between each other is that they share a common key value at the same key-index number in the four-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 four 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 four keys. As long as there is one comon key, 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 MAC Address of the station. High-Rate Wireless LAN currently does not support that feature of the standard WEP function.

When planning to use 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 High-Rate Wireless LAN stations).

- The requirements for smooth transition from one key to another
- The minimization of 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 (AP) and High-Rate Wireless LAN Station (STA) over time is detailed in the tables below. Each table reflects a certain key roll-over strategy. Notice that the Outward key column shows which key is used to encrypt traffic from AP to STA, and the Inward Keys column indicates the keys 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 Tx column 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 Keys 1-2-3-4 column shows an equal sign (=) when the value does not change from the previous period. This is relevant when it concerns the High-Rate Wireless LAN stations keys, since knowledge of the key values is typically not transferred to the users, so they have to return their High-Rate Wireless LAN station equipment to an IP department to get the key values changed. Changing the Tx key 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

The following table 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 of keys at all High-Rate Wireless LAN stations synchronous with the access point configuration changes. This is not practical; there are four keys.

By initially configuring all stations with the keys for the first four 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.

Notice that in the transition periods 1, 3 and 5 the end users can switch from one Txkey index to the next. At the end of this period, all stations must be switched 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 lifetime 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.

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

Single key - transition period

To introduce a transition period between the main life of the successive keys, the scheme must be changed as shown in the following table.

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

Alternative schemes

Alternative schemes can have main life periods where two or more keys are active.

The following table 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 High-Rate Wireless LAN stations. This scheme works better than the scheme in Single key — Transition period because it requires less frequent configuration changes at all Access Points.

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

Advanced Network Configurations

This section contains information on the following advanced configurations of the High-Rate Wireless LAN network:

- Advanced parameters
- Configuring large networks
- Modifying the configuration
- Restoring a backup configuration
- Dual PC Card configuration
- IP addresses and subnets

Advanced parameters

You might want to use the Advanced parameters options that are supported by your High-Rate Wireless LAN Access Points, especially when you are administering larger High-Rate Wireless LAN networks that include more than 10 access points.

Advanced parameter options include:

- Advanced High-Rate Wireless LAN parameters, such as multiple frequency channel configurations, RTS/CTS Medium Reservation, and Distance Between Access Points
- Bridge parameters that enable you to filter specific networking protocols or traffic between specific stations
- High-Rate Wireless LAN Access Point parameters
- SNMP parameters

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

Note: The advanced parameters described below as “common” parameters are the same for all High-Rate Wireless LAN Access Points in your network.

To set the advanced parameters, follow the instructions in “Configuring infrastructure networks” on page 1-13, to connect to the access point that you want to configure.

Advanced High-Rate Wireless LAN parameters

If you created a basic access point configuration you might have already noticed the additional buttons in the High-Rate Wireless LAN setup window.

Using the frequency menu: The Frequency menu enables you 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.

To change the frequency parameters, click **Advanced** on the **Wireless Interfaces** tab of the edit mode.

To optimize network traffic, assign different operating frequencies to High-Rate Wireless LAN Access Points that service neighboring wireless cells so that stations in each of the cells will be able to use the maximum bandwidth available to their cell.

Wireless stations equipped with High-Rate Wireless LAN PC Cards can dynamically change the operating channel when roaming between access points that operate at different sub-channels.

Enabling RTS/CTS medium reservation: FRTS/CTS medium reservation might provide a solution for networks where:

- Density of High-Rate Wireless LAN stations and access points is very low.
- There is poor network performance due to excessive frame collisions at the access points.

In most networking environments, however, it is unlikely that you will need to enable RTS/CTS medium reservation on the access point to prevent collisions. Before you change this setting for the High-Rate Wireless LAN Access Point, read the information about “Optimizing wired connections” on page 1-36.

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

Activating interference robustness: You can enable the Interference Robustness in exceptional cases when you troubleshoot slow performance of your High-Rate Wireless LAN network that could be related to in-band interference such as from microwave ovens. Interference usually is indicated by 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” High-Rate Wireless LAN 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 **Advanced** on the **Wireless Interfaces** tab in the edit mode to display the Advanced Setup window; then select **Interference Robustness**.

Distance between access points: In networking environments where you have data intensive users or a large number of users in a small area, you might want to increase the number of High-Rate Wireless LAN Access Points (making the distance between access points smaller), and then adjust 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 **Advanced**. In the **Distance Between APs** field, select one of the following density options:

- **Large** (default)
- **Medium**
- **Small**

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

Note: 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 might have unpredictable performance results for wireless (mobile) stations in your network.

Select the **Medium** setting for environments where High-Rate Wireless LAN 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 **Large** setting creates overlapping radio cells that might cause stations in one cell to defer data transmission for stations located in the neighboring cell.

Only select the **Small** setting when you are designing a wireless infrastructure that includes a high concentration of High-Rate Wireless LAN Access Points, that is, when the total cost of hardware investments is less critical than the maximum data throughput per cell.

Note: The **Medium** or **Small** settings require a excellent quality of radio communications throughout the entire wireless coverage area. In environments where the actual placement of High-Rate Wireless LAN 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** does not yield better results. In fact, changing the distance might seriously affect the roaming performance of your wireless stations, risking network communication errors caused by "out-of-range" situations.

Before using the **Medium** or **Small** setting to create a high performance network, be sure to read "Frequency channel management" on page 1-42.

For more information about access point density, go to "Optimizing performance" on page 1-33.

Multicast rate: The Multicast Rate identifies the preferred transmission speed for your High-Rate Wireless LAN Access Point broadcast traffic as forwarded by the access point. Where transmissions at lower data rates are usually more reliable, you might prefer higher throughput performance rather than greater coverage for your wireless radio signal.

For more information about Multicast Rate, refer to the help-file of the AP Manager program.

Setting 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 might include:

- Specific network protocols exchanged by networking devices such as servers, that are not relevant to the wireless stations.
- Broadcast or multicast messages exchanged by specific networking devices such as servers that are not specifically addressed to the wireless stations.
- "Junk traffic", such as, 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 through 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
- Filtering traffic exchanged between two specific stations that are identified by their static MAC address
- Enabling the spanning tree mechanism to resolve the closed network loops errors
- Storm threshold filtering to limit the number of messages per port and/or station from being bridged

Note: The Bridge parameter settings are typical "common" parameters, that is, the Bridge parameter settings are the same for all High-Rate Wireless LAN Access Points.

To set the Bridge parameters, connect to the access point and select the **Bridge** tab to display the bridge parameters

Protocol filtering: The filtered protocols are displayed in the top section of the **Bridge** tab. The factory-set default of the High-Rate Wireless LAN Access Point is `None`, which enables all protocols to be transmitted to the wireless medium. Use this setting when you do not require specific protocols to be filtered.

To filter specific protocols, do the following:

1. Determine the minimum set of protocols that must be bridged.
2. Click the **Edit** button to display the Filter Ethernet Protocols window.
3. Click the check boxes 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 **Custom** to enter the protocol manually and then click **OK** to return to the **Bridge** tab as shown.

   All selected protocols and all custom protocols that you have added manually, will be listed in the Protocols to Filter field.
5. 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 High-Rate Wireless LAN AP Manager window.

Static MAC address filter: To filter out traffic exchanged between stations that is not required to be sent or received using the wireless interface, you can set the Static MAC address Filter in the bottom section of the **Bridge** tab. The default value, `None`, is acceptable for most networking environments.

You can use the MAC filtering option to filter broadcast or multicast messages exchanged between wired servers that can also exchange messages using 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.

When messages are filtered, one of the listed stations sends a message to a MAC address that has been identified as a pair and the High-Rate Wireless LAN Access Point will not forward it using the wireless station. All traffic that one of the stations wants to send to any other (non-paired) MAC address will be forwarded.

Using the Spanning Tree feature: The **Spanning Tree** button enables 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 backup to the main wireless link.

To enable the spanning tree feature, do the following:

1. Click **Spanning Tree** to open the Spanning Tree Setup window.
2. Click the **Enable Spanning Tree** check box.
3. Use the default values.
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 High-Rate Wireless LAN AP Manager window. If you do not want to save this configuration, continue changing other parameters.

   Be sure to create a backup file, as described in “Step 4: Creating a backup file of your configuration” on page 1-15.

Storm Thresholds: You can use the **Storm Thresholds** button to set parameters that are used in protecting the network against message overload as received from a single station or from a specific port.

You can use the Storm Thresholds window to determine the maximum number of multicast and broadcast messages that will be forwarded from one port (or address) per second.

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

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

Setting access point IP parameters

You can use the **Access Point IP** tab to set the common IP parameters and to change the unique IP address of your High-Rate Wireless LAN Access Points.

To change the IP parameters, do the following:

1. Be sure you are connected to the right access point in the edit mode and click the **Access Point IP** tab to display the IP parameters.
2. Verify 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).
3. When you are finished, continue with configuring other parameters or click **OK** to save the configuration and return to the main High-Rate Wireless LAN AP Manager window

IP Address: Each Access Point needs an unique IP address. Use one of the following methods for IP addresses:

- DHCP, to obtain an IP address automatically
- Manually enter an IP address

Note: All High-Rate Wireless LAN Access Points must have a unique IP address value to enable you to address each access point specifically. Duplicate IP address values might cause unexpected behavior of the network or negative impact on network performance.

Manually assigning an IP address: To manually assign an IP address, use the Access Point IP Address field to enter a value from the range of IP addresses assigned to your organization.

The IP address is primarily used to address this High-Rate Wireless LAN Access Point when you use the High-Rate Wireless LAN AP Manager program to configure or monitor that device.

When your organization does not use IP addressing, you can enter a user-defined value. For example, you can enter 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 assigning an IP address: In case when a DHCP server is available on the network, an IP address can be automatically assigned to the Access Point by the DHCP server. To enable automatically obtaining an IP address form the DHCP server, select the **Obtain an IP address from the DHCP server** field in the **Access Point IP** tab window.

For more information about DHCP, see “BOOTP and DHCP” on page 1-73.

Subnet Mask: The Access Point Subnet Mask field is a common parameter and must be the same for ALL network devices within your IP subnet. You can use 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 Default Router IP field is an optional field for when you want to use the High-Rate Wireless LAN Access Point support for TRAP messages. See “SNMP parameters” on page 1-66.

You can use the Default Router IP field to identify the IP address of the router that the High-Rate Wireless LAN Access Point will use to find the Trap Host IP Address (identified in the SNMP Parameters).

Note: The default router and the trap host IP address 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 Default TTL (Time To Live) field identifies the maximum number of hops for an IP message generated by the High-Rate Wireless LAN 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, that is, they are the same for ALL High-Rate Wireless LAN Access Points in your network.

To set the SNMP parameters, do the following:

1. Make sure you are connected to the right access point and select the **SNMP** tab to display the SNMP parameters.
2. Verify or modify the parameters of your choice.

   The parameters that you need to specify are:

   - Read/Write Password to restrict access to the configuration of your High-Rate Wireless LAN Access Points, and
   - System Name to allow easy identification of the access point when using the diagnostic options of your High-Rate Wireless LAN software tools.
3. When you have finished setting the SNMP parameters, continue 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 to prevent unauthorized access to the High-Rate Wireless LAN Access Points.

A read password is requested when you connect to an access point 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 to prevent unauthorized access to the High-Rate Wireless LAN 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 System Contact field to enter a generic name for the network supervisor or department, such as, “Your LAN Administrator”.

System name: Use the field System Name field to enter a generic logical location of an High-Rate Wireless LAN Access Point, such as, “Incoming Goods Department”.

System locations: Use the System Location field to enter a generic physical location of an High-Rate Wireless LAN Access Point, such as, access point floor.

Trap Host IP Address: If you plan to use the trap alert system as described on “Trap host alerts” on page 1-56, 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”.

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 might have been erroneously sent to the trap host station.

SNMP IP Access List: You can use the SNMP IP Access List to create an extra level of security in addition to the read and read/write passwords. You can authorize a limited number of administrator's stations to view or modify the configuration of the High-Rate Wireless LAN Access Points, based upon the IP address of these stations.

In the SNMP IP Access List field, include the IP address of all administrator's stations that will use the AP Manager to configure and/or monitor your access points.

To authorize a administrator's station you must enter:

- The IP address of the stations
- The High-Rate Wireless LAN Access Point network interface through which they will access the access point. To indicate the interface, use either:
    - — 1 for Ethernet
    - — 2 for the High-Rate Wireless LAN network interface in socket A
    - — 3 for the High-Rate Wireless LAN network interface in socket B

You can also use the value x to enable the identified IP address to access the access point through any of the available interfaces.

To allow multiple administrator's stations to access the High-Rate Wireless LAN Access Point configuration or monitor parameters, you can also assign a range of IP addresses. Enter a subnet mask value that will indicate the subnet from which all stations are authorized to modify the SNMP setup.

Configuring large networks

Each High-Rate Wireless LAN Access Point configuration is characterized by two types of parameters:

- Common parameters that must be the same for all access points in your network
- Unique parameters that must be unique for each access point in your network

In larger networking organizations, it might become cumbersome to copy the common parameters to each of the access points in the network to provide consistency throughout the entire network. As the number of access points increases, the risk of errors (for example, as a result of typos) might increase as well.

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

Create a template file that contains all of the common parameter settings that apply to every High-Rate Wireless LAN Access Point within the network.

Common parameters

Common parameters, such as the High-Rate Wireless LAN 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 the following table, with the High-Rate Wireless LAN AP Manager tabs where you can view or modify the parameters.

Parameter	AP Manager tab
• High-Rate Wireless LAN 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 the following table.

Parameter	High-Rate Wireless LAN 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 High-Rate Wireless LAN 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 High-Rate Wireless LAN Access Point, modify the parameters identified as the unique parameters to differentiate the access point from the other access points in this network.

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 High-Rate Wireless LAN Access Point from the other access points.

Note: Create a backup file for each unique High-Rate Wireless LAN Access Point configuration, using the Download Config File item from the Access Point menu in the main High-Rate Wireless LAN 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, do the following:

- Unpack the High-Rate Wireless LAN Access Points and record their serial number and MAC address on the Configuration record, found under "Configuration record" on page A-3.
- Make a list of IP addresses available in your network. You need one IP address for each access point.
- Use the Configuration record to assign one IP address to each of your access points.
- Record the intended system location of each access point on the Configuration record.

Creating a template file: To create a template file, do the following:

1. Configure the first High-Rate Wireless LAN Access Point as described in "Configuring infrastructure networks" on page 1-13.
2. Save the configuration of this access point to disk as described in "Step 4: Creating a backup file of your configuration" on page 1-15.
3. Create a copy of the back-up file with the name COMMON.CNF or any other name that enables you to easily recognize the file as the actual template file that you will use as the basis to configure the other access points in your network.

Note: Do not start using your original backup file as a 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 backup copies on a separate disk or location.

Configuring other access points: When you have created the template file, you can start configuring the other High-Rate Wireless LAN Access Points in batch-mode. For each access point, do the following:

1. Start the High-Rate Wireless LAN 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 R**efresh Access Point List** from the Access Point menu.
3. If the selected access point is still using the factory-set IP address, such as when you are configuring a new out-of-the-box access point, you are prompted to change the default IP address.
4. When you are prompted, navigate to the disk or folder where you stored the template file.
5. Select the template configuration file (for example. COMMON.CNF) and click **Open**.

Attention: The IP address that was displayed in the list in the main High-Rate Wireless LAN 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 might lead to multiple High-Rate Wireless LAN Access Points being configured with the same IP address, resulting in unpredictable network behavior.

The High-Rate Wireless LAN AP Manager program has now loaded the settings as identified in the template file. You must change all the parameters that should be unique to this access point (see “Unique parameters” on page 1-69) before saving the configuration and returning to the main High-Rate Wireless LAN Access Point window by clicking **OK**.

6. Set the unique parameters that apply to this access point.
7. Save the configuration to the access point by clicking **OK**. You return to the main High-Rate Wireless LAN Access Point window.
8. Create a backup 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) Flash ROM of the High-Rate Wireless LAN 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 want to configure.

Completing the installation: If you configure the High-Rate Wireless LAN Access Points at your desk, when the access points are 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 configuration data and the location where you will install the access point on the Configuration record.
3. When you are finished, store the back-up files (.CNF), your template file (COMMON.CNF) and your Configuration record in a safe place, such as your computer or a diskette.

Modifying the configuration

You can modify the High-Rate Wireless LAN Access Point configuration parameters using the **Edit** button from the main High-Rate Wireless LAN AP Manager window.

Be sure 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 might need to modify the High-Rate Wireless LAN interface parameters of the station to match the values that were originally stored in the High-Rate Wireless LAN Access Point.

If you have forgotten the read/write password, or any other setting required to access the access point, you might need to perform a forced reload, as described in Appendix C, “Forced reload procedure” on page C-1.

When you make changes to the configuration of a particular access point, update the Configuration record to reflect these changes.

Changing common parameters

If you need to make changes to the common parameters, do as follows:

1. Change the common parameters for one access point.
2. Save the changes to a new template file (for example, COMMON.CNF).
3. Follow the procedure as described in “Configuring other access points” on page 1-70.

Restoring a backup configuration

To restore previously saved back-up configuration files to your High-Rate Wireless LAN Access Point, do the following:

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; then click **Open**.
5. When prompted to confirm the upload, verify whether the displayed 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 are loaded into the Flash ROM of the High-Rate Wireless LAN Access Point. The parameters remain intact whenever the access point is reset or switched off and on again. To change the parameters again, repeat the procedure as described in this section to reconfigure your access points.

Dual PC Card Configuration

You can use two PC Cards in one High-Rate Wireless LAN Access Point to:

- Migrate between various generations of the High-Rate Wireless LAN products
- Double the capacity of the Access Point

The dual slot design of the High-Rate Wireless LAN Access Point enables you to configure the access point to operate with almost any combination of the wired and wireless network interfaces listed above. so that your access point can provide easy migration paths between various generations of High-Rate Wireless LAN products.

A second PC Card inserted in the second slot of the Access Point will double the capacity of the access point. This option might be used in cases where a high rate of lost messages prevent fast data communication.

IP addresses and subnets

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

When installing an High-Rate Wireless LAN infrastructure into this type of network architecture, note that all High-Rate Wireless LAN Access Points and wireless stations must be installed on the same subnet, that is, on the same side of the router or gateway.

The roaming function does not work over routers. When access points are connected to different subnets, a mobile station might lose its network connection when it enters an area where the access points are connected to a different subnet.

The configuration and management of your access points is managed through the TCP/IP protocol stack. Each access point and computer that you want to use to configure the access points must have a unique IP address.

Assign "static" IP addresses to the access points to ensure that the access points at specific locations always have the same IP address. For the administrator's stations, you can use a "static" IP address or a dynamic IP address that is assigned by a BOOTP or DHCP server.

When assigning IP addresses to administrator's stations and access points, be 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 High-Rate Wireless LAN infrastructure is just the physical medium to connect a computer to an access point, like using wire to connect it to an Ethernet infrastructure.

However, in environments where the network operating system uses the TCP/IP protocol, stations might need to have an IP address as well to use specific networking services, for example, access to the Internet.

BOOTP and DHCP

When turned on for the first time, the High-Rate Wireless LAN Access Point will broadcast a request for an IP address. If your network includes a BOOTP or DHCP server, this server automatically assigns an available IP address to the access point.[4]

Subject to the settings of your BOOTP or DHCP services, you might need to introduce the High-Rate Wireless LAN Access Point MAC address to the BOOTP or DHCP server. Refer to 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. If the access point is reset, the DHCP server might assign another IP address. To obtain consistency in the IP address, 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.

[4] Older versions of the Access Point do not support dynamically assigning IP addresses. Assign an IP address to these access points. These access points can be updated with new software to support the dynamically assigning IP addresses.

Appendix A. Access point startup configuration

Your High-Rate Wireless LAN access point comes with the access point operating software factory installed. With this software, the access point has also been loaded with a factory-set configuration that allows for out-of-the box operation.

The factory-set configuration is not the default configuration. If you reset the access point or perform a Forced Reload, the unit will not return to the factory-set configuration.

To connect to a access point, configure the High-Rate Wireless LAN network parameters of each wireless station to match the values as identified for the access point.

When you turn on an access point for the first time, these values match the values listed in the table under Factory set configurations.

For normal operation, match these values with the ones you identified when configuring the access point. Record this information on the Configuration record in this appendix.

Factory set configurations

This table provides information on the factory set startup configuration and the interface startup configuration for the High-Rate Wireless LAN Access Point.

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*[a] • Trap Host IP address: 0.0.0.0[b] • 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

a. Ethernet MAC address of the device (printed on a label on the processor module).

b. No SNMP traps are sent with this IP address.

High-Rate Wireless LAN network name	High-Rate Wireless LAN network[a]
RF-Channel: 2.4 GHz	2.462 MHz: France 2.484 MHz: Japan 2.422 MHz: All other countries
Closed wireless system	disabled
Encryption	disabled
Medium reservation	disabled
Microwave oven robustness support	disabled
DTIM period	1
Distance between APs	Large
Multicast rate	2 MBps

[a] When your network includes MS-DOS stations using the High-Rate Wireless LAN DOS ODI driver, change the value to a name that consists of upper-case characters only.

Configuration record

This section contains a table to record your configuration information.

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: ______________

	Serial Number	MAC Address	IP Address	IF	Frequency	Device Location	Date Installed	Configuration File
Access Point Unique Identifiers				□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 the access point

This section provides information on troubleshooting the High-Rate Wireless LAN Access Point.

Problem-solving approach

Problems experienced in wireless LAN operation can be related to:

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

To resolve a configuration mismatch you need to compare the configuration parameter settings of both High-Rate Wireless LAN Access Points and all High-Rate Wireless LAN stations in use.

To determine a component failure, check the LED activity of the access point. For the High-Rate Wireless LAN Access Point, use the table in this appendix to determine if a problem has a hardware-related cause (component failure). This table might also provide help in diagnosing and solving operational problems that have other possible causes.

When your access point appears to have stopped responding to normal bridging requests, try resetting the device as described in “Resetting the access point” on page B-3.
In exceptional cases, you might consider performing a forced reload procedure as described in Appendix C, “Forced reload procedure” on page C-1.

LED errors

This table provides information on the LEDs for the access point.

Power ⏻	**Ethernet** ●—●	**Wireless interface A** ∿ A	**Wireless interface B** ∿ B	**Description/action**
Steady green	Flicker green	Flicker green	Flicker green	Normal operation
Steady green	Off	Off	Off	Normal operation (no LAN activity)
Off	Off	Off	Off	No power. Check the power cord and power supply
Steady green	Flicker green	Amber	-	Network overload. Run Remote statistics or eliminate redundant traffic.
Steady green	Flicker green	-	Amber	Network overload. Run Remote statistics or eliminate redundant traffic.

Power ⏻	**Ethernet** ●—●	**Wireless interface A** ∿ A	**Wireless interface B** ∿ B	**Description/action**
Steady green	Green	Amber	Amber	Network overload. Run Remote statistics or eliminate redundant traffic.
Steady green	Flash red	-	-	Frames are rejected. Run remote statistics to verify the number of packets in error. If that number is high, run a remote link test to determine the problem station.
Steady green	-	Flash red	-	Frames are rejected. Run remote statistics to verify the number of packets in error. If that number is high, run a remote link test to determine the problem station.
Steady green	-	-	Flash red	Frames are rejected. Run remote statistics to verify the number of packets in error. If that number is high, run a remote link test to determine the problem station.
Amber	Off	Off	Off	Forced reload. See Appendix C, “Forced reload procedure” on page C-1.
Amber	Amber	Amber	Amber	Forced reload. See Appendix C, “Forced reload procedure” on page C-1.
Amber	Flicker green	Off	Off	Forced reload. See Appendix C, “Forced reload procedure” on page C-1.
Amber	Off	Flicker Green	Off	Forced reload. See Appendix C, “Forced reload procedure” on page C-1.
Amber	Off	Off	Flicker green	Forced reload. See Appendix C, “Forced reload procedure” on page C-1.
Red	-	-	-	General hardware failure. Reset the access point using instructions in “Resetting the access point” on page B-3.
-	Amber	-	-	Ethernet hardware failure. Reset the access point using instructions in “Resetting the access point” on page B-3.

Power ⏻	**Ethernet** ●—●	**Wireless interface A** ∿A	**Wireless interface B** ∿B	**Description/action**
-	-	Amber	-	High-Rate Wireless LAN hardware failure. Reset the access point using instructions in “Resetting the access point” on page B-3.
-	-	-	Amber	High-Rate Wireless LAN hardware failure. Reset the access point using instructions in “Resetting the access point” on page B-3.
Off	Off	Amber	Off	The PC Card is not recognized. This might occur in the following situations: • The access point is loaded with outdated software • The inserted PC Card is not a High-Rate Wireless LAN PC Card Update the software for the access point (see Appendix D, “Upgrading access point software” on page D-1) or replace the PC Card. Refer to the README.TXT file in the AP Manager for more information.

Resetting the access point

If a High-Rate Wireless LAN Access Point has stopped responding to normal bridging requests, you can reset the access point manually or remotely.

Upon reset, the High-Rate Wireless LAN Access Point runs the startup diagnostics and startup bridging operation using the configuration parameters as they were stored in the access point prior to the restart. For out-of-the-box access points, these parameters will be as identified in “Factory set configurations” on page A-1.

Resetting the access point manually

To reset the High-Rate Wireless LAN Access Point manually, do the following:

1. Remove the cover of the access point (see your *High-Rate Wireless LAN Access Point Quick Start Guide* for assistance if needed).
2. Locate the two small holes on the bottom of the processor module, marked **Reset** and **Reload**.

3. Use a small pointed object, such as the tip of a ball-point pen, to press the **Reset** button.

   The access point will restart and run the startup diagnostics, characterized by a LED sequence where the LEDs change color in the from red to amber to green.

4. When the Power LED is green, and other LEDs are off or flickering (indicating LAN activity), mount the cover of the access point.

After approximately 15 seconds, the unit starts the bridging operation using the configuration parameters as they were stored in the access point prior to the restart.

Resetting the access point remotely

To reset an High-Rate Wireless LAN Access Point from a remote location, do the following:

1. Start the High-Rate Wireless LAN 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. Click **Reboot Access Point**.
5. The AP Manager program prompts you to enter the password required to reset the device. Enter the Read/Write password; then click **OK**.

   The access point restarts and runs the startup diagnostics.

After approximately 15 seconds, the access point starts the bridging operation, using the configuration parameters as they were stored in the access point prior to the reset.

If you want to display the configuration file or monitor the performance of the access point after a reset, you might have to wait until the unit completes the startup diagnostics before you can access the access point again.

Appendix C. Forced reload procedure

By performing a forced reload, you can recover from a situation where:

- The High-Rate Wireless LAN Access Point has stopped responding to the system
- You have misplaced the unique identifiers such as IP address, SNMP read/write password, or other parameters that prevent communication with the access point
- The High-Rate Wireless LAN Access Point has been configured with incorrect High-Rate Wireless LAN parameters, preventing you to access the access point via the High-Rate Wireless LAN network interface.

Attention:

When you must perform a forced reload, remember the following:

- Access points equipped with High-Rate Wireless LAN network interfaces that are set to Forced Reload mode cannot be accessed through the High-Rate Wireless LAN network interface.
- Do not perform a forced reload procedure for more than one access point at a time.

  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 stops the bridging operation. The access point is only capable of accepting a new software image to be programmed into the Flash ROM.

To access a High-Rate Wireless LAN Access Point in Forced Reload mode, you might need to reconfigure your LAN administrator's station.

If your access points are equipped with only High-Rate Wireless LAN PC Cards, you might want to perform the forced reload using a configuration scenario as described in "Configuration scenarios" on page 1-11.

Performing a forced reload

To perform a forced reload procedure on your High-Rate Wireless LAN Access Point, do the following:

Step 1: Preparing for the forced reload procedure

A forced reload procedure can only be performed when you have physical access to the High-Rate Wireless LAN Access Point. Determine the answers to the following questions:

- Do you need special equipment to access the access point?
- Do you have a backup copy of the access point's current configuration file (.CNF)?

  If Yes, you can use the backup copy to restore the original configuration.

  If No, you must reset all of the user-defined parameters for the access point that apply in your network.

Backup copies might have been created upon initial installation, using the Download Config File option of the High-Rate Wireless LAN AP Manager program.

If you have access to the High-Rate Wireless LAN Web site, you can download the latest software (.BIN files) available for your access point.

Specify a temporary IP address for the access point. To enter this temporary IP address, do the following:

1. Open the AP Manager program.
2. In the Tools menu, click **Options**.
3. Enter the temporary IP address in the Temporary IP address field.

   The temporary IP address is assigned to the access point in Forced Reload mode. This is enables configuring and uploading the software file, before the access point has a definite IP address.

Two configurations of your LAN administrator’s station are possible to enable you to logically access the High-Rate Wireless LAN Access Point:

- Your LAN administrator’s station is a High-Rate Wireless LAN station.
- Your LAN administrator’s station is a wired (Ethernet) station.

Your LAN administrator’s station is a High-Rate Wireless LAN station

When using IP addressing, write down the IP address that the access point should use.

You can only use a wireless LAN administrator’s station to access a High-Rate Wireless LAN Access Point in Forced Reload mode if the station has indirect access to the access point.

Be sure that your LAN administrator’s station matches the settings of the access point that you use to establish the connection to in Forced Reload mode.

Be sure the LAN administrator’s station is within range of the access point.

When using IP addressing, write down the new IP address that you want to assign to the access point in Forced Reload mode.

Your LAN administrator’s station is a wired (Ethernet) station

Your LAN administrator’s station is connected to the High-Rate Wireless LAN Access Point through the Ethernet interface of the access point.

Be sure the LAN administrator’s station and the access point are connected to the same LAN segment (subnet).

To communicate with an access point in Forced Reload mode, there cannot be any routers between the target access point and the LAN administrator’s station.

Step 2: Setting the access point to Forced Reload mode

To set the access point to Forced Reload mode, do the following:

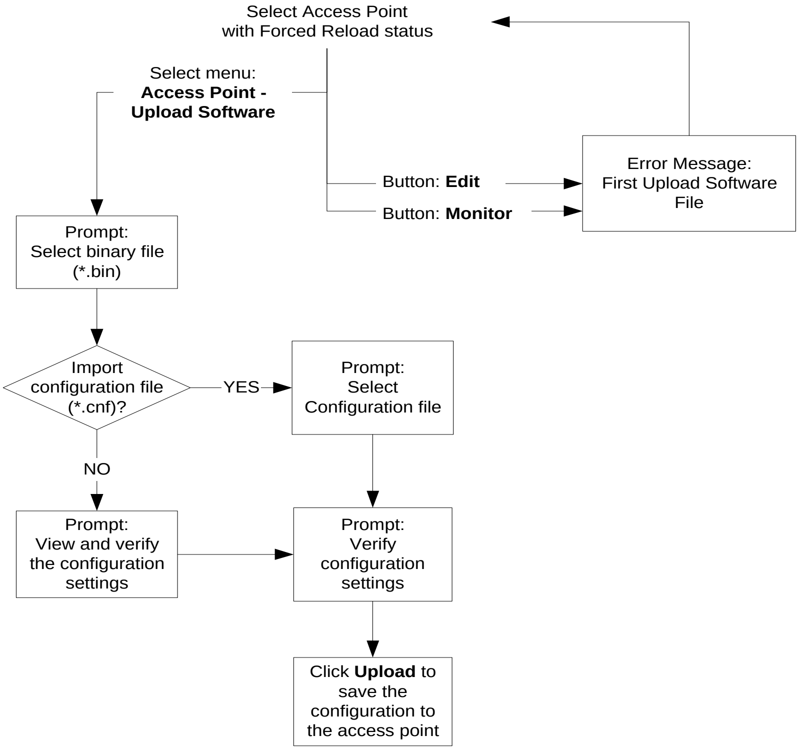
1. Remove the cover of the High-Rate Wireless LAN Access Point.
2. Locate the two small holes on the long-edge side of the processor module, marked **Reset** and **Reload**.

3. Use a small pointed object, such as the tip of a ball-point pen, to press the **Reset** button.
4. Release the **Reset** button and wait five seconds. The access point will perform start-up diagnostics, characterized by LED activity, where the color of the LEDs change from amber to red to green.
5. After approximately five seconds, use the small pointed object again to press the **Reload** button for approximately 30 seconds. The color of the LEDs will change from amber to red to green again.
6. When all LEDs turn amber, release the **Reload** button.

   The Power LED turns to amber. Other LEDs will be off, or might flicker green to indicate LAN activity on the associated interface.
7. Start the High-Rate Wireless LAN AP Manager program; then continue with step 3.

Configuring and uploading files

Use the following illustration to see the complete configuration and upload procedure of the forced reload procedure.


Select Access Point
with Forced Reload status
Select menu:
Access Point - Upload Software
Button: **Edit**
Button: **Monitor**
Error Message:
First Upload Software File
Prompt:
Select binary file (*.bin)
Import configuration file (*.cnf)?
YES
NO
Prompt:
Select Configuration file
Prompt:
View and verify the configuration settings
Prompt:
Verify configuration settings
Click **Upload** to save the configuration to the access point

To configure the access point in forced reload status and to upload the configuration, do the following:

1. From the AP Manager, select the access point that is in Forced Reload mode.

   An access point in Forced Reload mode is displayed in the main AP Manager window at the top of the list, and can be recognized by the following:

   - The access point is marked with the forced reload icon
   - The access point is marked with the forced reload status
   - The access point has the IP address 153.69.254.254.

2. Select **Upload Software** from the Access Point menu to start the configuration and upload procedure.

   If you click **Edit** or **Monitor** 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 High-Rate Wireless LAN Access Point software from the High-Rate Wireless LAN Web site, select the directory where you saved the downloaded file.

4. From the list of displayed files, select **WPNT*XXX*.**BIN (where *XXX* identifies the version of the access point software).

5. Click **Open** to open the software file.

   You can now upload a backup configuration file to the access point.

   Note: When importing a configuration file, be sure to import the correct backup file. Configuring a High-Rate Wireless LAN Access Point with a configuration file that is identical to the configuration of another access point might lead to unpredictable behavior of your High-Rate Wireless LAN network.

   If you have a backup configuration file and if you want to use this file to configure the access point, click **Yes**; then elect the backup configuration file (.CNF) and click **Open** to open the backup configuration settings. Click **OK** to check the configuration settings.

   If you do not have a backup 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 must manually modify or verify the configuration settings of the access point (assign a unique IP address, set up the High-Rate Wireless LAN parameters and, (if applicable) the other access point identifiers such as the IP Address and SNMP passwords).

   The Edit Configuration window opens. The Edit Configuration window does not contain an **OK** button, but contains an **Upload** button to upload the configuration settings to the access point, indicating that you are editing a local configuration file but you are not yet connected to the access point.

6. View (or modify) the configuration settings in all tabs.

   See “Basic network configuration” on page 1-12 for information on how to change the configuration settings.

7. Click **Upload** 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` is displayed. While trying to connect to the access point, the IP address in the configuration settings is pinged.

You are prompted to enter a new IP address only if the IP address specified in the configuration already exists. If the IP address does not yet exist, 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.

8. When you are prompted to confirm the Reload of the Remote System, click **Yes**.

   The local software file imports the configuration settings and saves these to the software (binary) file. The old software file is overwritten by the new software file. This does not influence the functionality of the software file. For more information, see "Uploading software" on page D-1.

   When you want to preserve the original software file, make a backup copy of this file.

9. You are again prompted to confirm the Reload of the Remote System. Thoroughly check the list of parameters displayed to make sure all settings are correct.

   If the window that opens does not display the correct IP address or SNMP passwords, click **No** to cancel.

   If the IP address and SNMP passwords in the window are correct, click **Yes** to continue.

10. The High-Rate Wireless LAN AP Manager program uploads the new (restored) configuration to your access point and loads it into the Flash ROM. The access point resets and start the bridging operation in approximately 60 seconds.

Step 4: Creating a backup file

Save the configuration parameters of the High-Rate Wireless LAN Access Point to a backup file (.CNF). To create a backup file, use the Download Config File option from the access point menu.

Create a backup file in case there are network errors that might force you to perform a forced reload in the future.

Save the backup file under a name that allows for easy identification in the future.

Appendix D. Upgrading access point software

The High-Rate Wireless LAN Access Point runs on embedded software, 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.

However, you might choose to load new access point software into the Flash ROM of your access points if:

- You want to upgrade your access point to support new functions
- You need to perform a forced reload procedure

The High-Rate Wireless LAN Access Point software is a binary file of the format WPNT*XXX*.BIN, where *XXX* is the version of the access point software.

You can find a copy of this file in the program directory where you installed the High-Rate Wireless LAN AP Manager program. For the latest version of the access point software versions, consult the IBM High-Rate Wireless LAN Web site at

http://www.ibm.com/pc/

The access point software file consists of the following information areas that are stored in the Flash ROM of the High-Rate Wireless LAN Access Point Bridge:

- The actual software program area. The data in this area cannot be configured by the user.
- The Configuration Parameters area, which contains user-defined settings of the access point. The data in this area can be modified at any moment when you use the High-Rate Wireless LAN AP Manager program to open and save a remote configuration file.

The High-Rate Wireless LAN AP Manager program merges the configuration parameters retrieved from the access point with the software information from the access point software file. These will be saved to disk first, prior to uploading the information into the access point.

Uploading software

When uploading access point software, no changes are made to the configuration of the access point. However, create a backup file using the Download Config File from the Access Point menu in case no backup file exists of the current configuration setting. To upload software, do the following:

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 High-Rate Wireless LAN AP Manager program prompts you to open an access point software file (.BIN).
3. Move to the directory where you have installed the High-Rate Wireless LAN AP Manager program file, or the directory where you saved the access point software file you downloaded from the High-Rate Wireless LAN Web site.

4. From the list of displayed files, select the file **WPNT*XXX*.BIN**, where *XXX* is the version of the access point software.

5. Click **Open** to open the access point software file.

6. Enter the password for the access point if you are prompted to; then click **OK**.

7. When prompted to confirm the access point software upload, click **Yes**.

   The High-Rate Wireless LAN Access Point will now reset and start the bridging operation using the parameters as set in the software file.

Confirming uploaded access point software

When you try to upload an High-Rate Wireless LAN Access Point software file to your access point, a window opens prompting you to confirm:

1. The upload of software to the access point

2. The overwriting of the access point software file 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, because it will not affect operation or the features of the access point.

Yes, upload access point software

When you select **Yes, upload access point software**, the High-Rate Wireless LAN AP Manager program will:

1. Save the access point software file back to disk, using the same filename. The software file you opened is overwritten.

2. 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 High-Rate Wireless LAN Access Point or imported from the backup file. The “Software Area” of the access point software file remains unchanged. See the last section for more information.

Since the “Software Area” remains unchanged, overwriting the software file does not affect the operation 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 High-Rate Wireless LAN AP Manager program aborts the upload operation.

If you would still like to upload the access point software, but do not want to overwrite the original software file, make a backup copy of the original software file and save it to a separate disk drive.

Part Number:
File Number:

Printed in the United States of America
on recycled paper containing 10&
recovered post-consumer fiber.