InstantWave™

11-Mbps

Wireless Access Point

User's Guide

Version A1
July 2002

NWH660

National Datacomm Corporation
4th Fl., No. 24-2, Industry East Road IV
Science-based Industrial Park
Hsinchu, Taiwan, R.O.C.

Technical Support
E-mail: techsupt@ndc.com.tw

NDC World Wide Web
www.ndclan.com

TRADEMARKS

NDC and InstantWave are trademarks of National Datacomm Corporation. All other names mentioned in this document are trademarks/registered trademarks of their respective owners.

NDC provides this document “as is,” without warranty of any kind, neither expressed nor implied, including, but not limited to, the particular purpose. NDC may make improvements and/or changes in this manual or in the product(s) and/or the program(s) described in this manual at any time. This document could include technical inaccuracies or typographical errors.

FCC WARNING

This equipment has been tested and found to comply with the limits for a Class B Digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters (8 inches) between the radiator and your body.

Packing List

Your NWH660 package should contain the following items:

- One InstantWave NWH660 11-Mbps Wireless Access Point (AP)
- One mounting kit (mounting template, screws, and screw anchors)
- InstantWave Management System (IWMS) and AP COMFig software and user manuals, and this user's guide, in electronic form (one CD-ROM or four floppy disks)
- One RS-232C serial cable

Contents

Figures

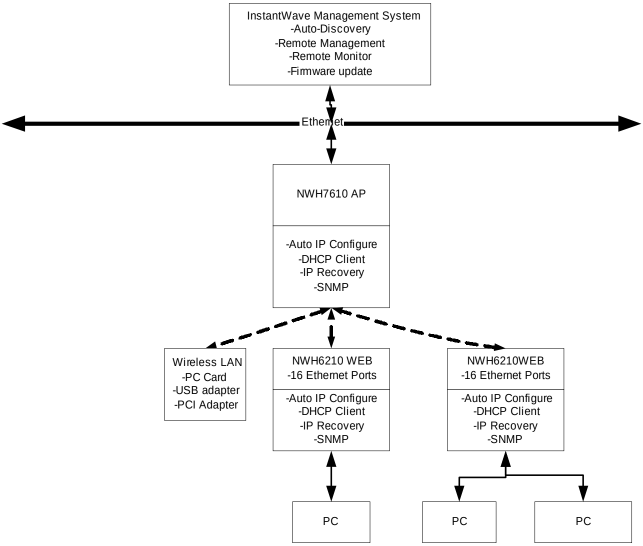
Introduction

Congratulations on choosing an InstantWave wireless product. This guide gives comprehensive instructions on installing and using the InstantWave NWH660 11-Mbps Wireless Access Point (AP), and also explains how to install and use the InstantWave Management System (IWMS) software.

InstantWave Wireless LAN Products

InstantWave wireless products provide an integrated solution to your wireless networking requirements.

- For indoor applications: Access points, wireless workgroup bridges, wireless ethernet clients, and wireless adapters with various bus interfaces (PCMCIA, USB, and PCI).
- For outdoor applications: The InstantWave building-to-building bridge connects two independent Ethernet LANs via a radio link, making expensive outdoor cabling unnecessary. High-gain directional antennas provide the greatest possible transmission range.
- Management tools: InstantWave products support the industry-standard Simple Network Management Protocol (SNMP) and the SNMP-based InstantWave Management System (IWMS), a powerful set of utilities for managing not only devices but whole networks and internetworks.



IWMS — The InstantWave Management System

IWMS is a powerful network management system that is fully compatible with the industry-standard Simple Network Management Protocol (SNMP). It features:

- Automatic discovery of all InstantWave devices that are configured within the same subnet
- Individual and batch-mode remote management of InstantWave devices, including Multi-Monitor, Batch-Upgrade, Batch-Reset, and Batch-LoadDefault functions. Batch-mode operation is ideal when deploying multiple InstantWave products.
- A friendly end-user interface with a consistent look and feel.

Automatic Discovery of InstantWave Devices

A powerful auto-discovery algorithm is built into the InstantWave Network Management System. With a simple click on the Auto Discovery icon, all InstantWave devices within the subnet will be discovered. This discovery feature is based on the following techniques:

- DHCP client and IP recovery: The NWH660 has a built-in DHCP client, and will request an IP address from a DHCP server so that SNMP management can be carried out. Should there be a failure of the DHCP server, the NWH660 will auto-assign itself an IP address (see next) and then automatically negotiate for a new IP address when the server recovers.

- Auto-IP: When the NWH660 cannot get an IP address from the DHCP server, it will auto-assign itself an IP address of 169.254.x.x and a subnet mask of 255.255.0.0. A Windows-based system configured as a DHCP client will follow the same algorithm to assign itself an IP address in the same subnet. *When the DHCP server comes back on line, users may need to renew their* *stations' IP settings as described below;* otherwise, Windows may continue to use the previous IP address instead of executing the auto-IP procedure.

Windows 95/98

step 1. Click ***Start/Run***, type *winipcfg*, and click ***OK***. The *IP Configuration* dialog box will open.

step 2. Select the network adapter you use to connect to the NWH660. Click ***Release***.

step 3. Click ***Renew*** to retrieve new information (IP address, subnet mask, and default gateway address) from the DHCP server. Click ***OK*** to save the changes and exit the program.

Windows NT 4.0

step 1. Click ***Start/Programs/Command Prompt***. Type *ipconfig /release* (with a space after *ipconfig*) and press ***Enter***.

step 2. Type *ipconfig /renew* (with a space after *ipconfig*) and press ***Enter*** to retrieve new information (IP address, subnet mask, and default gateway address) from the DHCP server.

step 3. Type *exit* and press ***Enter***.

Windows 2000/XP

step 1. Click ***Start/Programs/Accessories/Command Prompt***. Type *ipconfig /release* (with a space after *ipconfig*) and press ***Enter***.

step 2. Type *ipconfig /renew* (with a space after *ipconfig*) and press ***Enter*** to retrieve new information (IP address, subnet mask, and default gateway address) from the DHCP server.

step 3. Type *exit* and press ***Enter***.

IWMS Hardware and Software Requirements

System requirements for installing and operating the InstantWave Management System are:

- An x86-based microcomputer running Microsoft Windows 95, 98, Me, NT 4.0, 2000, or XP
- Microsoft Internet Explorer 4.01 or later
- A connection to an Ethernet network

Particular versions of Windows have the following additional requirements:

1. On Windows 95, Microsoft DCOM95 must be installed. You can obtain DCOM95 from the following Microsoft Web page:
   http://www.microsoft.com/com/dcom/dcom95/download.asp
   DCOM95 can also be found on the Microsoft Visual Basic 5.0 CD-ROM (Enterprise, Professional, or Standard edition), in the directory \Pro\Tools\DCOM95.

2. On Windows 98 (with the exception of Windows 98SE, which already includes this component), Microsoft DCOM98 must be installed. You can use the following link to download it:
   http://www.microsoft.com/com/dcom/dcom98/download.asp

3. On Windows NT 4.0, Service Pack 4 or later must be installed.

Terminology Used in this Guide

BSSID/MAC ID

The BSSID (Basic Service Set ID) is a factory-set ID unique to each InstantWave WLAN product. It is identical to the MAC ID (Media Access Control ID). It allows each InstantWave product to be identified on the wireless network.

ESSID

An Extended Service Set ID (often referred to as Service Set ID, or SSID) identifies the wireless LAN domain that an AP is in. A domain is generally composed of wireless APs you are most likely to communicate with. You can type an existing domain name or create a new one that contains up to 32 characters.

Regulatory Domain

InstantWave products use the license-free ISM (Industrial, Scientific, and Medical) band to communicate through radio waves. Different countries offer different radio frequencies to be used as the ISM band. There are four frequency bands defined by IEEE 802.11: Japan (2.471 to 2.497 GHz), USA, Extended Japan, Canada, and Europe (2.4 to 2.4835 GHz), Spain (2.445 to 2.475 GHz), and France (2.4465 to 2.4835 GHz). To use InstantWave products in a country not listed above, check with your government’s regulating body to find the correct frequency band to use. All InstantWave products are supplied preset to the country of sale’s frequency band.

WEP

WEP stands for Wired Equivalent Privacy. It is an encryption scheme that provides secure wireless data communications. WEP uses a 40-bit or 128-bit key to encrypt data. In order to decode the data transmission, all wireless clients on the network must use identical keys.

How to Use this Guide

This user's guide gives complete instructions for installation and use of the InstantWave NWH660 11-Mbps Wireless Access Point (AP).

Before putting the NWH660 into operation on your LAN, it is important that you adjust the unit's settings to conform to your networking environment. This can be done with either of two tools included in the NWH660 package: the AP COM-port Configuration utility (AP COMFig) or the InstantWave Management System (IWMS).

AP COMFig lets you carry out basic configuration of the NWH660 off-line, through the supplied serial cable, using a networked or stand-alone computer. IWMS is a powerful yet easy-to-use SNMP-based software package for configuration and management of InstantWave devices over network and internetwork links.

Read through the next section, "Planning the Network," to learn how to get the best possible performance from your InstantWave wireless network.

Step 1: Plan the wireless network	See "Planning the Network," page 15, for details.
Step 2: Pre-configure the AP before installing it on an existing Ethernet network	See "Hardware Pre-configuration," page 22, for details.
Step 3: Install the AP on the Ethernet network	See "Installing the InstantWave Management System," page 36, for details.
Step 4: Carry out on-line configuration and management of the AP via IWMS	See "Using the InstantWave Management System," page 39, for details.

Planning the Network

Infrastructure Network Types

An infrastructure network is formed by several stations and one or more access points (APs), with the stations within a set distance from the AP or APs. Figure 1 depicts a typical infrastructure network topology.

There are three infrastructure network setups that are commonly used. It is a good idea to understand the possible network setups and configuration requirements before planning your wireless network.

Type 1. The simplest wireless infrastructure network is composed of one access point (AP) and a few wireless stations communicating via radio waves (Figure 1). This setup enables mobile stations to communicate with each other. The main benefit of this type of network is to extend the range of the network. If an AP is placed between the stations, the radio transmission distance is effectively doubled since wireless computer #1 can talk to wireless computer #2 through the AP. The drawback of this configuration is that the effective bandwidth is halved since all communication is relayed by the AP.

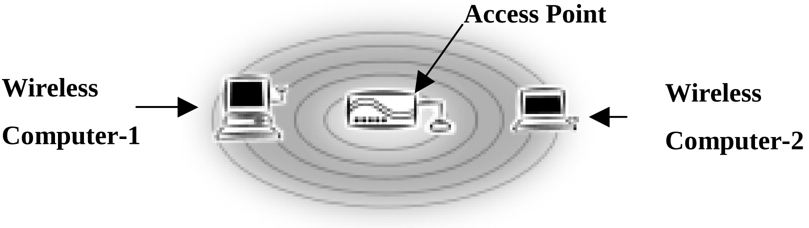


Figure 1. Simple Wireless Infrastructure Network

Type 2. The next simplest wireless network is very similar to the Type 1 network. This time the AP is connected to a wired Ethernet network as a node. In this configuration the AP operates as a bridge between the wired Ethernet network and the wireless networks (Figure 2).

Wireless users have the same access to network resources as they would have if they were wired. Such a configuration is often used to allow roaming, or to extend an existing network into a hard-to-wire environment.

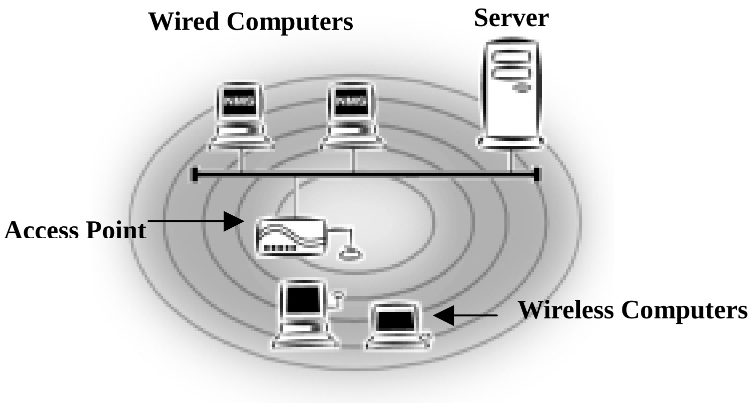


Figure 2. Single AP Network

Type 3. The third type of network is composed of multiple APs and multiple stations (Figure 3).

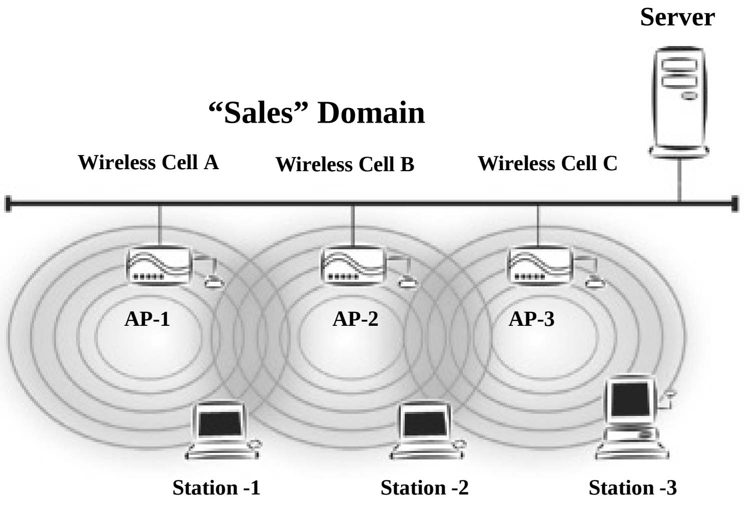


Figure 3. Multiple-AP Network

The reasons for having multiple APs installed are:

1. To increase bandwidth in order to boost overall network performance
2. To extend the coverage range

Any other configuration is usually a mix of these commonly used types.

Planning an Infrastructure Network

This section explains some of the factors you need to consider when planning an infrastructure network. Setting up is a two-step process:

1. Install and configure the InstantWave wireless products.
2. Decide the best physical location of the InstantWave wireless products so as to optimize performance.

The following section gives quick guidelines for these two steps. First, decide whether to have a single AP wireless network or a multiple AP network.

Single AP Installation

If you are setting up a simple network with only one AP and a few stations (a Type 1 or Type 2 network configuration as described in “Infrastructure Network Types,” page 15), all you need to do is make sure the AP and all the wireless stations hold the same domain name (SSID) and security (WEP) settings in their configuration.

Adding a new station to an existing infrastructure network is easy. Again, all you need to do is to set the newly added station’s domain name (SSID) and security (WEP) settings to be the same as those of the AP.

Multiple AP Installation

***Installing multiple APs on the same network (or domain) with overlapping signals (Figure 3, page 15*)**

- Use the same domain name (SSID) and security (WEP) settings.
- Enable the Roaming function on stations that require it.

Note: A station will automatically connect to whichever AP in the same domain is currently offering the best signal.

Roaming

InstantWave products allow wireless stations to roam freely within an infrastructure domain composed of multiple APs with overlapping signal coverage (as in the Type 3 network configuration described in the previous section). For example, roaming enables Station 1 to move from the AP 1 signal coverage area to the AP 2 signal coverage area without disconnecting from the network. The handover is achieved transparently; the Station 1 user would not realize he had moved from AP 1 to AP 2.

The requirements for a roaming environment are:

a) Multiple APs with overlapping signal coverage (see “Multiple AP Installation,” page 18)

b) The APs must be configured to have the same domain name (SSID) and security (WEP) settings (see “Encryption,” page 27).

c) The mobile stations must have the same domain name (SSID) and security (WEP) settings as the APs.

It is advisable that APs on different TCP/IP subnets be given different domain names to avoid roaming confusion (see the note below).

Note: For a mobile station to move between APs without losing its network link, the Roaming function must be enabled on the station, and the APs that the station roams to must be configured with the same domain name. If a station detects that the signal quality on the link to the current AP is poor, it will search for an AP in the same domain with better signal quality and automatically associate (establish a connection) with it. The station’s IP address, however, will not change. A TCP/IP router will not route packets to a mobile station that has associated with an AP on a different TCP/IP subnet. In other words, if your network consists of two subnets connected by a router, a mobile station may roam to a different subnet with the same domain name and then be unable to communicate with other network devices via TCP/IP. To avoid this problem, you must assign different domain names to different TCP/IP subnets.

Hardware Description

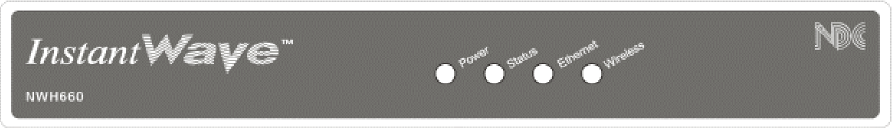


Figure 4. NWH660 Front Panel

LED Indicators

The NWH660's LEDs show the status of the unit and its connections.

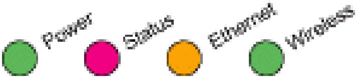


Figure 5. LED Indicators

LED	*Color*	*Meaning*
Power	Green	Off: Device not receiving power Blinking: Diagnostic test in progress On: Normal operation
Status	Red	Off: Normal operation On: Normal operation interrupted
Ethernet	Orange	Off: No Ethernet link On: Ethernet link up but idle Blinking: Ethernet activity
Wireless	Green	Off: No wireless link On: Wireless link up but idle Blinking: Wireless activity

Connectors and Switches

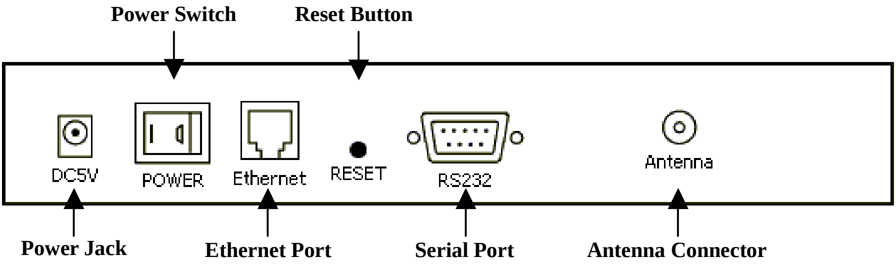


Figure 6. NWH660 Rear Panel

Item	*Function*
Power jack	DC 5V power input
Power switch	Device on/off
Ethernet port	RJ-45 jack for connection to 10Base-T Ethernet LAN
Reset button	If held down more than 3 seconds, reloads factory settings and restarts device. Power LED will blink during reset and then go off to indicate that button can be released.
Serial port	9-pin D-shell connector for RS-232 connection to computer running AP COMFig utility
Antenna connector	Reverse SMA connector for antenna

Hardware Pre-configuration

Before adding the NWH660 to an existing Ethernet network, you may need to set basic parameters — e.g., SSID, security settings (WEP), AP name, channel number, and IP address — to make the AP compatible with the existing network.

From the AP COMFig utility:

Follow the steps below to connect the AP to a PC for configuration:

step 1. Connect the supplied RS-232 cable to the AP's serial port and connect the other end to a serial port (COM port) on the PC.

step 2. Power up the AP.

Or from IWMS:

The NWH660's Ethernet port supports a speed of 10 Mbps. Using regular Category 3 or higher UTP/STP cable, you can connect it directly to a hub or switch.

step 3. Connect the NWH660 and your PCs/network devices to the Ethernet hub or switch.

step 4. Power up the NWH660.

Installing the AP Management Tools

step 1. Insert disk 1 in drive A and click ***Start/Run***. Type *a:/menu.exe* and click ***OK*** to open the main menu.

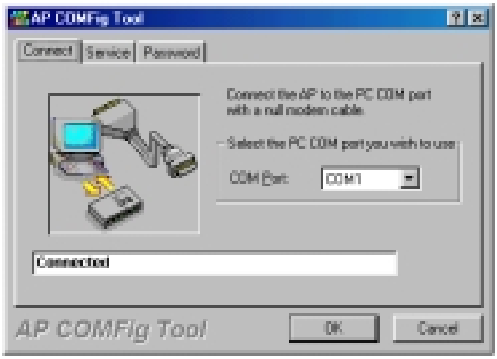
step 2. Click ***Install AP Management Tools*** to install the *AP COMFig Tool, InstantWave Management System (IWMS)* and *Trap Server* utility on your system.

Using the AP COMFig Tool

The AP COMFig Tool is a Windows-based utility used to configure the AP via a COM port connection between the AP and a PC. It provides the following functions:

- Sets AP parameters (e.g., IP address, domain name [SSID], security, etc.)
- Diagnoses the AP hardware and shows the results
- Upgrades the AP firmware
- Resets the AP configuration

To start the AP COMFig Tool, click ***Start/Programs/InstantWave High Rate AP/AP COMFig Tool***. The program opens with the *Connect* panel displayed. It will show *Connected* when a connection is made.



Connect the AP to the PC COM port with a null modem cable.

Select the PC COM port you wish to use

COM Port: COM1

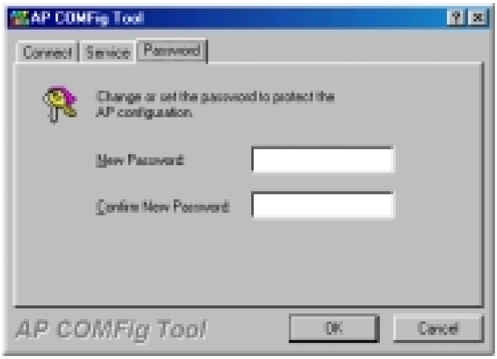
Connected

Figure 7. AP COMFig Tool/Connect

AP COMFig/Password

Click the *Password* tab to open the *Password* panel. Setting a password prevents unauthorized changes to the AP configuration settings.

Note: The password will be shared with the IWMS program on the same PC.



Change or set the password to protect the AP configuration.

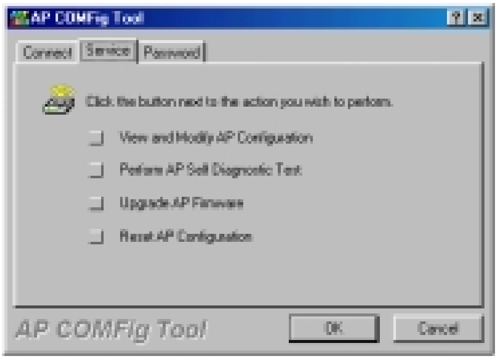
New Password:

Confirm New Password:

Figure 8. AP COMFig Tool/Password

AP COMFig/Service

After connecting with the AP, click the *Service* tab to open the *Service* panel (**Figure 9**). The *Service* panel provides access to AP management features.



Click the button next to the action you wish to perform.

□ View and Modify AP Configuration

□ Perform AP Self Diagnostic Test

□ Upgrade AP Firmware

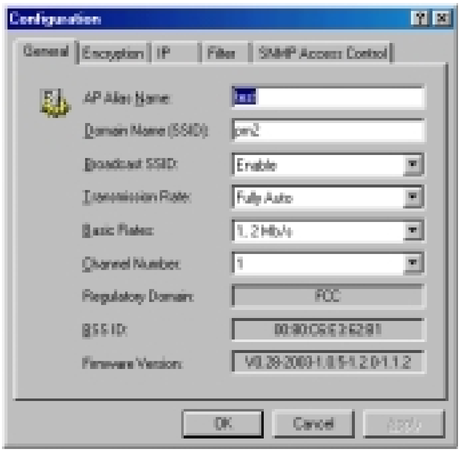
□ Reset AP Configuration

Figure 9. AP COMFig Tool/Service

Click the *View and Modify AP Configuration* button. The *Configuration* window will open (**Figure 10**).

General:

The *General* panel (**Figure 10**) is the first panel in the *Configuration* section.



AP Alias Name: test

Domain Name (SSID): pm2

Broadcast SSID: Enable

Transmission Rate: Fully Auto

Basic Rates: 1, 2 Mb/s

Channel Number: 1

Regulatory Domain: FCC

BSS ID: 00:90:C6:E2:62:81

Firmware Version: V0.29-2003-1.0.5-1.2.0-1.1.2

Figure 10. Configuration/General

On this panel, you can set and view general AP settings. These settings are explained in the table below.

AP Alias Name	Assigns the AP a unique human-friendly name that allows the AP to be easily identified.
Domain Name (SSID)	This is commonly called the domain name but is defined in the IEEE 802.11b wireless standard as SSID. Stations and APs in the same group must use the same domain name.
Transmission Rate	Sets the transmission rate at which data packets are transmitted by the AP.
Basic Rates	This value determines the basic rates used and reported for this BSS by the AP. The highest rate specified will be the rate that the AP will use when transmitting broadcast/multicast and management frames. Available options are: • 1 and 2 Mbps • All (1, 2, 5.5, and 11 Mbps)
Channel Number	You can change the channel number from here. Refer to the Appendix, page 73, for channels supported in each regulatory domain.
Secure SSID	Click to enable or disable the secure SSID option. • Blocks a connection request from a station without the correct SSID. • Hides the SSID in outgoing beacon frames. A site-survey tool will not find the SSID.
Regulatory Domain	Identifies the country where the AP is used. Each country has defined its available channel numbers and transmission power (see Appendix, page 73)
BSSID	This is the MAC ID of the AP
Firmware Version	The current AP firmware version

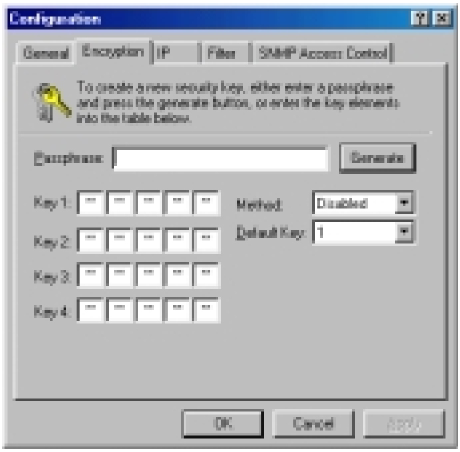
Important:

In a multiple cell network topology, overlapping and/or adjacent cells using different channels can operate simultaneously without interference if the frequency distance between the center frequencies is at least 30MHz. For example channels **1, 7, and 13** are non-overlapping frequency channels.

After making any changes, click the ***Apply*** button to make the changes effective immediately, without closing the dialog box, or click ***OK*** to accept the changes and close the box.

Encryption:

Data encryption provides more secure wireless data communications. Click the *Encryption* tab to create or change the security settings (**Figure 11**). The default is *Disabled* and initially the keys section will be blank.



To create a new security key, either enter a passphrase and press the generate button, or enter the key elements into the table below.

Method: Disabled

Default Key: 1

Figure 11. Configuration/Encryption

The dropdown *Method* box lists three options:

1. Disabled (default) - Disable data encryption
2. 40-bit WEP - Enable use of 40-bit WEP
3. 128-bit WEP - Enable use of 128-bit WEP

Key Generation - There are two ways to generate a security key.

The first is by entering any text in the *Passphrase* field. Click the ***Generate*** button. For 40-bit WEP, it will generate four keys, **Key 1**, **Key 2**, **Key 3,** and **Key 4**. Select a key number from the dropdown list of the *Default Key* box. If you do not manually select a key, key 1 will be selected. For 128-bit WEP, only one key will be generated. Click ***Apply***.

Another WEP key generation method is to insert the key values directly from the keyboard. Enter your own key into one of the *Key 1~4* fields. Select that field number in the *Default Key* field. If the WEP key is enabled on the AP, all clients must use the same WEP key. Click ***OK***.

IP:

The InstantWave NWH660 is a DHCP client. It will automatically try to get IP settings from a DHCP server on the LAN. If it fails to get IP settings from a DHCP server, it will assign itself an IP address in the 169.254.x.x range.

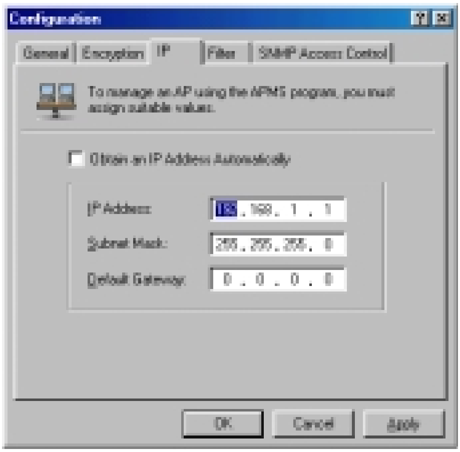
From the IP panel (**Figure 12**), you can assign an NWH660 a fixed IP address by unchecking the *Obtain IP from DHCP* box. This lets you view or modify the access point's TCP/IP address, configure its subnet mask, or add a default gateway (see note below).

Note: An AP will send SNMP response packets (confirmation packets) directly to an IWMS PC if the two devices are on the same TCP/IP subnet. If an SNMP response packet from an AP is destined for an IWMS PC on another subnet, the SNMP response packet needs to go through a router or similar gateway. The Default Gateway setting is the IP address of such a gateway. If you set the correct default gateway, then you can use an IWMS PC physically located on a different subnet to manage this AP.

If you assign a fixed IP address to an NWH660, make sure that all NWH660s within the same network have IP addresses on the same TCP/IP subnet.

Obtain IP from DHCP	Automatically retrieves an IP address for the NWH660 from a Dynamic Host Configuration Protocol (DHCP) server. This option is enabled by default
IP Address	Manually assigns an IP address to the NWH660
Subnet Mask	Manually assigns a subnet mask to the NWH660
Default Gateway	Manually specifies the default gateway IP address (if required)

If you wish to change the defaults, set each AP to its new IP address before introducing it on the running network.



To manage an AP using the APMS program, you must assign suitable values.

□ Obtain an IP Address Automatically

IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255 . 255 . 255 . 0

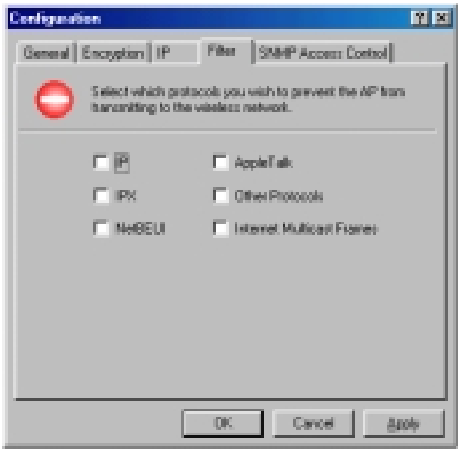
Default Gateway: 0 . 0 . 0 . 0

Figure 12. Configuration/IP

After making any changes, click the ***Apply*** button to make the changes effective immediately, without closing the dialog box, or click ***OK*** to accept the changes and close the box.

Filter:

The next tab on the dialog box is *Filter* (**Figure 13**). This is a one-way protocol filtering mechanism that prevents the AP from transmitting specified protocols from a wired Ethernet LAN into the wireless LAN. If you do not require particular protocols on the wireless part of your network, you can save bandwidth by enabling the protocol filter.



Select which protocols you wish to prevent the AP from transmitting to the wireless network.

□ IP
□ IPX
□ NetBEUI
□ AppleTalk
□ Other Protocols
□ Internet Multicast Frames

Figure 13. Configuration/Filter

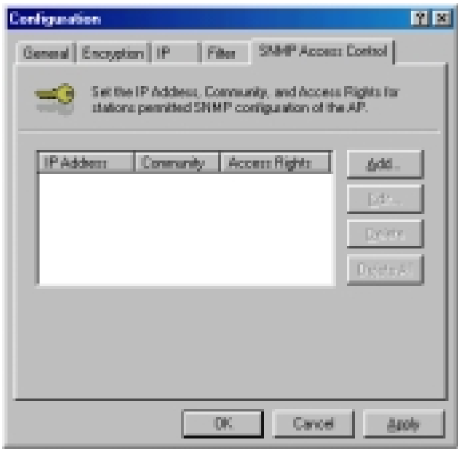
From the *Filter* panel, some, all, or none of the protocols listed may be selected for filtering out:

- IP Protocol
- IPX Protocol
- NetBEUI Protocol
- AppleTalk Protocol
- Other Protocols
- Internet Multicast Frames

After selecting a protocol to be filtered, click the ***Apply*** button to make the changes effective immediately, without closing the dialog box, or click ***OK*** to accept the changes and close the box.

SNMP Access Control:

SNMP Access Control is the next tab on the box (**Figure 14**).

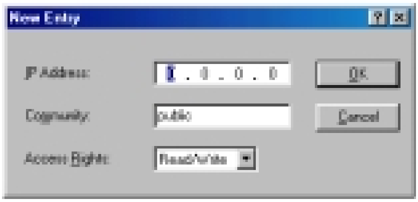


Set the IP Address, Community, and Access Rights for stations permitted SNMP configuration of the AP.

Figure 14. Configuration/SNMP Access Control

The AP's access control is managed by a control table on the AP. The first time this box is opened, the table will be empty. This means that there are no restrictions on who can access and reconfigure the AP and any user may modify the AP's operation. To avoid chaos on the network, access to the AP configuration should be restricted to only those for whom it is necessary.

Click ***Add*** to open the *New Entry* dialog box (**Figure 15**).



IP Address: 0 . 0 . 0 . 0

Community: public

Access Rights: Read/Write

Figure 15. New Entry

Two levels of access are available:

Read	Read-only rights. The user may read everything except the Access Control settings, but cannot alter anything
Read/Write	The user may read and alter all settings

Enter your IP address and then set your own access rights to Read/Write (see the following note).

Note: Do not set all the stations in the Access Control table to Read-only. Once this is set and enabled, it will be difficult to modify the AP. Should this situation occur, use the AP COMFig utility to reset the configuration.

To set a stations access rights, enter a station's IP address and community string (the community string is used as a password to access the AP) and choose *Read* or *Read/Write*.

When all the settings are made, click ***OK*** to return to the *Access Control* panel. On the *Access Control* panel, click the ***Apply*** button to make the changes effective immediately, without closing the dialog box, or click ***OK*** to accept the changes and close the box.

Perform AP Self Diagnostic Test

On the *Service* panel, click *Perform AP Self Diagnostic Test*. The *Hardware Diagnosis* window will open (**Figure 16**).

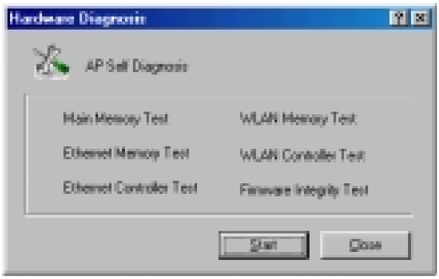


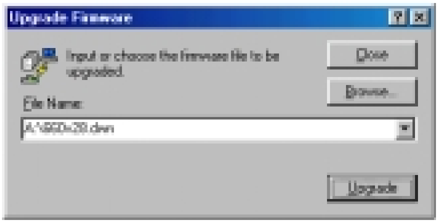
Figure 16. Hardware Diagnosis

Click ***Start*** and the tests will commence. As each item is tested, a yellow arrow will appear alongside it. If the test is successful, the arrow will change to a green check mark. If a failure occurs, an “X” will appear. You can click ***Cancel*** at any time to stop the tests. When the tests are finished, the ***Cancel*** button will change to a ***Close*** button. Click ***Close*** to return to the *Service* panel.

Upgrade AP Firmware

From time to time updated firmware is released and may be downloaded from our website at http://www.ndc.com.tw/support/support.htm

The updated firmware may be installed via a COM port using the AP COMFig tool. Click on ***Upgrade AP Firmware*** (Figure 9, page 24). The *Upgrade AP Firmware* dialog box will open (**Figure 17**).


Input or choose the firmware file to be upgraded.

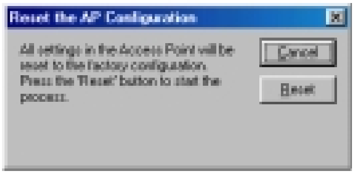
File Name: A:\800x28.dwn

Figure 17. Upgrade AP Firmware

Use the *Browse* button to choose the file to be uploaded to the AP, or type the file location and name in the *File Name* field. The ***Upload*** button will then become enabled. Click ***Upload***. The new firmware will be loaded into the AP's flash memory area. When the file transfer is complete, click ***OK*** to begin the AP's internal firmware updating process.

Reset AP Configuration

Click ***Reset AP Configuration*** to open the dialog box shown in Figure 18, and click ***Reset*** to restore the factory default configuration to the access point.



Reset the AP Configuration

All settings in the Access Point will be reset to the factory configuration. Press the 'Reset' button to start the process.

Figure 18. Reset the AP Configuration

InstantWave Product Placement Guidelines

A few tips to mention that are particularly significant in a radio wave communications system:

1. Radio waves reflect or refract from buildings, walls, metal furniture, or other objects. This could result in performance degradation due to the fluctuation of the received signal.

2. Microwave ovens use the 2.45-GHz frequency band. InstantWave also functions in the 2.4 to 2.5-GHz band, and therefore shares some of the band with microwave ovens. This means that when a nearby microwave oven is in use, it may interfere with InstantWave signals, resulting in performance degradation on the wireless network.

For the best performance, follow the guidelines below in placing the product:

- Place as high as possible, in as open an area as possible
- Avoid placing the AP (especially the antenna) close to metal objects (e.g. file cabinets, metal cubicles, etc.)
- Keep APs and stations as far away as possible from microwave ovens (10 meters min. is advisable)

When you have decided on a location, follow the steps below to complete the installation.

step 1. Screw the antenna into the back of the AP. Place the AP in the chosen location.

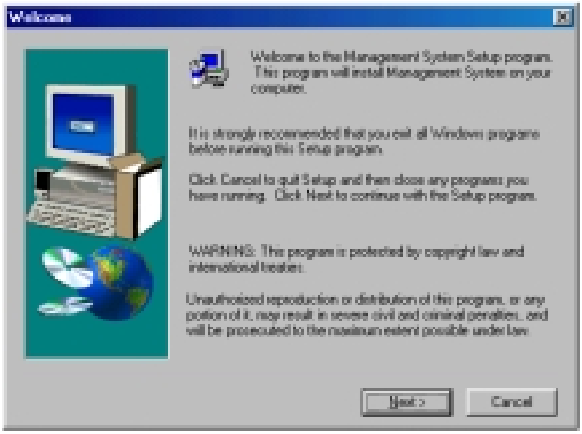
step 2. Connect one end of an Ethernet network cable to the UTP port of the AP, and the other end to an Ethernet hub or switch.

step 3. Connect the power adapter to the electricity outlet and then to the access point’s DC-In jack.

step 4. Turn on the AP’s power switch.

Installing the InstantWave Management System

step 1. Insert the InstantWave Management System disk into floppy drive A:. Click ***Start/Run*** and type *a:\setup.exe*. The setup program will prepare the InstallShield Wizard and then display a *Welcome* window.



Welcome

Welcome to the Management System Setup program. This program will install Management System on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup program.

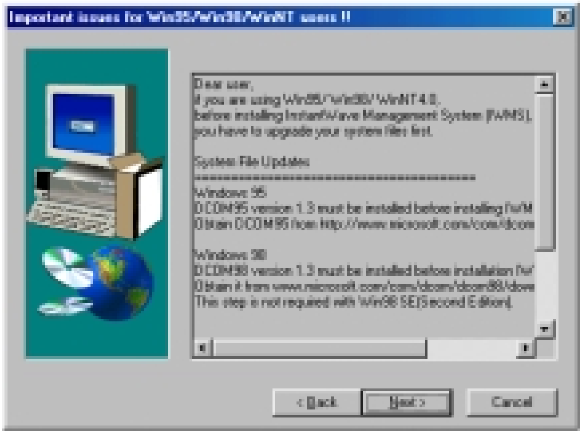
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Figure 19. Welcome

step 2. Click ***Next***.



Important issues for Win95/Win98/WinNT users !!

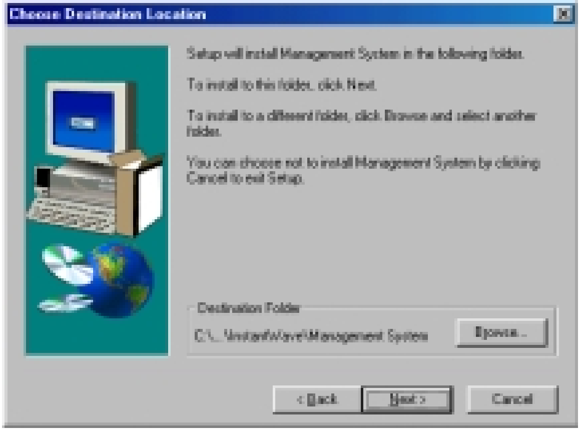
Dear user,
If you are using Win95/Win98/WinNT 4.0,
before installing InstantWave Management System (IWMS),
you have to upgrade your system files first.

System File Updates
==
Windows 95
DCOM95 version 1.3 must be installed before installing IWM
Obtain DCOM95 from http://www.microsoft.com/com/dcom

Windows 98
DCOM98 version 1.3 must be installed before installation IW
Obtain it from www.microsoft.com/com/dcom/dcom98/dow
This step is not required with Win98 SE(Second Edition).

Figure 20. Important Issues

step 3. Older operating systems may need to update some system files to function correctly with the InstantWave Management System. If required, follow the on-screen instructions to download the required file (Figure 20). Click ***Next*** to open the ***Choose Destination Location*** window (Figure 21).



Choose Destination Location

Setup will install Management System in the following folder.

To install to this folder, click Next.

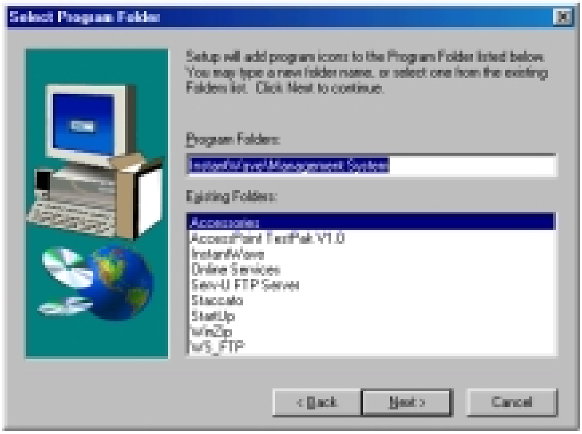
To install to a different folder, click Browse and select another folder.

You can choose not to install Management System by clicking Cancel to exit Setup.

Destination Folder
C:\...\InstantWave\Management System

Figure 21. Choose Destination Location

step 4. Click ***Next***.



Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing Folders list. Click Next to continue.

Program Folders:

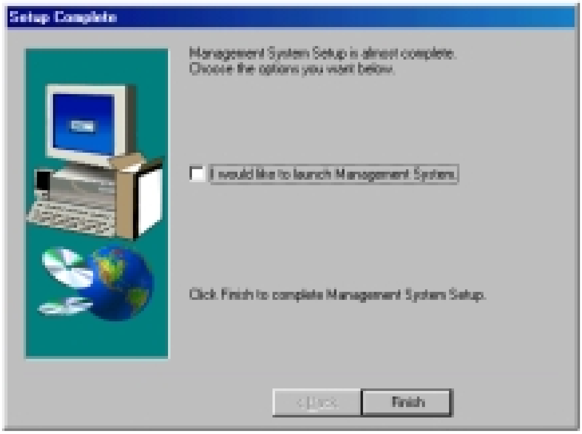
InstantWave\Management System

Existing Folders:

Accessories
AccessPoint TestPak V1.0
InstantWave
Online Services
Serv-U FTP Server
Staccato
StartUp
WinZip
WS_FTP

Figure 22. Select Program Folder

step 5. Click ***Next*** again (Figure 22).



Management System Setup is almost complete.
Choose the options you want below.

□ I would like to launch Management System.

Click Finish to complete Management System Setup.

Figure 23. Setup Complete

step 6. Check “I would like to launch InstantWave Management System” and click ***Finish***.

Using the InstantWave Management System

Once the NWH660 is connected to an Ethernet network, a network administrator can connect to it from any PC on the same network via the InstantWave Management System (IWMS) utility.

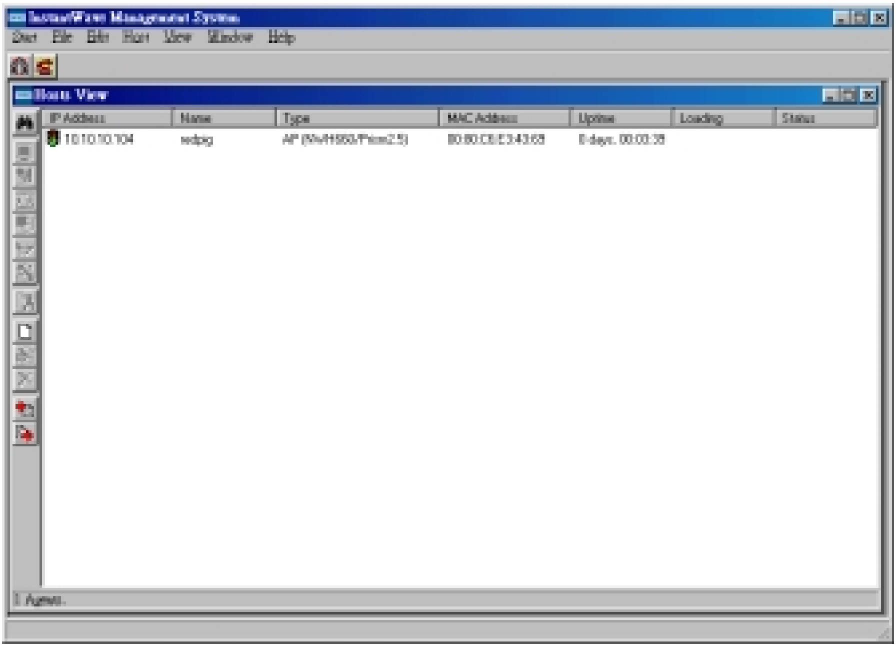
The IWMS utility is a Windows-based SNMP management tool allowing network administrators to remotely configure and monitor the NWH660 through both an Ethernet and a wireless connection. To launch the IWMS utility:

step 1. Click ***Start/Programs/InstantWave/Management System/InstantWave Management System***. The main IWMS window will open. Click ***Start/Start Hosts View***.

Auto-Discovery

This discovery protocol can discover all InstantWave wireless operating devices connected to the Ethernet LAN within the same subnet.

step 1. Click the Auto Discovery icon (a pair of binoculars) on the left side of the Hosts View window. All working InstantWave devices will automatically be discovered (Figure 24).



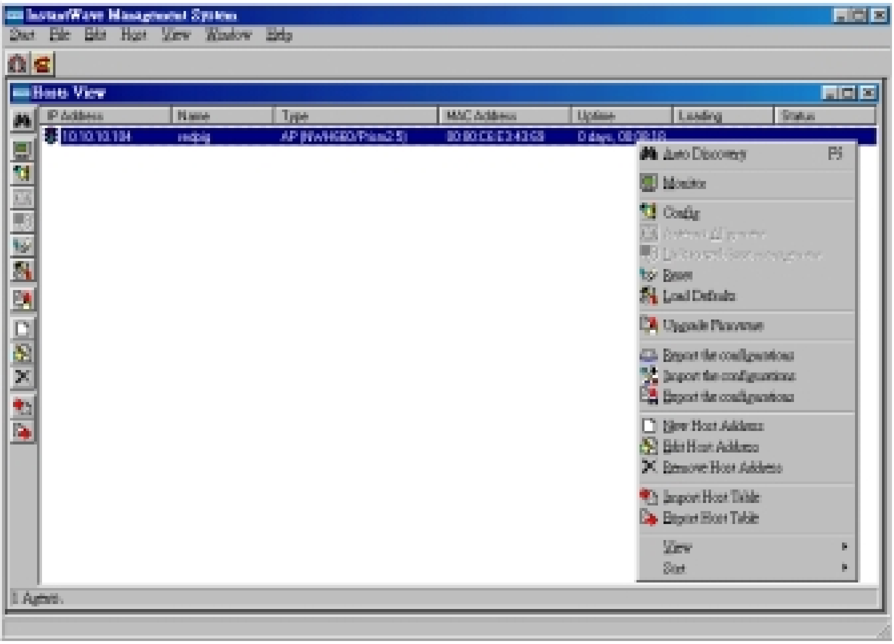
InstantWave Management System
Start File Edit Host View Window Help
Hosts View
1 Agents.

IP Address	Name	Type	MAC Address	Uptime	Loading	Status
10.10.10.104	redpig	AP (NWH660/Prism2.5)	00:80:C8:E3:43:68	0 days, 00:03:39		

Figure 24. InstantWave Management System

step 2. Select one of the wireless devices on the list. The utility buttons on the left toolbar will be enabled (Figure 25).

step 3. Right-clicking on a particular device will open a popup menu offering the same functions as the toolbar.



IP Address	Name	Type	MAC Address	Uptime	Loading	Status
10.10.10.104	redpig	AP (NWH660/Prism2.5)	00:60:C6:E3:43:68	0 days, 08:08:18		

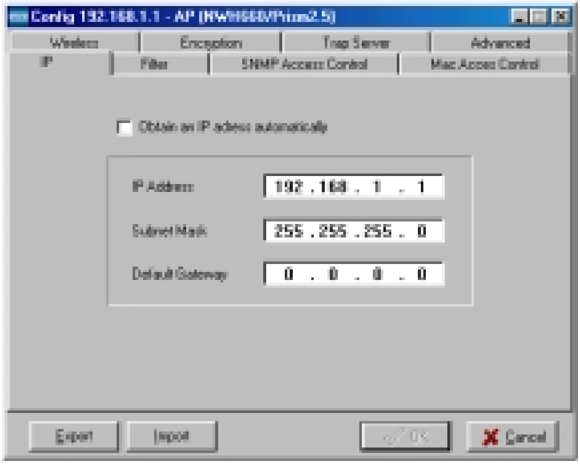
Figure 25. Popup Menu

Configuration

step 1. For configuration, select the AP (NWH660) on the *Hosts View* window (Figure 24)

step 2. Right-click the NWH660 to open the popup menu

step 3. Click ***Config*** to go to the configuration dialog box (Figure 26)



□ Obtain an IP adress automatically

IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 0 . 0 . 0 . 0

Figure 26. IP Configuration

IP

IP Address Setting: The InstantWave NWH660 is a DHCP client. It will automatically ask the DHCP server to assign it an IP address. An administrator can assign a fixed IP to an NWH660 by unchecking the *Obtain IP from DHCP* box (Figure 26). You may also configure a subnet mask and add a default gateway.

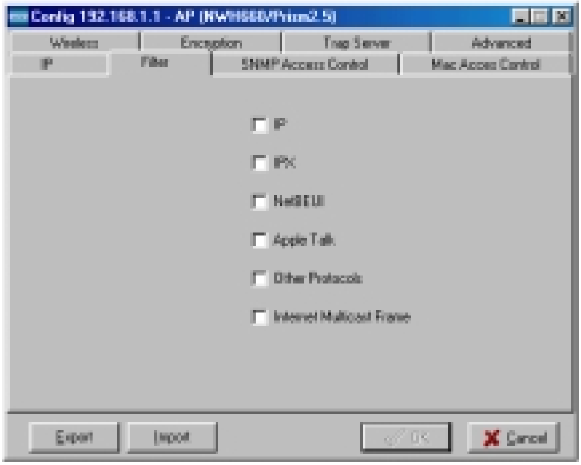
If you assign a fixed IP address to an NWH660, make sure that all NWH660s within the same network have the same TCP/IP subnet address.

Obtain IP from DHCP	Automatically retrieves an IP address for the NWH660 from a Dynamic Host Configuration Protocol (DHCP) server. This option is enabled by default
IP Address	Manually assigns an IP address to the NWH660
Subnet Mask	Manually assigns a subnet mask to the NWH660
Default Gateway	Manually specifies the default gateway IP address (if required)

Note: An NWH660 will directly transfer SNMP response packets (confirmation packets) to an IWMS PC if it is within the same LAN (the same subnet mask). If an SNMP response packet from an NWH660 is destined for an IWMS PC on *another LAN, the SNMP response packet needs to be forwarded by routers. The default gateway is the closest router to the NWH660. If the correct default gateway is set, you can use an IWMS manager (i.e. a PC running IWMS) physically located in a different subnet to manage this NWH660.*

Filter

The next panel in the configuration dialog box is *Filter* (Figure 27).



□ IP
□ IPX
□ NetBEUI
□ Apple Talk
□ Other Protocols
□ Internet Multicast Frame

Figure 27. Configuration/Filter

This is a one-way protocol filtering mechanism that prevents the NWH660 from transmitting specified protocols packet from a wired Ethernet LAN into the wireless LAN. If you do not require particular protocols on the wireless part of your network, you can save bandwidth by enabling the protocol filter.

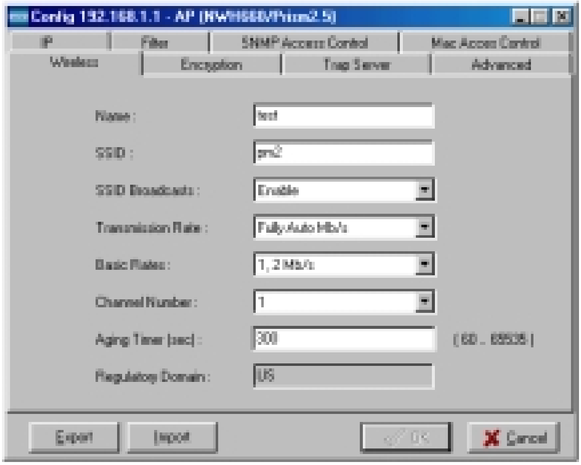
From the ***Filter*** panel, some, all, or none of the protocols listed may be selected for filtering out:

- IP Protocol
- IPX Protocol

- NetBEUI Protocol
- AppleTalk Protocol
- Other Protocols
- Internet Multicast Frames

Wireless

The *Wireless* panel (Figure 28) provides access to the Wireless settings.



Name : test

SSID : prn2

SSID Broadcasts : Enable

Transmission Rate : Fully Auto Mb/s

Basic Rates : 1, 2 Mb/s

Channel Number : 1

Aging Timer (sec) : 300 (60 .. 65535)

Regulatory Domain : US

Figure 28. Configuration/Wireless

These settings are explained in the following table.

Name	Assigns the NWH660 a unique name that allows the AP to be easily identified on the network.
SSID	Identifies the wireless LAN domain that this AP is in. A domain is generally composed of wireless APs you are most likely to communicate with. You can type an existing domain name or create a new one that contains up to 32 characters.

Broadcast SSID	Click to enable or disable the SSID broadcasting feature: If disabled, the NWH660 will: • Blocks a connection request from a station without the correct SSID • Hides the SSID in outgoing beacon frames. A site-survey tool will not find the SSID
Transmission Rate	Sets the transmission rate at which the data packets are transmitted by the NWH660. In high-interference environments a lower rate can increase overall transmission speed by reducing resends of lost packets
Basic Rates	This value determines the basic rates used and reported for this BSS by the NWH660. The highest rate specified is the rate that the NWH660 will use when transmitting broadcast/multicast and management frames. Available options are: • 1 and 2 Mbps • All (1, 2, 5.5, and 11 Mbps)
Channel Number	You can change the channel number from here. Refer to the Appendix, page 73, for channels supported in each regulatory domain. If the "auto" option is selected, the access point can choose the best available radio channel automatically.
Regulatory Domain	Identifies the country where the NWH660 is used. Each country has defined its available channel numbers and transmission power (see Appendix, page 73)

Important:

In a multiple cell network topology, overlapping and/or adjacent cells using different channels can operate simultaneously without interference if the difference between the center frequencies is at least 30 MHz. For example, channels 1, 7, and 13 are non-overlapping frequency channels.

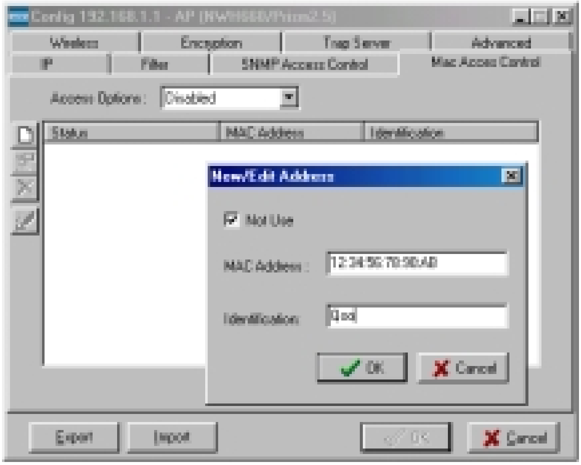
MAC Access Control

This feature lets you limit access to the network through the access point. You can list up to 1000 stations that are to be granted or denied access. A drop-down box lets you select the method of access control:

- **Disabled**: Disable MAC-address access control. This is the default setting.
- **Accepted List**: Only wireless stations whose MAC addresses are on the list are allowed to connect through the access point.
- **Denied List**: Wireless stations whose MAC addresses are on the list are prevented from connecting through the access point.

To add a wireless station to the list, click the New MAC Address icon (a sheet of paper with one corner folded) on the left side of the MAC Access Control panel. You will be prompted to enter:

- The wireless station's MAC address.
- A name for the station.
- The status of the station's entry on the list. Check the *Not Use* box to reverse the effect of access control on this station (for example, to deny access if Accepted List [see above] is selected). Clear the box to let the selected method of access control take effect on this station. This box has no effect if MAC-address access control is disabled.



Access Options: Disabled

☑ Not Use

MAC Address: 12:34:56:78:90:AB

Identification: Test

Figure 29. Configuration/Mac Access Control

Wireless stations registered in the MAC Address Control Table can be individually turned on or off. For example, if you have enabled the Accepted List option, you can check the Not Use option for any listed station; the access point will then refuse all connection attempts from that station.

***MAC Address List*:**

Status	Disables or enables an individual entry
Address	The MAC address of a wireless station
Identifier	Identification for the wireless station

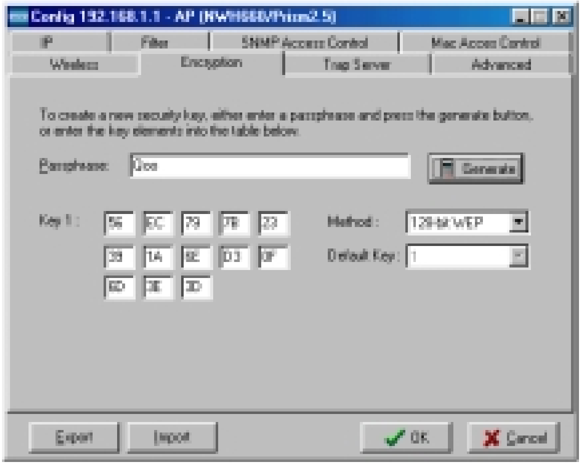
New: Click ***New*** to create a new entry in the MAC Address List.

Delete: Click ***Delete*** to remove a selected MAC address from the list.

Delete All: Click ***Delete All*** to remove all of the MAC addresses from the list.

Encryption

Click the *Encryption* tab (Figure 30) to set up the security options.



To create a new security key, either enter a passphrase and press the generate button, or enter the key elements into the table below.

Passphrase: Qoo

Key 1 : 56 EC 79 7B 23 39 1A 9E D3 0F 6D 3E 3D

Method : 128-bit WEP

Default Key : 1

Figure 30. Configuration/Encryption

The default setting is *Disabled* and initially the key sections are blank.

The pull-down *Method* box lists three options:

- Disabled (default) - Disable data encryption
- 40-bit WEP - Enable use of 40-bit WEP
- 128-bit WEP - Enable use of 128-bit WEP

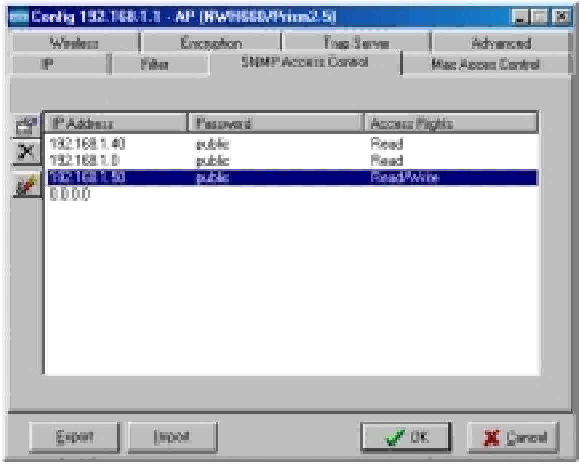
Key Generation - There are two ways to generate a security key. The first is by entering any text in the *Passphrase* field. Click the ***Generate*** button. For 40-bit WEP, it will generate four keys, Key 1, Key 2, Key 3, and Key 4. Select a key number from the dropdown list of the *Default Key* box. If you do not manually select a key, key 1 will be selected. For 128-bit WEP, only one key will be generated. Click ***OK***.

Another WEP key generation method is to insert the key values directly from the keyboard. Enter your own key into one of the *Key 1~4* fields. Select that field number in the *Default Key* field.

SNMP Access Control

The AP contains an SNMP access table to limit access to its configurations. By default there is no restriction on accessing the AP. To avoid chaos on the network, access to the NWH660 configuration should be restricted to only those who require access.

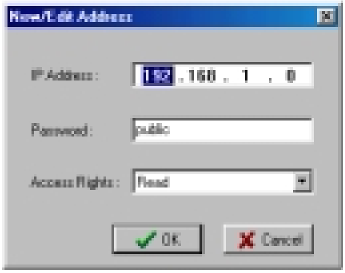
When you select SNMP Access Control, the system will display four blank wireless devices for setting (maximum of 4 SNMP devices can be set). Right-click on a device in the list and click ***Edit Address*** (Figure 31).



IP Address	Password	Access Rights
192.168.1.40	public	Read
192.168.1.0	public	Read
192.168.1.50	public	Read/Write
0.0.0.0		

Figure 31. Configuration/SNMP Access Control

The *New/Edit Address* dialog box will open (Figure 32).



IP Address: 192 . 168 . 1 . 0

Password: public

Access Rights: Read

Figure 32. New/Edit Address

Two levels of access may be assigned:

Read	Read-only rights. The user may read everything except the Access Control settings, but is not allowed to alter anything
Read/Write	The user may read and alter all settings

Enter your PC’s IP address and then set your own access rights to Read/Write (see the following note).

Note: Do not set all the stations in the Access Control table to Read only. Once this is set and enabled, it will be impossible to modify the NWH660. Should this situation occur, press the Reset button on the rear of the NWH660 to restore the factory configuration.

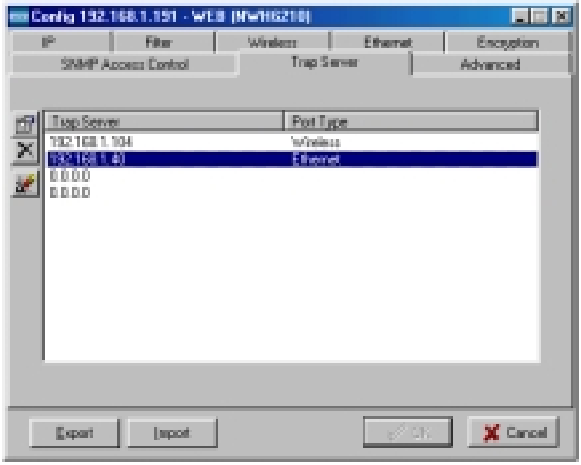
To set a stations access rights, enter a station’s IP address and password (the community string is used as a password to access the NWH660) and choose *Read* or *Read/Write*.

When a setting is made, click ***OK***. Repeat the procedure for the next PC. When all settings are made, click ***OK*** in the configuration dialog boxto make the changes effective.

Trap Server

When the NWH660 is powered on, or an Ethernet port becomes active, an event log will be generated indicating the time, the IP address of the reporting NWH660, and the event. You can save, open, and delete log files from the *File* menu.

To assign a trap server, click *Trap Server* (Figure 33).

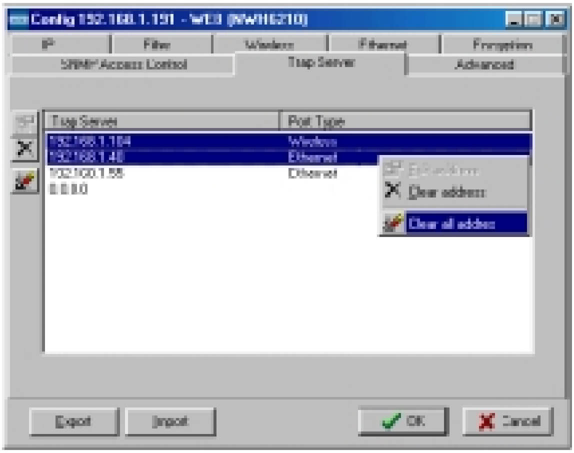


Trap Server	Port Type
192.168.1.104	Wireless
192.168.1.40	Ethernet
0.0.0.0	
0.0.0.0	

Figure 33. Configuration/Trap Server

Assign a station as a trap server by entering its IP address and network port type. Click ***Edit address***.

To remove a trap server from the list, highlight it and click ***Clear address***. Click ***Clear all address*** to remove all assigned trap servers from the list (Figure 34).



Trap Server	Port Type
192.168.1.104	Wireless
192.168.1.40	Ethernet
192.100.1.55	Ethernet
0.0.0.0	

Figure 34. Configuration/Clear all Address

To view trap log information, click the Start Trap View icon (a ringing telephone) in the upper left corner of the main IWMS window (see Figure 24, page 40). A window such as that shown below will appear (Figure 35).

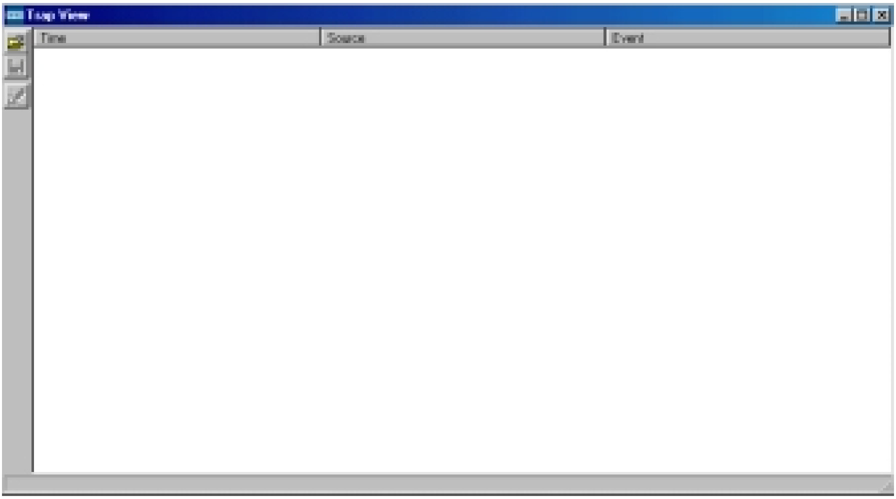
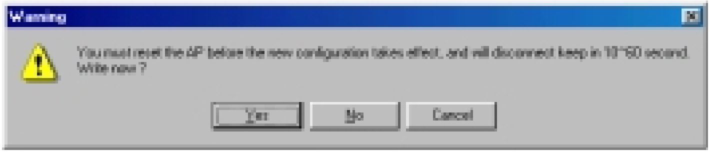


Figure 35. Trap View

The log shows when an NWH660 was powered on, or an Ethernet port became active, and the IP address of the reporting NWH660. You can save, open, and delete log files through the *File* menu.

Important:

Once all configurations have been completed, click ***OK***. You will be reminded that a reset is required to make the changes effective. Click ***Yes***.



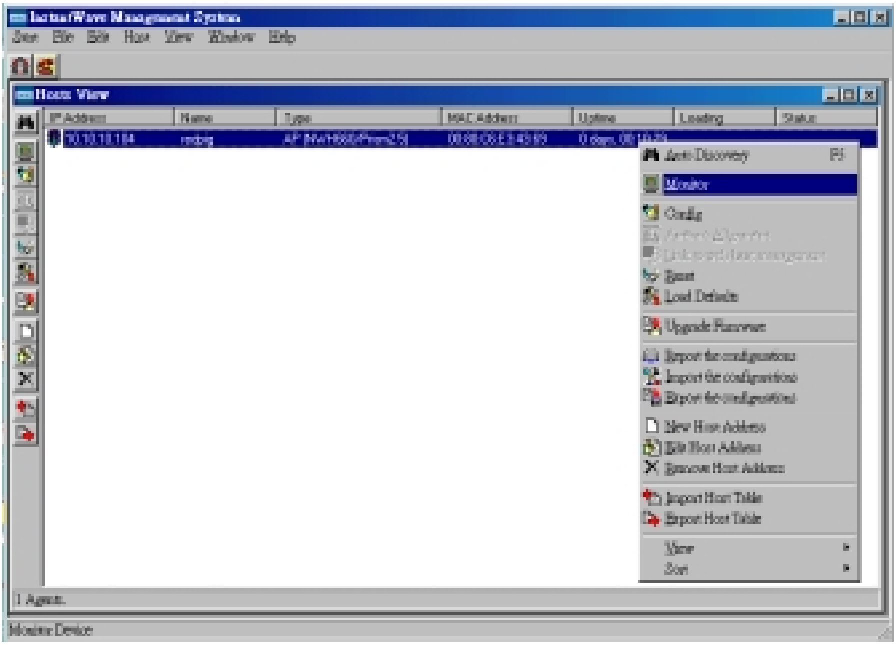
You must reset the AP before the new configuration takes effect, and will disconnect keep in 10~60 second.
Write now ?

Figure 36. Warning

Monitor

The Monitor tool allows the NWH660's status, Ethernet statistics, wireless statistics, and other configuration information to be viewed/monitored.

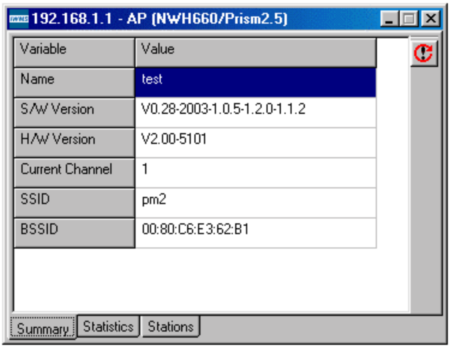
In the *Hosts View* window (Figure 37), select a device and click the ***Monitor*** button on the toolbar or on the popup menu.



IP Address	Name	Type	MAC Address	Uptime	Loading	Status
10.10.10.184	redbig	AP (NWH660/Prism2.5)	00:80:C8:E3:43:B9	0 days, 00:10:20		

Figure 37. Monitor

An information window will appear. The first of three panels in this window, the Summary panel, will be visible (Figure 38).



192.168.1.1 - AP (NWH660/Prism2.5)

Variable	Value
Name	test
S/W Version	V0.28-2003-1.0.5-1.2.0-1.1.2
H/W Version	V2.00-5101
Current Channel	1
SSID	pm2
BSSID	00:80:C6:E3:62:B1

Figure 38. Monitor/Summary

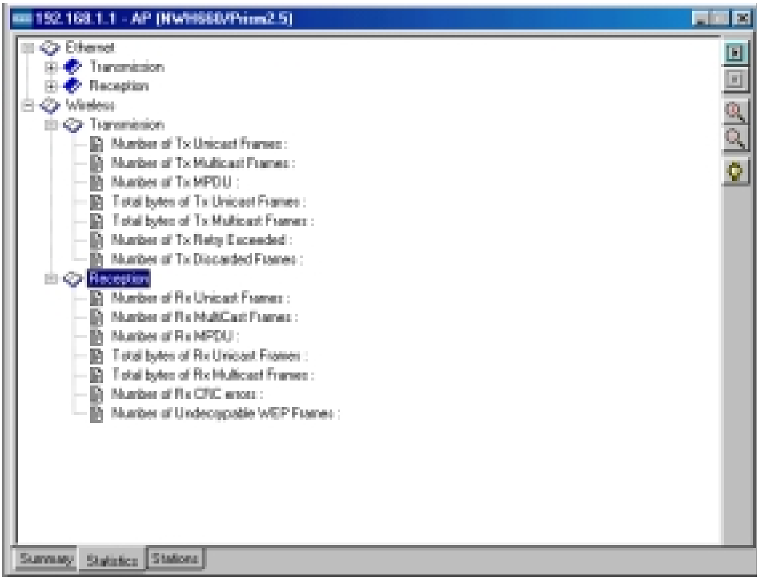
Summary Information

The information shown is read-only.

Device Name	IWMS system default category name
Name	Human-friendly name assigned by the user for easier identification
S/W Version	Shows the device software version number
H/W Version	Shows the device hardware version number
Channel	Shows the wireless channel currently in use on the device
Current BSSID	Shows the BSSID of the device (same as the device MAC address)

Statistics

The Statistics window shows both Ethernet and wireless transmission/reception statistics. To refresh the statistics, click on the ▸ button to continually refresh information. Click on the ■ button to stop update information.

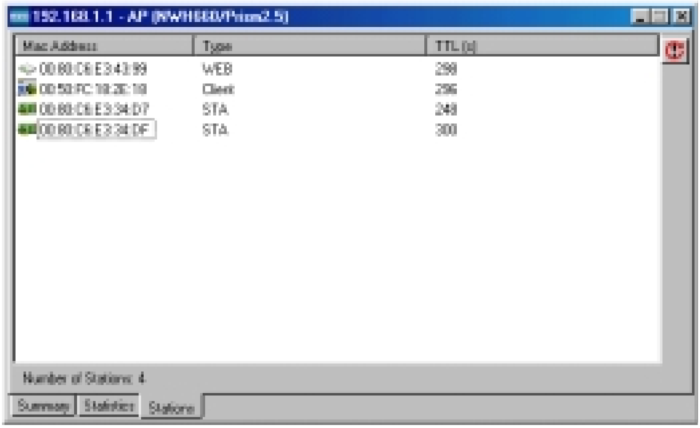


192.168.1.1 - AP (NWH660/Prism2.5)

- Ethernet
  - Transmission
  - Reception
- Wireless
  - Transmission
    - Number of Tx Unicast Frames :
    - Number of Tx Multicast Frames :
    - Number of Tx MPDU :
    - Total bytes of Tx Unicast Frames :
    - Total bytes of Tx Multicast Frames :
    - Number of Tx Retry Exceeded :
    - Number of Tx Discarded Frames :
  - Reception
    - Number of Rx Unicast Frames :
    - Number of Rx MultiCast Frames :
    - Number of Rx MPDU :
    - Total bytes of Rx Unicast Frames :
    - Total bytes of Rx Multicast Frames :
    - Number of Rx CRC errors :
    - Number of Undecryptable WEP Frames :

Figure 39. Monitor/Statistics

The *Connected Wireless Stations* window lists all the currently associated wireless station’s Media Access Control (MAC) addresses. When finished viewing, click **X** to close the window.



192.168.1.1 - AP (NWH660/Prism2.5)

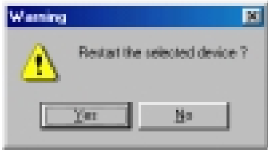
Mac Address	Type	TTL (s)
00:80:C6:E3:43:99	WEB	298
00:50:FC:18:2E:18	Client	296
00:80:C6:E3:34:D7	STA	248
00:80:C6:E3:34:DF	STA	300

Number of Stations: 4

Figure 40. Monitor/Stations

Reset

Resetting the NWH660 will take about 30 seconds (Figure 41).



Restart the selected device ?

Figure 41. Reset the AP Configuration

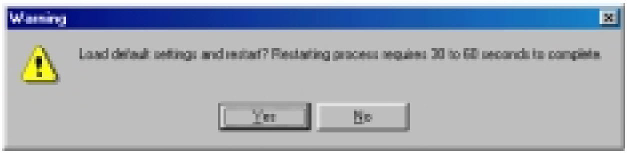
During this period, the IWMS program will not be able to query the NWH660 via the SNMP protocol and the NWH660 will not be available to its client stations.

If you try to access the device, the IWMS program will display the message "Timeout! No response from agent . . ."

Load Default

Click *Load Default* if you want to return the device to its factory default settings.

A warning dialog box will open (Figure 42).



Load default settings and restart? Restarting process requires 30 to 60 seconds to complete.

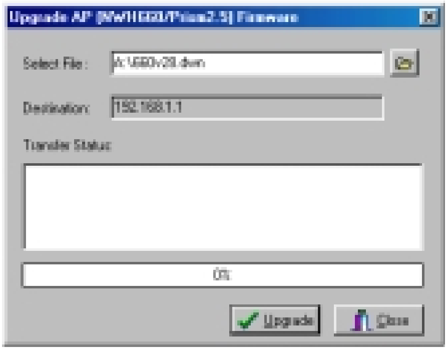
Figure 42. Load Default

Click ***Yes*** to return the NWH660 to the factory default settings.

Note: The NWH660 will be reset to complete the 'Load Default' operation.

Upgrade Firmware

The NWH660's embedded software is contained in "flash" ROM, and can be updated over your LAN via the IWMS program. To download new embedded software to the device, click *Upgrade Firmware*. The *Upgrade Firmware* dialog box will open (Figure 43).



Upgrade AP [NWH660/Prism2.5] Firmware

Select File : A:\660v28.dwn

Destination: 192.168.1.1

Transfer Status:

0%

Figure 43. Upgrade Firmware

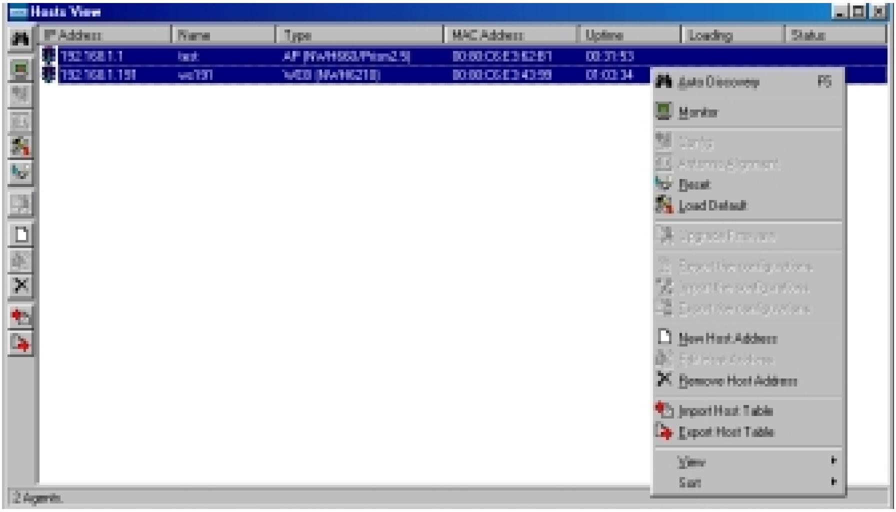
Browse for the file to be uploaded to the NWH660, or type the path and file name into the *Select File* field.

The *Upgrade* button will then become enabled. Click ***Upgrade*** to start downloading the file to the NWH660. The IWMS and the NWH660's built-in Trivial File Transfer Protocol (TFTP) client/server will load the new executable into the NWH660's flash ROM area. If the download activity fails, an error message will be shown in the message box. Once the file transfer is complete, click ***Close*** to close the window.

Advanced Settings

Batch mode operation

In order to maximize the efficiency of wireless LAN management, you can use batch mode operation to manage selected APs or WEBs. You can sort InstantWave devices by device type first. Then select the multiple APs or WEBs you would like to manage. Next, click the right mouse button to open the tool bar; then choose the functional tool you would like to use to work on these specific APs or WEBs.


Hosts View

IP Address	Name	Type	MAC Address	Uptime	Loading	Status
192.168.1.1	test	AP (IWN1553/Prism2.5)	00:80:C6:E3:62:B1	00:31:53		
192.168.1.151	ws151	WEB (IWN6218)	00:80:C6:E3:43:59	01:03:34		

2 Agents.

Figure 44. Batch Mode Operation List

Manage IWMS Host Table

Partition the network according to the physical location

The Host Table is a very powerful function to support the massive deployment of InstantWave products. You can combine several APs toghther with WEBs to form a group with a specific Host Table name so that you can divide the wireless network into many small groups. A wireless LAN in the hotel application will be a typical example.

InstantWave Product	Device Type	Alias Name	Host Table Name	Explanation
NWH660	AP	AP1-A-1F	A-1F	AP on first floor of building A
NWH660	AP	AP2-A-1F	A-1F	AP on first floor of building A
NWH6210	WEB	Room111	A-1F	AP on first floor of building A
NWH6210	WEB	Room112	A-1F	AP on first floor of building A
NWH660	AP	AP1-B-1F	B-1F	AP on first floor of building B
NWH660	AP	AP2-B-1F	B-1F	AP on first floor of building B
NWH6210	WEB	Room111	B-1F	AP on first floor of building A
NWH6210	WEB	Room121	B-1F	AP on first floor of building A

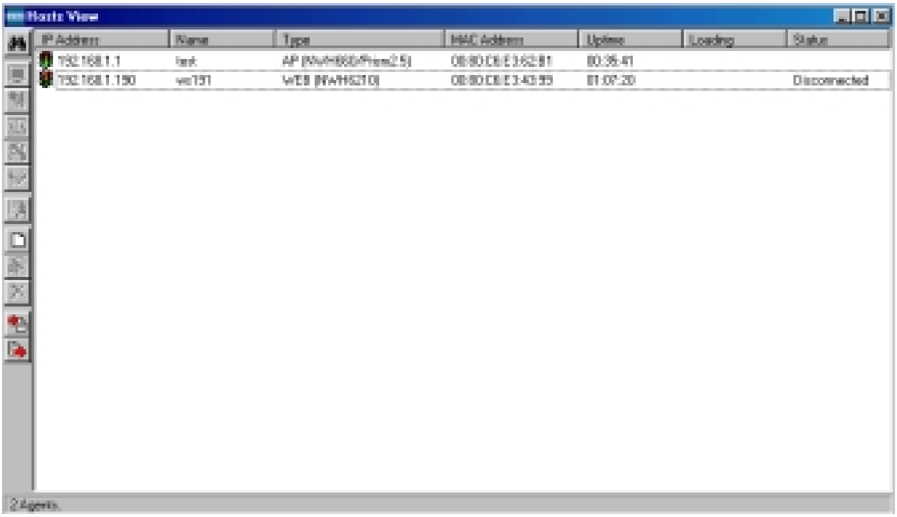
The wireless LAN is installed on the first floor of building A and the first floor of building B. You can assign a different Host Table for each wireless installation group. Once the wireless LAN is divided into many small groups. You can easily manage each wireless LAN group by managing its Host Table respectively.

Create Host Table via Automatic Discovery

Click “Automatic Discovery” to find all InstantWave devices. Select the desired APs and WEBs (for example, those on the first floor of building A). Click the right mouse button to open the tool bar. Choose “Export Host table” to save the Host Table to a file (for convenience, you can save the Host table on a network disk for ease of access).

Import Host Table to check device's availability

Import the Host Table from a file (for convenience, you can retrieve the Host table on a network disk for the ease of access). Once the Host Table is imported, IWMS will automatically check the availability of APs and WEBs listed in the Host Table. This is an extremely powerful feature to make up for the inadequacy of Auto-Discovery. Auto-Discovery can only find InstantWave devices when they are alive. Failed devices cannot be found via Auto-Discovery. The devices listed in the Host Table should be available and provide the service. If they do not exist, IWMS can report their absence immediately so that the system administrator can take immediate action.. The following chart is a typical example. The device with IP address 192.168.1.190 is not responding.



Hosts View

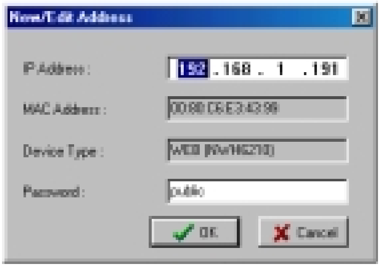
IP Address	Name	Type	MAC Address	Uptime	Loading	Status
192.168.1.1	test	AP (WAH660/Prism2.5)	00:80:C8:E3:62:81	00:36:41		
192.168.1.190	wc191	WEB (WAH6210)	00:80:C8:E3:43:99	01:07:20		Disconnected

2 Agents.

Figure 45. Import Host Table to Check Device

New/Edit/Delete a Host Address on Host Table

Click the Add new address under *IWMS* button to open the New/Edit Address dialog box (Figure 46). Only IP address is necessary for entering. IWMS will automatically find AP's and WEB's hardware address and device type.



IP Address : 192 . 168 . 1 . 191

MAC Address : 00:90:D6:E3:43:98

Device Type : WEB [illegible]

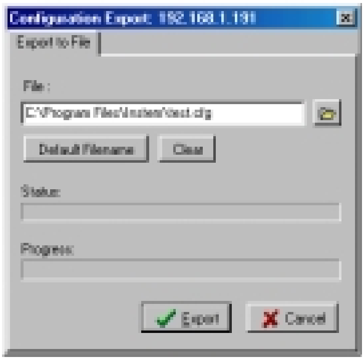
Password : public

Figure 46. New/Edit/Delete a Host Address

From here you can also select any AP or WEB on the table. Edit it for the modification or delete it whenever it is no longer necessary. This table can be saved and retrieved from the IWMS utility so that you don't need to create such a table again in the IWMS utility.

Export the Configuration profile to a File

The configuration file can be saved to a text file and safely kept. This configuration file can also be imported to recover the InstantWave Product's setting, if there is an accident. This profile can also be copied to the other InstantWave product of the same kind. To do this, first click the *Export* button in the *Configuration* window. Then enter the file name for the configuration profile to be saved to.

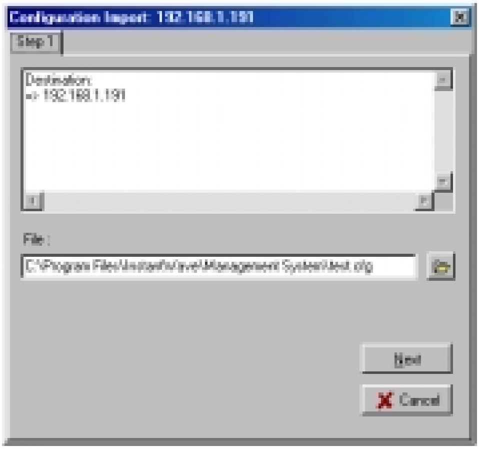


File : C:\Program Files\[illegible]\test.cfg

Figure 47. Export the Configuration Profile to a File

Import the Configuration Profile from a File

If there is an accident, the configuration file can also be imported to recover the InstantWave product's original settings. This profile can also be copied to the other InstantWave product of the same kind. To do this, first click the *Import* button in the *Configuration* window. Then; enter the file name for the configuration profile to be imported from. The user can also pre-select the session of the network profile to be imported and over-written first before clicking the *Import* button.



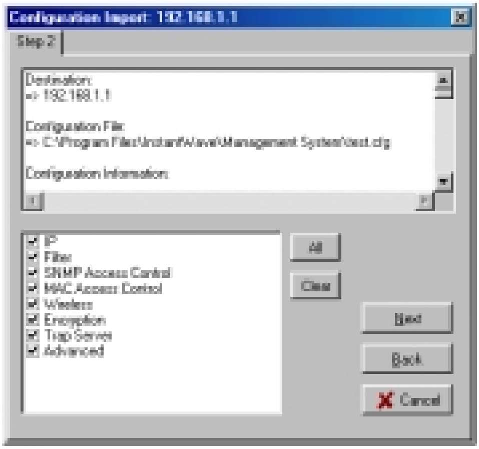
Configuration Import: 192.168.1.191

Step 1

Destination:
=> 192.168.1.191

File :
C:\Program Files\InstantWave\Management System\test.cfg

Figure 48. Import the Configuration Profile from a File (1)



Configuration Import: 192.168.1.1

Step 2

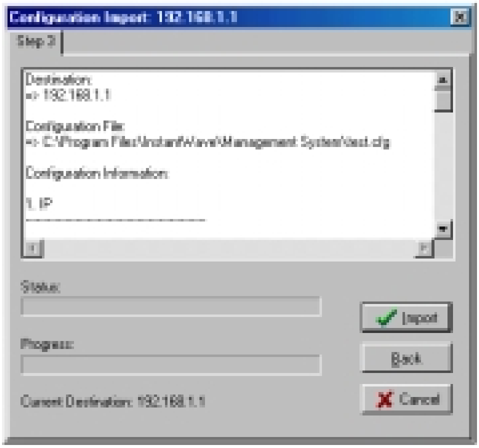
Destination:
=> 192.168.1.1

Configuration File:
=> C:\Program Files\InstantWave\Management System\test.cfg

Configuration Information:

☑ IP
☑ Filter
☑ SNMP Access Control
☑ MAC Access Control
☑ Wireless
☑ Encryption
☑ Trap Server
☑ Advanced

Figure 49. Import the Configuration Profile from a File (2)



```
Destination:
=> 192.168.1.1

Configuration File:
=> C:\Program Files\InstantWave\Management System\test.cfg

Configuration Information:

1. IP
-----------------------------------
```

Status:

Progress:

Current Destination: 192.168.1.1

Figure 50. Import the Configuration Profile from a File (3)

Encryption

The configuration file does not contain the security key settings. The attributes of security keys are externally **write-only** and cannot be saved into the configuration file. Click ***Encryption*** to set up the security keys manually.

FAQs

The FAQs section attempts to answer the most commonly asked questions about InstantWave wireless access points.

Question	***Answer***
At what radio frequency does an AP communicate?	In the U.S., wireless LAN radios transmit and receive on one of 11 channels in the 2.4-GHz frequency band. This is a public band, and does not require a license from the FCC.
How do I secure the data crossing an AP's radio link?	Enable the Wired Equivalency Protocol (WEP) to encrypt the payload of packets sent across a radio link.
What is the speed of the AP's Ethernet port?	The AP's Ethernet port (RJ-45 jack) supports 10 Mbps over a 10Base-T connection (half-duplex only).
What are possible sources of interference for the radio frequency link of the AP?	Interference can come from a number of sources, including 2.4-GHz cordless phones, improperly shielded microwave ovens, and wireless equipment manufactured by other companies. Police radar, electric motors, and moving metal parts of machinery can cause interference too.
How do I set the AP back to its factory default settings?	You can load default settings from the menu of the InstantWave Management System (IWMS), a Windows-based SNMP management tool. You may also press the reset button on the back panel of the AP.
What security features does the AP support?	SSID: By disabling the “Broadcast SSID” option Data security: The AP supports 40-bit and 128-bit Wired Equivalent Protocol (WEP). Management Security: SNMP Access Control

Troubleshooting

This section provides you with some troubleshooting info should you encounter installation or operation problems on InstantWave products. If the problems still cannot be remedied after going through the Troubleshooting section, check the FAQs on page 64 of this manual and at http://www.ndc.com.tw/support/faq.htm

If your problems still cannot be remedied after going through the FAQs and this Troubleshooting section, contact NDC technical support for assistance (see "Technical Support," page 67).

Symptom	***Suggested Solutions***
The NWH660 is switched on, but the Power LED on the NWH660 is off.	1. Make sure the power adapter is firmly connected to the power outlet and the NWH660 power connector. 2. The power adapter or NWH660 is defective.
The IWMS utility cannot detect an InstantWave NWH660 on the same network.	1. Make sure the NWH660 is powered on and connected to an Ethernet work. 2. Check the IP addresses assigned to the NWH660 and IWMS terminal PC. They should be in the same subnet and unique. For example, if the NWH660's IP address is 192.168.1.5 with a mask of 255.255.255.0, then the PC's IP address should be 192.168.1.x with a mask of 255.255.255.0.
The NWH660 powers up, but the Ethernet Link LED is off (no connection to an Ethernet network).	Make sure: 1. The Ethernet cable is connected firmly to both the AP and hub or switch. 2. The Ethernet hub or switch is powered on.
The Status LED on the NWH660 front panel is red and flashing.	Restart (power-cycle) the NWH660 and check the Status LED again. If it is still flashing, you need to return the NWH660 to the reseller for repair.

Transmission performance is slow or erratic.	1. Change the direction of the antenna slightly. 2. There may be interference, possibly caused by a microwave oven, 2.4-GHz wireless phone, or metal objects. Move these interference sources or change the location of the wireless PC or AP. 3. Change the wireless channel on the NWH660. 4. Check that the NWH660 antenna, connectors, and cabling are firmly connected.

Technical Support

Support from Your Network Supplier

If assistance is required, call your supplier for help. Have the following information ready before you make the call.

1. LED status
2. A list of the product hardware (including revision levels), and a brief description of the network structure
3. Details of recent configuration changes, if applicable

Support from NDC

If you have any problems that you cannot resolve with the information in troubleshooting, or the FAQs at

http://www.ndc.com.tw/support/faq.htm

please note the following information and contact our technical support team:

- What you were doing when the error occurred
- What error messages you saw
- Whether the problem can be reproduced
- The serial number of the product
- The firmware version and the debug information

NDC Technical Support is available via: E-mail: techsupt@ndc.com.tw

From time to time updated firmware is released and may be downloaded from the following URL: http://www.ndc.com.tw/support/support.htm

For other information about NDC, please visit us at: www.ndclan.com

NDC Limited Warranty

Hardware

NDC warrants its products to be free of defects in workmanship and materials, under normal use and service, for a period of 12 months from the date of purchase from NDC or its Authorized Reseller, and for the period of time specified in the documentation supplied with each product.

Should a product fail to be in good working order during the applicable warranty period, NDC will, at its option and expense, repair or replace it, or deliver to the purchaser an equivalent product or part at no additional charge except as set forth below. Repair parts and replacement products are furnished on an exchange basis and will be either reconditioned or new. All replaced products and parts will become the property of NDC. Any replaced or repaired product or part has a ninety (90) day warranty or the remainder of the initial warranty period, whichever is longer.

NDC shall not be liable under this warranty if its testing and examination disclose that the alleged defect in the product does not exist or was caused by the purchaser's, or any third party's misuse, neglect, improper installation or testing, unauthorized attempt to repair or modify, or any other cause beyond the range of the intended use, or by accident, fire, lightning, or other hazard.

Software

Software and documentation materials are supplied "as is" without warranty as to their performance, merchantability, or fitness for any particular purpose. However, the media containing the software is covered by a 90-day warranty that protects the purchaser against failure within that period.

Limited Warranty Service Procedures

Any product (1) received in error, (2) in a defective or non-functioning condition, or (3) exhibiting a defect under normal working conditions, can be returned to NDC by following these steps:

You must prepare:

- Dated proof of purchase
- Product model number and quantity
- Product serial number
- Precise reason for return
- Your name/address/email address/telephone/fax

1. Inform the distributor or retailer.
2. Ship the product back to the distributor/retailer with prepaid freight. The purchaser must pay the shipping fee from the distributor/retailer to NDC. Any package sent C.O.D. (Cash On Delivery) will be refused.
3. Charges: Usually RMA (Returned Material Authorization) items will be returned to the purchaser via airmail, prepaid by NDC. If returned by another carrier, the purchaser will pay the difference. A return freight and handling fee will be charged to the purchaser if NDC determines that the product was not faulty or that the damage was caused by the user.

Warning

NDC is not responsible for the integrity of any data on storage equipment (hard drives, tape drives, floppy diskettes, etc.). We strongly recommend that our customers back their data up before sending such equipment in for diagnosis or repair.

Services after Warranty Period

After the warranty period expires, all products can be repaired for a reasonable service charge. The shipping charges to and from the NDC facility will be borne by the purchaser.

Return for Credit

In the case of a DOA (Dead on Arrival) or a shipping error, a return for credit will automatically be applied to the purchaser's account, unless otherwise requested.

Limitation of Liability

All expressed and implied warranties of a product's merchantability, or of its fitness for a particular purpose, are limited in duration to the applicable period as set forth in this limited warranty, and no warranty will be considered valid after its expiration date.

If this product does not function as warranted, your sole remedy shall be repair or replacement as provided for above. In no case shall NDC be liable for any incidental, consequential, special, or indirect damages resulting from loss of data, loss of profits, or loss of use, even if NDC or an authorized NDC distributor/dealer has been advised of the possibility of such damages, or for any claim by any other party.

Specifications

General

Regulatory Compliance	FCC Part 15 Class B (U.S.)
Standards	Wireless LAN: IEEE 802.11b, Wi-Fi Compliant Ethernet: IEEE 802.3
Data Rate	11, 5.5, 2, and 1 Mbps, with auto fallback
Communication Method	Half-duplex
Security	40-bit and 128-bit WEP data encryption
LED Indicators	Power, Status, Ethernet, Wireless
Interfaces/Connectors	10Base-T: RJ-45 Reverse-type SMA Antenna Connector
Power	Input Voltage: 5.1 volts DC ±5% AC Adapter Input: 100 to 240 volts AC Power Consumption: 5.1 volts, 1.0 amperes (typical)
Dimensions	220 x 145 x 33 mm (8.66 x 5.71 x 1.30 in.)

Wireless Specifications

Emission Type	Direct Sequence Spread Spectrum
Radio Frequency Range	2471 to 2497 MHz (Japan) 2400 to 2483.5 MHz (North America, Europe, and Extended Japan Band) 2445 to 2475 MHz (Spain) 2446.5 to 2483.5 MHz (France)
Transmitter	RF Output Power: 20 dBm Frequency Stability: Within ±25 ppm Data Modulation Type: BPSK (1 Mbps), QPSK (2/5.5/11 Mbps) Data Modulation Speed: 11/5.5/2/1 Mbps with auto fallback
Receiver Sensitivity	-83 dBm at 11 Mbps
Antenna Type	Dual dipole diversity antenna (fixed or external)

Software

SNMP Functions	Configuration and management via SNMP in a Microsoft Windows environment through Ethernet or wireless MIB II (RFC 1213), Bridge MIB (RFC 1493), Enterprise MIB
Security	WEP data encryption SNMP access control
Firmware Upgrade	Firmware upgrade through Ethernet or wireless

Environment

Temperature	Operating: 0° to 50° C (32° to 122° F) Storage: -30° to 70° C (-22° to 158° F)
Humidity	85% at 40° C (104° F)

Appendix

This appendix lists the channels supported by the world's regulatory domains.

The channel numbers, channel center frequencies, and regulatory domains are shown in the table.

Channel Number	*Center Frequency (MHz)*	*FCC/ Canada*	*ETSI*	*Spain*	*France*	*Japan*
1	2412	O	O			O
2	2417	O	O			O
3	2422	O	O			O
4	2427	O	O			O
5	2432	O	O			O
6	2437	O	O			O
7	2442	O	O			O
8	2447	O	O			O
9	2452	O	O			O
10	2457	O	O	O	O	O
11	2462	O	O	O	O	O
12	2467		O		O	O
13	2472		O		O	O
14	2484					O

Index