InstantWave™

11Mbps Wireless

NWH6210 Wireless Workgroup Bridge

NWH2610 Wireless Ethernet Client/Pro

User's Guide

Rev. A1
April 2002

NWH6210
NWH2610

National Datacomm Corporation
4F, No. 24-2, Industry East 4th Road, Science Park
Hsin-Chu, 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

The NWH6210 package should contain the following items:

- One NWH6210 InstantWave Wireless Workgroup Bridge
- Dual Dipole Antenna
- A mounting kit (mounting template, screws, and rawl-plugs)
- One CD-ROM (Contains InstantWave Management System, User's Guide, links to online resources)
- One AC to DC power adapter
- One straight-through RT-45 UTP cable
- One cross-over RT-45 UTP cable

The NWH2610 package should contain the following items:

- One NWH2610 InstantWave Wireless Ethernet Client (Management Version)
- One CD-ROM (Contains InstantWave Management System, User's Guide, links to online resources)
- One AC to DC power adapter

Table of Contents

List of Figures

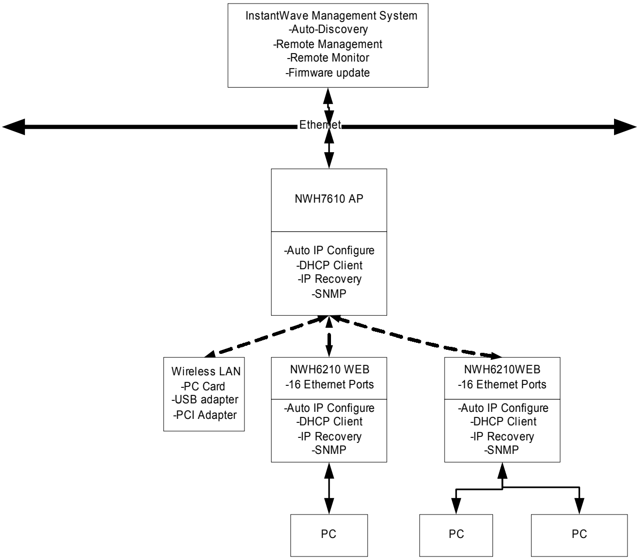
Introduction

Congratulations on choosing an InstantWave 11Mbps wireless product. This guide gives comprehensive instructions on installing and using the InstantWave 11Mbps NWH6210 Wireless Workgroup Bridge, the 11Mbps NWH2610 Wireless Ethernet Client/Pro, and also explains how to install and use the IWMS (InstantWave Management System) program.

InstantWave Wireless LAN Products

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

- Indoor applications: Access Point, Wireless Workgroup Bridge (WWB), Wireless Ethernet Client (WEC), and wireless adapters with various bus interfaces (PCMCIA, USB, and PCI)
- Outdoor applications: Building-to-Building Bridge. Connects two independent Ethernet LANs via a radio link to eliminate expensive cable laying. High gain directional antennas to increase transmission range
- Management tools: Supports SNMP (Simple Network Management Protocol) based InstantWave Management System (IWMS)



InstantWave Wireless LAN is built upon the following products.

- InstantWave Access Point (AP): This product provides a transparent bridged connection between a wired network and a wireless network and allows Wi-Fi compliant wireless stations to communicate with devices attached to a wired network. Not only does it support wireless stations with wireless LAN adapters, such as PC cards, PCI adapters, and USB adapters, but it also operates together with the NWH6210 Wireless Ethernet Bridge.

- NWH6210 Wireless Workgroup Bridge (WWB): This is a workgroup bridge that supports 16 Ethernet devices via an Ethernet Hub or Switch. The NWH6210 can only work together with an InstantWave Access Point under InstantWave's proprietary bridge protocol. It is very useful in conference rooms, hotels, etc. to connect wireless devices to the wired LAN environment.

- NWH2610 Wireless Ethernet Client (WEC): The WEC is an Ethernet client that supports a single Ethernet device. The NWH2610 can only work together with an InstantWave AP under InstantWave's proprietary bridge protocol. It is very useful in public places, hotel rooms, coffee shops etc. where temporary connection to a local LAN or the Internet is required.

- IWMS (InstantWave Management System): This is a powerful Network Management System that is fully compatible with the industry standard SNMP (Simple Network Management Protocol). It features:
    - ♦ Automatic discovery of all InstantWave APs, WWBs, and WECs that are configured within the same subnet

- Individual or batch mode remote management of the devices, including Multi-Monitor, Batch-Upgrade, Batch-Reset, and Bathc-LoadDefault. Batch mode operation is useful when deploying multiple InstantWave products
- Friendly user interface with a consistent look and feel

Automatic Discovery of InstantWave Products

A powerful automatic-discovery algorithm is built into the InstantWave Network Management System. With a simple click on the “Discovery” icon, all InstantWave APs, WWBs, and WECs within the subnet will be discovered. This discovery feature is based on the following techniques:

- DHCP Client and IP recovery: InstantWave APs, WWBs, and WECs have a built-in DHCP client and will request an IP address from a DHCP server so that SNMP (Simple Network Management Protocol) can be further applied. Should there be a failure of the DHCP server; when it recovers, the AP, WWB, and WEC will automatically negotiate for a new IP address

- Auto-IP: When the AP, WWB, or WEC cannot get an IP address from a DHCP server, they will auto-assign an IP address of 169.254.x.x , and a subnet mask of 255.255.0.0.
  A Windows OS PC originally configured as a DHCP client will follow the same algorithm to assign itself an IP address in the same subnet. Users may need to renew the IP settings (see the following section), otherwise Windows may continue to use the previous IP address instead of executing the Auto-IP procedure

Windows 95/98

Click ***Start/Run***, type *winipcfg*, and click ***OK***

step1. The *IP Configuration* dialog box will open

step2. Select the network adapter you use to connect to the AP, WWB, or WEC. Click ***Release***

step3. Click ***Renew*** to retrieve a new IP address, subnet mask, and default gateway address from the AP, WWB, or WEC. Click ***OK*** to save the changes and exit the program

Windows NT 4.0

step1. Click ***Start/Programs/Command Prompt***. Type "*ipconfig /release*" and press ***Enter***

step2. Type "*ipconfig /renew*", and press ***Enter*** to retrieve a new IP address, subnet mask, and default gateway address from the AP, WWB, or WEC

step3. Type ***Exit***

Windows 2000/XP

step1. Click ***Start/Programs/Accessories/Command Prompt.*** Type "*ipconfig /release*" and press ***Enter***

step2. Type "*ipconfig /renew*", and press ***Enter*** to retrieve a new IP address, subnet mask, and default gateway address from the AP, WWB, or WEC

step3. Type ***Exit***

System Requirements for the InstantWave Management System

System requirements to install and operate the InstantWave Management System are:

- An Ethernet drop (UTP) (used to connect to an Ethernet network)
- A PC running Windows 95/98/Me/NT4.0/2000/XP
- Microsoft Internet Explorer 4.01 or later is required
- OS Requirements:

1. On a Windows 95 computer, Microsoft DCOM95 must be installed. You may obtain DCOM95 for Windows 95 from the following Microsoft web location: http://www.microsoft.com/com/dcom/dcom95/download.asp DCOM95.exe is also available on the Microsoft Visual Basic 5.0 CD-ROM (Enterprise, Professional, and Standard editions) in the \Pro\Tools\DCOM95 directory.

2. On a Windows 98 computer (Windows 98SE already includes this component), Microsoft DCOM98 must be installed. Use the following link to download it from Microsoft's DCOM98 download site: http://www.microsoft.com/com/dcom/dcom98/download.asp

3. On Windows NT4.0, service pack 4 or later must be installed.

Terminology Used in this Guide

BSSID/MAC ID

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

Domain Name/SSID

A “Domain” is most commonly used to refer to a group of computers whose hostnames share a common suffix. The domain is usually defined by the network administrator as a segment/subnet of a large network and may be made up of overlapping wireless cells. Wireless nodes can roam freely within the same domain without disconnecting from the network.

Roaming

The concept is similar to that of a cellular phone moving from one base station (one AP) to another. InstantWave offers built-in high performance seamless roaming capabilities.

Regulatory Domain

InstantWave products use the unlicensed ISM (Industrial, Scientific, 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 (2.471GHz – 2.497 GHz), USA, Extended Japan, Canada, and Europe (2.4 GHz – 2.4835 GHz), Spain (2.445 GHz – 2.475 GHz), and France (2.4465 GHz – 2.4835 GHz). To use InstantWave 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 communication. WEP uses a 40-bit or 128-bit key to encrypt data. In order to decode the data transmission, each wireless client on the network must use identical keys.

How to Use this Guide

The User's Guide gives complete instructions for installation and use of the InstantWave Access Point (AP), Wireless Workgroup Bridge (WWB) and Wireless Ethernet Client (WEC). All of them share a common user interface. The major difference among them is:

- The AP has MAC address access control of the wireless stations
- The WWB's supports up to 16 Ethernet devices. An access table is provided by the WWB to allow 16 Ethernet devices' MAC addresses to be registered.
- The WEC supports one Ethernet attached device.

InstantWave products are supplied with factory set default network settings. Use the IWMS tool to change the default settings before introducing a new device to an already-established wireless network.

The IWMS program is a simple-to-use, yet extremely powerful, SNMP-based utility for online central configuration and network management from a remote station on the same subnet. A trap management program is also provided to monitor/diagnose InstantWave products.

Read through the next section ‘Plan the Network’, in order to get the best possible performance from the InstantWave wireless network.

Step 1: Plan the wireless network	Refer to Plan the Network, page 17, for details
Step 2: Pre-configure the AP, WWB, or WEC before installing it into an existing Ethernet network	Refer to Hardware Pre-Configuration, page 27, for details. If you wish to use the default settings for a simple wireless infrastructure network or single AP network, you may skip this step
Step 3: Install the AP, WWB, or WEC into the Ethernet network	Refer to Hardware, page 54, for details. *Note: If your network is a simple wireless infrastructure network, you need only place the AP in a suitable location to finish the AP installation*
Step 4: Make online configuration and manage the AP, WWB, or WEC via the IWMS utility	Refer to Install the InstantWave Management , page 27, and Using the InstantWave Management , page 28, for details

Plan the Network

Infrastructure Network Types

An infrastructure network is formed by several stations (WWBs or WECs) and one or more Access Points (APs), with the stations (WWB or WEC) within a set distance from the AP. 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 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.

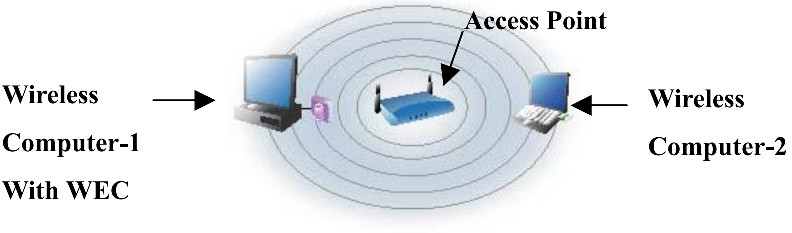


Figure 1. Simple Wireless Infrastructure Network

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 the network resources as they would have if they were wired. This type of network is usually used to extend an existing network into a difficult to wire or a roaming environment.

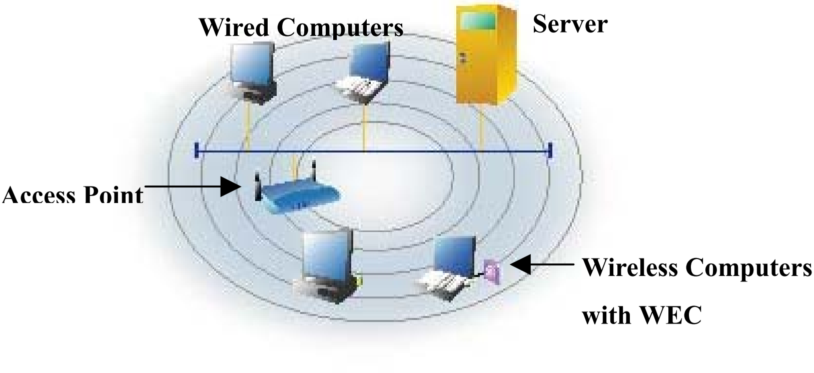


Figure 2. Single AP Network

Type 3. The third type of network is composed of multiple Access Point's and multiple stations (Figure 3).

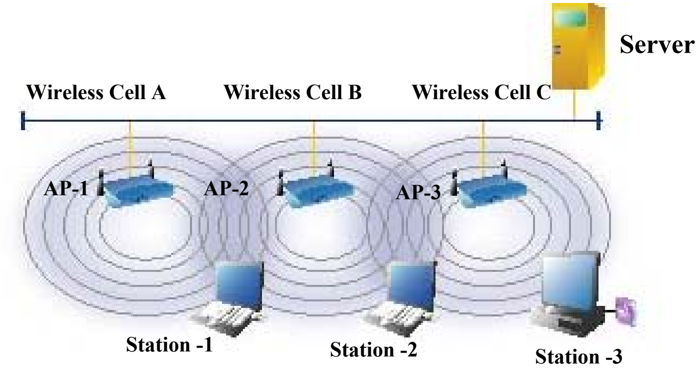


Figure 3. Multiple AP Network

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 type of configuration is usually a mix of these commonly used types.

Planning WWB and WEC for your wireless network

The InstantWave WWB may be used together with a hub or switch, and wirelessly associates to the existing network backbone via InstantWave APs. It can connect up to 16 users (per bridge) for temporary meeting areas, classrooms, etc.

The InstantWave WEC needs no extra drivers or wireless LAN configuration for wireless operation. It may be connected to most Ethernet-ready equipment, such as industrial PCs, scanners, etc.

Figure 4, on page 20, illustrates a complex infrastructure network that combines APs, WWBs, and WECs.

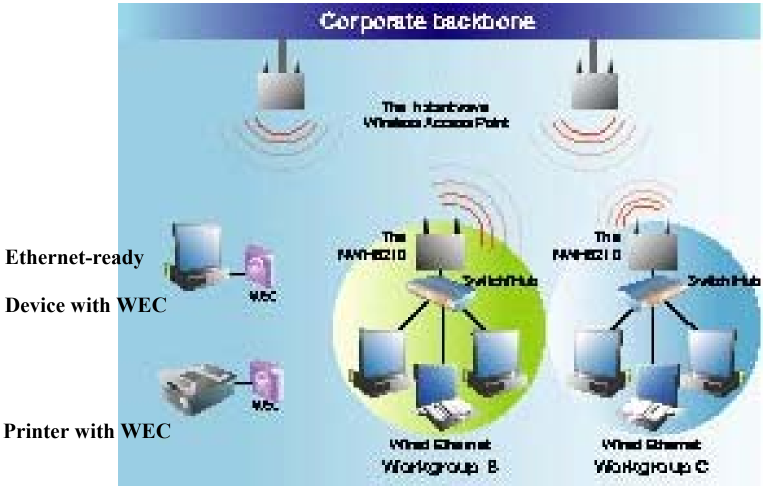


Figure 4. Complex Infrastructure network

Planning an Infrastructure Network

This section explains some of the things you need to consider in planning an Infrastructure network. Setting up is a two-step process.

1. Install and configure the InstantWave products
2. Decide the best physical location of the InstantWave 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 17), all you need to do is make sure the AP and all the wireless stations hold the same 'Domain Name' (SSID) & Security (WEP) setting 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) & Security (WEP) setting to the same as that of the AP's.

Multiple AP Installation

***Install multiple APs in the same network (or Domain) with an overlapping signal* (Figure 3, page 19)**

- Use the same Domain Name (SSID) & security (WEP) settings
- Enable the roaming function in the station if roaming is required

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

Roaming

InstantWave allows 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 21)

b) The APs must be configured to have the same Domain name (SSID) & security (WEP) setting (see Filter, page 33)

c) The mobile stations must have the same domain name (SSID) & security settings (WEP) as those of 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: If you want to move your mobile PC between different APs without terminating the existing networking link, you need to enable the roaming function on the station. The APs that a mobile station will roam to must be configured with the same domain name. If a station detects that the signal quality with the current linked AP is weak, it will search for an AP in the same domain with a better signal quality and automatically establish a new connection with it. When a station is roaming, it will always use the same IP address. The TCP/IP router will not route information packets to a mobile station if it associates with an AP that is in 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 fail to communicate with other network devices via TCP/IP. To avoid running into such an awkward situation, you must assign different domain names to different TCP/IP subnets.

Hardware Description

NWH6210 Panels and Connectors

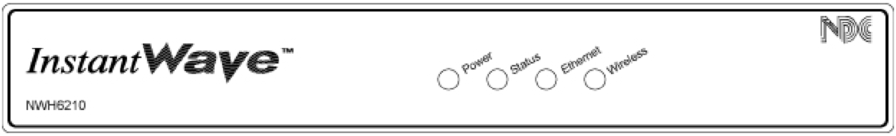


Figure 5. NWH6210 Front Panel

LED Indicators – NWH6210

The Access Point LEDs show the status of the connections.

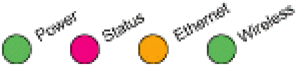


Figure 6. LED Indicators

LED	*Color*	*Function*
Power	Green	OFF: No power supply Blinking: Diagnostic test in progress ON: Normal operation
Status	Red	OFF: Normal operation ON: Operation interrupted
Ethernet	Orange	OFF: No Ethernet link ON: Ethernet connection Blinking: Ethernet activity
Wireless	Green	On: Wireless link up Blinking: Wireless activity

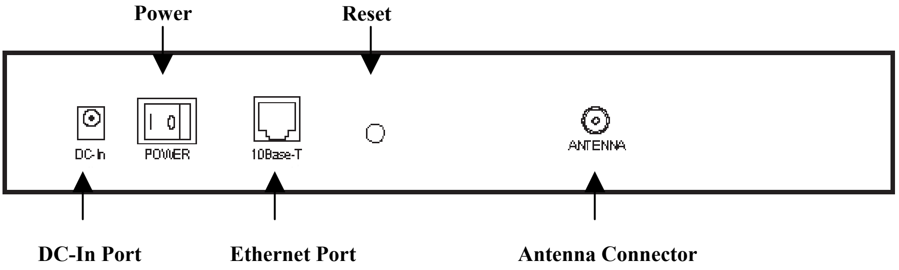


Figure 7. NWH6210 Rear Panel

Connectors

Connector	*Function*
DC Input	DC 5V input
Ethernet	Standard RJ-45 Ethernet connector
Rest Button	Resets the device if pressed for 1 second. Reboots and loads the factory default settings after a long press (over 5 seconds). The Power LED blinks during reset, and goes off once the reset is complete
Antenna Connector	Reverse SMA connector for Antenna (NWH6210 only)

NWH2610 Panels

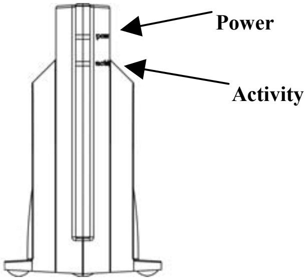


Figure 8. NWH2610 Front Panel

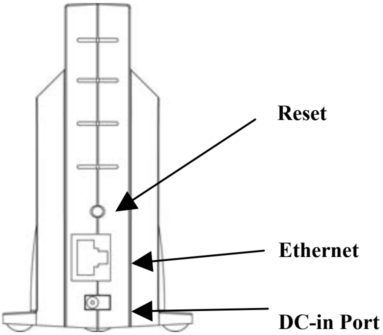


Figure 9. NWH2610 Rear Panel

LED Indicators – NWH2610

LED	*Color*	*Function*
Status	Green	OFF: Power OFF ON: Normal operation Blinking: Operation interrupted
Wireless	Green	On: Wireless link Blinking: Wireless activity

Hardware Pre-Configuration

Before adding a Wireless Workgroup Bridge (WWB) or Wireless Ethernet Client (WEC) into an existing Ethernet network, you may need to set basic configurations, e.g. domain name (SSID), security setting (WEP), WWB (or WEC) name, channel number, or IP address in order to make it compatible with the existing network.

Follow the steps below to connect the WWB (or WEC) to a PC for configuration:

step1. Use a standard Ethernet cable to connect a PC to an Ethernet port on the WWB (or WEC)

step2. Power on the WWB (or WEC)

Install the InstantWave Management System

step1. Insert the InstantWave CD into the CD-ROM drive. The InstantWave CD main menu will open automatically

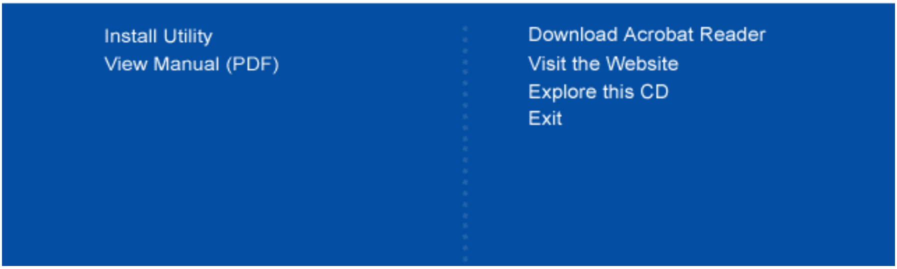


Figure 10. Welcome

step2. Click ***Install Utility*** to install the *InstantWave Management System (IWMS)* utility to your system

Using the InstantWave Management System

Once the WWB (or WEC) 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 WWB (or WEC) through both an Ethernet and a wireless connection. To launch the IWMS utility:

step1. Click ***Start/Programs/InstantWave/Management System/InstantWave Management System***. The main IWMS screen will open. Click ***Hosts View***

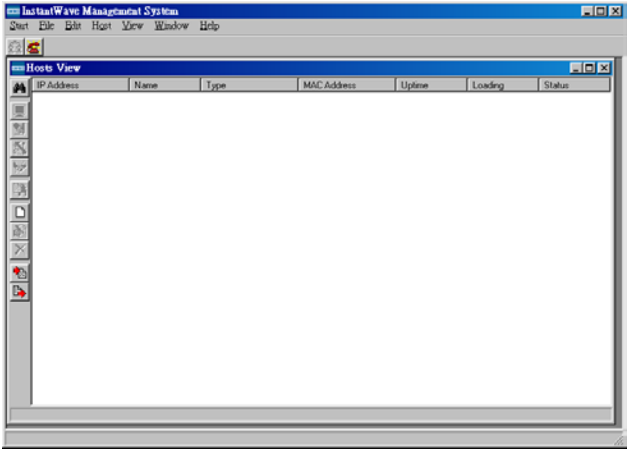
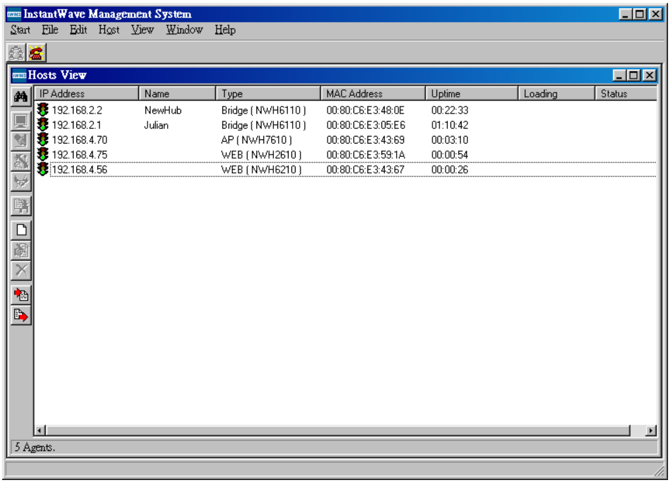


Figure 11. InstantWave Management System

Auto-Discovery

A powerful service discovery protocol has already been built into *IWMS* utility program. This Discovery Protocol can easily discover all the WWBs (or WECs) connected to the Ethernet back bone within the same subnet. Click the "Discover" Binoculars icon. All InstantWave's operating devices will be automatically discovered and shown on the *Hosts View* screen (Figure 13).

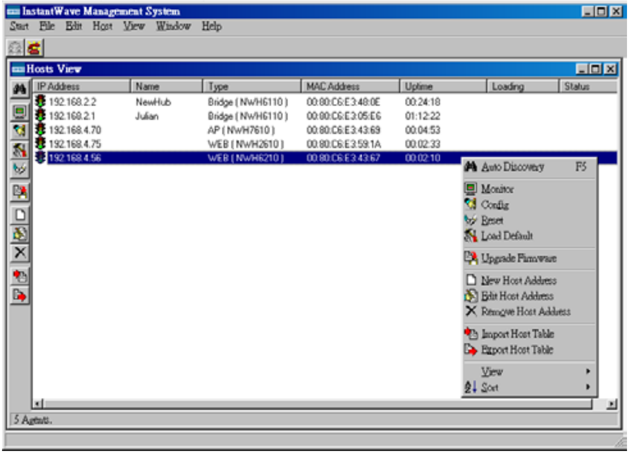


IP Address	Name	Type	MAC Address	Uptime	Loading	Status
192.168.2.2	NewHub	Bridge (NWH6110)	00:80:C6:E3:48:0E	00:22:33		
192.168.2.1	Julian	Bridge (NWH6110)	00:80:C6:E3:05:E6	01:10:42		
192.168.4.70		AP (NWH7610)	00:80:C6:E3:43:69	00:03:10		
192.168.4.75		WEB (NWH2610)	00:80:C6:E3:59:1A	00:00:54		
192.168.4.56		WEB (NWH6210)	00:80:C6:E3:43:67	00:00:26		

5 Agents.

Figure 12. Auto-Discovery

Select one of the wireless devices in the table. The buttons on the left toolbar will be enabled. Right-clicking on a particular device will open a popup menu offering the same functions as the toolbar (Figure 13).



IP Address	Name	Type	MAC Address	Uptime	Loading	Status
192.168.2.2	NewHub	Bridge (NWH6110)	00:00:C6:E3:48:0E	00:24:18		
192.168.2.1	Julian	Bridge (NWH6110)	00:00:C6:E3:05:E6	01:12:22		
192.168.4.70		AP (NWH7610)	00:80:C6:E3:43:69	00:04:53		
192.168.4.75		WEB (NWH2610)	00:80:C6:E3:59:1A	00:02:33		
192.168.4.56		WEB (NWH6210)	00:80:C6:E3:43:67	00:02:10		

5 Agents.

Figure 13. Popup Menu

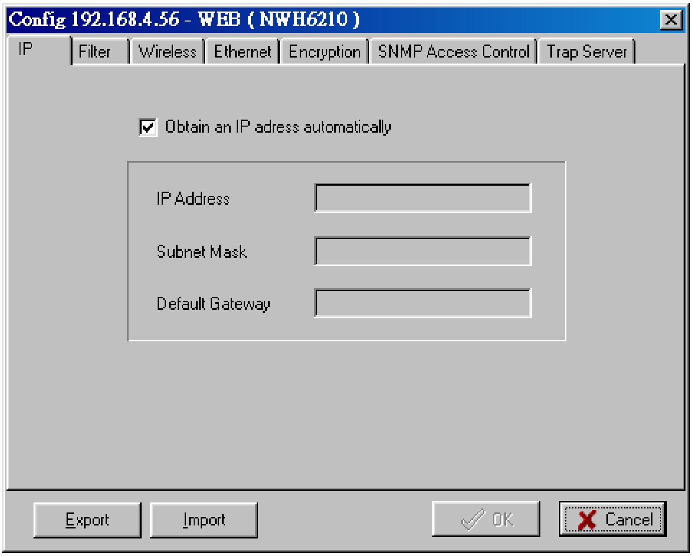
The Status bar at the bottom of the screen shows the number of connecting wireless devices. When the bar shows *Ready*, *Associated* will appear on the bar along with the IP address of the associated WWB (or WEC).

Configuration

step1. Select the device on the *Hosts View* screen (Figure 13)

step2. Right-click the device to open the popup menu

step3. Click ***Config*** to go to the configuration pages (Figure 14)



Config 192.168.4.56 - WEB (NWH6210)

☑ Obtain an IP adress automatically

IP Address

Subnet Mask

Default Gateway

Figure 14. DHCP Configuration

IP

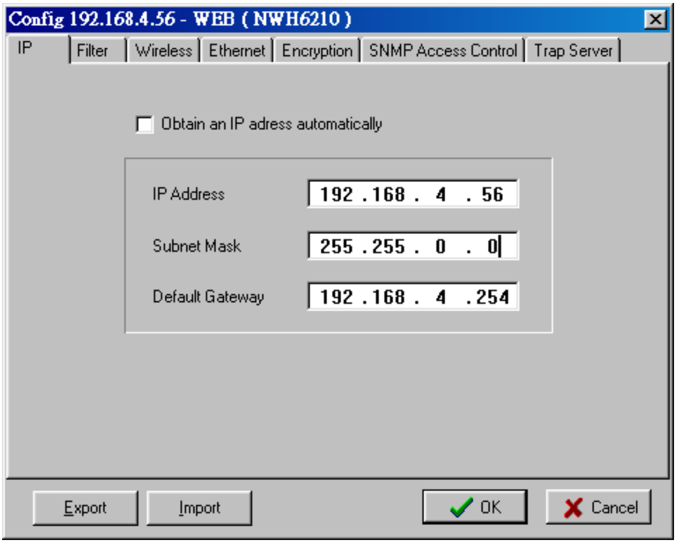
IP Address Setting: A DHCP Client is built into InstantWave WWB and WEC. They will automatically ask the DHCP Server to assign them an IP address. An administrator can assign a fixed IP to a WWB or WEC by un-checking the *Obtain IP from DHCP* box (Figure 14). You may also configure a subnet mask and add a default gateway.

If you assign a fixed IP address to an NWH6110, make sure that all WWBs (or WECs) within the same network have the same TCP/IP subnet address.

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

Note: A WWB (or WEC) will directly transfer SNMP respond packets (confirmation packets) to an IWMS PC if it is within the same LAN (the same subnet mask). If an SNMP respond packet from a WWB (or WEC) is destined for an IWMS PC on another LAN, then the SNMP respond packet needs to go through a router-gateway. The default gateway is the path to that router. If you set the correct default gateway, then you can use an IWMS manager (i.e. a PC running IWMS) physically located in a different subnet to manage this WWB (or WEC).

If you wish to change the defaults, set each WWB (or WEC) to its new IP address before introducing it to the open network. All WWBs (or WECs) within the same network must have the same TCP/IP subnet address.



□ Obtain an IP adress automatically

IP Address: 192 . 168 . 4 . 56

Subnet Mask: 255 . 255 . 0 . 0

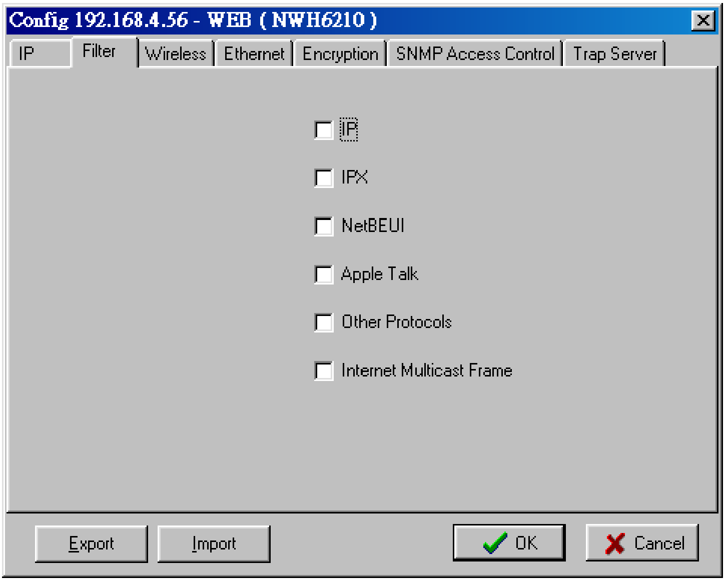
Default Gateway: 192 . 168 . 4 . 254

Figure 15. Static IP Configuration

After making any changes, click ***OK*** to accept the changes and close the box.

Filter

The next tab on the dialog box is *Filter* (Figure 16). This is a one-way protocol filtering mechanism that prevents the WWB or WEC 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.



□ IP

□ IPX

□ NetBEUI

□ Apple Talk

□ Other Protocols

□ Internet Multicast Frame

Figure 16. Configuration/Filter

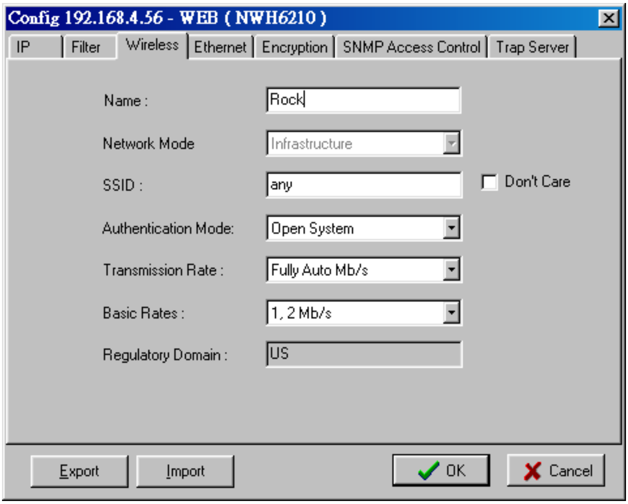
From the *Filter* card, some, all, or none of the protocols listed may be selected for filtering out:

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

After selecting a protocol to be filtered, click the ***OK*** button.

Wireless Setting

To establish radio communication, the following parameters should be properly set.



Name : Rock

Network Mode: Infrastructure

SSID : any

□ Don't Care

Authentication Mode: Open System

Transmission Rate : Fully Auto Mb/s

Basic Rates : 1, 2 Mb/s

Regulatory Domain : US

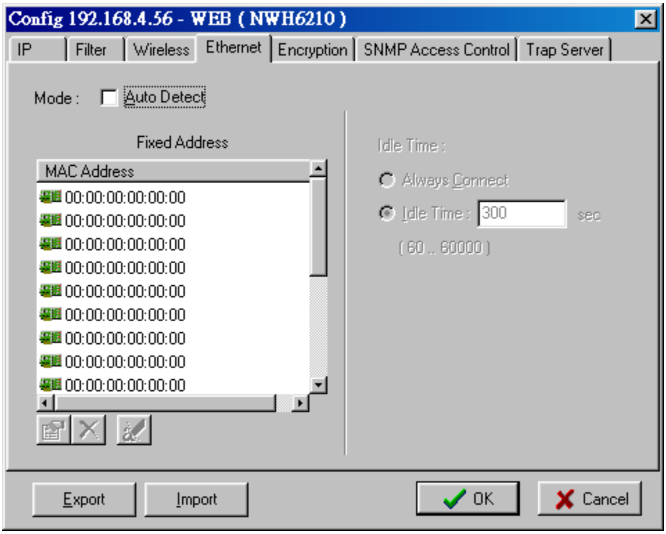
Figure 17. Configuration/Wireless Setting

Name	Assigns a unique human-friendly name that allows the WWB or WEC to be easily identified.
SSID (Domain Name)	This is commonly called the Domain Name and is defined in the IEEE 802.11b Wireless Standard as SSID. Stations, WWBs, WECs, and APs in the same group must use the same Domain Name.
Authentication Mode	From the dropdown list select: **Open system**, **Shared key**, or **Both**. **Open System**: no authentication required for connecting to other wireless devices **Shared Key**: uses the same shared key (automatically generated by the system) for all connecting wireless devices **Both**: the system will try shared key mode first. If that fails it will switch to open system.
Transmission Rate	Sets the transmission rate at which the data packets are transmitted by the WWB or WEC.
Basic Rates	This value determines the basic rates used and reported for this BSS by the WWB or WEC. The highest rate specified will be the rate that the WWB or WEC will use when transmitting broadcast/multicast and management frames. Available options are: • 1 and 2Mbps • All (1, 2, 5.5, and 11Mbps)
Regulatory Domain	Identifies the country where the WWB or WEC is used. Each country has defined its available channel numbers and transmission power (see Appendix, page 64)

Ethernet

The WWB can support up to 16 Ethernet PCs.

- Ethernet Access Control: Only an Ethernet device whose MAC address is pre-registered on this list is allowed to connect to a WWB (or WEC).



Config 192.168.4.56 - WEB (NWH6210)

Mode : □ Auto Detect

Fixed Address

MAC Address
00:00:00:00:00:00
00:00:00:00:00:00
00:00:00:00:00:00
00:00:00:00:00:00
00:00:00:00:00:00
00:00:00:00:00:00
00:00:00:00:00:00
00:00:00:00:00:00
00:00:00:00:00:00

Idle Time :
○ Always Connect
● Idle Time : 300 sec
(60 .. 60000)

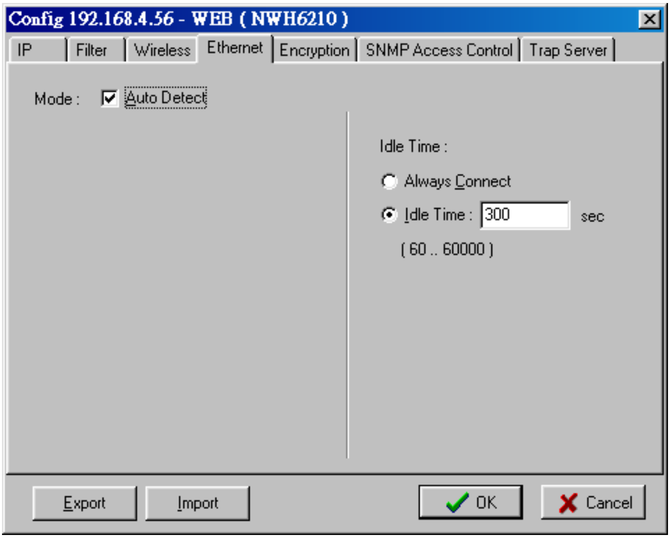
Figure 18. Ethernet/Fixed Address

1. Auto Detect: The WWB will automatically sense Ethernet devices connected to it. The maximum number of Ethernet devices is 16. The WEC supports only one Ethernet device.

2. Fixed Address: This option allows users to specify Ethernet MAC addresses for devices that are allowed to pass traffic through the WWB. The maximum number of Ethernet clients is 16. MAC addresses are 6 bytes long and are controlled by the IEEE. Also known as an *Adapter address*. Only hexadecimal characters (the numbers 0-9 and letters a-f) are acceptable.

Idle Time

A WWB (or WEC) can expire an Ethernet client when there is no traffic from the client within a set period. Specify an aging time to expire an idle client, or disable this function by checking "Always Connect". Click ***OK***.



Config 192.168.4.56 - WEB (NWH6210)

Mode : ☑ Auto Detect

Idle Time :

○ Always Connect

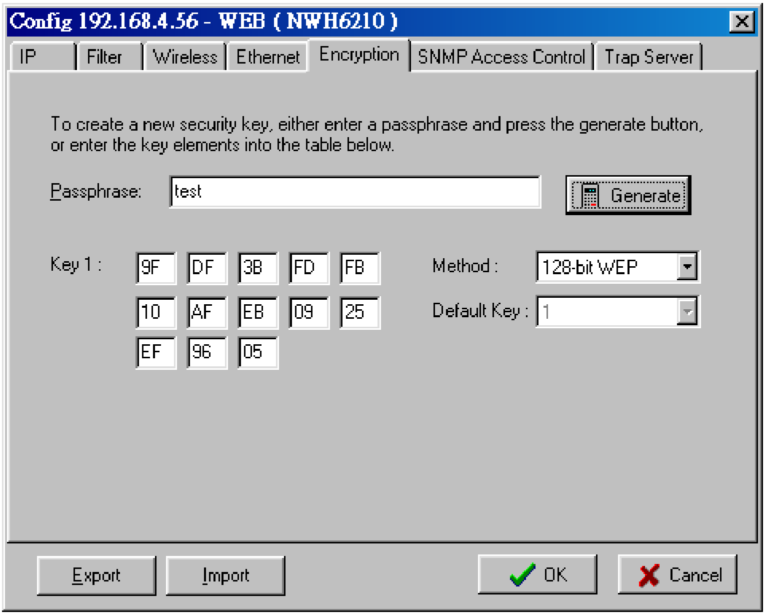
● Idle Time : 300 sec

(60 .. 60000)

Figure 19. Ethernet/Idle Time

Encryption

Data encryption provides secure wireless data communications. Click the *Encryption* tab to setup/change the security settings (Figure 20). The default is *Disabled* and initially the keys section will be blank.



Config 192.168.4.56 - WEB (NWH6210)

IP | Filter | Wireless | Ethernet | Encryption | SNMP Access Control | Trap Server

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: test

Generate

Key 1 :

9F	DF	3B	FD	FB
10	AF	EB	09	25
EF	96	05		

Method : 128-bit WEP

Default Key : 1

Export Import OK Cancel

Figure 20. Configuration/Encryption

The pull-down *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

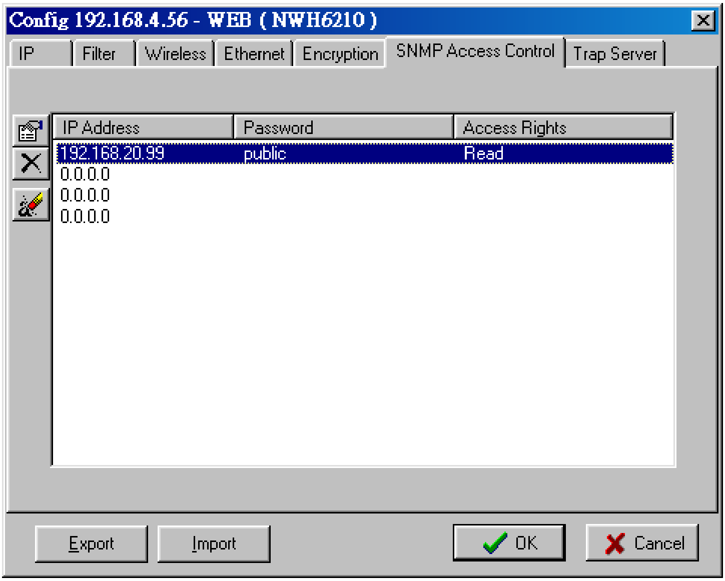
Key Generation - There are two ways to generate a security key.

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 ***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. If the WEP key is enabled on the AP or WEB, all clients must use the same WEP key. Click ***OK***.

SNMP Access Control

SNMP Access Control is the next tab on the box (Figure 21).

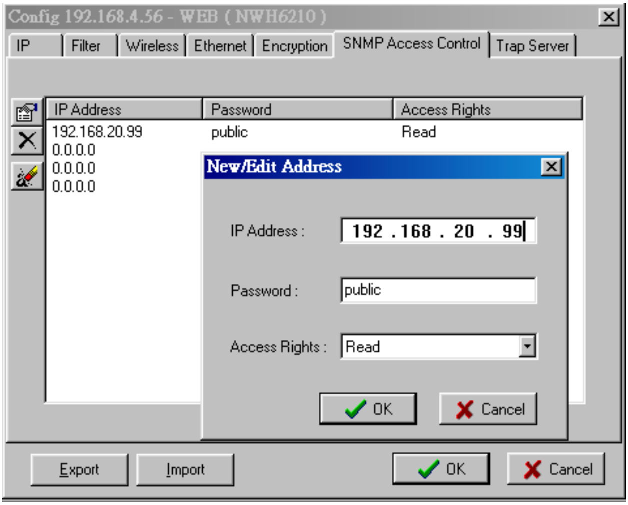


IP Address	Password	Access Rights
192.168.20.99	public	Read
0.0.0.0		
0.0.0.0		
0.0.0.0		

Figure 21. Configuration/SNMP Access Control

The WWB (or WEC) contains an SNMP access table to limit access to its configurations. 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 WWB (or WEC). To avoid chaos on the network, access to the WWB (or WEC) configuration should be restricted to only those for whom it is necessary.

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.*** The *New/Edit Address* screen will open (Figure 22).



IP Address	Password	Access Rights
192.168.20.99	public	Read
0.0.0.0		
0.0.0.0		
0.0.0.0		

New/Edit Address

IP Address : 192 . 168 . 20 . 99

Password : public

Access Rights : Read

Figure 22. 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 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. Once this is set and enabled, it will be impossible to modify the AP settings via IWMS. Should this situation occur, press the hardware Reset Button to restore the factory configuration.

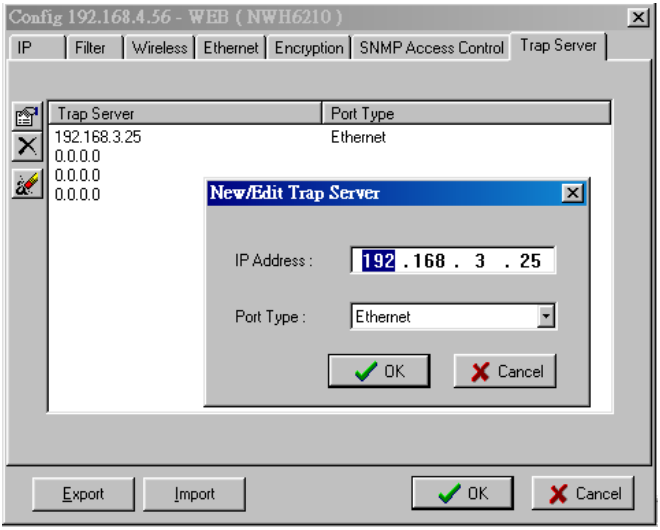
To set a stations access rights, enter a station's IP address and community string (the community string is used as a password to access the WWB or WEC) and choose *Read* or *Read/Write*.

When all the settings are made, click ***OK*** to return to the *SNMP Access Control* card.

Trap Server

Trap Management allows you to setup the configuration of the Trap Server program. When a WWB (or WEC) is powered on, or its Ethernet port becomes active, the WWB (or WEC) will send messages to the assigned trap server to report these activities.

To assign a trap server, click *New/Edit Trap Server* (Figure 23). Assign a station as a trap server by entering its IP address and network port type. Click ***OK***. To remove a trap server from the list, highlight it and click ***Delete***. Click ***Delete All*** to remove all assigned trap servers from the list.



Trap Server	Port Type
192.168.3.25	Ethernet
0.0.0.0	
0.0.0.0	
0.0.0.0	

IP Address : 192 . 168 . 3 . 25

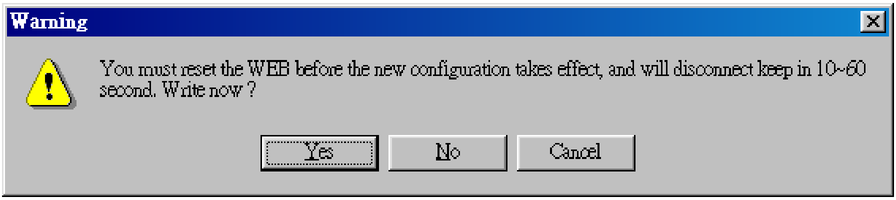
Port Type : Ethernet

Figure 23. Configuration/Trap Server

When the WWB (or WEC) is powered on, or an Ethernet port becomes active, an event log will be generated indicating the time, the MAC ID of the reporting WWB or WEC, and the activity. You may save, open, and delete log files from the *File* menu. To view trap log information, click the icon (***telephone set*** at the upper left corner on main user interface).

Important:

When all configurations have been completed, click Ok. A dialog box will remind you that a Reset will be required to make the changes effective.



Warning

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

Figure 24. Warning

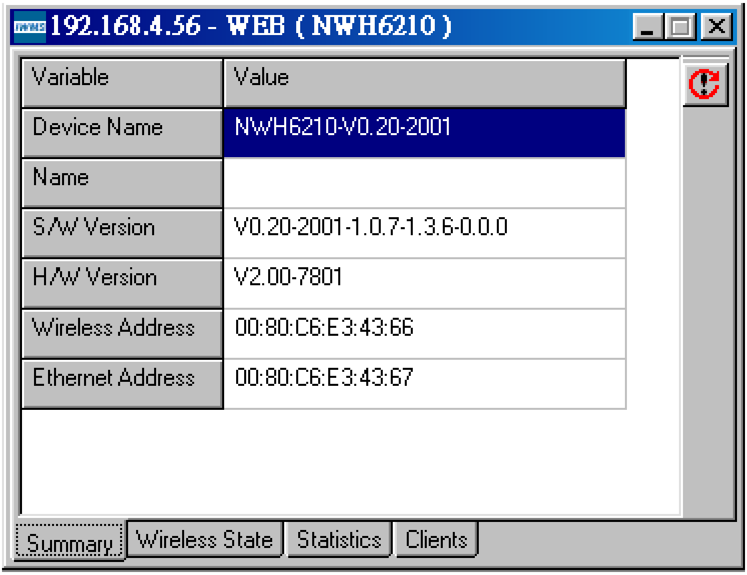
Monitor

The Monitor tool allows the status, Ethernet statistics, Wireless statistics, client list, and other configuration information to be viewed/monitored.

On the *Hosts View* screen, select a device and click the ***Monitor*** button on the toolbar or on the popup menu

Summary Information

The *Summary Information* screen will open (Figure 25). The information shown is read-only.



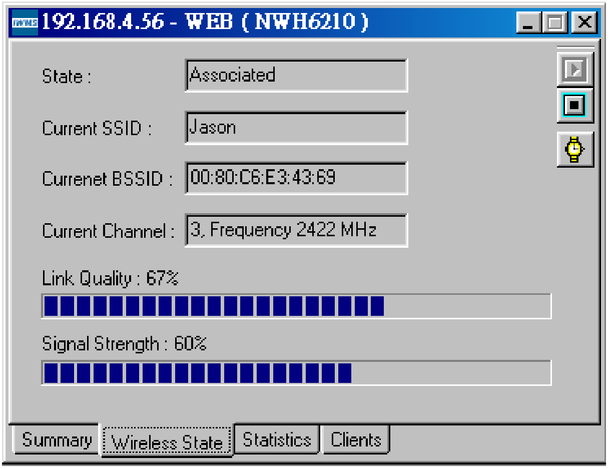
192.168.4.56 - WEB (NWH6210)

Variable	Value
Device Name	NWH6210-V0.20-2001
Name	
S/W Version	V0.20-2001-1.0.7-1.3.6-0.0.0
H/W Version	V2.00-7801
Wireless Address	00:80:C6:E3:43:66
Ethernet Address	00:80:C6:E3:43:67

Figure 25. Monitor/Summary

Wireless Statistics

Click *Wireless State* for current status (Figure 26).



192.168.4.56 - WEB (NWH6210)

State : Associated

Current SSID : Jason

Currenet BSSID : 00:80:C6:E3:43:69

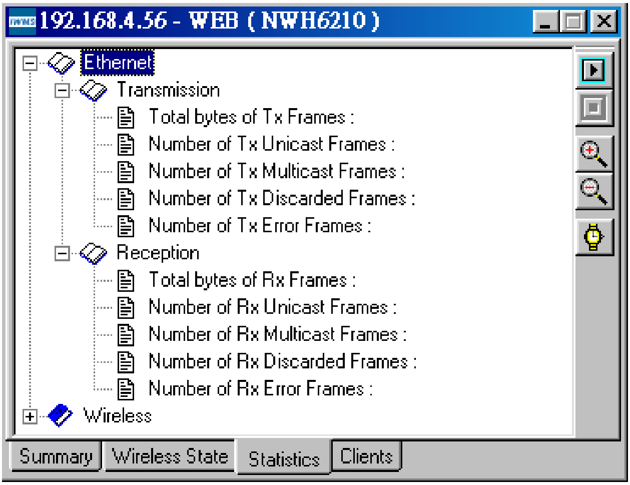
Current Channel : 3, Frequency 2422 MHz

Link Quality : 67%

Signal Strength : 60%

Figure 26. Monitor/Wireless State

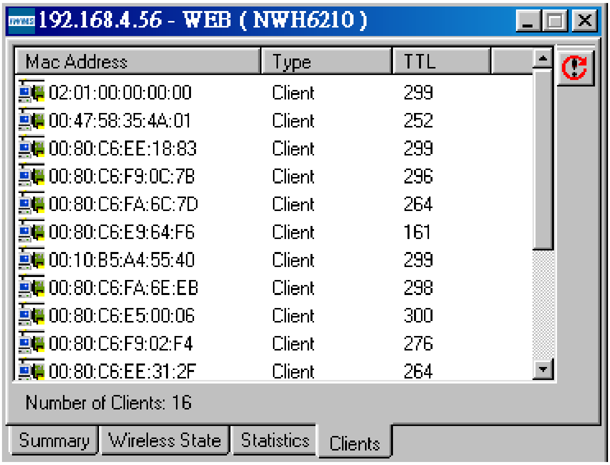
These statistics will be lost when the WWB (or WEC) reboots or is reset. To refresh the statistics, click on the ▶ button to continually refresh information. Click on the ■ button to stop update information



- Ethernet
  - Transmission
    - Total bytes of Tx Frames :
    - Number of Tx Unicast Frames :
    - Number of Tx Multicast Frames :
    - Number of Tx Discarded Frames :
    - Number of Tx Error Frames :
  - Reception
    - Total bytes of Rx Frames :
    - Number of Rx Unicast Frames :
    - Number of Rx Multicast Frames :
    - Number of Rx Discarded Frames :
    - Number of Rx Error Frames :
- Wireless

Figure 27. Monitor/Statistics

The *Clients* window lists all the currently connected Ethernet devices.



Mac Address	Type	TTL
02:01:00:00:00:00	Client	299
00:47:58:35:4A:01	Client	252
00:80:C6:EE:18:83	Client	299
00:80:C6:F9:0C:7B	Client	296
00:80:C6:FA:6C:7D	Client	264
00:80:C6:E9:64:F6	Client	161
00:10:B5:A4:55:40	Client	299
00:80:C6:FA:6E:EB	Client	298
00:80:C6:E5:00:06	Client	300
00:80:C6:F9:02:F4	Client	276
00:80:C6:EE:31:2F	Client	264

Number of Clients: 16

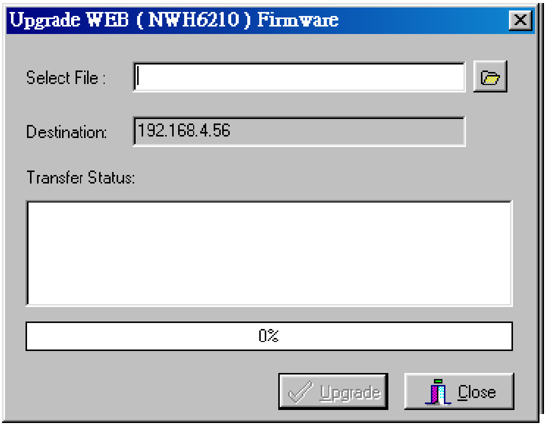
Figure 28. Monitor/Clients

Upgrade Firmware

Upgrade Firmware

The WWB's or WEC's embedded software (firmware) is burned into the flash ROM. However, an updated firmware can be installed over your LAN via the IWMS program. Click on *Upgrade Firmware*. The *Upgrade Firmware* dialog box will open (Figure 29).

Use the *Browse* button to choose the file to be uploaded to the WWB or WEC, or type the file name and path in the *Select File* field.



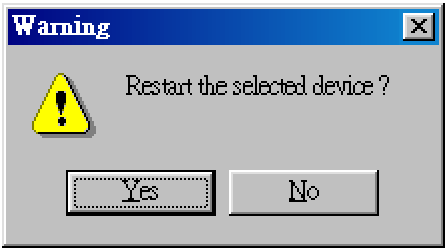
Destination: 192.168.4.56

Figure 29. Upgrade Firmware

The ***Upgrade*** button will then become enabled. Click ***Upgrade*** to start uploading the file to the WWB. The IWMS and the WWB's (or WEC's) built-in Trivial File Transfer Protocol (TFTP) command will upload the new executable into the WWB's or WEC's flash memory area. If the upload activity fails, an error message will be shown on the message box. When the file transfer is complete, click ***Close*** to close the window.

Reset

Resetting the WWB or WEC will take about 30 seconds. During this time, the IWMS program will not be able to query the WWB or WEC via the SNMP protocol and the WWB or WEC will not be available to other stations. If you try to access it, the IWMS program will display a “No response from the WEB or WEC” message.



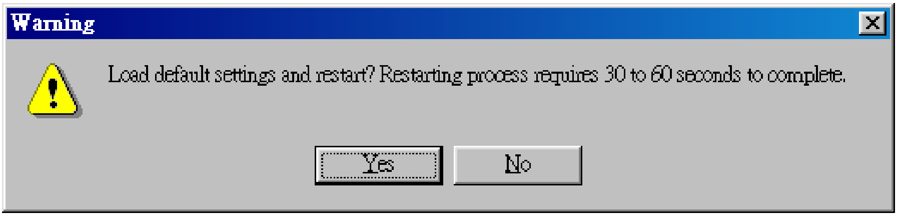
Warning

Restart the selected device ?

Figure 30. Reset the WWB or WEC Configuration

Load Default

Clicking *Load Default* opens a dialog box. Click ***Yes*** to return the WWB or WEC to the default settings. Note: The WWB or WEC will be reset to complete the ‘Load Default’ operation.



Warning

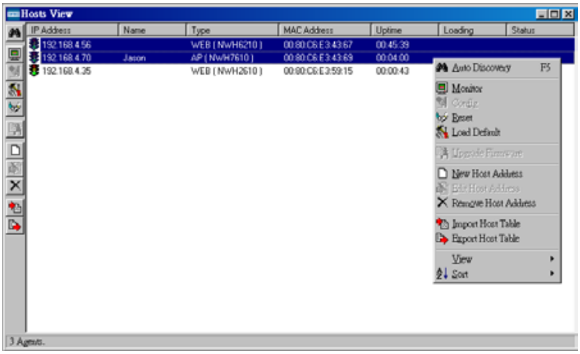
Load default settings and restart? Restarting process requires 30 to 60 seconds to complete.

Figure 31. Load Default

Advanced Setting

Batch mode operation

In order to maximize the efficiency of wireless LAN management, the user can apply batch mode operation to manage the selected WWBs or WECs. You can sort InstantWave devices by the device type first. Then select the multiple WWBs or WECs you would like to manage. Click the right mouse button to open the popup menu. Then choose the tool you would like to work on these specific WWBs or WECs with.



Hosts View

IP Address	Name	Type	MAC Address	Uptime	Loading	Status
192.168.4.56		WEB (NWH6210)	00:80:C6:E3:43:67	00:45:39		
192.168.4.70	Jason	AP (NWH7610)	00:80:C6:E3:43:69	00:04:00		
192.168.4.35		WEB (NWH2610)	00:80:C6:E3:59:15	00:00:43		

3 Agents.

Figure 32. Batch Mode Operation List

Manage the 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 may combine several APs together with WWBs (or WECs) 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 a hotel application would be a typical example.

InstantWave Products	Device	Alias Name	Host Table name	Explanation
NWH660	AP	AP1-A-1F	A-1F	AP located at building A and first floor
NWH7610	AP	AP2-A-1F	A-1F	AP located at building A and first floor
NWH6210	WWB	Room111	A-1F	AP located at building A and first floor
NWH6210	WWB	Room112	A-1F	AP located at building A and first floor
NWH7610	AP	AP1-B-1F	B-1F	AP located at building B and first floor
NWH7610	AP	AP2-B-1F	B-1F	AP located at building B and first floor
NWH6210	WWB	Room111	B-1F	AP located at building A and first floor
NWH6210	WWB	Room121	B-1F	AP located at building A and first floor

The wireless LAN is installed on the 1st floor of building A and the 1st floor of building B respectively. You may assign a different Host Table for each wireless installation group. Once the wireless LAN is divided into many small groups you may easily manage each wireless LAN group by managing its Host Table respectively.

Create a Host Table via Automatic Discovery

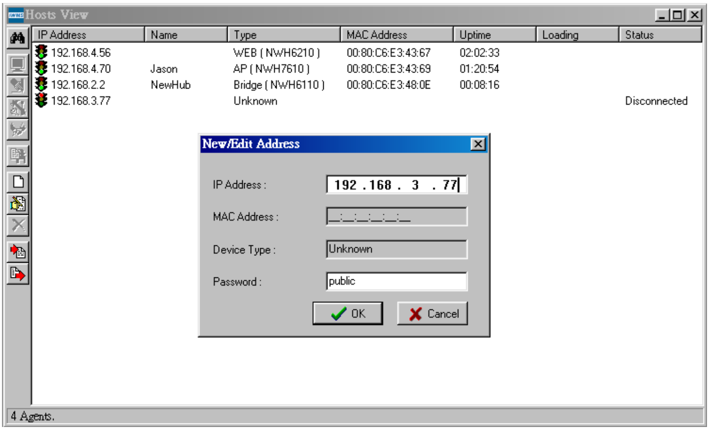
Click "Automatic Discovery" to find all InstantWave devices. Select the desired WWBs and WECs (for example; located on the 1st floor of building A). Click the right mouse button to open the popup menu. Choose "Export Host table" to save the Host Table to a file (for convenience you could save the Host 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 could retrieve the Host table from a network disk for ease of access). Once the Host Table has been imported, the IWMS will automatically check the availability of WWBs or WECs listed on the Host Table. This is an extremely powerful feature as Auto-Discovery can only find InstantWave's devices when they are alive. A failed device will not be found via Auto-Discovery. The devices listed in the Host Table should be available and provide a service. If they do not exist, the IWMS can report their absence immediately so that the system administrator can take immediate action.

New/Edit/Delete a Host Address on the Host Table

Click the *Add New Address* button to open the New/Edit Address dialog box (Figure 33). You only need enter an IP address; the IWMS will automatically find WWB and WEC hardware address and device types.



IP Address	Name	Type	MAC Address	Uptime	Loading	Status
192.168.4.56		WEB (NWH6210)	00:80:C6:E3:43:67	02:02:33		
192.168.4.70	Jason	AP (NWH7610)	00:80:C6:E3:43:69	01:20:54		
192.168.2.2	NewHub	Bridge (NWH6110)	00:80:C6:E3:48:0E	00:08:16		
192.168.3.77		Unknown				Disconnected

New/Edit Address

IP Address : 192 .168 . 3 . 77

MAC Address : __:__:__:__:__:__

Device Type : Unknown

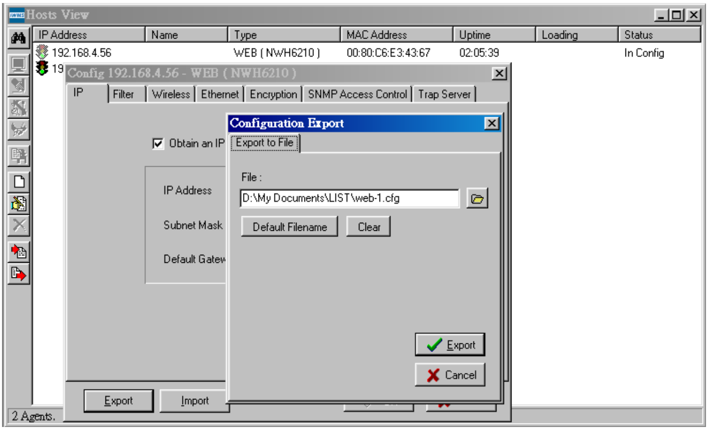
Password : public

Figure 33. New/Edit/Delete a Host Address

From here you can also select any WWB or WEC on the table. Edit it or delete it when it is no longer necessary. This table can be saved and retrieved from the IWMS utility so that you don't need to create it again.

Export a 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 an InstantWave Product's lost settings. The profile can also be copied to other InstantWave products of the same kind. To do this, first click the *Export* button on the *Configuration* screen. Enter the file name for the configuration profile to be saved to (Figure 34).



IP Address	Name	Type	MAC Address	Uptime	Loading	Status
192.168.4.56		WEB (NWH6210)	00:80:C6:E3:43:67	02:05:39		In Config
19						

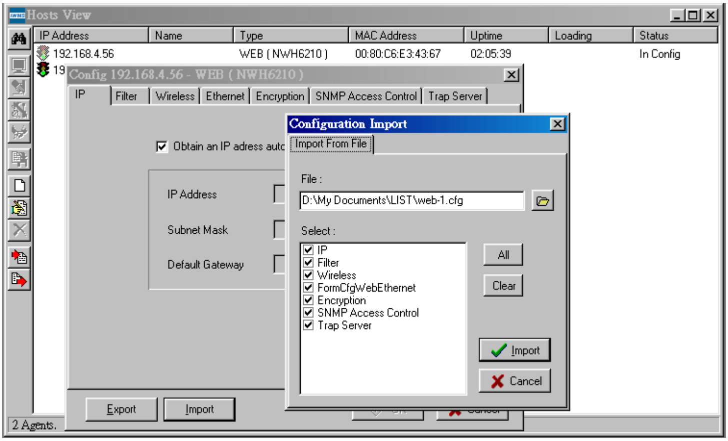
☑ Obtain an IP

File : D:\My Documents\LIST\web-1.cfg

Figure 34. Export the Configuration Profile to a File

Import the Configuration Profile from a File

The configuration file may be imported to recover an InstantWave Product's original settings. The profile can also be copied to other InstantWave products of the same kind. To do this, first click the *Import* button on the *Configuration* screen. 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 before clicking the *Import* button.



Hosts View

IP Address	Name	Type	MAC Address	Uptime	Loading	Status
192.168.4.56		WEB (NWH6210)	00:80:C6:E3:43:67	02:05:39		In Config
19						

Config 192.168.4.56 - WEB (NWH6210)

☑ Obtain an IP adress autc

Configuration Import

File : D:\My Documents\LIST\web-1.cfg

Select :

☑ IP
☑ Filter
☑ Wireless
☑ FormCfgWebEthernet
☑ Encryption
☑ SNMP Access Control
☑ Trap Server

2 Agents.

Figure 35. Import the Configuration Profile from a File

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 setup the security keys manually.

Hardware

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 ~ 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 WWB or WEC (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)

Mounting the WWB

The WEB may be either freestanding or wall-mounted. Screws and a template are provided for easy installation. The installation procedures to fix the WWB to a wall are as below:

step1. Temporarily stick the template sheet on the wall

step2. Drill holes at the places marked “+”

step3. Remove the template sheet

step4. Tap the rawl-plugs into the drilled holes

step5. Screw the supplied screws into the rawl-plugs

step6. Hang the WBB from the screws

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

If you still have a problem, contact NDC technical support for assistance (see Technical Support, page 58).

Before going through the following troubleshooting information, run the *Self Diagnostic Test* to ensure the major components are working.

If your problems still cannot be remedied after going through this Troubleshooting section, contact NDC technical support for assistance (see Technical Support, page 58).

Symptom	***Suggested Solutions***
The WWB is switched ON, but the Power LED on the WWB is OFF.	1. Make sure the power adapter is firmly connected to the power outlet and the WWB power connector. 2. The power adapter or WEB is defective.
The InstantWave IWMS utility cannot detect a WWB on the same network.	1. Make sure the WWB is powered on and connected to an Ethernet work. 2. Check the IP addresses assigned to the IWMS terminal PC. They should be in the same subnet and unique. For example, if the WEB'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 WWB 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 WWB and Hub/Switch. 2. The Hub/Switch is powered on.
The Status LED on the WWB panel is Red and flashing.	Restart (power cycle) the WWB and check the Status LED again. If it is still flashing, you need to return the WWB to the reseller for repair.
Transmission performance is slow or erratic.	1. Move your WWB closer to the AP to find a better signal. If the signal is still weak, change the direction of the antenna slightly. 2. There may be interference, possibly caused by a microwave oven, 2.4GHz 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 AP. 4. Check the WWB antenna, connectors, and cabling are firmly connected
The AP and WWB are working, but the PC cannot connect to the Ethernet network via the AP.	1. The AP's MAC access control function is enabled and the WWB is denied access. 2. The Protocol Filter has blocked required protocols, e.g. TCP/IP to the PC. Uncheck these protocols from the filtering list. See Figure 16, page 34. 3. The IP settings on the PC are not correct.

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

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

NDC Technical Support is available via:

E-mail: techsupt@ndc.com.tw

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 & 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 there was “No Problem Found” 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. (US)
Standards	Wireless LAN: IEEE 802.11b, Wi-Fi Compliant Ethernet: IEEE 802.3
Data Rate	11Mbps/5.5Mbps/2 Mbps/1Mbps auto fallback
Communication Method	Half-Duplex
Security	40-bit/128-bit WEP Data Encryption
LED Indicators	NWH6210: Power, Status, Ethernet, Wireless NWH2610: Status, Wireless
Interfaces/Connectors	10Base-T: RJ-45 Reverse Type SMA Antenna Connector (NWH6210 only)
Power	Power Voltage: DC 5.1Volt ± 5 % AC Adapter: AC 100V~240V Power Consumption: 5.1Volt, 1.0 A (Typical)
Dimensions	NWH6210: 220 x 145 x 33mm (8.66 x 5.71 x 1.30in) NWH2610: 103 x 116 x 66mm (4.05 x 4.56 x 2.60in.)

Wireless Specifications

Emission Type	Direct Sequence Spread Spectrum
RF Frequency Range	2471MHz ~ 2497MHz – Japan Band 2400MHz ~ 2483.5MHz – North America, Europe, and Extended Japan Band 2445MHz ~ 2475MHz – Spain 2446.5MHz ~ 2483.5MHz – France

Transmitter	RF Output Power: 20 dBm Frequency Stability: Within ± 25ppm Data Modulation Type: BPSK (1Mbps)/QPSK (2/5.5/11Mbps) Data Modulation Speed: 11Mbps/5.5Mbps/2Mbps/1Mbps with Auto Fallback
Receiver	Sensitivity: (Less than 8% of FER packet size is 1024 bytes) - 83 dBm (Typical @11Mbps)
Antenna Type	NWH6210: Dual Dipole Diversity Antenna (fixed type or external type) NWH2610: Internal patch antenna

Software

SNMP Functions	Configuration and management via SNMP in a Windows environment through Ethernet. MIB II (RFC 1213), Bridge MIB (RFC 1493) Enterprise MIB Trap Filter
Security	Data encryption Access control Password assignment and rights
Firmware Upgrade	Firmware upgrade via Ethernet or wireless

Environment

Temperature	Operating: 0°C ~ +50°C (32°F ~ 122°F) (Except RF output power and sensitivity) Storage: -30°C ~ +70°C (-22°F ~ 158°F)
Humidity	85% at 40°C

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