D-Link®

DWL-1000AP
11Mbps Wireless Access Point

User's Guide

Rev. A1 (August 2000)

Printed in Taiwan

LIMITED WARRANTY

- D-Link Systems, Inc. ("D-Link") provides this limited warranty for its product only to the person or entity who originally purchased the product from D-Link or its authorized reseller or distributor.

Limited Hardware Warranty: D-Link warrants that the hardware portion of the D-Link products described below ("Hardware") will be free from material defects in workmanship and materials from the date of original retail purchase of the Hardware, for the period set forth below applicable to the product type ("Warranty Period") if the Hardware is used and serviced in accordance with applicable documentation; provided that a completed Registration Card is returned to an Authorized D-Link Service Office within ninety (90) days after the date of original retail purchase of the Hardware. If a completed Registration Card is not received by an authorized D-Link Service Office within such ninety (90) period, then the Warranty Period shall be ninety (90) days from the date of purchase.

Product Type	***Warranty Period***
Product (excluding power supplies and fans), if purchased and delivered in the fifty (50) United States, or the District of Columbia ("USA")	As long as the original purchaser still owns the product
Product purchased or delivered outside the USA	One (1) Year
Power Supplies and Fans	One (1) Year
Spare parts and spare kits	Ninety (90) days

- D-Link's sole obligation shall be to repair or replace the defective Hardware at no charge to the original owner. Such repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement Hardware need not be new or of an identical make, model or part; D-Link may in its discretion may replace the defective Hardware (or any part thereof) with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. The Warranty Period shall extend for an additional ninety (90) days after any repaired or replaced Hardware is delivered. If a material defect is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to repair or replace the defective Hardware, the price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware (or part thereof) that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

- ***Limited Software Warranty:*** D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original delivery of the Software for a period of ninety (90) days ("Warranty Period"), if the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. D-Link's sole obligation shall be to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. The Warranty Period shall extend for an additional ninety (90) days after any replacement Software is delivered. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

- ***What You Must Do For Warranty Service:***

- Registration Card. The Registration Card provided at the back of this manual must be completed and returned to an Authorized D-Link Service Office for each D-Link product within ninety (90) days after the product is purchased and/or licensed. The addresses/telephone/fax list of the nearest Authorized D-Link Service Office is provided in the back of this manual. FAILURE TO PROPERLY COMPLETE AND TIMELY RETURN THE REGISTRATION CARD MAY AFFECT THE WARRANTY FOR THIS PRODUCT.

- Submitting A Claim. Any claim under this limited warranty must be submitted in writing before the end of the Warranty Period to an Authorized D-Link Service Office. The claim must include a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same. The original product owner must obtain a Return Material Authorization (RMA) number from the Authorized D-Link Service Office and, if requested, provide written proof of purchase of the product (such as a copy of the dated purchase invoice for the product) before the warranty service is provided. After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. The packaged product shall be insured and shipped to D-Link, 53 Discovery Drive, Irvine CA 92618, with all shipping costs prepaid. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

- ***What Is Not Covered:***

- This limited warranty provided by D-Link does not cover:

- Products that have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed;
- Initial installation, installation and removal of the product for repair, and shipping costs;
- Operational adjustments covered in the operating manual for the product, and normal maintenance;
- Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; and
- Any hardware, software, firmware or other products or services provided by anyone other than D-Link.
- ***Disclaimer of Other Warranties:*** EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.
- ***Limitation of Liability:*** TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT.
- ***GOVERNING LAW***: This Limited Warranty shall be governed by the laws of the state of California.
- Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This limited warranty provides specific legal rights and the product owner may also have other rights which vary from state to state.
-

Wichtige Sicherheitshinweise

1. Bitte lesen Sie sich diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den spätern Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Vervenden Sie keine Flüssig- oder Aerosolreiniger. Am besten dient ein angefeuchtetes Tuch zur Reinigung.
4. Um eine Beschädigung des Gerätes zu vermeiden sollten Sie nur Zubehörteile verwenden, die vom Hersteller zugelassen sind.
5. Das Gerät is vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sichern Stand zu achten. Ein Kippen oder Fallen könnte Verletzungen hervorrufen. Verwenden Sie nur sichere Standorte und beachten Sie die Aufstellhinweise des Herstellers.
7. Die Belüftungsöffnungen dienen zur Luftzirkulation die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
9. Die Netzanschlußsteckdose muß aus Gründen der elektrischen Sicherheit einen Schutzleiterkontakt haben.
10. Verlegen Sie die Netzanschlußleitung so, daß niemand darüber fallen kann. Es sollete auch nichts auf der Leitung abgestellt werden.
11. Alle Hinweise und Warnungen die sich am Geräten befinden sind zu beachten.
12. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
13. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. Elektrischen Schlag auslösen.
14. Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von authorisiertem Servicepersonal geöffnet werden.
15. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
    a – Netzkabel oder Netzstecker sint beschädigt.
    b – Flüssigkeit ist in das Gerät eingedrungen.
    c – Das Gerät war Feuchtigkeit ausgesetzt.
    d – Wenn das Gerät nicht der Bedienungsanleitung ensprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
    e – Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
    f – Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
16. Bei Reparaturen dürfen nur Orginalersatzteile bzw. den Orginalteilen entsprechende Teile verwendet werden. Der Einsatz von ungeeigneten Ersatzteilen kann eine weitere Beschädigung hervorrufen.
17. Wenden Sie sich mit allen Fragen die Service und Repartur betreffen an Ihren Servicepartner. Somit stellen Sie die Betriebssicherheit des Gerätes sicher.
18. Zum Netzanschluß dieses Gerätes ist eine geprüfte Leitung zu verwenden, Für einen Nennstrom bis 6A und einem Gerätegewicht gr ßer 3kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.75mm2 einzusetzen.

Trademarks

Copyright Statement

1 Contents

2 Introduction

Thank you for purchasing your DWL-1000AP 11Mbps Wireless LAN Access Point. This manual will assist you with the installation procedure for DWL-650,DWL-120 andDWL-500 models

The package you have received should contain the following items:

- DWL-1000AP
- User manual
- Quick installation guide
- Power adapter
- Diskette containing APManager Software

Note: if anything is missing, please contact your vendor

A wireless LAN is normally used in a predefined environment. In such a network, Access Points are mounted at assigned places, each covering its own area in which wireless nodes can operate. These Access Points are connected to a wired network to communicate with each other and with servers and clients on that network.

3 Installation

1. Mount the Access Point firmly to the wall on the position that is determined during the site survey. A drill model is supplied as a separate sheet with this manual.

2. Make sure the antennas are in a vertical position (if not, rotate over 90 degrees).

3. Insert the power connector.

4. Attach the UTP Ethernet cable to the Access Point.

5. Switch on the Access Point.

At the front of the Access Point you will see three LEDs.
If all goes well, the middle LED (power) is green and the leftmost (WLAN) and rightmost (wired network) LEDs flash whenever there is traffic on the respective networks which is at least ten times per second for the wireless LAN because of so-called 'beacons'.

The Access Point automatically selects the medium attached. When the cable network is detected, the network LED will turn yellow.

You can reset the Access Point's settings to factory defaults by pushing a paperclip in the little hole next to the power switch. The sequence of the ACT is on, and keep holding until the LED is being turned off.

When you push a paperclip in the reset hole while the Access Point is switched on, only the lock set by APManager (Par 4.5) is deactivated.

4 APManager Features

APManager provides a consistent view of the Wireless network. The systems administrator can use APManager to control a large number of Access Points from a single location. The Access Points are remotely updated via the SNMP (Simple Network Management Protocol).

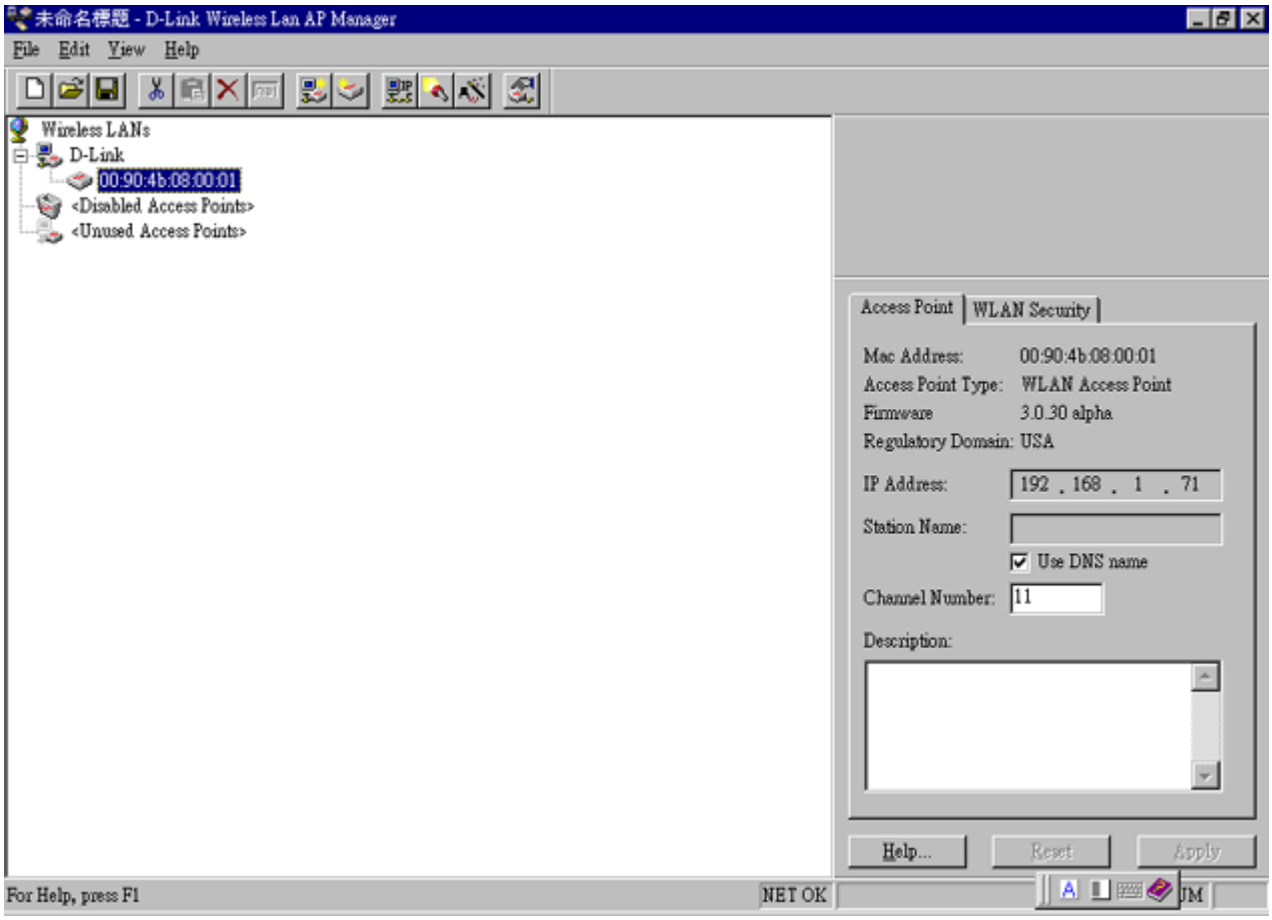
Among the supported features are:

- Adding and removing Access Points
- Restricting access to the Wireless network
- Managing data protection options such as IEEE 802.11b WEP
- Assigning radio channels for optimal cell management
- Grouping the wireless network into multiple WLANs with individual access control and security options
- Programming an Access Point with a specified IP address
- Setting the SNMP Write Community string
- Storing the Access Point configurations on disk
- Verifying the status of all Access Points in the network

4.1 APManager Main Window

The Main Window of APManager may look like this. Before going into detail it is good to have an idea of what kind of information to expect.

You may wish to skip to Quick Start to Wireless Networking.



The tree structure on the left of the window shows a list of WLANs (Wireless LANs) and the Access Points that are part of each WLAN. The sample image above shows a single Access Point with hardware address 00:00:4c:1c:30:06 that is assigned to the WLAN named “Network”. The icons indicate the status of the WLANs and their associated Access Points.

You can use clicking, double clicking, dragging etc. to view Access Point properties or move an Access Point to another WLAN etc. See Managing WLANs.

The name (or ESSID) of the WLAN is used for identifying the WLAN. Client stations can roam freely over Access Points that have the same ESSID. Therefore the security options for all Access Points with the same ESSID are identical. Security options can be managed through the WLAN Security property sheet. See the section on Managing Security.

The Access Point property sheet will mainly be used to select a radio channel for each Access Point. See *Managing Access Points below*.

4.2 Quick Start to Wireless Networking

Configuring a Wireless Network for the very first time, involves the following seven steps:

1. Physically connect the Access Points to the Ethernet LAN. Make sure they are switched on. The GemTek wireless network will be up and running immediately. If you are content with the default settings of the Access Points, you can stop right here. It is more likely however, that you want to assign different radio frequencies to each Access Point, or impose some restrictions on the use of your wireless network.
2. To be able to manage the Access Points via SNMP, every Access Point needs a unique IP address. If you provide a DHCP or BOOTP service on your LAN (and have sufficient free IP addresses available) this will be taken care of automatically. If not, please read the section Manually programming IP addresses.
3. Fire up APManager and configure the Network Settings to reflect your situation (Use the Edit/Network Settings… menu item). See the section Network Settings Dialog for details.
4. Create at least one WLAN (Edit/Insert Wireless LAN) and select the desired security configuration options.
5. Apply the built-in scanning function under Edit/Search Access Points to collect information about the Access Points. See the section Searching for Access Points for more information about the scanning function. Drag the new Access Points to the WLAN of your choice.
6. Select the radio channels of the Access Points according to your cell plan. See also More about Cells. Add descriptive information about each Access Point for later reference.
7. Save the configuration information to disk, and commit the new settings to the Access Points in your network. Using this button.

   Note that the actual settings of the Access Points will not be affected until the Commit to Network function is executed. If you quit APManager, you will be asked to both save and commit.
   See Updating Access Point Settings.

You can open the saved configuration file anytime you to make changes to the network.

4.3 Managing WLANs

A WLAN or "Wireless Local Area Network" consists of a number of Access Points that together provide seamless access to any wireless stations that are in reach of any of the Access Points.

	Create a WLAN	Select the Edit/Insert Wireless LAN menu item to insert a new WLAN into the list. Type the name (ESSID) of the new WLAN.
	Destroy a WLAN	Remove an empty WLAN by pressing Delete or selecting the Edit/Clear menu item.
	Rename a WLAN	Click on the label of the WLAN to change its name (ESSID). Note that client stations use the name to identify the WLAN.

You can move an Access Point from one WLAN to another by dragging it with the mouse or by selecting Edit/Cut followed by Edit/Paste.

There are two WLANs that have a special meaning in APManager. These are the Unused Access Points and Disabled Access Points special WLAN's.

	Unused Access Points	APManager does not manage the Unused Access Points within the context of the current document. In other words, these Access Points are ignored. You can view some information about them (e.g. radio channel), but not modify any of their properties. APManager does not change the settings of these Access Points when File/Commit to Network is selected. This is useful when different people manage different sets of Access Points.
	Disabled Access Points	Access Points that are moved to this folder will be made inaccessible for any client station as soon as they are updated.

4.4 Managing Access Points

Individual Access Points are identified by their hardware address (or MAC address). To insert a new Access Point into the APManager document by hand, its hardware address must be known. You can search for Access Points in your network automatically; see Searching for Access Points.

Insert an Access Point

Select the Edit/Insert Access Point menu item to insert a new Access Point into the selected WLAN. APManager will ask for the hardware address of the Access Point.

Disable an Access Point

Move an Access Point to the "Disabled" special WLAN by pressing Delete or selecting the Edit/Clear menu item. Access Points in this special WLAN will not be accessible for any client station. See Managing WLANs.

The Access Points are shown with one of the following icons.

On-line

The Access Point is accessible on-line.

Off-line

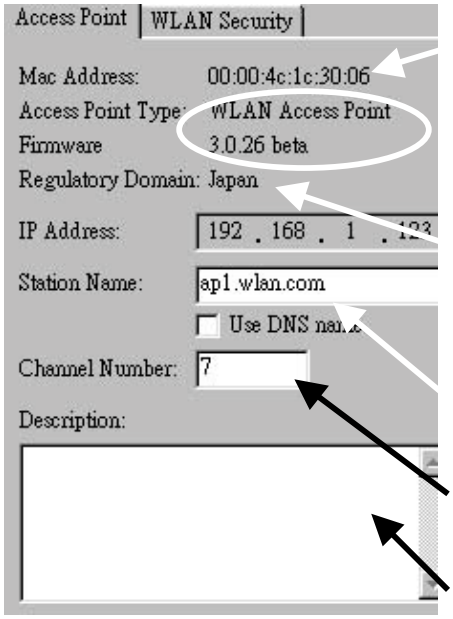
The Access Point is currently not accessible, or the IP address is not known or incorrect.

Locked

The Access Point is permanently locked. Its properties cannot be changed.

Select the Access Point property sheet to view or modify the settings of the selected Access Point. The main function is to be able to program the Access Point's radio channel to match the cell plan. See the section "More about Cells" for details.

Read-only features shown include hardware address, brand and version, and the regulatory domain.



Hardware address (MAC address)

Brand, type, and version information.

The regulatory domain for which the Access Point has been configured (factory setting). Note that it is illegal to use the Access Point outside the designated domain. See Regulatory Domains for details.

The IP address and the hostname of the Access Point.

The radio channel number. The permissible channels depend on the Regulatory Domain.

An optional description field for easy reference.

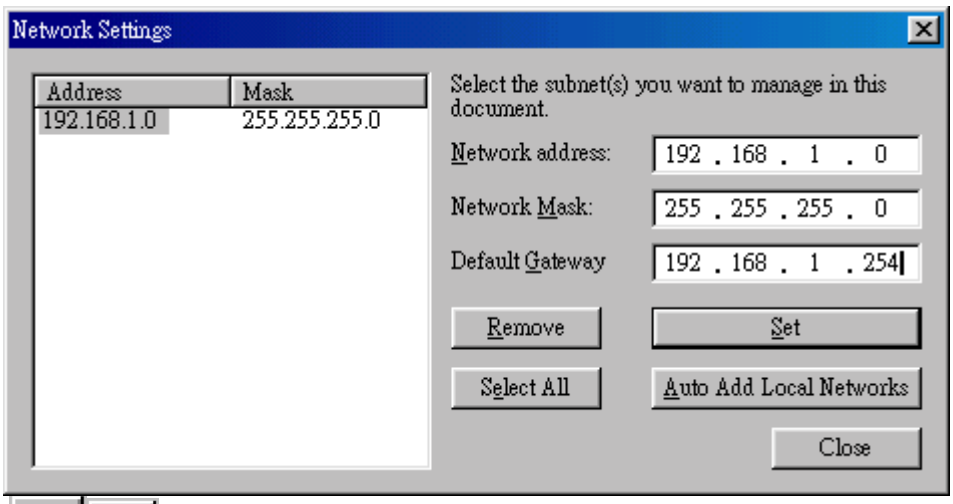
4.4.1 Network Settings Dialog

Selecting the Edit/Network Settings… menu item (or clicking the corresponding toolbar button) pops up the Network Settings dialog. Use this dialog to inform APManager about your network configuration. APManager needs this information to be able to scan for Access Points.

Add your network addresses (subnets) by entering the correct information in the Network address, mask and default gateway fields in the dialog, and clicking the Set button for each network/subnet. To view the details of a particular network, click on the Address field in the list. Click the Remove button to delete a network from the list.

If the computer on which APManager is running is connected to all your networks directly, you can try Auto Add Local Networks to insert them in the list. Note: if subnetting is used, the network addresses and masks generated by this function may not be correct and should be adjusted manually.

4.4.2 Searching for Access Points



APManager has an easy-to-use Access Point discovery function that simplifies the administration of the Access Points in your network. You normally apply the Search function in one of the following situations:

- New Access Points have been added to the network
- The IP address of one or more Access Points is no longer valid or known, possibly because the DHCP or BOOTP server has assigned it a different IP address. You may be informed of this fact because the Access Points will be reported off-line by APManager.

Invoke the Search function by selecting the menu command Edit/Search Access Points, or pressing the associated toolbar button. While APManager is scanning the network, you may continue work on the document. If necessary you can abort a scan by clicking on the Abort Search button.

A progress indicator will be shown in the status bar.

4.4.3 Manually programming IP addresses

The preferred method of providing IP addresses for your Access Points is applying a DHCP or BOOTP server in your network. If you do, the Access Points will acquire an IP address automatically from this server.
If you do not have a DHCP server it is possible to set the IP address of your Access Points from APManager.

1. Physically connect the Access Points and the computer on which you run APManager to the same Ethernet segment.
2. Make sure there is no DHCP or BOOTP server running.
3. Switch the Access Points on. The network LED should light up in red.
4. Configure the network you want your Access Points to be part of. See Network Settings Dialog for details.
5. Enter the hardware addresses of the Access Points by hand using the Edit/Insert Access Point menu command or clicking the appropriate toolbar button.
6. For each Access Point select Edit/Set IP Address menu command and enter the required IP address manually. As soon as you press apply, the Access Point should acquire the designated IP address. Within a few seconds the network LED on the Access Point should light up green.
   Note that you may or may not be able to communicate with the Access Point, depending on the validity of the IP address in the current Ethernet segment.

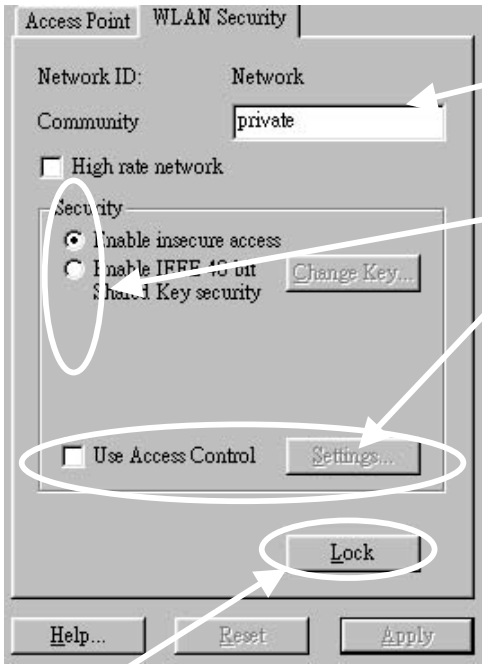
4.5 Managing Security

Maintaining security in a wireless LAN environment is somewhat different from a wired network, because the radio waves do not stop at your office walls. Eavesdropping or unauthorised access from outside your building can be a serious threat.
There are three types of actions involved:

- Protecting your data while it is transferred from one station to another. Encryption techniques will be necessary in most environments (Data Privacy).
- Control who can make use of the wireless network (Access Control).
- Protecting your network configuration against tampering from both inside and outside your organisation (Secure Management).

Data Privacy	An DWL-1000AP Access Point supports three different data privacy algorithms: unencrypted data; standardised IEEE 802.11b WEP (based on a 40 bit shared key, and generated 128 bit session keys).
Access Control	The IEEE 802.11b standard allows for Access Control rules based on the client station's hardware address, and is fully implemented by the WX-1500.
Secure Management	The primary protection against tampering for any SNMP agent is the Write Community String (WCS), which functions as a password for network management commands. The WCS is sent over your network in plain text, making it vulnerable to eavesdropping from within your organisation. The WCS is never sent over the radio, however. If you want you can lock your Access Points. After being locked they can no longer be managed via SNMP. Press the pinhole Reset switch on the back-panel of the Access Point to unlock the Access Point.

Select the required security options in the WLAN Security property sheet.



Edit the Community String field to modify the SNMP Write Community String for all Access Points in the selected WLAN.

Select the data privacy algorithm(s) you want to support in the Access Points.

See the section Access Control for details.
.

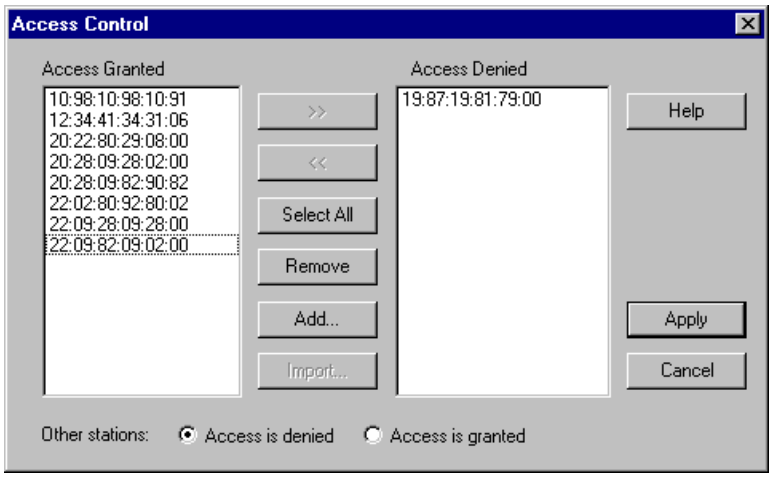
Use this button to lock the settings of the Access Points (almost) permanently

4.5.1 Access Control

Within the IEEE 802.11b framework, Access Control is based on the hardware address of the client stations. Per client you can select whether or not it will be allowed access to your wireless network infrastructure. On the WLAN Security tab, check the Use Access Control box to enable Access Control. If this box is not checked, any client station can associate with your network.

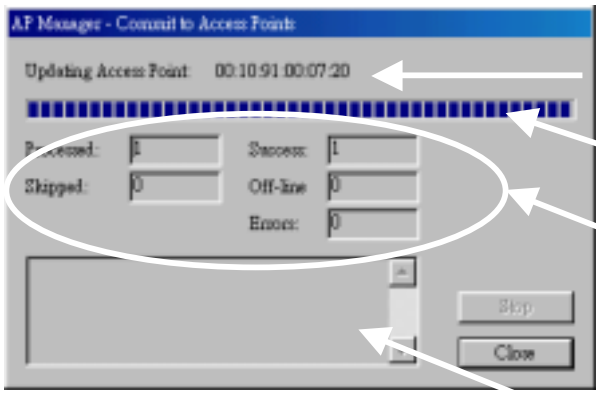
Click the Access Control Settings… button on the WLAN Security tab to pop up the Access Control Dialog. Press Add… to enter the client stations you want to grant access.

A default rule determines whether unregistered stations can join. You can move clients between Access Granted and Access Denied lists by clicking the >> and << buttons or pressing the left and right arrow keys.
Press Apply to confirm your changes and close the dialog.



4.6 Updating Access Point Settings

After modifying the open APManager document you should update the Access Points in your network with the new settings. This is done for all Access Points simultaneously by selecting the File/Commit to Network menu command. Or clicking the associated toolbar button. During the update the following Dialog is displayed:



Access Point that is currently being processed.

Progress indicator

Update result counters. The 'Skipped' count refers to Access Points in the 'Unused' special WLAN.

Specific error messages.

Within 10 seconds after the Access Point has been successfully updated it will disconnect all client stations that are joined with it, and restart with the new settings. While restarting it will show red LEDs for a short period of time.

4.7 IEEE 802.11b WEP Security

The IEEE 802.11b standard includes a Shared Key data privacy mechanism, called 'Wired Equivalent Privacy'.

Features of WEP are:

- Data encryption using a 40 bit shared key
- No key distribution mechanism. The shared key (password) must be distributed manually to all personnel and either be remembered or stored somewhere on the hard disk.
- Simple authentication of clients based on hardware address.

4.8 More about Cells

Each Access Point in the network forms the centre of a cell, or BSS. The Cells should overlap slightly to guarantee seamless wireless connectivity everywhere. Nearby Access Points should preferably send and receive on different channels for maximum throughput.

Creating a cell plan for your site can be complicated, and is usually done by experts employing special measuring equipment. Furthermore, the radio channels you may use depend on both the capabilities of the PC-Cards you are deploying, as well as the regulations in your area. The following table may be of help:

Regulatory Domain	**Area**	**Permissible Channels**
FCC	United States	1 – 11
RSS	Canada	1 – 11
ETSI	Europe except Spain and France	1 – 13
TELEC	Japan	1-14

5 Glossary

BSS	“Basic Service Set”. De facto an alias for Access Point.
Cell	Area in which the radio signal of an Access Point is sufficiently good to join with it.
ESS	“Extended Service Set”. A group of Access Points with identical settings among which a client system can roam. An ESS forms the heart of a WLAN.
Shared Key Algorithm	Encryption scheme for which both sender and receiver need to know the (same) encryption key.
SNMP	“Simple Network Management Protocol”
WLAN	“Wireless LAN” The set of Access Points and Wireless Clients that form a local area network.
Write Community String	SNMP password
WEP	“Wired Equivalent Protection” Data privacy mechanism based on a 40/128 bit shared key algorithm, as described in the IEEE 802.11b standard

6 Technical specifications of DWL-1000AP Series Access Points

6.1 Standards supported

- IEEE 802.11b standard for Wireless LAN
- All major networking standards (including IP, IPX)

6.2 Environmental

Operating temperature (ambient):

- -10 ~ 55°C

Humidity:

- Max. 95% Non-condensing

6.3 Power specifications

DC power supply

- Input : DC 100-240 50-60 Hz 1A
- Output: 5V DC 1A converter incl.

6.4 Radio specifications

Range:

- per cell indoors approx. 35-100 meters
- per cell outdoors up to 100-300 meters

Transmit power:

- Nominal Temp Range: 14 dBm, 12min.
- Extend Temp Range: 14 dBm, 11 dBm min.
- Transmit Power, 2.7 v to 3v: 14 dBm max,11 dBm min.

Frequency range:

- 2.4-2.4835 GHz, direct sequence spread spectrum

Number of Channels:

- Most European countries: 13
- US and Canada: 11 (3 non-overlapping)
- France: 4 (1 non-overlapping)
- Japan : 14

Antenna system:

- Dual antenna diversity system; 2dB gain with swivel neck

6.5 Specific features

Supported bit rates:

- 11 Mbps : CCK
- 5.5 Mbps : CCK
- 1 Mbps : DBSK
- 2 Mbps : DQPSK

Data encryption:

- 40-bit WEP Encryption, 128 bit WEP

Utility Software:

- AP Manager to manage wireless LAN, network connection and client access control

6.6 Physical Dimensions

136 x 126 x 40 mm, 227 x 126 x 40 mm with antennas extended