

No Wires Needed

11 Mbps WLAN Access Point User Manual

Version 3.0.1 – March 2000



CE 0122



Important Notice

This device is a 2.4 GHz low power Access Point transceiver intended for use in all EU memberstates, except for France where restrictive use applies. Please refer to page 9 of this manual for further details.

User manual

11Mbps WLAN Access Point

No Wires Needed
Rembrandtlaan 1a
3723 BG Bilthoven
The Netherlands

www.nwn.com

Version 3.0.1 – March 2000

Trade marks

Copyright © No Wires Needed

The publisher reserves the right to revise this publication and to make changes to any or all parts of this manual at any time, without obligation to notify any person or entity of such revisions or changes.

AirLock, APCenter, ASBF and Connect are trademarks of No Wires Needed. Other product and company names are registered trademarks or trademarks of their respective holders.

Copyright statement

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise without the prior writing of the publisher.

Printed in Velp, March 2000

Free Repair Period

NWN undertakes a Free Repair Period of 12 months from the date of Invoice. Within the Free Repair Period NWN repairs a faulty device free of charge or replaces it in case of irreparable damage.

Excluded from the Free Repair Period are malfunctions caused by operation outside the intended usage; by misuse or abuse; by service modifications or repairs performed by unauthorized persons or by other conditions not arising from defects in Product materials or workmanship.

The costs associated with physically replacing the defective part and re-installing is to be borne by the Buyer.

R&TTE Compliance Statement

This equipment complies with all the requirements of the DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE).

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this manual and of the computer manufacturer must therefore be allowed at all times to ensure the safe use of the equipment.

Restriction of use

The channel use of this Access Point differs regulatory domain. Please check if the regulatory domain mentioned on the sticker on the box and mentioned in APcenter fits your country. Please refer to chapter 4.5 for reading regulatory domain out of the Access point and to chapter 4.9 for the list of regulatory domains.

Using an Access Point with illegal regulatory setting creates a possibility of transmitting on channels that are not allowed by the government. If for some reason the regulatory domain is not correct, do not install your access point and contact immediate your Reseller.

Intended use

This product is a low power 2.4 GHz WLAN Access Point transceiver intended for home and office use.

EU Countries intended for use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France (with Frequency channel restrictions), Germany, Greece, Ireland, Italy, Luxembourg, The Netherlands, Portugal, Spain, Sweden and United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states Iceland, Liechtenstein, Norway and Switzerland.

EU Countries Not intended for use

None.

Potential restrictive use

France: Only channels 10,11,12, and13

RTTE Declaration of conformity



Declaration of Conformity

We, the undersigned,

Company: NoWiresNeeded
Address: Rembrandtlaan 1a, 3723 BG, Bilthoven
Country: The Netherlands
Telephone number: +31 30 2296060 fax number: +31 30 2296061

certify and declare under our sole responsibility that the following equipment:

Brand	Type	Product description / Supplementary info
NoWiresNeeded	11 Mbps WLAN Access Point	2.4 GHz Low Power WLAN Access Point transceiver

is tested to and conforms with the essential radio test suites included in following standards:

Standard	Issue date
ETS 300 328	Ed.2, Nov.1996
ETS 300 826	Ed.1, Nov. 1997
EN 60950	(1992), incl A1(1993), A2(1993),A3(1995), A4(1997)

and therefore complies with the essential requirements and provisions of the **Directive 1999/5/EC** of the European Parliament and of the council of 9 march 1999 on Radio equipment and Telecommunications Terminal Equipment and the mutual recognition of their conformity and Annex IV (Conformity Assessment procedure referred to in article 10(4)).

The following Notified Bodies have been consulted in the Conformity Assessment procedure:

Notified Body number	Name and address
0122	NMI Cerlin B.V., POB 15, 9822 ZG Niekerk, The Netherlands

The technical documentation as required by the Conformity Assessment procedure is kept at the following address

Company: NoWiresNeeded B.V.
address: Rembrandtlaan 1a, 3723 BG, Bilthoven
Country: The Netherlands
Telephone number: +31 30 2296060 fax number: +31 30 2296061

Drawn up in: Bilthoven..... on

28 April 2000..




Remi Blokker, VP

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with the minimum distance between your body, excluding hands, wrists, feet and ankles, and the antenna as shown in the table below:

Access Points which use the internal low gain indoor antennas (1.9dBi)	20cm (7 inches)
--	-----------------

Declaration of Conformity FCC

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.

**No Wires Needed 11 Mbps
WLAN Access Point**



Tested To Comply
With FCC Standards

FOR HOME OR OFFICE USE

1 Contents

1	Contents	10
2	Introduction	11
3	Installation	12
4	APCenter™ Features	15
4.1	Starting APCenter for the first time	16
4.2	APCenter™ Main Window	23
4.3	Quick Start to Wireless Networking	25
4.4	Managing WLANs.....	26
4.5	Managing Access Points.....	27
4.5.1	Network Settings Dialog	29
4.5.2	Searching for Access Points	30
4.5.3	Manually programming IP addresses	31
4.6	Managing Security.....	32
4.6.1	Access Control.....	33
4.7	Updating Access Point Settings.....	35
4.8	AirLock™ Security Architecture.....	36
4.9	More about Cells	36
4.10	Compatibility.....	37
5	Glossary	38
6	Technical specifications 11 Mbps Wlan	39
6.1	Standards supported	39
6.2	Environmental	39
6.3	Power specifications	39
6.4	Radio specifications.....	40
6.5	Specific features	40
6.6	Physical Dimensions.....	40

2 Introduction

Thank you for purchasing your No Wires Needed 11 Mbps WLAN Access Point. This manual will assist you with the installation procedure.

The package you have received should contain the following items:

- User manual
- 11 Mbps WLAN Access Point
- Mounting material
- Power adapter
- CD containing APCenter™ 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.

The 11 Mbps Wlan Access Point can be connected to a 10 or 100 Mbps Ethernet network through a RJ45 (UTP) connector.

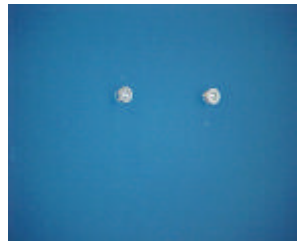
3 Installation

1. The AP can be installed in 3 different ways. These are Ceiling mount, Wall mount, and desktop mount. For each situation there are brackets available. The foot is typical for the desktop and ceiling mount, and the bracket is for wall mount. Important: What ever way you plan to mount the AP, please make sure the unit is always mounted in vertical position.

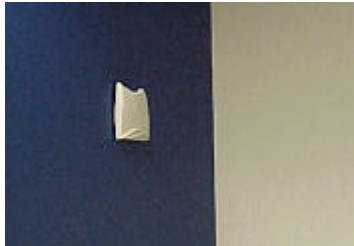
2. Desk mount: Click the foot on to the AP.



3. Wall Mount: Position the location you want to mount the AP. Drill holes for both mounting screws. Place the wall bracket against the wall and test if it fits. Remove the bracket from the wall again. Place it in its position on the backside of the housing. In the backside of the housing a small 'weak spot' is engineered. This spot is not visible but is located exactly in position with middle hole of the mounting bracket. The right place of the mounting bracket is determined by the position where the bracket is



clamped on the housing. If it is not clamped and it needs to be kept in place, the position of the bracket is wrong. When the right position is found, put the screw in. Now the unit can be placed on the predetermined wall position.



4. Ceiling mount: Place the foot on the housing and attach it to the T-bar bracket.
5. Insert the power connector.
6. Attach the UTP Ethernet cable to the Access Point.
7. Switch on the Access Point.

At the front of the Access Point you will see three LEDs.

If all goes well, the rightmost LED (power) is green and the leftmost (WLAN) and middle (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 no cable network is detected, the network LED blinks at a constant rate of approximate 3 times per second.

When the supplied power is too low or unstable the power LED will blink at a constant rate of approximate 3 times per second. All the LEDs will blink at the same rate if a firmware error is detected.

You can reset the Access Point's settings to factory defaults by pushing a paperclip in the little hole next to the Ethernet connector while inserting power to the Access Point.

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

4 APCenter™ Features

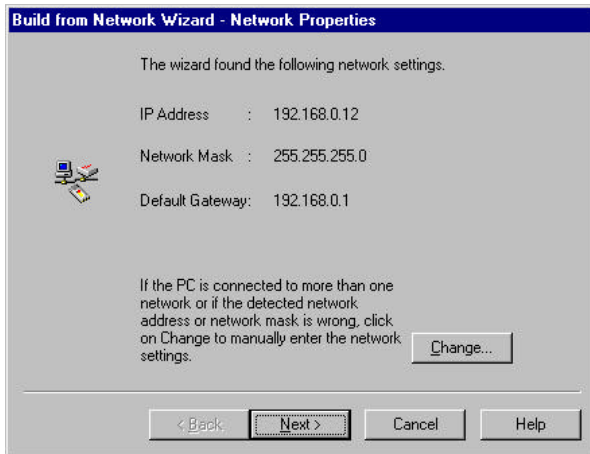
APCenter™ provides a consistent view of the Wireless network. The systems administrator can use APCenter™ to control a large number of 11 Mbps Wlan Access Points from a single location. The Access Points are remotely updated via the SNMP (Simple Network Management Protocol).

Among the supported features are:

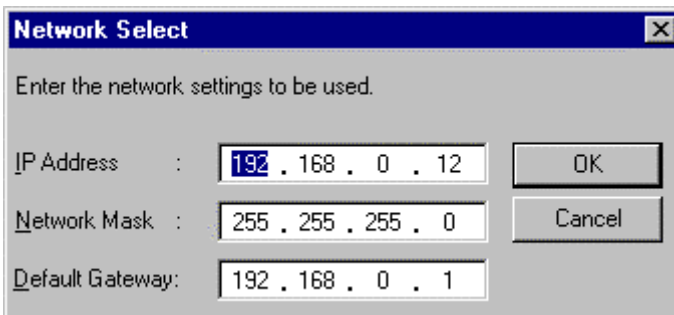
- Adding and removing Access Points
- Restricting access to the Wireless network
- Managing data protection options such as IEEE 802.11 WEP 40 and 128, and AirLock™ Security.
- Assigning radio channels for optimal cell management
- Grouping the wireless network into multiple WLANs with individual access 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
- Printing a summary of your configuration
- Verifying the status of all Access Points in the network

4.1 Starting APCenter for the first time

The first time you run APCenter, it will run in wizard mode. After the title screen, press the Next button to begin configuring your network. The following screen will appear:

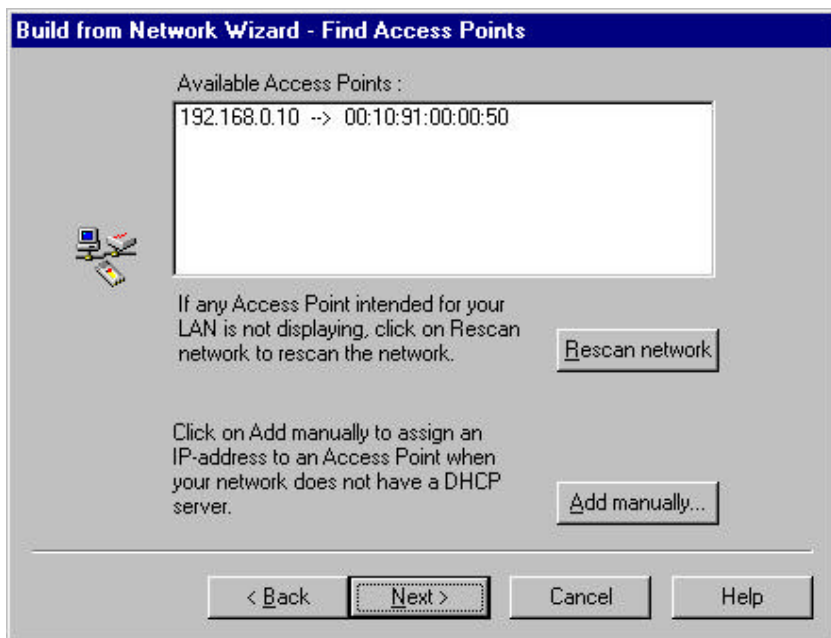


If these settings are correct, press Next to accept them, **or** if the PC is connected to more than one network address or the network mask is wrong, click on **Change**. The *Network Select* dialog box appears.



Enter the network settings to be used. Click on **OK** to return to the *Network Properties* dialog box, then click on **Next**.

The *Find Access Points* dialog box displays. The APCenter wizard scans for and displays all available Access Points on the network.

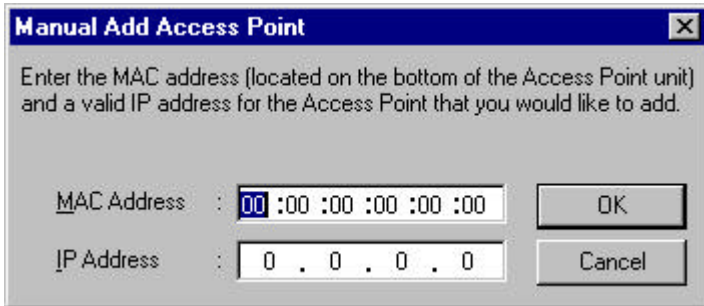


For APCenter to function properly, each Access Point it manages must have a unique IP address (APCenter uses SNMP to configure and manage the wireless network Access Points.) If your LAN does not provide either DHCP or BOOTP Protocol (which automatically assign IP addresses), you will need to manually assign a valid IP address to each Access Point.

If all Access Points are displayed, click on *Next*, OR

If any Access Point intended for your LAN is not displaying, click on **Rescan network** to rescan the network for all Access Points. If all Access Points are now displayed, click on **Next**, OR

To manually assign an IP address to an Access Point, click on **Add manual**. The *Manual Add Access Point* dialog box displays.




Enter the MAC address (located on the back of the Access Point unit) and a valid IP address. Click on **OK** to return to the *Find Access Points* dialog box, and click on **Next**.

The *Access Point Settings* dialog box displays. It is strongly recommended that the Network ID (SSID) be changed from the default ('default') to an SSID unique to your network. Only clients and Access Points that share the same SSID are able to communicate with each other. This screen also allows you to change the Channel used by the Access Point to transmit and receive information.

Build from Network Wizard - Access Point Settings

Enter the Network ID (SSID) and the Channel for the following Access Point.

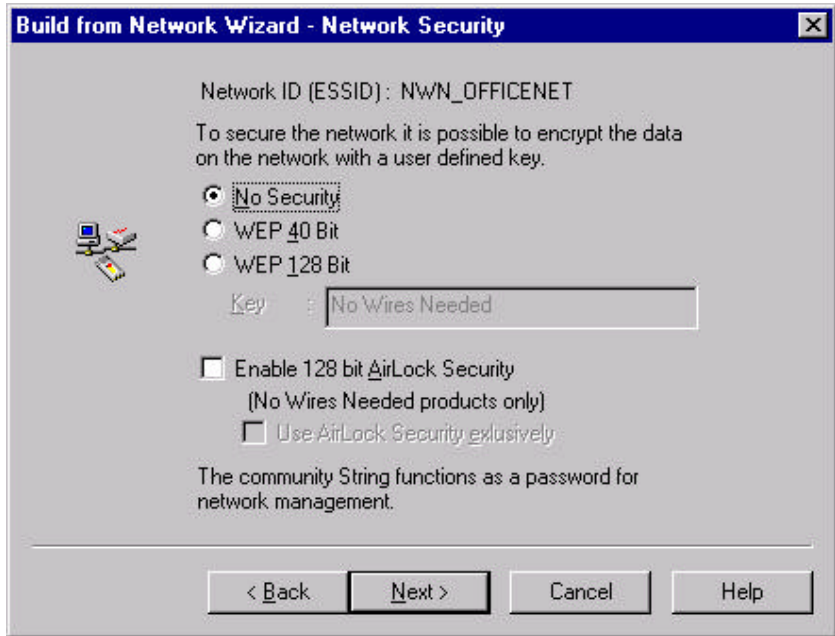
MAC Address : 00:10:91:00:00:50
IP Address : 192.168.0.10

 Network ID (SSID):

Channel :

< Back Next > Cancel Help

After you set the SSID and/or Channel, click on **Next**. If your network contains more than one Access Point, the wizard will display this screen again with the settings of the next Access Point. When you have set SSIDs and/or channels for all Access Points on your network, clicking on **Next** will take you to the *Network Security* dialog box.



It is possible to encrypt the data on the network using one of two different algorithms. It is strongly recommended that you enable security.

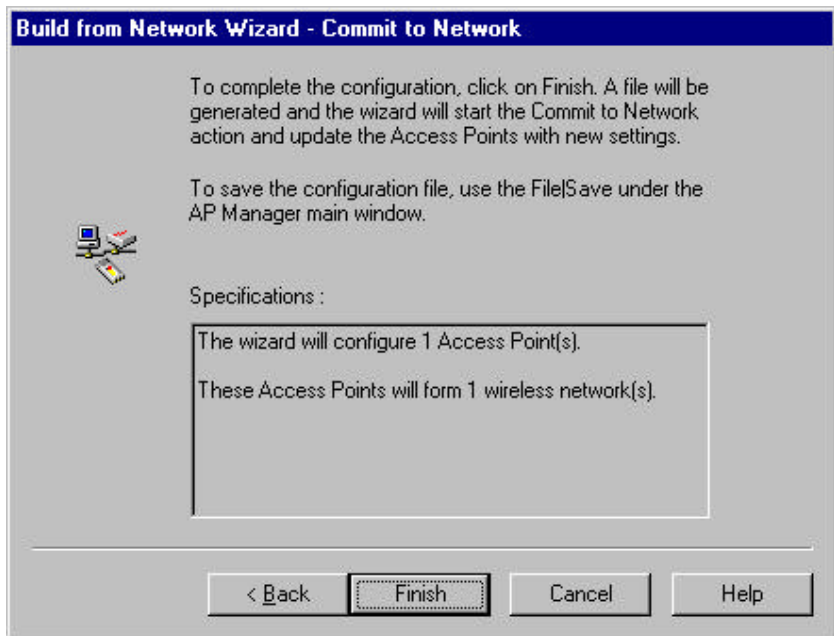
To enable the WEP security, check the *Enable WEP security* box and enter a WEP key in the *Key* field. Only clients and Access Points that share the same WEP key are allowed to associate with each other.

To enable No Wires Needed's much stronger AirLock™ security, check the *Enable 128 bit Airlock Security* box. Because the AirLock™ architecture works with public keys, you do not have to enter keys here. Clients that do not support AirLock™ will use WEP security if you selected WEP security in this dialog, or no security otherwise. By checking the *Use AirLock Security Exclusively* box, you indicate that clients can only join with AirLock™ security.

The Community String functions as a password for network management, preventing unauthorized persons from changing the network security and

Access Point settings. It is strongly recommended that the Community String be changed from the default (private).

Click on **Next**. If more than one Network ID (SSID) is defined on the network, the wizard will display this dialog box again with the settings of the next SSID. When you have selected security for all SSIDs on your network, clicking **Next** will take you to the *Commit to Network* dialog box.



To complete the configuration, click on **Finish**. The Commit to Network dialog box displays. APCenter generates a configuration file and updates the Access Point with new settings.

Note: The actual settings of the Access Points will not be affected until the Commit to Network function is executed.

Click on **Close** after APCenter completes the update.

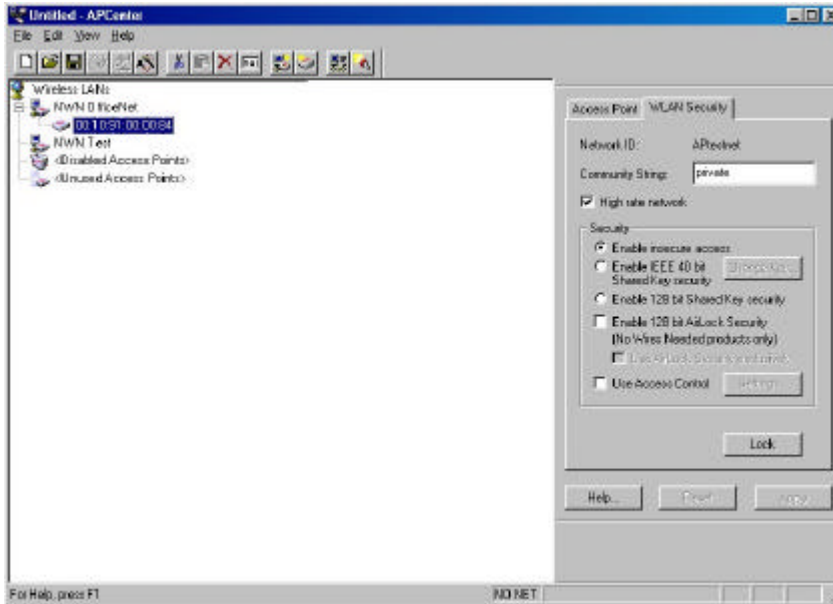
To save the configuration file you just created, select **File → Save** in the APCenter main window. You can open the saved configuration file anytime you want to make changes to the network.

To reset to defaults, push a paperclip in the little hole next to the power connector while simultaneously inserting power to the Access Point. If a paperclip is pushed in the reset hole while the Access Point is on, only the lock set by the APCenter is deactivated.

4.2 APCenter™ Main Window

The Main Window of APCenter™ 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 00:10:91:00:00:84 that is assigned to the WLAN named "NWN OfficeNet". 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*.

4.3 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 No Wires Needed wireless network will be up and running immediately. If you are satisfied 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 APCenter™ 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 APCenter™, 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.

4.4 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 APCenter™. These are the Unused Access Points and Disabled Access Points special WLAN's.



Unused
Access Points

APCenter™ 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. APCenter™ 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.

4.5 Managing Access Points

Individual Access Points are identified by their hardware address (or MAC address). To insert a new Access Point into the APCenter™ 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. APCenter™ 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.

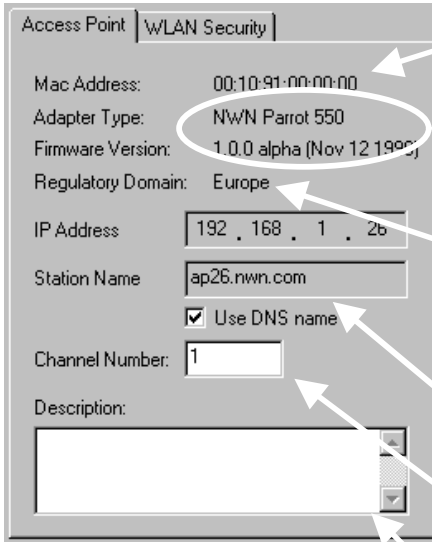


Locked

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.

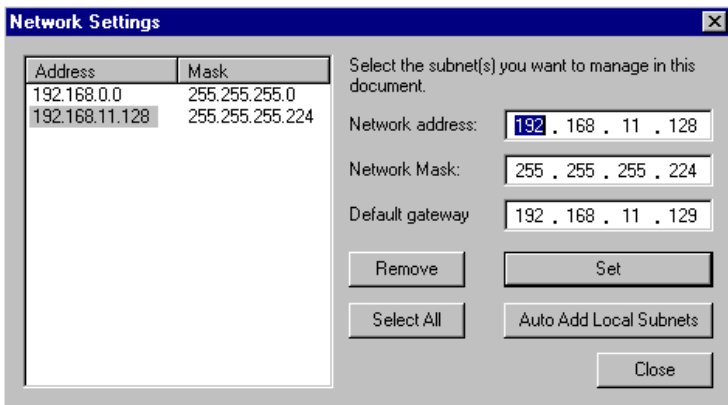
4.5.1 Network Settings Dialog



Selecting the Edit/Network Settings... menu item (or clicking the corresponding toolbar button) pops up the Network Settings dialog. Use this dialog to inform APCenter™ about your network configuration. APCenter™ 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 APCenter™ is running is connected to all your networks directly (this means without routers inbetween), 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.



4.5.2 Searching for Access Points



APCenter™ 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 APCenter™.

Invoke the Search function by selecting the menu command Edit/Search Access Points, or pressing the associated toolbar button. While APCenter™ 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.



4.5.3 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 APCenter™.

1. Physically connect the Access Points and the computer on which you run APCenter™ to the same Ethernet segment. (Subnet)
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. (Subnet Mask, etc)
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.

Note: If you skip point 4, you will not be able to find an AP!!

4.6 *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).

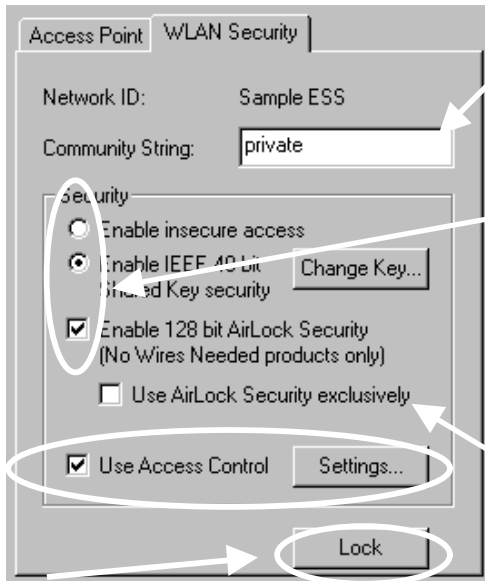
Data Privacy The 11 Mbps Wlan Access Point supports three different data privacy algorithms: unencrypted data; standardised IEEE 802.11 WEP (based on a 40 bit shared key), and No Wires™ Needed AirLock™ (based on automatically generated 128 bit session keys).

Access Control The IEEE 802.11 standard allows for Access Control rules based on the client station's hardware address, and is fully implemented by the 11 Mbps Wlan. If AirLock™ is enabled, the hardware address is also verified using cryptographic techniques. See the section on AirLock™ Security Architecture.

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. If AirLock™ is selected, client stations not supporting AirLock™ may still communicate with the Access Points through the ASBF™ mechanism.

In some situations it may be advisable to enforce AirLock™ as the only available mechanism.

See the section Access Control for details.

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

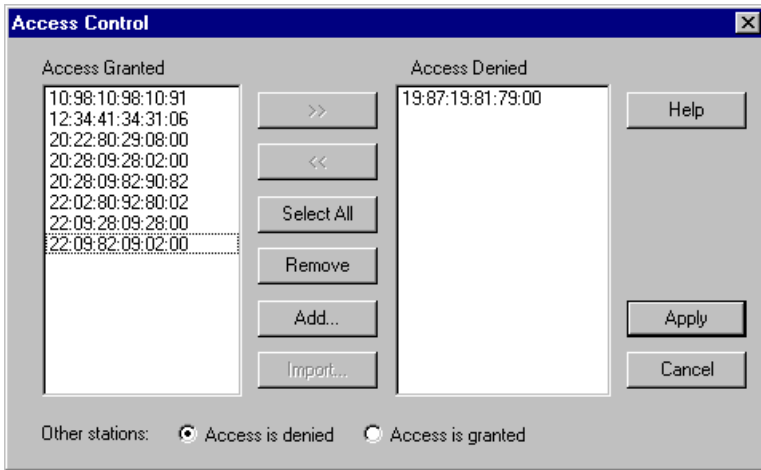
4.6.1 Access Control

Within the IEEE 802.11 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.

No Wires Needed

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.

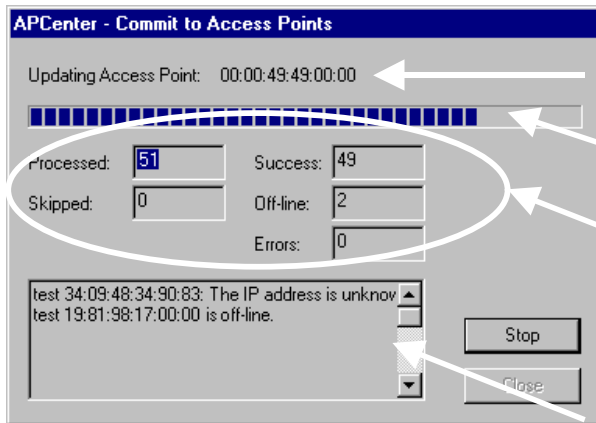
A default rule determines whether unregistered stations can join. You can move clients between **Access Granted** and **Access Denied** lists by clicking the **>>** and **<<** buttons or pressing the left and right arrow keys. Press **Apply** to confirm your changes and close the dialog.



4.7 Updating Access Point Settings



After modifying the open APCenter™ 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.

IEEE 802.11 WEP Security

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

Features of WEP are:

- Data encryption using a 40 or 128 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 AirLock™ Security Architecture

The No Wires Needed AirLock™ Security architecture provides superior protection of your data combined with improved ease of use through secure automated key management, while maintaining full compatibility with the IEEE 802.11 standard.

Some features of AirLock™ Security are:

- Data encryption using 128 bit random session keys
- Key management using a public / private key scheme. Keys are never transmitted as plain text
- Strong authentication of the client stations based on challenge / response.
- Automatic scale back function (ASBF™) maintains compliance to IEEE 802.11 shared key security for client stations that do not support AirLock™ Security.
- RC-4 encryption algorithm

4.9 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	11 Mbps WLAN AP predefined channels
FCC	United States	1 – 11	1, 6, 11
DOC	Canada	1 – 11	1, 6, 11
ETSI	Europe except France	1 – 13	1, 7, 13
FRANCE	France	10	10
MKK	Japan	14	14

4.10 Compatibility

The APCenter™ utility version 3.0.1 is compatible with the No Wires Needed 11 Mbps WLAN Access Points and the series 1100 Parrot Access point only. The 11 Mbps WLAN Access Point is also compatible with the Swallow 1100 series, for airlock, however, the Swallow 1100 requires an upgrade. The 1100 Parrot access point also requires an Airlock upgrade in order to work with an 11Mbps WLAN Pc Card.

5 Glossary

AirLock™ Security	No Wires Needed BV proprietary security architecture. AirLock™ Security provides the following functionality: <ul style="list-style-type: none">• 128 bit data encryption• secure Access Control based on a private/public key algorithm• Integrated automated key distribution algorithm See the AirLock™ Security white-paper for detailed information.
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.
No Wires Needed BV 11 Mbps Wlan Access Point	http://www.nwn.com 11/5.5/2.0/1.0 Mbps IEEE 802.11 Access Point by No Wires Needed BV.
Shared Key Algorithm	Encryption scheme for which both sender and receiver need to know the (same) encryption key.
SNMP 11 Mbps WLAN PC Card	“Simple Network Management Protocol” 11/5.5/2.0/1.0 Mbps IEEE 802.11 Wireless PC Card by No Wires Needed BV.
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 bit shared key algorithm, as described in the IEEE 802.11 standard

6 Technical specifications 11 Mbps WLAN AP

6.1 Standards supported

- Compliant with ETS 300 328 and ETS 300 826 (CE marked)
- IEEE 802.11 standard for Wireless LAN
- All major networking standards (including IP, IPX)

6.2 Environmental

Operating temperature (ambient):

- 0°C to 40°C (32°F to 104°F)

Humidity:

- 95%

6.3 Power specifications

DC power supply

- In 230 VAC 50 Hz 150 mA
- Out 5 VDC 2 A

11 Mbps Wlan Access Point

- In 5 VDC 1 A

6.4 Radio specifications

Range:

- per cell indoors approx. 50 meters (150 ft) or more
- per cell outdoors up to 300 meters (1000 ft)

Transmit power:

- +18 dBm

Frequency range:

- 2.4-2.4835 GHz, direct sequence spread spectrum

Number of Channels:

- Europe: 13 (3 non-overlapping)
- US: 11 (3 non-overlapping)
- France: 4 (1 non-overlapping)

Antenna system:

- Dual antenna diversity system; 2dB gain

6.5 Specific features

Supported bit rates:

- 11 Mbps
- 5.5 Mbps
- 1 Mbps (IEEE 802.11 DSSS compliant devices, using ASBF™)
- 2 Mbps (IEEE 802.11 DSSS compliant devices, using ASBF™)

Data encryption:

- AirLock™ security, 128-bit key length

Utility Software:

- APCenter™ management tool

Key Management:

- Automatic Dynamic Key Allocation (ADKA) through public key

6.6 Physical Dimensions

135x 106 x 20 mm

