

User Manual

11 Mbps Wireless LAN Access Point

Document version: preliminary 3

Document number: 555004.doc

Copyright © 2001 Intersil. All rights reserved.

Trademarks and copyright

Copyright © 2001 Intersil.

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.

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 written permission of the publisher.

AirLock, APCenter, ASBF Connect and KickStart are trademarks of Intersil. Other product and company names are registered trademarks or trademarks of their respective holders.

Safety

This equipment is designed with 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 electronic equipment. All guidelines of this manual and of the computer manufacturer must therefore be followed at all times to ensure the safe use of the equipment.

Important Notice

 The image shows the CE mark followed by the number 0122, and then a warning symbol consisting of an exclamation mark inside a circle.	This device is a 2.4 GHz low power RF device intended for home and office use in all EU member states except in France where restrictive use applies. Please refer to ‘Regulatory notes and statements’ on page 43 in this manual for further details.
---	--

Contents

1	Getting started	7
1.1	Introduction	7
1.2	Contents of this manual	8
1.3	Where to implement a wireless LAN	8
1.4	Adding Access Points to your (network) environment	9
1.4.1	Creating a wireless network	9
1.4.2	Extending a wired network with one or more Access Points	10
1.4.3	Connecting an Access Point directly to a computer	11
2	Installing the Access Point	13
2.1	Introduction	13
2.2	Access Point environment	13
2.3	Physical installation of the Access Point	13
2.4	Desktop mount installation	14
2.5	Wall mount installation	15
2.6	Connecting the Access Point	16
2.6.1	Power adapter	17
2.6.2	UTP port	17
2.7	LEDs	18
2.8	Unlocking the Access Point	18
2.8.1	Unlocking the Access Point to reconfigure	18
2.8.2	Resetting to the default factory setting	19
3	Configuring the Access Point	21
3.1	Introduction	21
3.2	When to configure the Access Point	21

3.3	Starting the Web Interface	22
3.3.1	Installing KickStart	22
3.3.2	Launch KickStart	23
3.3.3	Select wireless ethernet device	23
3.3.4	Device data	24
3.3.5	Scanning and rescanning for devices	24
3.3.6	IP settings	25
3.3.7	Static IP settings	26
3.3.8	IP settings	27
3.3.9	Changing IP settings	27
3.3.10	Ready to start the Web Interface	28
3.3.11	Web Interface is launched	28
3.4	Launching Web Interface manually	29
3.5	Contents of Web Interface	29
3.5.1	Settings Summary	29
3.5.2	Wireless Settings	30
3.5.3	Security against unauthorized network access	31
3.5.4	To add a a client to the exception list	32
3.5.5	To delete a client from the exception list	33
3.5.6	Security against eavesdropping	34
3.5.7	Change WEP password	34
3.5.8	Security against unauthorized configuration	35
3.5.9	Identity	36
3.5.10	IP Settings	37
4	Troubleshooting	39
4.1	If KickStart does not find the Access Point you are looking for	39
4.1.1	Problems on the wireless side	39
4.1.2	Problems on the wired side	40
5	Technical specifications 11 Mbps WLAN Access Point	41
5.1	General Specifications	41
5.2	Radio specifications	41
5.3	Security specifications	42
5.4	Other specifications	42
6	Regulatory notes and statements	43
6.1	Wireless LAN, Health and Authorization for use	43
6.2	Regulatory Information/disclaimers	43
6.3	USA-FCC (Federal Communications Commission) statement	43
6.4	FCC Radio Frequency Exposure statement	44
6.5	FCC Interference Statement	44
6.6	Export restrictions	44
6.7	Europe - EU R&TTE Declaration of Conformity	45
6.8	Restricted Wireless LAN device use in EU	46

Contents

A	TCP and IP settings	49
A.1	Introduction	49
A.2	How do computers communicate in a network	49
A.2.1	IP address	50
A.2.2	Subnet mask	50
A.2.3	IP address range	51
A.2.4	Reserved addresses	51
A.2.5	Gateway	51
A.2.6	MAC address	52
A.3	IP configuration	52
A.3.1	DHCP	52
A.3.2	Auto IP	52
B	Wireless LAN	55
B.1	Introduction	55
B.2	Wireless LAN	55
B.3	The Access Point	56
B.4	Service Set ID (SSID)	56
B.5	Physics of an Access Point	56
B.5.1	Range	56
B.5.2	Data rates	56
B.5.3	Regulatory Domain	57
B.5.4	Radio Channels	57
B.6	Security	57
B.6.1	IEEE authentication	58
B.6.2	Open Systems method	58
B.6.3	WEP method	58

1 Getting started

1.1

Introduction

Thank you for purchasing your 11 Mbps WLAN Access Point.



Figure 1-1 11 Mbps WLAN Access Point

The package you have received contains the following items:

- user manual,
- 11 Mbps WLAN Access Point,
- mounting material,
- power adapter,
- CD containing configuration software and this manual.

1.2

Contents of this manual

[Table 1-1](#) gives an overview of the contents of this manual.

Table 1-1 Contents of this manual

Chapter	When to read:
This chapter (“Getting started”)	Read this chapter on how to implement a Wireless LAN in your (network) environment.
Chapter 2: ‘Installing the Access Point’ on page 13	Read this for information on how to install and connect Access Point to your (network) environment.
Chapter 3: ‘Configuring the Access Point’ on page 21	Read this chapter when you want to adjust the settings of an Access Point. It is not always necessary to adjust the settings of an Access Point. This chapter will also explain when to adjust the settings.
Chapter 4: ‘Troubleshooting’ on page 39	Read this chapter when the Access Point does not function.
Chapter 5: ‘Technical specifications 11 Mbps WLAN Access Point’ on page 41	This chapter contains the technical specifications of the Access Point.
Appendix A: ‘TCP and IP settings’ on page 49	This appendix contains background information on TCP/IP settings. Read this appendix when you are not familiar with networking terminology.
Appendix B: ‘Wireless LAN’ on page 55	This appendix contains some background information on wireless LAN’s. Read this appendix when you are not familiar with radiographic terminology and wireless networking.

1.3

Where to implement a wireless LAN

Whether at home or at the office, a wireless LAN offers freedom moving around the area with the radiographic reach of the Access Points.

An Access Point is like a hub. They are mounted at assigned places, each covering its own area in which wireless nodes can operate.

The Access Points can be 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 an RJ45 (UTP) connector.

See chapter 5: 'Technical specifications 11 Mbps WLAN Access Point' on page 41.

1.4

Adding Access Points to your (network) environment

Where to place and how to connect an Access Point depends entirely on your specific (network) environment. In this section some guidelines on how to add Access Points to your environment are given.

An Access Point can be used to

- create a wireless network (see section 1.4.1),
- extend an existing wired network (see section 1.4.2),
- connect to a single computer (see section 1.4.3).

1.4.1

Creating a wireless network

You can use an Access Point to set up a wireless network, see Figure 1-2.

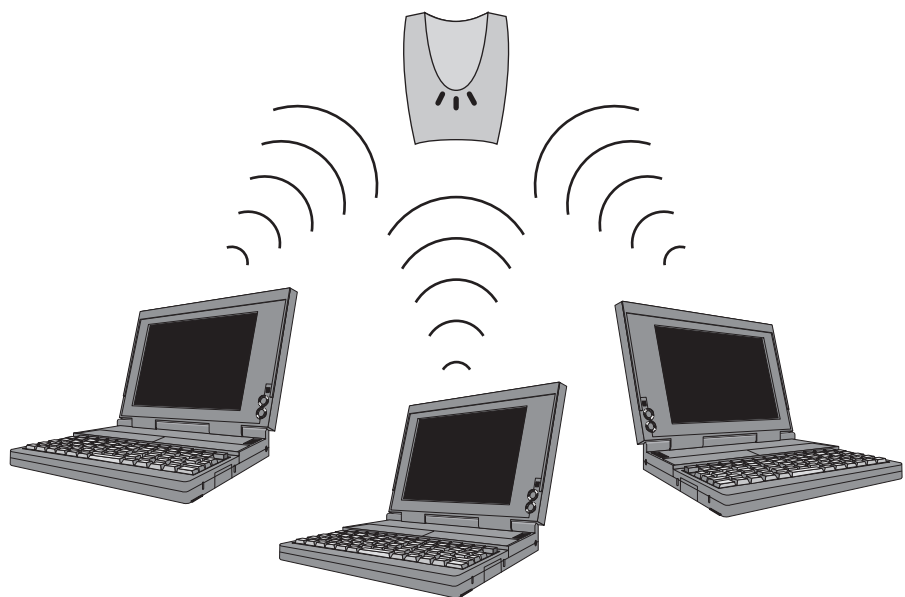


Figure 1-2 Wireless network

When you install a new wireless network, follow these steps:

1. Configure one client.
2. Select the IP settings of this client.
3. Install the Access Point and connect it.
4. Optionally, configure the Access Point from the already configured client using the Web Interface (see chapter 3: '[Configuring the Access Point](#)' on page 21).
5. Install other clients if this is applicable to your situation.

1.4.2 Extending a wired network with one or more Access Points

When your Access Point is an extension to a wired network, it is recommended that you make sure that the wired network is completely functional to exclude existing problems.

See [Figure 1-3](#).

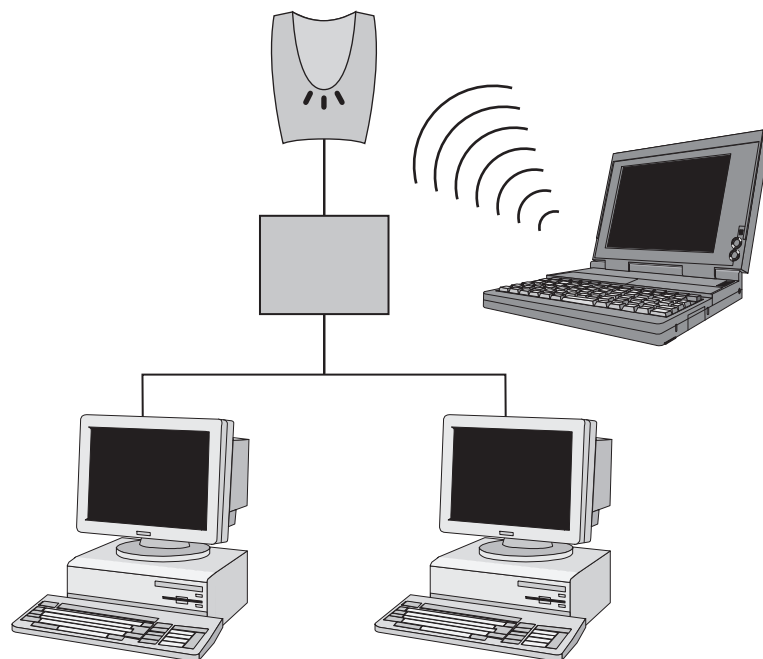


Figure 1-3 Adding an Access Point to a wired network

Follow these steps:

1. Install the Access Point and connect it.

2. Optionally, configure the Access Point from an existing computer in the network using Web Interface (see chapter 3: [‘Configuring the Access Point’ on page 21](#)).

The IP settings for the Access Point can be retrieved from the network (see also Appendix A: [‘TCP and IP settings’ on page 49](#)).

3. Install the client(s).

1.4.3 Connecting an Access Point directly to a computer

You can also add an Access Point directly to your computer. See [Figure 1-4](#).

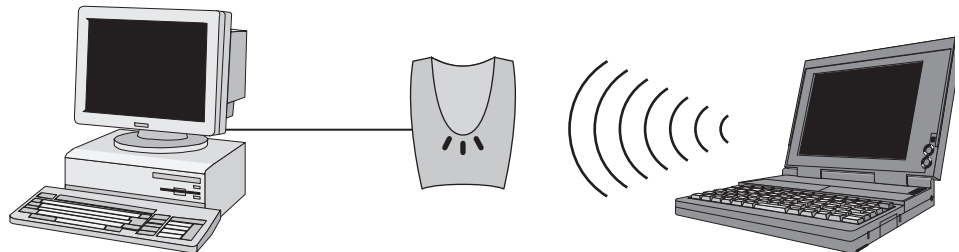


Figure 1-4 Connecting an Access Point directly to a computer. AP1

Follow these steps:

1. Install the Access Point and connect it to a network card in your computer.
2. Optionally, configure the Access Point from your computer using Web Interface (see chapter 3: [‘Configuring the Access Point’ on page 21](#)).
3. Install the client(s).

2 Installing the Access Point

2.1 Introduction

This chapter describes the physical installation of an Access Point.

Table 2-1 Overview of this chapter.

Section	Describes
2.2	Considerations about the physical environment of an Access Point.
2.3 , 2.4 , 2.5	How to install an Access Point.
2.6	How to connect the Access Point.
2.7	Explanation of the LEDs.
2.8	How to unlock/reset the Access Point.

2.2 Access Point environment

When you install an Access Point, you must consider the following items:

- Connection to the electricity net.
- Connection to the network.
- Environment of device (heat/humidity): see chapter 5: '[Technical specifications 11 Mbps WLAN Access Point](#)' on page 41.
- Range of device: see chapter 5: '[Technical specifications 11 Mbps WLAN Access Point](#)' on page 41.

2.3 Physical installation of the Access Point



The Access Point must be mounted in a vertical position always.

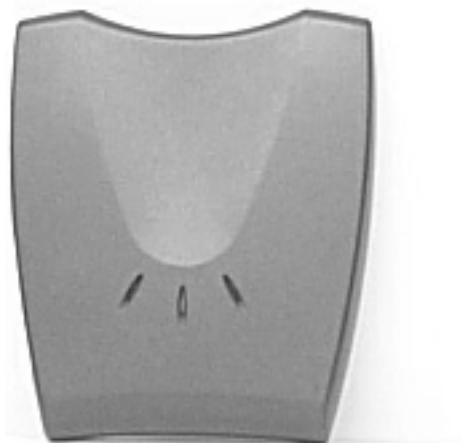


Figure 2-1 The Access Point

The Access Point can be installed in 2 different ways:

- desktop mount,
- wall mount.

The foot socket is used for the desktop mount.

2.4

Desktop mount installation

See chapter 5: [Technical specifications 11 Mbps WLAN Access Point](#) on page 41 for regulations on the required free space around the Access Point.

Determine where you want to place the Access Point. Make sure you have a clear area on a desktop.

You can insert the Access Point in the foot socket as shown in [Figure 2-2: 'Access Point for desktop use' on page 15](#).

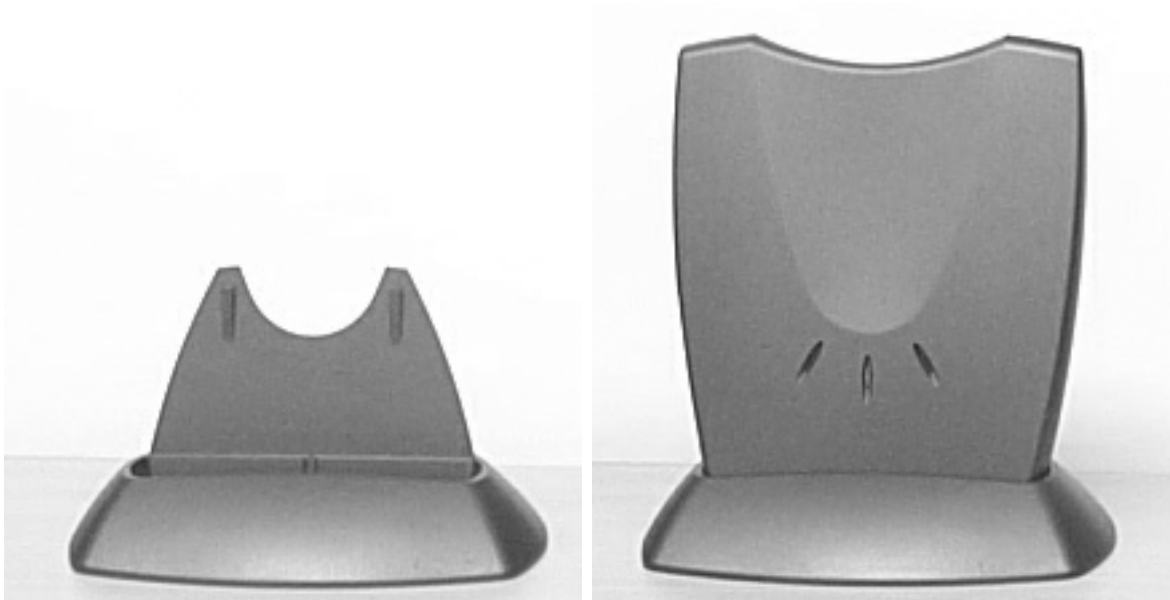


Figure 2-2 Access Point for desktop use

Step by step installation of the foot socket for desktop use:

Simply insert the Access Point into the foot socket.

2.5

Wall mount installation

See chapter 5: ['Technical specifications 11 Mbps WLAN Access Point' on page 41](#) for regulations on the required free space around the Access Point.



Before you start drilling holes into a wall, make sure that part of the wall is clear of electricity and water pipes.

The wall mount socket package contains two screws and plugs to fasten the socket to the wall (see [Figure 2-3: 'Backside of the Access Point' on page 16](#)).

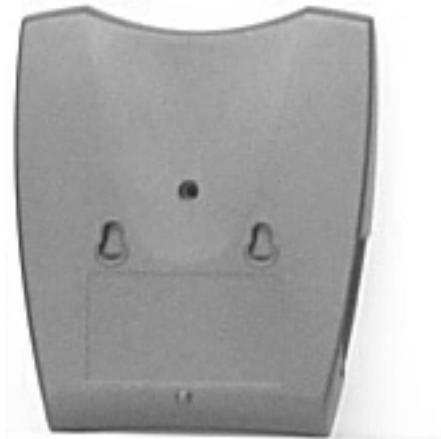


Figure 2-3 Backside of the Access Point

Step by step wall mount installation:

1. Determine the position of the screws. The screws must be 5 cm apart to fit the keyholes at the back of the Access Point.
2. Drill holes in the wall at the location of the dots,
3. Insert the plugs into the holes.
4. Fasten the screws into the plugs, and leave about 3 mm of space between wall and screw head.
5. Attach the Access Point to the screws.

2.6

Connecting the Access Point

Your Access Point is now ready to be connected to the electricity net and to your network. See [1.4: 'Adding Access Points to your \(network\) environment' on page 9](#) on how to add Access Points to your network or environment.

You can find the power input and the UTP port on the left hand side of the Access Point.

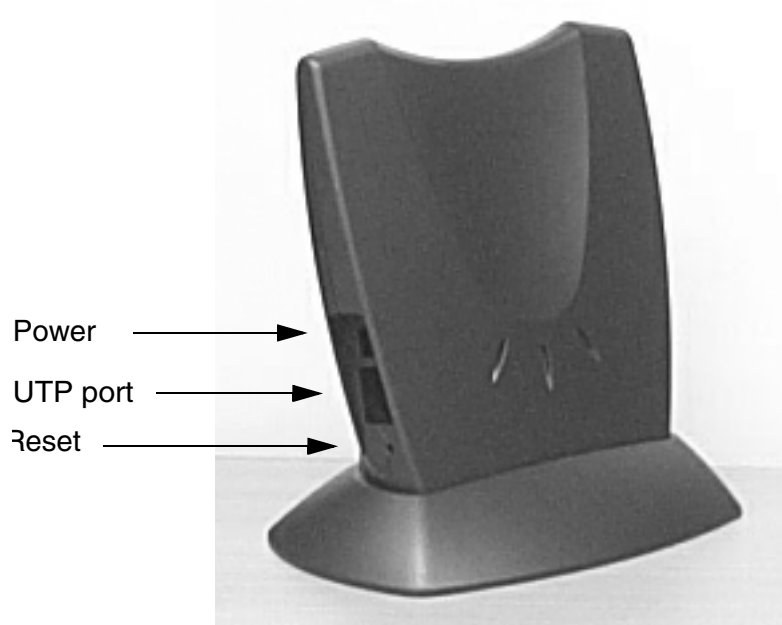


Figure 2-4 Connecting the Access Point

2.6.1 Power adapter

The Access Point package contains a power adapter. Attach it to the Access Point, and then check the power LED (see section [2.7: 'LEDs' on page 18.](#)) to see if you are connected properly.

2.6.2 UTP port

The UTP port can be found next to the power connector on the Access Point.

For a wired connection (see section [1.4.2: 'Extending a wired network with one or more Access Points' on page 10](#) and section [1.4.3: 'Connecting an Access Point directly to a computer' on page 11](#)), attach the UTP Ethernet cable to the Access Point and connect the cable on the other end to either a hub in the network, or a computer.

If you want to connect to an Access Point via a wired connection, it must be connected correctly:

- if the Access Point is connected to a hub or switch, a 'normal' (not a crosswired) cable must be used,
- if the Access Point is connected directly to a computer, a crosswired cable must be used.

2.7

LEDs

The Access Point has three LEDs.

Table 2-2 LEDs

LED	Function
Power	The power LED burns when the Access Point is connected to the electricity net. See also section 2.6: 'Connecting the Access Point' on page 16
Radio signal	The radio LED blinks when the Access Point is active.
Network connection	The network LED burns when the Access Point is used in the network.

[Figure 2-5: 'Access Point LEDs' on page 18](#) shows the LEDs.

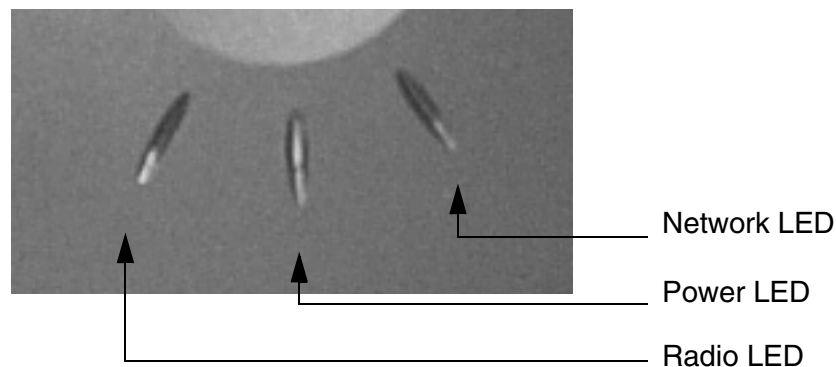


Figure 2-5 Access Point LEDs

2.8

Unlocking the Access Point

The unlock/reset button is found underneath to the power connector and UTP connector. It is a small hole for which you need the end of a paperclip.

You can unlock the Access Point in order to reconfigure it, or reset it to the default factory settings.

2.8.1 Unlocking the Access Point to reconfigure

From the Web Interface you can lock the Access Point, prohibiting configuration changes to it (see section [3.5.8: 'Security against unauthorized configuration'](#)).

To unlock the Access Point so that the configuration changes are allowed again:

1. Insert one end of a paperclip briefly in the hole of the reset button.

The Access Point lock is unlocked. All settings, including the IP settings, are retained.

2. You can now use the Web Interface to manage the Access Point again.

2.8.2 Resetting to the default factory setting

If you press the reset button longer, more than 5 seconds, the Access Point will be reset to the default factory settings:

1. Insert one end of a paperclip into the hole for the reset button and keep it pressed down.

The radio LED will first burn constantly.

2. Release the reset button when the LED has stopped burning.

All settings are deleted.

3. Use KickStart to install new IP settings.

If you have a DHCP server the IP settings will probably remain the same.

4. You can now use the Web Interface to manage the Access Point again.

3 Configuring the Access Point

3.1

Introduction

The Access Point is a ready to use device. It is delivered with default settings which allow you to have access to it without configuring it.

When you do configure the Access Point, you can change the settings with respect to security, radio channels, etc.

Whether you need to configure the Access Point or not, depends entirely on how you apply the Access Point to your environment.

Section [3.2: 'When to configure the Access Point' on page 21](#) discusses the consequences of configuring the Access Point or not.

[Table 3-1](#) describes the contents of this chapter:

Table 3-1 Overview of this chapter

Section	Description
2	When to configure the Access Point
3	Starting the Web Interface for the first time.
4	Launching the Web Interface
5	Web Interface Settings

3.2

When to configure the Access Point

Configuring the Access Point means installing settings with respect to the use of radio channels, security, identification, etc. You only need to configure the Access Point when you want to change these settings.

IP settings can be installed automatically or manually.

Table 3-2 Installing methods for IP settings

Install IP settings	When
Automatically	If the Access Point is part of a network with a DHCP server, the DHCP server assigns the IP settings to the Access Point for you. After that you can configure the Access Point by starting a web browser and inserting the IP address of the Access Point on the address bar. This will start the Web Interface, see section 3.4: 'Launching Web Interface manually' on page 29 .
Manually	If there is no DHCP server, you need to install the IP settings using the KickStart application, see 3.3: 'Starting the Web Interface' on page 22 .

3.3

Starting the Web Interface

When there is no DHCP server in your network, you can assign an IP address to the Access Point and start up the Web Interface with the KickStart application.

The KickStart application is needed only when:

- You start the Access Point for the first time, or
- You have reset the Access Point to factory defaults (see section [2.8.2: 'Resetting to the default factory setting' on page 19](#)) and must install the IP settings again.

The KickStart application can be found on the CD, see section [3.3: 'Starting the Web Interface' on page 22](#).

3.3.1 Installing KickStart

You can install KickStart on a PC in the network to which the Access Point will be connected. Follow the instructions of the install wizard.

3.3.2 Launch KickStart

Double click the KickStart icon. The application starts up.

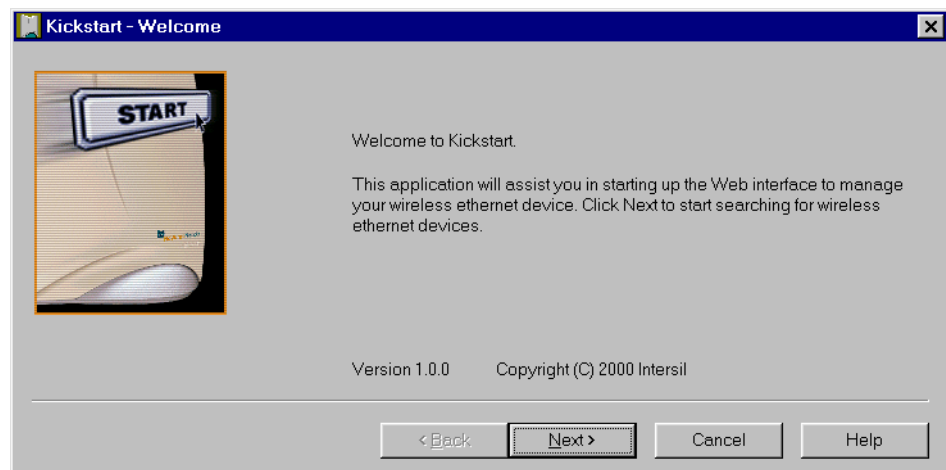


Figure 3-1 Opening screen of the KickStart application

When you click **Next**, KickStart will search for all Access Points within range, whether they have been configured properly or not.

3.3.3 Select wireless ethernet device

You can select the device you want to manage from the list as shown in [Figure 3-2: 'Screen: Select Wireless Ethernet Device' on page 23.](#)

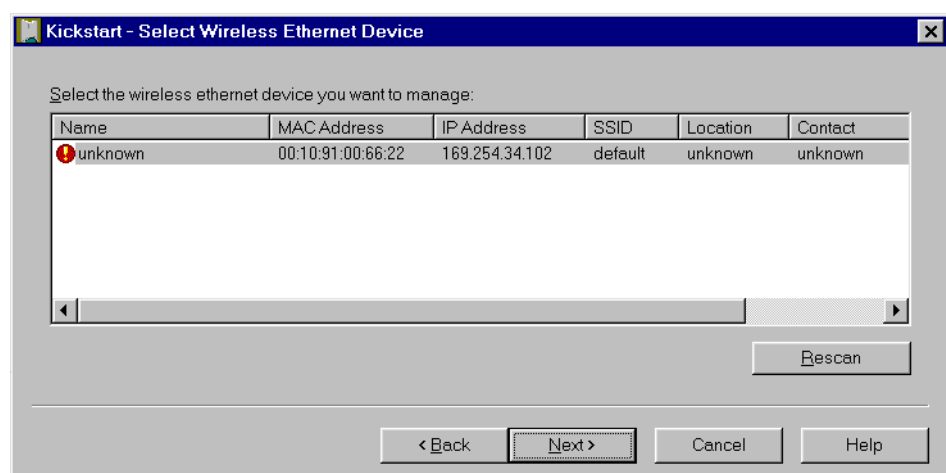


Figure 3-2 Screen: Select Wireless Ethernet Device

After that you can

- click on **Next** to continue to the next screen, or
- click on **Rescan** (see section [3.3.5: 'Scanning and rescanning for devices' on page 24](#)) to rescan for a wireless device.

Section [3.3.4: 'Device data' on page 24](#) explains the data in this screen.

3.3.4 Device data

The columns in the Scan Screen contain the data of the wireless devices that can be found. [Table 3-3](#) explains the device data in these columns (see also Appendix [A: 'TCP and IP settings' on page 49](#)):

Table 3-3 Description of the device data in the Select Wireless Device screen

Column	Description
MAC address	Every Ethernet device has a unique address that is permanently linked to that device. It cannot be changed. See section A.2.6: 'MAC address' on page 52
IP address	In order to access a TCP/IP network, a device must have an IP address in addition to its MAC address. See Appendix A: 'TCP and IP settings' on page 49
SSID	The SSID is also known as Service Set ID. This is the name of your wireless network. See section B.4: 'Service Set ID (SSID)' on page 56
Location	Here the location of the Access Point is displayed. See section 3.5.9: 'Identity' on page 36 on how to edit this field.
Contact	Here the name of the contact person for the Access Point is displayed. See section 3.5.9: 'Identity' on page 36 on how to edit this field.

3.3.5 Scanning and rescanning for devices

If the device that you want to manage is in the list, select it, and click **Next**.

If you click the `Rescan` button, KickStart will search for Access Points again. Use this e.g. to find Access Points that have just been switched on or reset.

If the device that you want to manage is not in the list and is not found after clicking the `Rescan` button, go to section [4.1: 'If KickStart does not find the Access Point you are looking for' on page 39](#).

3.3.6 IP settings

In this screen you can select to either use dynamic or static IP settings. (see chapter [A: 'TCP and IP settings' on page 49](#)).

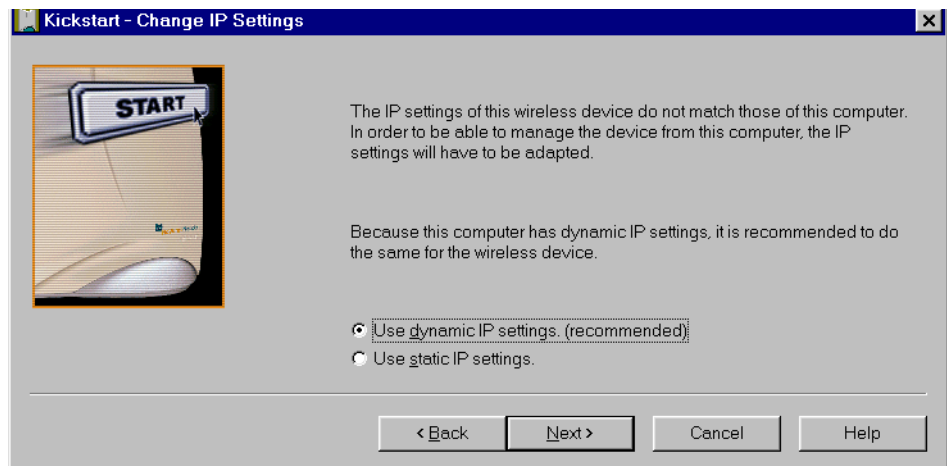


Figure 3-3 Screen: Change IP Settings

Select Dynamic IP settings when you install the Access Point in a network with a DHCP server or Auto IP.

Select Static IP settings when you want to configure the IP settings manually.

Click on the Next button to continue to the next screen.

- If you selected the option `Use dynamic IP settings`, you will continue to the screen Changing IP settings directly, see section [3.3.9: 'Changing IP settings' on page 27](#).
- If you selected the option `Use static IP settings`, you will continue to the screen Set IP address of Wireless Device, see section [3.3.7: 'Static IP settings' on page 26](#).

3.3.7 Static IP settings

When you have selected the option `Use static IP setting` in [Figure 3-3: 'Screen: Change IP Settings' on page 25](#), [Figure 3-4: 'Screen: Set IP Address of Wireless Device' on page 26](#) appears..

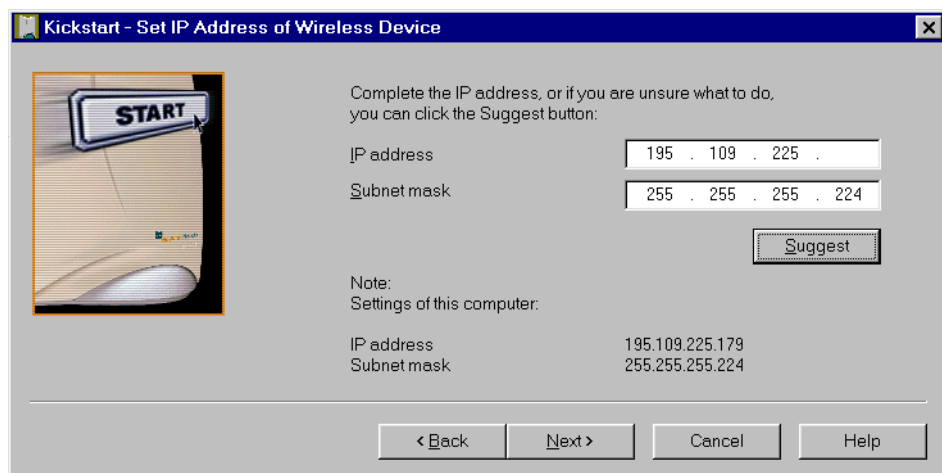


Figure 3-4 Screen: Set IP Address of Wireless Device

In this screen you can either manually insert the IP address and/or Subnet mask, or you can click on the button `Suggest` to let the system find the IP settings.

Click `Next` to continue to the next screen. The screen “Set Gateway of Wireless Device” appears, see section [3.3.8: 'IP settings' on page 27](#).

3.3.8 IP settings

In this screen you can install the Gateway address of the wireless device. Setting a Gateway is optional.

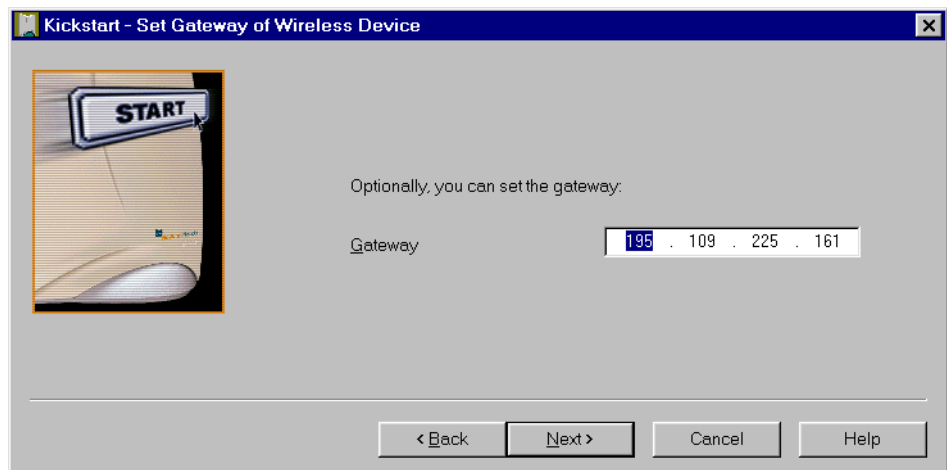


Figure 3-5 Screen: Set Gateway of Wireless Device

Click on **Next** to continue to the next screen, see section [3.3.9: 'Changing IP settings' on page 27](#).

3.3.9 Changing IP settings

KickStart will install the proper IP settings of the device.

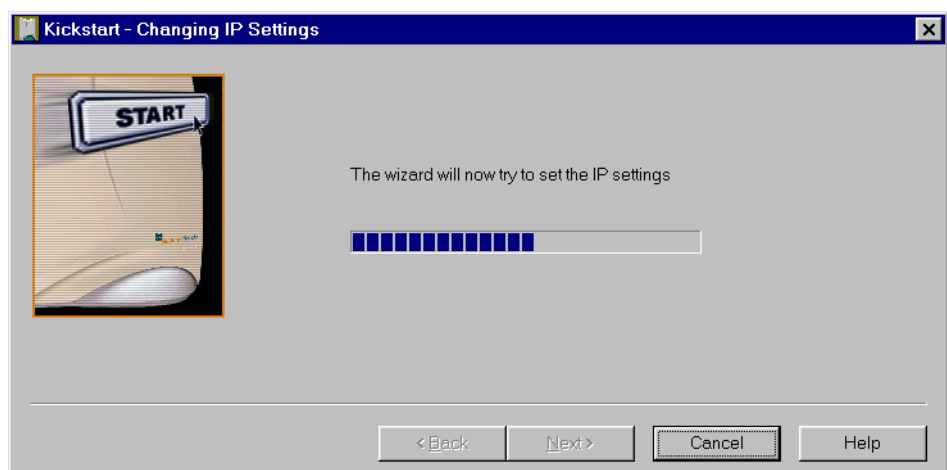


Figure 3-6 Screen: Changing IP settings

If it cannot install the proper IP settings, a warning is given. With the **Back** button you can return to [Figure 3-3: 'Screen: Change IP Settings' on page 25](#) where you can select another method for installing the IP settings.

If the IP settings were successful, the **Next** button becomes active. Click on the **Next** button, and the screen “Ready to KickStart” appears.

3.3.10 Ready to start the Web Interface

If you click **Finish** in this screen, KickStart will launch a Web browser and open the administration page (Web interface) for the Access Point you have chosen. Then KickStart quits.

You can now go to section [3.5: 'Contents of Web Interface' on page 29](#).

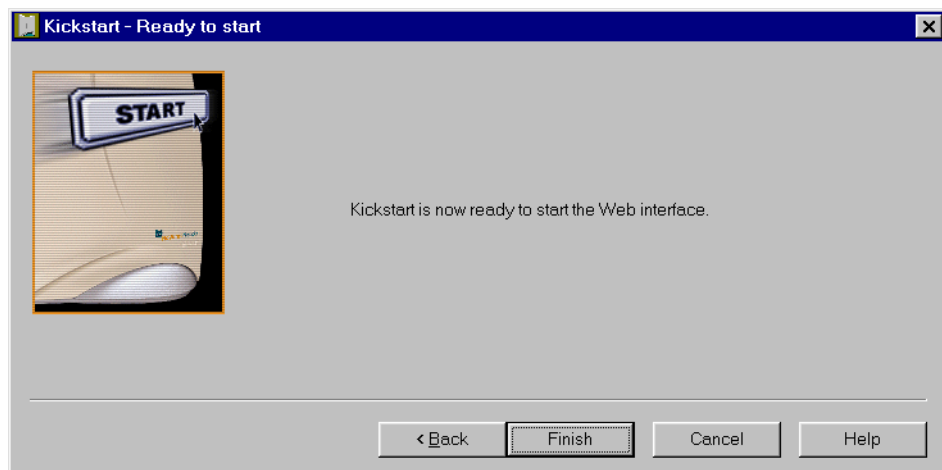


Figure 3-7 Screen: Finish KickStart

When you use KickStart to find an Access Point with correct IP settings, KickStart will go to this page immediately.

It will not allow you to change the [IP address](#) settings. If you want to change these, you must return to [Figure 3-3: 'Screen: Change IP Settings' on page 25](#) where you can select another method for installing the IP settings.

3.3.11 Web Interface is launched

Once the KickStart application has finished and the Access Point is available for configuration in the network, the Web Interface application is launched in a web browser.

You can now edit the settings for the Access Point.

3.4 Launching Web Interface manually

When you know the IP address of an Access Point, you can launch the Web Interface in a web browser for editing.

1. Open a web browser.
2. Insert the web address of the Access Point on the address bar as follows:

http://IP address of the Access Point/

It is recommended to bookmark your web address for the Web Interface.

3.5 Contents of Web Interface

The Web Interface application contains the following subjects:

Table 3-4 Contents of Web Interface

Page	Description
Settings Summary	On this page you will find an overview of the current settings.
Wireless Settings	The settings of the wireless device are displayed here, and you can edit some of these settings.
Security against unauthorized network access	On this page you can allow or deny access to the Access Point by clients.
Security against Eavesdropping	On this page you can install security methods to prevent eavesdropping on the connection to the Access Point.
Security against unauthorized configuration	On this page you can manage the Write Community String for the Access Point and lock the management of the Access Point.
Identity	Here the identity data of the Access Point are displayed, and you can edit some of these data.
IP Settings	The IP, subnet, and gateway addresses of the Access Point are displayed here.

3.5.1 Settings Summary

This page contains a summary of the settings of the Access Point.

To display the Settings Summary page, click .

You cannot change any of the settings in this page. [Table 3-5](#) contains the references to the pages where these settings can be changed.

Table 3-5 Web Interface page: Settings Summary

Setting	Refer to Web Interface page
SSID	see section 3.5.2: 'Wireless Settings' on page 30
IP address	see section 3.3.8: 'IP settings' on page 27
Access Control	see section 3.5.3: 'Security against unauthorized network access' on page 31
Eavesdropping mode	see section 3.5.6: 'Security against eavesdropping' on page 34

To change these settings:

SSID

IP address

Access Control

Eavesdropping mode

3.5.2 Wireless Settings

On this page you can install items such as the identification of the device and the radio channel.

To display the Wireless Settings page, click .

[Table 3-6](#) contains the descriptions of the options in this page.

Table 3-6 Web Interface page: Wireless Settings

Option	Description
SSID	This is the Service Set ID. Only Access Points and clients that share the same SSID are able to communicate with each other. See also section B.4: 'Service Set ID (SSID)' on page 56 .

Table 3-6 Web Interface page: Wireless Settings

Option	Description
Radio Channel	This is the channel that the Access Point uses to transmit and receive information (see also section B.5.4: 'Radio Channels' on page 57). The channel that you select here is restricted to the channels that can be used within your Regulatory domain.
Regulatory Domain	The Regulatory domain is displayed here. Every country has a Regulatory Domain concerning radio channels that can be used to transmit and receive signals (see also section B.5.3: 'Regulatory Domain' on page 57). This setting is a factory default that cannot be changed.

3.5.3 Security against unauthorized network access

To protect your network against unauthorized network access you can create an Access Control List (ACL).

To display the Security against unauthorized network page,

click .

You can choose to allow access to all clients or deny access to all clients, and create a list of exceptions for both options.

The changes to the Access Control List on this page are accepted when you click on the OK button.

The first section in this page contains two **Access options**. [Table 3-7](#) describes these options.

Table 3-7 Web Interface page: Security against unauthorized network access.

Options	Description
All clients are accepted	When you select this option, you allow access to all PC Cards, except for ones that you specify in the Exception list. This option can be useful if you do not want to keep track of all PC Cards but you do know some PC Cards that need to be denied access because they were stolen.
Deny all clients	When you select this option, you deny access to all PC Cards except the ones you specify in the Exception List

Once you have selected whether you want to allow access to all clients or deny all clients, you can create an **Exception List**. See section [3.5.4: 'To add a a client to the exception list' on page 32](#) and section [3.5.5: 'To delete a client from the exception list' on page 33](#).



Note. The title of the Exceptions list shows

- “denied clients” when the exceptions are applicable to the option *Allow access to all clients*.
- “accepted clients” when the exceptions are applicable to the option *Deny access to all clients*.

3.5.4 To add a a client to the exception list

Follow these steps to add a client to the exception list (see section):

1. Click on the button `Add client...` and a separate window opens

(see [Figure 3-8](#)).

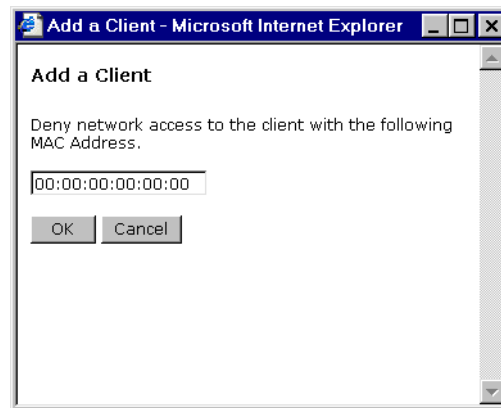


Figure 3-8 Web Interface dialog window: Add client

If you selected “Allow access to all clients, you can type the MAC address of the client that you want to deny access to in the field `MAC Address`.

If you selected “Deny access to all clients, you can type the MAC address of the client that you want to allow access to in the field `MAC Address`.

2. Then click on the button `OK`. The client is now added to the exception list.

3.5.5 To delete a client from the exception list

Follow these steps to add a client to the exception list (see section):

1. Click on the button `Delete clients`. A separate window opens in which the Exception list is displayed (see [Figure 3-9](#)).

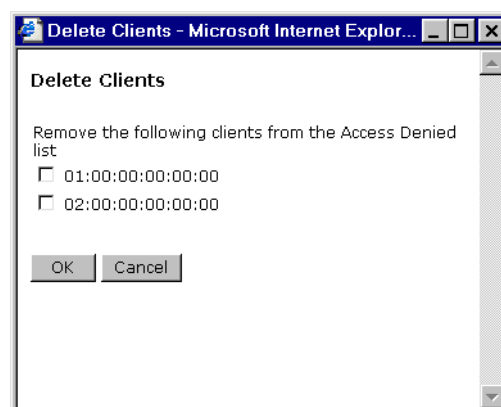


Figure 3-9 Web Interface dialog window: Delete clients

2. Select the MAC Address(es) of the client(s) that you want to remove from the list.
3. Then click on the button **OK**. The exception list is updated.

3.5.6 Security against eavesdropping

On this page you can install the encryption methods that secure the data flow from and to the Access Point.

To display the Security against eavesdropping page,

click .

You can use the different authentication methods. [Table 3-8](#) describes the available methods.

Table 3-8 Web Interface page: Security against eavesdropping

Option	Description
IEEE Authentication	Select this method to allow clients to access to the Access Point either without security (Open Systems) or with a WEP security method. (See Appendix B.6.1: 'IEEE authentication' on page 58.)
Open System	When you select this option, clients have access without a password. (See Appendix B.6.2: 'Open Systems method' on page 58.)
WEP Change password	When you select this option, you can activate the WEP security method. (See Appendix B.6.3: 'WEP method' on page 58.) A Web Page Dialog called Enter New Password appears, see section 3.5.7: 'Change WEP password' on page 34.

3.5.7 Change WEP password

When you have selected the option **WEP Change password**, the web page of [Figure 3-10: 'Web Interface dialog window: Enter the WEP settings' on page 35](#) appears. Follow the instructions below to change

the WEP password:

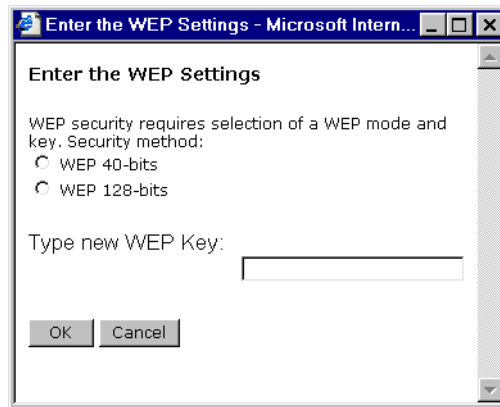


Figure 3-10 Web Interface dialog window: Enter the WEP settings

1. Select the WEP method: 40 bit or 128 bit.

2. Enter a password:

WEP 40: the password must contain exactly 10 characters,

WEP 128: the password must contain exactly 26 characters.



Only the following alphanumeric characters are allowed in the password:

- 0 to 9,
- a to f.

3. Click on OK.

3.5.8 Security against unauthorized configuration

On this page you can install a password, the so-called “Write Community String”, that is required to make changes to the Access Point and lock the Access Point.

To display the Security against unauthorized configuration page,

click .

1. Change Password.

Click on the button **Change Password** and a window opens (see [Figure 3-11](#)) in which you can enter a password that is required to edit the settings of the Access Point with the Web Interface.

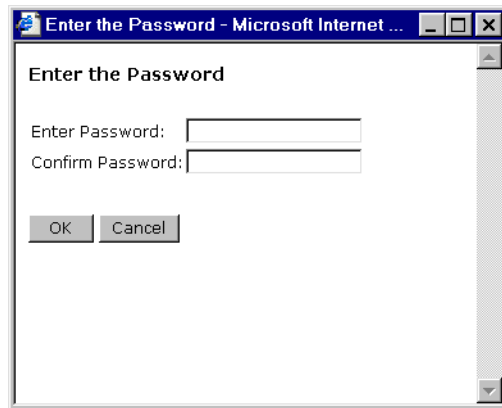


Figure 3-11 Web Interface dialog window: Enter the Password

2. Lock Access Point.

- Click on the button **Lock Access Point** to lock it.

A warning appears: “Are you sure to lock the Access Point? this will immediately prevent making configuration changes. You will still be able to view the current settings.”

- Click on **OK** to lock the Access Point.

No more configuration changes to the Access Point are allowed.

To unlock the Access Point: see section [2.8.1: ‘Unlocking the Access Point to reconfigure’ on page 18](#).

3.5.9 Identity

This page contains the physical information on the Access Point.

To display the Identity page, click .

[Table 3-9](#) explains the options in this web page.

Table 3-9 Web Interface page: Identity of the Access Point.

Option	Description
Location	This is a text field in which you can enter e.g. where the Access Point is installed (“Room 412”). You can put any text into this field; the text has no influence on how the Access Point works.
Contact	This is a text field in which you can enter e.g. the name of the systems administrator responsible for the Access Point (“admin@domain.com”). You can put any text into this field; the text has no influence on how the Access Point works.
MAC address	The MAC address is displayed here. See section A.2.6: ‘MAC address’
Access Point Type	Information on your type of Access Point is displayed here.
Firmware Version	Here the version of the Access Point firmware is displayed.

When you have filled in or changed your data:

- Click on `Cancel` to discard the changes.
- Click on `Apply` to apply the changes to the Access Point.

3.5.10 IP Settings

To display the IP Settings page, click .

On this web page the following IP settings are displayed:

- IP Address
- Subnet mask
- Gateway

It is not possible to change these addresses from within the Web Interface.

If you want to change the IP settings of an Access Point that has already proper IP settings, you need to use KickStart and change them manually (see [Section 3.3: ‘Starting the Web Interface’ on page 22](#)).

4 Troubleshooting

4.1 If KickStart does not find the Access Point you are looking for

There are several possible causes depending on the way the Access Point is connected to the network.

4.1.1 Problems on the wireless side

Always check the status of the LEDs to see whether you have:

- electricity problems,
- radio signal problems, or
- networking problems.

Table 4-1 Troubleshooting the wireless connection of an Access Point

Possible cause	Solution
Is the Access Point powered up.	Check the power LED. Check if the Access Point is connected.
Is the Access Point is in range of the WLAN card on your computer?	Check the radio signal LED. See section 5.2: 'Radio specifications' on page 41 to check for possible problems with respect to range.

Table 4-1 Troubleshooting the wireless connection of an Access Point (vervolg)

Possible cause	Solution
Is there a network connection?	Check the network LED. The Access Point may take up to a minute to find an IP address it can use if Auto IP is used to assign an IP address.
Client cannot make connection	A wireless client is not (yet) connected to the Access Point. Refer to the manual of the wireless client on how to connect.

4.1.2 Problems on the wired side

Always check if your cables and connections are in good order and properly installed.

Table 4-2 Troubleshooting the wired connection of an Access Point

Possible cause	Solution
Has the proper cable been used?	• If the Access Point is connected to a hub, a 'normal' (not a crosswired) cable must be used, • If the Access Point is connected directly to a computer, a crosswired cable must be used.

5 Technical specifications

11 Mbps WLAN Access Point

5.1 General Specifications

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)	

Environmental specifications	
Operating temperature (ambient)	0°C to 40°C (32°F to 104°F)
Humidity	95%

Power specifications	
DC power supply	In 110-230 VAC 50 Hz 150 mA
	Out 5 VDC 1 A
11 Mbps WLAN Access Point	In 5 VDC 1 A

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™)	

5.2 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	

5.3 Security specifications

Data encryption	
AirLock™ Security Software, 128-bit key length	
Key Management	
Automatic Dynamic Key Allocation (ADKA) through public key	

5.4 Other specifications

Utility Software	
Web Interface	
KickStart	
Physical Dimensions	
Height	145 mm
Width	121 mm, with foot socket 141 mm
Depth	26, with foot socket 10,1

6 Regulatory notes and statements

6.1 Wireless LAN, Health and Authorization for use

Radio frequency electromagnetic energy is emitted from Wireless LAN devices. The energy levels of these emissions however are far much less than the electromagnetic energy emissions from wireless devices like for example mobile phones. Wireless LAN devices are safe for use by consumers, because they operate within the guidelines found in radio frequency safety standards and recommendations. The use of Wireless LAN devices may be restricted in some situations or environments for example:

- On board of airplanes, or
- In an explosive environment, or
- In case the interference risk to other devices or services is perceived or identified as harmful.

In case the policy regarding the use of Wireless LAN devices in specific organizations or environments (e.g. airports, hospitals, chemical/oil/gas industrial plants, private buildings etc.) is not clear, please ask for authorization to use these devices prior to operating the equipment.

6.2 Regulatory Information/disclaimers

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment. The Manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, or the substitution or attachment of connecting cables and equipment other than manufacturer specified. It is the responsibility of the user to correct any interference caused by such unauthorized modification, substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from failing to comply with these guidelines.

6.3 USA-FCC (Federal Communications Commission) statement

This device complies with Part 15 of FCC Rules.

Operation is subject to the following two conditions:

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

6.4

FCC Radio Frequency Exposure statement

This Wireless LAN radio device has been evaluated under FCC Bulletin OET 65C and found compliant to the requirements as set forth in CFR 47 Sections 2.1091, 2.1093, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices. The radiated output power of this Wireless LAN device is far below the FCC radio frequency exposure limits. Nevertheless, this device shall be used in such a manner that the potential for human contact during normal operation is minimized. When using this device, a certain separation distance between antenna and nearby persons has to be kept to ensure RF exposure compliance. In order to comply with RF exposure limits established in the ANSI C95.1 standards, the distance between the antennas and the user should not be less than 30 cm (12 inches).

6.5

FCC Interference Statement

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. If not installed and used in accordance with the instructions, it 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 and correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the distance between the equipment and the receiver.
3. Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

6.6

Export restrictions

This product or software contains encryption code which may not be exported or transferred from the US or Canada without an approved US Department of Commerce export license.

6.7

Europe - EU R&TTE Declaration of Conformity

This Wireless LAN Radio device is tested to and conforms with the essential radio test suites included in following standards:

Standard	Description
EN 60950,ed. (1992), incl. A1(1993), A2(1993), A3(1995) and A4(1997)	Safety of information technology equipment, including electrical business equipment.
ETSI EN 300 328 Part 1 V1.2.2 (2000-07) Part 2 V1.1.1 (2000-07)	Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Part 1: Technical characteristics and test conditions Part 2: Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive.
ETSI EN 301 489 Part 1 V1.2.1 (2000-08) Part 17 V1.1.1 (2000-09)	Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements Part 17: Specific conditions for Wideband data and HIPERLAN equipment

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)).

6.8

Restricted Wireless LAN device use in EU

Restricted use of this Wireless LAN device in EU member countries is as follows:

EU country	Local restriction
Belgium /België /Belgique	Indoor operation allowed in channels 1 to 13 in frequency band 2400-2483.5MHz. Outdoor operation is limited to 2460-2483.5. Please contact “Belgisch Instituut voor Post and Telecommunicatie” (BIPT) for authorization, registration and licensing. Gebruik binnen gebouwen toegestaan in frequentie band op kanalen 1 tot en met 13 (2400-2483.5MHz). Gebruik buiten gebouwen is gelimiteerd tot 2460-2483.5MHz. Neem voor registratie of licentie contact op met “Belgisch Instituut voor Post and Telecommunicatie” (BIPT). L'utilisation en intérieur est autorise sur les canaux 1 a 13 (2400 - 2483.5 MHz). L'utilisation en extérieur est limitée au fréquences 2460 - 2483.5 MHz. Pour les autorisations, enregistrements et licences, veuillez contacter l'IBPT (Belgisch Instituut voor Post en Telecommunicatie).
Germany /Deutschland	Outdoor use allowed only with a license. Please contact “Regulierungsbehörde für Telekommunikation und Post “ (REGTP) for authorization, registration and licensing. Im Freiegebrauch ließ nur mit einer Lizenz. Bitte kontaktes “Regulierungsbehörde für Telekommunikation und Post “ (REGTP) für Ermächtigung, Ausrichtung und das Genehmigen.
France	Indoor use only, no outdoor use allowed. Only channels 10 to 13 (2457 MHz to 2483.5 MHz respectively) are authorized for indoor use in France. Operation of this device on any other channel is not allowed. Indoor installation is required to have a license. Please contact ART (Autorite de Regulation des Telecommunications. Http://www.art-telecom.fr) for authorization, registration and licensing. Seuls les canaux 10 a 13 (2457-2483.5MHz) peuvent etre utilises en France. L'utilisation de ce produit sur d'autres frequences n'est pas autorisee. Toute utilisation , qu'elle soit interieure ou exterieure est soumise a autorisation. Vous pouvez contacter l'ART (Autorite de Regulation des Telecommunications. Http://www.art-telecom.fr) pour la procedure a suivre.

Italy /Italia	Indoor use only, no outdoor use allowed. Indoor installation is required to have a license. Please contact “Ministero delle Comunicazioni, Direzione Generale Pianificazione e Gestione Frequenze” (DGPF) for authorization, registration and licensing. Usare soltanto all'interno, non e' consentito l'uso all'esterno. E' necessaria l'installazione interna per ottenere una licenza. Per ottenere l'autorizzazione, la registrazione e la licenza, contattate l' “Ministero delle Comunicazioni, Direzione Generale Pianificazione e Gestione Frequenze” (DGPF).
Netherlands / Nederland	Indoor operation allowed in frequency band 2400-2483.5MHz. Outdoor operation is limited to 2451-2471 MHz and is required to have a license. Please contact “Rijks Dienst Radio communicatie” (RDR) for authorization, registration and licensing. Gebruik binnen gebouwen toegestaan in frequentie band 2400-2483.5 MHz. Gebruik buiten gebouwen is gelimiteerd tot 2451-2471 MHz en is gebonden aan een licentie. Neem voor registratie of licentie contact op met de “Rijks Dienst Radio communicatie” (RDR).

A TCP and IP settings

A.1

Introduction

Before installing a wireless network device you must analyze your the network environment. The information in this appendix is only helpful in determining which information is needed for a proper installation of such a device.

This appendix explains how devices in a network are identified in order to communicate with each other. Chapter 3: '[Configuring the Access Point](#)' on page 21 contains the instructions on how to apply this information to your situation

Table A-1 Overview of this chapter

Section	Description
A.2	Communication in a network
A.3	IP configuration

A.2

How do computers communicate in a network

Computers use protocols to communicate to each other. The protocol that is used between computers (and other network devices) that are connected to the internet is TCP/IP (Transmission Control Protocol/ Internet Protocol). This is also the main protocol in many other computer networks.

The internet resembles the telephone network to some extent. Like a phone number that uniquely identifies one telephone connection, IP addresses are used to determine to which computer the data must be sent. An [IP address](#) looks like this: 192.168.201.160. Each of the four groups is represented in the computer by one byte, so only numbers from 0 to 255 can be used for a group.

IP addresses are meant to be unique world-wide. To achieve this, IP addresses are assigned (you can't just start using random addresses, but you have to ask for them). Usually, your Internet Service Provider will assign you a [IP address range](#) you can use.

A.2.1 IP address

An IP address consists of two parts. The table below describes these two parts.

Table A-2 Sections of the IP address

Part	Identifies	Description
First part All addresses on the subnet share this part of the IP address.	subnet (local network) to which the computer is attached	This part of the address is also known as the 'network portion'; it is similar to the area code of a telephone number.
Second part	identification of the device	This part of the address is also known as the 'node portion', it is like the subscriber number in a telephone number.

The division between network portion and node portion is not obvious from what the IP address looks like. The division isn't in a fixed place either. This is because not all subnets have the same size. Subnets can be small (16 computers) or very large (16 million computers).

To indicate which part of an IP address is the subnet, and which is the computer identification, IP uses a [Subnet mask](#).

A.2.2 Subnet mask

The subnet mask defines which IP addresses are 'local' (i.e. are part of your subnet) and which are not local (but have to be reached via the internet). Compare this to calling someone via telephone: you can reach 'local' numbers by just entering the subscriber's number, but for numbers that aren't local you need the area code plus the subscriber's number.

The subnet mask looks like an [IP address](#). When you translate the subnet mask to a binary number, it breaks down into two sections: first a series of 1s and then a series of zeroes (e.g. a subnet mask of 255.255.255.0 translates to 11111111.11111111.11111111.00000000). The 1s identify the network portion, the zeroes identify the node portion of the address. The subnet mask in this example has 8 bits available for local addresses (i.e. 256 different local addresses can be used).

An example: on a computer, the network settings are defined with an IP address of 192.168.201.173 and a subnet mask of 255.255.255.224. These would be represented in binary like this:

IP address:

```
11000000.10101000.11001001.10101101
```

subnet mask:

```
11111111.11111111.11111111.11100000
```

The subnet mask shows that the first 27 bits are the network portion of the address, the last 5 bits are the node portion, which means there is room for 32 addresses on this network (all numbers between 00000 and 11111 in binary).

A.2.3 IP address range

All addresses in this network share the first 27 bits. The first address in the local network is 192.168.201.160. The last address is 192.168.201.192. In binary:

First address:

```
11000000.10101000.11001001.10100000
```

Last address:

```
11000000.10101000.11001001.10111111
```

Such a group of addresses is also called an IP address range.

A.2.4 Reserved addresses

The first and last addresses in a range cannot be assigned to computers in your network. These addresses have special functions.

The first address in a range is also known as the network address, the last address is the broadcast address.

Subnet masks are sometimes written down as 192.168.201.160/27, where 192.168.201.160 is the first address (or 'network address') in the range, and 27 is the number of 1s in the binary representation of the subnet mask (this subnet mask can also be written as 255.255.255.224).

A.2.5 Gateway

If a device wants to communicate with another device it will determine if that [IP address](#) is in the same subnet as its own IP address. If it is, it can communicate directly with the other, if it isn't, the situation is more complicated; it has to communicate with another subnet.

To communicate between subnets there has to be a connection between the 2 subnets. This connection is made via devices known as gateways. If a device wants to communicate with a device in another subnet it sends the information to the gateway, and the gateway takes care of the rest of the transport.

In order to do this, the sender needs to have the IP address of the gateway for his subnet. Normally, the lowest available node number in the subnet (the network address plus one) is used as the gateway address.

A.2.6 MAC address

Every Ethernet device has a unique address that is permanently linked to that device. It cannot be changed. On every wireless device, the MAC address is printed on its type label.

The MAC address consists of six groups of two digits each (e.g. 00:10:91:00:00:00).

A.3 IP configuration

The most basic way to configure IP settings is by entering the numbers manually on every host. This is somewhat complicated because every host in the subnet has to have the same subnet number but a unique node number. Also, the correct [Subnet mask](#) will have to be entered. Not doing this properly will result in errors.

To simplify managing an IP network, several automated methods have been introduced. The two most important ones are [DHCP](#) and [Auto IP](#).

A.3.1 DHCP

When a network uses DHCP (Dynamic Host Configuration Protocol), one host in the network contains a DHCP server. Whenever a device joins the network it asks the DHCP server for an [IP configuration](#).

The DHCP server sends back a unique [IP address](#), the [Subnet mask](#) for this subnet and the IP address of the [Gateway](#). The DHCP server keeps track of which hosts have requested an IP address and which IP they have been given.

For large networks, DHCP is a convenient way of managing IP configurations, but in small networks the benefits do not compensate the overhead of managing the DHCP server.

You must make a reservation in the DHCP server for the [MAC address](#) of a wireless network device before you configure the device. With the KickStart application you are then able to scan for the MAC address and obtain the IP address, subnet mask and/or gateway automatically.

A.3.2 Auto IP

Auto IP, also known as APIPA (Automatic Personal IP Assignment) is a method in which no server is needed.

Every host that joins the network will look for a unique node number in the subnet 169.254.____.____ (i.e. network address is 169.254.0.0, [Subnet mask](#) is 255.255.000.000).

The host will do this by randomly choosing a node number and then checking to make sure no other host is using that [IP address](#). If the IP address is already in use, the host will try again with another random IP number.

It is possible the address is used by a computer which was not switched on or connected during this verification; in that case you will likely get an error message on both computers later (when the other computer is switched on or connected).

APIPA is supposed to be used on a non-routed network (i.e. a network that will never be connected to other networks or the internet).

B Wireless LAN

B.1

Introduction

This Appendix explains some of the basic terms and concepts of Wireless LANs.

See the specifications of your device for details on the performance of your device

Table B-1 Contents of Appendix B. Wireless LAN's

Section	Description
B.2	This section explains the basic features of a Wireless LAN.
B.3	This section explains the basic features of an Access Point.
B.4	Wireless LAN's require an extra identification: the Service Set Identification.
B.5	This section describes some of the physics of an Access Point
B.6	Wireless LAN's require extra security on eavesdropping. This section describes some of the security methods.

B.2

Wireless LAN

Wireless LAN's transmit and receive data through the air through radio frequency (RF) technology, minimizing the need for wired connections. Wireless LAN's use Access Points (see section [B.3: 'The Access Point' on page 56](#)) to connect computers to each other and to the network.

Through Wireless LAN's, you can access shared information without looking for a place to plug in. A network administrators can install or expand networks without installing or moving wires.

Applications and networking on a Wireless LAN function just like they do on a wired LAN.

Most importantly: to use a wireless LAN, you do not need to be an expert. All you have to do is to find an Access Point in the range of your laptop and connect.

B.3 The Access Point

An Access Point is similar to a hub. It connects computers to each other and to a network. It functions as a node in a network. Only the Access Points on a Wireless LAN require cabling.

An Access Point in itself cannot give access to the Internet because data exchange with the Internet needs to be routed through a gateway. Whether an Access Points also gives access to the Internet depends on its firmware.

Different types of Access Points can use different types of Radio Frequency signals that are not compatible. It is recommended to check whether the type of Wireless LAN and your PC card are compatible when you connect in a unfamiliar network environment.

B.4 Service Set ID (SSID)

The Service Set ID is the name of your wireless network that you connect to.

All the wireless devices connected to each other must share this SSID.

B.5 Physics of an Access Point

B.5.1 Range

A wireless LAN device uses RF waves (Radio Frequency) to transmit and receive data. The range of the propagated power depends on the device and the environment. Indoor environments contain objects such as walls, metal objects, and even people that can effect the propagation of the radiated power.

Although RF energy can penetrate through most indoor walls and other obstacles, these obstacles may influence the quality of the signal of the wireless device.

When placing wireless LAN device you must consider all possible obstacles and test the range of the device using a client device to make a connection and moving around to test the strength of the signal.

When you place more than one wireless LAN device, consider the range that each device covers.

For the range of your device(s); see the specifications of your device.

B.5.2 Data rates

Wireless LAN devices operate at much faster speeds than modems.

The data rates on a wireless link are determined by:

- the range of the device,
- proper propagation of the signal ((conducting) obstacles,),
- interference of other devices
- number of users.

Some devices can handle more than one data rate; see the specifications of your device.

B.5.3 Regulatory Domain

Every region or country has an institution/agency that governs radio transmissions. Such a region is called a regulatory domain.

A wireless LAN uses a spectrum of radio frequencies for which no end-user license is needed.

Europe (excluding France and Spain) are governed by the ETSI (the European Telecommunications Standards Institute). This is a non-profit making organization whose mission is to produce telecommunications standards.

The ETSI regulates the radio channels (see section [B.5.4: 'Radio Channels' on page 57](#)) that can be used in your regulatory domain

B.5.4 Radio Channels

Each Access Point in the network forms the centre of a cell, i.e. an area in which the radio signal of an Access Point is sufficiently good to join with.

The radio channels that you are allowed to use depend on both the capabilities of the PC cards you are deploying, as well as the regulations in your area (see section [B.5.3: 'Regulatory Domain' on page 57](#)).

For a single Access Point you can choose any of the available channels. However, when there are more Access Points in the neighborhood, they must send and receive preferably on different channels for a maximum throughput. The cells should overlap slightly to guarantee seamless wireless connectivity everywhere.

B.6 Security

Wired LAN's require security techniques against unauthorized access to and management of the network.

Security on a Wireless LAN requires additional techniques to protect from eavesdroppers that want to listen in on the Wireless LAN traffic.

Every node (Access Point, PC card) in a wireless network must be secured against eavesdropping.

B.6.1 IEEE authentication

This method provides an encryption technique that makes it very difficult to have unauthorized access to the network. Other authentication methods may have been delivered for different types of Wireless LAN devices.

B.6.2 Open Systems method

This is an IEEE authentication method that does not require password protection.

B.6.3 WEP method

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

Only devices that share the same WEP key are allowed to communicate with each other.

Features of WEP are:

- Data encryption using a
 - 40 bit shared key (10 character password), or
 - 128-bit shared key (26 character password).
- 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.

Index

A

Access Control List 31
Access Point 55, 56
Allow clients 32
APIPA 52
Authentication method 34
Auto IP 52

B

Bit rates 41
Broadcast address 51

C

Contact 24, 37

D

Data rates 56
Deny clients 32
DHCP 22, 52
Dynamic IP settings 25

E

Exception List 32

G

Gateway 27, 51

I

IEEE authentication 34, 58
IP address 24, 49, 50
IP address range 49
IP settings 22, 37

K

KickStart 22

L

Location 24, 37
Lock Access Point 36

M

MAC address 24, 37, 52

N

Network address 51
Network LED 18

Network portion 50

Node portion 50

O

Open Systems 34, 58

P

Power LED 18

R

Radio channel 31, 42, 57
Radio LED 18
Radio specifications 41
Range 41, 56
Regulatory domain 31, 57
Rescan 25
Reset Access Point 19

S

Security 57
SSID 24, 30
Static IP settings 25, 26
Subnet 50
Subnet mask 50

T

TCP/IP 24

U

Unlock Access Point 18
UTP port 17

W

Web Interface 28
WEP 34, 35, 58
Wired connection 17
Wireless LAN 55

