NOKIA

Nokia A036 Wireless LAN Access Point User Manual

Contents

Contents 3

1 Introduction to Nokia A036 Wireless LAN Access Point 7
1.1 Nokia A036 technical overview **7**
1.2 Nokia A036 technical specifications **8**

2 Install 11
2.1 Fixing the mounting clamp **11**
2.2 Opening the casing **12**
2.3 Placing Access Point to the mounting clamp **14**
2.4 Connecting Ethernet cable **17**
2.5 Connecting power supply unit cable (if no PoE) **20**
2.6 Connecting cables for external antennas (optional) **23**
2.7 Closing the casing **24**

3 Upgrade 27
3.1 Upgrading via TFTP **27**
3.2 Upgrading via FTP **28**
3.3 Upgrading via web **29**

4 Commission 31
4.1 Configuring IP settings **31**
4.2 Configuring wireless settings **31**
4.3 Setting Access Point identity information **33**
4.4 Setting WEP policy **34**

5 Administer 37
5.1 Accessing command line interface **37**
5.2 Accessing web user interface **37**
5.3 Changing password **38**
5.4 Setting internet access **39**
5.5 Setting access to management functions **40**
5.6 Enabling Zone Privacy **41**
5.7 Configuring DHCP **42**
5.8 Uploading configuration file via TFTP **43**
5.9 Uploading and downloading files via FTP **44**
5.10 Using SNMP **45**

6 Statistics 47
6.1 Measuring air interface **47**
6.2 Measuring LAN interface **48**

7 Commands, parameters and alarms 49
7.1 Supported CLI commands **49**
7.2 Set command parameters **50**
7.3 SNMP traps **54**

8 Files 57

8.1 config.txt **57**
8.2 stat.txt **58**
8.3 System log **60**

The information in this document is subject to change without notice and describes only the product defined in the introduction of this document. This document is intended for internal use only. This document is not an official customer document and Nokia does not take responsibility for any errors or omissions in this document. No part of it may be reproduced or transmitted in any form or means without the prior written permission of Nokia. The document has been prepared to be used by professional and properly trained personnel, and the customer assumes full responsibility when using it. Nokia welcomes customer comments as part of the process of continuous development and improvement of the documentation.

The information or statements given in this document concerning the suitability, capacity, or performance of the mentioned hardware or software products cannot be considered binding but shall be defined in the agreement made between Nokia and the customer.

Nokia WILL NOT BE RESPONSIBLE IN ANY EVENT FOR ERRORS IN THIS DOCUMENT OR FOR ANY DAMAGES, INCIDENTAL OR CONSEQUENTIAL (INCLUDING MONETARY LOSSES), that might arise from the use of this document or the information in it. UNDER NO CIRCUMSTANCES SHALL NOKIA BE RESPONSIBLE FOR ANY LOSS OF USE, DATA, OR INCOME, COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, PROPERTY DAMAGE, PERSONAL INJURY OR ANY SPECIAL, INDIRECT, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES HOWSOEVER CAUSED.

THE CONTENTS OF THIS DOCUMENT ARE PROVIDED "AS IS". EXCEPT AS REQUIRED BY APPLICABLE MANDATORY LAW, NO WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT, ARE MADE IN RELATION TO THE ACCURACY, RELIABILITY OR CONTENTS OF THIS DOCUMENT. NOKIA RESERVES THE RIGHT TO REVISE THIS DOCUMENT OR WITHDRAW IT AT ANY TIME WITHOUT PRIOR NOTICE.

1 Introduction to Nokia A036 Wireless LAN Access Point

1.1 Nokia A036 technical overview

Nokia A036 Wireless LAN Access Point serves as a wireless hub that coordinates and controls a wireless LAN. Portable devices equipped with IEEE802.11(b) compatible adapters can communicate with a wired LAN or with each other through the Nokia A036. A wireless LAN can be implemented as an extension to GSM, GPRS and UMTS networks or to an existing wired LAN. Nokia A036 is Wi-Fi certified.

Access Point management

Nokia A036 Wireless LAN Access Point management interface is designed to work with Internet Explorer. In addition, Nokia A036 can be managed via command line interface. New configuration data can be downloaded via TFTP and FTP in an authorised manner. Nokia A036 can also be configured remotely via the web user interface and SMNP.

Security

Nokia A036 supports both types of authentication specified in the IEEE802.11b standard; Open system authentication (Open Mode) and WEP (Wired Equivalent Privacy) key authentication. In the Open Mode, authentication and the transfer of user data is not encrypted. In terms of WEP, Nokia A036 supports encryption with the 40-bit option or extended 128-bit high-level security.

In addition, the design of Nokia A036 provides physical security from unauthorised access. All connectors are hidden inside the casing and there are no screws to open, preventing unathorised opening. Only authorised personell know how to open the casing.

Power Over Ethernet

Nokia A036 has an built-in Power Over Ethernet client compliant to IEEE802.3af standard. The client allows both PoE installation and conventional power supply.

Antennas

Nokia A036 is equipped with fully balanced and high quality internal antennas resulting in an optimal RF performance. The antennas have been designed to optimise coverage and reception propability when Nokia A036 is wall mounted.

Nokia A036 also allows the installation of external antennas. External antennas may be needed if the access point needs to be hidden or, for example, an omni-directional coverage is required. Three different types of external antennas are available by order. For more information on external antennas, see Nokia A036 technical specification.

Wi-Fi 802.11b functionality

Nokia A036 Wireless LAN Access Point follows the Wi-Fi recommendation for default settings, as specified in the Wi-Fi System Interoperability Test Plan version 1.1a. Therefore, Nokia A036 needs no reconfiguration to achieve Wi-Fi compatibility.

1.2 Nokia A036 technical specifications

Physical specifications

Product name	Nokia A036 Wireless LAN Access Point
Type	Stand alone unit
Dimensions	202mm x 152mm x 29mm (8" x 6" x 1")
Weight	350g
Standards	IEEE802.11b (Wireless LAN), IEEE802.3 (Ethernet), IEEE802.3af (PoE)
Internal antenna	Sector
External antenna	OMNI, dual slant sector, bi-sector, with 2m/6ft cable

Electrical specifications

Power source	Power over Ethernet, 110V - 230V AC 50/60Hz (EU, UK, US)
Operating power consumption	< 5 W
Output power	max. 20 dBm

Reception sensitivity	min. -90 dBm
EMC emissions	FCC class B requires the use of shielded Ethernet cable. FCC/EN55022 class A.
EMC immunity	EN55024
Storage temperature	0 - 60 degrees celcius
Operating temperature	0 - 40 degrees celcius

Radio

WLAN standard	IEEE802.11b
Default settings	Wi-Fi Interoperability Test Plan version 1.1a
Channels	13 (depending on local regulations)
Max data rate	11 Mb/s
Modulation technique	Direct Sequence Spread Sprectrum (DSSS)

Functional specifications

Management options	Web based, Telnet, SNMP
Management connection	Ethernet, air interface
File transfer	FTP, TFTP
Access security	WEP (40 bits, 128 bits)
Multi-Access Point roaming	Nokia Inter Access Point Protocol
LED indicator	Power status

Interfaces

Ethernet connection	IEEE802.3 automatic 10/100baseT (RJ-45)
Power over Ethernet	IEEE802.3 af
Power supply	EU, UK and US standard AC power

2 Install

2.1 Fixing the mounting clamp

Nokia A036 is installed using a mounting clamp. You can either fix the clamp to the wall with screws or fasten it with tie wraps. See (3) in figure 1 for holes for tie wraps.

To fix the mounting clamp to the wall with screws:

Steps

1. **Place the mounting clamp against the wall and mark fixing points**

   See (1) and (2) in figure 1 for marking fixing points. It is recommended you use the horizontal holes (1) as they are stronger than the vertical holes (4).

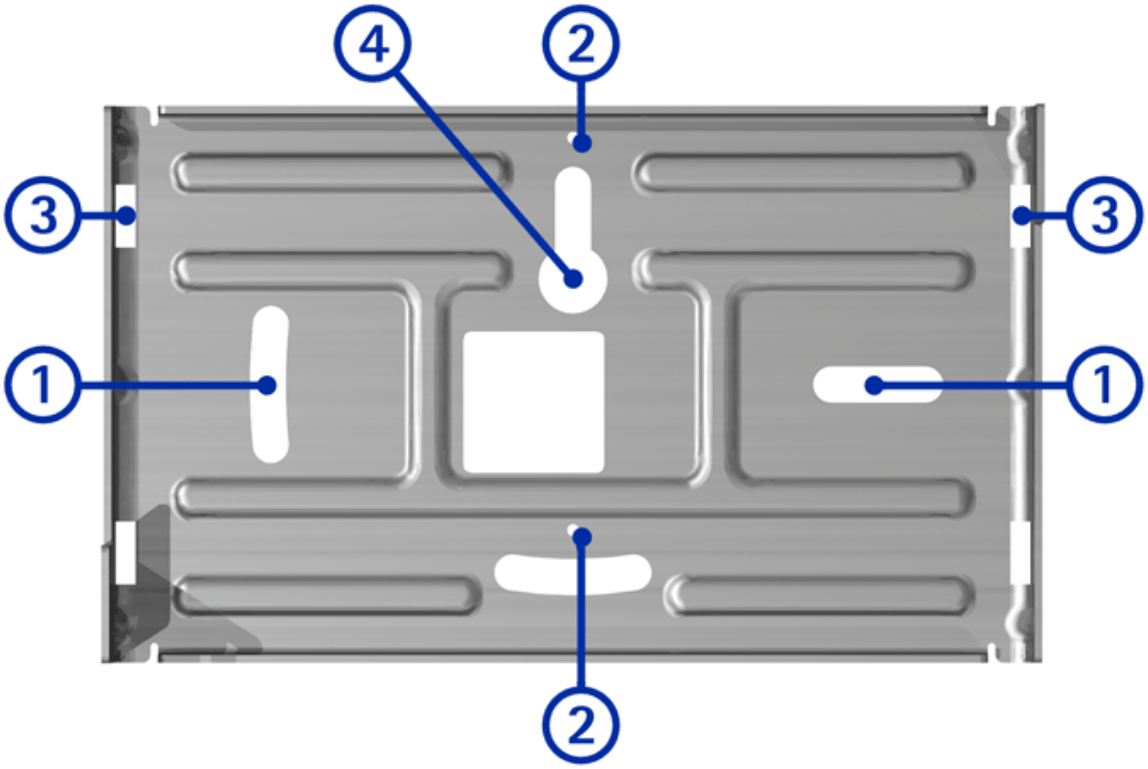

Figure 1. Mounting clamp

2. **Drill holes**

3. **Fasten the mounting clamp with screws**

2.2 Opening the casing

The Nokia A036 casing needs to be opened before placed to the mounting clamp.

Steps

1. **To open the casing before installation, place the device the back cover facing up**

2. **Press on both sides of the casing**

The pressing points are shown in figure 2. See figure 3 for pressing points when the device is installed.

Figure 2. Opening the casing before installation

Figure 3. Opening the installed casing

3. The cover clicks open

2.3 Placing Access Point to the mounting clamp

Before you start

You can feed the Ethernet cable or optionally power supply unit cable in three ways:

- through the top cable inlet
- through the cable inlet in the middle of the back cover
- through the bottom cable inlet

Depending on how you feed the cable, remove the appropriate cable inlet cover by pressing it gently (see figure 4). To avoid injury to your hands, use a tool for removing the cover.

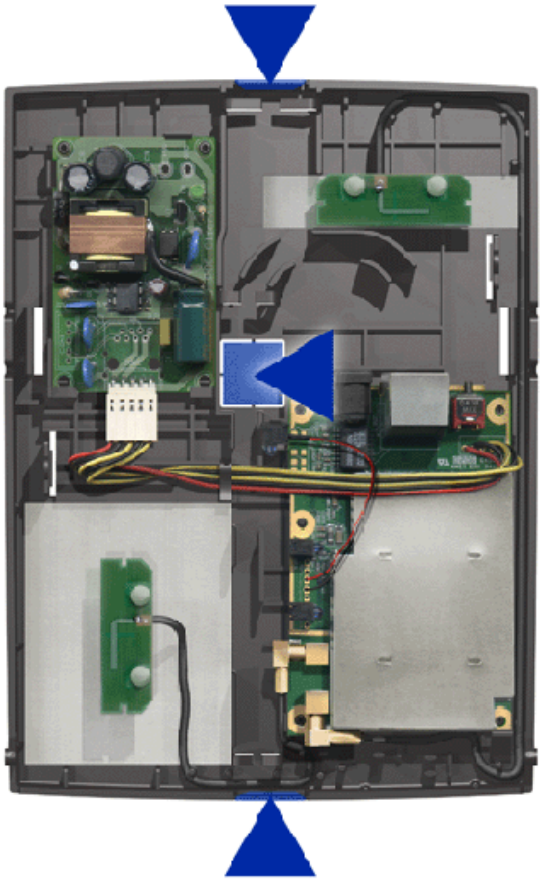

Figure 4. Cable inlets

Steps

1. Place Access Point to the mounting clamp

See figures 5 and 6 for how to place the device to the mounting clamp.

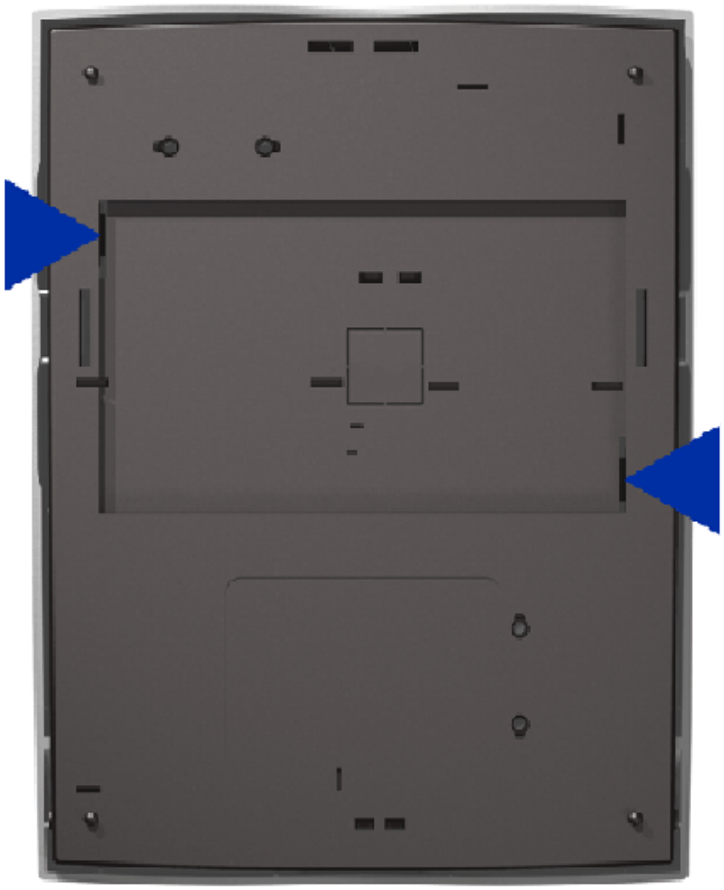

Figure 5. Back cover

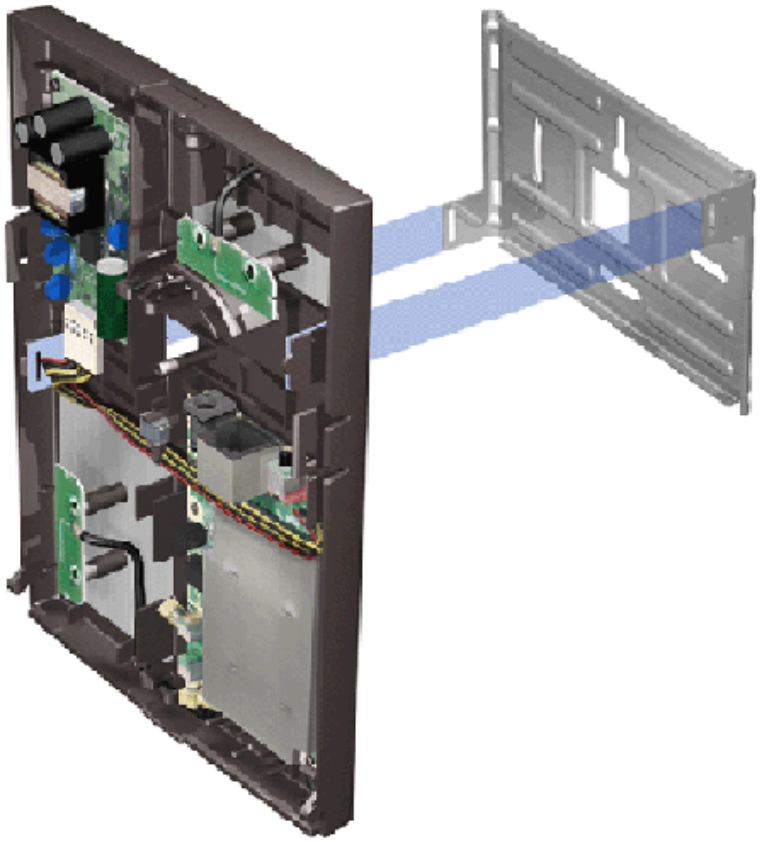

Figure 6. Placing Access Point to the mounting clamp

2.4 Connecting Ethernet cable

Steps

1. **You can connect the Ethernet cable in three ways**

   a) through the top cable inlet, see figure 7

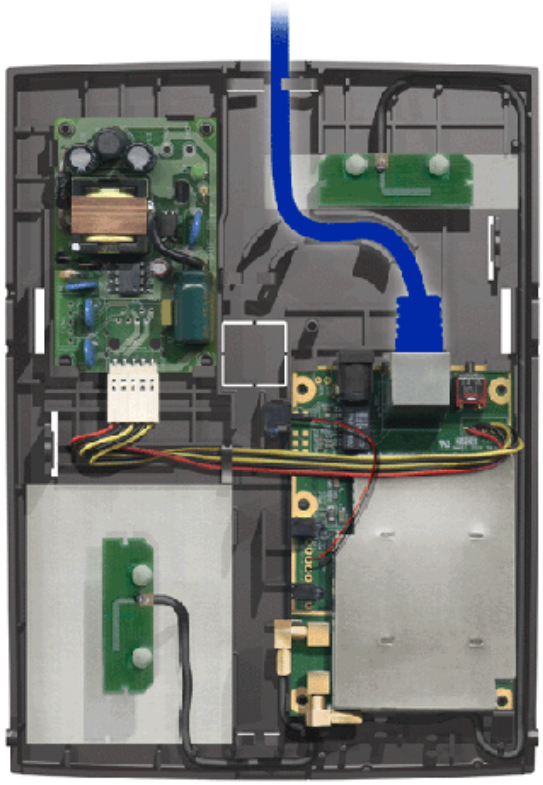

Figure 7. Ethernet cable through the top cable inlet

b) through the cable inlet in the middle of the back cover, see figure 8

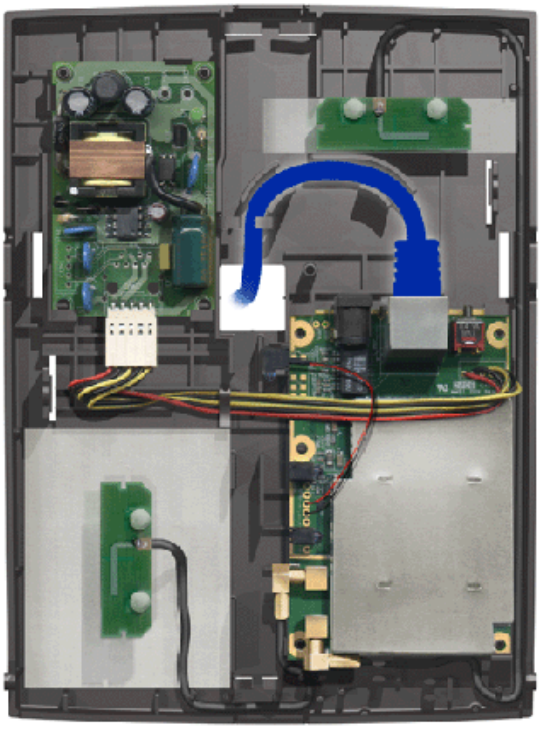

Figure 8. Ethernet cable through the middle cable inlet

c) through the bottom cable inlet, see figure 9

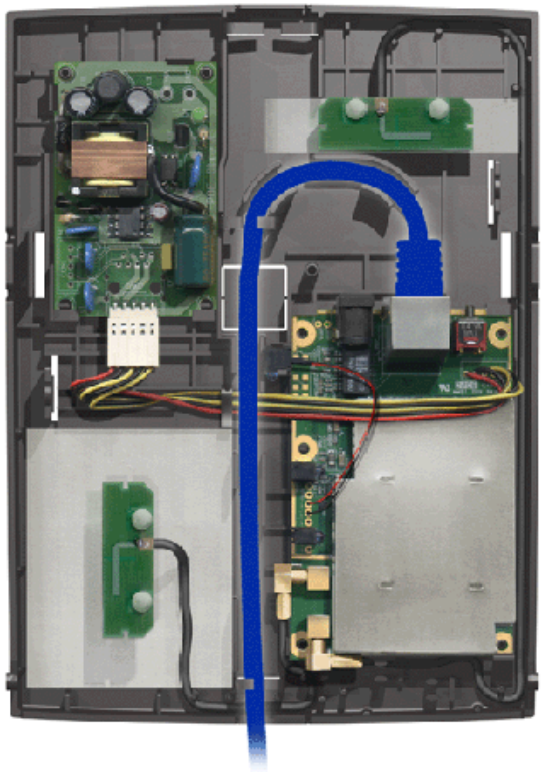

Figure 9. Ethernet cable through the bottom cable inlet

Note

Do not leave any extra cable inside the back cover.

2.5 Connecting power supply unit cable (if no PoE)

If Power over Ethernet is used, there is no need for power supply unit cabling.

Steps

1. You can connect the PSU cable in three ways

a) through the top cable inlet, see figure 10

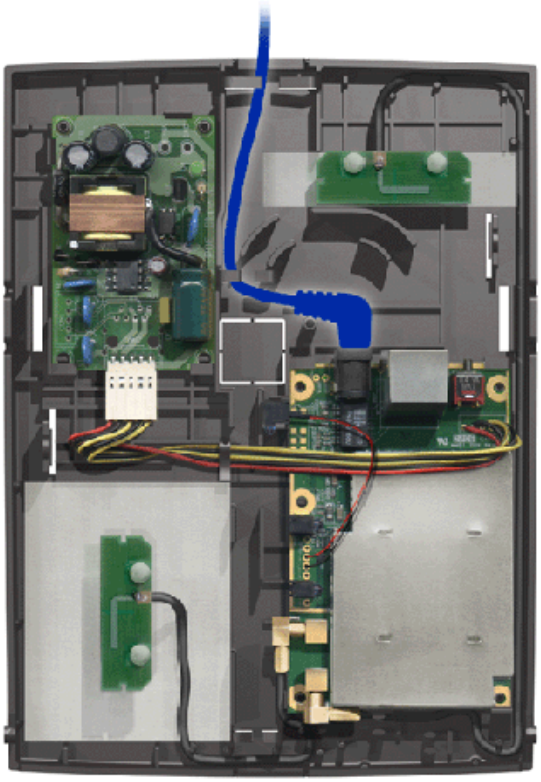

Figure 10. Power supply unit cable through the top cable inlet

b) through the cable inlet in the middle of the back cover, see figure 11

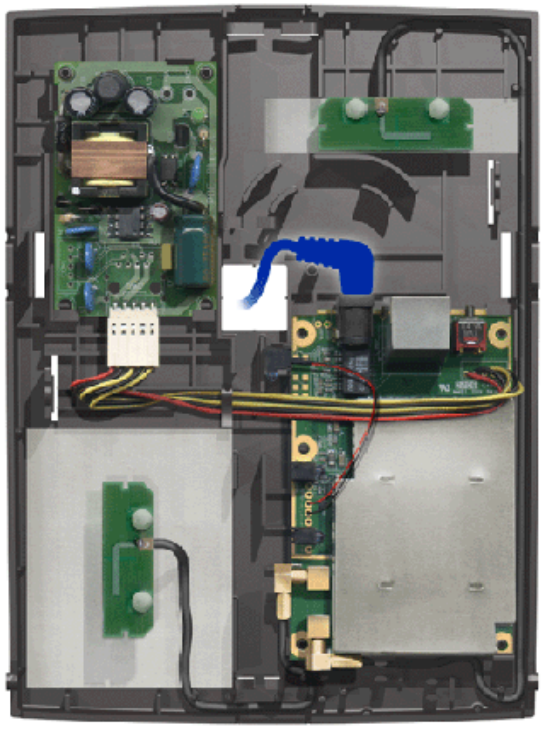

Figure 11. Power supply unit cable through the middle cable inlet

c) through the bottom cable inlet, see figure 12

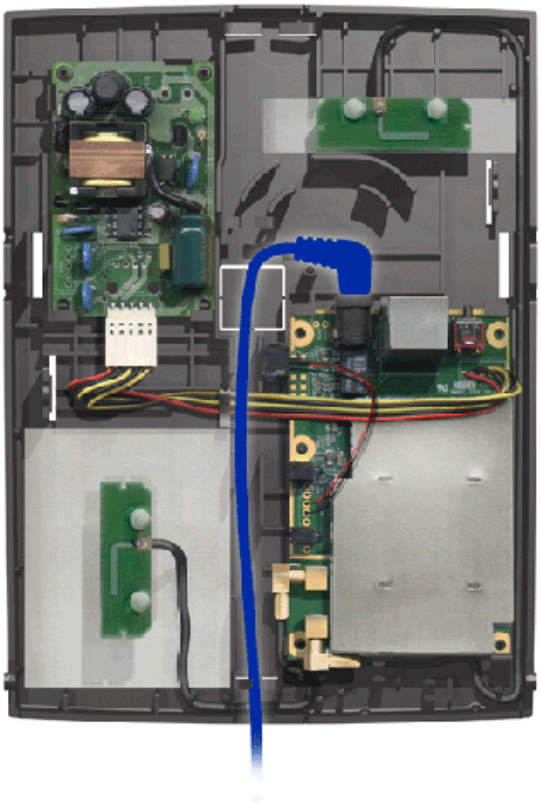

Figure 12. Power supply unit cable through the bottom cable inlet

Note

Do not leave any extra cable inside the back cover.

2.6 Connecting cables for external antennas (optional)

Steps

1. **Place the connectors in parking slots**

2. Connect cables

See figure 13.

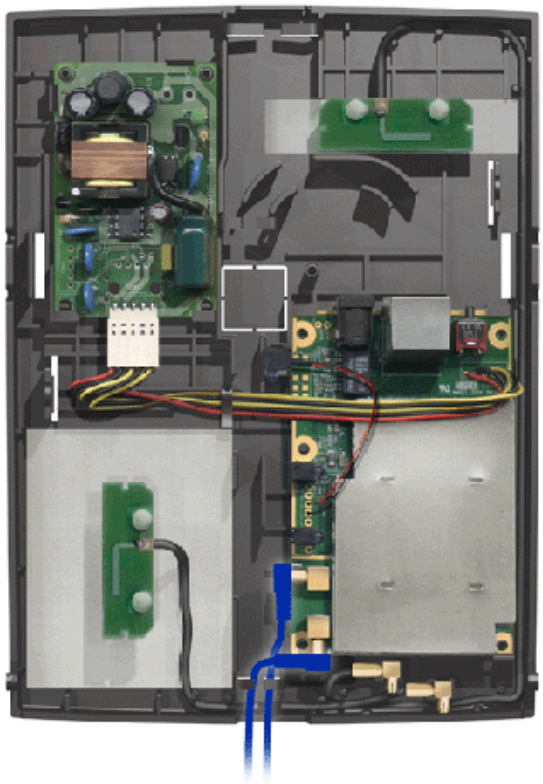

Figure 13. External antenna cabling

2.7 Closing the casing

Steps

1. To close the casing, place the front cover on top of the back cover

Place the front cover so that the top part is approximately 1-2 mm lower than the top of the back cover. See figures 14 and 15.

Figure 14. Closing the casing - front view

Figure 15. Closing the casing - side view

2. Press gently and the front cover snaps to its place

3 Upgrade

3.1 Upgrading via TFTP

Use TFTP client software and command line interface to upgrade Nokia A036. The uploaded file can be a plain image file (system, rescue or MVC), or if the file is tarred and compressed, more images can be uploaded in a single upload session

Steps

1. **Run your TFTP software and input the following information:**

```
<HOST>: IP address of Nokia A036
<Port>: 69 (port number for TFTP)
<LocalFirmwareFile>: the name of the new firmware file
you want to upgrade
<RemoteFileName>: password of the Web/SNMP
(default password: private)
```

2. **On the workstation, click Start -> Run to open a command window**

3. **In the command window, type the following command:**

```
tftp-i <IPAddress> put <FirmwareFile> <RemoteFileName>
where
<IPAddress> = IP address of Nokia A036
<FirmwareFile> = name of the firmware
<RemoteFileName> = password of Web/SNMP
(default password: private)
```

Note

Make sure that the file is available in the directory from where you run this command.

After entering the command line, click OK.

Expected outcome

The TFTP client should inform of a successful transfer. The upgrade will be finished a few minutes after this notification, as the upgrade process might take about 2-3 minutes to restart the system.

Further information

For other means of upgrading Nokia A036, see *Upgrading via FTP* and *Upgrading via web*.

3.2 Upgrading via FTP

Use FTP client software and command line interface to upgrade Nokia A036. The uploaded file can be a plain image file (system, rescue or MVC), or if the file is tarred and compressed, more images can be uploaded in a single upload session.

Steps

1. **Run your FTP software and input the following information to logon to the FTP server**

```
<HOST>: IP address of Nokia A036
<Port>: 21 (port number for FTP)
<UserID>: login name (default login name: root)
<Password>: password of the Web/SNMP (default password:
private)
```

   After connected, upload the new firmware to the current directory.

2. **On the workstation, click Start -> Run to open a command window**

3. **Type the following command to connect to Nokia A036**

```
ftp <IPAddress>
where
<IPAddress> = IP address of Nokia A036
```

   After connected, enter username and password.

   Default username: root

   Deafult password: private

4. **After a succesful login, enter the following command:**

```
put <FirmwareFile>
where
<FirmwareFile> = name of the firmware
```

Expected outcome

The FTP client should inform of a successful transfer. The upgrade will be finished a few minutes after this notification, as the upgrade process might take about 2-3 minutes to restart the system.

Further information

For other means of upgrading Nokia A036, see *Upgrading via TFTP* and *Upgrading via web*.

3.3 Upgrading via web

You can use the upgrade function in the Nokia A036 web user interface to upgrade firmware:

Steps

1. **Click the Firmware upgrader link**
2. **Select the firmware file to be uploaded**
3. **Start the upgrade by clicking Apply**

Expected outcome

The upgrade process takes approximately 2-3 minutes, after which Nokia A036 will restart.

Further information

For more information on the Nokia A036 web user interface, see *Accessing web user interface*.

4 Commission

4.1 Configuring IP settings

To define Nokia A036 IP settings via command line interface, set the following parameters using the set command:

Parameter	Default value	Range	Description
ip_address {dotted-quad}	none	IP address	IP address of the Access Point (for management purposes).
subnet_mask {dotted-quad}	255.255.0.0	Any valid mask.	Subnet mask for network (used to determine broadcast addresses).
gateway {dotted-quad}	none	IP address	Default gateway for packets not on the local subnet, or the address of the zone controller if zone privacy is set.

You can also configure IP settings to an external DHCP server and set the DHCP mode to "client", or you can use the ifconfig command.

For a full list of parameters available in Nokia A036, see *Set command parameters*.

4.2 Configuring wireless settings

You can configure wireless settings via the web user interface of command line interface.

Configuring wireless settings via web user interface

To configure wireless settings via the web user interface, enter the following information:

SSID (Service Set ID)	802.11 network name.
Radio channel	The channel that the Access Point uses to transmit and receive information.
Regulatory domain	The domain for which the device is certified. The amount of available radio channels depends on the regulatoy domain.
Basic rate	You can choose all or specific. If specific, select either low or high rate.
Peer AP's for wireless distribution system.	You can list MAC addresses of peer Access Points after which the Access Point will try to establish a link with those listed. In this way the AP's will form a wireless backbone or a wireless distribution system.

Configuring wireless settings via command line interface

To configure wireless settings via command line interface, set the following parameters using the set command:

Parameter	Default value	Range	Description
net_name {name}	Nokia WLAN	up to 32 characters	802.11 network name (ASCII, case-sensitive)
channel {value}			Radio channel and domain are linked: the domain parameter selects the regulatory domain governing channel assignment, and is used to constrain the choice of channels.
	10	1-13	ETSI
	10	1-11	USA and Canada
	10	10-13	France
	14	14	Japan
domain {[usa | canada | etsi | france | japan]}	usa	usa canada etsi france japan	The regulatory domain.

Parameter	Default value	Range	Description
basic_rate {rates}	All	1000 2000, 5500 11000, All	A list of all basic rates supported by the access point (this should be limited to rates that all stations can support).
brgtable {[add | del] {MAC}}	none	add or del	Adds/deletes a given MAC address to/from bridge table.

For a full list of parameters available in Nokia A036, see *Set command parameters*.

4.3 Setting Access Point identity information

Define the following Nokia A036 identity information via the web user interface or command line interface:

SNMP name	Name of the Access Point device (max 32 characters).
SNMP location	The physical location of the device, e.g., 2nd floor, room 3 (max 64 characters).
SNMP contact	The person responsible for the device. This can be, e.g., an email address (max 32 characters).
AP name	Hostname of the Access Point (max 15 characters).

To define identity information via command line interface, set the following parameters using the set command:

Parameter	Default value	Range	Description
snmp_sys_name {string}	Sys Name	up to 32 characters	SNMP system name, from the RFC1213 MIB (case sensitive).
snmp_location {string}	Location	up to 64 characters	SNMP location data, from the RFC1213 MIB (case sensitive).
snmp_contact {string}	Contact	up to 32 characters	SNMP contact name, from the RFC1213 MIB (case sensitive).
ap_name {name}	LocalAP	Up to 15 characters	Access Point name (equivalent to hostname).

For a full list of parameters available in Nokia A036, see *Set command parameters*.

4.4 Setting WEP policy

Use the web user interface or command line interface to define WEP (Wired Equivalent Privacy) policy. Nokia A036 supports both types of authentication specified in the IEEE802.11b standard; Open system authentication (Open Mode) and WEP (Wired Equivalent Privacy) key authentication. In the Open Mode, authentication and the transfer of user data is not encrypted. In terms of WEP, Nokia A036 supports encryption with the 40-bit option or extended 128-bit high-level security:

40 bits	The key is 10 hex characters long.
128 bits	The key is 26 hex characters long.

The web user interface allows these keys also to be entered in ASCII.

Set WEP policy via web user interface

In the web user interface, choose either one of the following:

Open system	Clients can access Nokia A036 without a WEP key.
WEP	Clients need a WEP key to access Nokia A036.

If you choose WEP, the system requires you to specify a key size and a key. You can directly enter hexadecimal characters or enter ascii characters that will be automatically transformed to hexadecimal characters.

Set WEP policy via command line interface

To define WEP policy via command line interface, set the following parameters using the set command:

Parameter	Default value	Range	Description
wep_mode {mode}	open		Determines the Access Point authentication policy:
		open	Accept open system.

Parameter	Default value	Range	Description
		wep	Wep key is required.
wep_key {1-4} {KEY}]	none	1-4, hex string	Sets default key to value hex string. The hex string will be 10 or 26 hex characters, according to the strength of WEP key being entered
wep_key_length {[normal | high]}	normal	normal, high	"normal" sets the wep-key length to 40 bits, "high" sets the wep-key length to 128 bits
wep_key_active [1-4}	1	1-4	Specifies which one of the four wep keys is active.

For a full list of parameters available in Nokia A036, see *Set command parameters*.

5 Administer

5.1 Accessing command line interface

To use Telnet on a Windows machine:

Steps

1. **On the workstation, click Start -> Run**
2. **Type "telnet" and the IP address of Nokia A036 and press OK**

   Telnet window opens with a logon prompt.
3. **Type username and password**

   Defaulf username: root

   Default password: private

   It is highly recommended to change the default password as soon as possible.

Expected outcome

You are now ready to enter commands.

Further information

For more information on using the command line interface, see *Supported CLI commands* and *Set command parameters*.

5.2 Accessing web user interface

You can use the Nokia A036 web user interface to modify the following settings:

- wireless settings
- Nokia A036 identity information
- WEP
- password
- internet access
- management IP address
- Zone Privacy

The web user interface also provides:

- upgrade function
- Nokia A036 statistics

You can access the Nokia A036 web user interface using Internet Explorer. To access the user interface:

Steps

1. **Open the web browser**
2. **Enter the IP address of Nokia A036 and press Enter**

   A logon prompt appears.
3. **Enter password and press Enter**

   Default password: private

Expected outcome

The home page of the Nokia A036 web user interface appears.

5.3 Changing password

You can change the password needed for management access via the web user interface or command line interface.

To change the password via command line interface, set the following parameter using the set command:

Parameter	Default value	Range	Description
password {password}	private	up to 16 characters in sets of a - z, A - Z and 0 - 9	Password for management access to Access Point (case sensitive).

For a full list of parameters available in Nokia A036, see *Set command parameters*.

5.4 Setting internet access

Use the Nokia A036 web user interface or command line interface to configure internet access settings.

Setting internet access via web user interface

You can configure internet access via the web user interface by selecting the appropriate settings:

none	Internet access is not restricted.
MAC address based	Allows clients with specified MAC addresses to access the network. You can add/delete addresses to/from the list.
Port based	Radius servers are in control of the client access. You can add/delete Radius servers to/from the list.
Require authentication every .. seconds	Specifies how often the system requires authentication.
Distribute a random WEP key to clients	Random WEP keys are distributed to clients.
Refresh key every .. seconds	Specifies how often the WEP key is refreshed.

Setting internet access via command line interface

To configure internet access via command line interface, set the following parameters using the set command:

Parameter	Default value	Range	Description
wep_mode {mode}	open		Determines the Access Point authentication policy:

Parameter	Default value	Range	Description
		open	Accept open system.
		wep	Wep key is required.
radius_server {1-2} {ip_addr}	none	1, IP address or 2, IP address	IP address of primary (1) and secondary (2) Radius servers.
shared_secret {1-2} {secret}	none	up to 16 characters	An ASCII string giving the shared secret for the Radius server.

For a full list of parameters available in Nokia A036, see *Set command parameters*.

5.5 Setting access to management functions

You can define access to management functions via the web user interface or command line interface.

Setting access via web user interface

You can modify the following settings in the web user interface:

Manager IP method	Select "any" or "specific". If you choose "any", any IP address can access Nokia A036. If "specific", you must specify which IP address can access Nokia A036. You can list 1-4 IP addresses for this purpose.
Web port	Enter the Web server port number.
Telnet port	Enter the Telnet server port number.

Setting access via command line interface

To specify access to management functions via command line interface, set the following parameters using the set command:

Parameter	Default value	Range	Description
manager {[any | specific]}	any	any, specific	Limits management access to specific IPs, or disables it altogether.
manager_ip {1-4} {ip_addr}	none	1-4, IP address	Allows one of out of four IP addresses specific management

Parameter	Default value	Range	Description
			access.
telnet_port {port}	23	0-65535	Telnet server port number (0 disables access).
http_port {port}	80	0-65535	Web server port number (0 disables access).

For a full list of parameters available in Nokia A036, see *Set command parameters*.

5.6 Enabling Zone Privacy

Nokia A036 Wireless LAN Access Point has a unique feature that secures shared files: the Zone Privacy feature. When Zone Privacy is enabled, Nokia A036 filters data traffic at a low level to ensure that wireless users are protected from malicious protocol attacks. The feature also protects the wireless user from other users viewing or accessing files on shared directories on their laptop hard disk drives.

You can enable the Zone Privacy feature via the web user interface or command line interface.

Enabling Zone Privacy via web user interface

You can enable the Zone Privacy feature via the web user interface by entering the following information:

AC IP address	Access Controller IP Address
AP IP address	Access Point IP Address
AP Address Mask	Access Point Subnet Mask
AP gateway	Access Point Gateway
Zone Privacy	Select "on" or "off"

Enabling Zone Privacy via command line interface

To enable the Zone Privacy feature via command line interface, set the following parameter using the set command:

Parameter	Default value	Range	Description
zone_privacy {[on | off]}	off	on or off	Enables the zone privacy feature.

For a full list of parameters available in Nokia A036, see *Set command parameters*.

5.7 Configuring DHCP

Use the command line interface to configure DHCP settings.

Configuring DHCP Relay

As Nokia A036 supports both IEEE802.1x and open system authentication, every Access Point has a DHCP relay function with two DHCP pools. The DHCP relay function acts as a standard BOOTP relay, checking the terminal's authentication type and forwarding DHCP queries to the relevant DHCP server. The DHCP relay function is based on RFC1534 and the DHCP server on RFC2131.

To configure DHCP relay function, set the following parameters using the set command:

Parameter	Default value	Range	Description
dhcp_relay {[on | off]}	off	on or off	Enables the DHCP relay functionality.
ip_address_1x {dotted-quad}	none	IP address	IP address of the AP to be used in DHCP relay when forwarding requests for 802.1x users (giaddr).
ip_address_OpenSystem {dotted-quad}	none	IP address	IP address of the AP to be used in DHCP relay when forwarding requests for OpenSystem users (giaddr).

Configuring DHCP server

You can also use Nokia A036 as a DHCP server by setting the following parameters with the set command:

Parameter	Default value	Range	Description
dhcp_base	192.168.5.100	IP address	The base address of the DHCP pool.
dhcp_pool	16	0-254	The number of entries in the pool for DHCP server (0 disables the DHCP server).
dhcp_gateway	none	IP address	The gateway address for dhcp clients.
dhcp_dns	192.168.1.1	IP address	The DNS server address for dhcp clients.

For a full list of parameters available in Nokia A036, see *Set command parameters*.

5.8 Uploading configuration file via TFTP

Use TFTP client software and command line interface to upload configuration file. After a successful upload, Nokia A036 will first check the validity of parameters and then change the settings according to the configuration file.

Steps

1. Run your TFTP software and input the following information:

```
<HOST>: IP address of Nokia A036
<Port>: 69 (port number for TFTP)
<Configurefile>: name of the configuration file you
want
to upload (the file name must be config.txt)
<RemoteFileName>: password of the Web/Telnet/SNMP and
the file name of the configuration file
(default: private#config.txt)
```

2. On the workstation, click Start -> Run to open a command window

3. In the command window, type the following command:

```
tftp-i <IPAddress> put <Configurefile> <RemoteFileName>
where
<IPAddress> = IP address of Nokia A036
<Configurefile> = name of the configuration file
<RemoteFileName> = password of Web/Telnet/SNMP and
```

```
the file name of the configuration file
(default: private#config.txt)
```

After entering the command line, click OK.

Expected outcome

The TFTP client should inform of a successful transfer. After the upload Nokia A036 starts to use the new configuration.

5.9 Uploading and downloading files via FTP

Use FTP client software and command line interface to download and upload configuration file and to download statistics file.

Steps

1. **Run your FTP software and input the following information to logon to the FTP server**

```
<HOST>: IP address of Nokia A036
<Port>: 21 (port number for FTP)
<UserID>: login name (default login name: root)
<Password>: password of the Web/Telnet/SNMP (default
password: private)
```

After connected, upload the new firmware to the current directory.

2. **On the workstation, click Start -> Run to open a command window**

3. **Type the following command to connect to Nokia A036**

```
ftp <IPAddress>
where
<IPAddress> = IP address of Nokia A036
```

After connected, enter username and password.

Default username: root

Default password: private

4. **After a succesful login, enter the following commands:**

```
put <Configurefile>
when you want upload a new configuration file
```

```
get <Configurefile>
when you want to download a new configuration file

or
get <Statisticsfile>
when you want to download a new statistics file
```

Expected outcome

The FTP client should inform of a successful transfer.

5.10 Using SNMP

Nokia A036 has a built-in SNMP (Simple Networking Management Protocol) agent capability which allows integration into SNMP managed enterprise environments. The agent supports SNMP V1.0 and V2c requests and provides data from the following MIBs:

MIB-II
IEEE802.11 MIB
Ethernet-like MIB
IANA interface MIB

The default value for SNMP use is "off". To set up Nokia A036 for use with SNMP:

Steps

1. In Telnet session, set the following parameters using the set command

Parameter	Default value	Range	Description
community_get {string}	public	up to 16 characters	Community name for SNMP get operations (case sensitive).
community_set {string}	private	up to 16 characters	Community name for SNMP set operations (case sensitive).
snmp_contact {string}	Contact	up to 32 characters	SNMP contact name, from the RFC1213 MIB (case sensitive).
snmp_sys_name {string}	Sys Name	up to 32 charac-	SNMP system name, from the

Parameter	Default value	Range	Description
		ters	RFC1213 MIB (case sensitive).
snmp_location {string}	Llocation	up to 64 charac-ters	SNMP location data, from the RFC1213 MIB (case sensitive).
All or one of the following parameters must be set 'on' in order to enable SNMP use:			
snmp_enable_set	off	on, off	Enable or disable SNMP SETs
snmp_enable_get	off	on, off	Enable or disable SNMP GETs
snmp_enable_trap	off	on, off	Enable or disable SNMP traps.

2. Set up your SNMP client

SNMP client set up is client-specific.

6 Statistics

6.1 Measuring air interface

The Nokia A036 web user interface provides information on the following radio statistics:

Radio statistics

Bytes received	Total number of bytes received.
Unicast packets received	Number of unicast packets received.
Nonunicast packets received	Number of nonunicast packets received.
Received packets dropped	Number of received packets dropped.
Received packets errors	Number of received packets dropped by errors.
Bytes transmitted	Total number of bytes transmitted.
Unicast packets transmitted	Total number of bytes transmitted.
Nonunicast packets transmitted	Number of nonunicast packets transmitted.
Transmitted packets dropped	Number of transmitted packets dropped.
Transmitted packets errors	Number of transmitted packets dropped by errors

Radio detail statistics

aTransmitted_MPDU_Count	Number of frames transmitted.
aTransmitted_MSDU_Count	Number of data frames transmitted.
aMulticast_Transmitted_Frame_Count	Number of Multicast send.
aFailed_Count	Number of frames which could be send after retry.

aRetry_Count	Number of frames resent.
aMultiple_Retry_Count	Occurrences when multiple retries were needed to send a frame.
aFrame_Duplicate_Count	Count of RTS that received no response.
aRTS_Success_Count	Count of CTS received in response to RTS.
aRTS_Failure_Count	Count of RTS that received no response.
aACK_Success_Count	Number of times ACK was not received after transmission.
aReceived_Frame_Count	Number of received frames.
aMulticast_Received_Count	Number of Multicast frames received.
aFCS_Error_Count	Number of frames received with checksum errors.

6.2 Measuring LAN interface

The Nokia A036 web user interface provides information on the following LAN statistics:

Bytes received	Total number of bytes received.
Unicast packets received	Number of unicast packets received.
Nonunicast packets received	Number of nonunicast packets received.
Received packets dropped	Number of received packets dropped.
Received packets errors	Number of received packets dropped by errors.
Bytes transmitted	Total number of bytes transmitted.
Unicast packets transmitted	Total number of bytes transmitted.
Nonunicast packets transmitted	Number of nonunicast packets transmitted.
Transmitted packets dropped	Number of transmitted packets dropped.
Transmitted packets errors	Number of transmitted packets dropped by errors

7 Commands, parameters and alarms

7.1 Supported CLI commands

The following table outlines the commands available in Nokia A036. In addition to CLI commands, some standard Unix and Linux commands can be used with Nokia A036. In the CLI command descriptions below, the following conventions are used:

- Parameters appear in curvy brackets {}, e.g., {item}
- Square brackets [] denote the parameter is optional, e.g., [{data}].
- Vertical line | in square brackets [] denotes a selection of parameters, e.g., [ON | OFF].

Command	Function
arp	Displays the ARP table.
restart	Reboots A036.
ping {ip_address}	Sends an ICMP echo request to the IP address.
set {item} [{parameter} [{parameter} ..]]	Sets a configuration item to a given value.
ver version	Displays code version numbers.
show [wep | config | {item}]	Displays the values of system settings.
logout exit	Disconnets from session.
help	Displays available commands.
brgtable	Displays the contents of the Ethernet bridge table.

Command	Function
save	Saves current parameters to configuration file.
stats [lan | air | ip | tcp | udp | snmp]	Displays selected statistics and generates the stats.txt file.
; Comment text	A comment line that can be used in configuration files.

Note

- You can correct typing errors using the backspace key.
- You can use the arrow keys to browse previously entered commands.

For more information on using the command line interface, see *Accessing command line interface* and *Set command parameters*.

7.2 Set command parameters

Parameter	Default value	Range	Description
channel {value}			Radio channel and domain are linked: the domain parameter selects the regulatory domain governing channel assignment, and is used to constrain the choice of channels.
	10	1-13	France
	10	1-11	USA and Canada
	10	10-13	France
	14	14	Japan
domain {[usa | canada | etsi | france | japan]}	usa	usa canada etsi france	The regulatory domain.

Parameter	Default value	Range	Description
		japan	
net_name {name}	Nokia WLAN	up to 32 characters	802.11 network name (ASCII, case-sensitive)
frag_threshold {value}	2346	256-2346 (even numbers only)	Fragmentation threshold for 802.11 packets. Frames larger than this value will be broken into multiple smaller packets.
rts_threshold {value}	2301	0-2347	The size of data frame above which the IEEE802.11 RTS/ CTS collision avoidance method is used.
short_retry {value}	8	0-31	The number of times a fragment is retried in the event of a transmission failure.
long_retry {value}	4	0-31	The number of times a frame is retried in the event of a transmission failure.
basic_rate {rates}	All	1000 2000, 5500 11000, All	A list of all basic rates supported by the access point (this should be limited to rates that all stations can support).
beacon_interval {value}	100	1-65535	The time interval between beacons (in milliseconds).
dtim_interval {value}	1	1-255	The number of beacons to count between DTIMs.
ed_threshold {value}	127	10-127	Energy detection threshold.
wep_mode {mode}	open		Determines the Access Point authentication policy:
		open	Accept open system.
		wep	Wep key is required.
ip_address {dotted-quad}	none	IP address	IP address of the Access Point (for management purposes).
ip_address_OpenSystem {dotted-quad}	none	IP address	IP address of the AP to be used in DHCP relay when forwarding requests for OpenSystem users.

Parameter	Default value	Range	Description
ip_address_1x {dotted-quad}	none	IP address	IP address of the AP to be used in DHCP relay when forwarding requests for 802.1x users.
subnet_mask {dotted-quad}	255.255.0.0	Any valid mask.	Subnet mask for network (used to determine broadcast addresses).
gateway {dotted-quad}	none	IP address	Default gateway for packets not on the local subnet, or the address of the zone controller if zone privacy is set.
telnet_port {port}	23	0-65535	Telnet server port number (0 disables access).
http_port {port}	80	0-65535	Web server port number (0 disables access).
manager {[any | specific]}	any	any, specific	Limits management access to specific IPs, or disables it altogether.
password {password}	private	up to 16 characters in sets of a - z, A - Z and 0 - 9	Password for management access to Access Point (case sensitive).
ap_name {name}	LocalAP	Up to 15 characters	Access Point name (equivalent to hostname).
protocol_filter {[tcpip | all]}	all	all, tcp/ip	Enables packet filtering, discarding all non-TCP/IP traffic.
zone_privacy {[on | off]}	off	on or off	Enables the zone privacy feature.
community_get {string}	public	up to 16 characters	Community name for SNMP get operations (case sensitive).
community_set {string}	private	up to 16 characters	Community name for SNMP set operations (case sensitive).
snmp_contact {string}	Contact	up to 32 characters	SNMP contact name, from the RFC1213 MIB (case sensitive).
snmp_sys_name {string}	Sys Name	up to 32 characters	SNMP system name, from the RFC1213 MIB (case sensitive).
snmp_location {string}	Location	up to 64 characters	SNMP location data, from the RFC1213 MIB (case sensitive).
snmp_secret {secret}	default	up to 16 charac-	An ASCII string giving the

Parameter	Default value	Range	Description
		ters in sets of a - z, A - Z and 0 - 9	shared secret for the radius server.
snmp_enable_set	off	on, off	Enable or disable SNMP SETs
snmp_enable_get	off	on, off	Enable or disable SNMP GETs
snmp_enable_trap	off	on, off	Enable or disable SNMP traps.
cca_mode {param}	cs_only	ed_only, cs_only, ed_and_cs, ed_or_cs	Specifies the CCA (Clear Channel Assessment) to be used.
wep_key {1-4} {KEY}	none	1-4, hex string	Sets default key to value hex string. The hex string will be 10 or 26 hex characters, according to the strength of WEP key being entered (note: the web user interface allows these keys to be entered also in ASCII.)
wep_key_length {[normal | high]}	normal	normal, high	"normal" sets the wep-key length to 40 bits, "high" sets the wep-key length to 128 bits
wep_key_active {1-4}	1	1-4	Specifies which one of the four wep keys is active.
radius_server {1-2} {ip_addr}	none	1 or 2, IP addresses	IP address of primary (1) and secondary (2) Radius servers.
shared_secret {1-2} {secret}	none	up to 16 characters	An ASCII string giving the shared secret for the Radius server.
shared_password {password}	Nokia WLAN	up to 16 characters	An ASCII string giving the dummy password for the Radius server.
ip_address_ac {dotted-quad}	none	IP address	Access Controller IP address in a configurable parameter in Access Point.
dhcp_relay {[on | off]}	off	on or off	Enables the DHCP relay functionality.
brgtable {[add | del] {MAC}}	none	add or del	Adds/deletes a given MAC address to/from bridge table.
manager_ip {1-4} {ip_addr}	none	1-4, IP address	Allows one of out of four IP addresses specific manage-

Parameter	Default value	Range	Description
			ment access.
ac_iapf_port	2236	0-65535	Port number for IAPF messages coming from AP to AC.
dhcp_base	192.168.5.100	IP address	The base address of the DHCP pool.
dhcp_pool	16	0-254	The number of entries in the pool for DHCP server (0 disables the DHCP server).
dhcp_gateway	none	IP address	The gateway address for dhcp clients.
dhcp_dns	192.168.1.1	IP address	The DNS server address for dhcp clients.

For more information on using the command line interface, see *Accessing command line interface* and *Supported CLI commands*.

7.3 SNMP traps

Nokia A036 supported traps

Trap	Description
ColdStart	Sent when Nokia A036 starts up.
WarmStart	Sent after a system restart.
LinkDown	Sent when a failure is detected in a network interface.
LinkUp	Sent when a network interface has started.
AuthenticationFailure	Sent when an unauthenticated protocol message is received.
EnterpriseSpecific	A trap defined by Nokia for A036.

Enterprise specific traps

Trap	Value	Description
ENT_AUTH_FAIL	1	Sent when a login fails (telnet server).
ENT_MGMT_OPEN	2	Sent when someone successfully logs into Nokia A036 via Web of telnet serve.
ENT_TFTP_TRANSFER	3	Sent when a TFTP transfer has taken place.
ENT_CLI_ERROR	7	Sent when an error is detected in a CLI command.

8 Files

8.1 config.txt

The configuration file is a text file containing all configurable parameters of Nokia A036. You can modify the parameters in the configuration file and then upload the file to Nokia A036 using FTP or TFTP. After a successful upload, Nokia A036 will first check the validity of parameters and then change the settings according to the configuration file.

Record structure of the file

```
%channel: 10
%domain: usa
%net_name: "Nokia WLAN"
%frag_threshold: 2346
%rts_threshold: 2301
%short_retry: 8
%long_retry: 4
%Basic_rate: All
%beacon_interval: 100
%dtim_interval: 1
%ed_threshold: 127
%wep_mode: "open"
%ip_address: none
%subnet_mask: 255.255.0.0.
%ip_address_OpenSystem: none
%ip_address_1x: none
%gateway: none
%telnet_port: 23
%http_port: 80
%manager: "any"
%ap_name: "LocalAP"
%protocol_filter: all
%zone_privacy: off
%community_get: "public"
%community_set: "private"
%snmp_contact: "Contact"
%snmp_sys_name: "Sys Name"
%snmp_location: "Location"
%snmp_secret: "default"
%snmp_enable_set: "off"
```

```
%snmp_enable_get: "off"
%snmp_enable_trap: "off"
%cca_mode: cs_only
%wep_key: 1,none
%wep_key: 2,none
%wep_key: 3,none
%wep_key: 4,none
%wep_key_range: none
%radius_server: none
%shared_secret: none
%ip_address_ac: none
%dhcp_relay: off
%brgtable: none
%manager: any
%manager_ip: 1,none
%manager_ip: 2,none
%manager_ip: 3,none
%manager_ip: 4,none
%ac_iapf_port: 2236
%wep_key_active: 1
%dhcp_base: 192.168.5.100
%dhcp_pool: 16
%dhcp_gateway: none
%dhcp_dns: 192.168.1.1
```

8.2 stat.txt

The stat.txt file contains Nokia A036 network statistics. The file is generated using any stats command. For more information, see *Supported CLI commands*.

Record structure of the file

```
LAN:
Bytes Received :                    4907980
Unicast Packets Received :          15935
Nonunicast Packets Received :       0
Received Packets Dropped :          0
Received Packets Errors :           0
Bytes Transmitted :                 28239288
Unicast Packets Transmitted :       91686
Nonunicast Packets Transmitted :    0
Transmitted Packets Dropped :       0
Transmitted Packets Errors :        0

AIR:
Bytes Received :                    0
Unicast Packets Received :          0


Nonunicast Packets Received :       0
Received Packets Dropped :          0
```

```
Received Packets Errors :         0

Bytes Transmitted :               7084
Unicast Packets Transmitted :     23
Nonunicast Packets Transmitted :  0
Transmitted Packets Dropped :     0
Transmitted Packets Errors :      13

IP:
Forwarding :                      2
DefaultTTL :                      64
InReceives :                      14693
InHdrErrors :                     0
InAddrErrors :                    0
ForwDatagrams :                   0
InUnknownProtos :                 0
InDiscards :                      0
InDelivers :                      14577
OutRequests :                     5509
OutDiscards :                     0
OutNoRoutes :                     0
ReasmTimeout :                    0
ReasmReqds :                      57
ReasmOKs :                        10
ReasmFails :                      0
FragOKs :                         0
FragFails :                       0
FragCreates :                     0

TCP:
RtoAlgorithm :                    1
RtoMin :                          0
RtoMax :                          0
MaxConn :                         0


ActiveOpens :                     1
PassiveOpens :                    0
AttemptFails :                    0
EstabResets :                     0
CurrEstab :     Gauge:            3
InSegs :                          4668
OutSegs :                         3549
RetransSegs :                     0

UDP:
InDatagrams :                     9496
NoPorts :                         19
InErrors :                        0
OutDatagrams :                    1984

SNMP:
snmpInPkts :                      814
snmpOutPkts :                     814
snmpInBadVersions :               0
```

```
snmpInBadCommunityNames:          0
snmpInBadCommunityUses :          0
snmpInASNParseErrs :              0
snmpInTooBigs :                   0
snmpInNoSuchNames :               0
snmpInBadValues :                 0
snmpInReadOnlys :                 0
snmpInGenErrs :                   0
snmpInTotalReqVars :              824
snmpInTotalSetVars :              0
snmpInGetRequests :               827
snmpInGetNexts :                  0
snmpInSetRequests :               0
snmpInGetResponses :              0
snmpInTraps :                     0
snmpOutTooBigs :                  0
snmpOutNoSuchNames :              0
snmpOutBadValues :                0
snmpOutGenErrs :                  0
snmpOutGetRequests :              0
snmpOutGetNexts :                 0
snmpOutSetRequests :              0
snmpOutGetResponses :             838
snmpOutTraps :                    0
snmpEnableAuthenTraps :           2
```

8.3 System log

var/log/messages

This is a system log file where application error and status messages are recorded. Use the following command to view the file:

```
cat /var/log/messages
```

/usr/etc/ucd-snmp/syslog_hostlist.conf

This is a simple syslogd configuration file. It is possible to direct syslog messages to an external machine that is running syslog.

The file does not exist by default but can be generated for example with the following command:

```
printf "remotehost <ip address>\\n" >
/usr/etc/ucd-snmp/syslog_hostlist.conf

where
<ip address>
= ip address of the remote machine running syslogd
```

Federal Communication Commission 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 and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

FCC Caution: To assure continued compliance, (example - use only shielded interface cables when connecting to computer or peripheral devices) any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

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 minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.