NOKIA
A032

Wireless LAN Access Point Advanced User Guide

NOKIA
CONNECTING PEOPLE

Copyright notices

We reserve the right to make changes and improvements to any of the products described in this guide without prior notice. Nokia is not responsible for any loss of data, income or any consequential damage howsoever caused.

ISSUE 2

Welcome

This guide tells you how to operate the Nokia A032 Wireless LAN Access Point, and provides information about configuration options, management and performance tuning.

How to use this guide

You should first have read and followed the instructions in the *Getting Started* guide.

The material in this guide is for more advanced users and system managers who want to customize and fine-tune the Nokia A032's performance.

- *Using the Web manager* – This describes the web browser-based interface for configuring and monitoring the Nokia A032.
- *Command line interface* – This describes other ways of configuring the Nokia A032.
- *NID naming and security* – How to use MAC addresses to control network access.
- *Using TFTP* – How to upload and download configuration files and firmware updates.
- *SNMP manager* – Explains the capabilities of the Nokia A032 SNMP agent.
- *Appendices* – These provide more detailed material, such as WEP security measures, using wireless repeaters and bridges, upgrading instructions and troubleshooting tips.

Conventions used in this guide

Internet gateway information

Information relating to use of the Nokia A032 as an Internet access device, either by dial-up or NAT, is shown with a bar on the right-hand side of the page:

Internet Gateway

Such information includes Internet settings and NAT addressing and firewalls.

Notes

You'll find tips or other useful facts in side notes throughout the manual.

Your Nokia A032 can transfer information between a wired LAN and a wireless LAN.

Pay particular attention to notes that start with **Note** or **WARNING.**

Text conventions

The following conventions are used throughout this manual:

- `courier` is used for file names, or to denote text that appears on your screen.
- **`courier bold`** is used to denote text that you should type in.
- new terms are shown in *italic* text the first time they appear.
- **bold** text denotes the name of a physical button or LED on the **Nokia A032** unit (e.g. the **alert** LED) or a button on screen that you need to click (e.g. "click **Restart**").

Table of contents

1. Using the Web manager

The *Getting Started* guide explained how to perform initial configuration by putting the Nokia A032 into Learn mode.

In some cases, you can only configure the Nokia A032 from a nominated station. See Management security options on page 45.

Now you can access *all* of the Nokia A032's setup pages from any station (wired or wireless), using a standard browser interface, while the Nokia A032 is in Normal mode.

This is the easiest way of configuring your Nokia A032. The other methods available are described in *Command line interface* on page 67, *Using TFTP* on page 103 and *Appendix G – Upgrading.*

The browser interface also provides comprehensive status monitoring capabilities.

- *Displaying the Access Point home page*, below, explains how to access the browser-based setup and configuration pages.
- *Status monitoring* on page 5 explains how to monitor wireless link statistics, modem and LAN activity, for example, using the browser interface.
- *Web-based setup* on page 32 gives a detailed description of every parameter available for customizing the A032.

Displaying the Access Point home page

To display the Access Point home page:

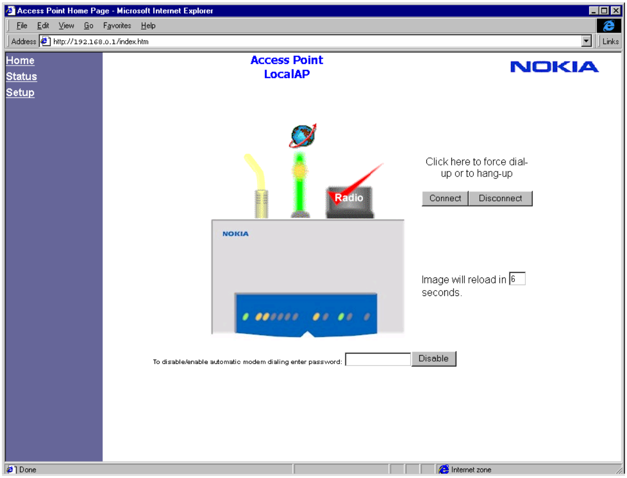
1 If necessary, start up the Nokia A032 in Normal mode.

2 From any wired or wireless LAN station, start a web browser (such as Internet Explorer).

3 Point the browser to the IP address of the Access Point. For example:

`http://192.168.0.1`

You'll see the Nokia A032 home page:



Access Point Home Page - Microsoft Internet Explorer

http://192.168.0.1/index.htm

Access Point
LocalAP

Click here to force dial-up or to hang-up

Image will reload in 6 seconds.

To disable/enable automatic modem dialing enter password:

Done

Internet zone

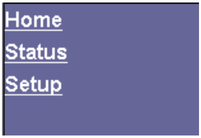
From here, you can access all of the Nokia A032's Status and Setup pages, as described below.

You can return to this home page at any time during status monitoring or configuration by clicking **Home** in the lefthand frame.

Home page features

The Home page gives a graphical indication of the status of the Nokia A032 and allows quick navigation to other status screens. The components shown here will depend on your setup.

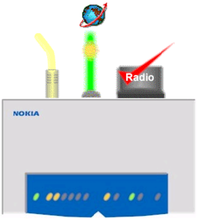
Menu bar



Down the lefthand side of the Home page there's a menu bar with the following links:

- **Home** – Displays the Home page.
- **Status** – Displays a brief summary of the A032's current status (see *Main status screen* on page 8).
- **Setup** – Allows you to enter the web-based configuration manager (see *Displaying Setup pages* on page 32 for more information).

Graphical cues and links



The image of the A032 on the Home page gives you a quick idea of the status of the various interfaces. You can click different parts of the image to view certain status pages.

See *Status summary and graphical links* on page 6 for more details.

Internet link action buttons

When dial-up Internet access is enabled, three buttons on the Home page give you manual control over dialing the modem:

- **Connect** – If the Internet link is down, click this to make a connection.
- **Disconnect (Abort) –** If the Internet link is up, click here to disconnect immediately. While the unit is dialing or in the process of connecting the button will display **Abort** but the result is the same.
- **Disable (Enable) –** Sometimes you need to prevent the unit from attempting to make automatic connections to the Internet. You can disable automatic dialing by entering the management password and clicking **Disable.** After the Internet connection has been disabled the unit will no longer attempt to dial out when users try to access the Internet. However, it will still be possible to force a connection by clicking **Connect.**

  While automatic dialing is disabled the button text reads **Enable**; enter the password and click here to reenable.

Status monitoring

You can use the Home page to monitor status, manually initiate or terminate the dial-up Internet link and navigate to other status screens.

Navigating the Status pages

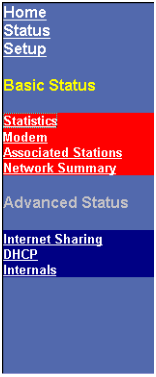
There are two ways of viewing the Status pages:

- Clicking the **Status** link in the lefthand menu bar
- Clicking various active parts of the image on the Home page.

Using the Status link

Click the **Status** link in the lefthand menu bar.

- You'll see a summary of the Nokia A032's status (see *Main status screen* on page 8).
- The menu bar will change, giving you links to all the status pages:



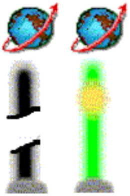
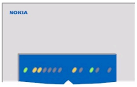
The status screens are described in detail later in this section (starting with *Main status screen* on page 8).

Status summary and graphical links

The image on the Home page gives you visual cues as to the current status of the LAN, Internet and wireless subsystems.

As a short-cut, you can click various active parts of the Nokia A032 image on the Home page.

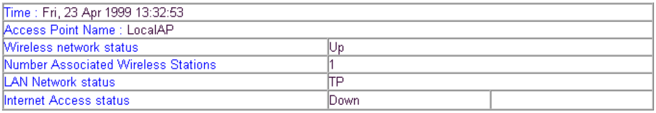
The following table summarizes these features.

Active image	Click to display...	Status summary indication
LAN 	LAN statistics see page 15	If a 10baseT LAN connection is present, a beige connector is shown. If no connection is present, no picture is shown.
Radio 	Radio statistics see page 11	If the radio is operating normally it will be shown with a red check mark. If the radio is not present, or operating incorrectly, the radio is shown with a large red cross.
Internet 		When dial-up Internet access is configured, this shows whether the modem link is currently connected. When there is no connection, the link is shown as a black broken line. When the unit is in the process of dialing or connecting, the link is shown as a solid dark green line. A successfully connected link is indicated by a bright green line with moving yellow bullets.
Globe	Modem statistics see page 19	
Link to globe	PPP statistics see page 16	
A032 unit 	Internals status see page 30	None.

Main status screen

You see this page when you click **Status** in the lefthand menu.

This gives a summary of the access point status:



Time : Fri, 23 Apr 1999 13:32:53		
Access Point Name : LocalAP		
Wireless network status	Up	
Number Associated Wireless Stations	1	
LAN Network status	TP	
Internet Access status	Down	

The lefthand menu changes to give links to all the detailed status reports.

The screen provides the following information:

Field	Description
Time	Current date and time as set in the unit
Access Point Name	The user-defined name for the unit (also appears in the screen header)
Wireless network status	This will normally indicate **Up**. If the radio is not present or faulty this will indicate **Down**
Number of Associated Wireless Stations	This shows how many wireless users are attached to the Nokia A032
LAN Network status	**TP** – 10baseT (twisted pair) **OFF** – the LAN has been disabled by the user.

Field	Description
Internet Access status	This shows the current state of the Internet Access port. Possible values are: • **Disabled** – Internet Access is configured off • **Down** – link is disconnected • **Backoff** – Link is down and in *backoff* mode due to previous failure to connect. Condition will clear after a period of time or can be overridden by a manual dial request • **Dialing** – Unit is currently dialing to the Internet • **Connecting** – Unit has connected to remote modem and is negotiating link parameters • **Up** – link is active • **AIR** – The NAT firewall is configured to the radio port • **LAN** – The NAT firewall is configured to the LAN port

The following sections explain the status screens displayed when you click on any of the links in the lefthand menu.

Statistics screens

There are four screens of data traffic statistics for the Nokia A032:

- Radio
- Radio detail – provides more basic information from the PCMCIA radio card
- LAN
- PPP.

To view these screens:

1. Click **Statistics** in the lefthand menu.

   This will show Radio statistics by default.

2. You can access the other screens by clicking the appropriate links at the bottom of the page (**Show Radio**, **Show Radio Detail** and **Show LAN**).

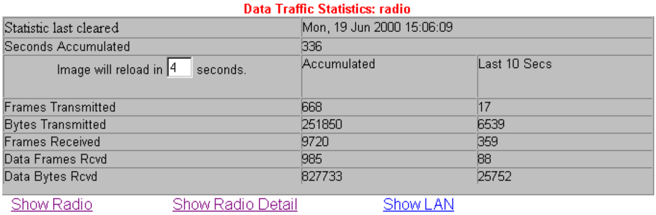
The difference between the two sets of **Radio** information is subtle but important. For example, if the radio receives data frames which have a bad check word, the PCMCIA radio card will count these frames but will not pass them on to the software in the main access point unit. Therefore information about CRC errors is best obtained from the radio Management Information Base (MIB) as described in *Radio card statistics* on page 13. In practice retransmission will normally ensure that the lost data is recovered. The A032 has information about both the radio interface and the LAN interface and gives a good summary of network activity.

All tables of statistics have the following fields in common:

Field	Description
Statistics last cleared	This shows the time and date when the accumulated statistics were reset to zero. Often this will be the last time the unit was restarted.
Seconds Accumulated	The number of seconds over which statistics have been accumulated. This can be useful for computing averages. Note that the largest value that can be displayed is about 4 billion (2^{32}). After this, the display will start counting from zero again.

Radio statistics

This is the default screen displayed when you click Statistics in the lefthand menu:



Data Traffic Statistics: radio

Statistic last cleared	Mon, 19 Jun 2000 15:06:09	
Seconds Accumulated	336	
Image will reload in 4 seconds.	Accumulated	Last 10 Secs
Frames Transmitted	668	17
Bytes Transmitted	251850	6539
Frames Received	9720	359
Data Frames Rcvd	985	88
Data Bytes Rcvd	827733	25752

This screen shows various statistics data for the wireless link.

The lower half of the table shows data specific to the interface – in this case the radio. Information is shown for the accumulated value and for the last 10 second sample.

The following fields are provided:

Field	Description
Frames Transmitted	Number of data and management frames sent over link
Bytes Transmitted	Number of bytes of data sent over the link
Frames Received	Number of data and MAC management frames received
Data Frames Rcvd	The number of frames received from the radio which are data frames (as opposed to management frames etc.).
Data Bytes Rcvd	Number of bytes in received data frames

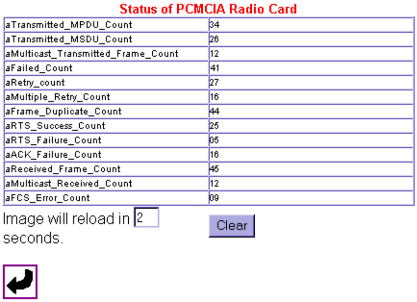
It is important to note that these statistics are collected by the A032 based on the frames sent between it and the PCMCIA radio card. The PCMCIA radio card does not forward all data to the A032 main processor. For example, CRC errors on received frames will be ignored by the radio card and not passed to the A032 main processor.

Radio card statistics

To view the **raw** statistics from the radio card click **Show Radio Detail** at the bottom of the radio statistics page.

To return to the Radio statistics page, click the Back icon or click **Statistics** in the lefthand menu.

This shows statistics collected by the radio card, presented in a form that matches the MIB definition of IEEE802.11.



Status of PCMCIA Radio Card

aTransmitted_MPDU_Count	34
aTransmitted_MSDU_Count	26
aMulticast_Transmitted_Frame_Count	12
aFailed_Count	41
aRetry_count	27
aMultiple_Retry_Count	16
aFrame_Duplicate_Count	44
aRTS_Success_Count	25
aRTS_Failure_Count	05
aACK_Failure_Count	16
aReceived_Frame_Count	45
aMulticast_Received_Count	12
aFCS_Error_Count	09

Image will reload in 2 seconds.

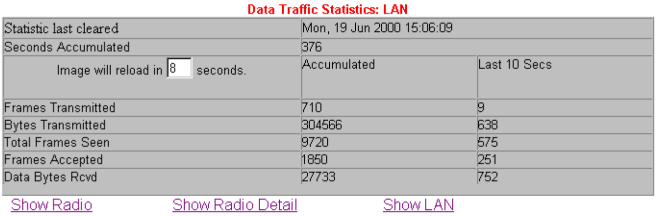
The meaning of the fields in this screen is given in the following table.

Field	Description
aTransmitted_MPDU_Count	Number of frames transmitted
aTransmitted_MSDU_Count	Number of data frames transmitted
aMulticast_Transmitted_Frame_Count	Number of Multicasts sent
aFailed_Count	Frames which could not be sent after retry
aRetry_Count	Frames which were resent
aMultiple_Retry_Count	Occurrences when multiple retries were needed to send a frame
aFrame_Duplicate_Count	Number of duplicate frames received (and discarded)
aRTS_Success_Count	Count of CTS received in response to RTS
aRTS_Failure_Count	Count of RTS that received no response
aACK_Failure_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

The fields update regularly. Click **Clear** to set them all to zero.

LAN statistics

To view statistics for the LAN link click **Show LAN** at the bottom of the radio statistics page. This will result in a screen as shown below:



Data Traffic Statistics: LAN

Statistic last cleared	Mon, 19 Jun 2000 15:06:09	
Seconds Accumulated	376	
Image will reload in 8 seconds.	Accumulated	Last 10 Secs
Frames Transmitted	710	9
Bytes Transmitted	304566	638
Total Frames Seen	9720	575
Frames Accepted	1850	251
Data Bytes Rcvd	27733	752

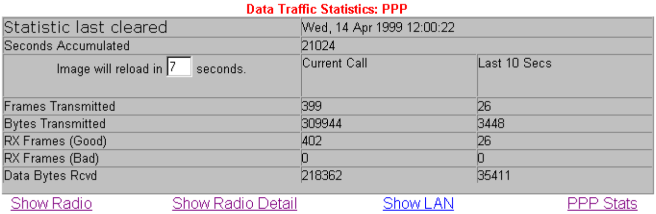
The meaning of the fields is given below:

Field	Description
Frames Transmitted	The number of frames transmitted from the Access Point to the Ethernet LAN.
Bytes Transmitted	The number of bytes in the frames transmitted.
Total Frames Seen	The number of frames seen on the LAN. In a busy network most of these will not be for wireless stations and will be ignored.
Frames Accepted	The number of frames accepted by the Access Point. These are either frames destined for wireless stations, the Internet connection or for the Access Point management.
Data Bytes Rcvd	The count of bytes contained in frames accepted by the Access Point.

PPP statistics

If Internet access functions are enabled, to view serial port PPP statistics, click **PPP Stats** at the bottom of the radio statistics page. The information reported depends on the state of the dial-up link.

- If a call is in progress the table shows the total statistics for the call and the statistics for the last 10 second sample:

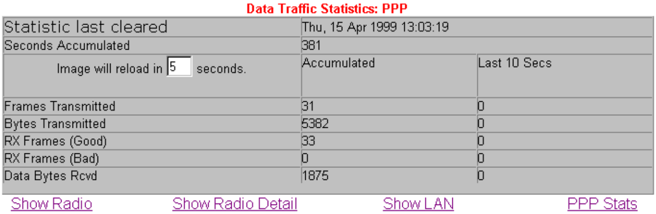


Data Traffic Statistics: PPP

Statistic last cleared	Wed, 14 Apr 1999 12:00:22	
Seconds Accumulated	21024	
Image will reload in 7 seconds.	Current Call	Last 10 Secs
Frames Transmitted	399	26
Bytes Transmitted	309944	3448
RX Frames (Good)	402	26
RX Frames (Bad)	0	0
Data Bytes Rcvd	218362	35411

Show Radio Show Radio Detail Show LAN PPP Stats

- If the link is down (no call in progress) the table shows accumulated total statistics:



Data Traffic Statistics: PPP

Statistic last cleared	Thu, 15 Apr 1999 13:03:19	
Seconds Accumulated	381	
Image will reload in 5 seconds.	Accumulated	Last 10 Secs
Frames Transmitted	31	0
Bytes Transmitted	5382	0
RX Frames (Good)	33	0
RX Frames (Bad)	0	0
Data Bytes Rcvd	1875	0

Show Radio Show Radio Detail Show LAN PPP Stats

The fields have the following meanings:

Field	Description
Frames Transmitted	Number of frames sent over PPP link
Bytes Transmitted	Number of bytes in transmitted PPP frames
RX Frames (Good)	Number of PPP frames received
Rx Frames (Bad)	Number of PPP frames discarded due to incomplete or CRC error
Data Bytes Rcvd	Number of data bytes in good received frames.

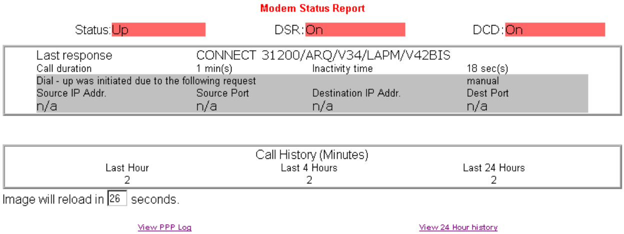
Status screens

Use the lefthand menu to access status screens. Some status screens have hyperlinks which take you to related status screens:

To view this Status screen...	Do this...
Associated wireless stations	Click **Associated Stations** in the lefthand menu.
All wireless stations	Click **Wireless Stations** in the Associated Stations screen.
All associated stations (wired and wireless)	Click **All** in the Associated Stations screen, or the **Network Summary** link in the lefthand menu
DHCP	Click **DHCP** in the lefthand menu.
Internals (diagnostics)	Click **Internals** in the lefthand menu.
Modem	Click **Modem** in the lefthand menu.
PPP log	Click **View PPP Log** in the Modem screen.
24hr dial-up history	Click **View 24 Hour History** in the Modem screen.
Advanced Internet sharing	Click **Internet Sharing** in the lefthand menu.

Modem status screen

To view the status of the serial port modem interface, click **Modem** in the lefthand menu. The screen displays slightly different information depending on connection status.



Modem Status Report

Status: Up DSR: On DCD: On

Last response	CONNECT 31200/ARQ/V34/LAPM/V42BIS		
Call duration	1 min(s)	Inactivity time	18 sec(s)
Dial - up was initiated due to the following request			manual
Source IP Addr.	Source Port	Destination IP Addr.	Dest Port
n/a	n/a	n/a	n/a

Call History (Minutes)

Last Hour	Last 4 Hours	Last 24 Hours
2	2	2

Image will reload in 26 seconds.

This screen is sometimes helpful when diagnosing dialing problems. The information on this screen is as follows:

Field	Description
Status	When the modem is connected the status will show **UP**.
DSR	When the modem is connected and powered on the DSR box should be red to indicate that the modem is ready
DCD	Indicates that the modem is currently receiving carrier – generally this means that it has made a connection to another modem.
Last Response	Shows the last message sent by the modem to the A032 during a dial attempt. This can be useful in several ways. If a connection is successful this usually shows the connect message received from the modem. This often has useful information about the type and speed of connection. If a connection fails, this might show the error message returned by the modem.

Field	Description
Backoff time	(Modem disconnected) When the modem is in backoff mode due to a previous failed dial attempt, this field indicates the number of seconds until the backoff state will clear. Backoff is designed to prevent the unit dialling repeatedly when the attempts keep failing. Backoff can be overridden using manual dialing.
Call duration	(Modem connected) Shows how many minutes the call has been active.
Inactivity timer	(Modem connected) Shows how many seconds the modem port has been inactive. When the inactivity timer reaches the configured level (default 3 minutes) the link will disconnect.
Reason	Why the last call was initiated. This can be useful if your system keeps dialing out unexpectedly. This field shows which computer on your network sent the frame which caused dialling, the type of frame and its destination.
Call History	The number of minutes the modem has been connected. Information is provided for the past 24 hours, 4 Hours and 1 Hour. A more detailed log of modem usage can be obtained by clicking **View 24 Hour History** (see below). Note that the values are reset to zero when the Access Point is restarted.

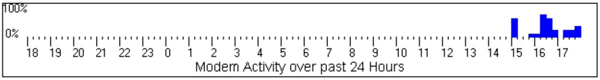
There are two links at the bottom of this screen:

- **View PPP Log**
- **View 24 Hour history**

See below for descriptions.

View 24 Hour History

This shows the usage of the modem over the last 24 hours (or since the last restart):

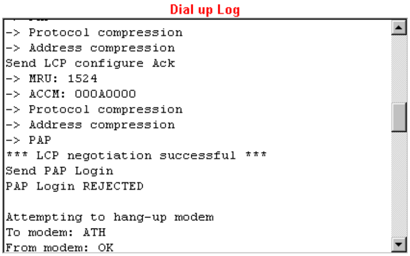


The chart shows the amount the modem was connected in each 15-minute interval. For example if the modem was connected twice within the period, once for 3 minutes and once for 5 minutes, the log will show 50% connected (8 minutes out of 15 minutes).

To return to the Modem statistics page, click the Back icon or click **Modem** in the lefthand menu.

View PPP Log

This screen keeps a log of the dialing and PPP negotiation for the previous call:



```
-> Protocol compression
-> Address compression
Send LCP configure Ack
-> MRU: 1524
-> ACCM: 000A0000
-> Protocol compression
-> Address compression
-> PAP
*** LCP negotiation successful ***
Send PAP Login
PAP Login REJECTED

Attempting to hang-up modem
To modem: ATH
From modem: OK
```

This is useful if you have a problem connecting to the Internet. If the ISP does not correctly negotiate the PPP link (and typically hangs up) you may be able to determine the reason from the log.

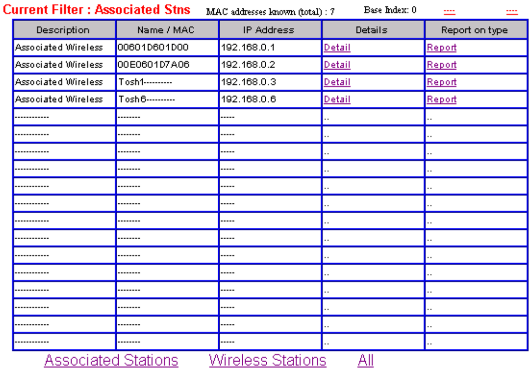
A common problem is to mis-type the password; the PPP log can help you here. You'll find useful information in *Troubleshooting dial-up connections* on page 185. You might not understand all the information in the PPP log, but it is invaluable if you use technical support to diagnose a connection problem.

The log is cleared each time a dial-up connection is attempted. In this way the last call is always captured regardless of whether it succeeded or failed.

↩ To return to the Modem statistics page, click the Back icon or click **Modem** in the lefthand menu.

LAN station status

Clicking **Associated Stations** in the lefthand menu displays information about wireless stations which are currently connected to (associated with) the A032:



Current Filter : Associated Stns MAC addresses known (total) : 7 Base Index: 0 ---- ----

Description	Name / MAC	IP Address	Details	Report on type
Associated Wireless	00601D601D00	192.168.0.1	Detail	Report
Associated Wireless	00E0601D7A06	192.168.0.2	Detail	Report
Associated Wireless	Tosh1----------	192.168.0.3	Detail	Report
Associated Wireless	Tosh6----------	192.168.0.6	Detail	Report
------------	--------	-----	..	..
------------	--------	-----	..	..
------------	--------	-----	..	..
------------	--------	-----	..	..
------------	--------	-----	..	..
------------	--------	-----	..	..
------------	--------	-----	..	..
------------	--------	-----	..	..
------------	--------	-----	..	..
------------	--------	-----	..	..
------------	--------	-----	..	..
------------	--------	-----	..	..
------------	--------	-----	..	..
------------	--------	-----	..	..

Associated Stations Wireless Stations All

Each line in the table shows data for one wireless station. If there are more stations than can be shown in a single screen, click **NEXT** at the right top corner of the status display to see more (the field **Base Index** increases as you click down through the entries to show that you are not at the start of the list).

The fields in the table have the following meaning:

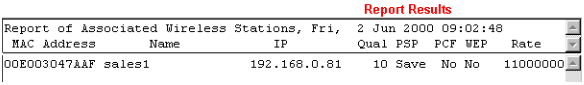
Field	Description
Description	The type of station. This can be any of the following: • Associated Wireless • Other Wireless (not associated) • Wired device (i.e. on LAN) • Via Wireless Bridge • Bridge Partner (another Access Point acting as a bridge) • Local Access Point (another Access Point on the current LAN) • Unknown
Name / MAC	The network name or MAC address of the station.
IP Address	For TCP/IP stations this may show the IP address of the station.
Detail link	See page 25.
Report on type link	See page 25.

Three hyperlinks are available at the bottom of the table:

- **Associated Stations** – (This screen) Shows wireless LAN stations currently associated with this A032. This includes other access points which are attached as bridges or repeaters
- **Wireless Stations** – Shows all wireless stations of which the Access Point is aware. There are several means by which the access point may discover other wireless stations including the Nokia Inter Access Point Protocol.
- **All** – Shows both wired and wireless stations.

Detail and Report screens

If you click the **Detail** link for a station in the table of associated stations, you'll see the following screen



Report Results

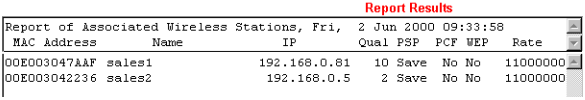
```
Report of Associated Wireless Stations, Fri,  2 Jun 2000 09:02:48
 MAC Address          Name              IP          Qual PSP  PCF WEP    Rate
00E003047AAF sales1                 192.168.0.81     10 Save  No No    11000000
```

As well as the station's MAC address, IP address and network name, this shows:

- Qual – a number from 1 to 10 indicating signal strength (10 is best)
- PSP – indicates whether the station is in power save mode
- PCF – indicates whether the station is operating in *point coordination* mode
- WEP – whether WEP security features are enabled
- Rate – The rate at which the station is currently communicating.

Point coordination function (PCF) is a mode of IEEE802.11 that can improve performance for certain types of data transfer.

If you click the **Report** link for a station in the table of associated stations, you'll see details for all similar stations (for example, all associated wireless stations, or all bridging partners):



Report Results

```
Report of Associated Wireless Stations, Fri,  2 Jun 2000 09:33:58
 MAC Address          Name              IP          Qual PSP  PCF WEP    Rate
00E003047AAF sales1                 192.168.0.81     10 Save  No No    11000000
00E003042236 sales2                  192.168.0.5      2 Save  No No    11000000
```

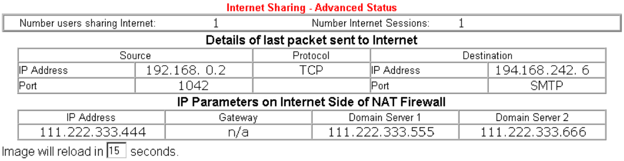
Network summary

Clicking this link on the lefthand menu has the same effect as clicking the **All** link on the Associated Stations screen.

Advanced Internet sharing status

Click **Internet Sharing** in the Advanced Status section of the lefthand menu.

This screen provides information related to the NAT firewall and the PPP IPCP negotiation:



Internet Sharing - Advanced Status

Number users sharing Internet:	1	Number Internet Sessions:	1

Details of last packet sent to Internet

Source		Protocol	Destination	
IP Address	192.168. 0.2	TCP	IP Address	194.168.242. 6
Port	1042		Port	SMTP

IP Parameters on Internet Side of NAT Firewall

IP Address	Gateway	Domain Server 1	Domain Server 2
111.222.333.444	n/a	111.222.333.555	111.222.333.666

Image will reload in 15 seconds.

There are three sections to the display:

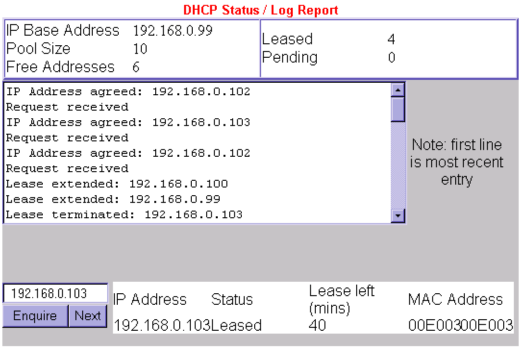
- Summary of NAT Tables entries
- Data about most recent packet forwarded
- PPP IPCP summary.

Field	Description
Number of users sharing Internet	Number of users on the local network that are currently using (or have recently accessed) the Internet. Each user may access more than one Internet site.
Number Internet Sessions	Number of entries currently used in the NAT table. Even when a user is accessing a single web-site the number of sessions may increase rapidly as most browsers open a new session for each component of a web page. The maximum number of Internet Sessions (NAT table entries) the A032 can handle is 256.
Details of last packet send to Internet	Source and destination information for the most recent packet forwarded. This information might be useful if the link is staying up unexpectedly. If the link does not drop, this screen enables you to find out which computer is sending packets to the Internet. Note that if system is configured such that inbound packets from the Internet clear the inactivity timer, the link may stay up due to incoming packets which would not be shown on this screen. This screen only records outbound packets. In this case check the PPP statistics screen (see page 16) and look for evidence of inbound packets
IP Parameters on Internet Side of NAT Firewall	IP information that has been received from the network (or configured by the user).

DHCP status screen

Click **DHCP** in the Advanced Status section of the lefthand menu.

The DHCP status screen allows you to see which DHCP addresses are assigned. It also keeps a running log of the most recent activity:



DHCP Status / Log Report

IP Base Address	192.168.0.99	Leased	4
Pool Size	10	Pending	0
Free Addresses	6		

```
IP Address agreed: 192.168.0.102
Request received
IP Address agreed: 192.168.0.103
Request received
IP Address agreed: 192.168.0.102
Request received
Lease extended: 192.168.0.100
Lease extended: 192.168.0.99
Lease terminated: 192.168.0.103
```

Note: first line is most recent entry

192.168.0.103

IP Address	Status	Lease left (mins)	MAC Address
192.168.0.103	Leased	40	00E00300E003

The screen is divided into three sections:

- Summary information about the DHCP server
- The DHCP log
- Detailed information about a specific DHCP address.

Summary fields

The Summary fields are as follows:

Field	Description
IP Base Address	The DHCP base address as configured by the manager
Pool Size	The DHCP pool size as configured by the manager
Free Addresses	The number of unassigned addresses
Leased	The number of addresses currently assigned and in use
Pending	The number of addresses reserved due to pending requests

DHCP log

The DHCP log records when stations request an address and also when an address is leased. Since the lease is renewed every hour this will be the most common message. Note that new entries in the log are placed at the top of the list. This avoids the need to scroll down the list to get the most recent information.

Detailed DHCP address information

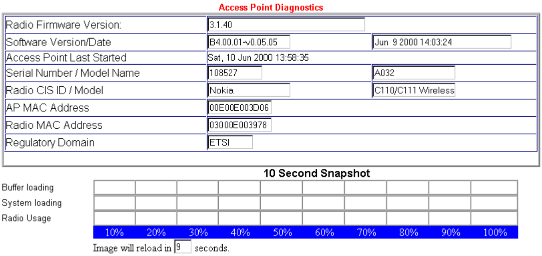
The lower section of this screen allows a manager to get specific information for an address. To obtain the information:

1. Enter the IP address in the lefthand field.
2. Click **Enquire**. The system will display the lease status, lease duration and the MAC address of the station to which the lease has been granted.
3. To view the next IP address in the pool, click **Next**.

The lease status may be *Open* (unassigned) *Pending* or *Leased*. If the status shows "*****" the selected address is outside the DHCP address pool.

Internals status screen

This status screen provides information about the internal operation of the A032:



Access Point Diagnostics

Radio Firmware Version:	3.1.40	
Software Version/Date	B4.00.01-v0.05.05	Jun 9 2000 14:03:24
Access Point Last Started	Sat, 10 Jun 2000 13:58:35	
Serial Number / Model Name	108527	A032
Radio CIS ID / Model	Nokia	C110/C111 Wireless
AP MAC Address	00E00E003D06	
Radio MAC Address	03000E003978	
Regulatory Domain	ETSI	

10 Second Snapshot

Image will reload in 9 seconds.

The first part of the screen provides information about the A032 and the PCMCIA radio cards (if inserted). The fields are explained below:

Field	Meaning
Radio Firmware Version	The version number of the firmware for the radio card. (it may be required or useful to quote if you require technical assistance during a support call).
Software Version/Date	The first part of the version number (*x.xx.xx*) is the release number of the Nokia A032 software `img1.bin`. The second part (*yy.yy*) is the version number of the Nokia A032 BIOS (`bios.bin`). The Date code shows the build date for the Nokia A032 software which can be useful for technical support.
Access Point Last started	The timestamp when the access point was last restarted. Note that this is the timestamp as it existed during start up. If you change the system time and date, the start timestamp will be unaffected.
Serial Number / Model Name	This should correspond to the serial number printed on the label on the unit, and displays the type of Access Point (A032).
Radio CIS ID / Model	This shows information about the radio card inserted in the Nokia A032.

Field	Meaning
AP MAC Address	The MAC address of the access point. This is the address used by all management accesses to the unit.
RADIO MAC Address	The MAC address of the radio card. This is used for IEEE802.11 transmissions and is permanently stored in the radio card.
Regulatory Domain	The regulatory domain is set in the configuration section (see *Basic Access Point setup* on page 35) according to the country in which the access point is operating. The Access Point will not attempt to set frequency channels outside the allowed range of the regulatory domain.

Three bar graphs are shown at the bottom of the screen. These provide information about the state of the system and radio:

- **Buffer Loading** – The A032 depends on memory buffers to store data passing through the unit. This graph shows how many of the buffers are used. If the graph approaches 100% you might see some reduction in throughput or lost packets. Under normal circumstances the buffer utilization should be under 60%
- **System Loading** – Utilization of the processor in the A032. Normally this will be less that 50%
- **Radio Usage** – Utilization of the radio link.

The first bar indicates a value between 0 and 10%. The second bar 10% – 20% and so on. The graph is refreshed every 10 seconds.

Web-based setup

This section explains all the options available on the Setup pages.

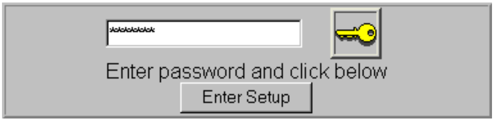
Displaying Setup pages

You can only configure the Nokia A032 if you know the management password – this is set to `default` at the factory. The system manager should change this as soon as possible (see *Management security options* on page 45).

Before you can begin configuring the Nokia A032, you need to log on:

1 Click the **Setup** link in the lefthand frame of the Home page.

This will display a log-on screen:



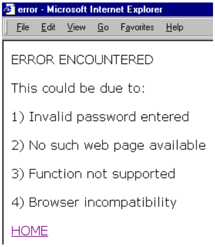
****

Enter password and click below

2 Note that if the password is `default`, this will be entered automatically by the access point and shown as *******.

3 Click **Enter Setup.**

4 If you enter the password incorrectly, or there are other problems, you'll see the following message:


error - Microsoft Internet Explorer
File Edit View Go Favorites Help

ERROR ENCOUNTERED

This could be due to:

1) Invalid password entered

2) No such web page available

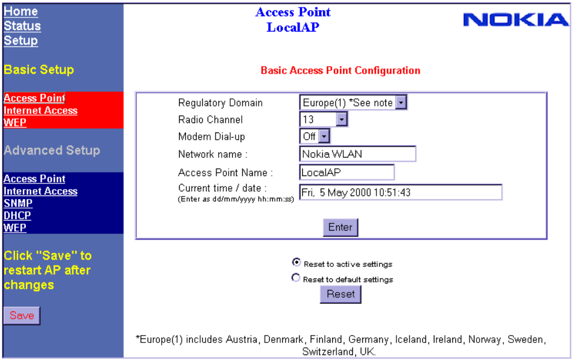
3) Function not supported

4) Browser incompatibility

HOME

Click **HOME** and try again.

After correctly entering the password you'll see the basic setup page:



Basic Access Point Configuration

Regulatory Domain	Europe(1) *See note
Radio Channel	13
Modem Dial-up	Off
Network name :	Nokia WLAN
Access Point Name :	LocalAP
Current time / date : (Enter as dd/mm/yyyy hh:mm:ss)	Fri, 5 May 2000 10:51:43

● Reset to active settings
○ Reset to default settings

*Europe(1) includes Austria, Denmark, Finland, Germany, Iceland, Ireland, Norway, Sweden, Switzerland, UK.

(For a description of these options, see page 35.)

Basic and Advanced links

The links on the left give access to the various set-up screens. These are divided into two sections labelled **Basic** and **Advanced**. The basic parameters include most of the required parameters for normal operation.

Making changes

In general, to alter configuration parameters:

1. Click a link in the lefthand frame to display the appropriate configuration page.
2. Make any changes, as necessary.
3. On many screens you need to click **Enter** (or in some cases **Add**) in order for the changes to be recorded.
4. If necessary, repeat steps 1, 2 and 3 until you've completed configuration.
5. Click **Save** in the lefthand frame. This will cause the new parameters to be written to permanent memory; the Nokia A032 will restart, putting the changes into effect.

Important: *Don't miss out this step.*

Reverting to active or default settings

Many configuration screens have the following radio buttons at the bottom:

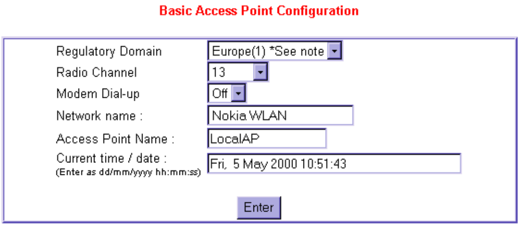
- **Reset to active settings** – This causes the original settings (as at the last restart) to be restored.
- **Reset to default settings** – This causes the factory default settings to be loaded (*only* those shown on this screen – not all parameters).

To reset:

1. Select the appropriate radio button.
2. Click **Reset**.
3. Click **Save**.

Basic Access Point setup

The first screen you see after successfully entering the setup password correctly is the Basic Access Point configuration page:



Basic Access Point Configuration

Regulatory Domain: Europe(1) *See note

Radio Channel: 13

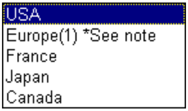
Modem Dial-up: Off

Network name : Nokia WLAN

Access Point Name : LocalAP

Current time / date : (Enter as dd/mm/yyyy hh:mm:ss) Fri, 5 May 2000 10:51:43

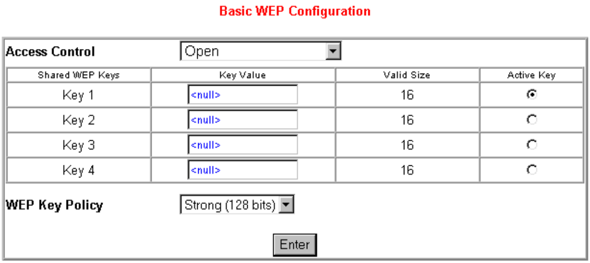
The following options are available.

Option	Description
Regulatory Domain	This defines the radio channels you are allowed to use, depending on which country is set. If this is the first time you have used the access point: 1 Select your country from the **Regulatory Domain** drop-down:  USA Europe(1) *See note France Japan Canada 2 Click **Enter**. 3 Select a **Radio Channel**. 4 Click **Enter**. **Important**: Use only the region setting appropriate for the area where the wireless LAN card is used at the present time. Using the Nokia Wireless LAN adapter card in any other region or with an incorrect region setting may be illegal. Note that choosing European Domain will cause the date fields to be interpreted in European format (dd/mm/yyyy).
Radio Channel	Specifies the operating channel for the Nokia A032.

Option	Description
Modem Dial-up	Set this to **`On`** to enable Internet sharing and dial-up Internet access. See *Basic Internet Access setup* on page 39 for more information.
Network name	String specifying the network name for the wireless LAN in Infrastructure mode. The entry can be up to 32 alphanumeric characters, and may include spaces. If you're only using one network, you can use the default (**`Nokia WLAN`**).
Access Point Name	String up to 15 characters used to give the Nokia A032 an identifier name. Useful if you have multiple access points on a network.
Current time / date	Allows you to update the real time clock in the Nokia A032. This takes immediate effect and does not require the unit to be restarted. To change the time, either edit the string or delete the entire field and enter the format ***`mm/dd/yyyy hh:mm:ss`*** (or ***`dd/mm/yyyy hh:mm:ss`*** in Europe).

Basic WEP setup

This screen allows you to configure the most commonly-used WEP functions (for a description of WEP, see *Data encryption and security* on page 127):



Basic WEP Configuration

Access Control: Open

Shared WEP Keys	Key Value	Valid Size	Active Key
Key 1	<null>	16	●
Key 2	<null>	16	○
Key 3	<null>	16	○
Key 4	<null>	16	○

WEP Key Policy: Strong (128 bits)

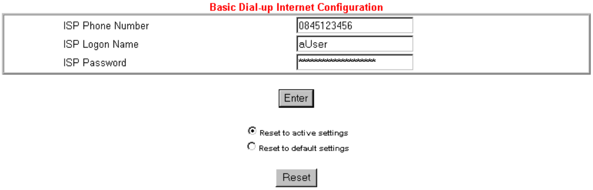
The following options are available.

Option	Description
Access Control	Determines how WEP operates on the access point. Values are: • **Open** – Least restrictive mode. Allows the same stations as **WEP**, plus non-WEP stations using open authentication (no key required). Note that the Nokia A032 is forced to use open access in Learn mode. • **WEP** – Allows the same stations as **Personal WEP Only**, plus stations with a valid shared WEP key. • **Personal WEP Only** – Most restrictive mode. Only allows stations with a valid personal WEP key. • **WiFi WEP** – Special mode used with some non-Nokia WiFi compatible systems. Station may use open authentication (no key required) to associate with the access point and then switch to WEP encryption using a shared WEP key. Personal WEP keys are not supported. This mode is provided for compatibility with some other vendor equipment but is not generally recommended.

Option	Description
Key 1 **Key 2** **Key 3** **Key 4**	These fields are used to enter the shared WEP key values. Note that the values are not displayed after entry (they appear as ****). If you want to enter keys in hexadecimal, prefix them with **`0x`**. **Important**: The keys will only work if their length is within the **Valid Size** limits (see below). A valid key is shown in green. If you enter a key that is too long, it will be shown in red.
Valid Size	(Read only) Tells you the valid size of the password for the current setting of WEP Key Policy. This indicates how many characters should be in the WEP key.
Active Key	This determines which of the four shared WEP keys is active (i.e. used for transmission).
WEP Key Policy	This parameter determines the number of bits allowed for the WEP keys. • **Normal** – IEEE802.11 compatible mode: 40 bits • **Strong** – 128-bit key length • **Custom** – See Min and Max key length settings in *Advanced WEP setup* on page 49

Basic Internet Access setup

Most of the settings required for use with the Internet Access (dial-up networking) function of the Nokia A032 can be configured from this screen:



Basic Dial-up Internet Configuration

ISP Phone Number	0845123456
ISP Logon Name	aUser
ISP Password	********************

This section assumes you're using a modem for Internet access. If you've specified LAN or Radio for **NAT Port** under the advanced configuration, see *Advanced Internet Access setup (LAN or Wireless)* on page 60.

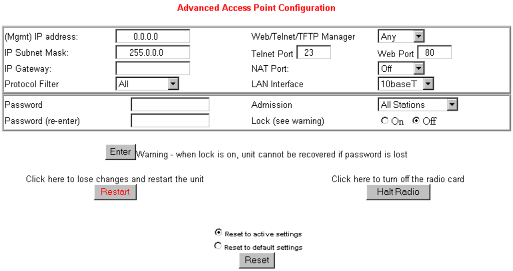
This screen is designed for use with most Internet service providers. Note that some providers require the use of a logon script (see page 55).

The following options are available:

Option	Description
ISP Phone Number	Your ISP's phone number for a dial-up Internet connection; you can use commas to cause delays between digits.
ISP Logon Name	ISP user name for dial-up networking under Windows.
ISP Password	ISP password for dial-up networking under Windows.

Advanced Access Point setup

This screen allows access to a number of special configuration modes and security-related functions:



Advanced Access Point Configuration

(Mgmt) IP address:	0.0.0.0	Web/Telnet/TFTP Manager	Any
IP Subnet Mask:	255.0.0.0	Telnet Port 23	Web Port 80
IP Gateway:		NAT Port:	Off
Protocol Filter	All	LAN Interface	10baseT
Password		Admission	All Stations
Password (re-enter)		Lock (see warning)	○ On ● Off

Warning - when lock is on, unit cannot be recovered if password is lost

Click here to lose changes and restart the unit

Click here to turn off the radio card

● Reset to active settings

○ Reset to default settings

Action buttons

Two action buttons are provided on the advanced screen.

- **Restart** – causes the A032 to perform a power-on reset. Any pending changes which have not been saved will be discarded.
- **Halt Radio** – disables the radio in the unit. This is a way of ensuring that the access point is disconnected from the radio network even though the management functions of the access point are still accessible from the wired LAN or serial port. The radio can only be restarted by performing a power-on reset or by using the **Restart** button).

TCP/IP-related settings

Note: *If you modify the IP address settings, you may need to renew the IP information in your wireless station – see page 175.*

For basic operation as an access point the Nokia A032 does not need to be assigned TCP/IP information. The default state of the unit is to have no IP address assigned. However, in order for you to be able to use most of the management utilities and the Internet access functions the access point needs an IP address (which you can assign manually, or automatically using the DHCP function).

The options associated with the TCP/IP information are:

Option	Description
(Mgmt) IP address	The IP address assigned to the Nokia A032 for management purposes. Normally the network system administrator will select this value. If you do not want to assign an IP address, or if you want to configure the Nokia A032 to assign itself an IP address using its own DHCP server, set this field to **`0.0.0.0`** Changes to this field do not take effect until the unit is restarted so that it is possible to change the IP value without interfering with operation of the web browser.
IP Subnet Mask	This must be set to the value used on the local IP subnetwork to which the unit is attached
IP Gateway	This is the address of the gateway router on the local network. It is required if the access point management functions will be accessed from outside the local sub-network. Note that when Internet access is enabled, the access point also acts as the gateway for the local LAN segment; in that case the gateway value is assigned automatically and cannot be overridden.

Protocol filtering

This is used to restrict the type of frames which are forwarded by the Nokia A032 from the wireless clients to the LAN (and back).

Setting	Description
All	All frames are forwarded (default).
TCP/IP	The Nokia A032 only forwards TCP/IP frames. This is useful in networks which have a large amount of mixed traffic. In particular, some older systems using MAC level multicast (e.g. DEC LAT) to communicate between terminals and Mainframe computers. These multicasts are generally not useful to wireless clients but can use up a significant amount of the wireless bandwidth. Selecting **Filter TCP/IP** prevents non TCP/IP traffic from being forwarded and may improve data throughput.

Telnet/Web ports

For security reasons or for remote access you may want to make the Nokia A032 respond to non-standard port numbers for Telnet and Web access.

The Telnet and/or Web manager functions can be disabled by selecting port **`0`**. The default values for the Telnet and Web ports are **`23`** and **`80`** respectively.

Most browsers allow access to a non-standard port numbers using a URL of the form
`http:`*`//static_IP_address:port_number`*

NAT port selection

See *Appendix H* for a complete description of NAT firewalls and port selection.

Usually you'll use the **Modem** or **off** setting here:

- **Modem** – used for dial-up networking
- **off** – disables Internet access.

Selection of the NAT port affects some of the other screens, notably the Internet Access setup (which uses different parameters depending on whether the NAT port is applied to the LAN or Radio interface).

LAN interface

Use this option to control the LAN interface. Options are as follows:

- **10baseT active**
- **Off** – Disables the LAN interface.

Management security options

You can prevent unauthorized access to the management function by selecting the level of security and the password.

The configuration fields associated with Security settings are:

Field	Description
Web/Telnet/TFTP Manager	Use this to restrict access to the Web, Telnet and TFTP management interfaces. The options are as follows: • **Any** - Allows any LAN or WLAN station to use the management functions. • **None** – disables access to the management functions. **Use this with caution**. When this option is selected the only management method remaining is to use the command line monitor via the serial port. If you have the serial port assigned to the modem interface, you can activate the serial port command line manager by starting in Learn mode. • **Specific** – Restricts access to the management functions to machines with IP addresses defined in the Set Specific Managers screen (see below).
Password	Used to enter a new access point password. You need to enter the password twice then click **Enter**.
Admission	Used in conjunction with the NID naming capability, this menu box can allow selective authorization of wireless clients and prevent unauthorized network access. See *NID naming and security* on page 97. Options are: **All Stations** – accept any wireless client **Named Stations** – accept only those for which a NID Name is defined **No Stations** – reject all wireless clients
Lock	This can be set **On** or **Off** and takes effect as soon as you click **Enter**– see page 46.

Warning: *If the password is forgotten when locked, the unit cannot be unlocked.*

Locking the password

The lock feature is designed to prevent unauthorized changes to the configuration – even in cases where the unit is mounted in an insecure area. Setting lock on has the following results:

- The password cannot be changed.
- The *Reset unit to default* feature is disabled so that the unit cannot be reconfigured even with physical access.
- The *backdoor* password is disabled – Nokia Technical support can normally recover a unit when the password has been forgotten using a backdoor password. When locked, this is disabled.
- TFTP functions are disabled.
- Normal Learn mode is disabled. When in learn mode the only difference compared to Manual mode is that the serial port is assigned to the command line monitor instead of the Internet Access function.

The net effect of locking the unit is that it is impossible to change the configuration of the unit without knowledge of the configuration password. This means that if the password is lost or forgotten, the unit cannot be recovered without physical repair at the factory. Such repair is **not** covered by the warrantee.

Setting specific managers

The A032 can be configured so that only specific workstations are allowed to access the management functions. This is especially important for TFTP protection.

The TFTP function (see page 103) allows you to reconfigure and download firmware to the unit.

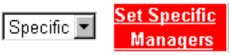
However, the TFTP function is not password protected. If you are concerned about security you may choose to disable the TFTP function (except when required) or specify the IP addresses of up to four managers' workstations which are allowed to perform the task. In this case the A032 will only accept transfers from workstations with those specified IP addresses. In addition, only the named managers will be allowed to access the Telnet or web functions.

To set specific managers:

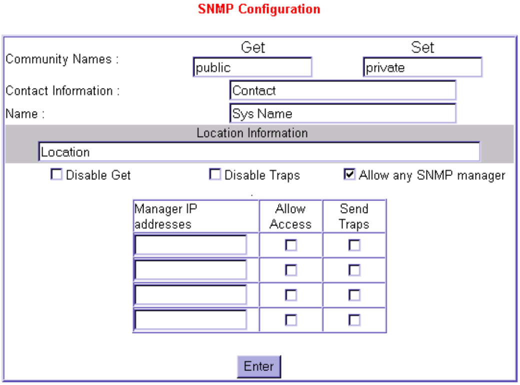
1 Set **Specific** in the **Web/Telnet/FTP Manager** field on the Advanced Access Point setup screen.

2 Click **Enter.**

3 Click the new button **(Set Specific Managers)** that appears next to the Web/Telnet/FTP Manager field.



You'll see the following screen:



SNMP Configuration

Community Names : Get: public Set: private

Contact Information : Contact

Name : Sys Name

Location Information: Location

☐ Disable Get ☐ Disable Traps ☑ Allow any SNMP manager

Manager IP addresses	Allow Access	Send Traps
	☐	☐
	☐	☐
	☐	☐
	☐	☐

Some of these fields are only relevant for SNMP – see SNMP setup on page 63.

4 In the **Manager IP addresses** fields, enter the IP addresses of up to four workstations which you want to be able to configure the A032.

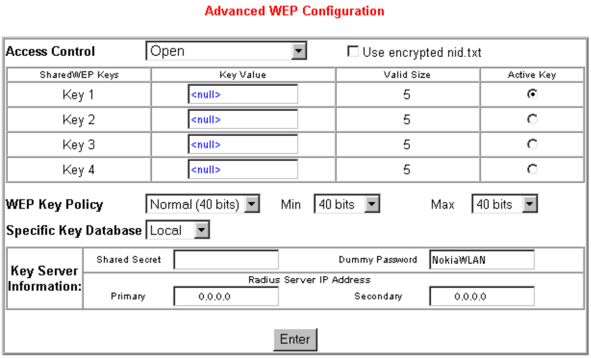
5 Use the **Allow Access** boxes to switch access on or off for each workstation.

6 Click **Enter**.

7 If necessary, click the Back button to return to the Advanced setup screen.

Advanced WEP setup

This screen allows you to configure all the WEP functions (for a description of WEP, see *Data encryption and security* on page 127):



Advanced WEP Configuration

Access Control: Open ▾ □ Use encrypted nid.txt

SharedWEP Keys	Key Value	Valid Size	Active Key
Key 1	<null>	5	●
Key 2	<null>	5	○
Key 3	<null>	5	○
Key 4	<null>	5	○

WEP Key Policy: Normal (40 bits) ▾ Min: 40 bits ▾ Max: 40 bits ▾

Specific Key Database: Local ▾

Key Server Information:

Shared Secret		Dummy Password	NokiaWLAN
Radius Server IP Address			
Primary	0.0.0.0	Secondary	0.0.0.0

Enter

In addition to the basic functions described in *Basic WEP setup* on page 37, the following options are available.

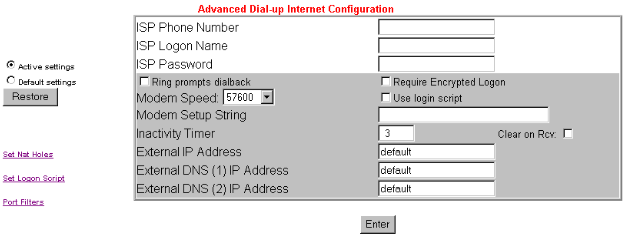
Option	Description
Use encrypted nids.txt	Affects the format of the nids.txt file used to load specific keys (nids.txt is generated by WEPGen – see page 163). When this box is checked, the file must be in encrypted form. When unchecked, the file must be in normal text mode (keys are still encrypted in the file).
Min, Max key length	When the **WEP Key Policy** is set to **Custom**, the values of min and max show the encryption strengths, and can take the following values: **40** (enter keys as ten octets) **56** (enter keys as 14 octets) **64** (enter keys as 16 octets) **96** (enter keys as 24 octets) **128** (enter keys as 32 octets)

Option	Description
Specific Key Database	Determines which key database the Nokia A032 will use for clients with personal WEP keys. • **Local** – The Nokia A032 will only use the keys stored in its internal flash memory • **RADIUS** – The Nokia A032 will only use keys obtained from the external key database via RADIUS • **Either** – The Nokia A032 will first look in its internal key database and, if not found, then access the external database.
Shared Secret	An alphanumeric string of up to 16 characters specifying the shared secret assigned to this access point. This value must match that in the RADIUS servers and that used by the WEPGen utility (see *Appendix E – Using the WEPGen utility*).
Dummy Password	An alphanumeric string of up to 16 characters specifying the dummy password, also stored in the RADIUS server. Each key entry in the server is given the same dummy password.
RADIUS Server IP Addresses	The IP address of the RADIUS server. Two addresses can be entered, a primary and a secondary. The secondary value is optional.

Advanced Internet Access setup (modem)

This screen is available if your Internet access is via a modem.

This screen displays all the options associated with the Basic Internet Access configuration screen, along with some more advanced ones:



● Active settings
○ Default settings
Restore

Set Nat Holes
Set Logon Script
Port Filters

Advanced Dial-up Internet Configuration

ISP Phone Number		
ISP Logon Name		
ISP Password		
☐ Ring prompts dialback	☐ Require Encrypted Logon	
Modem Speed: 57600	☐ Use login script	
Modem Setup String		
Inactivity Timer	3	Clear on Rcv: ☐
External IP Address	default	
External DNS (1) IP Address	default	
External DNS (2) IP Address	default	

Enter

The available configuration options are as follows:

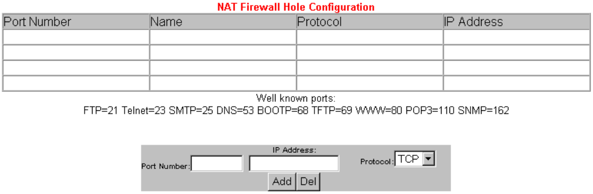
Option	Description
ISP Phone Number	Your ISP's phone number for a dial-up Internet connection; you can use commas to cause delays between digits.
ISP Logon Name	ISP user name for dial-up networking under Windows.
ISP Password	ISP password for dial-up networking under Windows.
Ring prompts dialback	In some circumstances you may need to initiate communication with the network from outside the NAT firewall. You can achieve this in conjunction with the Set NAT Holes sub-screen (see page 54). However, this requires that the dial-up connection be established. The **Ring Prompts Dialback** function provides a means of forcing the A032 to connect to the ISP. First call the phone number of the modem to which the A032 is connected. The modem will not answer but the A032 will observe that the line is ringing. Now hang up – within 30 seconds the A032 will dial out and connect to the Internet. Now you can access the server as required.

Option	Description
Require Encrypted Logon	If checked, the A032 will refuse to log on to ISPs which do not support encrypted log-on (i.e. PPP-MD5CHAP). If this option is disabled, and your ISP doesn't support encrypted logons, the A032 may use a less secure method (PAP) in which the username and password are sent in clear text format.
Modem Speed	Specifies the data rate used to communicate between the Nokia A032 and a modem. Note that this is not necessarily the rate that the modem will support when it communicates to the ISP. Generally the modem will not connect at a speed higher than this rate but it may connect at a speed which is lower.
Use Logon Script	This check box informs the A032 that it must use a logon script in order to connect to the network. When this box is checked you must configure the script using the **Set Logon Script** sub-screen (see page 55).
Modem Setup String	This allows you to send commands to the modem prior to dialing. Typically these would be AT commands to set various modes and options. Most modems do not require any special setup to operate.
Inactivity Timer	This determines how many minutes of inactivity are allowed before the modem connection is dropped. The default is 3 minutes.
Clear on Rcv	This is related to the Inactivity timer. It determines whether *received* frames (i.e. from the ISP to the Access Point) are considered to be 'activity'. It is off by default, preventing the problem where the link is kept up indefinitely due to spurious frames sent from the ISP to the account. The only time it may be necessary to set this checkbox is if you are using a non-acknowledged download such as a UDP multicast session for real time video.

Option	Description
External IP Address	If your ISP does not allocate IP addresses dynamically, set your static IP address here. Otherwise, leave it blank.
External DNS IP Address (1 & 2)	Most modern ISP accounts send DNS server information to a user's computer when logging on, so you can usually leave these blank. However, some accounts require that you configure the DNS addresses manually.

Setting NAT Holes

The NAT firewall normally prevents computers outside the firewall from accessing computers on your network. However, in some cases you may want to allow such accesses – if you have a web server on your local network, for example. The Set NAT Holes screen allows you to define up to four *NAT holes* and allow external access to specific machines on your LAN:



NAT Firewall Hole Configuration

Port Number	Name	Protocol	IP Address

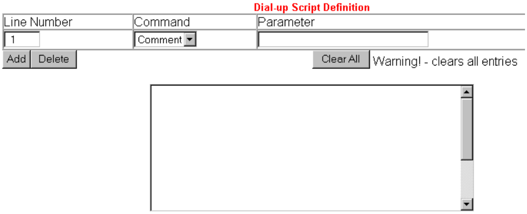
Well known ports:
FTP=21 Telnet=23 SMTP=25 DNS=53 BOOTP=68 TFTP=69 WWW=80 POP3=110 SNMP=162

Port Number:
IP Address:
Protocol: TCP

Please see *Setting NAT holes – providing external access* on page 201 for a detailed description.

Setting a logon script

Most ISPs don't require you to specify a logon script. Your ISP will tell you if you need to do this:



Dial-up Script Definition

Line Number	Command	Parameter
1	Comment	

To enter a line in the script:

1. Enter the **Line Number** (you can leave this step out to add a line to the end of the script).
2. Choose a **Command** from the drop-down menu.
3. Enter a suitable **Parameter** value.
4. Click **Add**.

To delete a line, enter its number and click **Delete**.

Each line of the script can be one of the following types:

Command	Parameter	Action
Comment	`Comment Text`	Inserts text into the script which may be useful for your future reference. Comment lines serve no function in the operation of the script.
Mode	**odd**, **even** or **none**	Some ISPs require that the serial line be configured for even or odd parity. In these cases the Mode command must be used. The parity of the serial port will be restored to "none" when the script has completed execution
delay	**seconds**	Causes the script to stop and wait for the specified number of seconds. This may be useful at the start to ensure that the ISP is ready to activate.
wait	**Text String**	Causes the script to wait until the ISP sends the specified text string. Typically the script waits for a log in prompt and a password prompt. The script will wait for 5 seconds. If the text is not found in that time, the script is aborted and the log on attempt fails.
SendCR	**none**	Sends the new line sequence to the ISP.
Send	**Text String**	Sends text to the ISP. It also supports two special tokens: `$USER`, `$PASSWORD`. If one of these tokens is used as the parameter, it will be replaced by the configured username or password (from the Internet Access Screen) when the script is run.

Example script

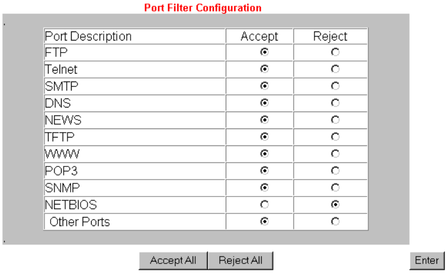
An example of a script is shown below:

```
1: / Example Script
2: delay 2
3: sendcr
4: wait "username:"
5: send "$USER"
6: sendcr
7: wait "protocol:"
8: send "PPP"
9: sendcr
```

Line 1	Comment only
Line 2	Delay 2 seconds
Line 3	Sends CRLF to ISP (Often required to get the login prompt)
Line 4	Access Point waits until the ISP sends the text `"username:"`
Line 5	Access Point sends the username. Note you can type in the username or $USER will cause it to substitute the username defined in the Access Point configuration. ($PASSWORD also works)
Line 6	Sends CRLF at entry of username
Line 7	Access Point waits for prompt: `"protocol"`
Lines 8, 9	Access Point sends `"PPP<CRLF>"`

Set port filters

By default, all IP frames which are addressed off the local network will be passed by the A032 to the Internet. If a connection is not available, a dial-up procedure will be initiated. Sometimes you might want to disable certain Internet applications or prevent unwanted dialing by filtering out some port numbers. The Port Filters allow you to select which types of frames will be forwarded:



Port Filter Configuration

Port Description	Accept	Reject
FTP	●	○
Telnet	●	○
SMTP	●	○
DNS	●	○
NEWS	●	○
TFTP	●	○
WWW	●	○
POP3	●	○
SNMP	●	○
NETBIOS	○	●
Other Ports	●	○

For entries set to **Accept**, TCP and UDP frames sent to the listed ports (at an external IP address) will cause a dial-up connection to be established and will be forwarded to the network.

For entries set to **Reject**, frames sent to that port type will be ignored.

Note: *You should normally set NetBios to* **Reject**. *Windows programs often issue NetBios server requests which may cause spurious dial-up connections to be made.*

Note that DNS will normally need to be enabled in order for network names to be used. This means that even if WWW is disabled, a user trying to browse a site will cause a dial event due to a DNS access by their browser, even though they will not subsequently be able to access the site.

There would be no point in setting all entries to Reject as this would effectively disable the Internet connection. However, if you only want to enable a few entries, click **Reject All** and then enable those that are required.

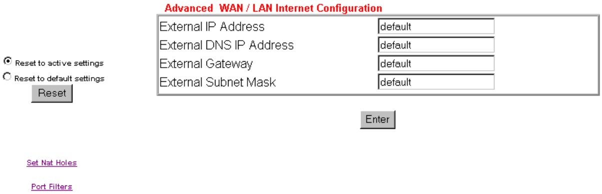
Note that some applications use dynamic port assignment using arbitrary port numbers. In particular, FTP transfers define a port number for the transfer. In the case of using FTP, you need to enable the **Other Ports** selection to allow files to be transferred.

Advanced Internet Access setup (LAN or Wireless)

If you intend to use the Nokia A032 only with a dial-up modem you can skip this section.

In most cases the NAT firewall will be used in conjunction with the serial port and modem for Internet access. In certain applications it may be convenient to connect the Ethernet LAN port or the wireless interface to the external side of the NAT firewall. A description of such applications is beyond the scope of this section, but there is a brief description in *LAN and radio port options* on page 199.

If you set the NAT function to **LAN** or **AIR** in the Advanced Access Point setup screen (see page 40), the Internet Access Setup screen (both basic and advanced) will show a different set of parameters:



Advanced WAN / LAN Internet Configuration

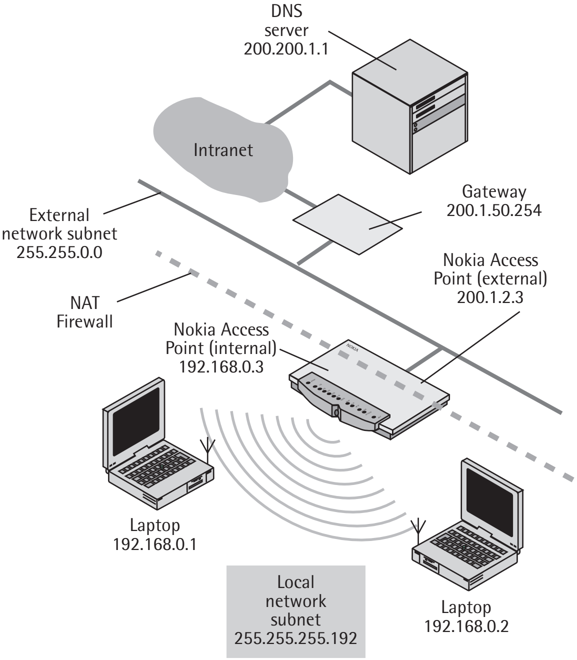
External IP Address	default
External DNS IP Address	default
External Gateway	default
External Subnet Mask	default

● Reset to active settings
○ Reset to default settings

For correct operation of the unit when connected to an external LAN or wireless LAN, all four of the parameters must be correctly specified.

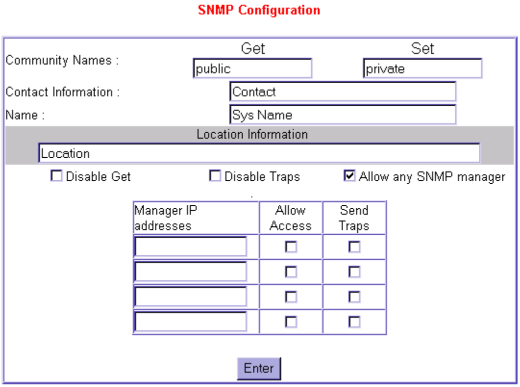
Field	Description
External IP Address	Although there may be many IP addresses on the local network, the A032 can only have one IP address on the external side of the firewall. When PPP is used this address may be dynamically configured. However when LAN or AIR ports are assigned to NAT the external IP address must be manually configured using this parameter
External DNS IP address	This parameter defines the IP address of the DNS server on the external network. DNS requests on the local network will be sent to the A032. The A032 will then convert the destination address to the correct external address as defined in this field before forwarding
External Gateway, External Subnet Mask	These parameters must be defined for the external network to enable the A032 to successfully interface to the external network.

The following diagram shows an example network:



SNMP setup

This screen allows you to set up the A032 for use with Simple Networking Management Protocol (SNMP):



SNMP Configuration

	Get	Set
Community Names :	public	private

Contact Information : Contact

Name : Sys Name

Location Information

Location

□ Disable Get   □ Disable Traps   ☑ Allow any SNMP manager

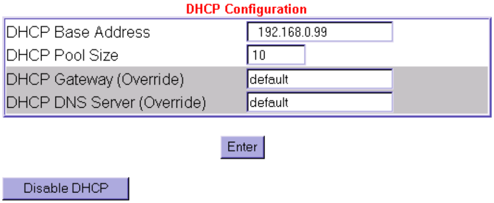
Manager IP addresses	Allow Access	Send Traps
	□	□
	□	□
	□	□
	□	□

Some of the parameters on this screen are also used to control access to the Telnet, Web and TFTP management interfaces. Please see *Setting specific managers* on page 46. This section deals with the SNMP-specific settings:

Field	Description
Community Names	This must match the string in your SNMP utility. • **Get** – Check to allow users in your community to get SNMP information (maximum 16 characters). • **Set** – Not supported.
Contact Information **Name** **Location Information**	These fields are inserted into the MIB II system information. Maximum name lengths are 32 characters (Contact Information and Name), 64 characters (Location).
Disable Get	Globally disables the Get function.
Disable Traps	Globally disables the ability to generate traps (system events) generated by the A032.
Allow any SNMP manager	When checked, allows any workstation to get SNMP information. When unchecked, restricts Gets to specific **Manager IP addresses** in the table at the bottom of the SNMP page (see also page 46)

Advanced DHCP setup

The DHCP server function is useful for auto-configuration of wired and wireless clients. The default server settings enable the Internet access features of the unit.



DHCP Configuration

DHCP Base Address	192.168.0.99
DHCP Pool Size	10
DHCP Gateway (Override)	default
DHCP DNS Server (Override)	default

In order to be enabled, the DHCP server requires that a pool of IP addresses be defined. The minimum pool size is one address and the maximum 64. However, it is recommended that no fewer than 8 addresses be assigned to the pool for normal operation.

Field	Description
DHCP Base Address	This field defines the starting IP address of the pool. It is important that the IP address chosen is a valid address for the local IP subnet and on the same IP subnet as the A032's own IP address.
DHCP Pool Size	This field defines the number of addresses in the pool. To disable the DHCP function enter **0** in this field (or click **Disable DHCP**).
DHCP Gateway, **DHCP DNS Server**	These fields may be left as default for most applications. The default setting causes the DHCP server to instruct the clients to use the A032 as their gateway and (proxy) DNS server. This is required for normal Internet access through the A032. If you have another gateway or DNS server and are not using the Internet Access function of the A032, you can override the default values by inserting the appropriate IP address in these fields. These fields should be filled in with the gateway address and DNS Server address as appropriate for the local subnet.

2. Command line interface

The command line manager (CLM) gives you complete control over the Nokia A032 via a text-based interface.

This chapter

- explains how to access the CLM
- explains how to configure the Nokia A032 using the `set` command
- lists *all* the commands available from the CLM.

Accessing the command line manager (CLM)

Throughout this chapter, the command line manager is referred to as the CLM for brevity.

The Web browser-based interface described in the previous chapter is the normal method by which you customize your Nokia A032. However, there are times when the methods described in this chapter are more appropriate. In particular, the CLM is the only method supported via the serial port.

Your Nokia A032 has a command line interface, which you can access in one of two ways:

Important!! *You need a null-modem cable if you want to communicate via the serial port.*

- Using a PC terminal attached to the serial port via a *null-modem* cable
- Using a Telnet session on a wired or wireless LAN attached station.

Using the serial port

Important!! *You need a null-modem cable for this operation.*

To use the serial port connection, attach a terminal (usually a PC workstation) with the settings **`9600,8,N`** (9600 Baud, 8 bits, no parity) via a suitable cable to the serial port connector on the Nokia A032.

If you are using another PC with a terminal emulation program you'll need to use a *null modem*. The Nokia A032 requires a DB9 female connector. Cables designed for PC-PC data transfer using the serial port generally have the null modem function built in and are suitable.

Once connected physically, you can use a terminal emulator such as Hyperterminal.

Using a Telnet session

In order to use Telnet, the Nokia A032 needs to have an IP address configured.

You can use any LAN station to access the CLM on the Nokia A032. To use Telnet on a Windows 95/98 machine:

1. On the workstation, choose **Run** from the **Start** menu.
2. Type **`Telnet`**.

   If this fails for any reason, use the Find Files utility to search for `Telnet`. This should find a program called `Telnet.exe`, on which you should double-click. It's a good idea to create a shortcut to the Telnet program for future use.
3. In the Telnet window, choose **Remote system** from the **Connect** menu.
4. Enter the IP address of the Nokia A032 and press Enter.

   At this point, the Nokia banner should appear, followed by a logon prompt.

5 At the `Password:` prompt, enter your password. The factory default password is `default`. It's best to change this as soon as possible – see *Management functions* on page 79.

You'll now see the following prompt in the Telnet window:

```
CMD:
```

You're now ready to enter commands.

Setting the time and date

You can use the commands `time` and `date` to update the Nokia A032.

To set the time, enter the following:

`time` ***`hh:mm:ss`***

where:

hh = hours (0 – 23)
mm = minutes (0 – 59)
ss = seconds (0 – 59)

To set the date, enter the following:

`date` ***`mm/dd/yyyy`***

(or ***`dd/mm/yyyy`*** in Europe)

where:

mm = month (1 - 12)
dd = date (1 - 31)
yyyy = year

The effect of the commands is immediate and the clock is updated with the new values. The clock will continue to keep time regardless of whether the unit is powered on or off.

Using the CLM ‘set’ command

There are many commands available from the CLM. This section discusses the `set` command and its associated parameters, which you can use to configure the `Nokia A032`. For a complete list of available commands, see *CLM commands* on page 90.

The procedure for entering commands to configure the Nokia A032 is the same, whether you’re using a Telnet session or a terminal emulator via the serial port.

The basic command syntax is:

```
set parameter value
```

The format of `value` depends on the parameter you’re setting. Some values are simple numbers, some are strings and some are special values such as IP addresses.

For a full list of parameters and their associated values, see *Optional parameter summary* on page 71 and *Default value ‘set’ parameter descriptions* on page 74.

To see a list of all available set parameters, enter the following:

`set help`
or
`set ?`

Optional parameter summary

The following table gives a complete list of the parameters available when using the `set` command. After the table an explanation of each parameter is given. In most cases you'll need to restart the unit in order for the change to take effect (the CLM will prompt you to do this when necessary).

If you are changing the parameters remotely you can initiate a restart using the CLM `restart` command.

Parameter	Function
Radio-related	
channel	Sets radio frequency channel
domain	Regulatory domain
rts_threshold	IEEE802.11 parameter
short_retry	IEEE802.11 parameter
long_retry	IEEE802.11 parameter
sifs_time	IEEE802.11 parameter
frag_threshold	IEEE802.11 parameter
basic_rate	Sets the 802.11 basic rate set
Access Point functions	
net_name	Logical name of wireless network
ap_name	Identifier name for access point
protocols	Selects protocol filtering
TCP/IP parameters	
ip_address	Sets IP address of Nokia A032
subnet_mask	Sets Subnet Mask for local network
gateway	Sets Default Route when TCP/IP filtering

Parameter	Function
Management functions	
password	Sets password of Command Line Manager
telnet	Sets Telnet port
web	Sets WWW port
admission	Controls wireless LAN access via NID names
manager	Specifies access to management functions
manager_ip	Defines IP addresses of specific managers
lock	Higher security password lock function
lan	Controls the LAN port on the A032 hardware
WEP security functions	
wep_mode	Specifies access policy
wep_key_range	Specifies encryption level
wep_key	Assigns a value to one of the four shared WEP keys
wep_key_active	Specifies which of the four shared WEP keys is active
radius_server	IP addresses of primary and backup key servers
shared_secret	Specifies authentication key (shared secret) between access point and external key server, and key encryption password (RADIUS password) held on external server
use_encrypted_nid	Affects the format of the nids.txt file used to load specific keys.
DHCP functions	
dhcp_base	Sets start address of DHCP address pool
dhcp_pool	Sets size of DHCP address pool
dhcp_gateway	Sets alternate gateway for client notification
dhcp_dns	Sets alternate DNS server for client notification

Parameter	Function
Internet service provider information	
isp_num	Phone number of ISP
isp_user	Login Username for ISP account
isp_pwd	Login Password for ISP account
isp_dns1	Fixed value of ISP DNS server
isp_dns2	Fixed value of ISP DNS server
isp_ip_address	Fixed value of external (ISP) IP address.
Modem setup	
mdm_speed	Data rate between A032 and modem
mdm_init	AT command initialization string sent to modem
mdm_holdtime	Minutes of inactivity to go on hook
NAT setup	
nat_port	Determines on which interface NAT is active
nat_subnet	Subnet mask of external LAN
nat_gateway	Gateway address of external LAN
SNMP setup	
community_get	Determines which SNMP users can access information.
community_set	Not supported

Default value ‘set’ parameter descriptions

Many parameters are optional and may be left with the default value. The default value of each parameter is shown below.

To set a parameter back to its default value use the set command but leave the parameter field blank. For example:

```
set ip_address
```

Radio-related

Parameter	Description	Default
channel	Specifies the operating channel for the Nokia A032.	**10**
domain	Sets the operating area and enables valid channels.	depends on where unit was purchased
rts_threshold	Determines whether RTS/CTS frames should be sent on the wireless link and what size frames they should be used for. Frames larger than the parameter value will be preceded by an RTS/CTS exchange.	**2301**
short_retry	Specifies the number of retries the radio will use during an RTS/CTS attempt before aborting.	**15**
long_retry	Specifies the number of retries the radio will use during a data transmission attempt before aborting.	**15**
sifs_time	SIFS is an IEEE802.11 parameter which affects turnaround time. The value is specified in IEEE802.1 and the normal setting for this parameter is 0. A value of 0 is treated as default and causes the system to use the IEEE802.11 compatible value. In some special applications where IEEE802.11 is not required an alternate value may be specified. It is **highly recommended** that the default value be used unless you have expert advice.	**0**
frag_threshold	frag_threshold is an IEEE802.11 parameter which determines the maximum size of frames sent by the radio. Frames larger than frag_threshold are sent in several pieces. Lowering the value of frag_threshold can improve throughput for poor radio conditions, but reduces throughput for good radio conditions.	**2346**

Parameter	Description	Default
basic_rate	Used to set the 802.11 basic rate set (the set of data transfer rates that all the stations in a BSS will be capable of using to receive frames from the wireless medium). In practical terms, multicasts and requests are restricted to use of the basic rate. The basic rates are set in kHz. Valid values include 5500 and 11000	**1000** **2000**

Access point functions

Parameter	Description	Default
net_name	String up to 32 characters specifying the network name for the wireless LAN in Infrastructure mode. Names which contain non-alphanumeric characters or spaces must be enclosed in double quotes (for example, `“Nokia WLAN”`).	**`Nokia WLAN`**
ap_name	String up to 15 characters used to give the Nokia A032 a name. Useful if you have multiple access points on a network for roaming (assign the same `network-name` but a different `ap_name` to each access point). This name is displayed in some of the management commands.	**`LocalAP`**
protocols	The default mode of the A032 is to pass all protocols. Some non-TCP/IP protocols issue frequent broadcasts or multicast messages. These can use up the available data bandwidth on the wireless LAN and slow down response time. If your wireless stations only use TCP/IP you can set the value of `protocols` to `TCPIP`. In this case non-TCP/IP messages are not passed by the access point. Note that if your network uses BootP or RARP messages you should select `all` for the protocol value.	**`all`**

TCP/IP parameters

Parameter	Description	Default
IP_address	Used to assign a TCP/IP address to the Nokia A032.	No IP address assigned
subnet_mask	Used to define the TCP/IP subnet mask. This field should be set if you plan to use the built in management features.	**255.0.0.0**
gateway	Only used if you have `protocols` set to `TCPIP` rather than the default `all`. In this case `gateway` should be the IP address of the gateway router. This may also be known as the *default IP route*. If you do not have a local gateway this field is not required.	**0.0.0.0** (no gateway)

Management functions

Parameter	Description	Default
password	Sets the password access to the CLM and the web interface. The password is an alphanumeric string up to 16 characters long.	**`default`**
telnet	`on` enables built-in Telnet management function `off` disables Telnet management function *`port`* sets the number for the Telnet server port (e.g. **`set telnet 23`**). Setting `off` will not affect a terminal attached via the serial port (which is always enabled when a terminal is attached).	**`23`**
web	`on` enables built-in Web management function `off` disables Web management function *`port`* sets the number for the web server port (e.g. **`set web 80`**). To access the web server on a different port (for example 6000) enter the URL on your browser as **`http://`*`xxx.xxx.xxx.xxx`*`:6000`** using the IP address appropriate for your access point.	**`80`**
admission	Determines which wireless stations can communicate with the access point. Possible values are: `all` any station can communicate with the access point `named` only those stations that have a NID name entry are accepted (see *NID naming and security* on page 97); all others are blocked `none` all stations are blocked; use this to temporarily disable the access point while allowing access from the LAN for management reasons	**`all`**

Parameter	Description	Default
manager	Used to control access to web, Telnet and TFTP management functions. Possible values are: `none` disables the management functions `any` allows any station to use management functions `specific` allows access by specific stations only (see *manager_ip* below).	**`any`**
manager_ip	Specifies up to four stations allowed to use management functions (if `set manager specific` applies). The format of the command is: **`set manager_ip`** ***`number ip_address y z`*** where: *`number`* 1, 2, 3 or 4 (to set 1st, 2nd, 3rd or 4th manager) *`ip_address`* IP address of nth manager's station *`y`* 1 = accept management requests 0 = requests not allowed. *`z`* 1 = send traps 0 = traps not sent. For example: **`set manager_ip 2 192.168.0.1`** sets the second of four managers as having IP address 192.168.0.1. **`set manager_ip 2`** clears the second entry in the management table. There is no default value.	

Parameter	Description	Default
lock	**Warning**: Use this option with caution (see page 46). The unit has the option to be password *locked* by issuing the command `set lock on`. Locking the unit has the following results: • The password can not be changed, even in the configuration screen. • The *reset unit to default* feature is disabled so that the unit cannot be reconfigured even with physical access • The *backdoor* password is disabled – Nokia Technical support can normally recover a unit when the password has been forgotten using a backdoor password. • TFTP functions are disabled.	**`off`**
lan	Controls the LAN port on the A032 hardware. The format of the command is: **`set lan`** Valid values are: `10baseT` (default) `off` (disables the LAN interface altogether)	**`10baseT`**

WEP security functions

Parameter	Description	Default
wep_mode	Specifies access policy. Optionally specifies key databases for personal WEP keys. Format is: `set wep_mode` ***`mode database`*** where ***`mode`*** can take the following values: `open` Allows same stations as `WEP`, plus non-WEP stations via open authentication (no key) `wep` Allows same stations as `personal`, plus those with valid shared WEP key. `personal` Only allows authentication via personal WEP key. It is advisable to set one active shared WEP key, used when access point sends broadcasts/multicast messages. All wireless clients must have same shared WEP key (plus personal WEP key) to receive broadcasts. If no shared WEP keys defined, broadcasts sent unencrypted. `wifi` Special mode used with some non-Nokia WiFi compatible systems. Station may use open authentication to associate with the access point then switch to shared WEP key. Personal WEP keys not supported. Mode provided for compatibility with other vendor equipment; not generally recommended. and ***`database`*** can take the following values: `local` Flash-based database in A032 used `radius` External key database used `either` Local database used; if not found in local database, ext. database used. For example: **`set wep_mode personal radius`** only wireless clients with personal WEP keys held in external database are recognized.	**`wep`** (but forced to **`open`** in Learn mode)

Parameter	Description	Default
wep_key_range	Sets WEP key policy (see *Setting WEP key policy* on page 138). Command takes the form: `set wep_key_range` *`min max`* where min and max show the encryption strengths, and can take the following values: `40` enter keys ten octets 56 enter keys as 14 octets 64 enter keys as 16 octets 96 enter keys as 24 octets `128` enter keys as 32 octets For example: **`set wep_key_range 56 96`** means the Access Point will accept 56, 64 or 96-bit keys (custom mode). You can also use the following versions of the command: **`set wep_key_range normal`** which means the Access Point will **only** accept 40-bit keys **`set wep_key_range high`** which means the Access Point will **only** accept 128-bit keys (strong mode).	**`40`**
wep_key	Assigns a key value to one of the four shared WEP keys. The command takes the form: `set wep_key` *`n key`* where ***n*** selects which shared WEP key (1, 2, 3 or 4) is being entered, and *`key`* assigns it a value. *`key`* must follow the WEP key policy set by the `wep_key_range` command (see above). Examples: **`set wep_key 2 ae325e092c`** assigns the value ae325e092c to shared WEP key number 2. **`set wep_key 3 n`** assigns a null value, deactivating shared WEP key number 3.	

Parameter	Description	Default
wep_key_active	Specifies which of the four shared WEP keys is active. For example: **`set wep_key_active 3`** means shared WEP key 3 is active.	
radius_server	IP address of primary and backup key servers (you must previously have used `set wep_mode` to specify that a RADIUS server is being used).	
shared_secret	Command takes the form: `set shared_secret` *`secret passwd`* *secret* is text string of up to 16 characters, used as a lightweight authentication check between the access point and the external server. See *Setting up a RADIUS external key database* on page 141. *psswd* is the radius password, an alphanumeric string of up to 16 characters specifying the dummy password, also stored in the RADIUS server (see page 144). Each key entry in the server is given the same dummy password.	
use_encrypted_nid	Affects the format of the nids.txt file used to load specific keys (nids.txt is generated by WEPGen – see page 163). When set to **`true`**, the file must be in encrypted form. When **`false`**, the file must be in normal text mode (keys are still encrypted in the file).	**`false`**

Please see *Data encryption and security* on page 127 for more information on WEP security.

DHCP functions

Parameter	Description	Default
dhcp_base	Defines the start of the pool of IP addresses available for assignment by the internal DHCP server.	**192.168.5.100**
dhcp_pool	Defines the size of the pool of IP addresses available for assignment by DHCP. For example if this has a value of 16, then 16 addresses will be available starting with the address defined in dhcp_base. A value of zero for this parameter disables the internal DHCP server.	**0** (DHCP disabled)
dhcp_gateway	The IP address of the gateway which is sent to DHCP clients when the IP address is assigned. If the Nokia A032 is used as an Internet access device, the gateway of attached clients must be set to the IP address of the Nokia A032. The default value of dhcp_gateway provides the IP address of the A032. If the DHCP server is used in conjunction with an alternate gateway, the IP address of that gateway can be set using this parameter. This will ensure that the clients get the desired configuration information.	IP address of Nokia A032
dhcp_dns	The IP address of the DNS server which is sent to DHCP clients when the IP address is assigned. If the Nokia A032 is used as an Internet access device, the DNS server of attached clients must be set to the IP address of the Nokia A032. The default value of dhcp_dns provides the IP address of the A032. If the DHCP server is used in conjunction with an alternate gateway, the IP address of that DNS server can be set using this parameter. This will ensure that the clients get the desired configuration information.	IP address of Nokia A032

Internet service provider information

Parameter	Description	Default
isp_num	Your ISP's phone number for a dial-up Internet connection.	(empty)
isp_user	Your ISP user name used in dial-up networking under Windows.	(empty)
isp_pwd	Your ISP password used in dial-up networking under Windows.	(empty)
isp_dns1, **isp_dns2,** **isp_ip_address**	Some older ISPs may require that this information be programmed into the Nokia A032 manually. Use `isp_ip_address` if your ISP has allocated you a *static IP address.*	(empty)

Modem setup

Parameter	Description	Default
mdm_speed	Specifies the data rate used to communicate between the Nokia A032 and a modem. Note that this is not necessarily the rate that the modem will support when it communicates to the ISP. Generally the modem will not connect at a speed higher than this rate but it may connect at a speed which is lower. Valid values: 9600, 19200, 38400, 57600, 115200.	**57600** (bps)
mdm_init	Use this to specify any special AT commands necessary to set your modem in the correct mode (only older modems require this – most modems work in their default mode with the Nokia A032.) See the modem's manual or contact Nokia Technical support.	(empty)
mdm_holdtime	Sets the number of minutes for which the link needs to be inactive before the connection is broken and the modem disconnected. A value of zero indicates that the modem will remain connected indefinitely.	**3** (minutes)

NAT setup

Parameter	Description	Default

nat_port	Determines on which interface NAT is active. Can be one of the following:
	`off`
	`modem`
	`LAN`
	`radio`
		`off`

nat_subnet	Subnet mask of external LAN (see page 199).	**`0.0.0.0`**
nat_gateway	Gateway address of external LAN (see page 199).	**`0.0.0.0`**

SNMP setup

Parameter	Description	Default
community_get	Allows users in your community to get SNMP information.	**`public`**
community_set	Not supported	

CLM commands

This section gives a complete listing of the CLM commands available on the Nokia A032. For an explanation of how to access the CLM, see page 67.

The basic command syntax is:

```
command parameter1 value
```

The format of *value* depends on the parameter you're changing. Some values are simple numbers, some are strings and some are special values such as IP addresses.

The command and parameters are separated by spaces.

- You can correct typing errors using the backspace key.
- You can terminate commands and return to the command prompt by pressing **Ctrl-C**.
- You can repeat the previous command by pressing the space bar at the command prompt.

Help on commands

- To see a summary of commands, type:

  `help` (or **`?`**)

- To get help on a specific command, type:

  `help` ***`command`*** (or **`?`** ***`command`***)

  For example:

  `help ping`

- To see a list of parameters for the `set` command, type:

  `set help` (or **`set ?`**)

Command summary

Command	Description
arp	ARP stands for *Address Resolution Protocol.* This is an IP protocol used to bind an IP address to Ethernet/802.3 addresses. ARP uses broadcast messages to determine the MAC address corresponding to a particular internetwork address. Ethernet or 802 LANs use ARP to dynamically discover media addresses and IP addresses. The `arp` command yields a table showing the MAC addresses, associated IP addresses and age of each entry that the Nokia A032 has detected. Since the associations are dynamically discovered, all ARP tables have an aging process, which removes entries from the table after a period of inactivity.
arp nat	This produces an arp table for machines outside the firewall (only if using NAT LAN or NAT Air).
bridge	The bridge command is fully described in *Appendix B – Wireless bridges and repeaters*.
broadcast	Puts the Nokia A032 into a special test mode. The format is: `broadcast` *`IP_address`* This causes the Nokia A032 to generate a continuous stream of UDP packets to the specified IP address (this could be a wireless station, a computer on your wired LAN, or even on the Internet). To terminate the broadcast, type **Ctrl-C**. This is useful for site survey work – you can broadcast to a wireless station, moving it around to test your network coverage. **Important**: This command effectively disables all other wireless stations, as the broadcast data occupies all available wireless bandwidth. **Note**: Issuing a `broadcast` command with no IP address parameter sends packets to all wireless stations.
config	Displays current system configuration settings.
config+	This works like the config command but shows the settings that will take effect on the next restart.
date	Sets the current. date: `date` *`mm/dd/yyyy`* or *`dd/mm/yyyy`*

Command	Description
dhcp	Displays current DHCP settings: • Address range – the current range of addresses available • Number in range – the number of addresses available within that range
dhcp+	This provides the same information as the dhcp command, but shows the settings as they will be after the next restart.
disable LAN	Disables the wired LAN interface. Once disabled, you can only reenable the interface by restarting the Nokia A032.
disable radio	Disables the radio interface. Once disabled, you can only reenable the interface by restarting the Nokia A032.
exit	Performs a logout from the command line (and is functionally identical to the logout command). For a telnet connection, it also disconnects the telnet session. On the serial port, it returns to a login prompt.
log dump	Displays the contents of the initialization log on the screen (you'll find more on this in *Appendix F*).
log clear	Clears out the log information.
logout	Exits the CLM. Re-enter the password to use CLM.
isp dial	Forces the modem to dial up to the ISP.
isp hangup	Forces the modem to hang up.
nat	Displays current NAT settings: • NAT port • External IP Address • External DNS Address (1 & 2) • NAT holes (IP addresses for external access – see page 201)
nat+	This works like the nat command but shows the settings that will take effect on the next restart.
ppp	Displays current settings and statistics for PPP. The information displayed here is similar to that generated in the PPP Statistics web screen (see page 16).
nid	The `nid` command is fully described in *NID naming and security* on page 97.

Command	Description
ping	Causes the Nokia A032 to issue an ICMP Echo request (PING) to a specified IP address. The format of the command is: `ping` *`xxx.xxx.xxx.xxx yy`* where *xx.xx.xx.xx* is the destination IP address *yy* is an optional parameter which causes the command to enter a loop and ping the address every *yy* seconds. If yy is specified the command will repeat indefinitely; type **Ctrl-C** to terminate the command and return to the `CMD:` prompt.
restart	Causes the Nokia A032 to re-initialize. This is equivalent to turning the power off and on again. Normally this command is issued after configuration changes. Restarting the unit can be disruptive to currently connected users.
set	See page 70.

Command	Description
show	Displays information similar to the Stations screen of the web interface. The command lists information about stations which the Nokia A032 has seen or associated with. In the case of wireless stations the command displays status information about the stations. `show G` Lists all known stations attached via the wired LAN port. `show S` Lists all known associated wireless stations. `show A` Shows all wireless stations of which the Access Point is aware. There are several means by which the access point may discover other wireless stations including the Nokia Inter Access Point Protocol. The result of the command is a list providing the following information (fields depend on station type selected) **Net ID** MAC address of the station **State** Current relationship of device with Nokia A032: Associated, Disconnected, Detected, is bridging, bridged, Local AP, Unknown. **Channel** Radio channel. **Power** The power measurement of the access point with which the unit is associated **IP Address** IP address of the device (if known)
stats lan **stats air** **stats ppp**	Displays traffic statistics for the last 10-second interval (cumulative since last cleared or system reset). Clear stats using the command **`stats clear`**.
time	Sets the current. time: `time` *`hh:mm:ss`*

Command	Description
trace	Displays the contents of the trace buffer, which stores the last 128 *events* (e.g. new associations, or the detection of an aging-out of network addresses). This command does *not* clear the trace buffer.
traceclr	Clears entries which have been read by the trace command. This does not clear entries which have not yet been displayed – that is, if new events occur between the last trace command and the traceclr command, the new events are not lost.
tracelp	Causes the display to enter a loop. At a regular interval the access point does the equivalent of a `trace` command followed by a `traceclr` command. To exit this mode, press **Ctrl-C**. The `tracelp` command has one optional parameter to control the refresh speed as follows: `tracelp` Updates the screen every 5 seconds. `tracelp Q` Updates display every second (Quick). `tracelp S` Updates display every minute (Slow).
traceon	Activates tracing for certain events (see traceoff).

traceoff	Deactivates tracing for certain events. The command is in the form:
	`traceoff <specifier> <specifier>`
	where <specifier> is one of the following strings:
	`br+` trace new MAC addresses which are detected
	`br-` trace MAC addresses which are dropped due to inactivity
	`IP+` trace new TCP/IP addresses
	`sys` trace authenticate, associate, and other system events
	`all` turn off (or on) tracing of all events
	The default (starting) state is:
	`traceoff br+ br- IP+`
	`traceon sys`

ver	Displays product name, along with version and copyright information for the A032 software.

3. NID naming and security

This chapter explains how to use NID names to:

- identify and keep track of Nokia A032 users
- control access to a Nokia A032 network.

NID names provide level 1 security features (see *Authentication and encryption* on page 128).

Overview

MAC addresses

Each station on a network, whether it be wireless or wired, has a unique identifying number called the *MAC address*.

Both Ethernet and IEEE802.11 stations use a 48-bit number, usually expressed as six bytes in hexadecimal notation. An example of a MAC address is:

```
00e003123456
```

The address is associated with the network adapter card and *not* the computer, so that if you move an Ethernet card or wireless LAN card to a new computer, the number will transfer to the new location. No two adapters in the world can legally have the same MAC address.

NID names

Because the MAC address is unique, it can be used to identify a particular user to the system. However, the MAC address by itself is not very informative, so the Nokia A032 allows a system manager to assign a text string, or name, to each MAC address in the network.

The combination of the MAC address and the name string is called a *NID name* (NID stands for Network IDentifier).

How are NID names useful?

Once you have assigned NID names, you'll be able to see active stations listed by these names rather than by MAC address in all the Nokia A032 management screens. See *LAN station status* on page 23 or *show* on page 94.

NID names can also be used as a security measure, as described on page 101.

NID name table

The Nokia A032 can store a list of up to 200 NID names in its flash memory, in the *NID name table*.

Initially, the NID name table is empty. To assign a NID name to a MAC address, you need to update the NID name table. You can do one of the following:

- Use the CLM to add or remove NID name entries one at a time (see page 99)
- Use TFTP to upload and download the whole NID name table (this is useful for altering many entries in one go – see *nids.txt* on page 112.

Note: *nids.txt is also used to store WEP key information if you are using WEP security functions (see Data encryption and security on page 127)*

Using NID names

The basic approach to using NID names is as follows:

1 Ascertain the MAC addresses of the cards to which you want to assign NID names.

2 Assign the NID names, thereby updating the NID name table.

3 If necessary, restrict network access to stations listed in the NID name table.

How to find the MAC address

The MAC address for an adapter card is not normally visible to a user. Also note that the MAC address is not related to the IP address of the network connection. There are two methods you can use to view MAC addresses:

- View the MAC address of a specific station
- View MAC addresses for all currently active stations.

Displaying the current station's MAC address

If you are using Windows NT4 or 2000, open a console window and enter **`IPConfig`**.

If you're using TCP/IP under Windows 95/98 you can use a utility called `WinIPcfg` to view the MAC address of the station at which you're currently working:

1 Open an MS DOS window, or choose **Start, Run**.

2 Enter **`WinIPcfg`**.

3 Select the wireless LAN adapter entry.

If you have a LAN adapter correctly installed on the computer, WinIPcfg will tell you the MAC address for that adapter.

Displaying all active MAC addresses

You can use the CLM (see *nid* on page 92) or Web browser interface (see page 23) to see which stations are currently connected. This display shows the MAC address of each station and its IP address.

Assigning NID names

To assign a NID name using the CLM:

1 Make sure the CLM is running on your station (see page 67).

2 Decide on a NID name for your chosen MAC address.

This can be any alpha-numeric string, up to 16 characters long, but may not include spaces.

Note: *There may be a short delay after entering the command while the flash memory is updated.*

3 Enter the following command:

```
NID add 123456789abc name
```

where *123456789abc* is the MAC address and *name* is the name you're assigning.

If necessary, repeat steps 2 and 3 for any other NID names you're assigning or (if you're entering lots of NID names) use TFTP to fetch your simple nids.txt file, edit it to add as many entries as necessary, then send it again (see *Using the TFTP client program* on page 105).

Removing a NID name

To delete an existing NID name use the command:

```
NID delete 123456789abc
```

where *123456789abc* is the MAC address of the NID name to be deleted.

You cannot delete using the name string - you must use the NID value. This is because only the MAC address is unique.

Alternatively, delete lines from the nids.txt file (send and fetch the file as described in *Using the TFTP client program* on page 105)

Listing NID names

To find out which NID names have been entered, use the command:

```
NID list
```

This displays the NID name table.

Using NID names for security

Management security options on page 45 and *Management functions* on page 79 explain how to set the `admission` parameter to control which stations can access the wireless LAN.

Use the CLM to issue the command:

```
set admission named
```

After that, the Nokia A032 will only accept new connections with wireless stations which have a defined NID name (i.e. those listed in the NID name table). All other wireless stations will be blocked, ensuring that unauthorized users cannot access the network.

You can also use WEP keys for security – see *Data encryption and security* on page 127.

4. Using TFTP

Overview

For the most part, you use the web interface or CLM to update the configuration and display the status of the Nokia A032. However, some information is too big or unwieldy to handle using a terminal style interface.

For example, the NID name table can hold up to 200 entries. It is difficult to manage those entries simply using add, delete and list commands.

To handle this, and provide other useful functions, the Nokia A032 supports a standard method for transferring information across the wired or wireless LAN to or from a station equipped with TCP/IP and a TFTP client program.

What is TFTP?

TFTP stands for *Trivial File Transfer Protocol*. It is a standard TCP/IP utility and performs a similar task to File Transfer Protocol (FTP).

TFTP is implemented using two components: a *TFTP server* and a *TFTP client*. The client makes requests to the server and can send and fetch files of information. If both the server and the client run on conventional computers, the files are typically stored in a directory or folder at each end.

Nokia A032 as a TFTP server

The Nokia A032 acts as a TFTP server. You run a TFTP client on a station to perform the file transfers.

The term *files* applies in the conventional sense to client machines. The A032 has no hard disk, but it still uses file names to identify its stored information.

Installing a TFTP client program

The *Nokia A032 Utilities CD-ROM* provides a TFTP utility program. However, the Nokia A032 will work with any TFTP client program. If you have one installed, you can use that.

If you need to install the Nokia TFTP client, see *Appendix D – Utilities CD-ROM.*

Sending and fetching files

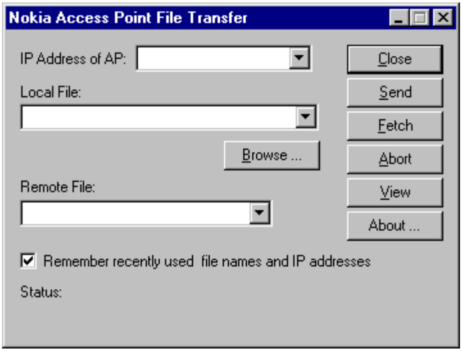
Using the TFTP client program

This section explains how to use the TFTP client supplied on the *Nokia A032 Utilities CD-ROM* (if you need to install the Nokia TFTP client, see *Appendix D*). It gives general information on sending and fetching files. For a description of the files which you can transfer, see *TFTP-accessible data* on page 107.

To use the TFTP program:

1 Choose **Start** > **Programs** > **Nokia A032** > **Nokia TFTP client.**

You'll see the following window:



☑ Remember recently used file names and IP addresses

2 If you want, place a check in the **Remember recently used file names and IP addresses** box. This will save time next time you use TFTP.

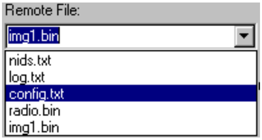
3 Enter the IP address of the Nokia A032 into the **IP Address of AP** field.

You can click **Browse** *to specify a file.*

The drop-down menu lists recently-used files.

4 In the **Local File** field, enter the name of the source file (when sending) or destination file (when fetching) on your local disk or network drive.

5 In the **Remote File** field, choose the name of the A032 'file' you want to send or fetch from the drop-down menu.



A description of these files is given in *TFTP file descriptions* on page 108.

You can click **Abort** *to interrupt a send or fetch.*

6 Click **Send** or **Fetch.**

If the operation is successful you'll see a progress bar.

Possible error messages

You may see one or more of the following error messages during file transfer:

Message	Possible causes
`timed out`	You typed the wrong IP address, you have not connected to the Nokia A032, or the Nokia A032 is configured not to accept TFTP from your station.
`unknown file`	You probably made an invalid entry in the **Remote File** field.
`upload in progress`	Another station is performing an upload at the same time, or the previous upload was not completed successfully. Try again after 30 seconds

TFTP-accessible data

The Nokia A032 TFTP server makes various 'files' available for upload or download.

Overview

This section lists all the files available for upload or download and gives a brief summary of each. The following section describes each file in detail.

File	Send/ Fetch?	Description
log.txt	fetch	This copies the contents of the initialization log file to your client.
config.txt	fetch	This creates a text file on your client with the current configuration settings of your Nokia A032.
	send	This sends a configuration file to the Nokia A032 and updates all the operating parameters. This will usually be a configuration that has been previously downloaded, and may have been edited.
nids.txt	fetch	This creates a file on your client containing the NID table and bridge table entries. Potentially, it also contains the WEP information, which may be encrypted, or in editable text form (see *Data encryption and security* on page 127 and *Using the WEPGen utility* on page 163).
	send	This copies a list of NID and bridge table entries to the Nokia A032. The file will usually be one that has previously been fetched from the Nokia A032 or generated by the WEPGen utility.
img1.bin	send	This writes a new copy of firmware into the Nokia A032 for upgrade purposes.

TFTP file descriptions

This section gives a detailed description of each file available for transfer between a client and the Nokia A032 using TFTP.

log.txt

The Nokia A032 maintains a log file which is updated when the unit is initialized.

This file keeps a record of each initialization. The contents of the log file is explained more fully in *Appendix F*. The uploaded log file is stored in regular text format.

An example of a log file is shown below:

```
 Message :  CLM Request

Initializing version: B4.00.01 on Fri, 12 May 2000 11:27:16
Initialize LAN port...
LAN Port ready, Message :  Web Request

Initializing version: B4.00.01 on Fri, 12 May 2000 11:28:22
Initialize LAN port...
LAN Port ready,
Initializing version: B4.00.01 on Fri, 12 May 2000 11:30:14
Initialize LAN port...
LAN Port ready,
```

config.txt

This file is a text file containing all the Nokia A032's important configuration settings.

Note: *This does not save or restore NID name, Bridge Table or password entries.*

A system manager may want to keep a record of the Nokia A032's configuration settings for future reference, or as a backup before performing any new configuration.

You can use a backup copy of config.txt if you run into problems while configuring or upgrading the Nokia A032.

An example of a config.txt file is shown below:

```
/Config.txt for AP(ourap) on Fri, 12 May 2000 11:32:49
%channel: 7
%net_name: "NokiaWLAN"
/*%rts_threshold: 02301
/*%frag_threshold: 02346
/*%short_retry: 00015
/*%long_retry: 00015
/*%gateway: 0.0.0.0
%subnet_mask: 255.255.0.0
%ip_address: 192.168.100.100
%ap_name: "ourap"
/*%LAN_if: "10baseT
%domain: ETSI
/*%sifs_time: 000
/*%telnet:00023
/*%web:00080
%wep_mode: any radius
/*%protocols:all
%admission:all
%manager: any 0 0 1
%basic_rate: 1000 2000
%wep_key_range: 40 128
%dhcp_pool: 6
%dhcp_base:192.168.100.100
%isp_num:0800123456
%isp_user:"ispuser"
%mdm_speed:57600
%mdm_holdtime: 00003
%nat_port: serial
%community_get:public
%community_set:private

/*default setting
```

Modifying the config.txt file

Note that some entries are commented out (lines starting with '`/*`'). This denotes entries that are set to a default value. You can delete these lines without affecting the result when the file is downloaded to the Nokia A032.

If you want to modify a parameter, delete the comment characters and amend the parameter accordingly.

For example, to change the radio channel:

1. Use a text editor to open `config.txt`.
2. Modify the file as follows:

   Old line: `/*%channel: 10`
   Modified line: `%channel: 11`
3. Save `config.txt`.
4. Send the file to the Nokia A032 using the TFTP client.

When you send `config.txt`, the following action is taken by the Nokia A032:

1. The new configuration file is read in and checked for format. If there are any format errors the configuration is not updated
2. If the send is good, all the parameters (except password) are reset to their default value.
3. New settings from the config.txt file are loaded into the Nokia A032.
4. The Nokia A032 performs a restart with the new settings.

nids.txt

If you have only a few wireless stations it is easy to enter and manage the NID names using the CLM (see *Appendix 3*). However, if you have many users it is more convenient to do so via TFTP.

Using TFTP you can:

1. Fetch the current `nids.txt` as a text file to use for backup purposes.
2. Edit the file to add, delete or modify users.
3. Send a modified `nids.txt` file to the Nokia A032.

When you retrieve `nids.txt` from the Nokia A032 it will be stored in a disk file with one line for each NID Table or Bridge Table entry (for more on bridges, see *Appendix B – Wireless bridges and repeaters*).

An example of a NID file is shown below:

```
/ NID/Bridge list for AP(LocalAP) on Fri, 23 Apr 1999
15:17:41
49f7eb38d93682ac9ab3472e5b6e8ff3
0102f03404e1 User1 0B123272F2,N
0020f0123456 User2 02468EF246,N
002003456789 bridgeX 01234987A6B,B
```

The file contains the following information:

- The first line shows the date on which the upload was performed. The access point name is shown in parentheses “()”
- The second line is a security field which should not be changed

- Each NID Table entry has the following format:

  ```
  MAC_address Username
  Personal_WEP_key,N
  ```

  where

  - *`MAC_address`* is the MAC address of a station
  - *`Username`* is a user-friendly name for the station
  - *`Personal_WEP_key`* is the station's key when using WEP encryption (see *Personal WEP keys* on page 133
  - `,N` – this field is used by the tools and should not be changed. Note: the first letter indicates whether the entry is a station (N) or bridge (B) device.

img1.bin

`img1.bin` is the name of the ‘file’ on the A032 where the firmware for the Nokia A032 and the Nokia C111 Wireless LAN Card is stored.

From time to time during the warrantee period, Nokia may make new versions of firmware available. New releases might have additional features or might fix anomalies that have been reported in the operation of the unit. In such cases Nokia will provide a binary file as denoted by the extension `.bin` (e.g. `a032.bin`), along with upgrade instructions.

For example, to upgrade the A032 firmware:

1. Using the TFTP client, select `a032.bin` as the **Local File**, and `img1.bin` as the **Remote File.**
2. Click **Send.**

A note on security

You should be aware that the TFTP ‘files’ on the A032 contain important configuration. Overwriting them may cause your Nokia A032 to behave unexpectedly, or cease to function.

Note: *It is not possible to overwrite the management password by TFTP – the original password will be maintained.*

TFTP can be used to update the configuration without knowledge of the management password. This could allow unauthorized users to update the unit.

There are two ways to disable TFTP access:

- Set a specific manager’s IP address (see page 46) to prevent unauthorized TFTP transfers. See *Management functions* on page 79.
- Set the security `lock` parameter **on**. See page 79.
  When the security lock is on, the config.txt upload feature is disabled.

5. SNMP manager

The Nokia A032 has a built-in SNMP Agent capability which allows integration into SNMP managed enterprise environments. The Agent supports SNMP V1.0 requests and provides data from the following MIBs (supplied as files when you install from the *Nokia A032 Utilities CD-ROM*, as explained in *Appendix D*):

Data	Supplied in file
RFC1213 (MIBII)	`RFC1213.mib` `IANAifType.mib`
IEEE802.11 MIB	`IEEE80211.mib`
ETHERLIKE MIB (partial)	`ETHERLIKE.mib`
Nokia A032 Proprietary MIB	`Nokia-A032-MIBv1.mib`

The source text for these MIBs is provided on the Utilities CD-ROM supplied with your Access Point. The MIBs are provided in ASCII text format for easy incorporation into SNMP Manager Products.

The Nokia A032 supports Get, Get Next and Trap operations but does not support Set operations

Items which are listed as Read/Write in the MIB will cause an error response if a Set command is issued.

MIB Summary – RFC1213 – MIB II (1.3.6.1.2...)

The Version of RFC1213 supplied has been modified to recognize the IEEE802.11 interface type The following is a summary of the sections of MIBII indicating which parts of the MIB are supported:

System	All fields supported (Read only). The Contact, Name and Location values can be set using the Web manager function (see page 63).
Interfaces	All fields supported. There are two entries in the Interface table. Interface 1 is the Ethernet Interface and Interface 2 is the IEEE802.11 Interface.
AT	Not Supported.
Internet Protocol	All fields supported (Static information).
ICMP	Supported as appropriate.
TCP	TCP connections are shown in an eight-row table. All fields are supported in each table row. However, the table size is fixed. If there are more than 8 TCP active connections to the Access Point, only the first eight will be shown.
UDP	Supported for UDP listeners TFTP and SNMP.
EGP	Not supported.
Transmission	DOT3 Stats Table supported (partial).
SNMP	All fields supported.

IEEE802.11 MIB (1.2.840.10036...)

The IEEE802.11 Standard MIB is defined as an SNMP V2.0 MIB. The MIB supplied on the *Nokia A032 Utilities CD-ROM* has been converted to an SNMP V1.0 format for easy integration into a wide range of managers. Many of the entries in the MIB are not relevant to the Access Point because they refer to some capability (such as frequency hopping) which is not supported. The following groups are supported:

Dot11SMT	Station Configuration Table	All entries supported (Read only)
Dot11SMT	Authentication Algorithms Table	All entries are static
Dot11SMT	WEP Default Keys	Not supported
Dot11SMT	WEP Key Mapping Table	Not supported
Dot11SMT	Privacy Table	Supported
Dot11SMT	SMT notification	Not supported
Dot11MAC	Operation Table	Fully supported (Read only)
Dot11MAC	Counters Table	Fully Supported
Dot11MAC	Group Addresses Table	Not Supported
Dot11RES	Static entry	
Dot11PHY		Fully supported for Direct Sequence

Nokia A032 proprietary MIB

The following information is provided as part of the Nokia A032 MIB.

A032 system information

The entries in this section describe characteristics of the A032 unit:

Serial number	Serial number of unit hardware. Should correspond to exterior label.
Hardware Information	Special information about this unit (normally shows `Unknown`).
Software Version	Shows Version number of firmware and BIOS in flash memory.
Software Build Date	Compile date of firmware (may be useful for support).
System Loading	Shows current processor load for Access Point (0 – 100%).
Buffer Utilization	Percentage of memory buffers used (0 – 100).

A032 system configuration

The entries in this group relate to the current configuration of the A032:

AP Name	User assigned name of Access Point. Default is LocalAP.
Net Name	Network Name in ASCII text format.
Admissions Mode	Indicates access security in effect (all, named, none).
Protocols	Protocol filter (all, or TCP/IP).
Telnet Access	indicates whether Telnet access is enabled.
Telnet Port	TCP/IP port number on which Telnet service is provided.
Web Access	indicates whether Web access is enabled.
Web Port	TCP/IP port number on which Web service is provided.
Management Enable	Global setting of Management enable flag (all, none, specific).
Gateway Address	IP address of network gateway configured into Access Point.
Current Time	Time and date in Access Point.

A032 radio table

Note that the counters in this group are measured from the Access Point’s perspective, treating the PCMCIA radio card as an independent device. Since the PCMCIA radio card contains its own MAC processor there may be small differences between the numbers reported in this group and those reported by the IEEE802.11 MIB which are measured inside the PCMCIA radio card. Note that counters are 32-bit and overflow back to 0.

Radio Interface Index	Fixed value of 2.
Radio Status	indicates up, down or `not present`. The latter is the case if the PCMCIA slot is empty.
Radio Type	Identifies the type of PCMCIA radio card installed.
Radio Description	Taken from the CIS of the PCMCIA Radio card.
Radio Firmware	Indicates the version of firmware used by the PCMCIA radio MAC processor.
Radio Usage	The percentage utilization over a recent 10 second interval (0 – 100%).
Radio Rx All Frames	Counter of frames received from PCMCIA card.
Radio Rx Mgmt Frames	Counter of management frames received from PCMCIA card.
Radio Rx Data Frames	Counter of data frames received from PCMCIA card.
Radio Rx Copied Octets	Counter of total bytes copied from PCMCIA radio card.
Radio Rx Frame Discards	Frames discarded by AP due to unspecified problem.
Radio Tx All Frames	All frames sent to the PCMCIA radio card.
Radio Tx Sent Octets	Counter of total bytes copied to PCMCIA radio card.
Radio Tx Fails	Count of frames for which re-transmission was required.

A032 LAN table (Ethernet)

Note that counters are 32 bit and overflow back to 0.

LAN Interface Index	Fixed value of 1.
LAN Status	Indicates up or down (if disabled by management process).
LAN Current Interface	Indicates 10baseT.
LAN Rx All Frames	Counter of all frames received by LAN interface.
LAN Rx Accept frames	Counter of frames which are copied into Access Point for processing.
LAN Rx Copied Octets	Counter of bytes transferred into Access Point from LAN interface.
LAN Rx Frame Discards	Frames discarded by Access Point due to unspecified problem.
LAN Tx All Frame	Counter of all frames sent to LAN interface.
LAN Rx Sent Octets	Counter of Bytes transferred to LAN interface.

A032 serial table

These entries pertain to the serial port on the back of the A032 unit.

Serial Status	Indicates up or down depending on the state of DTR.

A032 distribution

This section relates to the Access Point function of the A032.

Number Associations	How many wireless stations are currently associated with the Access Point.
Number of LAN entries	How many MAC addresses have been detected on the LAN interface.

Traps

The A032 supports a number of traps which are generated upon specific events and forwarded to configured managers. The following traps are supported:

SNMP standard traps

Trap Cold Start	Generated whenever the unit restarts.
Trap Warm Start	Not supported.
Trap Link Down	Generated when the LAN or Radio links are disabled.
Trap Link Up	Generated when the LAN and/or Radio links are initialized (during restart only).
Trap Authenticate Fail	Generated if a bad password in entered in the management log on.
Trap EGP Loss	Not supported.
Trap Enterprise	Supported as below.

Enterprise-specific traps

The following traps are generated as specified in the Nokia Private MIB:

A032 Authenticate Fail	Generated in the event that a station tries to associate but is refused due to the fact that the NID Name security or WEP feature is enabled. Note that this trap is limited to being generated no more than once every 30 seconds to prevent flooding due to denial of service attack.
A032 Bridge Down	If the bridge/repeater function is active, this trap is generated when a bridge link is lost.
A032 Management login	Generated whenever the Management password is successfully entered in one of the management utilities.
A032 TFTP Access	Generated whenever a TFTP transfer is initiated to or from the unit.

SNMP configuration

Specific details of setting up the SNMP agent in the Access Point are given in *SNMP setup* on page 63. Three types of information can be configured:

- The configuration allow for the System info (Name, Location, Contact) to be configured and stored.
- The configuration allows for up to four SNMP managers to be defined. This is not required if only Get functions are required. By checking the **allow any manager** box in SNMP configuration, access restrictions are removed. However, traps can only be sent to nominated managers as defined in the configuration.
- The configuration screen allows entry of the SNMP community names for both Get and Set. Although set is not supported in the Access Point, the definition of the community name is provided for consistency.

Appendix A – Data encryption and security

The WEP encryption method is defined by IEEE802.11. This means that you can use the Nokia A032 in conjunction with other vendors' wireless LAN clients which adhere to the standard.

This chapter gives a detailed overview of the *wire equivalent privacy* (WEP) security measures supported by the Nokia A032. You can employ these measures to safeguard your network against unauthorized access.

You'll need to refer to the following sections for specific instructions on using WEP:

- *Basic WEP setup* on page 37 and *Advanced WEP setup* on page 49– Configuring WEP settings using the web browser interface
- *WEP security functions* on page 82 – Configuring WEP settings via the CLM
- *Using the WEPGen utility* on page 163 – Managing keys using the supplied utility.

General security overview

One of the useful characteristics of wireless LAN is that the radio signal can penetrate walls and windows to increase coverage. However, if you don't take steps to protect your network, unauthorized users could intercept data or even gain access to your network. The Nokia A032 provides comprehensive security measures to counter eavesdropping and to control access.

- Access control depends principally on *authentication* (password-protection).

- Eavesdropping is prevented by the use of *encryption* (data is scrambled such that only the sender and receiver can understand it).

Authentication and encryption

The Nokia A032 provides several levels of authentication and encryption. Choose the level that is appropriate for your environment:

Level	Authentication	Encryption
Level 0	Open authentication (accept anyone)	None
Level 1	Only named wireless clients are allowed (identified by MAC address)	None
Level 2	IEEE802.11-compatible mode: 40-bit password	40-bit
Level 3	128-bit password	128-bit

Level 0

Level 0 or *open* system operation offers no special security provisions.

You might have an alternative security system in operation, or feel that the administration of passwords is not warranted by the low risk of an eavesdropper wanting to intercept your data.

Network access should be taken more seriously – you should not leave unsecured network resources such as servers or shared directories on an open wireless LAN. Use password locking at the operating system level for these resources to provide effective access security.

Level 1

Level 1 provides protection against unauthorized network access. It does not provide any protection against eavesdropping.

The use of Level 1 is described in *NID naming and security* on page 97. Basically, the access point only allows access to wireless clients with specific MAC addresses.

This protects you from other normal wireless LAN users, who might (inadvertently or otherwise) attempt to join your wireless LAN, but not against a determined *masquerade* attack (where a hacker illegally discovers and uses your MAC address).

Levels 2 and 3

Levels 2 and 3 use WEP (wire equivalent privacy). WEP is designed to provide both access control and eavesdropping protection. WEP depends on the use of keys (equivalent to passwords). Both the access point and the wireless client must know the key. The success of WEP depends on keeping the key away from unauthorized persons.

The WEP encryption method is defined by IEEE802.11. This means that you can use the Nokia A032 in conjunction with other vendors' wireless LAN clients that adhere to the standard.

WEP security overview

Secret keys

WEP depends on the fact that both the access point and the wireless client know a numeric password called a *key*. You might enter the key as a string (e.g. **`secret`**) or as a number (e.g. **`01524364732`**) but as far as the system is concerned it is just a sequence of bits – both the access point and the wireless client must store the sequence and prove to each other that the sequence is identical.

Key strength

The number of bits used for the key determines the *strength* of the key. Generally, the more bits there are in the key the harder it is for someone else to crack the code. Some governments restrict the use of very secure keys and for this reason the IEEE802.11 standard specifies 40-bit keys for general use. 40-bit keys provide a high degree of security uncrackable by all but the most determined attackers. The Nokia A032 allows the use of longer keys where local regulations permit, up to 128 bits in length. Such keys are essentially uncrackable by known methods.

To put the key strength in perspective, a 40-bit key might be cracked in about one month using a machine capable of trying 100,000 different keys a second. By comparison, the same machine would take many million times the age of the universe to crack a 128-bit key using the same approach!

Authentication

Because secrecy of the key is paramount, WEP never transmits a key value over the network. The wireless client only needs to prove to the access point that it has a matching key. It achieves this using a method known as *challenge-response*:

1. The wireless client indicates to the access point that it wants to connect.
2. The access point sends a random number (the *challenge*) to the wireless client.
3. The wireless client performs a computation using its key and the random number, and sends the result (the *response*) back to the access point.
4. The access point performs the same computation, using the same random number and its copy of the key.
5. If the keys match, the result of the computation will match that sent by the wireless client – the wireless client is authenticated and may be accepted.

The computation is such that a hacker intercepting both the challenge and the response cannot work back to find out the key. Intuitively you might think that if you can compute the response from the key you should be able to "uncompute" to get the key from the response. However, this is not the case.

As an example, suppose you pick ten random prime numbers and multiply them together to get a result. Now take the result and ask a friend to figure out which ten prime numbers you started with. Such computations are much easier in one direction than the other.

Encryption

Once a wireless client has been authenticated and accepted onto the network, any communications can be encrypted using the secret key. Since both the wireless client and the access point have proved to each other that they have the same secret key, it can be used as a scrambler and descrambler making it very hard for unauthorized users to extract anything useful from intercepted transmissions.

Key management

Because secrecy of the key is so important, careful attention must be paid to the way in which keys are created, stored and passed to users. Even the most secure system is worthless if the secret keys are intercepted.

Key management is a general term for the way in which you allocate and control key (password) allocation to users. The Nokia A032 provides two basic approaches for key management:

- *Shared WEP keys* – All wireless clients in a group use the same key
- *Personal WEP keys* – Each wireless client has an individual key.

The choice of key management method depends on your security requirements and administration methods.

Shared WEP keys

Shared WEP keys are suitable for small organizations or individual offices. Shared WEP keys may be referred to as default keys by other vendors.

In this case all the wireless clients are loaded with the secret key information. The same key is loaded into the access point.

The advantage of this approach is that it is simple to manage, since there is only one key active at a given time (chosen from an available ‘pool’ of up to four keys). You can change the key on a regular basis without disrupting the network (see *Using shared WEP keys* on page 136).

The disadvantage of a shared WEP key is that if it is known by a number of people there is a greater chance of it being disclosed outside the organization. Every time someone leaves the group it may be necessary to change the shared WEP key to maintain security.

Personal WEP keys

When using personal WEP keys:

- Each wireless client is assigned a personal WEP key
- A list of personal WEP keys is held by the access point, or is accessible via an external database (see *Key databases* on page 140).
- An access point uses a different key for each client which is being addressed. This provides a high level of security.

In a large organization it may be more convenient to use this method. If someone leaves the company, or if a laptop is stolen for example, you only need to remove or change one key in the database.

Entering keys

Entering keys in the wireless client

Unfortunately there is no standard way in which keys are stored or entered into a wireless client. The method will depend on the vendor of the radio card, and you should consult the manual supplied with your wireless client. Some methods you might encounter are:

- Keys are entered manually using a utility program on the wireless client.
- Keys are entered manually using a task bar application to access the wireless client setup
- Keys are entered from an encrypted data file, read by a utility on the wireless client – a convenient method for sending keys to users on a floppy diskette without disclosing the actual key values.
- Keys are stored on some other medium, such as a smart card which can be inserted into the wireless LAN adapter card.

Nokia wireless LAN adapters support a range of these options.

If you are required to enter a WEP key manually, you might be able to use an ASCII text string (e.g. **`mypwd`**). However many adapters will require you to enter the key using hexadecimal notation, e.g. **`0x12A3D4`**. The important thing is that the same key value must be entered both at the access point side of the network and on the wireless client.

Also note that if the client provides the option for different key lengths, the key length must be the same at the access point side and the client side. If the client does not provide the option to specify the key length, you should assume that the key length is 40 bits (IEEE802.11) and set the access point accordingly.

Entering the keys at the Access Point

If you are using shared WEP keys it is relatively easy to enter the keys into the access point and maintain them. This is because there are only four shared WEP keys used at any one time. If you have multiple access points and want wireless clients to be able to roam, it is of course necessary to ensure that all the access points are programmed with the same shared WEP keys. The method for entering shared WEP keys is described in *Basic WEP setup* on page 37 (if you're using the web interface) and *WEP security functions* on page 82 (if you're using the CLM).

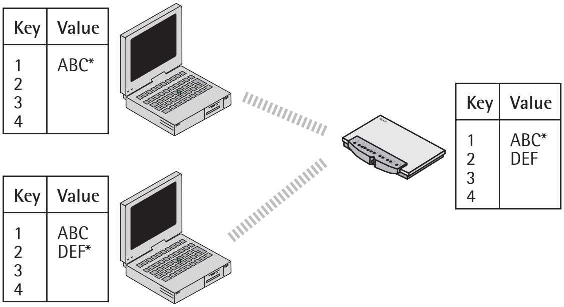
If you are using personal WEP keys, the problem of key management can be much harder. This is because there can be a different key for *each* wireless station in your organization.

To assist in the management process Nokia provides a key management utility (WEPGen) with the Nokia A032 access point. This utility allows you to enter and modify lists of users and to store the lists (suitably encrypted) on a disk file. The disk file can then be uploaded into the access points or used to enter the users and keys into a key server database (see *Key databases* on page 140). The use of the key management utility is described fully in *Using the WEPGen utility* on page 163.

Using shared WEP keys

The Nokia A032 can store up to four shared WEP keys simultaneously.

An access point only transmits data using one of the shared WEP keys – the active key – but can receive data from clients using any of the four shared WEP keys it knows about:



Key	Value
1	ABC*
2	
3	
4	

Key	Value
1	ABC
2	DEF*
3	
4	

Key	Value
1	ABC*
2	DEF
3	
4	

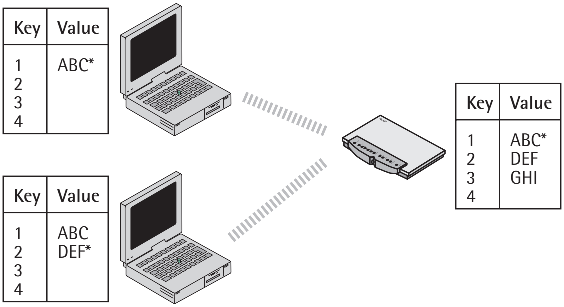
As you can see from the figure above, the active key (denoted by the asterisk *) does not have to be the same on each client, but each client’s active key must be recognized by the access point.

The active shared WEP key is also used to transmit broadcast and multicast frames even to wireless clients which are using personal WEP keys for normal data. This means that even if you are using personal WEP keys, you should always define at least one active shared (default) key to the access points and wireless clients.

Changing a shared WEP key

Having a pool of shared WEP keys makes it easy to change a key without disrupting network operation:

1 Add a new shared WEP key to the access point, but don’t make it the active key yet:

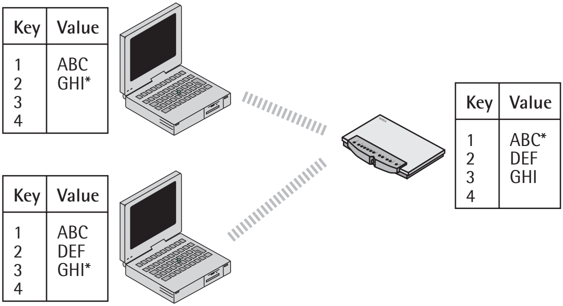


Key	Value
1	ABC*
2	
3	
4	

Key	Value
1	ABC
2	DEF*
3	
4	

Key	Value
1	ABC*
2	DEF
3	GHI
4	

2 Instruct all clients to add the new shared WEP key to their list and make it the active key immediately:



Key	Value
1	ABC
2	GHI*
3	
4	

Key	Value
1	ABC
2	DEF
3	GHI*
4	

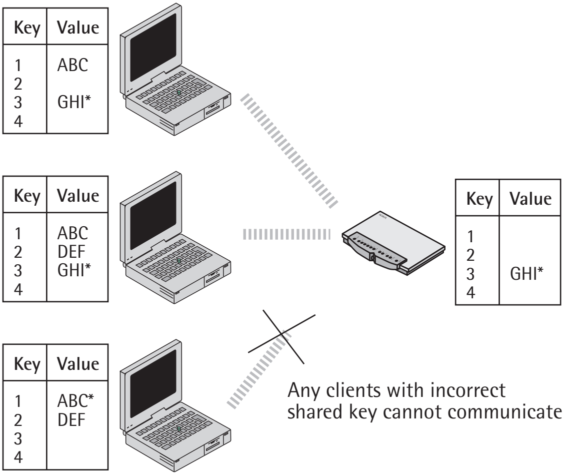
Key	Value
1	ABC*
2	DEF
3	GHI
4	

They will be able to transmit using the new key, as the access point already knows about it.

3 When all clients have been updated, switch the access point to use the new key as its active key.

At this point you can delete the old key values from the access point.

Any clients using the old key will now be unable to use the network:



Key	Value
1	ABC
2	
3	GHI*
4	

Key	Value
1	ABC
2	DEF
3	GHI*
4	

Key	Value
1	ABC*
2	DEF
3	
4	

Key	Value
1	
2	
3	GHI*
4	

Any clients with incorrect shared key cannot communicate

The Nokia A032 provides configuration options for setting the shared WEP keys and selecting the active key using either the web interface (see *Basic WEP setup* on page 37) or the CLM (see *WEP security functions* on page 82).

Setting WEP key policy

At time of going to press, the IEEE802.11 standard specifies the use of 40-bit keys (five bytes). However, the Nokia A032 provides the option to use longer (i.e. stronger) keys if the network administrator chooses. Key lengths of 40, 56, 64, 96 and 128 bits are supported. The key size (or range of allowed sizes) must be specified in the access point through configuration (the default is 40 bits). This entry is used to determine the access point’s *WEP key policy*.

Note that the selected key length policy does not affect the size of the keys which can be entered and stored in the Nokia A032. Even if you have selected the use of 40-bit keys, it is possible to enter and store 128-bit keys (16 bytes) in the access point. However, keys which fall outside the current key length policy are considered to be invalid by the access point and will not result in successful authentication.

The Nokia A032 supports three WEP key policies: Normal, Strong and Custom.

- Normal mode – all keys must be 40 bits (5 bytes) long. This is also IEEE802.11-compatible mode
- Strong mode – all keys must by 128 bits (16 bytes) long. This is the highest security mode.
- Custom mode – other key lengths, or ranges of key lengths, can be used. When Custom WEP key policy is selected, the administrator must also select a key length range by specifying and minimum and maximum value. Suppose for example the range is defined as 40 – 128 bits. In this case any key size in the range will be authenticated providing both the content and the length of the key stored in the access point matches that in the wireless client.

Key databases

The Nokia A032 supports two types of key database to store personal WEP keys:

- Local key database – The simplest type of key database is a local list which is stored inside the access point using flash memory. This list can hold up to 200 entries.
- External key database – This allows you to store more than 200 keys in a centralized location. The Nokia A032 can access an external key database across the LAN.

Local key database

Each access point contains a NID name list (see *NID name table* on page 98). This contains up to 200 client or bridge entries, consisting of the MAC address, WEP key and a user-assigned name.

If the local database is selected and personal WEP key operation is activated, each time a wireless client attempts to communicate, the access point will search for the client's entry in the NID name list and use the corresponding WEP key to authenticate the client.

The limitations of the local database are:

- A maximum of 200 entries.
- If there are multiple access points, each one must be loaded with the same copy of the NID name table; any change to one access point must be made to all the others.

External key database

Rather than storing the keys on the access points, the Nokia A032 offers you the option to store them using an *authentication* server. The authentication server must support the RADIUS protocol. Many vendors, including Nokia, sell such authentication servers.

Using an external server has the following advantages:

- You can store a large number of keys.
- All the keys are stored at a central location – you don't need to update all the access points individually when a key is added, deleted or modified.

If you are using an authentication server, you'll need to enter the keys manually by reading the text file `nids.txt`.

Note that the value of the key which is stored in the authentication server is itself encrypted. This means that the key cannot be discovered while being retrieved by the access point across the network. On arrival at the access point, the key is decrypted using the RADIUS Shared Secret of the access point.

Setting up a RADIUS external key database

The Nokia A032 can use RADIUS to access an external key database. There are several parameters which must be configured to allow this feature to work. To understand these parameters it is necessary to describe the way in which the keys are accessed.

In this section we will use the term *RADIUS server* to refer to an "Authentication Database server accessed using the RADIUS protocol". Such servers are widely available from various vendors for most platforms.

General RADIUS operation

The primary purpose of the RADIUS server is to authenticate a user. The basic mode of operation is as follows:

1. A RADIUS request is made including a username and password.
2. The password is encrypted using a secret known by the requestor and the server (the shared secret).
3. The Server looks up the username in its database and then checks the password for a match. If the match is made an “accept” message is returned. If the match is bad a “reject” message is returned.

Nokia-specific implementation of RADIUS operation

The above mode of operation doesn’t quite suit the requirements of the access point. The access point does not want the *server* to make the decision to accept or reject the wireless client. Indeed, at the time the RADIUS request is made no challenge has yet been issued to the client. The access point wants the RADIUS server to return the value of the WEP key corresponding to the username.

RADIUS has a provision for the server to return a value with the accept message. We utilize that value to store and return the WEP key for the user.

In the Nokia A032 implementation, the sequence of events is as follows:

1. The access point receives an authenticate request from a wireless client.
2. The access point formulates a RADIUS request using the wireless client's identifier (usually the MAC address) as the username and a fixed string (called the *dummy password*) for the password field. Consistent with normal RADIUS operation, the password is encrypted using a *shared secret*.
3. The RADIUS server decrypts the password value using the appropriate shared secret and then looks up the username in its database.
4. If the username is not found, the server replies with a reject message. If the username is found the server checks that the value of dummy password is correct and then replies with an accept message, containing the WEP key.
5. The access point now uses the WEP key to challenge the wireless client and make a decision whether to admit it to the network.

RADIUS dummy password

Note that all the usernames entered into the RADIUS database will have the same password field (= dummy password). There can be a different shared secret for each access point – the RADIUS server will identify the correct shared secret based on the IP address of the requesting access point.

The WEP key is sent across the link in plain text. This means that the RADIUS server does not encrypt the WEP key. However, the Key generator utility (WEPGen) encrypts the WEP key before it is entered into the RADIUS database. Therefore the system is protected from unauthorized interception.

The Nokia A032 allows you to enter the IP addresses of two RADIUS servers. If a request to the primary server does not receive a reply a second attempt will be made to the secondary server. In this way a redundant backup can be maintained.

Appendix B – Wireless bridges and repeaters

This appendix explains how to use the Nokia A032 as a wireless bridge or repeater.

For information on security issues, refer to *Data encryption and security* on page 127.

Overview

This section introduces the concepts of wireless bridges and repeaters. The following sections tell you how to configure a network using Nokia A032s as bridges or repeaters.

Important note!!

Roaming is possible but not recommended.

This version of the Nokia A032 does not support roaming by wireless stations from one bridge to another. To avoid this, each Nokia A032 used as a bridge should be assigned a unique network name. This will prevent inadvertent roaming.

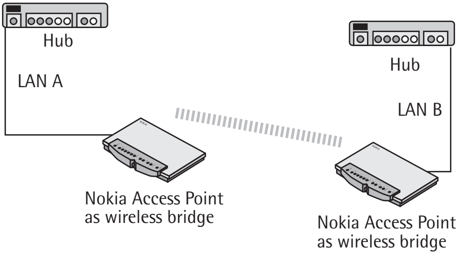
Wireless bridges

Important note!!

The Access Points must be on the same channel to bridge.

A LAN MAC bridge has a specific meaning in LAN networks and should not be confused with a *wireless point-to-point bridge*. A wireless bridge is one of a pair of units used to connect LAN segments together using wireless.

In the example below, LAN A and LAN B are bridged together and act, in principle, as a single LAN.

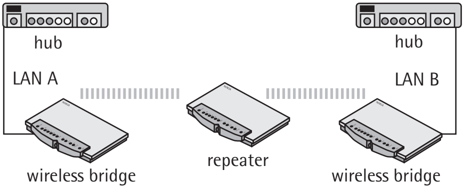

Hub
LAN A
Hub
LAN B
Nokia Access Point as wireless bridge
Nokia Access Point as wireless bridge

Notes

- Only the data that needs to be sent over the wireless link is transmitted. Data which is sent locally on LAN A is not transmitted to LAN B. This is to reduce congestion on the wireless link and allow operation of the LANs at a higher data rate than supported by the radio link.
- There is no loss in the data rate when two access points are configured without repeaters, as in the above example.
- Many access points can be configured into a bridging network. However, using multiple bridges the data rate will be affected by the amount of broadcast messages sent. Each broadcast message is copied by the originating access point and sent to each bridged access point individually, the more broadcast messages sent the slower the network will be. In practice, if you need to use more than three or four bridges in your network, you may need to rethink your network topology.

Wireless repeaters

In addition to the wireless bridge function, Nokia access points can act as wireless *repeaters*, and extend the range of a system by receiving and re-transmitting the data at a mid-point in the communication path:



In the example above, the data from LAN A which needs to be sent to LAN B is first sent to the repeater. It is then re-transmitted from the repeater to LAN B.

Note: Data rate does become degraded, the more repeaters you use:

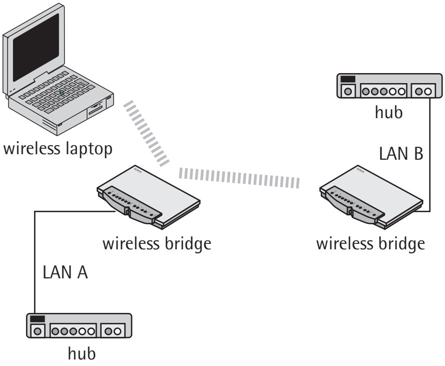
> degradation of data rate = data rate / (number of repeaters + 1)

Examples

- For one repeater the data rate is halved.
- For two repeaters, the data rate is divided by three, and so on.

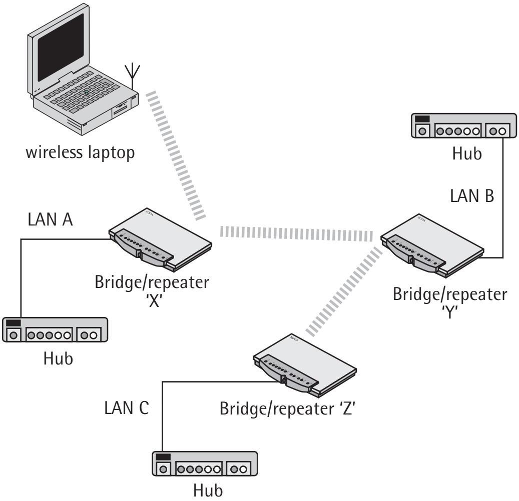
A special case – wireless client

A special case of a repeater function is where a wireless LAN workstation forms part of LAN A. The example in the figure below looks like a wireless bridge, but actually there is a repeater function in operation, because the wireless laptop sends data across the first wireless link and the data has to be re-transmitted to LAN B.



Hybrid and multiple repeater configurations

The Nokia A032 is capable of supporting repeater and bridging functions simultaneously. In addition, it can support multiple hops (more than one repeater) as well as multiple bridge paths:



Important!! *X and Z must not see each other as bridge partners. This would create a loop around which data would circulate continuously, leading to a blockage of communication.*

The above figure shows a combination of repeater and bridging functions demonstrating the use of multiple simultaneous functions, including:

- Bridging two LANs

  LAN A is bridged to LAN B via the wireless bridges, X and Y

- Bridging LANs via a repeater

  LAN A is bridged to LAN C using wireless bridge Y as a repeater.

- Repeater function for wireless workstations

  The wireless laptop can communicate to LAN B using wireless bridge X as a repeater.
- Multiple repeater operation

  The wireless laptop can communicate to LAN C using both X and Y as repeaters. First, the data is sent to X which retransmits it to Y. Y then retransmits it to Z.
- Multiple bridge paths

  LAN B can communicate with LAN A and LAN C. In this case the wireless bridge Y will choose to send the data either to X or Z according to the destination LAN.

Configuring for wireless bridge/repeater operation

Before you can use Nokia access points as bridges, you need to configure them manually to:

- tell them specifically which other access points are available as bridge partners
- ensure that no loops are created.

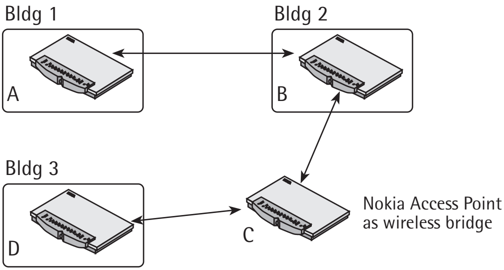
Step-by -step procedure

Gathering the information

Before you connect and configure your network, make sure you have all the necessary information to hand:

1. Draw a topology map, showing all the Nokia A032s you plan to include in the bridge/repeater function.
2. On the map show the bridge partner relationships and make sure that there are no loops.

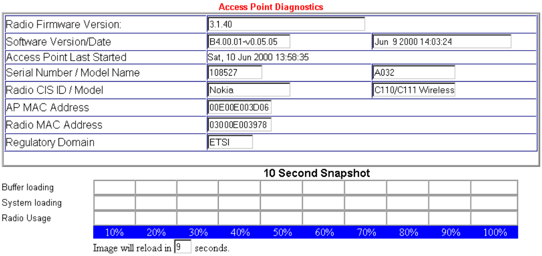
   In the example below, involving four access points, A and D act as wireless bridges. B acts as a wireless bridge and repeater, having a local LAN attached. C acts only as a repeater:



3 Determine the **Radio MAC Address** (i.e. that of the *radio card* in each Nokia A032, *not* the MAC address of the access point itself).

You can obtain this information using the `config` command via the serial port or Telnet interface to the Nokia A032 (see *config* on page 91) or by using the diagnostics screen of the web interface (see *Internals status screen* on page 30).

An example of the Web diagnostics screen is shown below – the **Radio MAC Address** can be seen clearly.



Access Point Diagnostics

Radio Firmware Version:	3.1.40	
Software Version/Date	B4.00.01-v0.05.05	Jun 9 2000 14:03:24
Access Point Last Started	Sat, 10 Jun 2000 13:58:35	
Serial Number / Model Name	108527	A032
Radio CIS ID / Model	Nokia	C110/C111 Wireless
AP MAC Address	00E00E003D06	
Radio MAC Address	03000E003978	
Regulatory Domain	ETSI	

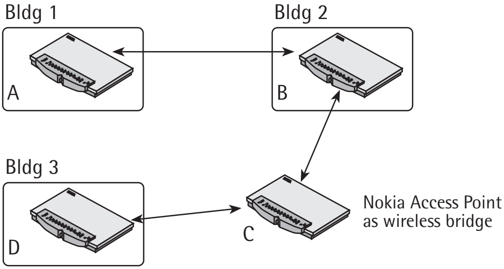
10 Second Snapshot

Buffer loading
System loading
Radio Usage

10% 20% 30% 40% 50% 60% 70% 80% 90% 100%

Image will reload in 9 seconds.

4 Write down the MAC addresses (and access point IP addresses, if you're going to use Telnet to configure the A032s) on your topology map and keep it to hand:



AP	radio MAC*	IP address
A	00E003001234	192.168.0.1
B	00E003008192	192.168.0.2
C	00E00300A04C	192.168.0.3
D	00E00300BC12	192.168.0.4

*MAC address of radio card, not that of access point.

Setting up the bridges

Each Nokia A032 must be individually programmed to identify its bridge partners. You can only do this using the serial port or Telnet interface:

1. Power up a Nokia A032 and log into the serial port or Telnet interface program (see *Accessing the command line manager (CLM)* on page 67).
2. Enter the information for all the A032's bridge partners using the `bridge` command, which has the format:

   ```
   bridge add MAC Name
   ```

   where *`MAC`* is the MAC address of a bridge partner and *`Name`* is a name for that partner, of up to 16 characters, which you can choose.
3. Repeat steps 1 and 2 for all the other access points.
4. Restart all the A032s.

Once all the Nokia A032s are operating they will automatically learn where the various network-attached computers reside and bridge data to the correct location.

An example using Telnet

To set up bridge partners as shown in the last figure, via Telnet, you would proceed as follows:

1 Connect to access point A (IP address 192.168.0.1).

2 Enter the following command:

```
bridge add 00e003008192 bridgeB
```

3 Connect to access point B (IP address 192.168.0.2).

4 Enter the following commands:

```
bridge add 00e003001234 bridgeA
bridge add 00e00300a04c bridgeC
```

5 Connect to access point C (IP address 192.168.0.3).

6 Enter the following commands:

```
bridge add 00e003008192 bridgeB
bridge add 00e00300bc12 bridgeD
```

7 Connect to access point D (IP address 192.168.0.4).

8 Enter the following command:

```
bridge add 00e00300a04c bridgeC
```

9 You can use the command `bridge list` to show the entries. Also you can use the command `bridge delete` to remove entries made in error or no longer required.

10 When you've specified all the entries, restart the Nokia A032s.

The connections should be established.

11 To check that the connections are working, go to the wireless status screen in the web interface or use the CLM `show` a command. The bridge partners should be shown by their user-friendly name and listed as `Is Bridging`. It may take up to 30 seconds for the bridge partners to connect.

Restarting bridges and repeaters

If one or more of the Nokia A032s is restarted, bridging information will be temporarily lost. This may result in loss of communication in the network for up to 5 minutes until the information is re-learned from the network.

Associated CLM commands

- `bridge list` – shows any bridge partners associated with the current access point
- `bridge add` – adds the MAC address of a new bridge partner to the bridge list

  ```
  bridge add MAC Name
  ```
- `bridge delete` – deletes a bridge partner from the current access point

  ```
  bridge delete MAC Name
  ```

Setting up bridges using WEPGen

You can use the WEPGen utility to specify to the access point which devices are peer bridges. See *Using the WEPGen utility* on page 163.

Appendix C – Factory defaults

Parameter	Function	Default
Radio-related		
channel	Set radio frequency channel	10
domain	Set regulatory domain	(depends where unit purchased)
frag_threshold	IEEE802.11 parameter	2346
long_retry	IEEE802.11 parameter	15
rts_threshold	IEEE802.11 parameter	2301
short_retry	IEEE802.11 parameter	15
sifs_time	IEEE802.11 parameter	0
Access Point functions		
ap_name	Identifier name for access point	LocalAP
net_name	Logical name of wireless network	"Nokia WLAN"
protocols	Selects protocol filtering	all
TCP/IP parameters		
gateway	Sets Default Route when TCP/IP filtering	0.0.0.0 (none)
ip_address	Sets IP address of Nokia A032	0.0.0.0 (none)
subnet_mask	Sets Subnet Mask for local network	255.0.0.0
Management functions		
admission	Enables Association screening	all
basic_rate	The basic rates are set in kHz. Valid values also include 1000, 2000, 5500 and 11000	1000 2000
lan	Controls LAN port on A032 hardware.	10baseT
password	Sets password of Command Line Manager	default
telnet	Controls Telnet functions	on:23
web	Controls WEB browser monitor function	on:80

Parameter	Function	Default
DHCP functions		
dhcp_base	Sets start address of DHCP address pool	192.168.5.100
dhcp_dns	Sets alternate DNS server for client notification	-
dhcp_gateway	Sets alternate gateway for client notification	-
dhcp_pool	Sets size of DHCP address pool	0
WEP security functions		
radius_server	IP address of backup key server	-
shared_secret	Authentication key between Access Point and external key server, and RADIUS password (key encryption password, held on external server)	-
use_encrypted_nid	Affects the format of the nids.txt file used to load specific keys.	false
wep_key	Assigns a value to one of the four default keys	-
wep_key_active	Specifies which of the four default keys is active	-
wep_key_range	Specifies encryption level	40
wep_mode	Specifies management access	wep
Internet service provider information		
isp_dns1	Fixed value of ISP DNS server	-
isp_dns2	Fixed value of ISP DNS server	-
isp_ip_address	Fixed value of external (ISP) IP address.	-
isp_num	Phone number of ISP	-
isp_pwd	Login Password for ISP account	-
isp_user	Login Username for ISP account	-

Parameter	Function	Default
Modem setup		
mdm_holdtime	Minutes of inactivity to go on hook	3
mdm_init	AT command initialization string sent to modem	-
mdm_speed	Data rate between A032 and modem	57600
NAT setup		
nat_gateway	Gateway address of external LAN	0.0.0.0
nat_port	Determines on which interface NAT is active	off
nat_subnet	Subnet mask of external LAN	0.0.0.0
SNMP setup		
community_get	Determines which SNMP users can access information.	public
community_set	Not supported	private

Appendix D – Utilities CD-ROM

The *Nokia A032 Utilities CD-ROM* is supplied with the Nokia A032. It contains, among other things:

- Nokia software utilities
- A032 user guides in Adobe Acrobat PDF format.

This chapter explains how to add items to your **Start** menu and install various programs, files and utilities on your hard disk.

Installing the Nokia A032 utilities

To install the Nokia A032 utilities:

1. Insert the *Nokia A032 Utilities CD-ROM* into the computer's CD-ROM drive.
2. Select your language.
3. Read the Nokia license conditions. If you agree to them, click **Agree**.
4. Follow the remainder of the on-screen instructions to install the software.
5. Click **Finish**.

The files installed are as follows:

- Nokia TFTP Utility
- AP_load.exe – utility for upgrading the Nokia A032
- A032.bin – A032 firmware
- WEP key generator
- Nokia MIBs – SNMP MIB files.

If you accepted the default settings during installation, click **Start > Programs > Nokia A032**. You should see the following entries:

- **Nokia Access Point Upgrade**
- **Nokia TFTP Client**
- **Nokia WEP Key Generator**
- **Remove Nokia Wireless LAN Utilities**

See *Upgrading* on page 191 for upgrade instructions.

See *Using TFTP* on page 103 for instructions on using the Nokia TFTP client.

See *Using the WEPGen utility* on page 163 for more information on using WEPGen (the Nokia WEP key generator).

Removing the Nokia A032 utilities

To uninstall the Nokia A032 utilities:

1 Click **Start > Programs > Nokia A032 > Remove Nokia Wireless LAN Utilities.**

Appendix E – Using the WEPGen utility

The *Nokia A032 Utilities CD-ROM* includes a tool called WEPGen which helps you to manage users in the event that you are using personal WEP keys. The utility allows you to:

- Enter and store lists of users and keys
- Download the keys into an access point
- Save a disk file which can be used to load keys into an authentication server.

Installing the WEPGen utility

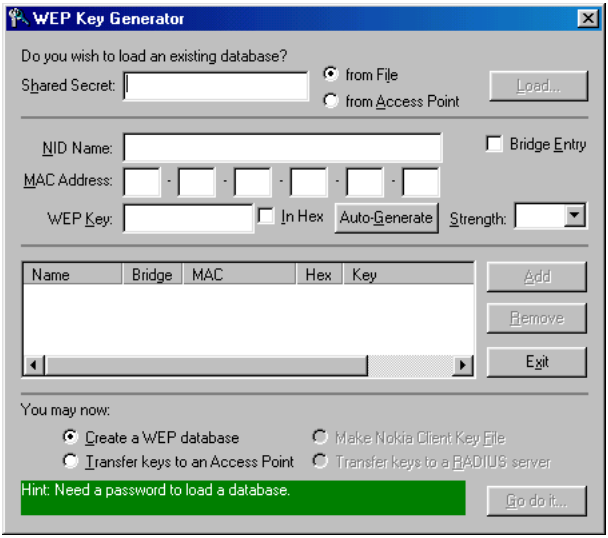
The WEPGen utility is installed as part of the Nokia A032 utilities suite – see *Utilities CD-ROM* on page 161.

Running the WEPGen utility

To run the WEPGen utility:

1 Click **Start** > **Programs** > **Nokia A032** > **Nokia WEP Key Generator**.

You'll see the following window:



Hint: Need a password to load a database.

2 Enter a **Shared Secret**.

The shared secret is a text string up to 16 characters long. It must be the same as that configured into the access points with which you intend to use the generated keys.

The shared secret is used as follows:

- An encrypted version of the secret is placed at the start of the key information when it is transferred to the access point. The access point will reject the transfer unless the secret matches its own stored value.
- The WEP keys which are transferred to the access point or entered into an external Authentication database are encrypted using the shared secret. Before the access point uses the keys it internally decrypts them using its own copy of the shared secret.
- The shared secret is also checked when the utility loads a previously stored set of keys.

There's more on this in *Setting up a RADIUS external key database* on page 141.

After entering the secret you can do one of two things:

- Load a previously stored key file
- Start to create a new stored key file.

Loading a previously stored key file

To load a previously stored file:

1. Click the **from File** radio button next to the Load button.
2. Click **Load**... at the top of the window.
3. When prompted, navigate to the file you want to load.
4. Make sure the **Fully encrypted** option is set correctly according to the file contents (see *Storing the entries in a database file* on page 168).
5. Click **Open**.

The key file is usually called `nids.txt`. You can also upload this file to the access point using the TFTP utility (see *Using TFTP* on page 103).

Entering users that have WEP keys

Now you are ready to add, delete or modify keys. The information you enter will depend on whether you are using a normal wireless client or a special Nokia wireless client using Smart Card WEP key storage.

Normal wireless client

In the case of a normal wireless client, take the following steps:

1. Enter a **NID Name**. This is normally a text string which you can choose. This name will be reported on management screen but is otherwise not used for security. It must be longer than four letters.
2. Enter the **MAC Address** of the wireless client.

3 Enter the **WEP Key** value for the wireless client. Here you have some choices:

- You can enter the key as a text string, taking care to enter the correct number of characters for the key length required. The utility will not accept keys which do not match the selected key size.
- By clicking the **In Hex** box you can enter the key as a hexadecimal number
- By clicking the **Auto Generate** box and selecting the key **Strength** from the drop-down menu (40, 56, 64, 96 or 128 bits) the utility will create a random number of its own choosing and enter it into the **WEP Key** field.
  In this case you should make a note of the hex value so that you can enter the same key into the wireless client later.

4 When you have entered the information, make sure that the **Bridge Entry** box is clear and click **Add**.

The key should appear in the display window.

Nokia Smart card solution

If you are using the Nokia Smart card solution you should follow the same procedure above, except that:

- The **NID Name** and the **WEP Key** must be entered as supplied with the Smart card
- The **MAC Address** field should be left clear.

Entering users that do not have WEP keys

If you are using NID names simply to identify MAC addresses, or as part of the NID name security feature, you can also enter those names using the WEPGen utility.

In this case enter the **NID Name** and the **MAC Address**, but leave the **WEP Key** field empty

Entering Bridge identifiers

If you are using the wireless bridging or repeater function of the access point, you need to specify to the access point which devices are peer bridges. You can use the WEPGen utility to enter these devices by adding the **NID Name** and **MAC Address** of the bridge device and checking the **Bridge Entry** box.

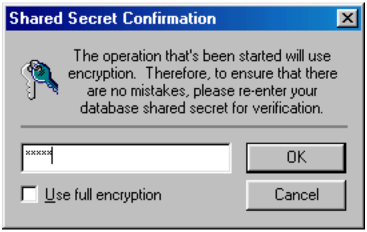
Storing the entries in a database file

When you have finished entering or modifying the key you can save it as a key database (recommended) or transfer the values directly to an access point using TFTP.

To save the information as a file:

1. Click the radio button **Create a WEP key database.**
2. Click **Go do it...**

3 When prompted, re-enter the shared secret as a confirmation:



Shared Secret Confirmation

The operation that's been started will use encryption. Therefore, to ensure that there are no mistakes, please re-enter your database shared secret for verification.

*****

□ Use full encryption

4 Specify whether you want the file to be fully encrypted. If you check the **Fully encrypted** box, the resulting file will be unreadable to a normal text editor. Otherwise the file will be written using a text format in which only the key values are encrypted.

5 Click **OK**.

6 Specify the file location for the database.

Transferring the key database to an access point

There are two methods by which you can transfer keys to an access point:

- Using the WEPGen utility
- Via a TFTP client.

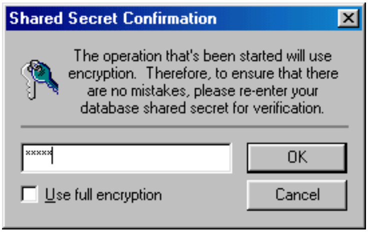
Both methods actually use TFTP to transfer via the LAN (or WLAN) network.

In both cases, the choice of encryption must match the configuration of the access point. In other words, if you choose the fully encrypted option the access point must also be configured with the check box **Use encrypted nids.txt** on the WEP screen setup page (see page 49).

Using the WEPGen utility

To transfer the database directly from the WEPGen utility to the access point:

1. Click the radio button **Transfer keys to an Access Point.**
2. Click **Go do it...**
3. When prompted, confirm the **Shared Secret** and set the encryption appropriately:



Shared Secret Confirmation

The operation that's been started will use encryption. Therefore, to ensure that there are no mistakes, please re-enter your database shared secret for verification.

*****

□ Use full encryption

4 Click **OK**.

5 Enter the IP address of the target access point.

6 Click **Send**.

The data will be transferred. Any errors which occur should be reported at this time. The TFTP dialog box will remain on the screen so that you can send to several access points in turn by modifying the IP address.

7 When you're finished, click **Close**.

Using TFTP

If you have saved a WEP key database using the name `nids.txt` you can transfer it to the access point using a TFTP client utility (see *Using TFTP* on page 103).

Briefly:

1 Enter the IP address of the access point.

2 Specify **`nids.txt`** as the target filename (destination).

Transferring a key database from an access point

If you want to retrieve the keys which are stored on an access point, you can:

- Download directly to the WEPGen utility using TFTP
- Read `nids.txt` via a TFTP client utility (see *Using TFTP* on page 103).

In the latter case the keys will be sent by the access point in the same format as generated by the WEPGen utility – either fully encrypted or partly encrypted, depending on the configuration of the access point.

Using the WEPGen utility

To transfer a key database from an access point directly into WEPGen:

1. Make sure that you have entered the **Shared Secret** corresponding to the access point.
2. Click the **from Access Point** radio button.
3. Click **Load**.
4. When prompted, confirm the **Shared Secret**.
5. Enter the IP address of the access point.
6. Specify whether the fully encrypted format is expected.
7. Click **OK**.

The transfer should occur and the keys will be displayed in the main key window from where they can be edited or saved.

Making a client key diskette

If you are using a Nokia wireless client, you can use the WEPGen utility to generate a file which can be loaded into the client to ensure that the client’s copy of the specific key matches that of the access point.

To create such a file:

1 Select one key in the key window.

1 Click the radio button **Make Nokia Client Key File.**

2 Click **Go do it...**

3 Confirm the **Shared Secret.**

4 Enter a key name and a comment.

5 Specify the destination for the file.

6 Click **OK** to create the file.

Appendix F – Troubleshooting

This appendix helps you resolve TCP/IP addressing conflicts, diagnose startup problems, and gives useful advice if you're having problems with your dial-up Internet connection.

Renewing client IP information

If you change the A032's IP address, you might not be able to access the A032 from a client machine.

If IP information in your client machine is obtained using DCHP, you may need to *renew* the information before you can access the A032.

Under Windows 95/98

Under Windows 95/98, you do this using WinIPcfg:

1. Choose **Run** from the **Start** menu.
2. Enter **`WinIPcfg`** and press **Return**.
3. Select the correct adapter card in the pull-down menu.
4. Click **Release**.
5. Click **Renew**.

Under Windows 2000/NT

1 Open a DOS prompt.

2 Enter **`ipconfig /release`**

  This will release the old address.

3 Enter **`ipconfig /renew`** to renew the address.

You should now be able to access the A032 from your client machine.

Startup problems

This section gives advice on troubleshooting problems during initialization (startup).

Initialization error codes

Note: *If the unit fails to perform the initialization sequence, it may need to be repaired. In this case contact your supplier for support.*

If the initialization procedure fails an error code should be displayed on the **info** LEDs and the **alert** LED will remain on.

The code should be read from left to right. To identify the code write down each LED as a ’1’ or ’0’ depending on its state (on = 1).

For example the pattern:

```
on on off off on off
```

would be written:

```
110010
```

The following table shows the meaning of the initialization error codes.

Code	Meaning	Log text
100001	Bad code image	<none>
110000	Bad PCMCIA hardware	PCMCIA hardware failure
110001	No PCMCIA	No PCMCIA card detected
110010	Bad PCMCIA card	Non-compatible PCMCIA card
110011	Bad radio (does not initialize)	Cannot initialize radio
110100	Bad firmware version	Incorrect firmware version
001000	Bad DRAM (stuck address)	Memory error type 1
001001	Bad Ethernet RAM (stuck address)	Memory error type 2
001010	Bad CMOS Memory	Configuration error – default loaded
101000	LAN controller error	LAN Interface Error
011000	Bad configuration	Configuration error
011001	Bad Manufacturer's info	Bad unit checksum
011010	Bad log sector	Log sector bad – recovered
011011	System error	System fault

The next section gives a more detailed explanation of the above error messages.

info LED error codes explained

100001: Bad code image

This error message indicates that the flash memory firmware is invalid or corrupted. Correct firmware is loaded at the factory prior to shipment. Therefore this problem may be the result of a problem during an upgrade procedure. *Appendix G* describes methods for reloading the firmware. If these procedures fail to solve the problem there may be a failure in the unit and it may need to be repaired.

110000: Bad PCMCIA hardware

Indicates that there is a failure of the PCMCIA slot. Unit must be repaired by dealer.

110001: No PCMCIA

Indicates that no PCMCIA card has been detected. This will occur if the PCMCIA slot is empty or the radio card did not seat properly. The unit may pause with this code for a short time, and then initialize properly.

110010: Bad PCMCIA card

Indicates that the PCMCIA card is not compatible with the Nokia A032. This may be because it is not a radio card or because it is an incompatible radio card.

110011: Bad radio (does not initialize)

Indicates that the PCMCIA radio card does not respond to initialization requests. This may indicate that the card is faulty. Try using an alternative radio card.

110100: Bad firmware version

Indicates that the PCMCIA radio card has an incompatible version of firmware loaded. The manufacturer of the radio card will normally supply utilities to allow you to upgrade the firmware in the cards to the required version.

001000: Bad DRAM (stuck address)
001001: Bad Ethernet RAM (stuck address)

Indicates a hardware memory problem in the unit. Unit must be repaired by dealer.

001010: Bad CMOS memory

Indicates that the configuration memory had a checksum error. This memory is used to store the optional settings for the unit. If a checksum error is encountered the Nokia A032 will automatically re-load the default configuration parameters.

101000: LAN controller error

Indicates failure of the Ethernet interface. Unit must be repaired by dealer.

011000: Bad configuration

Indicates that the configuration information is bad.

011001: Bad manufacturer's information

Indicates that the internal configuration information has been corrupted. Contact Nokia Technical Support.

011010: Bad log sector

Indicates that the log information in the flash memory has been corrupted. In this case the Nokia A032 will automatically restore an empty log file. The original log and NID name information will be lost but the unit will proceed with initialization.

011011: System error

Indicates failure of initialization due to an unknown cause. If this persists the unit must be returned to the dealer for repair.

Using the Initialization log file

The Initialization log file keeps a record of each time the Nokia A032 is restarted. You can use it to diagnose start-up problems.

During initialization, as each part of the system is started, entries are made in the log. If the startup is successful the resulting log file changes are written into the flash memory as a record of the event.

Note: *The log file only records successful initializations. If the Nokia A032 is failing to initialize, see page 183.*

The log file can hold data from approximately 30 restarts. After this the oldest entries are overwritten by new entries. To keep a more permanent record, upload the log file periodically using TFTP and save it to disk – see *Using the TFTP client program* on page 105.

An example log file

An example log file is shown below:

```
 Message :  CLM Request

Initializing version: B4.00.01 on Fri, 12 May 2000 11:27:16
Initialize LAN port...
LAN Port ready, Message :  Web Request

Initializing version: B4.00.01 on Fri, 12 May 2000 11:28:22
Initialize LAN port...
LAN Port ready,
Initializing version: B4.00.01 on Fri, 12 May 2000 11:30:14
Initialize LAN port...
LAN Port ready,
```

A log file shows the following information:

- The first line of an entry shows the time at the restart and records the version of Nokia A032 software (in this case 3.00).
- The next few lines show the progress of initialization. First the LAN port is initialized. Next the radio card is initialized. As part of radio card initialization, the log records the firmware version of the radio card.
- After the radio is initialized the unit is operating normally.

Real-time troubleshooting via the serial port

If there is a problem during initialization the Nokia A032 may stop and display an error code on the **info** LEDs. This presents two problems.

- You can’t view the contents of the log file because the Nokia A032 is not operating.
- The log file does not get updated with information because the file update only occurs after successful initialization.

To provide a solution to this problem, the Nokia A032 also writes all log file entries to the serial port *during* initialization. If the unit fails to initialize and you can’t discover the problem, try attaching a serial terminal to the unit.

Connect a serial terminal to the serial port with the following settings:

Baud rate: 9600 bps
#bits: 8
No parity

This will result in the display of progress messages. You’ll see log messages written to the terminal – these might provide useful information.

Typical error messages

Some examples of error messages that might be displayed on a serial terminal are:

- `PCMCIA hardware failure`
- `No PCMCIA card detected`
- `Non compatible PCMCIA card`
- `Cannot initialize radio`
- `Incorrect firmware version`
- `Memory error type 1`
- `Memory error type 2`
- `Configuration error – default loaded`
- `LAN Interface Error`
- `Configuration error`
- `Bad unit checksum`
- `Log sector bad – recovered`
- `System fault.`

Troubleshooting dial-up connections

The Nokia A032 uses PPP to connect and send data to an ISP. A basic understanding of its operation may be helpful if you're having problems with a dial-up connection.

There are four phases to the connection process:

1. Dialling the ISP phone number.

   This phase checks the compatibility of the modem on the other end of the phone line and negotiates the speed of the connection based on the quality of the phone line.
2. Talking to the ISP server and agree that it can use the PPP protocol.
3. Identifying the user to the ISP by sending a username and password.
4. Agreeing the IP addresses that will be used during the session.

If all four steps complete the Nokia A032 will be able to deliver and receive IP packets to and from the Internet.

We'll look at each phase in detail and highlight possible problems. You might find it helpful to view the PPP Log screen (see page 21).

Dialing phase

What happens	Possible problems and solutions
The Nokia A032 looks for a modem. The first required indication is that the DTR (Data terminal ready) signal at the serial port is active. This tells the Nokia A032 that there is a device connected to the serial port.	Verify that the DSR signal is active by viewing the Modem Status screen (see page 19) – the DTR box should be red. If it is blue ensure that the modem is powered on; check the cable connecting the modem to the Nokia A032.
After DSR is detected the Nokia A032 attempts to communicate with the modem using the industry standard AT command set.	If this step fails, make sure the modem is in its factory default state. Most modems automatically adapt to the data rate of the computer to which they are attached. If your modem has a fixed data rate you may need to specify that in *Advanced Internet Access setup (modem)* on page 51.
The Nokia A032 sends a reset command to the modem and then, optionally, sends a user-defined initialization string.	Most modems do not need an initialization string. However, if you are having problems, check the Nokia support site for more information on this.
The Nokia A032 issues the command to dial. You should hear the modem dialling and attempting to connect. If, successful the modem will notify the Nokia A032 and proceed to the next stage.	If the line is busy or you've specified the wrong ISP number, the connection will fail. One possible failure at this point is that the modem uses an unusual message to indicate connection. The last message received can be seen in the Modem Status web management screen (see page 19). It should normally contain the word "Connected". If not, you may need to use a special initialization string to get the correct message.

LCP phase

What happens	Possible problems and solutions
The Nokia A032 and the ISP agree to use PPP and negotiate the various options that might be available to improve efficiency. This phase of negotiation uses *Link Configuration Protocol* (LCP).	Looking in the PPP Log (see page 21) you should see entries labelled 'LCP' and identified as `configure request`, `configure reject` and `configure NAK`. These entries are normal and part of the bartering process. However, if the two sides are unable to agree one will eventually give up and drop the link. • If you see a long sequence of LCP messages followed by a hangup then there is probably a compatibility problem between the ISP and the Nokia A032. In this case you should contact Nokia technical support for advice. • If the PPP Log contains configure requests but no replies, the ISP either doesn't support PPP or needs some special procedure to turn on PPP. This will generally only be the case with older ISPs, although it may include some quite large services. In this case it may be necessary to use a *script* to log in and tell the ISP that you want to use PPP (see *Setting a logon script* on page 55.

The LCP phase will complete when both sides have sent an LCP configure request to the other and received an LCP configure ACK in reply.

Authentication phase (logging in)

Almost all ISPs require you to identify yourself by logging in after the LCP phase is complete.

What happens	Possible problems and solutions
The Nokia A032 will send the user name and password which you have previously configured. If the login is accepted you will see an `accept` message in the PPP log.	If the login is not accepted, you will either see a reject message in the PPP log, or the line will just be dropped by the ISP. If your password is not accepted there may be several causes including: • *Incorrect capitalization* With most ISPs, the password open is not considered the same as Open. • *Missing prefix* Sometimes the username needs to be prefixed with a network identifier. For example, an ISP called Fastnet Inc. might require the user name to be prefixed with the string FSN/. Check with your ISP. • *Login script required* The ISP does not accept logging in via PPP and requires the use of a login script. See *Setting a logon script* on page 55.

IPCP phase

The ISP agrees or assigns the IP address information you will use on its network.

What happens	Possible problems and solutions
In most cases, the ISP will send the IP address information to the Nokia A032 to use as its *external* IP address (see *Appendix H*). The negotiation during this phase is done in a similar way to the LCP negotiation. However, in this case the protocol is called *IP Configuration Protocol* (IPCP).	If the ISP fails at this point of the negotiation: • you may have programmed incorrect values in the Nokia A032, or • the ISP is unable to provide IP information automatically.

Resetting factory defaults

If you don't know the Nokia A032's current configuration status and you want to ensure that you are starting from a clean and known state, you can restore the factory default settings.

You might want to do this before using Learn mode to configure the Nokia A032.

Assuming the Nokia A032 is not security locked (see page 79 and page 45) you can use the following procedure:

1. Put the Nokia A032 into Learn mode (see the *Getting Started* guide).
2. Hold in the **mode** button.

   The LEDs perform a binary count, slowly coming on from left to right.
3. Keep holding the **mode** button until all the LEDs are on. This takes about 10 seconds.

The unit has now overwritten the configuration with the factory defaults; it should restart. Remember to hold the **mode** button again when the unit restarts if you want to return to Learn mode.

Appendix G – Upgrading

Important!! *You need a null-modem cable (also known as a data transfer cable) to communicate via the serial port.*

This appendix explains how to use the Nokia Access Point Upgrade utility to upgrade your Nokia A032 via a PC workstation connected to the serial port via a null-modem cable (also known as a data transfer cable).

You would do this in the following cases:

- If your client machine doesn't have TCP/IP installed; in this case you can't use TFTP to upgrade the Nokia A032 via the LAN
- If you need to upgrade the Nokia A032's system BIOS; the Nokia Access Point Upgrade utility is the only way to do this.

Note*: Upgrading the system BIOS should only be done on instructions from Nokia or your dealer.*

The Nokia Access Point Upgrade utility only runs under Microsoft Windows 95/98/2000 or NT.

Overview

The Nokia A032 uses flash memory for storage of important information including the operating firmware of the unit. Flash memory has the advantage that the memory contents are not lost when the unit is powered off. However, the contents can be changed by a special procedure. This allows the firmware in the unit to be upgraded in the field – a big advantage.

In addition to the flash memory, the Nokia A032 stores configuration information in special RAM called *non-volatile RAM*.

The Nokia A032 memory is organized into four parts:

- System BIOS – The system BIOS performs diagnostic checks after powerup and is the basic brains of the unit.
- Main firmware (called *img1*) – The main firmware is the software which performs the access point functions. When you upgrade the Nokia A032, this software can be overwritten using a special procedure.
- Log file, NID and Bridge name storage – The Log file keeps track of system information each time the unit is started. Information entered using the `nid add` or `bridge add` commands is also stored in this portion.
- Configuration information – This stores all the current operating parameters.

Using the Nokia Access Point Upgrade utility, you can upgrade the firmware and the BIOS. It is important to note that upgrade is not a required operation – in fact most users will not need to upgrade the unit.

Nokia Access Point Upgrade utility

You use the Nokia Access Point Upgrade utility to download new firmware (`img1`).

The Nokia Access Point Upgrade utility is also the only method of upgrading the system BIOS. Upgrading the system BIOS should only be done on instructions from Nokia or your dealer.

Upgrading the Nokia A032

This section explains how to use the Nokia Access Point Upgrade utility to upgrade the Nokia A032.

Connecting the PC workstation

Use the Nokia Access Point Upgrade utility to establish communication between a PC workstation and the Nokia A032:

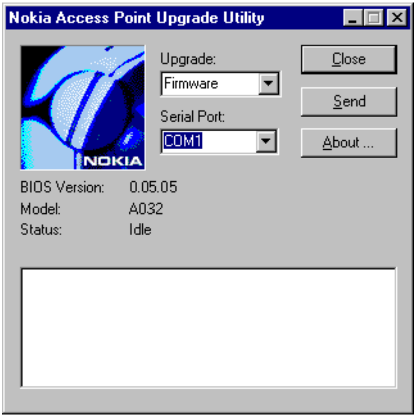
1 Make sure you have installed the Nokia utilities onto the PC workstation, as described in *Appendix D*.

2 Connect a serial cable between the PC and the Nokia A032.

Important!! The serial cable should be of the *null-modem* or *data transfer* type.

3 Choose **Start > Programs > Nokia Access Point Upgrade.**

You'll see the Nokia Access Point Upgrade utility window:



Upgrade: Firmware
Serial Port: COM1

BIOS Version: 0.05.05
Model: A032
Status: Idle

Initially, you'll see
`Status: Access Point not ready`

4 Select the correct **Serial Port** (e.g. **`COM1`**).

Steps 4-7: Restart the Nokia A032 in BIOS communication mode.

5 Switch off the Nokia A032.

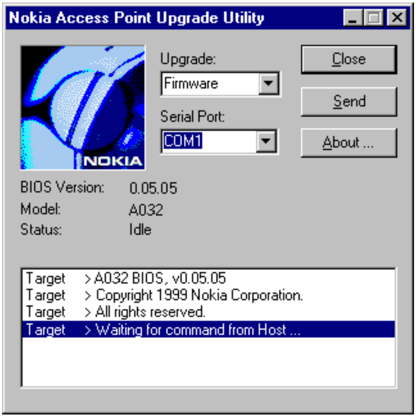
6 Press and hold the **mode** button and switch the unit on again. Continue to hold the **mode** button while the **info** LEDs all switch on, then go off. This takes about five seconds.

7 *Keep holding the button* until the **info** LEDs come on again. This happens about 5 seconds after they have gone off.

8 When the **info** LEDs come on again, release the button.

Assuming you have the correct serial cable and COM port a message will appear in the Nokia

Access Point Upgrade utility window and the status will indicate `Idle`.



Upgrade: Firmware

Serial Port: COM1

BIOS Version: 0.05.05

Model: A032

Status: Idle

```
Target    > A032 BIOS, v0.05.05
Target    > Copyright 1999 Nokia Corporation.
Target    > All rights reserved.
Target    > Waiting for command from Host ...
```

You’re now ready to upgrade the Nokia A032.

Performing the upgrades

In order to perform the following upgrades you must have the correct files in the same directory as the Nokia Access Point Upgrade utility.

These will have been extracted automatically as part of the utilities installation process (see *Appendix D*), or may be supplied as an update from Nokia.

For example, the firmware file may be called something like `03_A032.bin`.

If you do not have the required file for a given upgrade, the appropriate option in the Nokia Access Point Upgrade utility window will not appear.

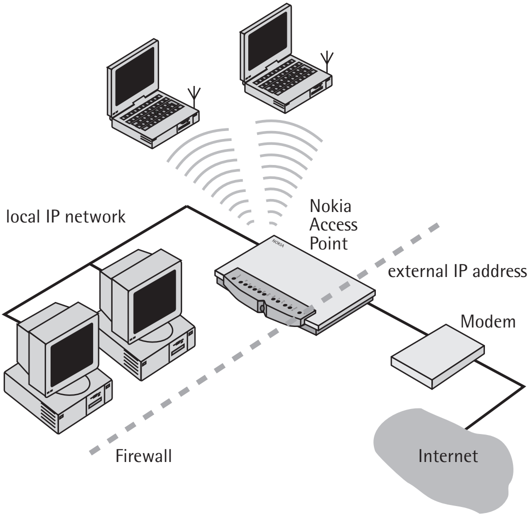
To perform an upgrade:

1. Select the appropriate option (**Firmware** or **BIOS**) from the **Upgrade** drop-down menu in the Nokia Access Point Upgrade utility window.
2. Click **Send**.

   You'll see a status bar indicating progress.
3. When the upgrade is complete, restart the Nokia A032 in normal mode.

Appendix H – NAT setup

The Nokia A032 can provide *NAT firewall* security, preventing unwanted access to your network from external Internet users.



The NAT firewall converts all IP addresses on your local network into a single *external* IP address for use on the intranet or Internet. Users outside the firewall have no visibility of the real IP address of your network.

The Nokia A032 refuses any external attempts to access your PC directly. It only accepts data sent to the external address (the Nokia A032 is the only device that knows how to convert the address back to that of a device on your internal LAN).

The NAT function normally works in conjunction with the dial-up networking function. Most ISPs allocate an IP address dynamically to a computer that dials in. The Nokia A032 uses that IP address as the external IP address to represent your LAN.

However, an advanced feature of the Nokia A032 is the ability to put the NAT firewall between the wireless and wired LAN, instead of using a modem connection.

Setting the NAT port

You can use the CLM (see page 67) or the Web interface (see page 43) to select the NAT port. This section uses the CLM point of view.

To set the NAT port, enter:

```
set nat_port parameter
```

where *parameter* can be one of the following:

- **off** – (this is the default) disables the NAT function if Internet access is not required
- **modem** – enables the NAT firewall function when using dial-up Internet access
- **LAN** – see below
- **radio** – see below.

LAN and radio port options

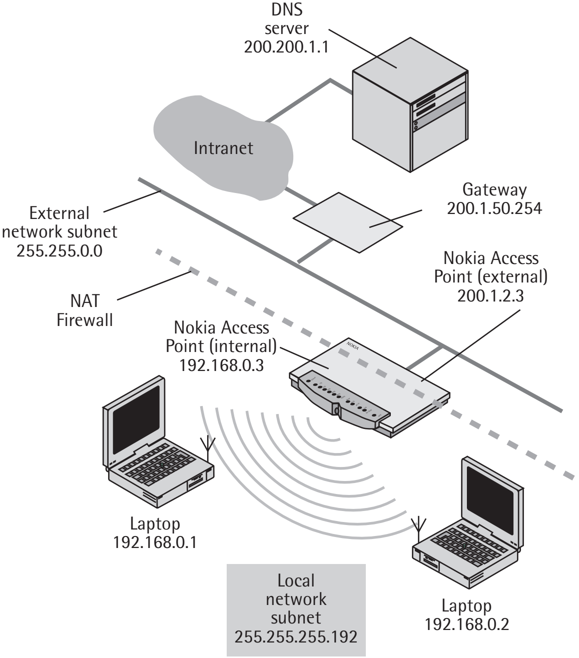
Some applications require the NAT function to be placed at the LAN or air (radio) interface. For example, an office workgroup could connect to a corporate LAN but have a locally administered IP domain by putting the NAT function on the LAN interface.

nat_subnet and nat_gateway

When the NAT port is set to `LAN` or `radio` the interface does not use PPP. Instead, the LAN on the other side of the NAT firewall is called the *external LAN*. The values of the gateway and subnet mask must be defined for the IP domain on the external LAN:

```
set nat_gateway gateway
set nat_subnet subnet
```

Both the above are set to 0.0.0.0 by default.


DNS
server
200.200.1.1
Intranet
Gateway
200.1.50.254
External
network subnet
255.255.0.0
Nokia Access
Point (external)
200.1.2.3
NAT
Firewall
Nokia Access
Point (internal)
192.168.0.3
NOKIA
Laptop
192.168.0.1
Local
network
subnet
255.255.255.192
Laptop
192.168.0.2

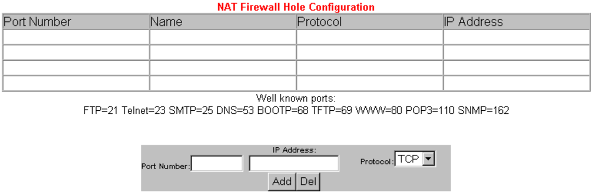
Setting NAT holes – providing external access

Note: *This function is only useful if you have a static IP address assigned to you by your ISP.*

Under normal operation the NAT firewall only allows sessions initiated from the local LAN or WLAN network (inside the firewall).

In certain cases you might want to allow users outside your firewall (i.e. on the public Internet or external LAN) access to resources on your local LAN, such as a web site or an FTP server. **You can only do this if your ISP allows you to have a static IP address assigned to the external interface.**

You can use the browser interface (page 54) to define a *NAT hole table* with up to four holes:



NAT Firewall Hole Configuration

Port Number	Name	Protocol	IP Address

Well known ports:
FTP=21 Telnet=23 SMTP=25 DNS=53 BOOTP=68 TFTP=69 WWW=80 POP3=110 SNMP=162

Port Number: [ ] IP Address: [ ] Protocol: TCP

A NAT hole defines a route through your NAT firewall to access one particular device.

For each NAT hole, you need to specify the following:

The port number selects the required service and distinguishes, for example, Web server requests from FTP requests.

Parameter	Description
Port number	Here are some well-known port assignments: • 21 – FTP • 23 – Telnet • 25 – SMTP • 53 – DNS • 68 – BOOTP • 69 – TFTP • 80 – WWW • 110 – POP3 • 162 – SNMP
Protocol	The protocol to be used (e.g. TCP).
IP Address	The IP address of the machine hosting the service on your local network.

As an example, if you set the following NAT hole parameters:

Port number: 80
Name: WWW
Protocol: TCP
IP address: 192.168.0.77

and your static external IP address is 200.1.2.3, an external user would enter the following URL:

```
http://200.1.2.3
```

but would actually access port 80 on machine with IP address 192.168.0.77. The NAT firewall would make the required address translation.

Index