LANCOM 3850 UMTS

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. LANCOM Systems shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software included with this product is subject to written permission by LANCOM Systems. We reserve the right to make any alterations that arise as the result of technical development.

All explanations and documents for registration of the products you find in the appendix of this documentation, if they were present at the time of printing.

Trademarks

Windows®, Windows Vista™, Windows XP® and Microsoft® are registered trademarks of Microsoft, Corp.

The LANCOM Systems logo, LCOS and the name LANCOM are registered trademarks of LANCOM Systems GmbH. All other names mentioned may be trademarks or registered trademarks of their respective owners.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit http://www.openssl.org/.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

The firmware of LANCOM VP-100 incorporates components available in source code as Open Source software with specific licenses and copyrights of various authors. In particular the firmware incorporates components which are subject to the GNU General Public License, version 2 (GPL). The license agreement including the text of the GPL can be found on the product CD in the product folder as LC-VP100-License-EN.txt. The source codes and all license texts can be obtained from LANCOM Systems GmbH FTP server electronically upon request.

Subject to change without notice. No liability for technical errors or omissions.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Wuerselen

Germany

www.lancom.eu

Wuerselen, September 2007

110536/0907

EN

Preface

Thank you for placing your trust in this LANCOM product.

The combination of UMTS/HSDPA, WLAN, DSL and VPN opens up a completely new range of possibilities in enterprise connectivity—for example, mobile conference rooms that are connected via UMTS/HSDPA and offer Internet access over WLAN or access to the company network via VPN.

As a back-up connection for site coupling, UMTS/HSDPA is cheaper and faster than the conventional alternative, ISDN. Furthermore, it is significantly less prone to failure as there are no cables which are at risk from construction works. Using VRRP with the LANCOM 3850 UMTS offers fully vendor-independent high availability and a completely transparent, automatic switch of media in the event of backup.

Apart from that, UMTS/HSDPA is able to bridge the "last mile" for customers who do not have access to an equivalent broadband connection. The UMTS/HSDPA card is simply operated in the CardBus expansion slot of the LANCOM 3850 UMTS. The device automatically switches Internet access between HSDPA, UMTS and GPRS depending on availability.

Security settings

To maximize the security available from your product, we recommend that you undertake all of the security settings (e.g. firewall, encryption, access protection) that were not already activated when you purchased the product. The LANconfig Wizard 'Security Settings' will help you with this task. Further information is also available in the chapter 'Security settings'.

We would additionally like to ask you to refer to our Internet site www.lancom.eu for the latest information about your product and technical developments, and also to download our latest software versions.

User manual and reference manual

The documentation of your device consists of the following parts:

- Installation guide
- User manual
- Reference manual

You are now reading the user manual. It contains all information you need to put your device into operation. It also contains all of the important technical specifications.

EN

The reference manual can be found on the LANCOM product CD as an Acrobat (PDF) document. It is designed as a supplement to the user manual and goes into detail on topics that apply to a variety of models. These include, for example:

- The system design of the operating system LCOS
- Configuration
- Management
- Diagnosis
- Security
- Routing and WAN functions
- Firewall
- Quality of Service (QoS)
- Virtual Private Networks (VPN)
- Virtual Local Networks (VLAN)
- Wireless networks (WLAN)
- Backup solutions
- Further server services (DHCP, DNS, charge management)

This documentation was created by …

… several members of our staff from a variety of departments in order to ensure you the best possible support when using your LANCOM product.

In case you encounter any errors, or just want to issue critics enhancements, please do not hesitate to send an email directly to:
info@lancom.eu

Our online services www.lancom.eu are available to you around the clock should you have any queries regarding the topics discussed in this manual or require any further support. The area 'Support' will help you with many answers to frequently asked questions (FAQs). Furthermore, the knowledgebase offers you a large reserve of information. The latest drivers, firmware, utilities and documentation are constantly available for download.
In addition, LANCOM support is available. For telephone numbers and

contact addresses of LANCOM support, please see the enclosed leaflet or the LANCOM Systems website.

Information symbols	
	Very important instructions. Failure to observe this may result in damage.
	Important instruction that should be observed.
	Additional information that may be helpful but which is not required.

EN

Contents

EN

EN

EN

1 Introduction

1.1 What is a Wireless LAN?

The following sections describe the functionality of wireless networks in general. The functions supported by your device are listed in the table 'What can your LANCOM do?'. Detailed information on Wireless LANs can be found in the LCOS reference manual.

A Wireless LAN connects single terminals (e.g. PCs or notebooks) to a local network (also LAN – **L**ocal **A**rea **N**etwork). In contrast to a conventional LAN, communication takes place via radio links rather than via network cables. This is the reason why a Wireless LAN is also called a **W**ireless **L**ocal **A**rea **N**etwork (WLAN).

All functions of a cable-bound network are also available in a Wireless LAN: access to files, servers, printers etc. is as possible as the connection of individual stations to an internal mail system or to the Internet access.

The advantages of Wireless LANs are obvious: notebooks and PCs can be set up just where they are needed. Due to Wireless LANs, problems with missing connections or structural alterations belong to the past.

Apart from that, wireless LANs can also be used for connections over longer distances. Expensive leased lines and the associated construction measures can be spared.

1.1.1 Which hardware to use?

Each station of the Wireless LAN needs access to the Wireless LAN in the form of a wireless interface. Devices which have no built-in wireless interface can be upgraded with a supplement card or an adapter.

LANCOM Systems offers wireless adapters by its LANCOM product line. An LANCOM wireless adapter enables a device (e.g. PC or notebook) for access to the Wireless LAN.

1.1.2 Operation modes of Wireless LANs and base stations

Wireless LAN technology and base stations in Wireless LANs are used in the following operation modes:

- Simple direct connections between terminals without base station (ad-hoc mode)

- Larger Wireless LANs, connection to LANs with one or more base stations (infrastructure network)
- Setting-up of an Internet access
- Connecting two LANs via a direct radio link (point-to-point mode)
- Connecting of devices with Ethernet interface via base stations (client mode)
- Extending an existing Ethernet network with WLAN (bridge mode)
- Relay function for connecting networks via multiple access points.
- Central Management with a LANCOM WLAN Controller

1.2 The advantages of the UMTS/HSPDA solution

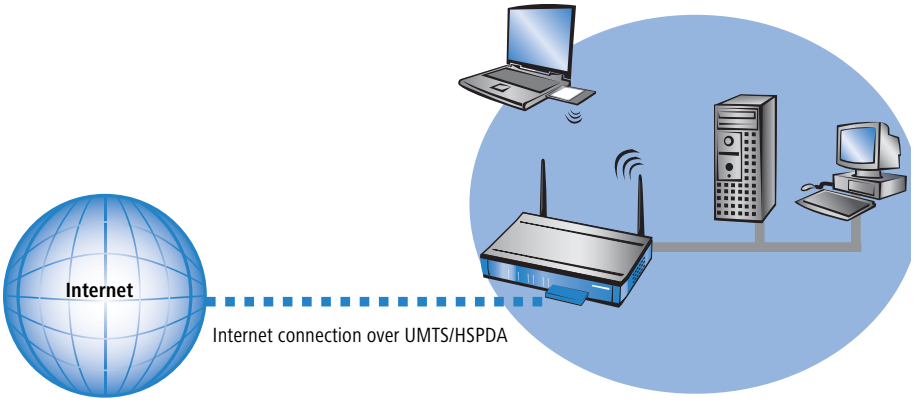
The combination of UMTS/HSPDA, WLAN, DSL and VPN opens up a completely new range of possibilities in enterprise connectivity—for example, mobile conference rooms that are connected via UMTS/HSPDA and offer Internet access over WLAN or access to the company network via VPN. As a back-up connection for site coupling, UMTS/HSPDA is cheaper and/or faster than the conventional alternatives, ISDN and Analog. Furthermore, it is significantly less prone to failure as there are no cables which are at risk from construction works. Apart from that, UMTS/HSPDA is able to bridge the "last mile" for customers who do not have access to an equivalent broad-band connection.

The UMTS/HSPDA card is simply operated in the CardBus expansion slot of the appropriate LANCOM devices. The device automatically switches Internet access between UMTS/HSPDA and GPRS depending on availability.

1.2.1 "Last mile" via UMTS/HSPDA

The Internet connection over UMTS/HSPDA is recommendable wherever a broadband Internet connection is not available. When accessing the Internet with UMTS/HSPDA you can currently reach significant higher downstream rates than with an ISDN connection.

EN



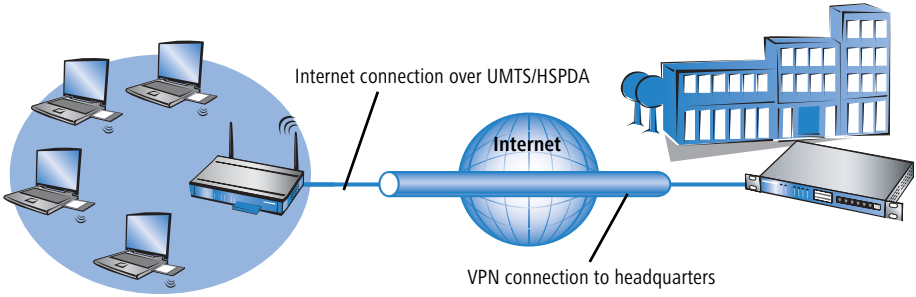
For a regular Internet connection over UMTS/HSPDA, various net providers offer so called "homezone" tariffs. With this tariff the data transfer within the homezone radio cell is usually far below the costs of the usual mobile tariffs where the data card is used in multiple radio cells.

A special application is the use of a WLAN Access Point with UMTS/HSPDA connection and LANCOM UMTS/VPN Option as a HotSpot in places without Internet via cable.

1.2.2 Mobile conference room

The modern business world requires ever increasing mobility from a growing number of employees. That means that a constant access to e-mails, Internet or to servers at headquarters is becoming more and more important.

A WLAN access point with UMTS/HSPDA connection provides the required flexibility for people who often work in different places. Nearly every modern notebook has a WLAN interface; the only thing missing for mobile Internet or VPN access is a WAN interface. With the wireless Internet access over UMTS/HSPDA or GPRS, mobile working areas can be created very easily.



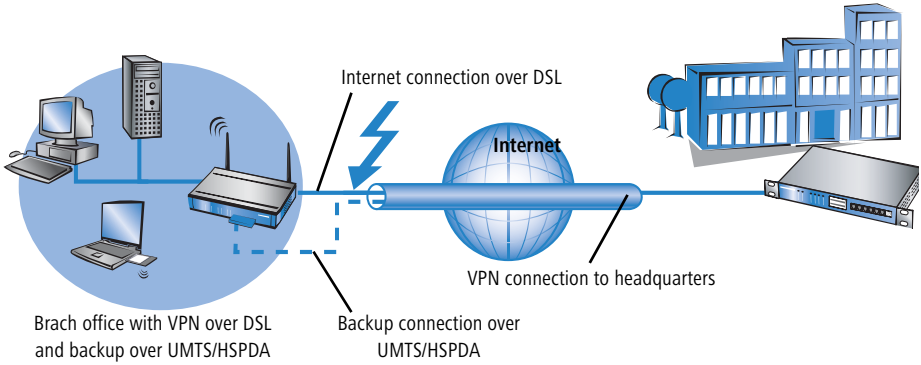
Mobile WLAN, e.g. for a „mobile conference room".

For a group of staff members, who e.g. often work together on projects at a customer's location, a so-called mobile conference room can be established. The access point then only has to be configured once by the administrator; the staff members on location simply have to supply the device with power and slot in the data card. With an appropriate configuration the router automatically builds up a connection to the Internet. The result is that all notebooks with a compatible passphrase in the WLAN configuration can directly access the Internet. As long as the router has a VPN connection to headquarters, the field staff can also access all of the services in the network of headquarters (fileserver, mailserver, data bases) from the mobile office.

With the LANCOM UMTS/VPN Option the VPN support with five connection channels is automatically activated. Further information to the configuration can be found in the LCOS reference manual.

1.2.3 UMTS/HSPDA Backup

The high availability of data lines e. g. between branch offices and headquarters in large company networks are in the majority of cases established over backup solutions with ISDN or analog. The standard Internet connection is then provided e. g. over a DSL connection, and an ISDN or analog line is used as a backup line in the case the DSL line breaks down.



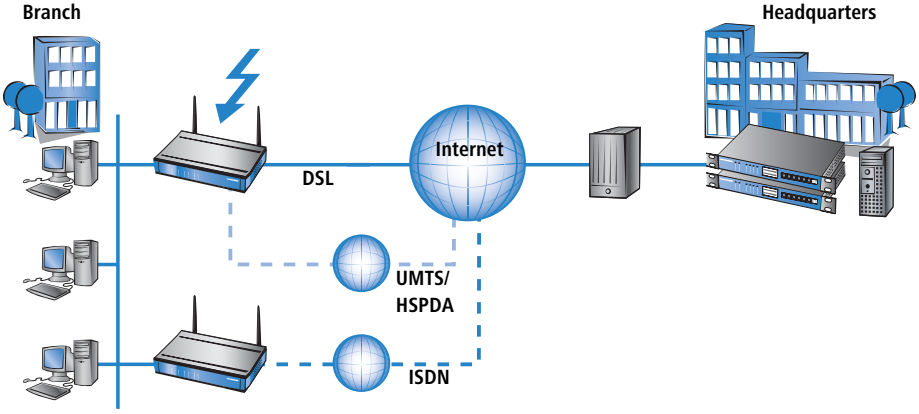
As an alternative to the ISDN or analog backup method, a UMTS/HSPDA connection can assure the availability of the data connection. If the connection to the Internet is established by a router with LANCOM UMTS/VPN Option, the UMTS/HSPDA connection can directly replace the DSL connection in the case of a breakdown. The advantages of the UMTS/HSPDA backup solution compared to the ISDN/analog option:

- Faster than ISDN/analog: the data rate with UMTS/HSPDA is considerably faster.
- Safer than ISDN or analog: if a physical damage of the DSL line is the reason for the breakdown, the ISDN/analog line usually breaks down as well because both use the same physical line.
- Cheaper than ISDN: the monthly charges for an UMTS/HSPDA account depend upon the tariff well under the charges for an ISDN account. Compared to the short time of breakdown of a DSL connection, the higher connection tariffs for the UMTS/HSPDA are not relevant.

Adding the UMTS/HSPDA backup to existing installations is often simply an issue of adding devices with LANCOM UMTS/VPN Option to existing LANCOM devices. In complicated scenarios an existing ISDN backup in a VPN router can be extended by the UMTS/HSPDA backup in a second device. In this case, the routers will exchange the information about accessible routes using the "Routing Information Protocol" (RIP).

A sophisticated backup system for protection against router hardware failure can be implemented by using VRRP. Two or more routers are installed in a network, one of which can replace the other in case of device failure. In addition to normal VRRP, LANCOM devices can link the backup event triggering function to the availability of a data connection. With this additional feature,

LANCOM devices with more than one WAN interface (e.g. DSL and UMTS/HSPDA interface) can be implemented flexibly in backup solutions. The backup event is triggered for example, when the default route is no longer available via the DSL interface. The device's UMTS/HSPDA interface can take its place further along in the backup chain should the backup router also fail.



Further information to the configuration of backup lines can be found in the LCOS reference manual.

1.3 What can your LANCOM Wireless Router do?

The following list shows you properties and functions of your device

	LANCOM 3850 UMTS
Applications	
Internet access	✔
IP router with Stateful Inspection Firewall	✔
DHCP and DNS server (for LAN and WAN)	✔
VPN gateway	✔
UMTS/HSPDA function for internet connection, as mobile conference room or as backup solution	✔
LAN-LAN coupling over VPN	✔

EN

	LANCOM 3850 UMTS
RAS server (over VPN)	✔
Wireless LAN	
Wireless transmission by IEEE 802.11g / IEEE 802.11b or wireless transmission by IEEE 802.11a	✔
Simultaneous dual band operation possible with additional radio card	✔
Point-to-point mode (six P2P paths can be defined per WLAN interface)	✔
Relay function to link two P2P connections	✔
Turbo Mode: Double the bandwidth at 2.4 GHz and 5 GHz.	✔
Super AG incl. hardware compression and bursting	✔
Multi SSID	✔
Roaming function	✔
802.11i / WPA with hardware AES encryption	✔
WEP encryption (up to 128 Bit key length, WEP152)	✔
IEEE 802.1x/EAP	✔
MAC address filter (ACL)	✔
Individual passphrases per MAC address (LEPS)	✔
Closed network function	✔
Integrated RADIUS server	✔
VLAN	✔
Traffic lock function	✔
QoS for WLAN (IEEE 802.11e, WMM/WME)	✔
WLANmonitor for visualization of access points and clients in larger WLANs	✔
WLAN group configuration for simultaneous configuration of multiple devices	✔

EN

	LANCOM 3850 UMTS
Connection to the LAN	
Fast-Ethernet-connection (10/100base-TX)	✔
Power-over-Ethernet (PoE)	✔
DHCP and DNS server	✔
Connection to the WAN	
WAN connection for DSL or cable modem	✔
UMTS/HSPDA connection via UMTS card in CardBus slot	✔
USB connector	
USB 2.0 host port (full speed: 12 Mbps) for connecting a USB printer and for future extensions	✔
Internet access (IP router)	
Stateful Inspection Firewall	✔
Firewall filter (address, port)	✔
IP masquerading (NAT, PAT)	✔
Quality of Service	✔
Digital certificates (X.509) incl. PKCS#12	✔
Advanced Routing and Forwarding (ARF networks)	8
N:N mapping for routing networks with the same IP-address ranges over VPN	✔
Policy-based routing	✔
Load balancing for bundling multiple DSL channels	2 channels
Backup solutions and load balancing with VRRP	✔
PPPoE server	✔
WAN RIP	✔
Rapid Spanning Tree Protocol	✔
Layer-2 QoS Tagging	✔

EN

	LANCOM 3850 UMTS
802.1p	✔
NAT Traversal (NAT-T)	✔
DMZ with configurable IDS checks	✔
Power supply	
12 V via separate power adapter (DC)	✔
Power-over-Ethernet (PoE) according to the standard IEEE 802.3af	✔
Configuration and firmware	
Configuration with LANconfig or with web browser, additionally terminal mode for Telnet or other terminal programs, SNMP interface and TFTP server function., SSH connection.	✔
Configuration wizards	✔
1-Click-VPN wizard for easiest setup of RAS access and site-to-site LAN coupling via VPN	✔
Serial configuration interface	✔
FirmSafe with firmware versions for absolutely secure software upgrades	✔
Optional software extensions	
LANCOM Public Spot Option	✔
LANCOM VPN Option with 25 active tunnels for protection of network couplings	✔
Optional hardware extensions	
AirLancer Extender antennas for extended range	✔
AirLancer MC-54 PC card for extension to a second radio cell (dual band)	✔
LANCOM ES-1108P PoE switch for Ethernet cabling; simultaneously supplies power over Ethernet	✔
Lightning-protection adapters SA-5 and SA-LAN	✔

2 Installation

2.1 Package contents

Please check the package contents for completeness before starting the installation. In addition to the LANCOM Wireless Router itself, the package should contain the following accessories:

	LANCOM 3850 UMTS
12V DC Power adapter	✔
Dual-band diversity antennas	2
PoE LAN connector cable (green plugs)	✔
DSL connector cable (deep blue plugs)	✔
Connector cable for the configuration interface	✔
Enclosure for cardbus slot	✔
LANCOM CD	✔
Printed documentation	✔

If anything is missing, please contact your retailer or the address stated on the delivery slip of the unit.

2.2 System requirements

2.2.1 Configuring the LANCOM devices

Computers that connect to a LANCOM must meet the following minimum requirements:

- Operating system that supports TCP/IP, e.g. Windows Vista™, Windows XP, Millennium Edition (Me), Windows 2000, Windows 98, Linux, BSD Unix, Apple Mac OS, OS/2.
- Access to the LAN via the TCP/IP protocol.

The LANtools also require a Windows operating system. A web browser under any operating system provides access to WEBconfig.

EN

2.2.2 Operating access points in managed mode

LANCOM Wireless Routers and LANCOM Access Points can be operated either as self-sufficient Access Points with their own configuration ("Access Point mode") or as components in a WLAN infrastructure, which is controlled from a central WLAN Controller ("managed mode").

For operation in managed mode the Access Points require firmware of version 7.22 or higher and a current loader (version 1.86 or higher).

2.3 Status displays, interfaces an hardware installation

2.3.1 Status display

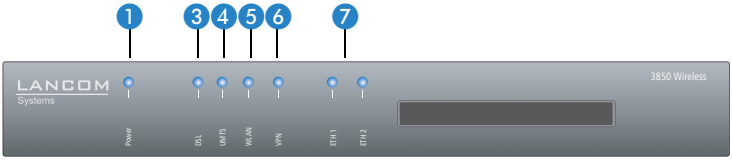
Meanings of the LEDs

In the following sections we will use different terms to describe the behaviour of the LEDs:

- **Blinking** means, that the LED is switched on or off at regular intervals in the respective indicated colour.
- **Flashing** means, that the LED lights up very briefly in the respective colour and stay then clearly longer (approximately 10x longer) switched off.
- **Inverse flashing** means the opposite. The LED lights permanently in the respective colour and is only briefly interrupted.
- **Flickering** means, that the LED is switched on and off in irregular intervals.

Front side

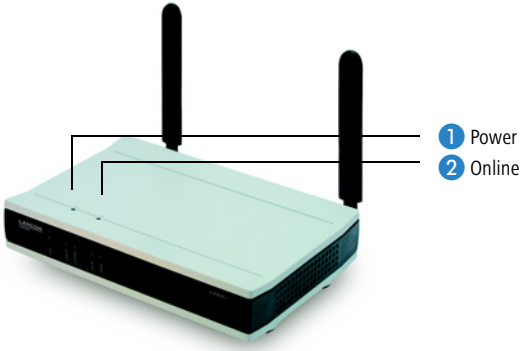
The LANCOM Wireless Routers have status displays on the front panel.



EN

Top panel

Two additional LEDs on the top panel provide a convenient overview of the most important status information, especially when the device is mounted vertically.



1 Power

This LED provides information on the device's operating state. After being switched on, it blinks green during the self-test. The LED then shines constantly to indicate operational readiness, unless an error is detected as indicated by a code blinked in red.

Off		Device switched off
Green	Blinking	Self-test after power-up
Green	On (permanently)	Device operational
Red/green	Blinking alternately	Device insecure: Configuration password not set
Orange/green	In the housing cover; blinking alternately with the online LED	At least one WLAN module is in managed mode and has not found a WLAN Controller yet. The corresponding WLAN module(s) is/are switched off until a WLAN Controller is found to supply a configuration, or until being switched manually into another operating mode.
Orange /red	In the housing cover; blinking alternately with the online LED	At least one WLAN module is in managed mode and has found a WLAN Controller. However, the WLAN Controller cannot assign a configuration because the firmware and/or the device's loader version is not compatible with the WLAN Controller.
Red	Blinking	Charge limit for online connections reached

The power LED blinks alternately in red/green until a configuration password has been set. Without a configuration password, the configuration data in the LANCOM are unprotected. Normally you would set a configuration password during the basic configuration (instructions in the following chapter). Information about setting a configuration password at a later time is available in the section 'The Security Wizard'.

EN

The power LED is blinking and no connection can be made?

Signal that a charge or time limit has been reached

If the power LED blinks red and no WAN connections can be established, there is no cause for concern. This merely means that a pre-set charge or time limit has been reached.

There are three ways to remove the lock:

- Reset the toll protection.
- Increase the limit.
- Deactivate the lock completely (set limit to '0').

LANmonitor shows you when a charge or time limit has been reached. To reset the toll protection, activate the context menu (right-mouse click) **Reset charge and time limits**. The charge settings are defined in LANconfig under **Management** ▶**Costs** (these settings are only available if the 'Complete configuration display' is activated under **Tools** ▶ **Options**).

With WEBconfig, resetting the toll protection and all parameters are found under **Expert configuration** ▶ **Setup** ▶ **Charges**.

2 Online

The online LED displays the general status of all WAN interfaces:

Off		No active connection
Green	Flashing	Opening the first connection
Green	Inverse flashing	Opening an additional connection
Green	On (permanently)	At least one connection is established

Red	On (permanently)	Error establishing the last connection
Orange/ green	In the housing cover; blinking alternately with the power LED	At least one WLAN module is in managed mode and has not found a WLAN Controller yet. The corresponding WLAN module(s) is/are switched off until a WLAN Controller is found to supply a configuration, or until being switched manually into another operating mode.
Orange / red	In the housing cover; blinking alternately with the power LED	At least one WLAN module is in managed mode and has found a WLAN Controller. However, the WLAN Controller cannot assign a configuration because the firmware and/or the device's loader version is not compatible with the WLAN Controller.

3 DSL

Status of DSL connections:

Off		No DSL connection
Green	Blinking	Establishing the first connection
Green	Flashing	Establishing an additional connection
Green	On (permanently)	At least one logical connection is established
Red	Blinking/Flashing	Data traffic (TX or RX)

4 UMTS

Status of UMTS connections:

Off		No UMTS connection
Orange	Flashing	Login to the UMTS network active
Orange	On (permanently)	Login to the UMTS network completed
Green	Blinking	Establishing the first connection
Green	Flashing	Establishing an additional connection
Green	On (permanently)	At least one logical connection is established
Green	Blinking/Flashing	Data traffic (TX or RX)
Red	Flickering	CRC error
Red/ Orange	Blinking	Hardware error

EN

5 WLAN

Provides information about the WLAN connections via the internal WLAN modules. The following can be displayed for WLAN link:

Off		No WLAN network defined or WLAN module deactivated. The WLAN module is not transmitting beacons.
Green		At least one WLAN network is defined and WLAN module activated. The WLAN module is transmitting beacons.
Green	Inverse flashing	Number of flashes = number of connected WLAN stations and P2P wireless connections, followed by a pause (default). Alternatively, the frequency of the flashed can indicate the input sensitivity.
Green	Blinking	DFS scanning or other scan procedure.
Green	Flashing	WLAN-Modul switched off due to fall below operating temperature
Red	Flickering	Error in wireless LAN (TX error, e.g. transmission error due to a poor connection)
Red	Blinking	Hardware error in the WLAN module

6 VPN

Status of a VPN connection.

Off		No VPN tunnel established
Green	Blinking	Connection establishment
Green	Flashing	First connection
Green	Inverse flashing	Other connections
Green	On (permanently)	VPN tunnels are established

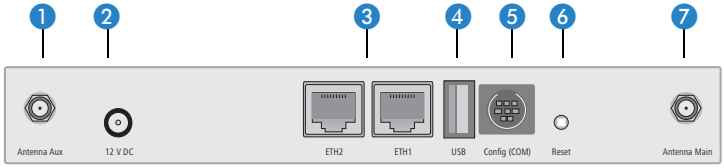
7 ETH

LAN connector status in the integrated switch:

Off		No networking device attached
Green	On (permanently)	Connection to network device operational, not data traffic
Green	Flickering	Data traffic
Red	Flickering	Data packet collision

2.3.2 The back of the unit

The connections and switches of the LANCOM Wireless Router are located on the back panel:



1. Connector for diversity antenna
2. Connection for the included power adapter
3. Switch with 10/100Base-Tx connectors

   The LAN connectors of the LANCOM 3850 UMTS supports the Power-over-Ethernet standard (PoE). You find further information about operating with PoE in the info box 'Power-over-Ethernet – elegant power supply through the LAN wiring'.
4. USB connector (USB host)
5. Serial configuration port (RS 232/V.24)
6. Reset button

The reset button offers two basic functions—boot (restart) and reset (to the factory settings)—which are called by pressing the button for different lengths of time.

Some devices simply cannot be installed under lock and key. There is consequently a risk that the configuration will be deleted by someone pressing the reset button too long. With the suitable setting, the behavior of the reset button can be controlled accordingly.

Configuration tool	Call
WEBconfig, Telnet	Expert configuration > Setup > Config

Reset button

This option controls the behavior of the reset button when it is pressed:

- ☐ Ignore: The button is ignored.

Please observe the following notice: The settings 'Ignore' or 'Boot only' makes it impossible to reset the configuration to the factory settings. If the password is lost for a device with this setting, then there is no way to access the configuration! In this case the serial commu-

EN

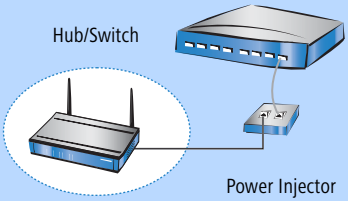
Power-over-Ethernet – elegant power supply through the LAN wiring

LANCOM Router base stations are prepared for the PoE power supply (Power-over-Ethernet), corresponding to the 802.3af standard. PoE-enabled network devices can be comfortably supplied with power feeding through the LAN wiring. A separate external power supply for each base station is unnecessary, which reduces the installation complexity considerably.

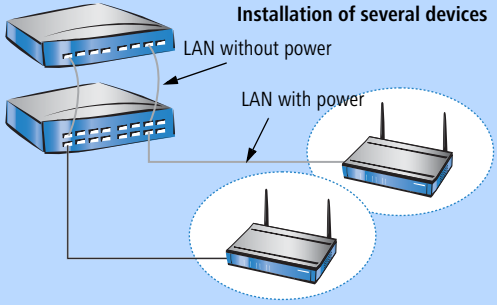
The power feeding into the LAN happens at a central position, either via a PoE power injector, or via a so-called powerhub/powerswitch. For the LAN wiring is to note that all 8 wires must be available by the cabling. PoE feeds the power over those four wires, which are normally not used for data transfer.

The PoE supply works only in such network segments, in which exclusively PoE-capable devices are operating. The protection of network devices without PoE support is guaranteed by an intelligent mechanism, that tests the network segment for devices without PoE support before starting the PoE power feeding. The power is only switched onto the segment, if only devices with PoE support were detected.

Installation of single devices



Installation of several devices



In a PoE installation use exclusively devices which correspond to the 802.3af standard! For damages caused by inadmissible devices no warranty may be claimed.

For the LANCOM 3850 UMTS, two LAN sockets can be used for redundant power supply. The device itself selects the power source to be used. If a power outage causes a switch between power sources, the device reboots so that the power feed is reactivated, if appropriate.

nications interface can be used to upload a new firmware version to the device–this resets the device to its factory settings, which results in the deletion of the former configuration. Instructions on firmware uploads via the serial configuration interface are available in the LCOS reference manual.

- Boot only: A press of the button prompts a restart, regardless of how long the it is held down.
- Reset-or-boot (standard setting): Press the button briefly to restart the device. Pressing the button for 5 seconds or longer restarts the device and resets the configuration to its factory settings. All LEDs on the device light up continuously. Once the switch is released the device will restart with the restored factory settings.

This hard reset causes the device to start with the default factory settings; all previous settings are lost!

Note that resetting the device leads to a loss on the WLAN encryption settings within the device and that the default WEP key is active again.

⑦ Connector for main antenna (if necessary is here the spot to connect AirLancer Extender additional antennas)

2.4 Hardware installation

The installation of the LANCOM Wireless Router takes place in the following steps:

① **Antennas** – Screw on the both included diversity antennas at the back of the LANCOM 3850 UMTS access point.

Antennas are only to be attached or changed when the device is switched off. Mounting or demounting antennas while the device switched on may cause the destruction of the WLAN module!

If the reverse SMA antennas are attached to the device directly, the quality of data transfer may be compromised if the internal WLAN module and an external WLAN card in the cardbus slot (e.g. AirLancer) are operated in the same frequency band at once. In this situation, at least one of the wireless modules should be operated with an external antenna.

EN

② **LAN** – You can first connect the access point to your LAN. For that purpose, plug the included network cable (green plugs) into the LAN connector of the device ③ and the other end into a free network connecting socket of your local network (resp. into a free socket of a hub/switch). Alternatively, you can connect also a single PC.

The LAN connector identifies automatically the contact assignment (Auto MDI/X) as well as the transfer rate (10/100 Mbp) of the connected network device (autosensing).

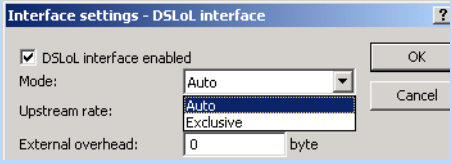
For information about the installation of PoE see the info box 'Power-over-Ethernet – elegant power supply through the LAN wiring'.

③ **DSLoL** – If you want to use your access point in DSLoL mode, you can either connect the device directly to the DSL modem (exclusive mode) or to a hub resp. switch of the cable-bound LAN (automatic mode).

- For the exclusive mode insert the included network cable (green plugs) into the LAN connector of the device ③ and the other end into the corresponding interface of the DSL modem.
- For the automatic mode for simultaneous operating with LAN and DSLoL insert the included network cable (green plugs) into the LAN connector of the device ③ and the other end into a free network connecting socket of your local network (resp. into a free socket of a hub/switch). More information about DSLoL can be found under 'LAN interface: exclusive or in parallel for DSLoL'.

LAN interface: exclusive or in parallel for DSLoL

There are two principle DSLoL operation modes available. Either use the exclusive mode when connecting your LANCOM Router directly to a DSL modem, or use the automatic mode when connecting the LANCOM Router to a hub or switch of a cable-bound LAN, and connect this hub/switch again to the DSL modem. If the LANCOM Router is broadcasted as gateway via DHCP, computers in LAN and WLAN can use the internet connection **simultaneously** via one physical interface. Set the desired mode in LANconfig in the Interface settings of the DSLoL interface.



DSLoL supports all PPPoE-based Internet access lines, as well as those that are supplied with a access router with multiple fixed IP addresses (such as many SDSL business lines).

④ **Connect up the power supply** – Use the supplied power supply unit to provide the device with power via connector Use the supplied power supply unit to provide the device with power via connector 2.

Use only the supplied power supply unit! The use of the wrong power supply unit can be of danger to the device or persons.

You can alternatively use the PoE facility for the power supply (also see 'Power over Ethernet-elegant power supply over LAN cabling').

The LANCOM 3850 UMTS enables two LAN sockets to be used for redundant power supplies. The device itself selects the power source to be used. If a power outage causes a switch between power sources, the device reboots so that the power feed is reactivated.

⑤ **Operational?** – After a short device self-test the Power LED will be permanently lit green resp. will blink alternately red and green as long as no configuration password has been given.

2.5 Software installation

The following section describes the installation of the Windows-compatible system software LANtools, as supplied.

You may skip this section if you use your LANCOM Router exclusively with computers running operating systems other than Windows.

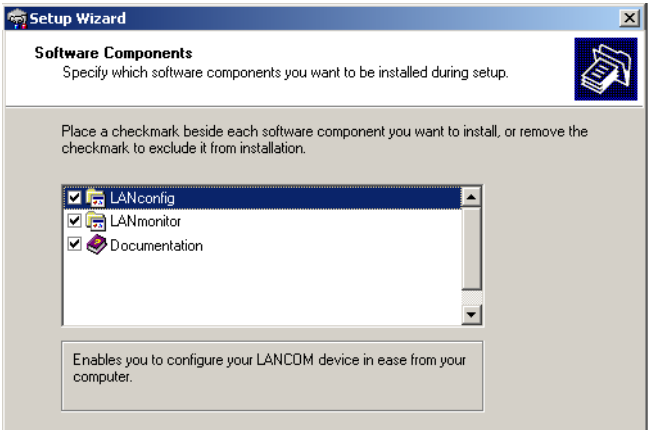
2.5.1 Starting Software Setup

Place the product CD into your drive. The setup program will start automatically.

If the setup does not start automatically, run AUTORUN.EXE in the root directory of the product CD.

EN

In Setup, select **Install Software**. The following selection menus will appear on screen:



2.5.2 Which software should I install?

- **LANconfig** is the Windows configuration program for all LANCOM routers and LANCOM access points. WEBconfig can be used alternatively or in addition via a web browser.
- With **LANmonitor** you can use a Windows computer to monitor all of your LANCOM routers and LANCOM access points.
- **WLANmonitor** enables the observation and surveillance of wireless LAN networks. Clients connected to the access points are shown, and even non-authenticated access points and clients can be displayed as well (rogue AP detection and rogue client detection).
- The **LANCOM Advanced VPN Client** enables VPN connections to be established over the Internet from a remote computer to a VPN router.
- With **Documentation** you copy the documentation files onto your PC.

Select the appropriate software options and confirm your choice with **Next**. The software is installed automatically.

3 Basic configuration

The basic configuration can be performed on a step-by-step basis using a convenient setup wizard to guide you through the setup process and prompt you for the required information.

First, this chapter will tell you which information is required for the basic configuration. Use this section to assemble the information you will need before you launch the wizard.

Next, enter the data in the setup wizard. Launching the wizard and the process itself are described step by step — with separate sections for LANconfig and WEBconfig. Thanks to the information that you have collected in advance, the basic configuration is quick and effortless.

At the end of this chapter we will show you the settings that are needed for the LAN's workstations to ensure trouble-free access to the device.

3.1 Which information is necessary?

The basic configuration wizard will take care of the basic TCP/IP configuration of the device and protect the device with a configuration password. The following descriptions of the information required by the wizard are grouped in these configuration sections:

- TCP/IP settings
- protection of the configuration
- information related to the Wireless LAN
- configuring connect charge protection
- security settings

3.1.1 TCP/IP settings

The TCP/IP configuration can be realized in two ways: either as a fully automatic configuration or manually. No user input is required for the fully automatic TCP/IP configuration. All parameters are set automatically by the setup wizard. During manual TCP/IP configuration, the wizard will prompt you for the usual TCP/IP parameters: IP address, netmask etc. (more on these topics later).

Fully automatic TCP/IP configuration is only possible in certain network environments. The setup wizard therefore analyses the connected LAN to determine whether it supports fully automatic configuration.

EN

New LAN—fully automatic configuration possible

If all connected network devices are still unconfigured, the setup wizard will suggest fully automatic TCP/IP configuration. This may be the case in the following situations:

- a single PC is connected to the WLAN Controller
- setup of a new network

Fully automatic TCP/IP configuration will not be available when integrating the WLAN Controller in an existing TCP/IP LAN. In this case, continue with the section 'Information required for manual TCP/IP configuration'.

The result of the fully automatic TCP/IP configuration: the router will be assigned the IP address '172.23.56.1' (netmask '255.255.255.0'). In addition, the integrated DHCP server will be enabled so that the WLAN Controller can automatically assign IP addresses to the devices in the LAN.

Configure manually nevertheless?

The fully automatic TCP/IP configuration is optional. You may also select manual configuration instead. Make your selection after the following considerations:

- Choose automatic configuration if you are **not** familiar with networks and IP addresses.
- Select manual TCP/IP configuration if you are familiar with networks and IP addresses, and one of the following conditions is applicable:
  - You have not yet used IP addresses in your network but would like to do so now. You would like to specify the IP address for your router, selecting it from the address range reserved for private use, e.g. '10.0.0.1' with the netmask '255.255.255.0'. At the same time you will set the address range that the DHCP server uses for the other devices in the network (provided that the DHCP server is switched on).
  - You have previously used IP addresses for the computers in your LAN.

Information required for manual TCP/IP configuration

During manual TCP/IP configuration, the setup wizard will prompt you for the following information:

- **IP address and netmask for the WLAN Controller**
  Assign a free IP address from the address range of your LAN to the WLAN Controller and specify the netmask.

EN

3.1.2 Configuration protection

The password for configuration access to the LANCOM protects the configuration against unauthorized access. The configuration of the device contains a considerable amount of sensitive information such as your Internet access information. We therefore strongly recommend protecting it with a password.

Multiple administrators can be set up in the configuration of the LANCOM, each with differing access rights. For a LANCOM, up to 16 different administrators can be set up. Further information can be found in the section 'Managing rights for different administrators' in the LCOS reference manual.

In the managed mode (see following) the LANCOM Wireless Routers and LANCOM Access Points automatically receive the same root password as the WLAN Controller, assuming that no root password has been set in the device itself.

3.1.3 Settings for the Wireless LAN

LANCOM Wireless Routers and LANCOM Access Points can be operated either as self-sufficient Access Points with their own configuration (WLAN modules in "Access Point mode") or as components in a WLAN infrastructure, which is controlled from a central WLAN Controller ("managed mode").

The managed mode has to be activated in the physical WLAN settings. In this operating mode the WLAN modules receive their configuration from the WLAN Controller, the WLAN settings in the LANCOM Wireless Routers and LANCOM Access Points have no influence.

For devices with two WLAN modules the operationg mode can be set up for each module seperately, i.e. the first WLAN module can be operated in managed mode while the second is working as self-sufficient Access Point.

The network name (SSID)

The basic configuration wizard asks for the network name of the base station (often designated as SSID – **S**ervice **S**et **Id**entifier). The network name will be registered in the base stations of the Wireless LAN. You can choose any name. Several base stations with the same network name form a common Wireless LAN.

As standard, WEP128 encryption is activated for every unconfigured device as standard. Further information can be found in the LCOS reference manual under "Standard WEP encryption".

Open or closed Wireless LAN?

Mobile radio stations dial-in the wanted Wireless LAN by declaration of the network name. The specification of the network name is facilitated by two technologies:

- Mobile radio stations can search for Wireless LANs in the environs („scan") and offer for selection the found Wireless LANs in a list.
- By using the network name 'ANY', the mobile radio station will enrol in the next available Wireless LAN.

The Wireless LAN can be „closed" to prevent this procedure. In this case, no enrolment with the network name 'ANY' will be accepted.

For standard, LANCOM base stations are responsive under the network name 'LANCOM'. The wireless basic configuration of a base station takes therefore place via this network name. If another network name is set during the basic configuration, also the Wireless LAN access of the configuring mobile base station must be changed to this new network name after closing the basic configuration.

Selection of a radio channel

The base station operates in a certain radio channel. The radio channel will be selected from a list of up to 11 channels in the 2.4 GHz frequency range or up to 19 channels in the 5 GHz frequency range. (in various countries some radio channels are restricted, see appendix).

The used channel and frequency range define the operating of the common radio standard, in doing so the 5 GHz frequency range correspond to the IEEE 802.11a/h standard and the 2.4 GHz frequency range to the IEEE 802.11g and IEEE 802.11b standard.

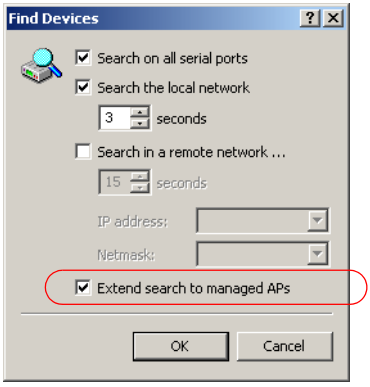
If no further base stations operate in reach of the base station, any radio channel can be adjusted. Otherwise, the channels in the 2.4 GHz band must be chosen in the way that they preferably do not overlap one another or have a distance as great as possible respectively. The automatic setting is normally enough in the 5 GHz band, in which the LANCOM Router base station itself adjust the best channel via TPC (Transmission Power Control) and DSF (Dynamic Frequency Selection).

Further information on TPC and DFS can be found in the LCOS reference manual.

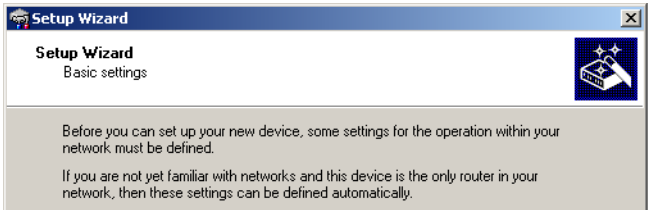
3.2 Instructions for LANconfig

① Start up LANconfig by clicking **Start** ▶ **Programs** ▶ **LANCOM** ▶ **LANconfig**. LANconfig automatically detects the new LANCOM devices in the TCP/IP network.

② As standard, LANCOM Wireless Routers and LANCOM Access Points in managed mode are **not** displayed by LANconfig carrying out its device search. To display these devices, activate the option 'Extend search for managed APs'.



③ If an unconfigured device is being found during searching, the setup wizard starts that will help you make the basic settings of the device or will even do all the work for you (provided a suitable network environment exists).



If the setup wizard does not start automatically, start a manual search for new devices on all ports (if the LANCOM is connected via a serial port) or in the network (**Device** ▶ **Find**).

EN

If you cannot access an unconfigured LANCOM, the problem may be due to the netmask of the LAN: with less than 254 possible hosts (netmask > '255.255.255.0'), please ensure that the IP address 'x.x.x.254' is located in your own subnet.

If you have chosen automatic TCP/IP configuration, please continue with Step ⑤.

④ If you would like to configure the TCP/IP settings manually, assign an available address from a suitable address range to the LANCOM. Confirm your choice with **Next**.

⑤ Specify whether or not the router should act as a DHCP server. Make your selection and confirm with **Next**.

⑥ In the following window, specify the password for configuration access. Note that the password is case-sensitive and ensure that it is sufficiently long (at least 6 characters).

In addition, you may specify whether the device may only be configured from the local network or whether remote configuration via the WAN (i.e. a remote network) is also permissible.

Please note that enabling this will also permit remote configuration via the Internet. You should always make sure that the configuration access is protected with a password.

⑦ Enter the wireless parameters. Select a network name (SSID) and a radio channel. Turn on if necessary the function for 'closed network'. Confirm your choice with **Next**.

⑧ In the next window, select your DSL provider from the list that is displayed. If you select 'My provider is not listed here,' you must enter the transfer protocol used by your DSL provider manually. Confirm your choice with **Next**.

⑨ Connect charge protection can limit the cost of DSL connections to a predetermined amount if desired. Confirm your choice with **Next**.

⑩ Complete the configuration with **Finish**.

Section 'TCP(IP settings to workstation PCs' will describe the settings required for the individual workstations in the LAN.

EN

3.3 Instructions for WEBconfig

To configure the router with WEBconfig you must know how to address it in the LAN. The reaction of the devices, as well as their accessibility for configuration via web browser is dependent on whether a DHCP server and a DNS server are already active in the LAN, and whether these two server processes exchange the assignment of IP addresses to symbolic names within the LAN between each other.

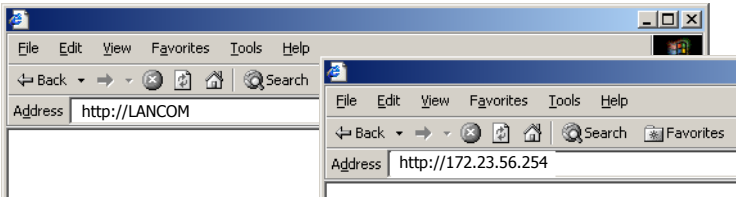
After powered on, unconfigured LANCOM devices check first, whether a DHCP server is already active in the LAN. Dependent on the situation, the device is able to switch on its own DHCP server or, alternatively, to activate its DHCP client mode. In this second operating mode, the device itself can obtain an IP address from a DHCP server already existing in the LAN.

If a LANCOM Wireless Router or LANCOM Access Point is centrally managed from a LANCOM WLAN Controller, the DHCP mode is switched from auto-mode to client mode.

Network without DHCP server

Not for centrally managed LANCOM Wireless Router or LANCOM Access Points

In a network without DHCP server, unconfigured LANCOM devices activate their own DHCP server service after starting, and assign appropriate IP addresses and gateway information to the other workstations within the LAN, provided that the workstations are set to obtain their IP address automatically (auto-DHCP). In this constellation, the device can be accessed with any web browser from each PC with activated auto-DHCP function through the name **LANCOM** or by its IP address **172.23.56.254**.



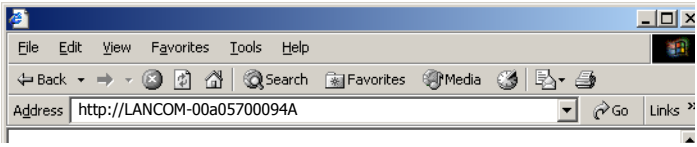
If the configuration PC does not obtain its IP address from the LANCOM DHCP server, figure out the current IP address of this PC (with **Start ▶ Execute ▶ cmd** and command **ipconfig** at the prompt under Windows 2000 or Windows XP, with **Start ▶ Execute ▶ cmd** and the command **winipcfg** at the prompt under Windows Me and Windows 9x, or with the command **ifconfig** on the console under Linux). In this case, the LANCOM is reachable under the IP

address **x.x.x.254** ("x" stands for the first three blocks in the IP address of the configuration PC).

Network with DHCP server

If a DHCP server is active in the LAN to assign IP addresses, an unconfigured LANCOM device will turn off its own DHCP server. It will change into DHCP client mode and will obtain an IP address from the DHCP server of the LAN. This IP address is not known at first. The accessibility of the device depends on the name resolution:

- If there is a DNS server for name resolution in the LAN, which interchanges the assignment of IP addresses to names with the DHCP server, then the device can be accessed by the name "LANCOM <MAC address>" (e.g. "LANCOM-00a057xxxxxx").



The MAC address can be found on a label at the bottom of the device.

- If there is no DNS server in the LAN, or it is not linked to the DHCP server, then the device can not be reached by the name. The following options remain in this case:
  - Figure out the DHCP-assigned IP address of the LANCOM by suitable tools and contact the device directly with this IP address.
  - Use LANconfig.
  - Connect a PC with a terminal program via the serial configuration interface to the device.

Starting the wizards in WEBconfig

① Start your web browser (e.g. Internet Explorer, Firefox, Opera) and call the LANCOM Router there:

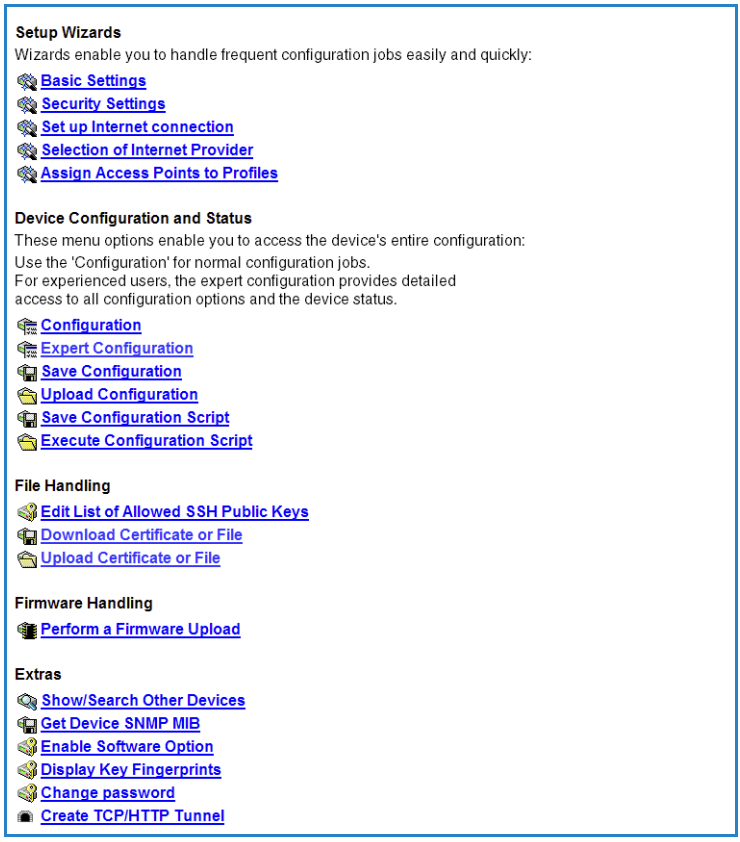
```
http://<IP address of the LANCOM>
```

(or with a name as discribed above)

If you cannot access an unconfigured LANCOM Router, the problem may be due to the netmask of the LAN: with less than 254 possible

hosts (netmask > '255.255.255.0'), please ensure that the IP address 'x.x.x.254' is located in your own subnet.

The WEBconfig main menu will be displayed:



The setup wizards are tailored precisely to the functionality of the specific LANCOM Router. As a result, your device may offer different wizards than those shown here.

If you have chosen automatic TCP/IP configuration, please continue with Step ③.

② If you would like to configure the TCP/IP settings manually, assign an available address from a suitable address range to the LANCOM Router. Also

EN

set whether or not it is to operate as a DHCP server. Confirm your entry with **Apply**.

③ Enter the wireless parameters. Select a network name (SSID) and a radio channel. Turn on if necessary the function for 'closed network'. Confirm your choice with **Next**.

④ In the following 'Security settings' window, specify a password for configuration access. Note that the password is case-sensitive and ensure that it is sufficiently long (at least 6 characters).

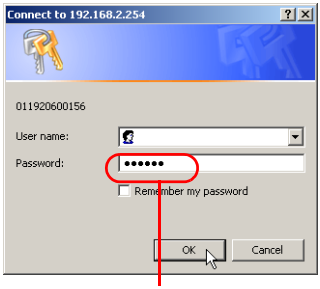
You may specify whether the device may only be configured from the local network or whether remote configuration via the WAN (i.e. a remote network) is also permissible.

Please note that enabling this will also permit remote configuration via the Internet. You should always make sure that the configuration access is suitably protected, e.g. with a password.

Entering the password in the web browser

When you are prompted for a user name and password by your web browser when accessing the device in the future, enter your personal values to the corresponding fields. Please note that the password is case-sensitive.

If you are using the common configuration account, enter the corresponding password only. Leave the user name field blank.



Entering the configuration password

⑤ In the next window, select your DSL provider from the list that is displayed. Confirm your choice with **Apply**.

If you select 'My provider is not listed here,' you must enter the transfer protocol used by your DSL provider manually in the next window. Confirm your choice with **Apply**.

⑥ Connect charge protection can limit the cost of DSL connections to a predetermined amount if desired. Confirm your choice with **Apply**.

⑦ The basic setup wizard reports that all the necessary information has been provided. You can end the wizard with **Go on**.

3.4 TCP/IP settings to workstation PCs

The correct addressing of all devices within a LAN is extremely important for TCP/IP networks. In addition, all computers must know the IP addresses of two central points in the LAN:

- Default gateway – receives all packets that are not addressed to computers within the local network.
- DNS server – translates network names (www.**lancom.de**) or names of computers (**www**.lancom.de) to actual IP addresses.

The LANCOM Router can perform the functions of both a default gateway and a DNS server. In addition, as a DHCP server it can also automatically assign valid IP addresses to all of the computers in the LAN.

The correct TCP/IP configuration of the PCs in the LAN depends on the method used to assign IP addresses within the LAN:

- **IP address assignment via the LANCOM Router (default)**

  In this operating mode the LANCOM Router not only assigns IP addresses to the PCs in the LAN, it also uses DHCP to specify its own IP address as that of the default gateway and DNS server. The PCs must therefore be configured so that they automatically obtain their own IP address and the IP addresses of the standard gateway and DNS server (via DHCP).

- **IP address assignment via a separate DHCP server**

  The workstation PCs must be configured so that they automatically obtain their own IP address and the IP addresses of the standard gateway and DNS server (via DHCP). The IP address of the LANCOM Router must be stored on the DHCP server so that the DHCP server transmits it to the PCs in the LAN as the standard gateway. In addition, the DHCP server should also specify the LANCOM Router as a DNS server.

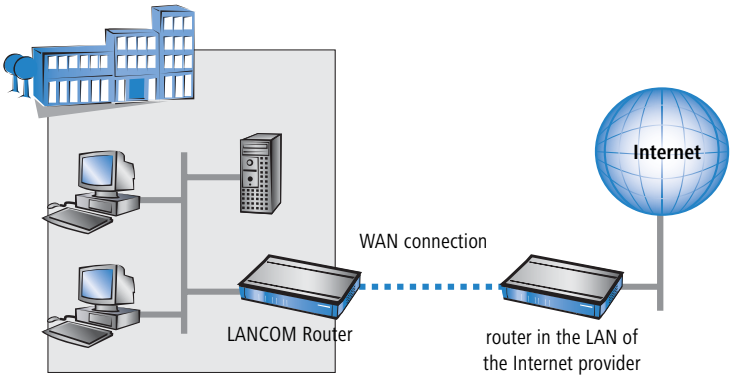
- **Manual IP address assignment**

  If the IP addresses in the network are assigned static ally, then for each PC the IP address of the LANCOM Router must be set in the TCP/IP configuration as the standard gateway and as a DNS server.

For further information and help on the TCP/IP settings of your LANCOM Router, please see the reference manual. For more information on the network configuration of the workstation computers, please refer to the documentation of your operating system.

4 Setting up Internet access

All computers in the LAN can take advantage of the central Internet access of the LANCOM. For models without WAN interface one LAN interface can be configured as a DSLoL interface.



Does the setup wizard know your Internet provider?

A convenient wizard is available to help you set up Internet access. The wizard knows the access information of major Internet providers and will offer you a list of providers to choose from. If you find your Internet service provider on this list, you normally will not have to enter any further transfer parameters to configure your Internet access. Only the authentication data that are supplied by your provider are required.

Additional information for unknown Internet providers

If the setup wizard does not know your Internet provider, it will prompt you for all of the required information step by step. Your provider will supply this information.

Additional connection options

You may also enable or disable further options in the wizard, depending on whether or not they are supported by your Internet provider:

- Time-based billing or flat rate – select the accounting model used by your Internet provider.

EN

- When using time-based billing, you can set the LANCOM Router to automatically close existing connections if no data has been transferred within a specified time (the so-called idle time).

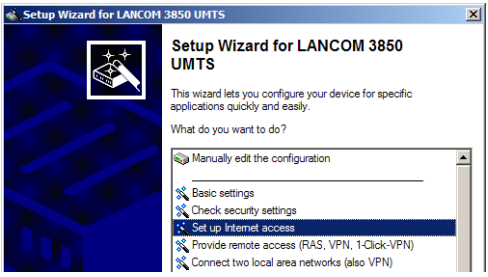
  In addition, you can activate a line monitor that identifies inactive remote stations faster and therefore can close the connection before the idle time has elapsed.

- Active line monitoring can also be used with flat rate billing to continuously check the function of the remote station.

  You also have the option of keeping flat rate connections alive if required. Dropped connections are then automatically re-established.

4.1 Instructions for LANconfig

① Highlight the LANCOM Router in the selection window. From the menu bar, select **Tools** ▶ **Setup Wizard**.



② From the menu, select the **Setup Internet access** wizard and click **Next**.

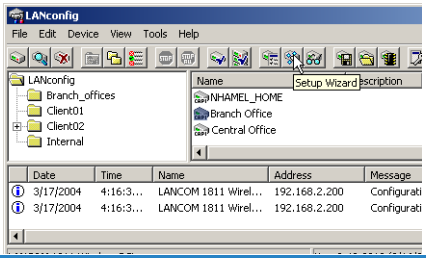
③ In the following window select your country and your Internet provider if possible, and enter your access information.

④ Depending on their availability, the wizard will display additional options for your Internet connection.

⑤ The wizard will inform you as soon as the entered information is complete. Complete the configuration with **Finish**.

LANconfig: Quick access to the setup wizards

Under LANconfig, the fastest way to launch the setup wizards is via the button on the toolbar.



4.2 Instructions for WEBconfig

① In the main menu, select **Setup Internet access**.

② In the following window select your country and your Internet provider if possible, and enter your access information.

③ Depending on their availability, the wizard will display additional options for your Internet connection.

④ The wizard will inform you as soon as the entered information is complete. Complete the configuration with **Apply**.

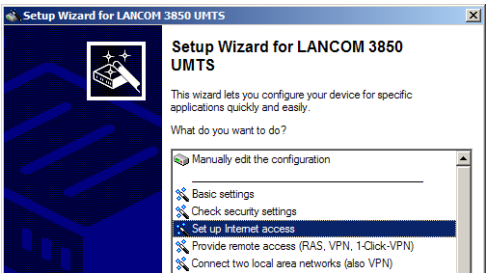
EN

5 Setting up the UMTS profile

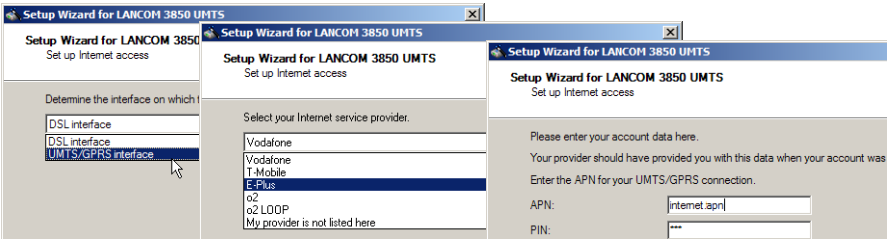
5.1 Internet access

The quickest way to set up Internet access via UMTS/HSPDA is to use the Internet Wizard in LANconfig.

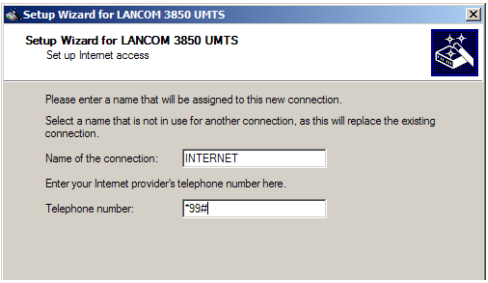
① Highlight the LANCOM Router in the selection window. From the menu bar, select **Tools** ▶ **Setup Wizard**.



② From the menu, select the **Setup Internet access** wizard and click **Next**.



③ To set up the Internet access, select the UMTS interface and your network operator and enter the APN (Access Point Name) and the PIN number for your SIM card. The Wizard then carries out all other settings automatically.



④ If your provider does not appear in the list, you can enter the necessary connection data manually. You will need the appropriate telephone number in your provider's mobile telephone network.

Your provider will supply this information to you upon request.

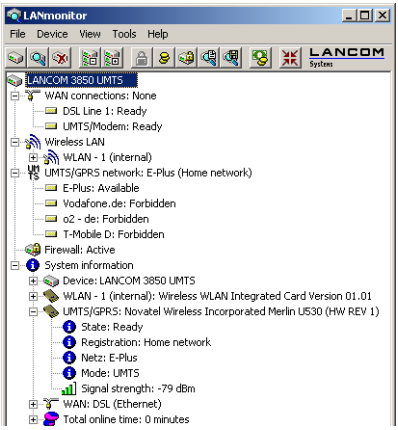
⑤ To conclude the configuration of the Internet access, you can activate the "Keep alive" option. This sets up the UMTS connection so that the connection is automatically established after switching on the device, and so that the connection is automatically re-established after being cut off—the Internet connection is "always on". This function is very useful for convenient access to the Internet or for VPN site coupling.

By activating the "keep alive" function, it is very easy to set up, for example, a mobile conference room that enables Internet access and, if need be, VPN-protected access to company networks from any location.

Depending on the tariff, always-on Internet connections can give rise to considerable costs, for example with time-based charging. Please ensure that you are familiar with the details of your provider's UMTS tariff.

⑥ Alternatively you can set up a suitable hold time for the UMTS connection. This means that the Internet connection is not started automatically, but only when data are to be transferred into the Internet. The connection will be automatically disconnected if data is not transmitted for the duration of the hold time.

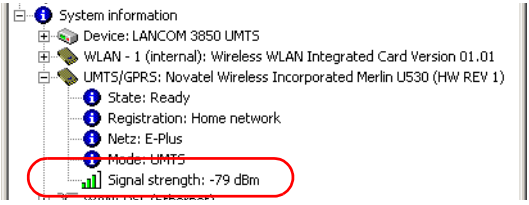
After setting up the Internet connection, you use LANmonitor to check for the available mobile telephone networks.



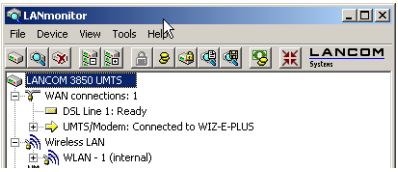
Even without an current connection, the active local networks are displayed in the 'UMTS/GPRS network' section. LANmonitor also indicates which networks are permitted and which networks the card cannot connect to.

⑦ In the System information section, LANmonitor displays the recognized data card and the signal strength of the home network with which the card is connected to the Internet. The display of signal strength an the operating mode is dependent on the UMTS card in use.

LANmonitor's signal strength display is highly useful for testing the reception quality at locations where the data card is to be put into service. With a displayed signal strength of three bars (green) you can safely assume that the signal strength is strong enough for good quality data transfer. With two bars (yellow) the quality of data transfer is questionable, and with one bar there will be no data transfer at all in most cases.



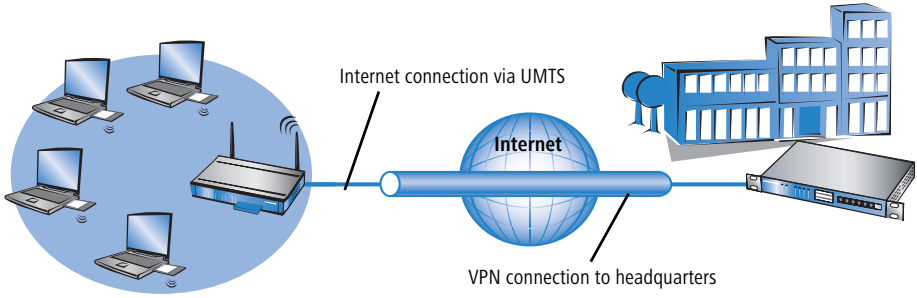
⑧ As soon as the Internet connection has been established, the section for WAN connections in LANmonitor shows the network being used for the connection.



The status of the data card is also displayed by its LEDs and coded flashing signals. Refer to the documentation for your data card for information about the LED signals.

5.2 VPN site coupling

As well as connection single workstations to the headquarters, the UMTS/HSPDA interface can be used for full-blown network coupling. This variant may be used for setting up "mobile conference rooms".



Mobile WLAN, e.g. for a "mobile conference room".

To couple two networks via a UMTS interface, the initial step is to set up network coupling between the two VPN routers, for example by using the Wizard in LANconfig.

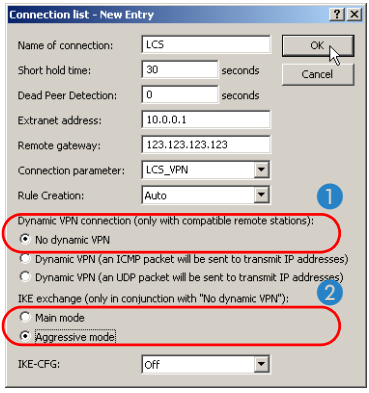
The following aspects must be considered for the configuration of network coupling via UMTS:

- When coupling networks with the Wizard, the secure "main mode" is initially used for the exchange of IKE keys. However, several mobile telephone operators only support the "aggressive mode". If no VPN

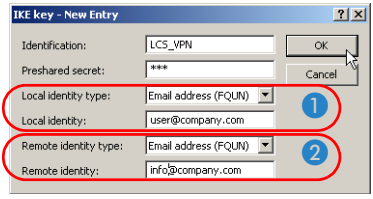
EN

connection can be established when using the main mode, adjust the method in the VPN connection list to "aggressive mode" in the appropriate profiles at both ends.

To do this in LANconfig , go to the 'VPN' configuration area on the 'General' tab and select the relevant connection from the 'Connection list'. First set the dynamic VPN option to 'No dynamic VPN' (1) and then activate 'Aggressive Mode' (2) as the IKE exchange mode.



In LANconfig,you then enter unique identities (e.g. unambiguous e-mail addresses) for the relevant connection in the configuration area 'VPN', tab 'IKE parameters', in the list for 'IKE key'



The settings for the aggressive mode must agree for all of the identities at both ends of the connection!

- The provider assigns a dynamic IP address to the UMTS card when it logs in to the mobile telephone network. Be aware of the corresponding settings when carrying out the configuration with the Setup Wizard.
- Since the UMTS card has a dynamic IP address but cannot be identified e.g. with an ISDN call (Dynamic VPN), the VPN connection must always be established from the VPN gateway with the UMTS card in the direction of the VPN gateway at the headquarters.

- To ensure that the VPN connection with the network at the headquarters is available on a continuous basis, set both the hold time for the Internet connection and the VPN hold time to '9,999' (keep alive). This is the only way to ensure that access from the headquarters to the UMTS-connected network is possible at all times (e.g. for connecting branches via UMTS where no broadband Internet access is available).

  The keep alive function also requires an entry in the polling table. To do this in LANconfig, create the entry for the appropriate connection with up to four IP addresses in the remote network, along with the related ping interval and the number of retries in the configuration area 'Communication' on the 'Remote sites' tab in the 'Polling table'.

- If line polling is to be used to monitor the VPN connection, then it also has to be initiated from the VPN gateway with the UMTS/HSPDA card and must be directed towards the remote VPN gateway. The interval times for the polling calls may have to be adjusted depending on the quality of the connection.

Depending on the tariff, always-on Internet connections can give rise to considerable costs, for example with time-based charging. Please ensure that you are familiar with the details of your provider's UMTS tariff.

5.3 Other settings

5.3.1 Choosing the mobile telephone network

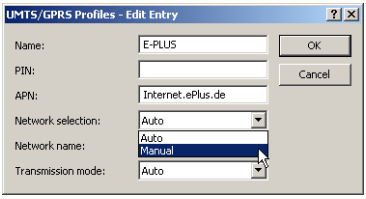
Most mobile data cards are programmed to log in to their own network when coverage is available, and there is no free choice of network.

Once the card is outside of "home network" coverage, there is normally a choice of alternative mobile networks (i.e. roaming, in particular when in another country). Generally speaking, the user now has a choice of network which is to be used for the Internet connection.

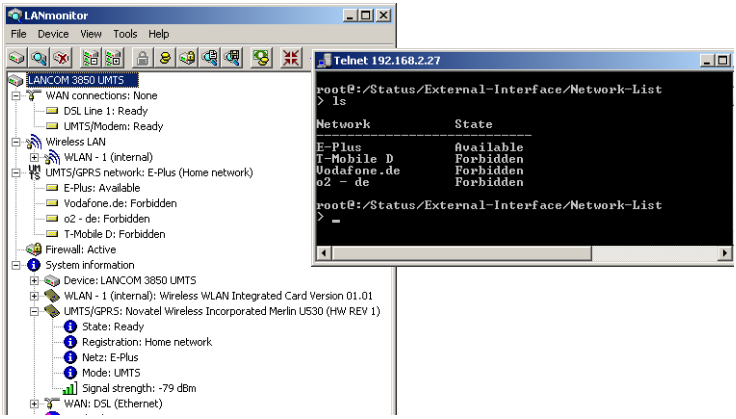
In the appropriate UMTS/GPRS profile, set the option for network selection to 'manual'. The entry for the name of the desired network should be the same as that identified by the data card's scanning procedure.

EN

The UMTS/GPRS profile settings are to be found in LANconfig in the configuration area 'Interface' on the 'WAN' tab with the **UMTS/GPRS profile** button.



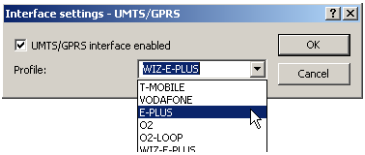
The name of the network can be read from LANmonitor or, for example, by using Telnet under `/Status/External-Interface/Network-List`. A manual network search can be initiated with the commands `do /Status/External-Interface/Scan-Networks` or `so Setup/Interfaces/UMTS-GPRS-parameters/Scan-Networks`.



5.3.2 Activate UMTS/GPRS profile

Operating the LANCOM devices with the UMTS/HSPDA function in varying locations or with different UMTS/GPRS data cards may well require different sets of settings. The relevant information for operating data cards is collected in a UMTS/HSPDA/GPRS profile. The profile can be switched very quickly via the interface settings for the UMTS interface.

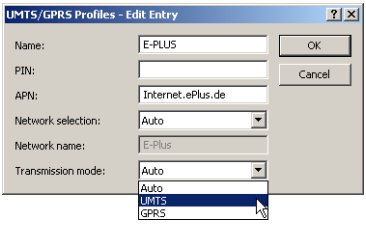
The activation of the UMTS interface and the selection of the profile are to be found in LANconfig in the configuration area 'Interfaces' on the 'WAN' tab with the **Interface settings** button.



5.3.3 UMTS/HSPDA only or automatic UMTS/HSPDA/GPRS selection

UMTS/HSPDA coverage is not yet universally available. It is still possible to establish a data connection even in areas without UMTS/HSPDA reception by selecting the 'automatic' operating mode. With this setting, the data card in the LANCOM will initially attempt to establish a connection via UMTS/HSPDA. The card will automatically switch to the GPRS network if the UMTS/HSPDA signal proves to be too weak to support data transfer of the necessary quality.

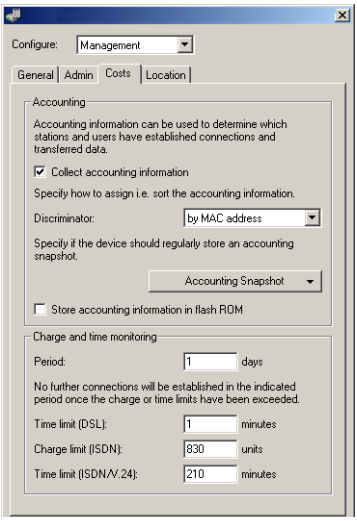
If required, the operating mode can be permanently set to either UMTS or GPRS. The desired operating mode can be set in the UMTS/GPRS profile settings which are to be found in LANconfig in the configuration area 'Interface' on the 'WAN' tab with the **UMTS/GPRS profile** button.



EN

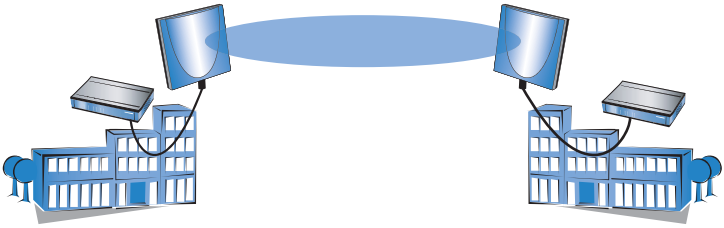
5.3.4 Set up a time limit

You can prevent excessive costs from arising from connections over the UMTS interface by setting up a time limit, for example under LANconfig in the 'Management' configuration area on the 'Costs' tab.



6 Point-to-point connections

LANCOM Wireless access points serve not only as central stations within a wireless network, they can also operate in point-to-point mode to bridge longer distances. For example, they can provide a secure connection between two networks that are several kilometers apart—without direct cabling or expensive leased lines.



The behavior of an access point when exchanging data with other access points is defined in the "Point-to-point operation mode".

- **Off:** The access point only communicates with mobile clients
- **On:** The access point can communicate with other access points and with mobile clients
- **Exclusive:** The access point only communicates with other base stations

In the 5 GHz band, the automatic search for vacant WLAN channels can lead to several simultaneous test transmissions from multiple access points, with the result that they do not find each other. This stalemate situation can be avoided with the appropriate "Channel selection scheme":

- **Master:** This access point takes over the leadership when selecting a free WLAN channel.
- **Slave:** All other access points will search for a channel until they have found a transmitting Master.

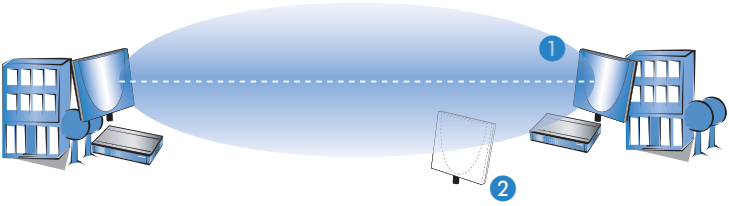
Thus it is recommended for the 5 GHz band that one central access point should be configured as 'Master' and all other point-to-point partners should be configured as 'Slave'. In the 2.4 GHz band, too, this setting simplifies the establishment of point-to-point connections if the automatic channel search is activated.

It is imperative that the channel selection scheme is configured correctly if the point-to-point connections are to be encrypted with 802.11i/WPA.

EN

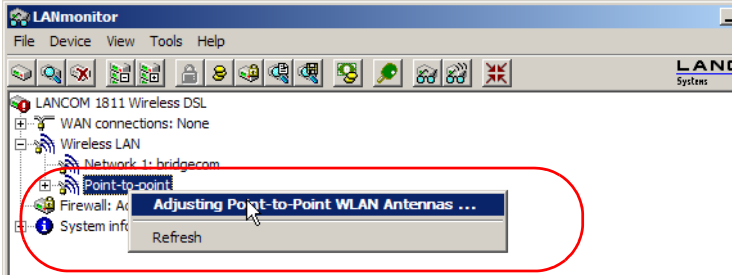
6.1 Antenna alignment for P2P operations

The precise alignment of the antennas is of considerable importance in establishing a P2P path. The more central the receiving antenna is located in the "ideal line" of the transmitting antenna, the better is the actual performance and the effective bandwidth 1. If the receiving antenna is outside of this ideal area, however, significant losses in performance will be the result 2.



Further information about the geometrical alignment of wireless paths and the alignment of antennas with the help of LANCOM software can be found in the LCOS reference manual.

To help find the best possible alignment for the antennas, LANmonitor can display the current signal quality over a P2P connection. The connection-quality display is opened with the context menu in LANmonitor. A click with the right-hand mouse key on the 'Point-to-point' entry prompts the command 'Adjusting Point-to-Point WLAN Antennas'



Configuration tool	Call
LANmonitor	Point-to-point ▶ context menu ▶ Adjusting Point-to-Point WLAN Antennas...

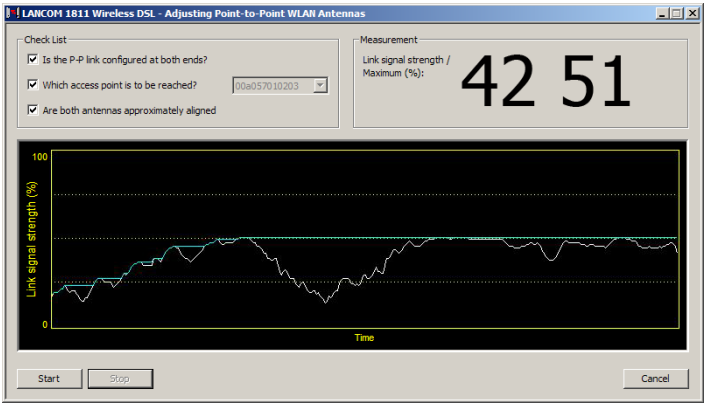
The entry 'Point-to-point' is only visible in LANmonitor if the monitored device has at least one base station defined as a remote

station for a P2P connection (LANconfig: **Wireless LAN ▶ General ▶ Physical WLAN settings ▶ Point-to-Point**).

In the dialog for setting up point-to-point connections, LANmonitor requests the required information for establishing the P2P connection:

- Assuming that the P2P path is configured at both ends, i.e. the two remote base stations are entered with their respective MAC addresses; has the point-to-point operating mode been activated?
- Which access point is to be monitored? All of the base stations defined as P2P remote stations in the respective device can be selected here.
- Are both antennas approximately aligned? The connection over the P2P path has to be functioning basically before you start fine-tuning with the aid of LANmonitor.

Once signal monitoring has commenced, the P2P dialog displays the absolute values for the current signal strength and the maximum value since starting the measurement. The development of the signal strength over time and the maximum value are displayed in a diagram.



Initially you should only adjust one of the two antennas until a maximum value is achieved. This first antenna is then fixed and the second antenna is then adjusted to attain the best signal quality.

6.2 Configuration

In the configuration of point-to-point connections, entries have to be made for the point-to-point operation mode, the channel selection scheme and the MAC addresses of the remote sites.

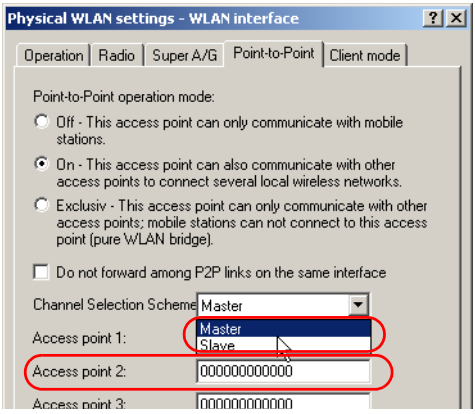
EN

Configuration with LANconfig

For configuration with LANconfig you will find the settings for P2P connections under the configuration area 'Interfaces' on the 'Wireless LAN' tab.

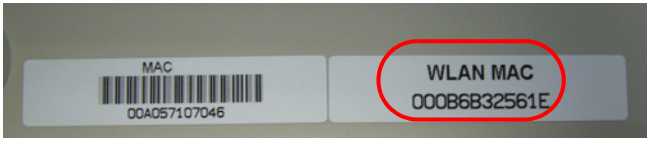
① Click on the button **Physical WLAN settings** to open the corresponding WLAN interface and select the tab for 'Point-to-Point'.

② Activate the suitable point-to-point operation mode here and set the channel selection scheme to either 'Master' or 'Slave'. Enter the appropriate MAC address for the WLAN card at the remote station (maximum 6).



Please observe that only the MAC addresses of the WLAN cards at the other end of the connections are to be entered here! Not the access point's own MAC address, and not the MAC addresses from any other interfaces that may be present in the access points.

You will find the WLAN MAC address on a sticker below the corresponding antenna connector. Only use the string that is marked as the "WLAN MAC" or "MAC-ID". The other addresses that may be found are not the WLAN MAC address but the LAN MAC address.



Alternatively you will find the MAC addresses for the WLAN cards in the devices under WEBconfig, Telnet or a terminal program under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Status ▶ WLAN-statistics ▶ Interface-statistics
Terminal/Telnet	`Status/WLAN-statistics/Interface-statistics`

Configuration with WEBconfig or Telnet

Under WEBconfig or Telnet you can set the settings for the point-to-point connections under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ Interfaces ▶ WLAN-Interfaces▶ Interpoint-Settings
Terminal/Telnet	`cd /Setup/Interfaces/WLAN-Interfaces/Interpoint-Settings`

6.3 Access points in relay mode

Access points equipped with two wireless modules can be used to establish wireless bridges across multiple stations. Each wireless module is configured as a 'Master' and then 'Slave' in turn.

The use of relay stations each equipped with two WLAN modules simultaneously solves the problem of the "hidden station", by which the MAC addresses of the WLAN clients are not transferred over multiple stations.

6.4 Security for point-to-point connections

IEEE 802.11i can be used to attain a significant increase in the security of WLAN point-to-point connections. All of the advantages of 802.11i such as the simple configuration and the powerful encryption with AES are thus available for P2P mode, as are the improved security of the passphrase from the LANCOM Enhance Passphrase Security (LEPS).

EN

6.4.1 Encryption with 802.11i/WPA

To activate the 802.11i encryption for a correctly configured P2P connection, adjust the settings for the first logical WLAN network in the appropriate WLAN interface (i.e. WLAN-1 if you are using the first WLAN card for the P2P connection, WLAN-2 if you are using the second card, e.g. as with an access point with two WLAN modules).

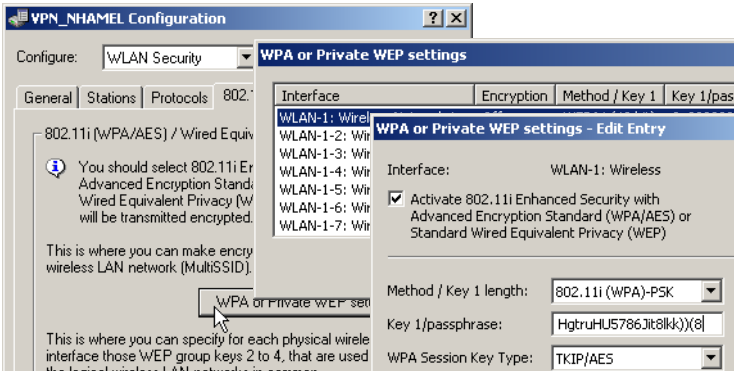
- Activate the 802.11i encryption.
- Select the method '802.11i (WPA)-PSK'.
- Enter the passphrase to be used.

The passphrases should consist of a random string at least 22 characters long, corresponding to a cryptographic strength of 128 bits.

When set as P2P Master, the passphrase entered here will be used to check the Slave's authorization to access. When set as P2P Slave, the access point transfers this information to register with the remote site.

Configuration with LANconfig

For configuration with LANconfig you will find the encryption settings under the configuration area 'WLAN Security' on the '802.11i/WEP' tab.



EN

Configuration with WEBconfig or Telnet

The encryption settings for the individual logical WLAN networks can be found under WEBconfig or Telnet under the following paths:

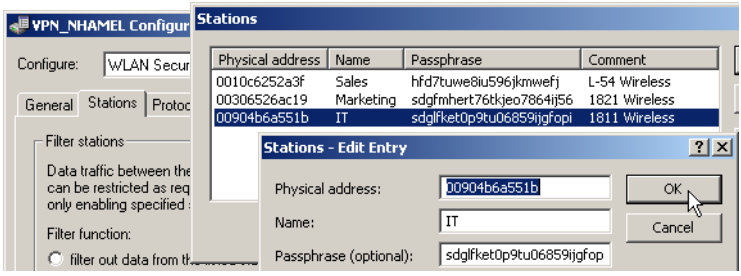
Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ Interfaces ▶ WLAN-Interfaces ▶ Encryption-Settings
Terminal/Telnet	`/Setup/Interfaces/WLAN-Interfaces/Encryption-Settings`

6.4.2 LEPS for P2P connections

A further gain in security can be attained by additionally using LANCOM Enhanced Passphrase Security (LEPS) which involves the matching of MAC address and passphrase.

LEPS can be used to secure single point-to-point (P2P) connections with an individual passphrase. Even if an access point in a P2P installation is stolen and the passphrase and MAC address become known, all other WLAN connections secured by LEPS remain secure, particularly when the ACL is stored on a RADIUS server.

When using LANconfig for the configuration, you enter the passphrases of the stations approved for the WLAN in the configuration area 'WLAN Security' on the 'Stations' tab under the button **Stations**.



Configuration with WEBconfig or Telnet

The access list for the matching of MAC addresses to the passphrases (LEPS) can be found under WEBconfig or Telnet under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ WLAN-module ▶ Access-list
Terminal/Telnet	`Setup/WLAN-module/Access-list`

7 Security settings

Your LANCOM device has numerous security functions. You find in this chapter all information needed for an optimal protection of the base station.

7.1 Security for the Wireless LAN

Reflecting on Wireless LANs often entails substantial doubts concerning security. Many people suppose that abuse of data transmitted via radio links is relatively simple.

Wireless LAN devices by LANCOM Systems permit the employment of modern security technologies:

- Closed network
- Access Control (via MAC addresses)
- LANCOM Enhanced Passphrase Security
- Encryption of data transfer (802.11i/WPA or WEP)
- 802.1x / EAP
- optional IPSec over WLAN (VPN), in combination with external VPN gateway

7.1.1 Closed network

Each Wireless LAN according to IEEE 802.11 has its own network name (SSID). This network name serves as identification and enables administration of Wireless LANs.

A Wireless LAN can be established in such a way that any user gets access to this network. Such networks are called open networks. Any user can access an open network also without knowledge of the WLAN network name reserved specifically for this network. Only requirement is the input of the network name 'ANY'.

In a closed network the access via 'ANY' is not possible. User have to specify the correct network name. Unknown networks stay hidden to them.

Ad-hoc-networks are automatically installed as closed networks and cannot be opened. Infrastructure networks can be run either in open or closed condition. You make the settings for this at the respective base station.

7.1.2 Access control via MAC address

Each network device has an special identification number. This identification number is the so-called MAC address (**M**edia **A**ccess **C**ontrol), which is worldwide unique per device.

The MAC address is programmed into the hardware and cannot be changed. Wireless LAN devices by LANCOM Systems have got a MAC address label on the casing.

The access to an infrastructure network can be restricted to known MAC addresses for certain Wireless LAN devices solely. To do so, Access Control lists are available within the LANCOM base stations, in which the granted MAC addresses can be deposited.

This method of access control is not available for ad-hoc networks.

7.1.3 LANCOM Enhanced Passphrase Security

With LEPS (**L**ANCOM **E**nhanced **P**assphrase **S**ecurity) LANCOM Systems has developed an efficient method which uses the simple configuration of IEEE 802.11i with passphrase and yet which avoids the potential error sources of passphrase sharing. LEPS uses an additional column in the ACL to assign an individual passphrase consisting of any 4 to 64 ASCII characters to each MAC address. The connection to the access point and the subsequent encryption with IEEE 802.11i or WPA is only possible with the right combination of passphrase and MAC address.

LEPS can be used locally in the device and can also be centrally managed with the help of a RADIUS server, and it works with all WLAN client adapters currently available on the market without modification. Full compatibility to third-party products is assured as LEPS only involves configuration in the access point.

An additional security aspect: LEPS can also be used to secure single point-to-point connections (P2P) with an individual passphrase. Even if an access point in a P2P installation is stolen and the passphrase and MAC address become known, all other WLAN connections secured by LEPS remain protected, particularly when the ACL is stored on a RADIUS server.

Guest access with LEPS: LEPS can also be set up to allow access to guests. To this end, all users of the internal WLAN network are given individual passphrases. Guests can make use of their own dedicated SSID and a global passphrase. To avoid abuse, this global passphrase can be changed on a regular basis—every few days, for example.

EN

7.1.4 Encryption of the data transfer

A special role comes up to the encryption of data transfer for Wireless LANs. For IEEE 802.11 radio transfer the supplementing encryption standards are 802.11i/WPA and WEP. The function of the encryption is to ensure the security level of cable-bound LANs also in Wireless LANs.

- Use encryption on the data transferred in the WLAN. Activate the strongest possible encryption available to you ((802.11i with AES, WPA or WEP) and enter the appropriate keys or passphrases into the access point and the WLAN clients.
- Regularly change the WEP keys in your access points. The passphrases for 802.11i or WPA do not have to be changed regularly as new keys are generated for each connection anyway. This is not the only reason that the encryption with 802.11i/AES or WPA/TKIP is so much more secure than the now aged WEP method.
- If the data is of a high security nature, you can further improve the encryption by additionally authenticating the client with the 802.1x method or activate an additional encryption of the WLAN connection as used for VPN tunnels ('IPSec over WLAN'). In special cases, a combination of these two mechanisms is possible.

Further details to WLAN security and the used encoding methods can be found in the LCOS reference manual.

Please take note of the information in the box “Standard WEP encryption”.

EN

Standard WEP encryption

As standard, WEP128 encryption is activated for every unconfigured device. This WEP encryption in WLAN devices being managed by a LANCOM WLAN Controller is overwritten by the central encryption settings in the profiles of the WLAN Controller.

The key consists of the first letter "L" followed by the LAN MAC address of the access point in ASCII characters. The LAN MAC addresses of the LANCOM devices always begin with the character string "00A057". You will find the LAN MAC address on a sticker on the base of the device. **Only** use the number labeled as "MAC address" that starts with "00A057". The other numbers that may be found are **not** the LAN MAC address!

A device with the LAN MAC address "00A0570FB9BF" thus has a standard WEP key of "L00A0570FB9BF". This key is entered into the 'Private WEP settings' of the device for each logical WLAN network as 'Key 1'.

To use a WLAN adapter to establish a connection to a new LANCOM access point, the WEP128 encryption must be activated for the WLAN adapter and the standard 13-character WEP key entered.

After registering for the first time, change the WEP password to ensure that you have a secure connection.

Note that a reset also causes the WLAN key settings to be lost from the device and the standard WEP key comes into effect again. WLAN access can only work after a reset if the standard WEP key is programmed into the WLAN adapter as well.

7.1.5 802.1x / EAP

The international industry standard IEEE 802.1x and the **E**xtensible **A**uthentication **P**rotocol (EAP) enables the realization of reliable and secure access controls for base stations. The access data is centrally administered on a RADIUS server then, and can be retrieved by the base station if required.

Moreover, this technology makes enables a secured dispatch and a regular automatic change of WEP keys. In this way IEEE 802.1x improves the protection efforts of WEP.

In Windows XP the IEEE-802.1x technology is already integrated by default. For other operating systems 802.1x client software is available.

The drivers for the LANCOM AirLancer wireless cards already feature an integrated 802.1x client.

EN

7.1.6 IPSec over WLAN

By means of IPSec over WLAN a radio network can be optimally secured in addition to the already introduced securing mechanisms. In order to run IPSec over WLAN you have to upgrade the base stations of the with the LANCOM VPN option and the LANCOM Advanced VPN Client, which runs under the operating systems Windows Vista™, Windows 2000 and Windows XP. For other operating systems client software from other manufacturers is available. The drivers for the LANCOM AirLancer wireless adapter are already equipped with a 802.1x client.

7.2 Tips for handling keys

The security of encryption procedures can be substantially increased the by paying attention to some important rules for handling keys.

- **Keep keys as secret as possible.**
  Never note a key. Popular, but completely unsuitable are for example: notebooks, wallets and text files in PCs. Do not share a key unnecessarily.
- **Select a random key.**
  Use randomized keys of character and number sequences. Keys from the general linguistic usage are insecure.
- **Change a key immediately in case of suspicion.**
  It is time to change the key of the Wireless LAN if an employee with access to a key leaves your company. The key should also be renewed in case of smallest suspicion of a leak.
- **LEPS prevents the global spread of passphrases.**
  Activate LEPS to enable the use of individual passphrases.

EN

7.3 The security settings wizard

Access to the configuration of a device permits not only to read out critical information (e.g. WEP key, Internet password). Rather, also the entire settings of the security functions (e.g. firewall) can be altered then. So an unauthorized configuration access endangers not only a single device, but the entire network.

Your LANCOM has a password protection for the configuration access. This protection is already activated during the basic configuration by entering a password.

The device locks access to its configuration for a specified period of time after a certain number of failed log-in attempts. Both the number of failed attempts and the duration of the lock can be set as needed. By default, access is locked for a period of five minutes after the fifth failed log-in attempt.

Besides these general settings you can also check the security settings of the wireless network with the security wizard as far as your device has a WLAN interface.

7.3.1 Wizard for LANconfig

① Mark your LANCOM Router in the selection window. Select from the command bar **Extras** ▶ **Setup Wizard**.

② Select in the selection menu the setup wizard **Control Security Settings** and confirm your choice with **Next**.

③ Enter your password in the following windows and select the allowed protocols for the configuration access from local and remote networks.

④ In a next step parameters of the configuration lock like number of failed log-in attempts and the duration of the lock can be adjusted.

⑤ Now you can set the security settings for the WLAN. These include the name of the wireless network, the closed network function and the WEP encryption. You can type in the parameters for both wireless networks separately on devices with the option of a second WLAN interface.

⑥ Now you specify filter lists for stations (ACL) accessing the WLAN and protocols. Thereby, you restrict data exchange between the wireless network and the local network.

⑦ Now activate Stateful Inspection, ping-blocking and Stealth mode in the the firewall configuration.

⑧ The wizard will inform you when entries are complete. Complete the configuration with **Finish**.

7.3.2 Wizard for WEBconfig

Under WEBconfig you have the possibility to run the wizard **Security settings** to control and change the settings. The following values are handled:

- password for the device
- allowed protocols for the configuration access of local and remote networks
- parameters of configuration lock (number of failed log-in attempts and duration of the lock)
- security parameters as WLAN name, closed network function, WEP key, ACL list and protocol filters

7.4 The firewall wizard

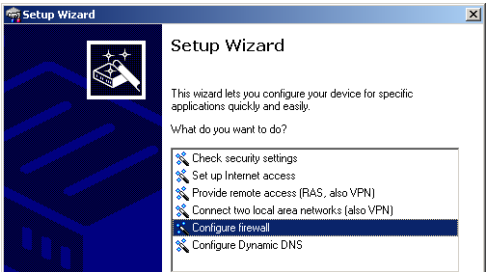
The LANCOM Router incorporates an effective protection of your WLAN when accessing the Internet by its Stateful Inspection firewall and its firewall filters. Basic idea of the Stateful Inspection firewall is that only self-initiated data transfer is considered allowable. All unasked accesses, which were not initiated from the local network, are inadmissible.

The firewall wizard assists you to create new firewall rules quickly and comfortably.

Please find further information about the firewall of your LANCOM and about its configuration in the reference manual.

7.4.1 Wizard for LANconfig

① Mark your LANCOM Router in the selection window. Select from the command bar **Extras** ▶ **Setup Wizard**.



② Select in the selection menu the setup wizard **Configuring Firewall** and confirm your choice with **Next**.

③ In the following windows, select the services/protocols the rule should be related to. Then you define the source and destination stations for this rule and what actions will be executed when the rule will apply to a data packet.

④ You finally give a name to the new rule, activate it and define, whether further rules should be observed when the rule will apply to a data packet.

⑤ The wizard will inform you as soon as the entries are complete. Complete the configuration with **Finish**.

7.4.2 Configuration under WEBconfig

Under WEBconfig it is possible to check and modify all parameters related to the protection of the Internet access under **Configuration** ▶ **Firewall / QoS** ▶ **Rules** ▶ **Rule Table.**

7.5 The security checklist

The following checklist provides a comprehensive overview of all security settings for professionals. Most of the points on this checklist are no subject of concern in simple configurations, since these generally adequate security settings are already implemented during basic configuration and by the security wizard.

Detailed information on the security settings listed here can be found in the reference manual.

EN

- **Have you assigned a password for the configuration?**

  The simplest option for the protection of the configuration is the establishment of a password. As long as a password hasn't been set, anyone can change the configuration of the device. The box for entering the password is located in LANconfig in the 'Management' configuration area on the 'Security' tab. It is particularly advisable to assign a password to the configuration if you want to allow remote configuration.

- **Have you permitted remote configuration?**

  If you do not require remote configuration, then deactivate it. If you require remote configuration, then be sure to assign a password protection for the configuration (see previous section). The field for deactivating the remote configuration is also contained in LANconfig in the 'Management' configuration area on the 'Security' tab. Select here under 'Access rights - of remote networks' for all types of configuration the option 'not allowed'.

- **Have you permitted the configuration by the wireless network?**

  If you do not require configuration by the wireless network, then deactivate it. The field for deactivating the configuration by the wireless network is also contained in LANconfig in the 'Management' configuration area on the 'Security' tab. Select here under 'Access rights - from Wireless LAN' for all types of configuration the option 'not allowed'.

- **Have you assigned a password to the SNMP configuration?**

  Also protect the SNMP configuration with a password. The field for protection of the SNMP configuration with a password is also contained in LANconfig in the 'Management' configuration area on the 'Security' tab.

- **Have you activated the Firewall?**

  The Stateful Inspection Firewall of the LANCOM ensures that your local network cannot be attacked from the outside. The Firewall can be enabled in LANconfig under 'Firewall/QoS' on the register card 'General'.

- **Do you make use of a 'Deny All' Firewall strategy?**

  For maximum security and control you prevent at first any data transfer through the Firewall. Only those connections, which are explicitly desired have to allowed by the a dedicated Firewall rule then. Thus 'Trojans' and certain E-mail viruses loose their communication way back. The Firewall rules are summarized in LANconfig under 'Firewall/Qos' on the register card 'Rules'. A guidance can be found in the reference manual.

- **Have you activated the IP masquerading?**

  IP masquerading is the hiding place for all local computers for connection to the Internet. Only the router module of the unit and its IP address are visible on the Internet. The IP address can be fixed or assigned dynamically by the provider. The computers in the LAN then use the router as a gateway so that they themselves cannot be detected. The router separates Internet and intranet, as if by a wall. The use of IP masquerading is set individually for each route in the routing table. The routing table can be found in the LANconfig in the 'IP router' configuration section on the 'Routing' tab.

- **Have you closed critical ports with filters?**

  The firewall filters of the LANCOM Router devices offer filter functions for individual computers or entire networks. Source and target filters can be set for individual ports or for ranges of ports. In addition, individual protocols or any combinations of protocols (TCP/UDP/ICMP) can be filtered. It is particularly easy to set up the filters with LANconfig. The 'Rules' tab under 'Firewall/QoS' can assist you to define and change the filter rules.

- **Have you excluded certain stations from access to the router?**

  Access to the internal functions of the devices can be restricted using a special filter list. Internal functions in this case are configuration sessions via LANconfig, WEBconfig, Telnet or TFTP. This table is empty by default and so access to the router can therefore be obtained by TCP/IP using Telnet or TFTP from computers with any IP address. The filter is activated when the first IP address with its associated network mask is entered and from that point on only those IP addresses contained in this initial entry will be permitted to use the internal functions. The circle of authorized users can be expanded by inputting further entries. The filter entries can describe both individual computers and whole networks. The access list can be found in LANconfig in the 'TCP/IP' configuration section on the 'General' tab.

- **Is your saved LANCOM configuration stored in a safe place?**

  Protect the saved configurations against unauthorized access in a safe place. A saved configuration could otherwise be loaded in another device by an unauthorized person, enabling, for example, the use of your Internet connections at your expense**.**

EN

- **Have you secured your wireless network encryption, an ACL and LEPS?**

  With the help of 802.11i, WPA or WEP, you can encrypt the data in your wireless network with different encryption methods such as AES, TKIP or WEP. LANCOM Systems recommends the strongest possible encryption by using 802.11i and AES. If the WLAN client adapters do not support these, then you should use TKIP or at least WEP. Make sure that the encryption function in your device is activated, and that at least one passphrase or WEP key has been entered and selected for application.

  Ex-factory, WEP128 encryption is activated for every unconfigured device as standard. This WEP encryption in WLAN devices being managed by a LANCOM WLAN Controller is overwritten by the central encryption settings in the profiles of the WLAN Controller.

  To check the WEP settings, open LANconfig, go to the configuration area and select 'WLAN security' on the '802.11i/WEP' tab to view the encryption settings for the logical and physical WLAN interfaces.

  Change the default WEP password immediately after configuring the router for the first time.

  With the Access Control List (ACL) you can permit or prevent the access to your wireless LAN by individual clients. The decision is based on the MAC address that is permanently programmed into wireless network adapters. To check the Access Control List, go to the configuration area in LANconfig and select 'WLAN security' on the 'Stations' tab.

  The LANCOM Enhanced Passphrase Security (LEPS) uses an additional column in the ACL to assign an individual passphrase consisting of any 4 to 64 ASCII characters to each MAC address. The connection to the access point and the subsequent encryption with IEEE 802.11i or WPA is only possible with the right combination of passphrase and MAC address.

- **Have you set the 802.1x functions for particularly sensitive data exchange in the wireless network?**

  If you have a particularly sensitive data exchange in your wireless network, you can use the IEEE-802.1x technology for a more extensive protection. To control or to activate the IEEE-802.1x settings, select in LANconfig the configuration area 'User registration'.

- **Have you activated the mechanism that protects your WAN lines if the device is stolen?**

  After being stolen, the device can theoretically be operated at another location by unauthorized persons. Password-protected device configurations offer no protection from the operation of the RAS access, LAN coupling or VPN connections that are set up in the device; a thief could gain access to a protected network.

  The device's operation can be protected by various means; for example, it will cease to function if there is an interruption to the power supply, or if the device is switched on in another location.

  The scripting function can store the entire configuration in RAM only so that restarting the device will cause the configuration to be deleted. The configuration is not written to the non-volatile flash memory. A loss of power because the device has been relocated will cause the entire configuration to be deleted. Further information can be found in the reference manual.

  For self-sufficient operations, the configuration for a WLAN interface being managed by a LANCOM WLAN Controller is stored in flash memory for a certain time only, or even in the RAM only. This device configuration is deleted if contact to the WLAN Controller is lost or if the power supply is interrupted for longer than the set time period.

- **Have you ensured that the reset button is safe from accidental configuration resets?**

  Some devices simply cannot be installed under lock and key. There is consequently a risk that the configuration will be deleted by mistake of a co-worker presses the reset button too long.

  With a suitable setting, the behavior of the reset button can be controlled; the button is then ignored or a press of the button prompts a re-start only, however long it is held down.

EN

8 Options and accessories

Your LANCOM device has numerous extensibilities and the possibility to use a broad choice of LANCOM accessories. You find in this chapter information about the available accessories and how to use them with your base station.

- The range of the base station can be increased by optional antennas of the LANCOM Wireless Router series and can be adapted to special conditions of environs.
- With the LANCOM Public Spot Option option it is possible to extend the LANCOM Router for additional billing and accounting functions in order to upgrade it to a Wireless Public Spot.

8.1 Optional LANCOM WLAN antennas

To increase the range of the LANCOM base station or to adapt the base station to special conditions of environs, you can connect LANCOM WLAN antennas at the base station. An overview of suitable antennas can be found on the LANCOM web site under www.lancom.eu.

For help with calculating the correct antenna setup for external LANCOM AirLancer Extender antennas or for antennas of other vendors, please refer to www.lancom.eu

When installing external antennas, ensure that you observe the statutory limitations of the country in which the WLAN device is being operated. To help with this, you can enter the transmitting power minus the cable loss into the LANCOM configuration. These data enable LCOS to automatically calculate the correct transmitting power for the selected country.

Antennas are only to be attached or changed when the device is switched off. Mounting or demounting antennas while the device switched on may cause the destruction of the WLAN module!

8.1.1 Antenna Diversity

The transmission of radio signals can suffer from significant signal losses because of reflection and scatter, among other reasons. In some areas, the interaction with the reflected radio waves can cause a drop in signal strength, or even cause it to be cancelled out completely.

EN

Transmission quality can be improved with so-called "diversity" methods. The principle of diversity methods relies on the fact that a transmitted signal is often received multiple times (generally twice). With appropriate processing, these signals can be re-combined into a single signal. The most common methods are space diversity and polarization diversity.

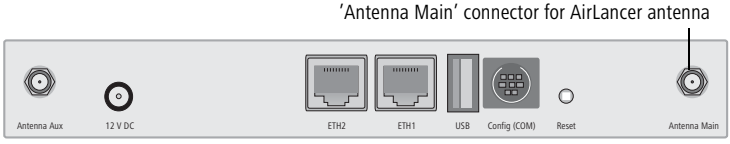
LANCOM Systems supplies a variety of polarization-diversity antennas as accessories for LANCOM Wireless Router. These models enable two orthogonally polarized signals to be received with a single antenna. Further information about this technique is available in our "Polarization Diversity" techpaper.

Polarization diversity antennas from LANCOM Systems:

- AirLancer Extender O-D80g (2.4 GHz band), item no. 61221
- AirLancer Extender O-D60a (5 GHz band), item no. 61222

8.1.2 Installation of AirLancer Extender antennas

For installation of an optional AirLancer antenna turn off the LANCOM Wireless Router by pulling out the power supply cable of the device. Remove now carefully the two diversity antennas on the back by screwing them out. Connect the AirLancer antennas to the antenna connector with the inscription 'Antenna Main'.



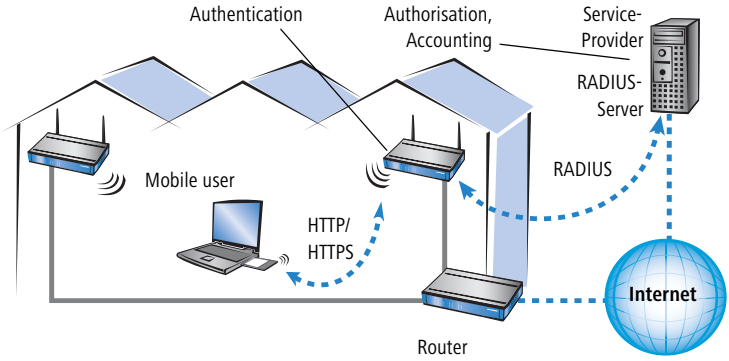
8.2 LANCOM Public Spot Option

Wireless public spots are publicly accessible points, at which users with their own mobile computers can dial wirelessly into a network, usually into the Internet.

The Wireless LAN technology is ideally suitable to offer wireless Internet services to the public at places such as airports, hotels, stations, restaurants or cafés, so-called Public Hot Spots. The LANCOM Public Spot Option is intended for operators of public wireless networks, and unveils additional functions for authentication and billing of public Internet services for the LANCOM Router base station, thus enabling a simple set-up and maintenance of public hot spots.

EN

The LANCOM Public Spot Option is the optimal solution for public Wireless LANs. Wireless LANs are very suitable for company networks and for wireless networking at home. But for public access services, there is a lack of mechanisms for authentication and billing of single users (AAA - Authentication / Authorisation / Accounting). This lack remedies the LANCOM Systems Open User Authentication (OUA), the main part of the LANCOM Public Spot Option. The OUA procedure realizes the authentication of all wireless clients via user name and password, and checks the authorization of single users via RADIUS. Accounting data (online time and data volume) can be transferred per user and per session to a central RADIUS server. Client PCs need only radio card (e.g. AirLancer), TCP/IP and an Internet browser. Additional software is not needed. Therefore, the public spot option is ideally suitable to install wireless Internet access services in hotels, restaurants, cafés, airports, stations, exhibition centres or universities.



With the LANCOM Public Spot Option you extend a base station additionally with these functions and upgrade it to a Wireless Public Spot.

9 Troubleshooting

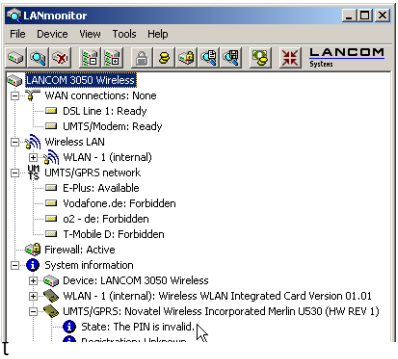
In this chapter, you will find suggestions and assistance for a few common difficulties.

9.1 PIN Handling

Depending on the configuration, a LANCOM with UMTS/HSPDA function and an inserted data card tries to establish a connection to the Internet immediately after being switched on. For this purpose, the PIN saved in the configuration of the device is transferred to the SIM card in the data card to enable the connection to an UMTS/HSPDA or GPRS net.

As soon as an incorrect PIN is stored in the configuration, the device transmits this invalid PIN to the SIM card. After three unsuccessful attempts, most cards are automatically locked and can only be reinstated by entering an additional number (depending on the provider PIN2 or PUK).

Whenever a device is set to automatically establish a connection to the Internet, three attempts with an invalid PIN may be performed within a few seconds without the user noticing. To prevent this, a LANCOM with the UMTS/HSPDA function disables further attempts as soon as the device makes an attempt to establish a connection to the Internet with an invalid PIN. LANmonitor displays this condition with the error message 'The PIN is invalid':



t

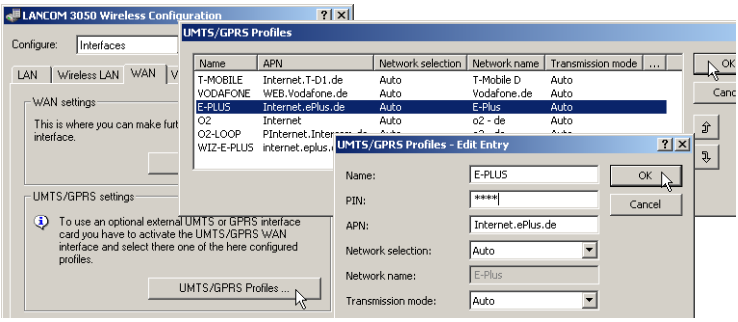
he connection to the Internet proceed as follows:

① Change the PIN in the UMTS/HSPDA/GPRS Profiles.

Configuration with LANconfig

The UMTS GPRS Profiles are located in LANconfig in the configuration area 'Interfaces' on the register card 'WAN' on the button UMTS/HSPDA/GPRS Profiles.

EN



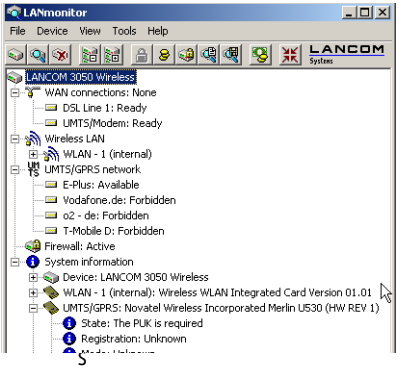
Configuration with WEBconfig or Telnet

Under WEBconfig or Telnet the UMTS/HSPDA/GPRS Profiles are located under the following directories:

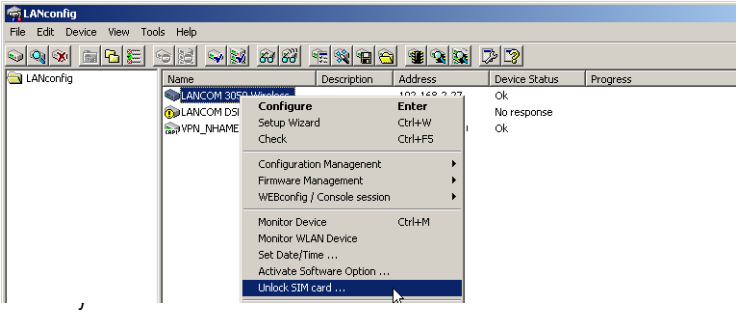
Konfigurationstool	Menü/Tabelle
WEBconfig	Expert-Configuration ▶ Setup ▶ Interfaces ▶ UMTS-GPRS-Parameters ▶ Profiles
Terminal/Telnet	`Setup/Interfaces/UMTS-GPRS-Parameters`

② The next attempt with the valid PIN number should occur without error.

After the third attempt with an invalid PIN the SIM card is locked. This error is also displayed on LANmonitor ('The PUK is required').



e you can unlock the SIM card with LANconfig over the context menu of the device.



a data card is supplied with the operating software from the net provider. With this software the PIN number of the SIM card can be changed whenever required.

EN

9.2 No DSL connection is established

After start-up the router automatically attempts to connect to the DSL provider. During this process, the DSL-LED will blink green. If successful, the LED will switch over to steady green. If, however, the connection can't be established, the DSL-LED will light up red. The reason for this is usually one of the following:

Problems with the cabling?

Only the cable provided with your device should be used to connect to DSL. This cable must be connected to the Ethernet port of your broadband access device. The DSL-LED must light green indicating the physical connection.

Has the correct transfer protocol been selected?

The transfer protocol is set along with the basic settings. The basic setup wizard will enter the correct settings for numerous DSL providers automatically. Only if your DSL provider is not listed, you will have to enter manually the protocol being used. In any case, the protocol that your DSL provider supplies you with should definitely work.

You can monitor and correct the protocol settings under:

Configuration tool	Run command
LANconfig	Management ▶ Interfaces ▶ Interface settings ▶ WAN Interface
WEBconfig	Expert Configuration ▶ Setup ▶ Interfaces ▶ WAN Interface

9.3 DSL data transfer is slow

The data transfer rate of an broadband (Internet) DSL connection is dependent upon numerous factors, most of which are outside of one's own sphere of influence. Important factors aside from the bandwidth of one's own Internet connection are the Internet connection and current load of the desired target. Numerous other factors involving the Internet itself can also influence the transfer rate.

Increasing the TCP/IP window size under Windows

If the actual transfer rate of a DSL connection is significantly below the fastest rate listed by the provider, there are only a few possible causes (apart from the above-mentioned external factors) which may involve one's own equipment.

One common problem occurs when large amounts of data are sent and received simultaneously with a Windows PC using an asynchronous connection. This can cause a severe decrease in download speed. The cause of this problem is what is known as the TCP/IP receive window size of the Windows operating system that is set to a value too small for asynchronous connections.

Instructions on how to increase the Windows size can be found in the Knowledge Base of the support section of the LANCOM web site (www.lancom.eu).

9.4 Unwanted connections under Windows XP

Windows XP computers attempt to compare their clocks with a timeserver on the Internet at start-up. This is why when a Windows XP in the WLAN is started, a connection to the Internet is established by the LANCOM.

To resolve this issue, you can turn off the automatic time synchronization on the Windows XP computers under **Right mouse click on the time of day** ▶ **Properties** ▶ **Internet time**.

10 Appendix

10.1 Performance data and specifications

EN

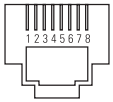
		LANCOM 3850 UMTS
Frequency band		2400 - 2483,5 MHz (ISM) or 5150 - 5750 MHz
Connections	ETH1, ETH2	10/100base-TX, autosensing
	WLAN1	Two reverse SMA connections with antenna diversity
	WLAN2	32 bit cardbus interface for optional UMTS or second radio card
Power supply	12V DC via external power supply adapter, or Power over Ethernet by IEEE 802.3 standard	
Antenna connection	Two reverse SMA connections for external LANCOM AirLancer-Extender antennas and 3-dBi-dipol dualband antennas (in package contents) Please respect the restrictions given in your country when setting up an antenna system. For information about calculating the correct antenna setup, please refer to www.lancom-systems.com.	
Housing	210 mm x 143 mm x 45 mm (B x H x T), rugged plastic case, stackable, provision for wall mounting	
Norms	CE compliant according to ETSI EN 300 328, ETSI EN 301 893, ETSI EN 301 489-1, ETSI EN 301 489-17, EN 60950 Radio licenses for all EU countries and Switzerland	
Regulations	Notified in Germany, Belgium, Netherlands, Luxemburg, Austria, Switzerland, United Kingdom, Italy, France, Spain, Portugal	
Environment	Temperature range 0 °C to +50 °C at 95 % max. humidity (non condensing)	
Service	Warranty: 3 years	
Support	Via hotline and Internet	
Accessories	■ LANCOM Modem Adapter Kit for connecting modems (analog or GSM) to the serial configuration interface (item no. 61500) ■ LANCOM Advanced VPN Client for Windows 98SE-XP, 1 License, item no. 61600 ■ LANCOM Advanced VPN Client for Windows 98SE-XP, 10 Licenses, item no. 61601 ■ LANCOM Advanced VPN Client for Windows 98SE-XP, 25 Licenses, item no. 61602 ■ LANCOM ES-1108P compact, robust 8-port Ethernet switch with 4 PoE interfaces, item no. 61450 ■ Lightning-protector adapter SA-5 (2.4 and 5 GHz), item no. 61212 ■ Lightning-protector adapter SA-LAN, item no. 61213 ■ LANCOM Rack Mount Option (item no. 61501)	
Options	■ LANCOM VPN Option 25 channels (hardware accelerated, max. 25 simultaneous connections, 50 connections configurable) for VPN in WAN (item no.60083) ■ LANCOM Public Spot Option (item no. 60642)	

EN

10.2 Contact assignment

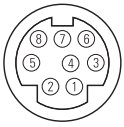
10.2.1 LAN/WAN interface 10/100Base-TX, DSL interface

8-pin RJ45 socket, corresponding to ISO 8877, EN 60603-7

Connector	Pin	IAE
	1	T+
	2	T-
	3	R+
	4	PoE/G
	5	PoE/G
	6	R-
	7	PoE/-48 V
	8	PoE/-48 V

10.2.2 Configuration interface (Outband)

8-pin mini-DIN socket

Connector	Pin	IAE
	1	CTS
	2	RTS
	3	RxD
	4	RI
	5	TxD
	6	DSR
	7	DCD
	8	DTR
	U	GND

10.3 Declaration of conformity

LANCOM Systems herewith declares that the devices of the type described in this documentation are in agreement with the basic requirements and other relevant regulations of the 1995/5/EC directive.

The CE declarations of conformity for your device are available in the appropriate product area on the LANCOM Systems web site (www.lancom.eu).

11 Radio channel regulations for WLANs

Information about approvals and notifications in various countries and the radio channel regulations can be found in the reference manual or on the LANCOM Systems web site (www.lancom.eu).

Index

EN

EN