

LANCOM 1751 UMTS

© 2008 LANCOM Systems GmbH, Wuerselen (Germany). All rights reserved.

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 (eyay@cryptsoft.com).

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

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, Oktober 2008

Preface

Thank you for your confidence in us!

With its integrated UMTS/HSxPA modem, the ADSL2+ router LANCOM 1751 UMTS sets standards in flexibility and redundancy. Should a standard DSL connection fail at a site, branch office or subsidiary, automatic compensation is provided by a broadband UMTS/HSxPA or EDGE backup connection. Alternatively the ISDN interface can be used as a further backup line or for remote access. Along with this unique level of high availability, the LANCOM 1751 UMTS is equipped as standard with 5 VPN channels (optionally 25), an integrated ADSL2+ modem and four separately configurable switch ports, so offering a huge variety of professional applications.

The SIM-card holder is easily accessible via the back cover and, by connecting an external UMTS antenna, indoor reception can be greatly improved. A real highlight: Anti-theft by ISDN self-callback and location determination by GPS!

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 also contains all of the important technical specifications.

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)
- Backup solutions
- LANCAPI
- 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.

Contents

1 Introduction	9
1.1 Various backup strategies	9
1.1.1 Backup via mobile-telephony lines	9
1.1.2 Backup via ISDN direct dial connection	11
1.1.3 Backup with VRRP	11
1.2 Location verification via ISDN or GPS	12
1.3 What can your LANCOM do?	13
2 Installation	16
2.1 Package content	16
2.2 System requirements	16
2.3 Status displays, interfaces	17
2.3.1 Status displays	17
2.3.2 Device connectors	22
2.4 Hardware installation	24
2.5 Software installation	25
2.5.1 Starting the software setup	25
2.5.2 Which software should I install?	26
3 Basic configuration	27
3.1 Which information is necessary?	27
3.1.1 TCP/IP settings	27
3.1.2 Configuration protection	29
3.2 Instructions for LANconfig	29
3.3 Instructions for WEBconfig	30
3.4 TCP/IP settings to workstation PCs	35
3.5 Location verification by ISDN or GPS	36
3.5.1 GPS location verification	36
3.5.2 ISDN location verification	36
3.5.3 Configuring location verification	36

4 Security settings	42
4.1 Tips for handling keys	42
4.2 The security settings wizard	42
4.2.1 Wizard for LANconfig	43
4.2.2 Wizard for WEBconfig	43
4.3 The security checklist	44
5 Setting up Internet access	47
5.1 The Internet Connection Wizard	49
5.1.1 Instructions for LANconfig	49
5.1.2 Instructions for WEBconfig	50
5.2 The Firewall Wizard	50
5.2.1 LANconfig Wizard	51
5.2.2 Configuration under WEBconfig	51
6 Connecting two networks	52
7 Providing dial-in access	54
8 Setting up the UMTS profile	56
8.1 Internet access	56
8.2 VPN site coupling	59
8.3 Other settings	61
8.3.1 Choosing the mobile telephone network	61
8.3.2 Activate UMTS/GPRS profile	62
8.3.3 UMTS/HSxPA only or automatic UMTS/HSxPA/GPRS selection	63
8.3.4 Set up a time limit	64
9 Troubleshooting	65
9.1 No DSL connection is established	65
9.2 DSL data transfer is slow	65
9.3 Unwanted connections under Windows XP	66

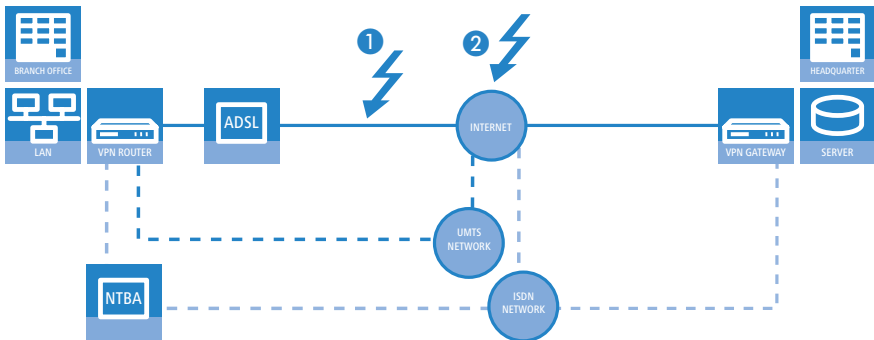
10 Appendix	67
10.1 Performance and characteristics	67
10.2 Contact assignment	68
10.2.1 ADSL interface	68
10.2.2 ISDN S ₀ interface	69
10.2.3 Ethernet interface 10/100Base-TX	69
10.2.4 Configuration interface (Outband)	70
10.3	70
10.4 Declaration of conformity	70
11 Index	71

1 Introduction

Networked cooperation between several offices or even between continents has become an everyday part of modern business. The paths of communication between headquarters, subsidiaries and field workers increasingly rely upon public infrastructures. VPN has become established as the de facto standard for cost-effective and secure enterprise communications over the Internet.

However, many of important elements in these network structures remain susceptible to failure which could have severe consequences for business operations:

- The Internet-access cable between the site and the provider ❶ could fail; after damage from construction work, for example.
- Provider's network ❷ may be disturbed or even fail.



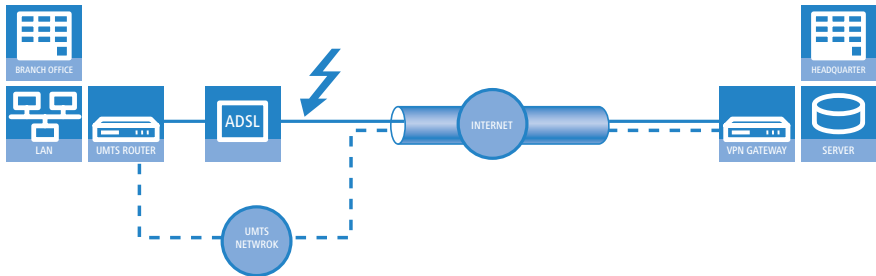
LANCOM UMTS Routers of the type LANCOM 1751 UMTS are equipped with a UMTS modem and an ISDN interface to offer two integrated options for establishing alternative connections. The LCOS operating system provides a range of security and backup functions to protect your multi-site network from disturbances of this type.

1.1 Various backup strategies

1.1.1 Backup via mobile-telephony lines

Backup solutions that rely on ISDN or analog telephone lines are the most common method used today to ensure high availability of data lines such as those between branch offices and computer centers in large company net-

works. The standard Internet connection is typically provided via an inexpensive DSL connection and a backup line in the form of an ISDN/analog line takes up the data traffic if the normal line should be disturbed.



As an alternative to this ISDN/analog backup scenario, mobile telephony connections can also be used to ensure the availability of data connections. If an Internet connection is operated via a LANCOM 1751 UMTS, then any interruption to the ADSL line can be immediately substituted by the mobile-telephony line. The LANCOM 1751 UMTS supports all current mobile technologies: GPRS, EDGE, UMTS and HSxPA.

The various mobile telephony technologies in overview:

- **GPRS:** General Packet Radio Service, technology for packet-orientated data transfer in GSM networks. Achieves in practice data-transfer speeds of up to 56 kbps.
- **EDGE:** Enhanced Data Rates for GSM Evolution is technology that increases data rates over GPRS by using an additional method of modulation. EDGE achieves theoretical data rates of up to 384 kbps downstream and ca. 110 kbps upstream. EDGE is widely available in many countries and offers an interesting alternative to UMTS.
- **UMTS:** The Universal Mobile Telecommunications System is also known as the third-generation mobile-telecommunications standard (3G). The first version of UMTS reaches download rates of 384 kbps.
- **HSxPA:** High Speed Downlink Packet Access (HSDPA) and High Speed Uplink Packet Access (HSUPA) are protocol additions to UMTS. Various versions of HSDPA achieve download rates of up to 14.6 Mbps, HSUPA reaches upload rates of up to 5.8 Mbps.

Actual available bandwidths depend on the version supported by the network operator and on the UMTS modem in use.

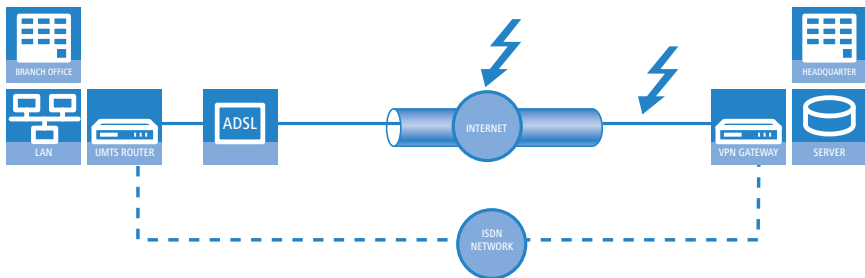
Advantages of mobile-telephony backup over ISDN/analog:

- Faster than ISDN/analog: Data throughput is far higher with UMTS/HSxPA.

- More secure than ISDN or analog: If physical damage should be the cause of ADSL-line failure then the ISDN/analog line will generally have been damaged at the same time because both methods use the same physical cable.
- Cheaper than ISDN: Depending on the tariff, monthly running costs for mobile telephony can be significantly lower than the costs for an ISDN connection. As actual downtimes of ADSL connections typically add up to just a few hours a year, the relatively high connection costs for mobile telephony are simply not relevant. According to needs, billing can be based on data volume instead of time.

1.1.2 Backup via ISDN direct dial connection

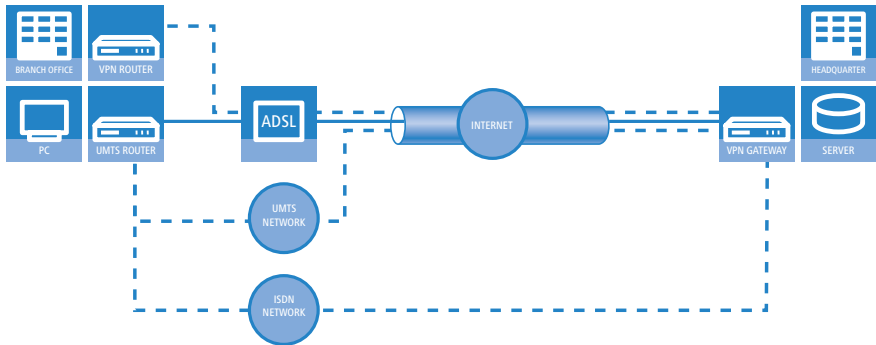
In the case that a branch office is connected to the headquarters via a VPN connection, it may well be worthwhile for the Internet-based VPN connection to be backed up by a direct ISDN dial-in connection in addition to the UMTS/HSxPA backup. Should the provider's network or the Internet connection to the headquarters fail, then data transmission can be continued over the ISDN coupling.



1.1.3 Backup with VRRP

A sophisticated backup system for protection against router hardware failure can be implemented with 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/HSxPA 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/HSxPA interface can take its place further along in the backup chain should the the backup router also fail.



Further information on backup solutions using VRRP are available in the LCOS reference manual.

1.2 Location verification via ISDN or GPS

In large-scale installations with unsupervised routers, there is a risk that the devices could be stolen and then operated at another location. If the devices have been configured for RAS access, LAN coupling or VPN connections, a thief could gain access from a different location to a protected network.

Location verification can prevent the misuse of a router: Each time it is switched on, the router carries out a check to make sure that it is installed at the intended location. Only after confirming its location will the router start transferring payload data over its WAN interfaces.

Two methods of location verification are available:

- Via an ISDN telephone call to itself the device can test whether it is connected to the expected ISDN telephone line.

Prerequisites for successful ISDN location verification:

- ☐ The device must be reachable from the public ISDN telephone network.
- ☐ The device needs two free B channels for the duration of the check. If just one channel is free, e.g. one channel at a point-to-multipoint connection with two B channels is being used for a telephone call, then the device cannot make a call to itself via ISDN.

- By means of GPS location determination the device can compare the actual geographical coordinates with the set values. A tolerance of a few meters is necessary.

Prerequisites for successful GPS location verification:

- ☐ A suitable GPS antenna must be connected to the AUX connector.
- ☐ The GPS signal must be of sufficient strength at the location.
- ☐ A SIM card for mobile telephone service is inserted and the device is connected to a cellular network.

1.3 What can your LANCOM do?

The following table shows the properties and functions of your device

LANCOM 1751 UMTS	
Applications	
Internet Access	✓
LAN to LAN coupling via VPN	✓
LAN to LAN coupling via ISDN	✓
RAS server (via VPN)	✓
RAS server (via ISDN)	✓
IP router	✓
NetBIOS proxy for coupling of Microsoft peer-to-peer networks via ISDN	✓
DHCP and DNS server (for LAN and WAN)	✓
Advanced Routing and Forwarding (ARF networks)	8
N:N mapping for coupling networks using the same IP address ranges	✓
Configuring LAN ports as additional WAN ports	✓
Policy-based routing for policy-based selection of target routes	✓
Load-balancing for bundling of multiple DSL channels	4 channels
Backup solutions and load balancing with VRRP	✓

LANCOM 1751 UMTS	
PPPoE Server	✓
WAN RIP	✓
Layer 2 QoS tagging	✓
802.1p	✓
NAT Traversal (NAT-T)	✓
DMZ with configurable IDS checks	✓
ISDN leased lines	✓
LANCAPi server to provide office applications such as fax or answering machine via the ISDN interface.	✓
WAN connections	
Integrated ADSL modem (with ADSL2+)	✓
Integrated UMTS/HSxPA modem (GPRS, EGDE, UMTS, HSxPA)	✓
ISDN S ₀ bus in multi device-mode or in point-to-point mode with automatic D-channel protocol identification. Supports static and dynamic channel bundling per MLPPP and BACP as well as Stac data compression (Hi/fn)	✓
LAN connection	
Separate FastEthernet LAN ports, individually switchable, e.g. as LAN switch or separate DMZ ports; auto crossover. Alternatively switchable as a WAN interface.	4
Security functions	
IPSec encryption via external software (VPN client)	✓
5 integrated VPN tunnels for secure network connections	✓
IPSec encryption in hardware (optional; activated with the VPN-25 option)	✓
IP masquerading (NAT, PAT) to conceal individual LAN workstations behind a single public IP address.	✓
Stateful-inspection firewall	✓
Firewall filter for blocking individual IP addresses, protocols and ports	✓

LANCOM 1751 UMTS	
MAC address filter regulates, for example, LAN-workstation access to the IP routing function	✓
Protection of the configuration from brute-force attacks.	✓
Anti-theft with verification via or ISDN or GPS.	✓
Configuration	
Configuration with LANconfig or via web browser; additional terminal mode for Telnet or equivalent terminal programs; SNMP interface and TFTP server function.	✓
1-Click-VPN wizard for easiest setup of RAS access and site-to-site LAN coupling via VPN	✓
Remote configuration via ISDN (with ISDN PPP connections, e.g. via Windows Dial-Up Networking).	✓
Serial configuration interface	✓
Call-back function with PPP authentication mechanisms allowing only predefined ISDN call numbers	✓
FirmSafe for no-risk firmware updates	✓
Optional software extensions	
LANCOM VPN Option with 25 active tunnels for secure network coupling; includes activation of the hardware accelerator	✓
Optional hardware extensions	
19" Rackmount-Adapter	✓

2 Installation

2.1 Package content

Before beginning with the installation, please check that nothing is missing from your package. Along with the LANCOM UMTS Router the box should contain the following accessories:


	LANCOM 1751 UMTS
12 V DC power adapter	✓
LAN cable (green connectors)	✓
ADSL connector cable (transparent connectors)	✓
ISDN connector cable (light-blue connectors)	✓
Connector cable for the configuration interface	✓
Two 2-dBi dipole UMTS/GPRS antennas (850-960 Mhz and 1700-2220 Mhz) with SMA connector	✓
GPS antenna with SMA connector and 5 m cable	✓
LANCOM CD	✓
Printed documentation	✓

Should anything be missing, please take up immediate contact to your dealer or to the address on the delivery note supplied with your device.

2.2 System requirements

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.

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

2.3 Status displays, interfaces

2.3.1 Status displays

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 UMTS Routers have status displays on the front panel.



Top

The two top-mounted LEDs enable the main function status to be assessed even if the device is positioned 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
Red	Blinking	Time or charge limit on online connections has been reached
Red	Blinking	The device is locked because location verification was not successful



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'.

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

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.



Signal that a 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

3 ADSL status

Information on connection status at the ADSL connector:

Off		Interface deactivated
Green	Blinking/flashing	Handshake/training
Green	Permanently	Synchronization successful
Red	Flickering	Error (CRC error, framing error, etc.)
Red	On (permanently)	No synchronization, searching for remote station
Red/orange	Blinking	Hardware error

4 ADSL data

Information on data traffic at the ADSL connector:

Off		No logical connection
Green	Blinking	Opening the first connection
Green	Inverse flashing	Opening an additional connection
Green	Permanently	At least one logical connection is established
Green	Inverse flickering	Data traffic (send or receive)

5 ISDN status

Information on connection status at the ISDN S₀ connector:

Off		Not connected or no S ₀ voltage (no error message)
Green	Blinking	D-channel initialization (establishing contact to provider)
Green	On (permanently)	D-channel operational
Red	Flickering	D-channel error
Red	On (permanently)	D-channel activation failed



If the ISDN status LED goes off automatically, this does not indicate an error at the S₀ bus. It is in fact because several ISDN connections and PBXs switch the S₀ bus into power-saving mode after a certain period of inactivity. When needed, the S₀ bus automatically reactivates and the ISDN status LED illuminates in green.

6 ISDN Data

Status display for both ISDN B channels:

off		No connection established
green	Blinking	Dialling
green	Flashing	Establishing first connection
green	Inverse flashing	Establishing further connection
green	Constantly on	Connection established via B channel
green	Flickering	Data traffic (send or receive)

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

8 UMTS Status

Status of UMTS connections:

Off		UMTS interface switched off
Red	On (permanently)	UMTS interface switched off, UMTS module not (yet) found
Red/ green	Blinking	SIM card error
Orange	Blinking/Flashing	UMTS module found, login to the UMTS network active
Orange	On (permanently)	UMTS module ready, login to the UMTS network completed
Green	On (permanently)	GPRS connection available
Green	Blinking 1x per second	EDGE connection available
Green	Blinking 4x per second with breaks	UMTS connection available
Green	Blinking 8x per second with breaks	HSxPA connection available

9 UMTS Data

Information on data traffic on the UMTS interface:

Off		No UMTS connection
Green	Blinking	Dialling
Green	Flashing	Establishing the first connection
Green	Inverse flashing	Establishing an additional connection
Green	On (permanently)	At least one logical connection is established
Green	Inverse blinking	Data traffic (TX or RX)



The UMTS network supports currently one connection only.

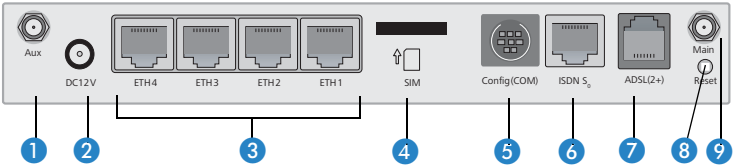
10 VPN

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

2.3.2 Device connectors

The rear panel accommodates the LANCOM UMTS Router's connectors:



1 Aux connector for a mobile-telephony or GPS antenna.

- If the Aux connector is being used for mobile telephony a diversity antenna is connected to the benefit of signal quality.
- If GPS location determination is to be used, a GPS antenna is connected to the Aux connector.



A GSM/UMTS/GPS combi antenna can be connected to the Aux connector, if GPS is used for location verification for a short while only. As soon as the location is correctly identified, the GSM/UMTS diversity function is available again and the GPS module is switched off automatically.

- 2 Connector for the supplied power adapter.
- 3 Switch with 10/100Base-Tx connectors
- 4 SIM card slot.
- 5 Serial configuration port (RS 232/V.24).
- 6 ISDN S₀ connection

- 7 ADSL connector (ADSL, ADSL 2, ADSL 2+)
- 8 Reset switch
- 9 Main connector for mobile telephony antenna. The Main connector is used for connecting the main antenna.

Reset button functions

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 mistake of a co-worker presses the reset button too long. With the suitable setting, the behavior of the reset button can be controlled.

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, there is no way to access the configuration! In this case the serial communications 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: 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.
- ☐ Reset-or-boot (standard setting): Press the button briefly to re-start 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.



After resetting, the device starts completely unconfigured and **all** settings are lost. If possible be sure to backup the current device configuration **before** resetting.

2.4 Hardware installation

Installation of the LANCOM UMTS Router involves the following steps:

- ① **Antennas** – screw the supplied mobile-telephony antennas to the rear panel of the LANCOM UMTS Router. Alternatively a GPS antenna can be screwed on to the Aux connector ① of the device.



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 UMTS module!



When mounting separately purchased mobile telephone antennas, please note that the maximum permitted transmission power for UMTS systems is not to be exceeded (0.25 W or 24 dBm EIRP). The system operator is responsible for observing these threshold values.

- ② **LAN** – First of all you can connect the LANCOM UMTS Router to the LAN. Plug in one end of the supplied network cable (green connectors) to a LAN connector on the device ③ and the other end into an available network connector socket in your local network or on a hub or switch. Alternatively you can connect a single PC.

The LAN connector automatically recognises the wiring (Auto MDI/X) and the transfer rate (10/100 Mbit) by autosensing.

Information about the installation of PoE can be found in the information box 'Power over Ethernet—elegant power supply over LAN cabling'.

- ③ **ADSL** – connect the ADSL interface ⑦ with the splitter by using the supplied ADSL connector cable (transparent connectors).



ADSL can be operated at analog telephone lines (Annex A) or at ISDN lines (Annex B). One of these two variants is on offer depending on the country and the provider. A LANCOM 1751 UMTS can be set up to the required version by uploading the appropriate firmware.

- ④ **Connecting to the ISDN** – to connect the LANCOM UMTS Router to the ISDN, plug in one end of the supplied ISDN cable (light-blue connectors) to an ISDN S_0 interface ⑥ Plug in the other end of the ISDN cable into an ISDN/ S_0 point-to-point line connector or point-to-multipoint line connector.
- ⑤ **Insert SIM card** – slide the SIM card into the slot ④, using the marker to ensure that the card is the right way round.



Please pay attention, that the SIM card snaps into the slot when sliding in. To remove the card from the device, slightly press the card into the device. After releasing, the card looses from the locked position in the slot.

- ⑥ **Power supply** – the socket ② is for connecting the supplied power supply unit.



Use only the power adapter mentioned in the technical data! The use of the wrong power adapter can be of danger to the device or persons.

- ⑦ **Ready for operation?** – After a brief self-test the power LED lights up permanently in green or it blinks alternately in red and green until a configuration password is set.

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 UMTS Router exclusively with computers running operating systems other than Windows.

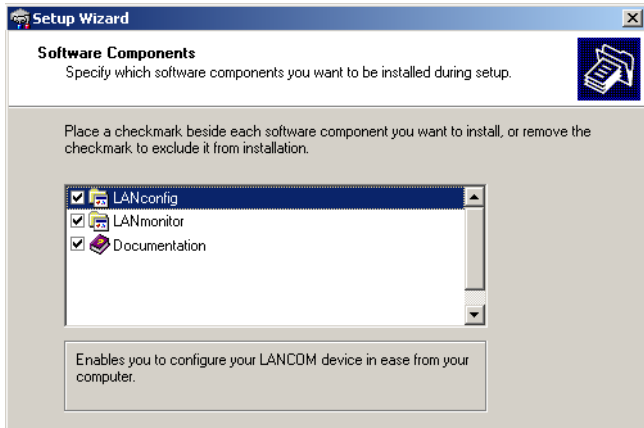
2.5.1 Starting the software setup

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 LANCOM CD.

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.
- 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
- 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.

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 LANCOM UMTS Router
- setup of a new network

Fully automatic TCP/IP configuration will not be available when integrating the LANCOM UMTS Router 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 LANCOM UMTS Router 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 LANCOM UMTS Router

Assign a free IP address from the address range of your LAN to the LANCOM UMTS Router and specify the netmask.

3.1.2 Configuration protection

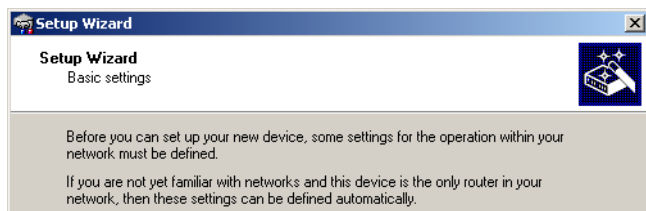
The password for configuration access to the LANCOM protects the configuration against unauthorized access. The configuration of the device contains a considerable amount of sensitive information such as your Internet access information. We therefore strongly recommend protecting it with a password.



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.

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 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 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.

- ③ 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**.

- ④ Specify whether or not the router should act as a DHCP server. Make your selection and confirm with **Next**.
- ⑤ 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.

- ⑥ 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**.
- ⑦ 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**.
- ⑧ Connect charge protection can limit the cost of DSL connections to a pre-determined amount if desired. Confirm your choice with **Next**.
- ⑨ Complete the configuration with **Finish**.



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

3.3 Instructions for WEBconfig

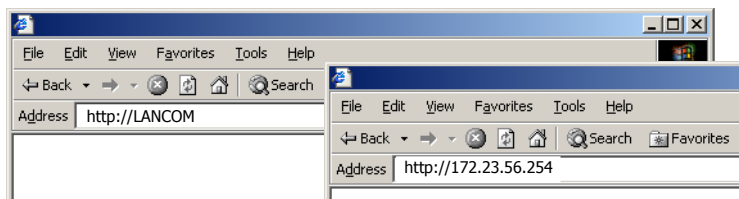
To configure the device with WEBconfig you must know how to address it in the LAN. The reaction of the devices, as well as their accessibility for configuration via web browser is dependent on whether a DHCP server and a DNS server are already active in the LAN, and whether these two server processes 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.

Network without DHCP server

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**.



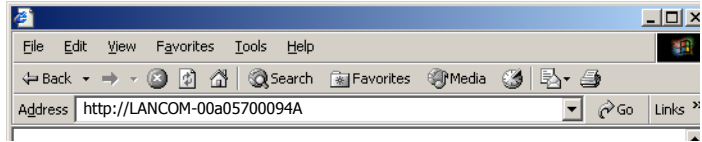
If the configuration PC does not obtain its IP address from the LANCOM DHCP server, figure out the current IP address of this PC (with **Start ► Execute ► cmd** and command **ipconfig** at the prompt under Windows 2000 or Windows XP, with **Start ► Execute ► cmd** and the command **winipcfg** at the 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-00a057xxxxx").



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.

Starting the wizards in WEBconfig

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

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

(or with a name as discribed above)



If you cannot access an unconfigured device, 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:

Setup Wizards

Wizards enable you to handle frequent configuration jobs easily and quickly:

-  [Basic Settings](#)
-  [Security Settings](#)
-  [Set up Internet connection](#)
-  [Selection of Internet Provider](#)
-  [Assign Access Points to Profiles](#)

Device Configuration and Status

These menu options enable you to access the device's entire configuration:

Use the 'Configuration' for normal configuration jobs.
For experienced users, the expert configuration provides detailed access to all configuration options and the device status.

-  [Configuration](#)
-  [Expert Configuration](#)
-  [Save Configuration](#)
-  [Upload Configuration](#)
-  [Save Configuration Script](#)
-  [Execute Configuration Script](#)







File Handling

-  [Edit List of Allowed SSH Public Keys](#)
-  [Download Certificate or File](#)
-  [Upload Certificate or File](#)

Firmware Handling

-  [Perform a Firmware Upload](#)

Extras

-  [Show/Search Other Devices](#)
-  [Get Device SNMP MIB](#)
-  [Enable Software Option](#)
-  [Display Key Fingerprints](#)
-  [Change password](#)
-  [Create TCP/HTTP Tunnel](#)




The setup wizards are tailored precisely to the functionality of the specific LANCOM model. 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. Also 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).

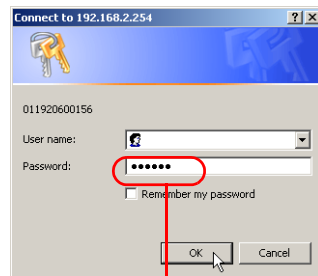
You may specify whether the device may only be configured from the local network or whether remote configuration via the WAN (i.e. a remote network) is also permissible.

-  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 pre-determined 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 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 (default)**

In this operating mode the LANCOM 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 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 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 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, 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.

3.5 Location verification by ISDN or GPS

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.

3.5.1 GPS location verification

GPS location verification enables a geographical position to be defined within the device. After being switched on the device automatically activates the GPS module and checks if it is located at the "correct" position. The router module is only switched on if the check is positive. After location verification has been carried out the GPS module is deactivated again, unless it was switched on manually.

3.5.2 ISDN location verification

ISDN location verification can prevent the misuse of a router. Each time it is switched on, the router carries out a check by making an ISDN telephone call to itself to ensure that it is installed at the intended location. Only after successful location verification is the router module activated.

Prerequisites for successful ISDN location verification:

- The device must be reachable from the public ISDN telephone network.
- The device needs two free B channels for the duration of the check. If just one channel is free, e.g. one channel at a point-to-multipoint connection with two B channels is being used for a telephone call, then the device cannot make a call to itself via ISDN.

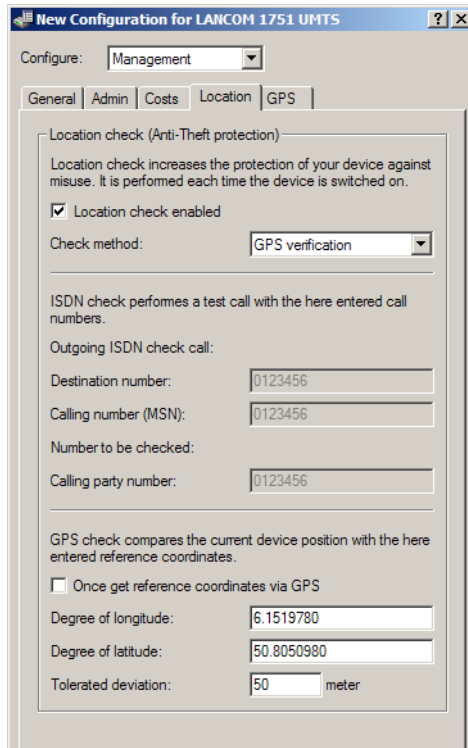
3.5.3 Configuring location verification

LANconfig

Parameters for location verification are to be found in LANconfig in the configuration area 'Management' on the 'Location' tab.



You can enable the GPS module on the 'GPS' tab independently from the location verification e. g. for monitoring the current GPS coordinates using LANmonitor.



New Configuration for LANCOM 1751 UMTS

Configure: Management

General | Admin | Costs | Location | GPS

Location check (Anti-Theft protection)

Location check increases the protection of your device against misuse. It is performed each time the device is switched on.

☒ Location check enabled

Check method: GPS verification

ISDN check performs a test call with the here entered call numbers.

Outgoing ISDN check call:

Destination number: 0123456

Calling number (MSN): 0123456

Number to be checked:

Calling party number: 0123456

GPS check compares the current device position with the here entered reference coordinates.

☐ Once get reference coordinates via GPS

Degree of longitude: 6.1519780

Degree of latitude: 50.8050980

Tolerated deviation: 50 meter

- Activate location verification with the 'Enable location check' option.
- Select the method for the location check:
 - ☐ 'Self call' for a check via ISDN by means of a return call.
 - ☐ 'Call forwarding check' via ISDN by requesting the call number from the exchange. No call-back is necessary in this case.
 - ☐ 'GPS verification' for a check on the geographical coordinates.



For a location check by GPS an appropriate GPS antenna must be connected to the AUX connector on the device. Additionally, a SIM card for mobile telephone operation has to be inserted and the device must be logged on to a mobile phone network.

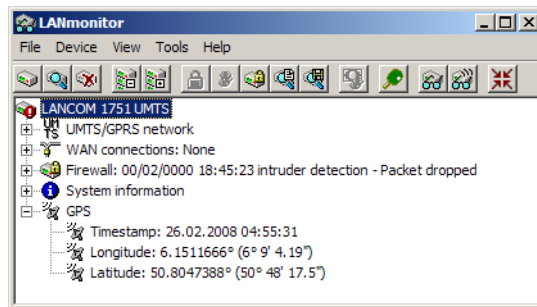
- For the location check enter 'Self call' or 'Call forwarding check' and enter the destination number as the telephone number to be used for the check.
- For location verification by GPS enter the necessary parameters:
 - ☐ Degrees latitude and longitude

- Deviation from the intended position in meters



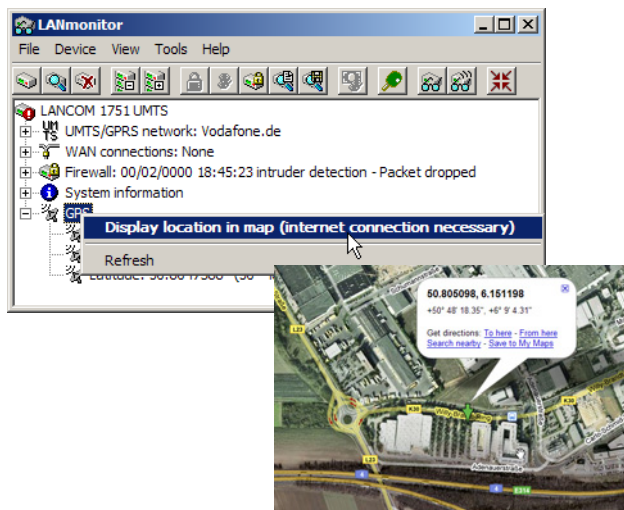
The device is itself able to determine the geographical coordinates for its current position by activating the 'Get reference coordinates via GPS' checkbox. Once the configuration is written back to the device, the current longitude and latitude are entered automatically, assuming that location verification is activated and a valid GPS position is available. Subsequently this option is automatically deactivated again.

As an alternative you can determine the geographical coordinates from tools such as Google Maps.





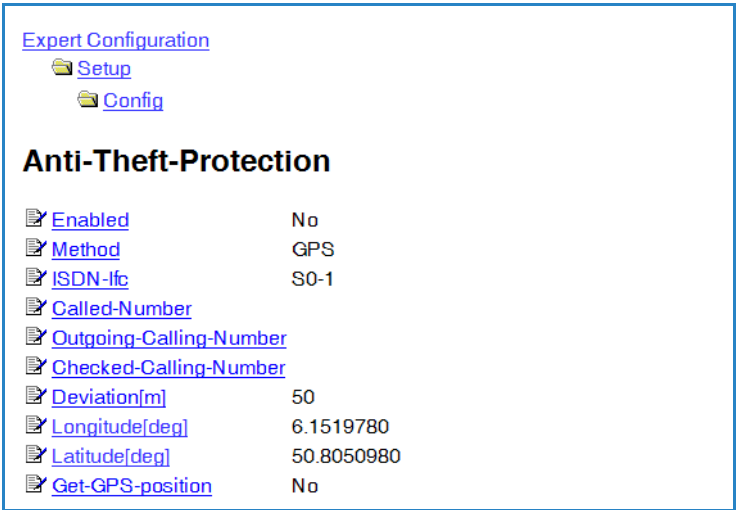
When the current geographical coordinates are displayed in LANmonitor, you can right-click with the mouse on the entry 'GPS' to call up that location in Google maps.



WEBconfig, Telnet
or terminal program

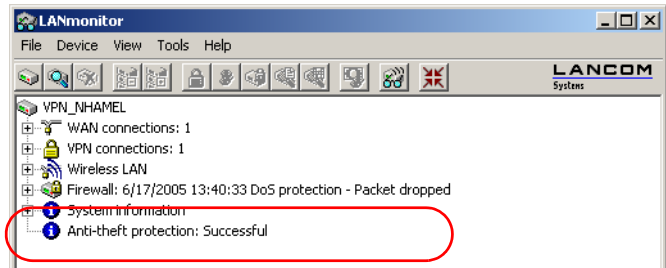
Under WEBconfig, Telnet or a terminal program, you will find the settings for location verification under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ► Setup ► Config ► Location verification
Terminal/Telnet	Setup/Config/Location verification



Location verification status request

The status of location verification can be viewed under LANmonitor:



With WEBconfig (**Expert configuration ▶ Status ▶ Config ▶ Location verification**) or Telnet (Status/Config/Location verification) you can view the status of the location verification:

[Expert Configuration](#)

📁 [Status](#)

📁 [Config](#)

Anti-Theft-Protection

👁	State	Successfull
👁	sending-call-to	
👁	waiting-for-call-from	
👁	last-seen-call-from	
👁	call-accepted	No
👁	incoming-call	No
👁	last-error	
👁	Method	GPS
👁	Position-valid	Yes
👁	Expected-Longitude[deg]	6.1518583
👁	Current-Longitude[deg]	6.1518555
👁	Expected-Latitude[deg]	50.8049638
👁	Current-Latitude[deg]	50.8049638
👁	Delta-Longitude[m]	1
👁	Delta-Latitude[m]	0

Only when the location verification has the status 'Successful' will the router data be transferred over the WAN interfaces.

- Location verification via ISDN is successful when the number 'Expect call from' agrees with the number 'Last call from'. This call is not picked up by the router. The status also displays whether a call was accepted at all.
- Location verification via GPS is successful when the GPS position is valid and within the tolerated range deviation from the known position.

4 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.



You can carry out the configuration of security settings very quickly and conveniently with the Security Wizards in LANconfig and WEBconfig.

4.1 Tips for handling keys

The security of encryption procedures can be substantially increased 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.

4.2 The security settings wizard

Access to the configuration of a device permits not only to read out critical information (e.g. 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.

4.2.1 Wizard for LANconfig

- ① Mark your LANCOM 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 activate Stateful Inspection, ping-blocking and Stealth mode in the the firewall configuration.
- ⑥ The wizard will inform you when entries are complete. Complete the configuration with **Finish**.

4.2.2 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)

4.3 The security checklist

The following checklists provide an overview of all security settings that are important to professionals. Most of the points in this checklist are uncritical for simple configurations. In these cases, the security settings in the basic configuration or that were set with the Security Wizard are sufficient.



Detailed information about the security settings mentioned here are to be found in the reference manual.

■ Have you protected the configuration with a password?

The simplest way of protecting the configuration is to agree upon a password. If no password has been agreed for the device, the configuration is open to be changed by anybody. The field for entering the password is to be found in LANconfig in the 'Management' configuration area on the 'Security' tab. It is absolutely imperative to assign a password to the configuration if you want to enable remote configuration!

■ Have you permitted remote configuration?

If you do not require remote configuration, please ensure to switch it off. If you need to make use of remote configuration, ensure that you do not fail to password-protect the configuration (see the section above). The field for disabling remote configuration is to be found in LANconfig in the 'Management' configuration area on the 'Security' tab. Under 'Access rights – From remote networks' select the option 'denied' for all methods of configuration.

■ Have your password-protected the SNMP configuration?

Protect the SNMP configuration with a password too. The field for password-protecting the SNMP configuration is also to be found in LANconfig in the 'Management' configuration area on the 'Security' tab.

■ Have you activated the firewall?

The stateful inspection firewall of LANCOM devices ensures that you local network cannot be attacked from the outside. Activate the firewall in LANconfig under 'Firewall/QoS' on the 'General' tab.

■ Are you using a 'deny all' firewall strategy?

Maximum security and control is initially achieved by denying all data traffic from passing the firewall. The only connections to be accepted by the firewall are those that are to be explicitly permitted. This ensures that Trojan horses and certain types of e-mail virus are denied communication

to the outside. Activate the firewall rules in LANconfig under 'Firewall/QoS' on the 'Rules' tab. Instructions on this are to be found in the reference manual.

■ Have you activated IP masquerading?

IP masquerading refers to the concealment of local computers while they access the Internet. All that is revealed to the Internet is the IP number of the router module of the device. The IP address can be fixed or dynamically assigned by the provider. The computers in the LAN then use the router as a gateway and are not visible themselves. The router separates the Internet from the intranet like a wall. The application of IP masquerading is set in the routing table for every route individually. The routing table can be found in the LANconfig in the configuration area 'IP router' on the 'Routing' tab.

■ Have you used filters to close critical ports?

The firewall filters in LANCOM devices offer filter functions for individual computers or entire networks. It is possible to set up source and destination filters for individual ports or port ranges. Furthermore, filters can be set for individual protocols or any combination of protocols (TCP/UDP/ICMP). It is especially convenient to set up the filters with the aid of LANconfig. Under 'Firewall/QoS', the 'Rules' tab contains the functions for defining and editing filter rules.

■ Have you excluded certain stations from accessing the device?

A special filter list can be used to limit access to the device's internal functions via TCP/IP. The phrase "internal functions" refers to configuration sessions via LANconfig, WEBconfig, Telnet or TFTP. As standard this table contains no entries, meaning that computers with any IP address can use TCP/IP and Telnet or TFTP to commence accessing the device. The first time an IP address is entered with its associated netmask, the filter is activated and only the IP addresses contained in this entry are entitled to make use of internal functions. Further entries can be used to extend the circle of authorized parties. The filter entries can describe individual computers or even entire networks. The access list can be found in the LANconfig in the configuration area 'TCP/IP' on the 'General' tab.

■ Do you store your saved LANCOM configuration to a safe location?

Protect your saved configurations in a location that is safe from unauthorized access. Otherwise, by way of example, an unauthorized person may load your stored configuration file into another device and they can access the Internet at your expense.

■ Have you activated the protection of your WAN access in case 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.

With the ISDN location verification, the device can only be operated at one particular ISDN connection. After being switched on, the device calls itself at the corresponding telephone number to check that it is still connected to the "correct" ISDN connection (for further information see the reference manual).

GPS location verification enables a geographical position to be defined within the device. After being switched on the device checks if it is located at the "correct" position. The router module is only activated after a positive check.

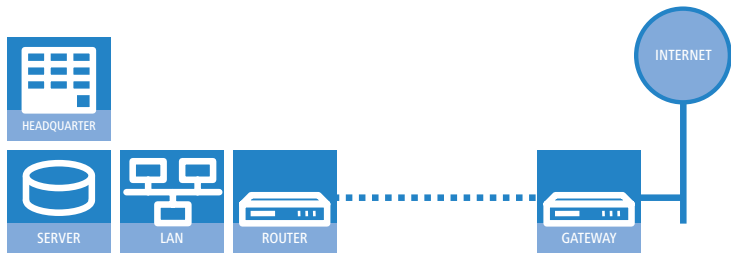
The scripting function can store the entire configuration in RAM only so that restarting the device will cause the configuration to be deleted. The configuration is not written to the non-volatile flash memory. A loss of power because the device has been relocated will cause the entire configuration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

■ 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 if a co-worker presses the reset button too long. The behavior of the reset button can be set so that a press is either ignored or it causes a re-start, depending on the time for which it is held pressed.

5 Setting up Internet access

The LANCOM provides a central point of Internet access for all of the computers in the LAN. The connection to the Internet provider can be established via any WAN connector, i.e. via ADSL, UMTS or ISDN (where available). Internet access via UMTS or ISDN can be used to backup an ADSL connection. When setting up Internet access via UMTS, please also take note of the information under the section → 'Setting up the UMTS profile'.



Which WAN interface?

Setting up the Internet access is carried out with the help of a convenient Wizard. In the first step you select the WAN interface that is to be used for establishing the Internet connection.

To establish an Internet connection via the DSL interface, an external ADSL modem first has to be connected to one of the device's ETH ports. When setting up the Internet access, you define which ETH port the ADSL modem has been connected to.

Does the Setup Wizard know your Internet provider?

The Wizard is preset with access data for the principal Internet providers in your country and offers you a selection list. If you find your Internet provider in this list, then you generally do not have to enter any additional parameters to set up your Internet access. All that is required is the authentication data as supplied to you by your Internet provider.

Internet provider unknown

If the list in the Setup Wizard does not contain your provider, you will be asked step-by-step for all of the necessary data. This access data will have been supplied to you by your Internet provider.

Other connection options

In addition you can use the Wizard to activate or deactivate additional options (if supported by your Internet provider):

- Billing by time or flatrate – select the method by which you are billed by your Internet provider.
 - In case of billing by time, you can set the LANCOM to cut connections automatically if no data flows for a certain time (the hold time).
You can also set up line polling that detects inactive remote stations very quickly and, in such cases, can close the connection before the hold time expires.
 - In case of flatrate billing you can also set up line polling to monitor the function of the remote station.
Apart from that you can opt to keep flatrate connections permanently active ("keep-alive"). In case a connection should fail, it is re-established automatically.
- Dynamic channel bundling (ISDN only)
 - If required, the second ISDN B-channel can be activated and added to the connection. The result is that bandwidth is doubled. However, under certain circumstances the connection fees may double as well. Furthermore your ISDN connection would be engaged, so preventing any other incoming or outgoing telephone calls from being made.
- Data compression (ISDN only)
 - This enables data transfer rates to be increased even further.

Creating a backup connection to the Internet

The most common utilization of the backup solution is to provide an auxiliary Internet connection. When setting up an Internet connection, an additional option is to create a second connection to the Internet via an alternative WAN interface. If the primary Internet access is set up to operate via the ADSL interface, you can set up your backup connection to operate via UMTS or ISDN.

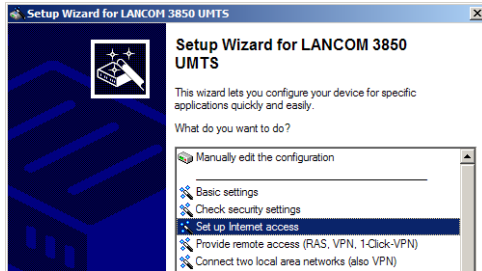


When configuring the backup connection you can set up an alternative provider, if available. This allows you not only to overcome problems with the physical line, but also problems in your provider's own network as well.

5.1 The Internet Connection Wizard

5.1.1 Instructions for LANconfig

- ① Mark your device in the selection window. From the command line, select **Extras ▶ Setup Wizard**.



- ② In the selection menu, select the Setup Wizard, **Set up Internet connection** and confirm the selection with **Next**.
- ③ In the following windows you select your country, your Internet provider if possible, and you enter your access data.
- ④ Depending on availability the Wizard provides further options for your Internet connection.
- ⑤ After entering all of the necessary data the Wizard then offers you the option of setting up a backup connection. Select the corresponding WAN interface to be used for the backup connection and enter the relevant access data for the Internet connection.

The Wizard then sets up the alternative Internet access and at the same time creates the necessary entries into the backup table and also in the PPP table for checking the Internet connection.

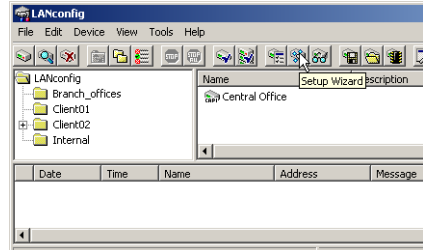


Please be aware that in the case of backup via UMTS, some of the services provided over the main Internet connection may not be available. Some UMTS service providers either prevent the use of VPN tunnels or VoIP applications or only allow them after payment of additional fees. Other providers assign IP addresses from an internal address range, so preventing applications that rely on public IP addresses from working. Please ask your UMTS provider for information on limitations that may apply.

- ⑥ The Wizard will inform you as soon as the entries are complete. Close the configuration with **Finish**.

LANconfig: Fast activation of the Setup Wizards

The fastest way of starting the Setup Wizards under LANconfig is to use the command button in the button bar.



5.1.2 Instructions for WEBconfig

- ① Select the entry **Set up Internet connection** from the main menu.
- ② In the following windows you select your country, your Internet provider if possible, and you enter your access data.
- ③ Depending on availability the Wizard provides further options for your Internet connection.
- ④ The wizard will inform you as soon as the entries are complete. Close the configuration with **Finish**.

5.2 The Firewall Wizard

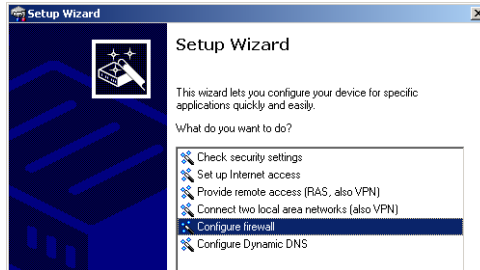
Your LANCOM features a stateful inspection firewall and firewall filter that provides effective protection from the Internet for your LAN. The core concept of the stateful inspection firewall is that the only data transfers that are considered to be valid are those implemented by the protected device itself. All access attempts that were not requested from within the local network are invalid.

The Firewall Wizard assists you to generate new rules for the firewall quickly and conveniently.

More information on your LANCOM's firewall and its configuration are available in the reference manual.

5.2.1 LANconfig Wizard

- ① Mark your LANCOM in the selection window. From the command line, select **Extras ▶ Setup Wizard**.



- ② In the selection menu, select the Setup Wizard, **Configure firewall** and confirm the selection with **Continue**.
- ③ In the windows that follow you select the services/protocols that the rule is to relate to. In the next step you define the source and destination stations that the rule applies to, and the actions that are to be carried out by the rule on a data packet.
- ④ Finally the new rule is given a name, it is activated, and you define whether further rules are to be considered when the rule acts on a data packet.
- ⑤ The wizard will inform you as soon as the entries are complete. Close the configuration with **Finish**.

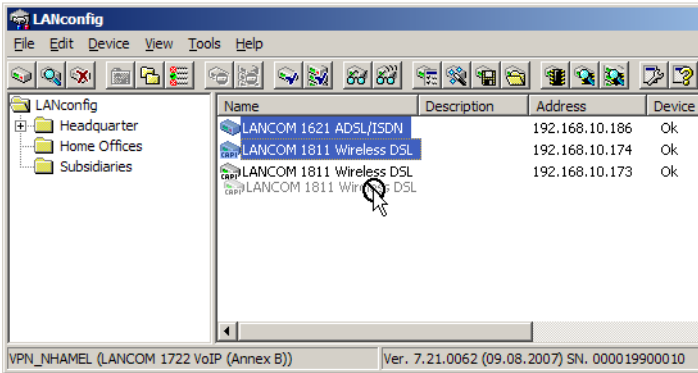
5.2.2 Configuration under WEBconfig

WEBconfig provides the option of checking and altering the parameters for Internet access under **Configuration ▶ Firewall / QoS ▶ Rules ▶ Rule table**.

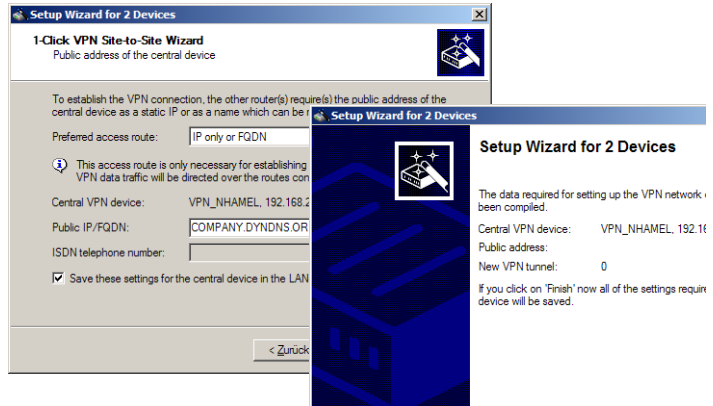
6 Connecting two networks

Network coupling, also known as LAN-LAN coupling, with the LANCOM Router is used for interconnecting two local area networks. The site-to-site coupling of networks is now very simple with the help of the 1-Click-VPN wizard. It is even possible to simultaneously couple multiple routers to a central network.

- ① In LANconfig, mark the routers at branch offices which are to be coupled to a central router via VPN.
- ② Use drag&drop by mouse to place the devices onto the entry for the central router.



- ③ The 1-Click-VPN Site-to-Site Wizard will be started. Enter a name for this access and select the address under which the router is accessible from the Internet.



- ④ Select whether connection establishment is to take place via the name or IP address of the central router, or via an ISDN connection. Enter the address or name of the central router, or its ISDN number.
- ⑤ The final step is to define how the networks are to intercommunicate:
- ☐ The INTRANET at headquarters only is to be provided to the branch offices.
 - ☐ All private networks at the branch offices can also be connected to one another via headquarters.



All entries for the central device are made just once and are then stored to the device properties.



The Wizard is not suitable for coupling networks via VPN under WEBconfig. The Expert Configuration has to be used instead. Refer to the reference manual for information on this.

7 Providing dial-in access

Your LANCOM UMTS Router can be set up with dial-in access accounts enabling individual computers to dial-in to your LAN and fully participate in the network for the duration of the connection. This service is called RAS (**R**emote **A**ccess **S**ervice).

On the accompanying CD, LANCOM Systems offers a 30-day test version of the LANCOM Advanced VPN Client for dialing-in to a network via VPN. A precise description of the VPN client and notes on its setup are also to be found on the CD.

VPN accesses for employees who dial into the network with the LANCOM Advanced VPN Client are very easy to set up with the Setup Wizard and exported to a file. This file can then be imported as a profile by the LANCOM Advanced VPN Client. All of the information about the LANCOM UMTS Router's configuration is also included, and then supplemented with randomly generated values (e.g. for the preshared key).

- ① Use LANconfig to start the 'Set up a RAS Account' wizard and select the 'VPN connection'.
- ② Activate the options 'LANCOM Advanced VPN Client' and 'Speed up configuration with 1-Click-VPN'.
- ③ Enter a name for this access and select the address under which the router is accessible from the Internet.
- ④ In the final step you can select how the access data is to be entered:
 - ☐ Save profile as an import file for the LANCOM Advanced VPN Client
 - ☐ Send profile via e-mail
 - ☐ Print out profile



Sending a profile via e-mail could be a security risk should the e-mail be intercepted en route!

To send the profile via e-mail, the device configuration must be set up with an SMTP account with the necessary access data. Further, the configuration computer requires an e-mail program that is set up as the standard e-mail application and that can be used by other applications to send e-mails.

When setting up the VPN access, certain settings are made to optimize operations with the LANCOM Advanced VPN Client, including:

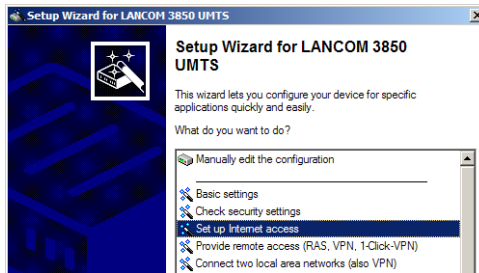
- Gateway: If defined in the LANCOM VPN Router, a DynDNS name is used here, or alternatively the IP address
- FQDN: Combination of the name of the connection, a sequential number and the internal domain in the LANCOM VPN Router.
- Domain: If defined in the LANCOM VPN Router, the internal domain is used here, or alternatively a DynDNS name or IP address
- VPN IP networks: All IP networks defined in the device as type 'Intranet'.
- Preshared key: Randomly generated key 16 ASCII characters long.
- Connection medium: The LAN is used to establish connections.
- VoIP prioritization: VoIP prioritization is activated as standard.
- Exchange mode: The exchange mode to be used is 'Aggressive Mode'.
- IKE config mode: The IKE config mode is activated, the IP address information for the LANCOM Advanced VPN Client is automatically assigned by the LANCOM VPN Router.

8 Setting up the UMTS profile

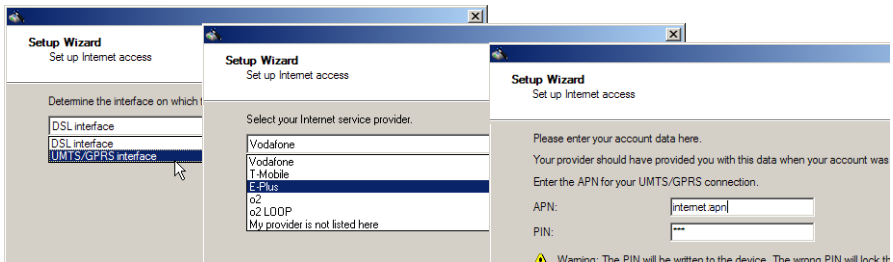
8.1 Internet access

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

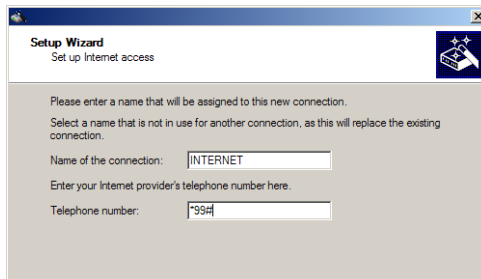
- ① Mark your LANCOM UMTS Router in the selection window. From the command line, select **Extras ▶ Setup Wizard**.



- ② In the selection menu, select the Setup Wizard, **Set up Internet connection** and confirm the selection with **Next**.



- ③ To set up the Internet access, select the UMTS interface, your network operator, 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. To do this you require the corresponding telephone number in your provider's mobile telephone network.



Your provider will supply this information to you upon request.

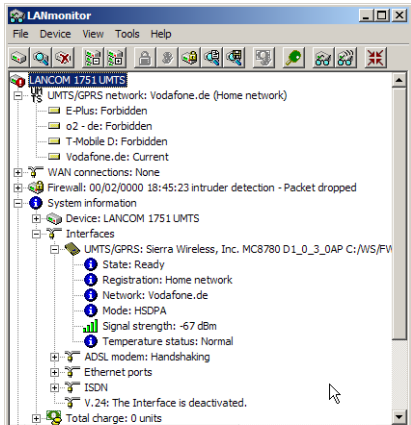
- ⑤ To conclude the configuration of the Internet access, you can activate the "Keep alive" option for the UMTS/HSxPA connection. This sets up the UMTS/HSxPA connection so that the connection is automatically established after the device is switched on, and so that the connection automatically re-establishes 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.



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 mobile provider's UMTS/HSxPA tariff.

- ⑥ Alternatively you can set up a suitable hold time for the UMTS/HSxPA 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.



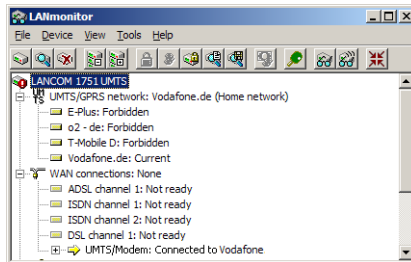
Even without an current connection, the active local networks are displayed in the 'UMTS/GPRS network' section. LANmonitor also indicates which networks are permitted and which networks the card cannot connect to.

- 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 and transfer mode depend on the type of card being used.

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 just one bar there will in most cases be no data transfer at all.

A close-up screenshot of the LANmonitor interface, focusing on the 'Signal strength' and 'Temperature status' fields. The signal strength is shown as three green bars and '-67 dBm'. The temperature status is 'Normal'. A red circle highlights the signal strength information.

- 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 UMTS connection is also displayed by flashing codes from the UMTS LEDs on the front of the device.

8.2 VPN site coupling

As well as connecting single workstations to the headquarters, the UMTS/HSxPA interface can be used for full-blown network coupling.

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/HSxPA:

- When dialing-in, some mobile telephone providers assign the UMTS card with an IP address from their own internal range of addresses. This represents no problem for a normal Internet connection. However, this can lead to problems when establishing a VPN connection as the IP addresses of the VPN devices may be required for the negotiation of the encryption parameters. With NAT-Traversal activated in the headquarter VPN gateway, it is possible to establish VPN connections from branch offices that use private IP addresses.



For further information on this subject refer to the LCOS reference manual.

- When coupling networks with the Wizard, the secure "main mode" is initially used for the exchange of IKE keys. Main Mode negotiation takes the IP addresses of the VPN terminals into account, which can lead to pro-

blems in the case of the assignment of a private IP address to the LANCOM UMTS Router.

If no VPN 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/HSxPA 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.

- If the UMTS/HSxPA card was assigned a private IP address and the LANCOM UMTS Router cannot, for example, be identified by an ISDN call (Dynamic VPN), the VPN connection must always be established from the VPN gateway with the UMTS/HSxPA 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/HSxPA-connected network is possible at all times (e.g. for connecting branches via UMTS/HSxPA where no broadband Internet access is available).
- 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/HSxPA 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 mobile provider's UMTS/HSxPA tariff.

8.3 Other settings

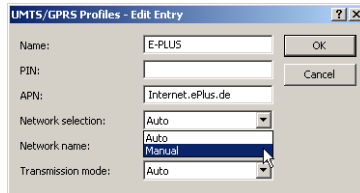
8.3.1 Choosing the mobile telephone network


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.

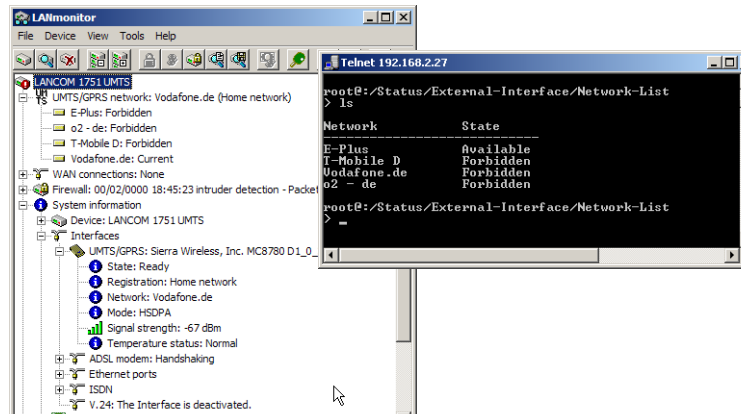
Once the card is outside of "home network" coverage, there is normally a choice of alternative mobile networks (i.e. roaming, in particular when in another country). Generally speaking, the user now has a choice of network which is to be used for the Internet connection.

In the appropriate UMTS/HSxPA/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.

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**.



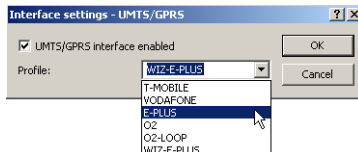
 The name of the network can be read from LANmonitor or, for example, by using Telnet under /Status/External-Interface/Network-List. A manual network search can be initiated with the commands do /Status/External-Interface/Scan-Networks or so Setup/Interfaces/UMTS-GPRS-parameters/Scan-Networks.



8.3.2 Activate UMTS/GPRS profile

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

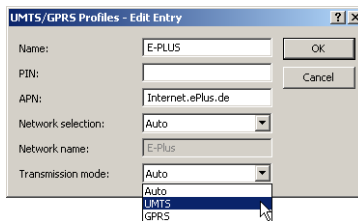
The activation of the UMTS/HSxPA interface and the selection of the profile are to be found in LANconfig in the configuration area 'Interfaces' on the 'WAN' tab with the **Interface settings** button.



8.3.3 UMTS/HSxPA only or automatic UMTS/HSxPA/GPRS selection

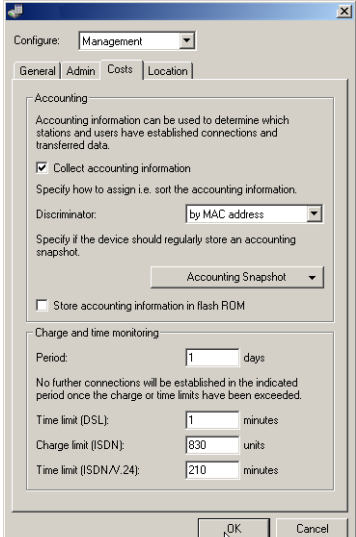
UMTS/HSxPA coverage is not yet universally available. It is still possible to establish a data connection even in areas without UMTS/HSxPA reception by selecting the 'automatic' operating mode. With this setting, the data card in the LANCOM will initially attempt to establish a connection via UMTS/HSxPA. The card will automatically switch to the GPRS network if the UMTS 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/HSxPA or GPRS. The desired operating mode can be set in the UMTS/HSxPA/GPRS profile settings which are to be found in LANconfig in the configuration area 'Interface' on the 'WAN' tab with the **UMTS/HSxPA/GPRS profile** button.



8.3.4 Set up a time limit

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



Configure: Management

General Admin Costs Location

Accounting

Accounting information can be used to determine which stations and users have established connections and transferred data.

☒ Collect accounting information

Specify how to assign i.e. sort the accounting information.

Discriminator: by MAC address

Specify if the device should regularly store an accounting snapshot.

Accounting Snapshot

☐ Store accounting information in flash ROM

Charge and time monitoring

Period: 1 days

No further connections will be established in the indicated period once the charge or time limits have been exceeded.

Time limit (DSL): 1 minutes

Charge limit (ISDN): 830 units

Time limit (ISDN/V.24): 210 minutes

OK Cancel

9 Troubleshooting

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

9.1 No DSL connection is established

After start-up the router automatically attempts to connect to the DSL provider. If successful, the LED will switch over to steady green. 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.

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

9.2 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).

9.3 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 and characteristics


LANCOM 1751 UMTS		
Connections	ETH1 to ETH4	10/100Base-TX, autosensing
	WAN or ADSL	ADSL over ISDN compliant with ITU G.992.1 Annex B (compatible to Deutschen Telekom U-R2 connections) or ADSL over POTS compliant with ITU G.992.1 Annex A ADSL2+ over ISDN compliant with ITU 992.3, ITU G.992.5 Annex B (ADSL2+) or ADSL2+ over POTS compliant with ITU G992.3 and ITU G.992.5 Annex A (ADSL2+)
	GSM/UMTS	UMTS, HSxPA, GPRS or Edge with the intergrated UMTS modem
	ISDN	ISDN-S ₀ bus
	Serial interface / COM port	Serial configuration interface / COM port (8-pin Mini-DIN): 9,600 - 115,000 baud
Power supply		12V DC via external power supply. Permitted power supplies: ■ NEST 12V/1A DC/S Hohlstkr 2.1/5.5mm (RoHS) LANCOM item no. 110524 Type identification on the power supply „Type: 15.22305“
Housing		Dimensions 210 mm x 143 mm x 45 mm (B x H x T), robust plastic housing, stackable, prepared for wall mounting
Conformity		CE conform with EN 60950
Approvals		Certifications notified in Germany, Belgium, Netherlands, Luxembourg, Austria, Switzerland, UK, Italy, Spain, France, Portugal
FCC		The devices with article no. 61626 (LANCOM 1751 UMTS FCC) additionally comly with the requirements of the FCC. FCC compliance text: This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions. 1) this device may not cause harmful interference. 2) this device must accept any interference received, including interference that may cause undesired operation. ■ FCC ID: N7NMC8781 ■ US: X1UDSNANLC1751
Environment/Temperature		Temperature range 5–35°C in continuous operation; humidity 0-80 %; non-condensing
Service		3-year warranty

LANCOM 1751 UMTS		
Support		Via hotline and Internet
Accessories		<ul style="list-style-type: none">■ LANCOM Rack Mount Option (item no. 61501)■ LANCOM LCOS Reference Manual (DE) (item no. 61700)■ LANCOM Advanced VPN Client for Windows® 2000, Windows® XP, Windows Vista™, single license, item no. 61600■ LANCOM Advanced VPN Client for Windows® 2000, Windows® XP, Windows Vista™, single license, item no. 61601■ LANCOM Advanced VPN Client for Windows® 2000, Windows® XP, Windows Vista™, 25 licenses, item no. 61602
Options		<ul style="list-style-type: none">■ LANCOM VPN-25 Option (25 channels, incl. activated VPN hardware accelerator), item no. 60083

10.2 Contact assignment

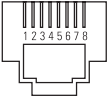
10.2.1 ADSL interface

6-pin RJ11 socket

Connector	Pin	IAE
	1	—
	2	—
	3	a
	4	b
	5	—
	6	—

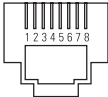
10.2.2 ISDN S₀ interface

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

Connector	Pin	Line	IAE
	1	–	–
	2	–	–
	3	T+	2a
	4	R+	1a
	5	R-	1b
	6	T-	2b
	7	–	–
	8	–	–

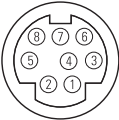
10.2.3 Ethernet interface 10/100Base-TX

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

Connector	Pin	IAE
	1	T+
	2	T-
	3	R+
	4	–
	5	–
	6	R-
	7	–
	8	–

10.2.4 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

10.4 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).

Index

Numerics

10/100Base-TX 22

A

ADSL

Connections 23

Autosensing 24

C

Call-back function 15

Charge limiter 19

Configuration access 30, 34

Configuration file 45

Configuration interface 15

Connector cable 16

Configuration password 44

Configuration port 22

Configuration protection 15, 29

Connect charge protection 30, 34

Contact assignment 68

ADSL interface 68

Configuration interface 70

DSL interface 69

ISDN interface 69

LAN interface 69

Outband 70

D

Default gateway 35, 45

DHCP 35

DHCP server 13, 28, 30, 33, 35

Dial-in access 54

DNS

DNS server 13, 35

Documentation 16

Download 4

DSL

provider 30, 34

transfer protocol 34

DSL connection

problems establishing the connection
65

DSL transfer protocol 30

E

EDGE 10

F

Firewall 14, 45

Block stations 45

Firewall filters 50

FirmSafe 15

Firmware 4

Flatrate 48

G

GPRS 10

GPS 12, 22, 24, 36

H

HSxPA 10, 56

I

ICMP 45

Information symbols 5

Installation 16

ADSL 24

Antennas 24

LAN 24

LANtools 25

Power adapter 25

Internet access 47

Authentication data 47

Flatrate 48

Internet access setup 47

Internet access via UMTS/HSPDA 56

Internet provider 47

Internet-Zugang 13

IP

- Block ports 45
 Filter 45
 IP address 28, 45
 IP masquerading 14, 45
 IP router 13
 ISDN
 Dynamic channel bundling 48
 ISDN data compression 48
 ISDN leased-line option 14
 ISDN S₀ connection 14, 67
- L**
 LAN to LAN coupling 13
 LANCAPI 14
 LANconfig 26, 29
 Starting the Wizards 50
 LAN-LAN coupling 52
 LANmonitor 26
 LANtools
 System requirements 16
 Location verification 36
- M**
 MAC address filter 15
 Mobile telephone network 61
- N**
 NAT – see IP masquerading
 NetBIOS proxy 13
 Netmask 28, 45
 Network coupling via UMTS/HSxPA 59
- P**
 Package content 16
 Password 29, 30
 PAT – see IP masquerading
 Power adapter 22
- R**
 Remote Access Service (RAS)
 Server 13
 Setup 54
 Remote configuration 30, 34
 Remote configuration via ISDN 15
 Reset switch 23
 Reset the toll protection 19
 Routing table 45
- S**
 Security checklist 44
 SNMP
 Configuration protection 44
 Software installation 25
 SSID 30, 34
 Stateful-inspection firewall 50
 Status display
 Power 17, 19
 Statusanzeigen 17
 Wireless Link 22
 Support 4
 Switch 22
 System requirements 16
- T**
 TCP 45
 TCP/IP 16
 Settings 27, 29, 33
 Settings to PCs in the LAN 35
 Windows size 66
 TCP/IP configuration 33
 Automatic 27, 28
 fully automatic 27, 28
 manual 14, 45
 TCP/IP filter 45
 Telnet 45
 TFTP 45
 Transfer protocol 65
- U**
 UDP 45
 UMTS 10, 24, 56
 Automatic switching to GPRS 63
 Choosing the mobile telephone net-

work	61	W	
Internet access	56	WEBconfig	30
Mobile conference room	59	password	34
Time limit	64	System requirements	16
V			
Virtual Private Network (VPN)	13		