LANCOM 1751 UMTS

LANCOM
Systems

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom.de

Würselen, Oktober 2008

110584/1008

DE

Ein Wort vorab

Vielen Dank für Ihr Vertrauen!

Mit seinem integrierten UMTS/HSxPA-Modem setzt der VPN-ADSL2+-Router LANCOM 1751 UMTS Maßstäbe in Sachen Flexibilität und Redundanz. Ausfälle der Standard-DSL-Anbindung von Standorten, Außenstellen oder Filialen können durch breitbandige und kostengünstige UMTS/HSxPA- oder EDGE-Backup-Verbindungen automatisch aufgefangen werden. Alternativ kann die ISDN-Schnittstelle als weitere Backup-Leitung oder für Remote-Zugriff verwendet werden. Neben dieser einzigartig gesicherten Hochverfügbarkeit bietet LANCOM 1751 UMTS eine Standardausstattung von 5 VPN-Kanälen (optional 25), ein integriertes ADSL2+-Modem und vier separat ansteuerbare Switch-Ports für äußerst vielfältige professionelle Einsatzmöglichkeiten.

Der SIM-Kartenhalter des UMTS-Modems ist über die Rückblende des Gerätes leicht zugänglich und durch den Einsatz einer externen UMTS-Antenne ist es möglich, den Empfang innerhalb von Gebäuden wesentlich zu verbessern. Ein echtes Highlight: der Diebstahlschutz per ISDN-Selbstanruf und GPS-Positionsbestimmung!

Sicherheitseinstellungen

Für einen sicheren Umgang mit Ihrem Produkt empfehlen wir Ihnen, sämtliche Sicherheitseinstellungen (z. B. Firewall, Verschlüsselung, Zugriffsschutz) vorzunehmen, die nicht bereits zum Zeitpunkt des Kaufs des Produkts aktiviert waren. Der LANconfig-Assistent 'Sicherheitseinstellungen' unterstützt Sie bei dieser Aufgabe. Weitere Informationen zum Thema Sicherheit finden Sie auch im Kapitel 'Sicherheits-Einstellungen'.

Zusätzlich bitten wir Sie, sich auf unserer Internet-Seite www.lancom.de über technische Weiterentwicklungen und aktuelle Hinweise zu Ihrem Produkt zu informieren und ggf. neue Software-Versionen herunterzuladen.

Benutzerhandbuch und Referenzhandbuch

Die Dokumentation Ihres Gerätes besteht aus folgenden Teilen:

- Installation Guide
- Benutzerhandbuch
- Referenzhandbuch

DE

Sie lesen derzeit das Benutzerhandbuch. Es enthält alle Informationen, die zur raschen Inbetriebnahme Ihres Gerätes notwendig sind. Außerdem finden Sie hier alle wichtigen technischen Spezifikationen.

Das Referenzhandbuch befindet sich als Acrobat-Dokument (PDF-Datei) auf der beiliegenden Produkt-CD. Es ergänzt das Benutzerhandbuch und geht ausführlich auf Themen ein, die übergreifend für mehrere Modelle gelten. Dazu zählen beispielsweise:

- Systemdesign des Betriebssystems LCOS
- Konfiguration
- Management
- Diagnose
- Sicherheit
- Routing- und WAN-Funktionen
- Firewall
- Quality-of-Service (QoS)
- Virtuelle private Netzwerke (VPN)
- Virtuelle lokale Netzwerke (VLAN)
- Backup-Lösungen
- LANCAPI
- weitere Server-Dienste (DHCP, DNS, Gebührenmanagement)

An der Erstellung dieser Dokumentation …

… haben mehrere Mitarbeiter/innen aus verschiedenen Teilen des Unternehmens mitgewirkt, um Ihnen die bestmögliche Unterstützung bei der Nutzung Ihres LANCOM-Produktes anzubieten.

Sollten Sie einen Fehler finden oder einfach nur Kritik oder Anregung zu dieser Dokumentation äußern wollen, senden Sie bitte eine E-Mail direkt an:
info@lancom.de

Sollten Sie zu den in diesem Handbuch besprochenen Themen noch Fragen haben oder zusätzliche Hilfe benötigen, steht Ihnen unser Internet-Server www.lancom.de rund um die Uhr zur Verfügung. Hier finden Sie im Bereich 'Support' viele Antworten auf „häufig gestellte Fragen ('FAQs')". Darüber hinaus bietet Ihnen die Wissensdatenbank einen großen Pool an Informationen. Aktuelle Treiber, Firmware, Tools und Dokumentation stehen für Sie jederzeit zum Download bereit.
Außerdem steht Ihnen der LANCOM-Support zur Verfügung. Telefon-

nummern und Kontaktadressen des LANCOM-Supports finden Sie in einem separaten Beileger oder auf der LANCOM Systems-Homepage.

Hinweis-Symbole	
	Sehr wichtiger Hinweis, dessen Nichtbeachtung zu Schäden führen kann.
	Wichtiger Hinweis, der beachtet werden sollte.
	Zusätzliche Informationen, deren Beachtung hilfreich sein kann aber nicht erforderlich ist.

DE

Inhalt

DE

DE

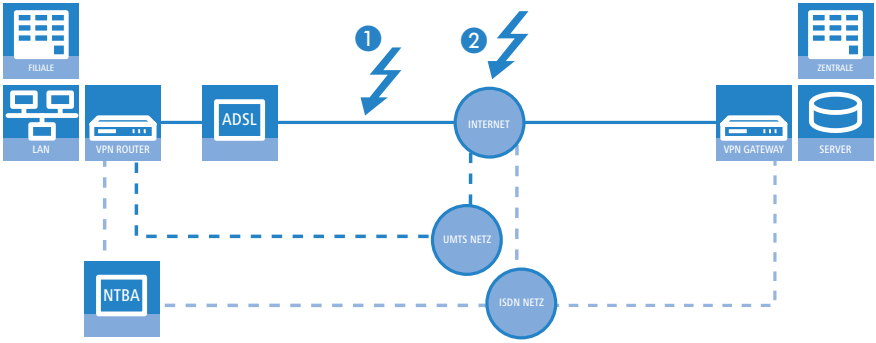
DE

1 Einleitung

Die vernetzte Zusammenarbeit über mehrere Standorte oder sogar über Kontinente hinweg ist aus dem modernen Wirtschaftsleben nicht mehr wegzudenken. Die Kommunikationswege zwischen Zentralen, Filialen oder Außendienstmitarbeitern setzen dabei immer mehr auf öffentliche Infrastrukturen auf. VPN hat sich als defacto-Standard für die kostengünstige und sichere Unternehmenskommunikation über das Internet etabliert.

Allerdings können bei diesen Netzwerkstrukturen eine Reihe von notwendigen Elementen von Störungen betroffen sein, die empfindliche Auswirkungen auf den Geschäftsbetrieb haben:

- Die Internetzugangsleitung zwischen dem Standort und dem Provider (1) kann ausfallen, z. B. durch Beschädigung des Kabels bei Bauarbeiten.
- Das Netzwerk des Providers (2) kann gestört sein oder ausfallen.



LANCOM UMTS Router vom Typ LANCOM 1751 UMTS bieten mit dem UMTS-Modem sowie der ISDN-Schnittstelle gleich zwei integrierte Möglichkeiten für den Aufbau von alternativen Verbindungen. Das Betriebssystem LCOS bietet dazu eine Reihe von Sicherheits- und Backup-Funktionen, mit denen Sie Ihr standortübergreifendes Netzwerk vor den Folgen dieser Störungen schützen können.

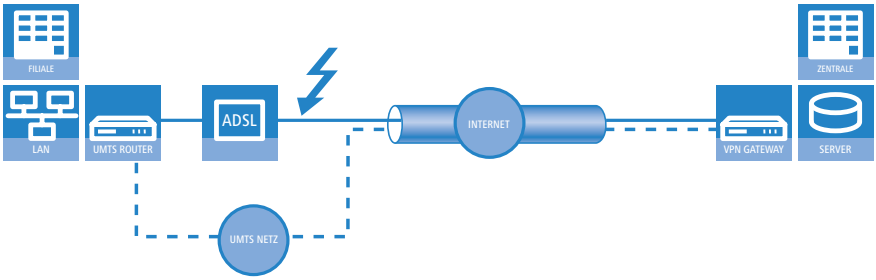
1.1 Verschiedene Backupstrategien

1.1.1 Backup über Mobilfunkleitungen

Die Hochverfügbarkeit von Datenleitungen z.B. zwischen Filialen und den zentralen Rechenzentren in größeren Unternehmensnetzwerken wird heute

DE

meistens über Backup-Lösungen mit ISDN- oder Analogleitungen realisiert. Die Standard-Internetverbindung wird dabei z. B. über einen günstigen DSL-Anschluss bereitgestellt, als Backup-Leitung übernimmt die ISDN/Analog-Leitung den Datenverkehr, wenn der normale Weg ins Internet gestört ist.



Als Alternative zu diesem ISDN/Analog-Backup-Verfahren kann auch eine Mobilfunk-Verbindung die Verfügbarkeit der Datenverbindungen sicherstellen. Wenn die Anbindung an das Internet über einen LANCOM 1751 UMTS erfolgt, kann die Mobilfunk-Verbindung sofort einspringen, wenn die ADSL-Leitung gestört ist. Das LANCOM 1751 UMTS unterstützt dabei alle aktuellen Mobilfunk-Techniken: GPRS, EDGE, UMTS und HSxPA.

Die verschiedenen Mobilfunktechniken im Überblick:

- **GPRS**: General Packet Radio Service, Technik zur paketorientierten Übertragung von Daten im GSM-Netz. Erreicht in der Praxis Datenübertagungsgeschwindigkeiten von ca. 56 kbit/s.
- **EDGE**: Enhanced Data Rates for GSM Evolution, ist eine Technik zur Erhöhung der Datenrate bei der GPRS-Übertragung durch ein zusätzliches Modulationsverfahren. EDGE erreicht Datenraten von theoretisch bis zu 384 kbit/s im Downstream und ca. 110 kbit/s im Upstream. EDGE ist in vielen Ländern nahezu flächendeckend verfügbar und bietet daher eine interessante Alternative zu UMTS.
- **UMTS**: Universal Mobile Telecommunications System, wird auch als Mobilfunkstandard der dritten Generation bezeichnet (3G). UMTS erreicht in der ersten Ausbaustufe Downloadraten von 384 kbit/s.
- **HSxPA**: High Speed Downlink Packet Access (HSDPA) und High Speed Uplink Packet Access (HSUPA) sind Protokollzusätze zu UMTS. HSDPA erreicht in verschiedenen Ausbaustufen Downloadraten von bis zu 14,6 Mbit/s, HSUPA erreicht Uploadraten von bis zu 5,8 Mbit/s.

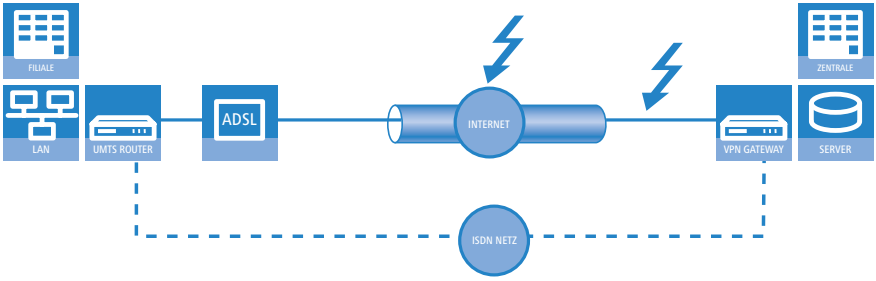
Die tatsächlich verfügbaren Bandbreiten hängen vom Ausbaustatus der jeweiligen Netzbetreiber-Infrastruktur und vom verwendeten UMTS-Modem ab.

Die Vorteile der Mobilfunk-Backuplösung gegenüber der ISDN/Analog-Variante:

- Schneller als ISDN/Analog: Der Datendurchsatz liegt bei UMTS/HSxPA wesentlich höher.
- Sicherer als ISDN oder Analog: Wenn eine physikalische Beschädigung der ADSL-Leitung der Grund für die Störung ist, ist in der Regel auch die ISDN/Analog-Leitung beschädigt, da beide Verfahren die gleiche physikalische Leitung nutzen.
- Günstiger als ISDN: Die monatlichen Bereitstellungskosten für Mobilfunk liegen je nach Tarif deutlich unter den Gebühren für einen ISDN-Anschluss. Da die tatsächlichen Ausfallzeiten der ADSL-Verbindung üblicherweise nur wenige Stunden im Jahr betragen, sind die ggf. höheren Verbindungskosten für den Mobilfunk oft nicht relevant. Je nach Bedarf kann anstelle einer Berechnung nach Zeit auch eine Berechnung des tatsächlich übertragenen Datenvolumens gewählt werden.

1.1.2 Backup über ISDN-Direktwählverbindung

Bei der Anbindung einer Filiale über eine VPN-Verbindung an die Zentrale kann es dennoch sinnvoll sein, die internetbasierte VPN-Verbindung zusätzlich zum UMTS/HSxPA-Backup durch eine direkte ISDN-Wählverbindung abzusichern. Falls das Netzwerk des Providers oder die Internetverbindung in der Zentrale ausfällt, kann die Datenübertragung über die ISDN-Kopplung fortgesetzt werden.

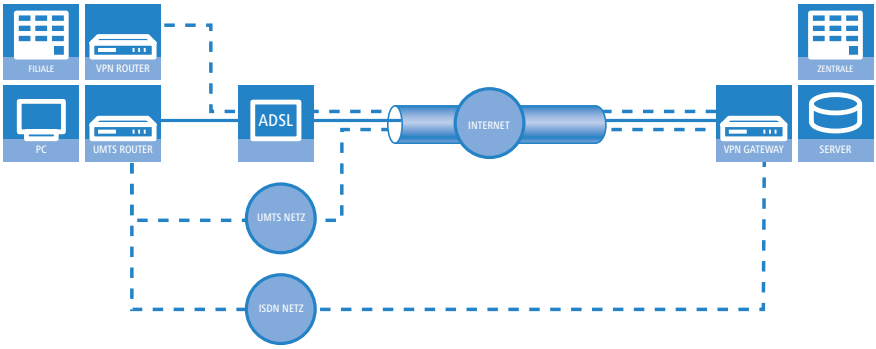


1.1.3 Backup mit VRRP

Ein besonders ausgefeiltes Backup-System zum Schutz vor Hardware-Ausfällen der Router kann mit dem Virtual Router Redundancy Protocol (VRRP) realisiert werden. Dabei werden in einem Netzwerk zwei oder mehrere Router

DE

installiert, die sich beim Ausfall eines Gerätes gegenseitig vertreten können. Zusätzlich zum normalen VRRP kann bei LANCOM-Geräten das Auslösen des Backup-Falls an die Verfügbarkeit einer Datenverbindung geknüpft werden. Mit dieser Zusatzfunktion können LANCOM-Geräte mit mehreren WAN-Interfaces (z. B. DSL- und UMTS/HSxPA-Interface) sehr flexibel in Backuplösungen eingesetzt werden. Der Backup-Fall wird dabei z. B. dann ausgelöst, wenn die Default-Route über das DSL-Interface nicht mehr erreichbar ist. Das UMTS/HSxPA-Interface des Gerätes kann aber einen weiteren Platz in der Backup-Kette einnehmen, wenn auch der Backup-Router gestört ist.



Weitere Informationen zu Backup-Lösungen mit VRRP finden Sie im LCOS-Referenzhandbuch.

1.2 Standortverifikation über ISDN oder GPS

In größeren Installationen mit zum Teil unbeaufsichtigt aufgestellten Routern besteht die Gefahr, dass Geräte entwendet werden und an einer anderen Stelle wieder eingesetzt werden. Wenn in den Geräten RAS-Zugänge, LAN-Kopplungen oder VPN-Verbindungen konfiguriert sind, kann sich ein Dieb mit dem gestohlenen Gerät von einem anderen Ort aus Zugang zu geschützten Netzwerken verschaffen.

Mit der Standort-Verifikation können Sie den Missbrauch eines Routers verhindern: Der Router überprüft dann nach jedem Einschalten, ob er am vorgesehenen Standort installiert ist. Erst wenn die Standort-Überprüfung erfolgreich ausgeführt wird, kann das Gerät Nutzdaten über die WAN-Interfaces übertragen.

Für die Standort-Verifikation stehen zwei Verfahren zur Auswahl:

- Über einen ISDN-Anruf zu sich selbst kann das Gerät prüfen, ob es an einem ISDN-Anschluss mit der festgelegten Rufnummer angeschlossen ist.

  Voraussetzungen für eine erfolgreiche ISDN-Standort-Verifikation:

  - Das Gerät muss aus dem öffentlichen ISDN-Netz erreichbar sein.
  - Während der Überprüfung mit dem Selbstanruf benötigt das Gerät zwei freie B-Kanäle. Solange nur ein freier Kanal bereitsteht, z. B. weil an einem Mehrgeräteanschluss mit zwei B-Kanälen ein Kanal zum Telefonieren verwendet wird, kann sich das Gerät nicht selbst über ISDN anrufen.
- Über eine GPS-Positionsbestimmung kann das Gerät die aktuellen Geo-Koordinaten mit den vorgegebenen Werten vergleichen. Dabei kann eine sinnvolle Toleranz von einigen Metern eingeräumt werden.

  Voraussetzungen für eine erfolgreiche GPS-Standort-Verifikation:

  - Am AUX-Anschluss des Gerätes muss eine geeignete GPS-Antenne angeschlossen sein.
  - Das GPS-Signal muss am aktuellen Standort stark genug sein.
  - Eine SIM-Karte für den Mobilfunkbetrieb ist eingelegt und das Gerät ist in ein Mobilfunknetz eingebucht.

1.3 Was kann Ihr LANCOM?

Die folgende Tabelle zeigt Ihnen die Eigenschaften und Funktionen Ihres Gerätes.

	LANCOM 1751 UMTS
Anwendungen	
Internet-Zugang	✔
LAN-LAN-Kopplung über VPN	✔
LAN-LAN-Kopplung über ISDN	✔
RAS-Server (über VPN)	✔
RAS-Server (über ISDN)	✔

	LANCOM 1751 UMTS
IP-Router	✔
NetBIOS-Proxy zur Kopplung von Microsoft-Peer-to-Peer-Netzwerken über ISDN	✔
DHCP- und DNS-Server (für LAN und DMZ)	✔
Advanced Routing and Forwarding (ARF-Netze)	8
N:N-Mapping zum Routen von Netzwerken mit den gleichen IP-Adresskreisen über VPN	✔
Konfiguration von LAN-Ports als zusätzliche WAN-Ports	✔
Policy-based Routing zur regelbasierten Auswahl der Zielroute	✔
Load-Balancing zur Bündelung von mehreren DSL-Kanälen	4 Kanäle
Backup-Lösungen und Load-Balancing mit VRRP	✔
PPPoE-Server	✔
WAN-RIP	✔
Layer-2-QoS-Tagging	✔
802.1p	✔
NAT Traversal (NAT-T)	✔
DMZ mit konfigurierbarer IDS-Prüfung	✔
ISDN-Festverbindungen	✔
LANCAPI-Server für den Einsatz von Office-Anwendungen wie Fax oder Anrufbeantworter über die ISDN-Schnittstelle.	✔
WAN-Anschlüsse	
Integriertes ADSL-Modem (mit ADSL2+)	✔
Integriertes UMTS/HSxPA-Modem (GPRS, EGDE, UMTS, HSxPA)	✔

DE

	LANCOM 1751 UMTS
ISDN-S_0-Anschluss in Punkt-zu-Mehrpunkt-Konfiguration (Mehrgeräteanschluss) oder in Punkt-zu-Punkt-Konfiguration (Anlagenanschluss) mit automatischer D-Kanal-Protokoll-Erkennung. Unterstützt statische und dynamische Kanalbündelung per MLPPP und BACP sowie Stac-Datenkompression (Hi/fn). Auch zum Aufbau von Dynamic VPN-Verbindungen zu Gegenstellen mit dynamischen IP-Adressen.	✔
LAN-Anschluss	
Individuelle Fast Ethernet LAN Ports, einzeln schaltbar, z.B. als LAN-Switch oder separate DMZ-Ports, Auto-Crossover. Alternativ schaltbar als WAN-Interface.	4
Sicherheitsfunktionen	
IPSec-Verschlüsselung über externe Software (VPN-Client)	✔
5 integrierte VPN-Tunnel zur Absicherung von Netzwerkverbindungen	✔
IPSec-Verschlüsselung über Hardware (optional, Aktivierung über VPN-25-Option)	✔
IP-Masquerading (NAT, PAT) zum Verstecken aller Arbeitsstationen im LAN hinter einer einheitlichen öffentlichen IP-Adresse.	✔
Stateful-Inspection-Firewall	✔
Firewall-Filter zur gezielten Sperrung von IP-Adressen, Protokollen und Ports	✔
MAC-Adressfilter kontrolliert u.a. den Zugriff von Arbeitsstationen im LAN auf die IP-Routing-Funktion	✔
Konfigurationsschutz zur Abwehr von „Brute-Force-Angriffen“.	✔
Diebstahlschutz durch Standortverifikation über ISDN oder GPS.	✔
Konfiguration	
Konfiguration mit LANconfig oder mit Webbrowser, zusätzlich Terminalmodus für Telnet oder andere Terminalprogramme, SNMP-Schnittstelle und TFTP-Serverfunktion	✔
1-Click-VPN-Assistenten zur besonders komfortablen Einrichtung von RAS-Zugängen und LAN-Kopplungen über VPN	✔
Fernkonfiguration über ISDN (mit ISDN-PPP-Verbindungen z. B. über das DFÜ-Netzwerk von Windows).	✔
Serielle Konfigurations-Schnittstelle	✔
Rückruffunktion mit PPP-Authentifizierung-Mechanismen zur Beschränkung auf festgelegte ISDN-Rufnummern	✔

DE

	LANCOM 1751 UMTS
FirmSafe zum Einspielen neuer Firmwareversionen ohne Risiko	✔
Optionale Software-Erweiterungen	
LANCOM VPN Option mit 25 aktiven Tunneln zur Absicherung von Netzwerkkopplungen inkl. Aktivierung des Hardware-Beschleunigers	✔
LANCOM Service-Option	✔
Optionale Hardware-Erweiterungen	
19" Rackmount-Adapter	✔

2 Installation

2.1 Lieferumfang

Bitte prüfen Sie den Inhalt der Verpackung auf Vollständigkeit, bevor Sie mit der Installation beginnen. Neben dem LANCOM UMTS Router sollte der Karton folgendes Zubehör für Sie bereithalten:

	LANCOM 1751 UMTS
12 V DC Steckernetzteil	✔
LAN-Kabel (grüne Stecker)	✔
ADSL-Anschlusskabel (transparente Stecker)	✔
ISDN-Anschlusskabel (hellblaue Stecker)	✔
Anschlusskabel für die Konfigurationsschnittstelle	✔
Zwei 2 dBi Dipol-UMTS/GPRS-Antennen (850-960 Mhz und 1700-2220 Mhz) mit SMA-Anschluss	✔
GPS-Antenne mit SMA-Anschluss und 5m Kabel	✔
LANCOM-CD	✔
Gedruckte Dokumentation	✔

Falls etwas fehlen sollte, wenden Sie sich bitte umgehend an Ihren Händler oder an die Kontaktadresse, die auf dem Lieferschein zu Ihrem Gerät angegeben ist.

2.2 Systemvoraussetzungen

Rechner, die mit einem LANCOM in Verbindung treten möchten, müssen mindestens die folgenden Voraussetzungen erfüllen:

- Betriebssystem mit TCP/IP-Unterstützung, z. B. Windows Vista™, Windows XP, Windows Millennium Edition (Me), Windows 2000, Windows 98, Linux, BSD Unix, Apple Mac OS, OS/2.

Die LANtools benötigen zudem ein Windows-Betriebssystem. Für den Zugriff auf WEBconfig ist ein Web-Browser unter einem beliebigen Betriebssystem erforderlich.

DE

2.3 Statusanzeigen und Schnittstellen

2.3.1 Statusanzeigen

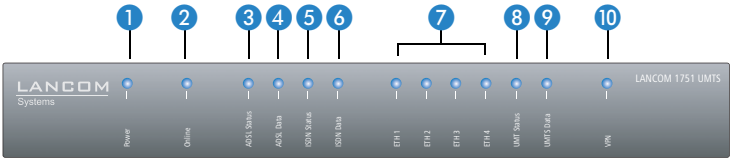
Bedeutung der LEDs

In den folgenden Abschnitten verwenden wir verschiedene Begriffe, um das Verhalten der LEDs zu beschreiben:

- **Blinken** bedeutet, dass die LED in gleichmäßigen Abständen in der jeweils angegebenen Farbe ein- bzw. ausgeschaltet wird.
- **Blitzen** bedeutet, dass die LED in der jeweiligen Farbe sehr kurz aufleuchtet und dann deutlich länger (etwa 10x so lange) ausgeschaltet bleibt.
- **Invers Blitzen** bedeutet das Gegenteil. Hier leuchtet die LED in der jeweiligen Farbe dauerhaft und wird nur sehr kurz unterbrochen.
- **Flackern** bedeutet, dass die LED in unregelmäßigen Abständen ein- und ausgeschaltet wird.

Vorderseite

Die LANCOM UMTS Router verfügen über Statusanzeigen auf der Vorderseite.



Oberseite

Die beiden LEDs auf der Oberseite ermöglichen ein bequemes Ablesen der wichtigsten Statusanzeigen auch bei vertikaler Befestigung des Gerätes.

1 Power

Diese LED gibt Auskunft über die Betriebsbereitschaft des Geräts. Nach dem Einschalten blinkt sie für die Dauer des Selbsttests grün. Danach wird entweder ein festgestellter Fehler als roter Blinkcode ausgegeben, oder aber das Gerät geht in Betrieb, und die LED leuchtet konstant grün.

aus		Gerät abgeschaltet
grün	blinkend	Selbsttest nach dem Einschalten
grün	dauerhaft an	Gerät betriebsbereit
rot/grün	abwechselnd blinkend	Gerät unsicher: Kein Konfigurationskennwort gesetzt
rot	blinkend	Zeit- oder Gebührenlimit für Online-Verbindungen erreicht
rot	blinkend	Gerät ist aufgrund nicht erfolgreich verlaufener Standort-Verifikation gesperrt.

Die Power-LED blinkt abwechselnd rot/grün, solange noch kein Konfigurationskennwort gesetzt wurde. Ohne Konfigurationskennwort sind die Konfigurationsdaten des LANCOM ungeschützt. Im Normalfall setzen Sie ein Konfigurationskennwort während der Grundkonfiguration (Anleitung im folgenden Kapitel). Informationen zur nachträglichen Vergabe eines Konfigurationskennworts finden Sie im Abschnitt 'Der Sicherheits-Assistent'.

DE

Blinkende Power-LED und keine Verbindung möglich?

Signal für ein erreichtes Zeit- oder Gebührenlimit

Blinkt die Power-LED rot und können keine WAN-Verbindungen mehr aufgebaut werden, so ist das kein Grund zur Besorgnis. Vielmehr wurde ein vorher eingestelltes Zeit- oder Gebührenlimit erreicht.

Es gibt drei Möglichkeiten die Sperre zu lösen:

- Gebührenschutz zurücksetzen.
- Das erreichte Limit erhöhen.
- Die erreichte Sperre ganz deaktivieren (Limit auf '0' setzen).

Im LANmonitor wird Ihnen das Erreichen eines Zeit- oder Gebührenlimits angezeigt. Zum Reset des Gebührenschutzes wählen Sie im Kontextmenü (rechter Mausklick) **Zeit- und Gebühren-Limits zurücksetzen**. Die Gebühreneinstellungen legen Sie in LANconfig unter **Management ▶ Kosten** fest (Sie können nur dann auf diese Einstellungen zugreifen, wenn unter **Extras ▶ Optionen** die 'Vollständige Darstellung der Konfiguration' aktiviert ist).

Mit WEBconfig finden Sie den Gebührenschutz-Reset und alle Parameter unter **Experten-Konfiguration ▶ Setup ▶ Gebühren-Modul**.

2 Online

Die Online-LED zeigt allgemein den Status aller WAN-Schnittstellen an:

aus		keine aktive Verbindung
grün	blitzend	Aufbau der ersten Verbindung
grün	invers blitzend	Aufbau einer weiteren Verbindung
grün	dauerhaft an	mindestens eine Verbindung aufgebaut
rot	dauerhaft an	Fehler beim Aufbau der letzten Verbindung

3 ADSL Status

Informationen über den Verbindungszustand am ADSL-Anschluss:

aus		Interface abgeschaltet
grün	blinkend/blitzend	Handshake/Trainingsphase
grün	dauerhaft	Synchronisation erfolgreich
rot	flackernd	Fehler (CRC-Fehler, Framing-Fehler etc.)
rot	dauerhaft an	Keine Synchronisation bzw. Suchen der Gegenstelle
rot/ orange	blinkend	Hardware-Fehler

4 ADSL Data

Informationen über den Datenverkehr am ADSL-Anschluss:

aus		keine logische Verbindung
grün	blitzend	Aufbau der ersten Verbindung
grün	invers blitzend	Aufbau der zweiten Verbindung
grün	dauerhaft an	Verbindung über einen B-Kanal aufgebaut
grün	invers flackernd	Datenverkehr (Versand oder Empfang)

5 ISDN Status

Informationen über den Verbindungsstatus am ISDN-S_0-Anschluss:

aus		nicht angeschlossen oder keine S_0-Spannung (keine Fehlermeldung)
grün	blinkend	Initialisierung D-Kanal (Kontaktaufnahme mit Verbindungsstelle)
grün	dauerhaft an	D-Kanal betriebsbereit
rot	flackernd	Fehler auf dem D-Kanal
rot	dauerhaft an	D-Kanal-Aktivierung fehlgeschlagen

Wenn die ISDN-Status-LED automatisch erlischt, so ist dies kein Zeichen für einen Fehler am S_0-Bus. Vielmehr schalten zahlreiche ISDN-Anschlüsse und Telefonanlagen den S_0-Bus nach einer bestimmten inaktiven Zeit in einen Stromsparmodus. Bei Bedarf wird der S_0-Bus automatisch reaktiviert und die ISDN-Status-LED leuchtet grün.

6 ISDN Data

Gemeinsame Information über den Datenverkehr auf beiden ISDN-B-Kanälen:

aus		keine Verbindung aufgebaut
grün	blinkend	Anwahl läuft
grün	blitzend	Aufbau der ersten Verbindung
grün	invers blitzend	Aufbau der zweiten Verbindung
grün	dauerhaft an	Verbindung über einen B-Kanal aufgebaut
grün	invers flackernd	Datenverkehr (Versand oder Empfang)

DE

7 ETH

Zustand der LAN-Anschlüsse im integrierten Switch:

aus		kein Netzwerkgerät angeschlossen
grün	dauerhaft an	Verbindung zu Netzwerkgerät betriebsbereit, kein Datenverkehr
grün	flackernd	Datenverkehr
rot	flackernd	Kollision von Datenpaketen

8 UMTS Status

Information über den Verbindungszustand des UMTS-Moduls:

aus		UMTS-Interface ausgeschaltet
rot	dauerhaft an	UMTS-Interface eingeschaltet, UMTS-Modul wurde (noch) nicht gefunden
rot/grün	blinkend	Fehler der SIM-Karte
orange	blitzend/blinkend	UMTS-Modul gefunden, Einbuchung in das UMTS-Netz läuft
orange	dauerhaft an	UMTS-Modul betriebsbereit, Einbuchung in das UMTS-Netz erfolgreich
grün	dauerhaft an	GPRS-Verbindung verfügbar
grün	blinken 1x pro Sekunde	EDGE-Verbindung verfügbar
grün	blinken 4x pro Sekunde mit Pausen	UMTS-Verbindung verfügbar
grün	blinken 8x pro Sekunde mit Pausen	HSxPA-Verbindung verfügbar

9 UMTS Data

Information über den Datenverkehr auf der UMTS-Schnittstelle:

aus		keine UMTS-Verbindung
grün	blinkend	Anwahl läuft
grün	blitzend	Aufbau der ersten Verbindung
grün	invers blitzend	Aufbau der weiteren Verbindung
grün	dauerhaft an	mindestens eine logische Verbindung aufgebaut
grün	invers flackernd	Datenverkehr (Versand oder Empfang)

Derzeit ist im UMTS-Netz jeweils nur eine Verbindung möglich.

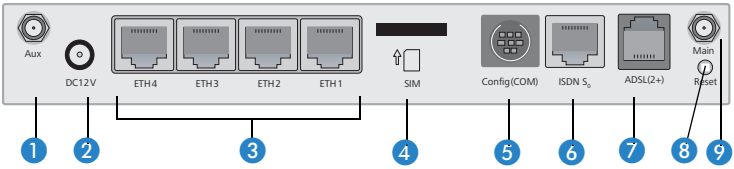
10 VPN

Status einer VPN-Verbindung.

aus		kein VPN-Tunnel aufgebaut
grün	blinkend	Verbindungsaufbau
grün	blitzend	erste Verbindung
grün	invers blitzend	weitere Verbindungen
grün	dauerhaft an	VPN-Tunnel sind aufgebaut

2.3.2 Die Anschlüsse des Geräts

Auf der Rückseite befinden sich die Anschlüsse des LANCOM UMTS Routers:



1 Aux-Anschluss für Mobilfunk- bzw. GPS-Antenne.

- Bei der Verwendung für den Mobilfunk wird an den Aux-Anschluss eine Diversity-Antenne zur Verbesserung der Empfangsqualität angeschlossen.
- Bei der Verwendung für die GPS-Positionsbestimmung wird an den Aux-Anschluss eine GPS-Antenne angeschlossen.

Alternativ kann am Aux-Anschluss auch eine GSM/UMTS/GPS-Kombiantenne betrieben werden, wenn GPS nur kurzfristig für die Standortüberwachung verwendet wird. Sobald der Standort als korrekt identifiziert ist, steht die GSM/UMTS-Diversity-Funktionalität wieder zur Verfügung, der GPS-Empfang wird automatisch deaktiviert.

2 Anschluss für das mitgelieferte Netzteil.

3 Switch mit 10/100Base-Tx-Anschlüssen.

4 Einschub für die SIM-Karte.

5 Serielle Konfigurationsschnittstelle (RS 232/V.24).

6 ISDN-S_0-Anschluss

7 ADSL-Anschluss (ADSL, ADSL 2, ADSL 2+)

8 Reset-Schalter

9 Main-Anschluss für Mobilfunk-Antenne. An den Main-Anschluss wird die Haupt-Antenne angeschlossen.

DE

Die Funktion des Reset-Tasters

Der Reset-Taster hat mit Booten (Neustart) und Reset (Rücksetzen auf Werkseinstellung) grundsätzlich zwei verschiedene Funktionen, die durch unterschiedlich lange Betätigungszeiten des Tasters ausgelöst werden.

Manche Geräte können jedoch nicht unter Verschluss aufgestellt werden. Hier besteht die Gefahr, dass die Konfiguration versehentlich gelöscht wird, wenn ein Mitarbeiter den Reset-Taster zu lange gedrückt hält. Mit einer entsprechenden Einstellung kann das Verhalten des Reset-Tasters gesteuert werden:

Konfigurationstool	Aufruf
WEBconfig, Telnet	Experten-Konfiguration > Setup > Config

- **Reset-Taster**

  Mit dieser Option wird das Verhalten des Reset-Tasters gesteuert:

  - Ignorieren: Der Taster wird ignoriert.

Bitte beachten Sie folgenden Hinweis: Mit der Einstellung 'Ignorieren' oder 'Nur-Booten' wird das Rücksetzen der Konfiguration auf den Auslieferungszustand durch einen Reset unmöglich gemacht. Falls für ein Gerät in diesem Zustand das Konfigurationskennwort nicht mehr vorliegt, gibt es keine Möglichkeit mehr, auf das Gerät zuzugreifen! In diesem Fall kann über die serielle Konfigurationsschnittstelle eine neue Firmware in das Gerät geladen werden – dabei wird das Gerät in den Auslieferungszustand zurückgesetzt, und die bisherige Konfiguration wird gelöscht. Hinweise zum Firmware-Upload über die serielle Konfigurationsschnittstelle finden Sie im LCOS-Referenzhandbuch.

  - Nur-Booten: Beim Druck auf den Taster wird nur ein Neustart ausgelöst, unabhängig von der gedrückten Dauer.
  - Reset-oder-Booten (Standardeinstellung): Ein kurzer Druck auf den Taster führt zum Neustart, ein Druck von 5 Sekunden oder länger führt zum Neustart mit dem Rücksetzen der Konfiguration auf den Auslie-

ferungszustand. Alle LEDs am Gerät leuchten dauerhaft auf. Sobald der Taster freigegeben wird, startet das Gerät mit Werkseinstellungen neu.

Das Gerät startet nach dem Reset neu im unkonfigurierten Zustand, **alle** Einstellungen gehen dabei verloren. Sichern Sie daher **vor** dem Reset nach Möglichkeit die aktuelle Konfiguration des Geräts!

2.4 Installation der Hardware

Die Installation der LANCOM UMTS Router erfolgt in folgenden Schritten:

① **Antennen** – schrauben Sie die mitgelieferten Mobilfunk-Antennen auf der Rückseite des LANCOM UMTS Routers an. Schrauben Sie alternativ eine GPS-Antenne an den Aux-Anschluss 1 des Geräts.

Antennen dürfen nur bei ausgeschaltetem Gerät montiert oder gewechselt werden. Die Montage oder Demontage bei eingeschaltetem Gerät kann zur Zerstörung der UMTS-Module führen!

Beachten Sie bei der Montage von separat erworbenen Mobilfunk-Antennen, dass die maximal zulässige Sendeleistung des UMTS-Systems von 0,25 W (entspricht 24 dBm) nach EIRP nicht überschritten werden darf. Für die Einhaltung der Grenzwerte ist der Betreiber des Systems verantwortlich.

② **LAN** – Sie können den LANCOM UMTS Router zunächst an Ihr LAN anschließen. Stecken Sie dazu das mitgelieferte Netzwerkkabel (grüne Stecker) in einen LAN-Anschluss des Geräts 3 und andererseits in eine freie Netzwerkanschlussdose Ihres lokalen Netzes (bzw. in eine freie Buchse eines Hubs/Switchs). Alternativ können Sie auch einen einzelnen PC anschließen.

Der LAN-Anschluss erkennt die notwendige Belegung des Anschlusses automatisch (Auto MDI/X), ebenso die Übertragungsrate (10/100 Mbit) des angeschlossenen Netzwerkgerätes (Autosensing).

Informationen zur Installation von PoE finden Sie in der Info-Box 'Power-over-Ethernet – elegante Stromversorgung über die LAN-Verkabelung'.

③ **ADSL** – verbinden Sie die ADSL-Schnittstelle 7 über das mitgelieferte ADSL-Anschlusskabel (transparente Stecker) mit dem Splitter.

Der Betrieb von ADSL ist sowohl über analoge Telefonanschlüsse (Annex A) als auch über ISDN (Annex B) möglich. Je nach Land und Anbieter wird eine der beiden Varianten angeboten. Ein LANCOM 1751 UMTS kann durch das Einspielen einer entsprechenden Firmware auf die gewünschte Verwendung eingestellt werden.

④ **Anschluss an das ISDN-Netz** – für den Anschluss des LANCOM UMTS Routers an das ISDN-Netz stecken Sie das eine Ende eines mitgelieferten ISDN-Anschlusskabels (hellblaue Stecker) in die ISDN-S_0-Schnittstelle 6. Stecken Sie das andere Ende des ISDN-Kabels in einen ISDN/S_0-Anlagenanschluss oder -Mehrgeräteanschluss.

⑤ **SIM-Karte einschieben** – schieben Sie die SIM-Karte in den Einschub 4 und beachten Sie dabei die Markierung für die richtige Lage der Karte.

Achten Sie beim Einschieben der SIM-Karte darauf, dass die Karte im Einschub einrastet. Um die Karte wieder aus dem Gerät zu entfernen, drücken Sie die Karte mit leichtem Druck in das Gerät hinein. Beim Loslassen löst sich die SIM-Karte aus der eingerasteten Position im Einschub.

⑥ **Mit Spannung versorgen** – versorgen Sie das Gerät an Buchse 2 über das mitgelieferte Netzteil mit Spannung.

Verwenden Sie ausschließlich das in den technischen Daten aufgeführte Netzteil! Die Verwendung eines ungeeigneten Netzteils kann zu Personen- oder Sachschäden führen.

⑦ **Betriebsbereit?** – nach einem kurzen Selbsttest des Geräts leuchtet die Power-LED permanent grün bzw. blinkt abwechselnd rot und grün solange noch kein Konfigurationspasswort gesetzt ist.

2.5 Installation der Software

Der folgende Abschnitt beschreibt die Installation der mitgelieferten Systemsoftware LANtools, die unter Windows läuft.

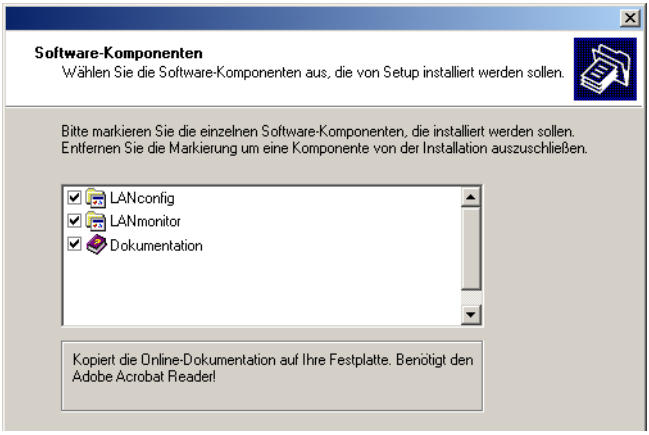
Sollten Sie Ihren LANCOM UMTS Router ausschließlich mit PCs verwenden, die unter anderen Betriebssystemen als Windows laufen, können Sie diesen Abschnitt überspringen.

2.5.1 Software-Setup starten

Legen Sie die Produkt-CD in Ihr Laufwerk ein. Daraufhin startet das Setup-Programm automatisch.

Sollte das Setup nicht automatisch starten, so rufen Sie die Datei AUTORUN.EXE aus dem Hauptverzeichnis der LANCOM-CD auf.

Klicken Sie im Setup auf **Software installieren**. Es erscheint folgendes Auswahlmenü auf dem Bildschirm:



DE

2.5.2 Welche Software installieren?

- **LANconfig** ist das Windows-Konfigurationsprogramm für alle LANCOM Router und LANCOM Access Points. Alternativ (oder ergänzend) kann über einen Web-Browser WEBconfig verwendet werden.
- Mit **LANmonitor** überwachen Sie auf einem Windows-Rechner alle LANCOM Router und LANCOM Access Points.
- Der **LANCOM Advanced VPN Client** ermöglicht den Aufbau von VPN-Verbindungen von einem entfernten Rechner über das Internet zu einem Router mit VPN-Funktion.
- Mit **Dokumentation** kopieren Sie die Dokumentationsdateien auf Ihren PC.

Wählen Sie die gewünschten Software-Optionen aus und bestätigen Sie mit **Weiter**. Die Software wird automatisch installiert.

3 Grundkonfiguration

Die Grundkonfiguration erfolgt mit Hilfe eines komfortablen Setup-Assistenten, der Sie Schritt für Schritt durch die Konfiguration führt und dabei die notwendigen Informationen abfragt.

Dieses Kapitel zeigt Ihnen zunächst, welche Angaben für die Grundkonfiguration erforderlich sind. Mit Hilfe dieses ersten Abschnitts stellen Sie sich schon vor Aufruf des Assistenten alle notwendigen Daten zusammen.

Anschließend erfolgt die Eingabe der Daten im Setup-Assistenten. Aufruf und Ablauf werden Schritt für Schritt beschrieben – in jeweils einem eigenen Abschnitt für LANconfig und WEBconfig. Dank der vorherigen Zusammenstellung aller notwendigen Angaben gelingt die Grundkonfiguration jetzt schnell und ohne Mühe.

Zum Abschluss dieses Kapitels zeigen wir Ihnen, welche Einstellungen an den Arbeitsplatzrechnern im LAN notwendig sind, damit der Zugriff auf das Gerät einwandfrei funktioniert.

3.1 Welche Angaben sind notwendig?

Der Grundkonfigurations-Assistent nimmt die TCP/IP-Grundeinstellung des LANCOM UMTS Routers vor und schützt das Gerät mit einem Konfigurationskennwort. Die folgende Beschreibung der vom Assistenten geforderten Angaben gliedert sich in die folgenden Konfigurationsabschnitte:

- TCP/IP-Einstellungen
- Schutz der Konfiguration
- Angaben zum ISDN-Anschluss
- Einstellung des Gebührenschutzes
- Sicherheitseinstellungen

3.1.1 TCP/IP-Einstellungen

Die TCP/IP-Konfiguration kann auf zweierlei Art erfolgen: Entweder vollautomatisch oder manuell. Bei der vollautomatischen TCP/IP-Konfiguration ist keine Benutzereingabe erforderlich. Alle Parameter werden selbstständig vom Setup-Assistenten gesetzt. Bei der manuellen TCP/IP-Konfiguration fragt der Assistent die üblichen TCP/IP-Parameter ab: IP-Adresse, Netzmaske etc. (dazu später mehr).

Die vollautomatische TCP/IP-Konfiguration ist nur in bestimmten Netzwerkumgebungen möglich. Deshalb analysiert der Setup-Assistent das ange-

schlossene LAN daraufhin, ob die vollautomatische Konfiguration möglich ist oder nicht.

Neues LAN – vollautomatische Konfiguration möglich

Sind alle angeschlossenen Netzwerkgeräte noch unkonfiguriert, dann bietet der Setup-Assistent die vollautomatische TCP/IP-Konfiguration an. Dazu kommt es normalerweise in folgenden Situationen:

- Nur ein Einzelplatz-PC wird an den LANCOM UMTS Router angeschlossen
- Neuaufbau eines Netzwerks

Wenn Sie den LANCOM UMTS Router in ein bestehendes TCP/IP-LAN integrieren, wird die vollautomatische TCP/IP-Konfiguration nicht angeboten. In diesem Fall können Sie mit dem Abschnitt 'Notwendige Angaben für die manuelle TCP/IP-Konfiguration' fortfahren.

Das Ergebnis der vollautomatischen TCP/IP-Konfiguration: Der LANCOM UMTS Router erhält die IP-Adresse '172.23.56.254' (Netzmaske '255.255.255.0'). Außerdem wird der integrierte DHCP-Server aktiviert, so dass der LANCOM UMTS Router den Geräten im LAN automatisch IP-Adressen zuweist.

Trotzdem manuell konfigurieren?

Die vollautomatische TCP/IP-Konfiguration ist optional. Sie können stattdessen auch die manuelle Konfiguration wählen. Treffen Sie diese Wahl nach folgenden Überlegungen:

- Wählen Sie die automatische Konfiguration wenn Sie mit Netzwerken und IP-Adressen **nicht** vertraut sind.
- Wählen Sie die manuelle TCP/IP-Konfiguration, wenn Sie mit Netzwerken und IP-Adressen vertraut sind und eine der folgenden Annahmen zutrifft:
  - Sie haben bisher in Ihrem Netzwerk noch keine IP-Adressen verwendet, möchten das ab jetzt aber gerne tun. Sie möchten die IP-Adresse für den Router selbst festlegen und geben ihm eine beliebige Adresse aus einem der für private Zwecke reservierten Adressbereiche, z.B. '10.0.0.1' mit der Netzmaske '255.255.255.0'. Damit legen Sie auch gleichzeitig den Adressbereich fest, den der DHCP-Server anschließend für die anderen Geräte im Netz verwendet (sofern der DHCP-Server aktiviert wird).
  - Sie haben auch bisher schon IP-Adressen auf den Rechnern im LAN verwendet.

Notwendige Angaben für die manuelle TCP/IP-Konfiguration

Bei der manuellen TCP/IP-Konfiguration fragt Sie der Setup-Assistent nach folgenden Daten:

- **DHCP-Betriebsart**
  - Aus: Die erforderlichen IP-Adressen müssen manuell eingetragen werden.
  - Server: Der LANCOM UMTS Router arbeitet als DHCP-Server im Netzwerk, zumindest die eigene IP-Adresse und die Netzmaske müssen angegeben werden.
  - Client: Der LANCOM UMTS Router bezieht als DHCP-Client die Adress-Informationen von einem anderen DHCP-Server, es müssen keine Adress-Informationen angegeben werden.
- **IP-Adresse und Netzwerkmaske für den LANCOM UMTS Router**
  Teilen Sie dem LANCOM UMTS Router eine freie IP-Adresse aus dem Adressbereich Ihres LAN zu, und geben Sie die Netzwerkmaske an.
- **Gateway-Adresse**
  Geben Sie die IP-Adresse des Gateways an, wenn Sie die DHCP-Betriebsart 'Aus' gewählt haben oder in der DHCP-Betriebsart 'Server' ein anderes Netzwerkgerät die Aufgabe des Gateways übernimmt.
- **DNS-Server**
  Geben Sie die IP-Adresse eines DNS-Servers zur Auflösung der Domain-Namen an, wenn Sie die DHCP-Betriebsart 'Aus' gewählt haben oder in der DHCP-Betriebsart 'Server' ein anderes Netzwerkgerät die Aufgabe des DNS-Servers übernimmt.

3.1.2 Konfigurationsschutz

Mit dem Kennwort schützen Sie den Konfigurationszugang zum LANCOM UMTS Router und verhindern so, dass Unbefugte diese modifizieren. Die Konfiguration des Gerätes enthält zahlreiche sensible Daten, wie beispielsweise die Daten für den Internet-Zugang, und sollte auf jeden Fall durch ein Kennwort geschützt sein.

In der Konfiguration des LANCOM können mehrere Administratoren angelegt werden, die über unterschiedliche Zugriffsrechte verfügen. Für einen LANCOM UMTS Router können bis zu 16 verschiedene Administratoren eingerichtet werden. Weitere Informationen finden

Sie im LCOS-Referenzhandbuch unter „Rechteverwaltung für verschiedene Administratoren".

3.1.3 Einstellungen für den ISDN-Anschluss

Wenn Sie den ISDN-Anschluss verwenden möchten, können Sie folgende Einstellungen vornehmen:

- Eine oder mehrere ISDN-MSNs, an der der Router Anrufe entgegennehmen soll. MSNs sind ISDN-Rufnummern, die Ihnen vom Telefonanbieter zugewiesen werden. Sie werden normalerweise ohne Vorwahl angegeben. Die angegebenen Nummern haben nur für Router-Funktionen (LAN-LAN-Kopplung, RAS) Bedeutung, nicht jedoch für die Fernkonfiguration und LANCOM VPN Option.
- Eine Amtsvorwahl für den Zugang zum öffentlichen Netz. Sie ist normalerweise nur beim Anschluss an einer ISDN-Telefonanlage erforderlich. Üblich ist die '0'. Diese Amtsvorwahl wird für alle ausgehenden Rufe verwendet.
- Schließlich sollten Sie wissen, ob die Telefongesellschaft den ISDN-Gebührenimpuls übermittelt. Dieser kann vom LANCOM Router für Gebührenbudgets und die Accounting-Funktion ausgewertet werden.

3.1.4 Gebührenschutz

Der Gebührenschutz verhindert den Verbindungsaufbau von DSL-Verbindungen über ein vorher eingestelltes Maß hinaus und schützt Sie so vor unerwartet hohen Verbindungskosten.

Wenn Sie den LANCOM Router an einem DSL-Anschluss betreiben, der zeitbasiert abgerechnet wird, können Sie die maximale Verbindungszeit in Minuten festsetzen.

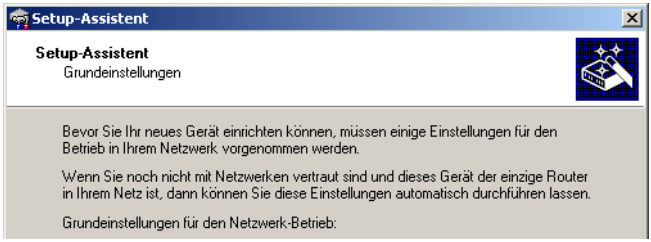
Das Budget kann durch Eingabe des Wertes '0' komplett deaktiviert werden.

In der Grundeinstellung ist der Gebührenschutz auf maximal 600 Minuten innerhalb von sieben Tagen eingestellt. Passen Sie diese Einstellung an Ihre persönlichen Bedürfnisse an oder deaktivieren Sie den Gebührenschutz, wenn Sie mit Ihrem Provider einen Pauschal-Tarif (Flatrate) vereinbart haben.

3.2 Anleitung für LANconfig

① Starten Sie LANconfig mit **Start** ▶ **Programme** ▶ **LANCOM** ▶ **LANconfig**. LANconfig erkennt neue LANCOM-Geräte im TCP/IP-Netz selbstständig.

② Wird bei der Suche ein unkonfiguriertes Gerät gefunden, startet der Setup-Assistent, der Ihnen bei der Grundeinstellung des Geräts behilflich ist oder Ihnen (die passende Netzwerkumgebung vorausgesetzt) sogar die gesamte Arbeit abnimmt.



Sollte der Zugriff auf einen unkonfigurierten LANCOM UMTS Router scheitern, so kann dieser Fehler auf die Netzmaske des LAN zurückzuführen sein: Bei weniger als 254 möglichen Hosts (Netzmaske > '255.255.255.0') muss sichergestellt sein, dass die IP-Adresse 'x.x.x.254' im eigenen Subnetz vorhanden ist.

Wenn Sie die automatische TCP/IP-Konfiguration wählen, fahren Sie mit Schritt ⑤ fort.

③ Geben Sie dem LANCOM eine verfügbare Adresse aus einem geeigneten IP-Adressbereich. Bestätigen Sie mit **Weiter**.

④ Im folgenden Fenster legen Sie zunächst das Kennwort für den Konfigurationszugriff fest. Achten Sie bei der Eingabe auf Groß- und Kleinschreibung, sowie auf eine ausreichende Länge (mindestens 6 Zeichen).

Ferner legen Sie fest, ob das Gerät nur aus dem lokalen Netzwerk heraus konfiguriert werden darf, oder ob auch die Fernkonfiguration über das WAN (also aus einem entfernten Netzwerk) erlaubt ist.

Bitte beachten Sie, dass mit dieser Freigabe auch die Fernkonfiguration über das Internet ermöglicht wird. Sie sollten in jedem Fall darauf achten, dass der Konfigurationszugriff durch ein Kennwort abgesichert ist.

DE

⑤ Der Gebührenschutz beschränkt auf Wunsch die Kosten von WAN-Verbindungen auf ein festgesetztes Maß. Bestätigen Sie Ihre Angaben mit **Weiter**.

⑥ Schließen Sie die Konfiguration mit **Fertig stellen** ab.

Im Abschnitt 'TCP/IP-Einstellungen an den Arbeitsplatz-PCs' erfahren Sie, welche Einstellungen an den Arbeitsplatzrechnern im LAN notwendig sind.

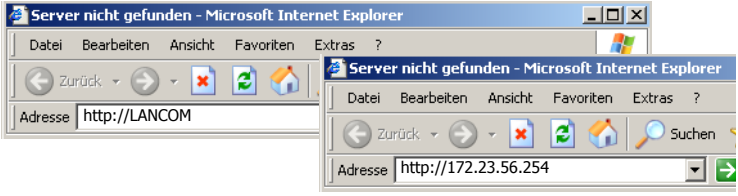
3.3 Anleitung für WEBconfig

Für die Konfiguration mit WEBconfig müssen Sie wissen, wie sich der LANCOM UMTS Router im LAN ansprechen lässt. Das Verhalten der Geräte sowie ihre Erreichbarkeit zur Konfiguration über einen Webbrowser hängen davon ab, ob im LAN schon DHCP-Server und DNS-Server aktiv sind, und ob diese beiden Serverprozesse die Zuordnung von IP-Adressen zu symbolischen Namen im LAN untereinander austauschen.

Nach dem Einschalten prüfen unkonfigurierte LANCOM-Geräte zunächst, ob im LAN schon ein DHCP-Server aktiv ist. Je nach Situation kann das Gerät dann den eigenen DHCP-Server einschalten oder alternativ den DHCP-Client-Modus aktivieren. In dieser zweiten Betriebsart kann das Gerät selbst eine IP-Adresse von einem im LAN schon vorhandenen DHCP-Server beziehen.

Netz ohne DHCP-Server

In einem Netz ohne DHCP-Server schalten unkonfigurierte LANCOM-Geräte nach dem Starten den eigenen DHCP-Serverdienst ein und weisen den anderen Rechnern im LAN die IP-Adressen sowie Informationen über Gateways etc. zu, sofern diese auf den automatischen Bezug der IP-Adressen eingestellt sind (Auto-DHCP). In dieser Konstellation kann das Gerät von jedem Rechner mit aktivierter Auto-DHCP-Funktion mit einem Webbrowser unter dem Namen **LANCOM** oder unter der IP-Adresse **172.23.56.254** erreicht werden.

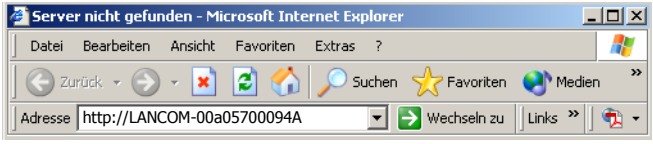


Falls der Konfigurations-Rechner seine IP-Adresse nicht vom LANCOM-DHCP-Server bezieht, ermitteln Sie die aktuelle IP-Adresse des Rechners (mit **Start ▶ Ausführen ▶ cmd** und dem Befehl **ipconfig** an der Eingabeaufforderung unter Windows 2000 oder Windows XP, mit **Start ▶ Ausführen ▶ cmd** und dem Befehl **winipcfg** an der Eingabeaufforderung unter Windows Me oder Windows 9x bzw. dem Befehl **ifconfig** in der Konsole unter Linux). In diesem Fall erreichen Sie das LANCOM unter der Adresse **x.x.x.254** (die "x" stehen für die ersten drei Blöcke in der IP-Adresse des Konfigurationsrechners).

Netz mit DHCP-Server

Ist im LAN ein DHCP-Server zur Zuweisung der IP-Adressen aktiv, schaltet ein unkonfiguriertes LANCOM-Gerät seinen eigenen DHCP-Server aus, wechselt in den DHCP-Client-Modus und bezieht eine IP-Adresse vom DHCP-Server aus dem LAN. Diese IP-Adresse ist aber zunächst nicht bekannt, die Erreichbarkeit des Geräts hängt von der Namensauflösung ab:

- Ist im LAN auch ein DNS-Server zur Auflösung der Namen vorhanden und tauscht dieser die Zuordnung von IP-Adressen zu den Namen mit dem DHCP-Server aus, kann das Gerät unter dem Namen "LANCOM-<MAC-Adresse>" (z.B. "LANCOM-00a057xxxxxx") erreicht werden.



Die MAC-Adresse finden Sie auf einem Aufkleber auf der Geräteunterseite.

- Ist im LAN kein DNS-Server vorhanden oder ist dieser nicht mit dem DHCP-Server gekoppelt, kann das Gerät nicht über den Namen erreicht werden. In diesem Fall bleiben folgende Optionen:
  - Die per DHCP an das LANCOM-Gerät zugewiesene IP-Adresse über geeignete Tools ausfindig machen und das Gerät mit dieser IP-Adresse direkt erreichen.
  - LANconfig verwenden.

Aufruf der Assistenten in WEBconfig

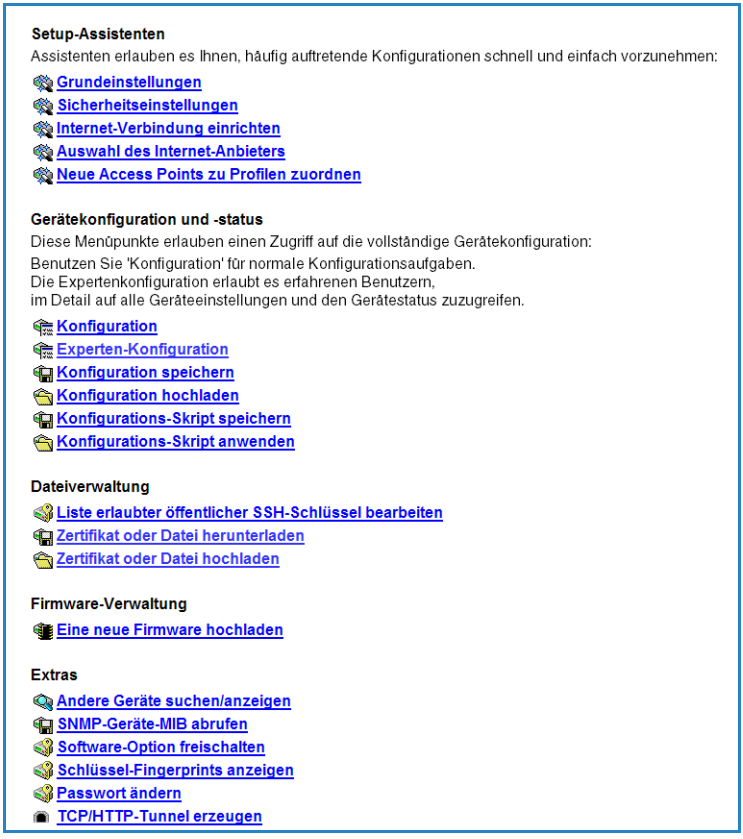
① Öffnen Sie also Ihren Web-Browser (z.B. Internet Explorer, Firefox, Opera) und rufen Sie dort den LANCOM UMTS Router auf:

`http://<IP-Adresse des LANCOM>`

(bzw. über beliebigen Namen)

Sollte der Zugriff auf einen unkonfigurierten LANCOM UMTS Router scheitern, so kann dieser Fehler auf die Netzmaske des LAN zurückzuführen sein: Bei weniger als 254 möglichen Hosts (Netzmaske > '255.255.255.0') muss sichergestellt sein, dass die IP-Adresse 'x.x.x.254' im eigenen Subnetz vorhanden ist.

Es erscheint das Hauptmenü von WEBconfig:



Die Setup-Assistenten sind exakt auf die Funktionalität des jeweiligen Modells zugeschnitten. Es kann daher sein, dass Ihr Gerät nicht alle hier abgebildeten Assistenten anbietet.

Wenn Sie die automatische TCP/IP-Konfiguration wählen, fahren Sie mit Schritt ③ fort.

② Wenn Sie die TCP/IP-Einstellungen selbst vornehmen wollen, dann geben Sie dem LANCOM eine verfügbare Adresse aus einem geeigneten IP-Adressbereich. Stellen Sie außerdem ein, ob er als DHCP-Server arbeiten soll oder nicht. Bestätigen Sie Ihre Eingabe mit **Setzen**.

③ Im folgenden Fenster 'Sicherheitseinstellungen' vergeben Sie zunächst ein Kennwort für den Konfigurationszugriff. Achten Sie bei der Eingabe auf Groß- und Kleinschreibung, sowie auf eine ausreichende Länge (mindestens 6 Zeichen).

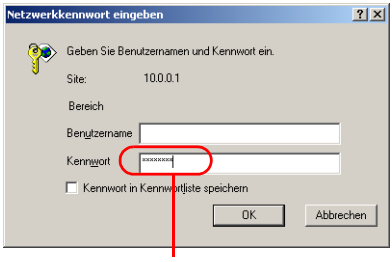
Legen Sie fest, ob das Gerät nur aus dem lokalen Netzwerk heraus konfiguriert werden darf, oder ob auch die Fernkonfiguration über das WAN (also aus einem entfernten Netzwerk) erlaubt ist.

Bitte beachten Sie, dass mit dieser Freigabe auch die Fernkonfiguration über das Internet ermöglicht wird. Sie sollten in jedem Fall darauf achten, dass der Konfigurationszugriff geeignet abgesichert ist, z. B. durch ein Kennwort.

Eingabe des Kennworts im Web-Browser

Wenn Sie beim Zugriff auf das Gerät von Ihrem Web-Browser zur Eingabe von Benutzername und Kennwort aufgefordert werden, tragen Sie Ihre persönlichen Werte in die entsprechenden Felder der Eingabemaske ein. Achten Sie dabei auf Groß- und Kleinschreibung.

Falls Sie den allgemeinen Konfigurationszugang verwenden, tragen Sie nur das entsprechende Kennwort ein. Das Feld Benutzername bleibt in diesem Fall leer.



Eingabe des Konfigurations-Kennworts

④ Wählen Sie im nächsten Fenster Ihren Internet-Provider aus der angebotenen Liste aus. Bestätigen Sie Ihre Wahl mit **Setzen**.

Bei Auswahl von 'Mein Anbieter ist hier nicht aufgeführt' müssen Sie im anschließenden Fenster das von Ihrem Internet-Provider verwendete Übertragungsprotokoll manuell angeben. In aller Regel funktioniert das Universal-Protokoll 'Multimode'.

⑤ Der Gebührenschutz beschränkt auf Wunsch die Kosten von WAN-Verbindungen auf ein festgesetztes Maß. Bestätigen Sie Ihre Angaben mit **Setzen**.

⑥ Der Grundeinrichtungs-Assistent meldet, dass alle notwendigen Angaben vorliegen. Mit **Weiter** schließen Sie ihn ab.

3.4 TCP/IP-Einstellungen an den Arbeitsplatz-PCs

Bei TCP/IP-Netzwerken ist die korrekte Adressierung aller Geräte im LAN außerordentlich wichtig. Ferner sollten alle Rechner die IP-Adressen von zwei zentralen Stellen im LAN kennen:

- Standard-Gateway – erhält alle Pakete, die nicht an Rechner im lokalen Netz adressiert sind
- DNS-Server – übersetzt einen Netzwerk- oder Rechnernamen in eine konkrete IP-Adresse.

Der LANCOM UMTS Router kann sowohl die Funktionen eines Standard-Gateways als auch die eines DNS-Servers übernehmen. Außerdem kann er als DHCP-Server allen Rechnern im LAN automatisch eine korrekte IP-Adresse zuweisen.

Die korrekte TCP/IP-Konfiguration der PC im LAN hängt entscheidend davon ab, nach welcher Methode im LAN die IP-Adressen vergeben werden:

- **IP-Adressvergabe über ein LANCOM**

  In dieser Betriebsart weist ein LANCOM den PCs im LAN und WLAN (bei Geräten mit Funkmodul) nicht nur eine IP-Adresse zu, sondern übermittelt per DHCP auch seine eigene IP-Adresse als Standard-Gateway und DNS-Server. Die PCs sind deshalb so einzustellen, dass sie ihre eigene IP-Adresse, ebenso wie die IP-Adressen von Standard-Gateway und DNS-Server automatisch (über DHCP) beziehen.

- **IP-Adressvergabe über einen separaten DHCP-Server**

  Die Arbeitsplatz-PCs sind so einzustellen, dass sie ihre eigene IP-Adresse, ebenso wie die IP-Adressen von Standard-Gateway und DNS-Server automatisch (über DHCP) beziehen. Auf dem DHCP-Server ist die IP-Adresse des LANCOMs so zu hinterlegen, dass der DHCP-Server sie an die PCs im LAN als Standard-Gateway übermittelt. Außerdem sollte der DHCP-Server den LANCOM als DNS-Server angeben.

- **Manuelle Zuweisung der IP-Adressen**

  Werden die IP-Adressen im Netzwerk statisch vergeben, so sind bei jedem PC im LAN die IP-Adresse des LANCOMs als Standard-Gateway und als DNS-Server in der TCP/IP-Konfiguration einzustellen.

Weitere Informationen und Hilfe zu den TCP/IP-Einstellungen Ihres LANCOM UMTS Routers finden Sie im Referenzhandbuch. Bei der Netzwerkkonfiguration der Arbeitsplatzrechner hilft Ihnen die Dokumentation des installierten Betriebssystems weiter.

3.5 Standort-Verifikation über ISDN oder GPS

Nach einem Diebstahl kann ein Gerät theoretisch von Unbefugten an einem anderen Ort betrieben werden. Auch bei einer passwortgeschützten Geräte-Konfiguration könnten so die im Gerät konfigurierten RAS-Zugänge, LAN-Kopplungen oder VPN-Verbindungen unerlaubt genutzt werden, ein Dieb könnte sich Zugang zu geschützten Netzwerken verschaffen.

Der Betrieb des Gerätes kann jedoch mit verschiedenen Mitteln so geschützt werden, dass es nach dem Wiedereinschalten oder beim Einschalten an einem anderen Ort nicht mehr verwendet werden kann.

3.5.1 GPS-Standort-Verifikation

Für die GPS-Standort-Verifikation können Sie im Gerät eine erlaubte geografische Position definieren. Nach dem Einschalten aktiviert das Gerät bei Bedarf automatisch das GPS-Modul und prüft, ob es sich an der „richtigen" Position befindet – nur bei einer positiven Prüfung wird das Router-Modul eingeschaltet. Nach Abschluss der Standort-Verifikation wird das GPS-Modul automatisch wieder deaktiviert, sofern es nicht manuell eingeschaltet ist.

3.5.2 ISDN-Standort-Verifikation

Mit der ISDN-Standort-Verifikation können Sie den Missbrauch eines Routers verhindern: Der Router überprüft dann nach jedem Einschalten über einen ISDN-Anruf zu sich selbst, ob er am vorgesehenen Standort installiert ist. Erst wenn die Standort-Überprüfung erfolgreich ausgeführt wurde, wird das Router-Modul eingeschaltet.

Voraussetzungen für eine erfolgreiche ISDN-Standort-Verifikation:

- Das Gerät muss aus dem öffentlichen ISDN-Netz erreichbar sein.
- Während der Überprüfung mit dem Selbstanruf benötigt das Gerät zwei freie B-Kanäle. Solange nur ein freier Kanal bereitsteht, z.B. weil an einem

Mehrgeräteanschluss mit zwei B-Kanälen ein Kanal zum Telefonieren verwendet wird, kann sich das Gerät nicht selbst über ISDN anrufen.

3.5.3 Konfiguration der Standort-Verifikation

LANconfig

Die Parameter für die Standort-Verifikation finden Sie im LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Standort'.

DE

Auf der Registerkarte 'GPS' können Sie das GPS-Modul unabhängig von der Standort-Verifikation einschalten, um z. B. die aktuellen Standortkoordination mit LANmonitor zu überwachen.

- Mit der Option 'Standort-Überprüfung einschalten' aktivieren Sie die Standort-Verifikation.
- Wählen Sie die Methode für die Standort-Überprüfung:
  - 'Selbst-Anruf' für die Überprüfung über ISDN mit einem Rückruf.

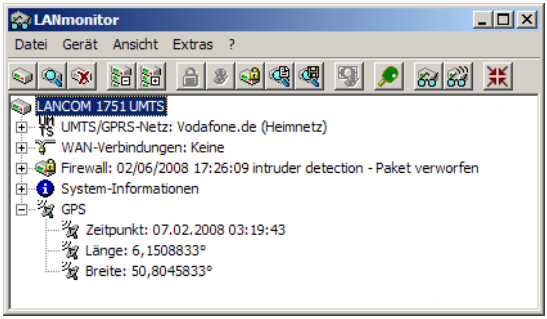
- 'Rufweiterleitungs-Überprüfung' für die Überprüfung über ISDN durch Abfrage der Rufnummer aus der Vermittlungsstelle. Hierbei ist kein Rückruf erforderlich.
- 'GPS-Verifikation' für die Überprüfung über die Geo-Koordinaten.

Für die Standort-Überprüfung über GPS muss eine entsprechende GPS-Antenne an den AUX-Anschluss des Gerätes angeschlossen werden. Zusätzlich muss eine SIM-Karte für den Mobilfunkbetrieb eingelegt werden und das Gerät muss in ein Mobilfunknetz eingebucht sein.

- Tragen Sie für die Standort-Überprüfung über 'Selbst-Anruf' oder 'Rufweiterleitungs-Überprüfung' als 'Ziel-Rufnummer' ein, auf welche Telefonnummer geprüft werden soll.
- Tragen Sie für die Standort-Überprüfung über GPS die Parameter für die GPS-Prüfung ein:
  - Längen- und Breitengrad
  - Abweichung von der erlaubten Position in Metern

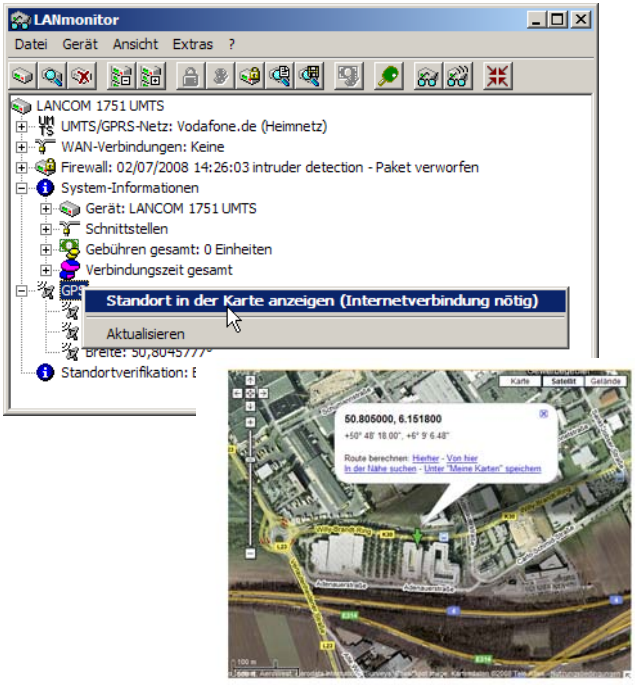
Die Geo-Koordinaten für den aktuellen Standort kann das Gerät selbst ermitteln, indem Sie den Schalter 'Referenz-Koordinaten per GPS holen' aktivieren. Nach dem Rückschreiben der Konfiguration in das Gerät werden automatisch die aktuellen Längen- und Breitengrade eingetragen, wenn die Standortverifikation aktiv ist und gültige GPS-Daten vorliegen. Anschließend wird diese Option selbsttätig wieder deaktiviert.

Alternativ können Sie die Geo-Koordinaten für beliebige Standorte über Tools wie z. B. Google Maps ermitteln.



DE

Wenn im LANmonitor die aktuellen Geo-Koordinaten angezeigt werden, können Sie mit einem rechten Mausklick auf den Eintrag 'GPS' den aktuellen Standort in der Satelliten-Ansicht von Google Maps aufrufen.



WEBconfig, Telnet oder Terminalprogramm

Unter WEBconfig, Telnet bzw. Terminalprogramm finden Sie die Einstellungen für die Standort-Verifikation auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Expertenkonfiguration ▶ Setup ▶ Config ▶ Standortverifikation
Terminal/Telnet	`Setup/Config/Standortverifikation`

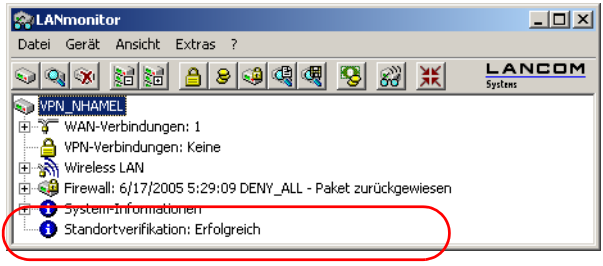
Experten-Konfiguration
Setup
Config

Standortverifikation

In-Betrieb	nein
Methode	GPS
ISDN-Ifc	S0-1
Zielrufnummer	
Abgehende-Rufnummer	
Erwartete-abgehende-Rufnummer	
Abweichung[m]	50
Laenge[Grad]	0
Breite[Grad]	0
Hole-GPS-Position	nein

Statusabfrage der Standort-Verifikation

Der Status der Standortverifikation kann über den LANmonitor eingesehen werden:



Mit WEBconfig (**Expertenkonfiguration ▶ Status ▶ Config ▶ Standort-verifikation**) oder Telnet (`Status/Config/Standortverifikation`) können Sie den Status der Standort-Verifikation einsehen:

Erst wenn die Standort-Verifikation im Zustand 'Erfolgreich' ist, kann der Router Daten über die WAN-Interfaces übertragen.

- Eine Standort-Verifikation über ISDN ist dann erfolgreich, wenn die Nummer 'Erwarte-Ruf-von' mit der Nummer der 'Zuletzt-gesehener-Ruf-von' übereinstimmt. Der Anruf wird dabei nicht vom Router angenommen. Der Status zeigt außerdem an, ob der Router überhaupt einen Ruf erkannt hat.
- Eine Standort-Verifikation über GPS ist dann erfolgreich, wenn die GPS-Position gültig ist und innerhalb der zulässigen Abweichung mit der Soll-Position übereinstimmt.

4 Sicherheits-Einstellungen

Ihr LANCOM verfügt über zahlreiche Sicherheitsfunktionen. In diesem Kapitel finden Sie alle Informationen, die Sie für eine optimale Absicherung des Gerätes benötigen.

Die Konfiguration der Sicherheitseinstellungen können Sie sehr schnell und komfortabel mit dem Sicherheits-Assistenten von LANconfig oder WEBconfig vornehmen.

4.1 Tipps für den richtigen Umgang mit Schlüsseln und Passphrases

Mit der Einhaltung einiger wichtiger Regeln im Umgang mit Schlüsseln erhöhen Sie die Sicherheit von Verschlüsselungsverfahren erheblich.

- **Halten Sie Schlüssel so geheim wie möglich.**
  Notieren Sie niemals einen Schlüssel. Beliebt, aber völlig ungeeignet sind beispielsweise: Notizbücher, Brieftaschen und Textdateien im Computer. Verraten Sie einen Schlüssel nicht unnötig weiter.
- **Wählen Sie einen zufälligen Schlüssel.**
  Verwenden Sie zufällige Buchstaben- und Ziffernfolgen. Schlüssel aus dem allgemeinen Sprachgebrauch sind unsicher.
- **Wechseln Sie einen Schlüssel sofort bei Verdacht.**
  Wenn ein Mitarbeiter mit Zugriff auf einen Schlüssel Ihr Unternehmen verlässt, wird es höchste Zeit, den Schlüssel des Funk-LANs zu wechseln. Der Schlüssel sollte auch bei geringstem Verdacht einer undichten Stelle erneuert werden.
- **LEPS verhindert die globale Verbreitung von Passphrases.**
  Nutzen Sie deswegen LEPS, um eine individuelle Passphrase nutzen zu können.

4.2 Der Sicherheits-Assistent

Der Zugriff auf die Konfiguration des Geräts erlaubt nicht nur das Auslesen kritischer Informationen (z. B. Internet-Kennwort). Vielmehr können auch die Einstellungen der Sicherheitsfunktionen (z. B. Firewall) nach Belieben geändert werden. Dadurch bringt der unbefugte Konfigurationszugriff nicht nur das einzelne Gerät, sondern das gesamte Netzwerk in große Gefahr.

DE

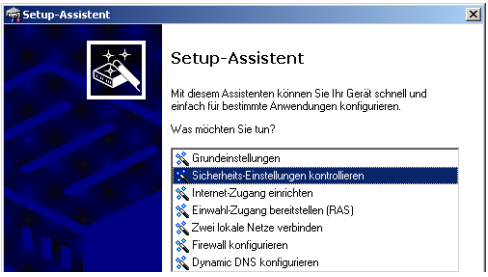
Ihr LANCOM verfügt über einen Kennwortschutz für den Konfigurationszugang. Dieser wird schon während der Grundkonfiguration durch Angabe eines Kennwortes aktiviert.

Das Gerät sperrt den Konfigurationszugang automatisch für eine festgelegte Dauer, wenn eine bestimmte Anzahl von Anmelde-Fehlversuchen festgestellt wird. Sowohl die kritische Anzahl Fehlversuche als auch die Dauer der Sperre lassen sich modifizieren. Standardmäßig sperrt das Gerät nach dem fünften Fehlerversuch für eine Dauer von fünf Minuten.

Neben diesen grundlegenden Einstellungen prüfen Sie mit dem Sicherheitsassistenten auch die Sicherheitseinstellungen für das Funknetzwerk, sofern Ihr Gerät über eine WLAN-Schnittstelle verfügt.

4.2.1 Assistent für LANconfig

① Markieren Sie Ihren LANCOM im Auswahlfenster. Wählen Sie aus der Befehlsleiste den Punkt **Extras** ▶ **Setup Assistent**.



② Wählen Sie im Auswahlmenü den Setup-Assistenten **Sicherheitseinstellungen kontrollieren** und bestätigen Sie die Auswahl mit **Weiter**.

③ In den folgenden Fenstern stellen Sie das Passwort ein und wählen die zulässigen Protokolle für den Konfigurationszugriff von lokalen und entfernten Netzwerken aus.

④ Für den Fern-Zugriff auf das Gerät über ISDN können Sie eine bestimmte Rufnummer (MSN) festlegen.

⑤ In einem weiteren Schritt werden die Parameter der Konfigurationssperre wie Anzahl der Fehllogins und Dauer der Sperre eingestellt.

⑥ Der Assistent informiert Sie sobald die Eingaben vollständig sind. Schließen Sie die Konfiguration mit **Fertig stellen** ab.

4.2.2 Assistent für WEBconfig

Unter WEBconfig besteht die Möglichkeit, den Assistenten **Sicherheitseinstellungen** aufzurufen und die Einstellungen zu kontrollieren und zu ändern. Dabei werden die folgenden Werte bearbeitet:

- Passwort für das Gerät
- zulässige Protokolle für den Konfigurationszugriff von lokalen und entfernten Netzwerken
- Parameter der Konfigurationssperre (Anzahl der Fehllogins und Dauer der Sperre)

4.3 Die Sicherheits-Checkliste

In der folgenden Checkliste finden Profis alle wichtigen Sicherheitseinstellungen im Überblick. Die meisten Punkte dieser Checkliste sind in einfachen Konfigurationen unbedenklich. In solchen Fällen reichen die Sicherheitseinstellungen aus, die während der Grundkonfiguration oder mit dem Sicherheits-Assistenten gesetzt werden.

Detaillierte Informationen zu den angesprochenen Sicherheitseinstellungen finden Sie im Referenzhandbuch.

- **Haben Sie ein Kennwort für die Konfiguration vergeben?**

  Die einfachste Möglichkeit zum Schutz der Konfiguration ist die Vereinbarung eines Kennworts. Solange Sie kein Kennwort vereinbart haben, kann jeder die Konfiguration des Gerätes verändern. Das Feld zur Eingabe des Kennworts finden Sie in LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Security'. Es ist insbesondere dann unerläßlich, ein Kennwort zur Konfiguration zu vergeben, wenn Sie die Fernkonfiguration erlauben wollen!

- **Haben Sie die Fernkonfiguration zugelassen?**

  Wenn Sie die Fernkonfiguration nicht benötigen, so schalten Sie sie ab. Wenn Sie die Fernkonfiguration benötigen, so vergeben Sie unbedingt einen Kennwortschutz für die Konfiguration (siehe vorhergehender Abschnitt). Das Feld zur Abschaltung der Fernkonfiguration finden Sie ebenfalls in LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Security'. Wählen Sie hier unter 'Zugriffsrechte - von entfernten Netzen' für alle Konfigurationsarten die Option 'nicht erlaubt'.

DE

- **Haben Sie die SNMP-Konfiguration mit einem Kennwort versehen?**

  Schützen Sie auch die SNMP-Konfiguration mit einem Kennwort. Das Feld zum Schutz der SNMP-Konfiguration mit einem Kennwort finden Sie ebenfalls in LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Security'.

- **Haben Sie die Firewall aktiviert?**

  Die Stateful-Inspection Firewall der LANCOM-Geräte sorgt dafür, dass Ihr lokales Netzwerk von außen nicht angegriffen werden kann. Die Firewall können Sie in LANconfig unter 'Firewall/Qos' auf der Registerkarte 'Allgemein' einschalten.

- **Verwenden Sie eine 'Deny-All' Firewall-Strategie?**

  Für maximale Sicherheit und Kontrolle unterbinden Sie zunächst jeglichen Datentransfer durch die Firewall. Nur die Verbindungen, die explizit gestattet sein sollen, sind in die Firewall einzutragen. Damit wird 'Trojanern' und bestimmten E-Mail-Viren der Kommunikations-Rückweg entzogen. Die Firewall-Regeln finden Sie in LANconfig unter 'Firewall/Qos' auf der Registerkarte 'Regeln' zusammengefasst. Eine Anleitung dazu findet sich im Referenzhandbuch.

- **Haben Sie IP-Masquerading aktiviert?**

  IP-Masquerading heißt das Versteck für alle lokalen Rechner beim Zugang ins Internet. Dabei wird nur das Router-Modul des Geräts mit seiner IP-Adresse im Internet bekannt gemacht. Die IP-Adresse kann fest vergeben sein oder vom Provider dynamisch zugewiesen werden. Die Rechner im LAN nutzen den Router dann als Gateway und können selbst nicht erkannt werden. Der Router trennt Internet und Intranet wie eine Wand. Die Verwendung von IP-Masquerading wird für jede Route in der Routing-Tabelle einzeln festgelegt. Die Routing-Tabelle finden Sie in LANconfig im Konfigurationsbereich 'IP-Router' auf der Registerkarte 'Routing'.

- **Haben Sie kritische Ports über Filter geschlossen?**

  Die Firewall-Filter des LANCOMs bieten Filterfunktionen für einzelne Rechner oder ganze Netze. Es ist möglich, Quell- und Ziel-Filter für einzelne Ports oder auch Portbereiche aufzusetzen. Zudem können einzelne Protokolle oder beliebige Protokollkombinationen (TCP/UDP/ICMP) gefiltert werden. Besonders komfortabel ist die Einrichtung der Filter mit Hilfe von LANconfig. Unter 'Firewall/QoS' finden Sie die Karteikarte 'Regeln', mit deren Hilfe Filterregeln definiert und verändert werden können.

- **Haben Sie bestimmte Stationen von dem Zugriff auf das Gerät ausgeschlossen?**

  Mit einer speziellen Filter-Liste kann der Zugriff auf die internen Funktionen der Geräte über TCP/IP eingeschränkt werden. Mit den internen Funktionen werden hierbei Konfigurationssitzungen über LANconfig, WEBconfig, Telnet oder TFTP bezeichnet. Standardmäßig enthält diese Tabelle keine Einträge, damit kann also von Rechnern mit beliebigen IP-Adressen aus über TCP/IP mit Telnet oder TFTP ein Zugriff auf das Gerät gestartet werden. Mit dem ersten Eintrag einer IP-Adresse sowie der zugehörigen Netzmaske wird der Filter aktiviert, und nur noch die in diesem Eintrag enthaltenen IP-Adressen werden berechtigt, die internen Funktionen zu nutzen. Mit weiteren Einträgen kann der Kreis der Berechtigten erweitert werden. Die Filter-Einträge können sowohl einzelne Rechner als auch ganze Netze bezeichnen. Die Zugangsliste finden Sie in LANconfig im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Allgemein'.

- **Lagern Sie Ihre abgespeicherte LANCOM-Konfiguration an einem sicheren Ort?**

  Schützen Sie abgespeicherte Konfigurationen an einem sicheren Ort vor unberechtigtem Zugriff. Eine abgespeicherte Konfiguration könnte sonst von einer unberechtigten Person in ein anderes Gerät geladen werden, wodurch z. B. Ihre Internet-Zugänge auf Ihre Kosten benutzt werden können.

- **Haben Sie die Möglichkeiten zum Schutz der WAN-Zugänge bei einem Diebstahl des Gerätes aktiviert?**

  Nach einem Diebstahl kann ein Gerät theoretisch von Unbefugten an einem anderen Ort betrieben werden. Auch bei einer passwortgeschützten Geräte-Konfiguration könnten so die im Gerät konfigurierten RAS-Zugänge, LAN-Kopplungen oder VPN-Verbindungen unerlaubt genutzt werden, ein Dieb könnte sich Zugang zu geschützten Netzwerken verschaffen.

  Der Betrieb des Gerätes kann jedoch mit verschiedenen Mitteln so geschützt werden, dass es nach dem Wiedereinschalten oder beim Einschalten an einem anderen Ort nicht mehr verwendet werden kann.

  Durch die Funktion der ISDN-Standort-Verifikation kann das Gerät nur an einem bestimmten ISDN-Anschluß betrieben werden. Nach dem Einschalten prüft das Gerät über einen Selbstanruf zu einer festgelegten Rufnum-

mer, ob es sich noch am „richtigen" ISDN-Anschluß befindet (weitere Informationen finden Sie im Referenzhandbuch).

Für die GPS-Standort-Verifikation können Sie im Gerät eine erlaubte geografische Position definieren. Nach dem Einschalten prüft das Gerät, ob es sich an der „richtigen" Position befindet – nur bei einer positiven Prüfung wird das Router-Modul eingeschaltet.

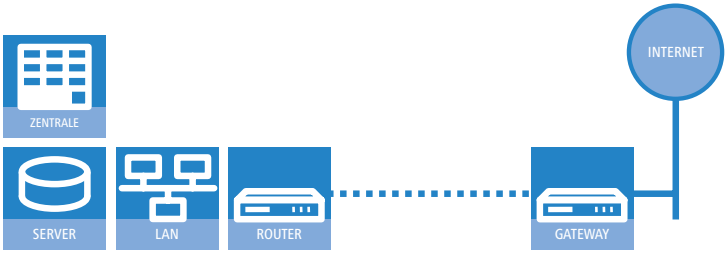
Mit den Funktionen des Scripting kann die gesamte Konfiguration des Gerätes nur im RAM gespeichert werden, der beim Booten des Gerätes gelöscht wird. Die Konfiguration wird dabei gezielt nicht in den bootresistenten Flash-Speicher geschrieben. Mit dem Trennen von der Stromversorgung und dem Aufstellen an einem anderen Ort wird damit die gesamte Konfiguration des Gerätes gelöscht (weitere Informationen finden Sie im Referenzhandbuch).

- **Haben Sie den Reset-Taster gegen das unbeabsichtigte Zurücksetzen der Konfiguration gesichert?**

  Manche Geräte können nicht unter Verschluss aufgestellt werden. Hier besteht die Gefahr, dass die Konfiguration versehentlich gelöscht wird, wenn ein Mitarbeiter den Reset-Taster zu lange gedrückt hält. Mit einer entsprechenden Einstellung kann das Verhalten des Reset-Buttons gesteuert werden, der Reset-Taster wird dann entweder ignoriert oder es wird nur ein Neustart ausgelöst, unabhängig von der gedrückten Dauer.

5 Den Internet-Zugang einrichten

Über den zentralen Internet-Zugang des LANCOM erhalten alle Rechner im LAN Zugriff auf das Internet. Die Verbindung zum Internetanbieter kann über jeden WAN-Anschluss aufgebaut werden, also neben ADSL auch über UMTS oder ISDN (sofern vorhanden). Ein Internet-Zugang über UMTS oder ISDN kann beispielsweise als Backup für ADSL eingesetzt werden. Bitte beachten Sie bei der Einrichtung eines Internetzugangs über UMTS auch das Kapitel → 'Einrichten der UMTS-Profile'.



Welches WAN-Interface?

Die Einrichtung des Internet-Zugangs erfolgt über einen komfortablen Assistenten. Im ersten Schritt wählen Sie aus, über welches WAN-Interface die Internetverbindung aufgebaut werden soll.

Um eine Internetverbindung über das DSL-Interface aufzubauen, müssen Sie an einem der ETH-Ports des Gerätes ein externes ADSL-Modem anschließen. Bei der Konfiguration des Internetzugangs geben Sie an, an welchem ETH-Port das ADSL-Modem angeschlossen wird.

Kennt der Setup-Assistent Ihren Internet-Anbieter?

Der Assistent kennt die Zugangsdaten der wichtigsten Internetanbieter in ihrem Land und bietet Ihnen eine Liste zur Auswahl an. Wenn Sie Ihren Internetanbieter in dieser Liste finden, so müssen Sie für die Einrichtung des Internet-Zugangs normalerweise keine weiteren Übertragungs-Parameter eingeben. Lediglich die Authentifizierungsdaten, die Ihnen Ihr Internetanbieter zur Verfügung stellt, sind noch erforderlich.

Zusätzlich Angaben bei unbekanntem Internet-Anbieter

Kennt der Setup-Assistent Ihren Internet-Anbieter nicht, so fragt er Sie Schritt für Schritt alle notwendigen Zugangsdaten ab. Diese Zugangsdaten stellt Ihnen Ihr Internet-Anbieter zur Verfügung.

Weitere Verbindungsoptionen

Zusätzlich können Sie (sofern von Ihrem Internetanbieter unterstützt) zusätzliche Optionen im Assistenten ein- oder ausschalten:

- Zeitliche Abrechnung oder Flatrate – wählen Sie aus, nach welchem Modell Ihr Internetanbieter die Nutzung abrechnet.
  - Bei der zeitlichen Abrechnung können Sie am LANCOM einstellen, dass bestehende Verbindungen automatisch abgebaut werden, wenn für eine bestimmte Dauer (die sogenannte Haltezeit) keine Daten mehr übertragen wurden.

    Zusätzlich können Sie eine Leitungsüberwachung aktivieren, die inaktive Gegenstellen schneller erkennt und in diesem Fall die Verbindung schon vor Ablauf der Haltezeit abbaut.
  - Bei Flatrate-Abrechnung haben Sie ebenfalls die Möglichkeit der aktiven Leitungsüberwachung, und können so die Funktion der Gegenstelle ständig überprüfen.

    Außerdem können Sie bei Flatrates Verbindungen dauerhaft aufrecht erhalten („Keep-alive"). Im Fall eines Verbindungsabbruchs wird diese automatisch wieder aufgebaut.
- Dynamische Kanalbündelung (nur ISDN)
  - Bei Bedarf wird automatisch der zweite ISDN-B-Kanal zur Verbindung hinzugeschaltet. Dadurch wird die Bandbreite verdoppelt. Unter Umständen werden aber auch die doppelten Verbindungsgebühren fällig. Außerdem ist Ihr ISDN-Anschluss in diesem Fall besetzt, zusätzliche ein- oder ausgehende Anrufe werden abgelehnt.
- Datenkompression (nur ISDN)
  - Sie ermöglicht eine zusätzliche Steigerung der Übertragungsgeschwindigkeit.

Backup-Verbindung zum Internet anlegen

Die Absicherung der Internetverbindung gehört zu den häufigsten Aufgaben der Backup-Lösungen. Bei der Einrichtung eines Internetzugangs haben Sie zusätzlich die Möglichkeit, eine zweite Verbindung zum Internet über ein alternatives WAN-Interface anzulegen. Haben Sie den Haupt-Internetzugang z. B. Über das ADSL-Interface angelegt, können Sie die Backup-Verbindung über UMTS oder ISDN einrichten.

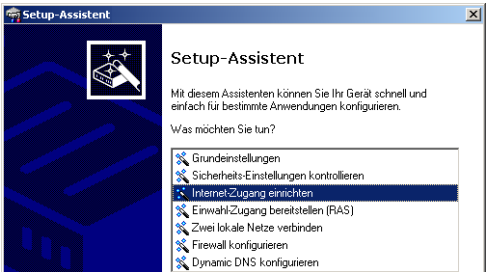
Bei der Konfiguration der Backup-Verbindung können Sie je nach Verfügbarkeit auch einen anderen Provider wählen. Damit überbrücken

Sie nicht nur die physikalische Leitung, sondern auch generelle Störungen im Netz des Providers.

5.1 Der Internet-Assistent

5.1.1 Anleitung für LANconfig

① Markieren Sie Ihr Gerät im Auswahlfenster. Wählen Sie aus der Befehlsleiste den Punkt **Extras** ▶ **Setup Assistent**.



② Wählen Sie im Auswahlmenü den Setup-Assistenten **Internet-Zugang einrichten** und bestätigen Sie die Auswahl mit **Weiter**.

③ In den folgenden Fenstern wählen Sie Ihr Land, nach Möglichkeit Ihren Internetanbieter, und geben Sie die Zugangsdaten ein.

④ Je nach Verfügbarkeit bietet Ihnen der Assistent weitere Optionen für die Internetverbindung zur Auswahl an.

⑤ Nach der Eingabe aller erforderlichen Daten bietet Ihnen der Assistent die Einrichtung einer Backup-Verbindung an. Wählen Sie dazu das WAN-Interface, über welches die Backup-Verbindung aufgebaut werden soll, und geben Sie die erforderlichen Zugangsdaten für den Internetzugang über dieses Interface ein.

Der Assistent richtet mit diesen Angaben den alternativen Internetzugang ein und erstellt gleichzeitig die erforderlichen Einträge in der Backup-Tabelle und in der PPP-Tabelle zur Überprüfung der Internetverbindung vor.

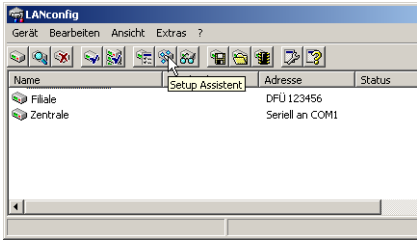
Bitte beachten Sie, dass bei einem Backup über UMTS möglicherweise nicht alle Dienste wie auf der Haupt-Internetverbindung verfügbar sind. Manche UMTS-Dienstanbieter ermöglichen die Nutzung von VPN-Tunneln oder VoIP-Anwendungen über Mobilfunkverbindungen

nur gegen zusätzliche Gebühren oder sperren diese ganz, andere Anbieter vergeben IP-Adressen aus einem privaten Adresskreis und behindern somit Anwendungen, die an eine öffentliche IP-Adresse geknüpft sind. Bitte erkundigen Sie sich bei Ihrem UMTS-Anbieter über evtl. vorhandene Einschränkungen.

⑥ Der Assistent informiert Sie, sobald die Eingaben vollständig sind. Schließen Sie die Konfiguration mit **Fertig stellen** ab.

LANconfig: Schneller Aufruf der Setup-Assistenten

Die Setup-Assistenten rufen Sie unter LANconfig am schnellsten über den Befehlsknopf in der Button-Leiste auf.



5.1.2 Anleitung für WEBconfig

① Wählen Sie im Hauptmenü **Internet-Zugang einrichten**.

② In den folgenden Fenstern wählen Sie Ihr Land, nach Möglichkeit Ihren Internetanbieter, und geben Sie die Zugangsdaten ein.

③ Je nach Verfügbarkeit bietet Ihnen der Assistent weitere Optionen für die Internetverbindung zur Auswahl an.

④ Der Assistent informiert Sie sobald die Eingaben vollständig sind. Schließen Sie die Konfiguration mit **Weiter** ab.

5.2 Der Firewall-Assistent

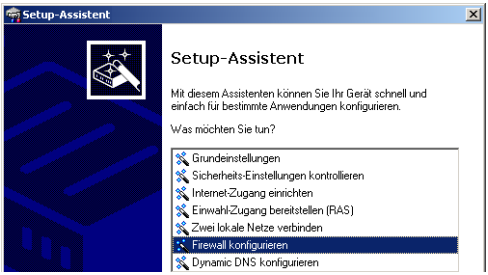
Ihr LANCOM verfügt über eine Stateful-Inspection-Firewall und Firewall-Filter zur wirksamen Absicherung Ihres LAN gegenüber dem Internet. Kernidee der Stateful-Inspection-Firewall ist, dass nur selbstinitiierter Datentransfer als zulässig betrachtet wird. Alle Zugriffe, die unaufgefordert nicht aus dem lokalen Netz heraus erfolgen, sind unzulässig.

Der Firewall-Assistent hilft Ihnen, schnell und komfortabel neue Regeln für die Firewall zu erstellen.

Nähere Informationen zur Firewall Ihres LANCOM und zu deren Konfiguration finden Sie im Referenzmanual.

5.2.1 Assistent für LANconfig

① Markieren Sie Ihr LANCOM im Auswahlfenster. Wählen Sie aus der Befehlsleiste den Punkt **Extras** ▶ **Setup Assistent**.



② Wählen Sie im Auswahlmenü den Setup-Assistenten **Firewall konfigurieren** und bestätigen Sie die Auswahl mit **Weiter**.

③ In den folgenden Fenstern wählen Sie aus, auf welche Dienste/Protokolle sich die Regel bezieht. Im nächsten Schritt legen Sie fest, für welche Quell- und Zielstationen die Regel gilt und welche Aktionen ausgeführt werden sollen, wenn die Regel auf ein Datenpaket zutrifft.

④ Zum Abschluss geben Sie der neuen Regel einen Namen, aktivieren sie und legen fest, ob weitere Regeln beachtet werden sollen, wenn die Regel auf ein Datenpaket zutrifft.

⑤ Der Assistent informiert Sie sobald die Eingaben vollständig sind. Schließen Sie die Konfiguration mit **Fertig stellen** ab.

5.2.2 Konfiguration unter WEBconfig

Unter WEBconfig besteht die Möglichkeit, die Parameter zur Absicherung des Internet-Zugriffs unter **Konfiguration** ▶ **Firewall / QoS** ▶ **Regeln** ▶ **Regeltabelle** aufzurufen, die Einstellungen zu kontrollieren und zu ändern.

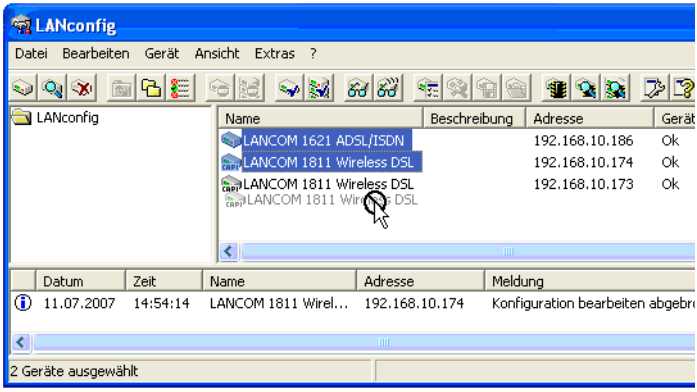
DE

6 Zwei Netzwerke verbinden

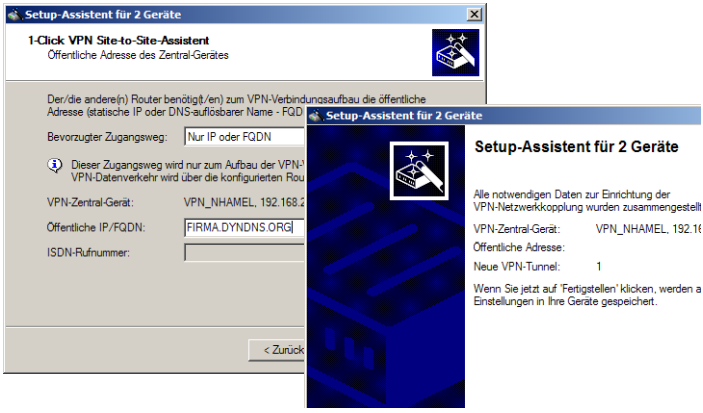
Mit der Netzwerkkopplung (auch LAN-LAN-Kopplung) des LANCOM Router werden zwei lokale Netzwerke miteinander verbunden. Die Einstellungen für die Kopplung von Netzwerken können sehr komfortabel über den 1-Click-VPN-Assistenten vorgenommen werden. Dabei können sogar mehrere Router gleichzeitig an ein zentrales Netzwerk gekoppelt werden.

① Markieren Sie in LANconfig die Router der Filialen, für die Sie eine VPN-Kopplung zu einem zentralen Router einrichten möchten.

② Ziehen Sie die Geräte mit der Maus auf den Eintrag für den zentralen Router.



③ Der 1-Click-VPN Site-to-Site-Assistent startet. Geben Sie den Namen für diesen Zugang ein und wählen Sie aus, über welche Adresse der Router aus dem Internet erreichbar ist.



④ Wählen Sie aus, ob der Verbindungsaufbau über den Namen bzw. die IP-Adresse des zentralen Routers oder über eine ISDN-Verbindung erfolgen soll. Geben Sie dazu die Adresse bzw. den Namen des zentralen Routers bzw. seine ISDN-Nummer an.

⑤ Im letzten Schritt legen Sie fest, wie die verbundenen Netzwerke untereinander kommunizieren können:

- ☐ Nur das INTRANET der Zentrale wird für die Außenstellen verfügbar gemacht werden.
- ☐ Alle privaten Netze der Außenstellen können ebenfalls über die Zentrale untereinander verbunden werden.

Alle Eingaben werden nur einmal für das Zentralgerät vorgenommen und dann in den Geräteeigenschaften hinterlegt.

Die Kopplung von Netzwerken über VPN kann unter WEBconfig nicht mit Hilfe des Assistenten, sondern nur in der Expertenkonfiguration eingerichtet werden. Details dazu finden Sie im Referenzhandbuch.

DE

7 Einwahl-Zugang bereitstellen

An Ihrem LANCOM UMTS Router können Sie Einwahl-Zugänge einrichten, über die sich einzelne Rechner in Ihr LAN einwählen können und für die Dauer der Verbindung vollwertiger Teilnehmer des Netzwerks werden. Dieser Dienst wird auch als RAS (**R**emote **A**ccess **S**ervice) bezeichnet.

LANCOM Systems bietet auf der beiliegenden CD eine 30-Tage-Testversion des LANCOM Advanced VPN Client zur Einwahl in ein Netzwerk über VPN an. Eine genaue Beschreibung des VPN-Client und Hinweise zur Einrichtung finden Sie ebenfalls auf der CD.

VPN-Zugänge für Mitarbeiter, die sich mit Hilfe des LANCOM Advanced VPN Client in ein Netzwerk einwählen, lassen sich sehr einfach mit dem Setup-Assistenten erstellen und in eine Datei exportieren, die vom LANCOM Advanced VPN Client als Profil eingelesen werden kann. Dabei werden die erforderlichen Informationen der aktuellen Konfiguration des LANCOM UMTS Routers entnommen und mit zufällig ermittelten Werten ergänzt (z.B. für den Preshared Key).

① Starten Sie über LANconfig den Setup-Assistenten 'Zugang bereitstellen' und wählen Sie die 'VPN-Verbindung'.

② Aktivieren Sie die Optionen 'LANCOM Advanced VPN Client' und 'Beschleunigen Sie das Konfigurieren mit 1-Click-VPN'.

③ Geben Sie den Namen für diesen Zugang ein und wählen Sie aus, über welche Adresse der Router aus dem Internet erreichbar ist.

④ Im letzten Schritt können Sie wählen, wie die neuen Zugangsdaten ausgegeben werden sollen:

- ☐ Profil als Importdatei für den LANCOM Advanced VPN Client speichern
- ☐ Profil per E-Mail versenden
- ☐ Profil ausdrucken

Das Versenden der Profildatei per E-Mail stellt ein Sicherheitsrisiko dar, weil die E-Mail unterwegs ggf. abgehört werden könnte!

Zum Versenden der Profildatei per E-Mail muss in der Konfiguration des Geräts ein SMTP-Konto mit den erforderlichen Zugangsdaten eingerichtet sein. Außerdem muss auf dem Konfigurationsrechner ein E-

Mail-Programm als Standard-Mail-Anwendung eingerichtet sein, über die auch andere Anwendungen E-Mails versenden dürfen.

Beim Erstellen des VPN-Zugangs werden Einstellungen verwendet, die optimal auf die Verwendung im LANCOM Advanced VPN Client abgestimmt sind, darunter z.B.:

- Gateway: Sofern im LANCOM VPN Router definiert, wird hier ein DynDNS-Name verwendet, ansonsten die IP-Adresse
- FQDN: Kombination aus dem Namen der Verbindung, einer fortlaufenden Nummer und der internen Domäne im LANCOM VPN Router
- Domäne: Sofern im LANCOM VPN Router definiert, wird hier die interne Domäne verwendet, ansonsten ein DynDNS-Name oder die IP-Adresse
- VPN IP-Netze: Alle im Gerät definierten IP-Netzwerke vom Typ 'Intranet'.
- Preshared Key: Zufällig generierter Schlüssel mit einer Länge von 16 ASCII-Zeichen.
- Verbindungsmedium: Für den Verbindungsaufbau wird das LAN genutzt.
- VoIP-Priorisierung: Die VoIP-Priorisierung ist standardmäßig aktiviert.
- Exchange Mode: Als Exchange-Mode wir der 'Aggressive Mode' verwendet.
- IKE-Config-Mode: Der IKE-Config-Mode ist aktiviert, die IP-Adress-Informationen für den LANCOM Advanced VPN Client werden automatisch vom LANCOM VPN Router zugewiesen.

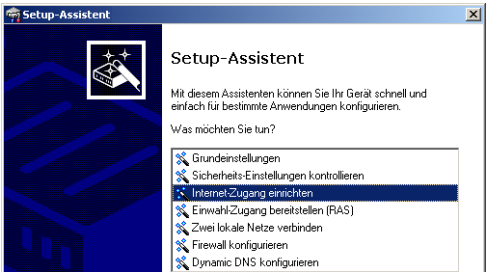
DE

8 Einrichten der UMTS-Profile

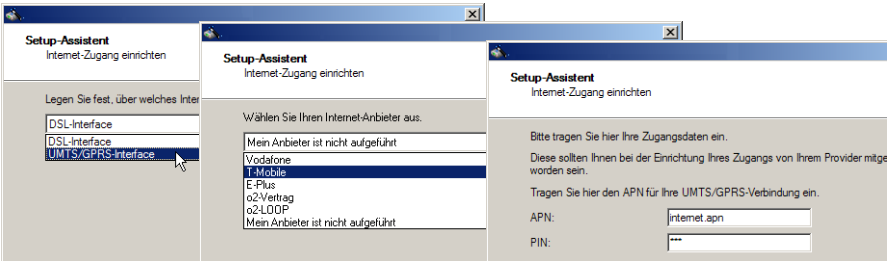
8.1 Internetzugang

Das Einrichten des Internetzugangs über UMTS/HSxPA gelingt am schnellsten mit dem Internet-Assistenten von LANconfig.

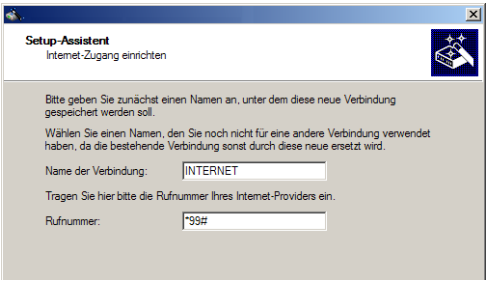
① Markieren Sie Ihren LANCOM UMTS Router im Auswahlfenster. Wählen Sie aus der Befehlsleiste den Punkt **Extras** ▶ **Setup Assistent**.



② Wählen Sie im Auswahlmenü den Setup-Assistenten **Internet-Zugang einrichten** und bestätigen Sie die Auswahl mit **Weiter**.



③ Bei der Einrichtung des Internetzugangs wählen Sie das UMTS-Interface sowie Ihren Netzbetreiber aus und geben den APN (Access Point Name) und die PIN Ihrer SIM-Karte ein. Der Assistent nimmt dann alle weiteren Einstellungen automatisch vor.



④ Sollte Ihr Provider nicht in der Liste aufgeführt sein, können Sie die notwendigen Verbindungsdaten auch manuell eintragen. Dazu benötigen Sie die entsprechende Rufnummer im Mobilfunknetz Ihres Providers.

Diese Informationen erhalten Sie bei Bedarf von Ihrem Mobilfunkprovider.

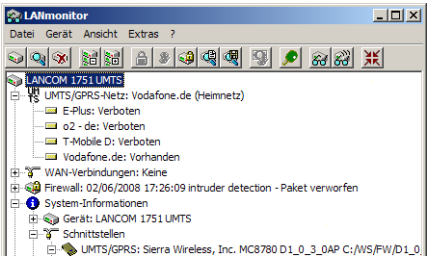
⑤ Zum Abschluss der Konfiguration des Internet-Zugangs können Sie für die UMTS/HSxPA-Verbindung die „Keep-Alive"-Option aktivieren. Damit wird die UMTS/HSxPA-Verbindung so eingerichtet, dass Sie nach dem Einschalten des Geräts automatisch aufgebaut wird und auch nach einer Trennung der Verbindung automatisch wieder hergestellt wird – die Internetverbindung ist „Always On". Diese Funktion ist sehr nützlich für den bequemen Internet-Zugang oder für VPN-Standortkopplungen.

Je nach Tarif können bei Always-On-Internetverbindung hohe Kosten entstehen, z.B. bei zeitbasierter Abrechnung. Bitte informieren Sie sich über die Details Ihres UMTS/HSxPA-Tarifs bei Ihrem Mobilfunk-Provider.

⑥ Alternativ können Sie für die UMTS/HSxPA-Verbindung eine geeignete Haltezeit einstellen. Die Internetverbindung wird dann nicht automatisch gestartet, sondern erst dann, wenn Daten ins Internet übertragen werden sollen. Werden dann für die Dauer der Haltezeit keine Daten mehr übertragen, wird die Verbindung automatisch abgebaut.

DE

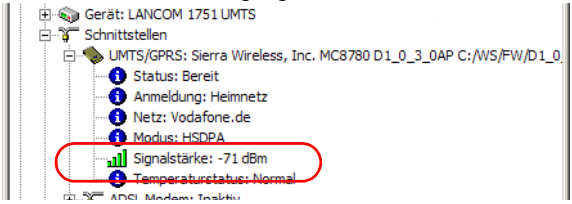
Im LANmonitor können Sie nach dem Einrichten des Internet-Zugangs prüfen, welche Mobilfunknetze verfügbar sind.



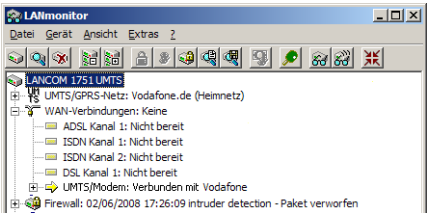
Auch ohne bestehende Verbindung sehen Sie im Bereich 'UMTS/GPRS-Netz' die gefundenen Netze. Darüber hinaus zeigt der LANmonitor hier an, welche Netze erlaubt sind und mit welchen Netzen sich die Karte nicht verbinden kann.

⑦ Im Bereich der Systeminformationen zeigt der LANmonitor die erkannte Datenkarte an und dazu die Signalstärke des Heimnetzes, mit dem sich die Karte für den Zugang zum Internet verbinden wird. Die Anzeige der Signalstärke sowie des Übertragungsmodus sind von der verwendeten Karte abhängig.

Die Anzeige der Signalstärke im LANmonitor leistet gute Dienste beim Testen der Empfangsqualität an Orten, an denen man die Datenkarte erstmals in Betrieb nehmen möchte. Ab einer Anzeige von drei Balken (grün) können Sie von einer ausreichenden Signalstärke für eine gute Datenübertragung ausgehen. Bei zwei Balken (gelb) ist eine ausreichende Qualität der Datenübertragung nicht mehr gewährleistet, bei nur einem Balken kommt normalerweise keine Datenübertragung mehr zustande.



⑧ Sobald die Verbindung zum Internet hergestellt wurde, zeigt der LANmonitor im Bereich der WAN-Verbindungen an, mit welchem Netz die Verbindung hergestellt wurde.



Der Zustand der UMTS-Verbindung wird ebenfalls über die UMTS-LEDs an der Fronseite des Gerätes mit verschiedenen Blink-Codes angezeigt.

8.2 VPN-Standort-Kopplung

Neben der Anbindung von einzelnen Arbeitsplatzrechnern an die Zentrale können über die UMTS/HSxPA-Schnittstelle auch vollständige Netzwerkkopplungen eingerichtet werden.

Für die Kopplung von zwei Netzwerken über ein UMTS-Interface wird zunächst beiden beteiligten VPN-Routern eine Netzwerkkopplung, z.B. mit dem Assistenten von LANconfig eingerichtet.

Bei der Konfiguration der Netzwerkkopplung über UMTS/HSxPA müssen folgende Aspekte berücksichtigt werden:

- Manche Mobilfunkanbieter weisen den UMTS-Karten bei der Einwahl eine IP-Adresse aus einem privaten Adresskreis zu. Für den normalen Internet-Zugang bedeutet das keine Einschränkung. Beim Aufbau von VPN-Verbindungen kann es jedoch zu Störungen kommen, weil je nach Einstellung der Verbindung die IP-Adressen der VPN-Gegenstellen zur Verhandlung der Verschlüsselungsparameter verwendet werden. Mit der Aktivierung des NAT-Traversal im VPN-Gateway der Zentrale können auch VPN-Verbindungen von Filialen mit privaten IP-Adressen aufgebaut werden.

Weitere Informationen zu diesem Thema finden Sie im LCOS-Referenzhandbuch.

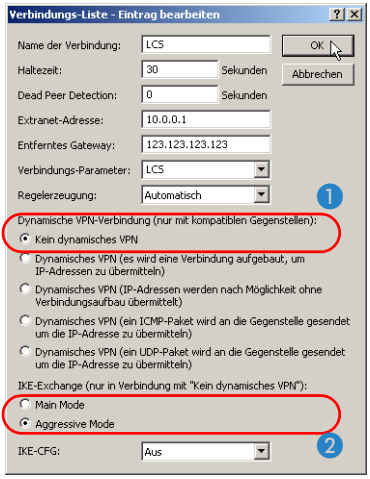
- Bei der Kopplung von Netzwerken über den Assistenten wird zunächst der sichere „Main Mode" für den Austausch der IKE-Schlüssel verwendet. In die Verhandlung des Main Mode fließt die IP-Adresse der VPN-Endpunkte

DE

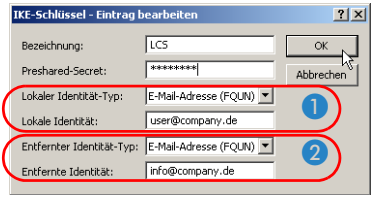
ein, was bei Zuweisung von privaten IP-Adressen an den LANCOM UMTS Router wieder zu Problemen führen kann.

Wenn bei der Verwendung des Main Mode keine VPN-Verbindung zustande kommt, stellen Sie das Verfahren in den entsprechenden Profilen auf beiden Seiten in der VPN-Verbindungsliste auf „Aggressive Mode“ um.

Wählen Sie dazu unter LANconfig im Konfigurationsbereich 'VPN' auf der Registerkarte 'Allgemein' in der 'Verbindungsliste' den Eintrag für die entsprechende Verbindung. Stellen Sie zunächst die Optionen für dynamisches VPN auf 'Kein dynamisches VPN' ein (1) und aktivieren Sie anschließend als IKE-Exchange-Modus den 'Aggressive Mode' (2).



Tragen Sie danach unter LANconfig im Konfigurationsbereich 'VPN' auf der Registerkarte 'IKE-Parameter' in der Liste der 'IKE-Schlüssel' für die entsprechende Verbindung **eindeutige** Identitäten ein (z.B. eindeutige E-Mail-Adressen).



Die Einstellungen für den Aggressive Mode mit den zu verwendenden Identitäten müssen auf beiden Seiten der Verbindung korrespondierend vorgenommen werden!

- Der UMTS/HSxPA-Karte wird beim Einbuchen in das Mobilfunknetz vom Provider eine dynamische IP-Adresse zugewiesen. Achten Sie auf die entsprechenden Einstellungen bei der Konfiguration mit dem Setup-Assistenten.
- Wenn der UMTS/HSxPA-Karte eine private IP-Adresse zugewiesen wurde und der LANCOM UMTS Router nicht z.B. über einen ISDN-Anruf identifiziert werden kann (Dynamic VPN), muss die VPN-Verbindung immer vom VPN-Gateway mit der UMTS/HSxPA-Karte in Richtung des VPN-Gateways in der Zentrale aufgebaut werden.
- Um die VPN-Verbindung mit dem Netzwerk der Zentrale dauerhaft verfügbar zu machen, stellen Sie sowohl die Haltezeit der Internetverbindung als auch die VPN-Haltezeit auf '9.999' ein (Keep Alive). Nur so wird auch der Zugriff aus der Zentrale auf die per UMTS/HSxPA angebundenen Netzwerke jederzeit möglich (z.B. bei der Anbindung von Filialen per UMTS/HSxPA an Standorten ohne breitbandigen Internetanschluss).
- Wenn die VPN-Verbindung durch ein Polling überwacht werden soll, müssen die Einstellungen für das Polling ebenfalls vom VPN-Gateway mit der UMTS/HSxPA-Karte ausgehen und auf das entfernte VPN-Gateway gerichtet sein. Je nach Qualität der Verbindung müssen dabei die Zeiten für die Pollingaufrufe angepasst werden.

Je nach Tarif können bei Always-On-Internetverbindung hohe Kosten entstehen, z.B. bei zeitbasierter Abrechnung. Bitte informieren Sie sich über die Details Ihres UMTS/HSxPA-Tarifs bei Ihrem Mobilfunk-Provider.

8.3 Weitere Einstellungen

8.3.1 Auswahl des Mobilfunknetzes

Solange sich eine Mobilfunkkarte im Bereich des eigenen Netzbetreibers befindet, ist sie normalerweise fest auf die Verwendung dieses Netzes gebunden – es ist keine freie Auswahl des Netzes möglich.

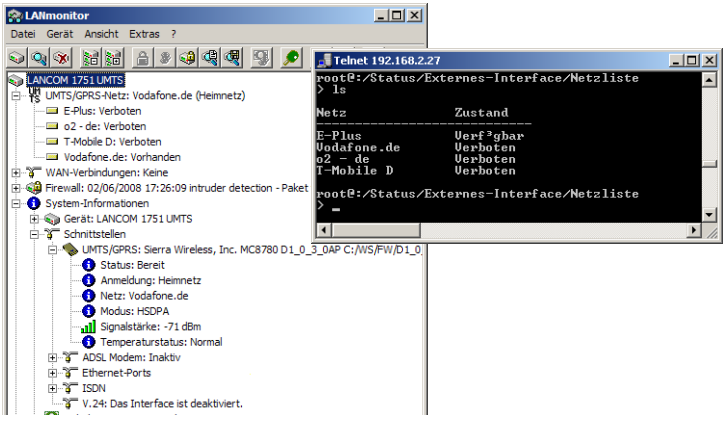
DE

Sobald sich die Karte jedoch außerhalb des eigenen „Heimnetzes“ befindet, stehen meistens mehrere Mobilfunknetze zur Auswahl, z.B. beim Betrieb im Ausland (Roaming). In diesem Fall kann der Anwender meistens aus allen angebotenen Netzen selbst ein Netz auswählen, über das er den Internetzugang herstellen möchte.

Stellen Sie die Netzwerkauswahl im entsprechenden UMTS/HSxPA/GPRS-Profil auf 'Manuell' ein. Als Netzwerk-Name geben Sie dann das gewünschte Mobilfunknetz so ein, wie es von der Datenkarte beim Scannen erkannt wurde.

Die Einstellungen für die UMTS/HSxPA/GPRS-Profile finden Sie im LANconfig im Konfigurationsbereich 'Interface' auf der Registerkarte 'WAN' unter der Schaltfläche **UMTS/GPRS-Profile**.

Den Namen der Netze können Sie im LANmonitor ablesen oder z.B. über Telnet unter `/Status/Externes-Interface/Netzliste` einsehen. Über die Befehle `do /Status/Externes-Interface/Netzsuche` oder `do Setup/Schnittstellen/UMTS-GPRS-Parameter/Netzsuche` können Sie die Netzsuche manuell anstossen.

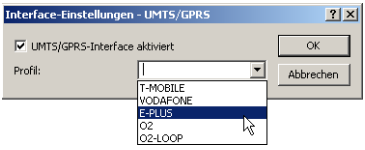


DE

8.3.2 UMTS/GPRS- Profil aktivieren

Beim Betrieb der LANCOM- Geräte mit UMTS/HSxPA- Funktion in wechselnden Umgebungen oder mit wechselnden UMTS/HSxPA/GPRS- Datenkarten sind ggf. unterschiedliche Einstellungen erforderlich. Die für den Betrieb der Datenkarten relevanten Informationen sind in einem UMTS/HSxPA/GPRS- Profil zusammengefasst. Über die Interface- Einstellungen für die UMTS/HSxPA- Schnittstelle können die Profile sehr schnell gewechselt werden.

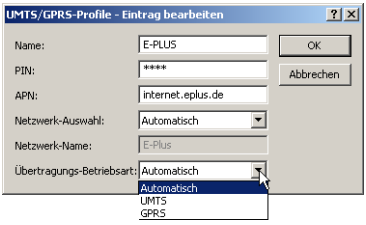
Die Aktivierung der UMTS/HSxPA- Schnittstelle und die Auswahl der Profile finden Sie im LANconfig im Konfigurationsbereich 'Interfaces' auf der Registerkarte 'WAN' unter der Schaltfläche **Interface- Einstellungen**.



8.3.3 Nur UMTS/HSxPA oder automatische UMTS/HSxPA/GPRS- Auswahl

In manchen Gebieten ist die Netzabdeckung der UMTS/HSxPA- Anbieter noch nicht vollständig abgeschlossen. Um in den Gebieten mit nicht ausreichendem UMTS/HSxPA- Empfang dennoch eine Datenverbindung aufbauen zu können, wird in der Regel die Übertragungsbetriebsart 'Automatisch' gewählt. In dieser Einstellung wählt die Datenkarte im LANCOM bevorzugt die Verbindung über UMTS/HSxPA. Nur wenn das UMTS- Signal so schwach ist, dass eine Datenübertragung in der erforderlichen Qualität nicht möglich ist, schaltet die Karte automatisch auf das GPRS- Netz um.

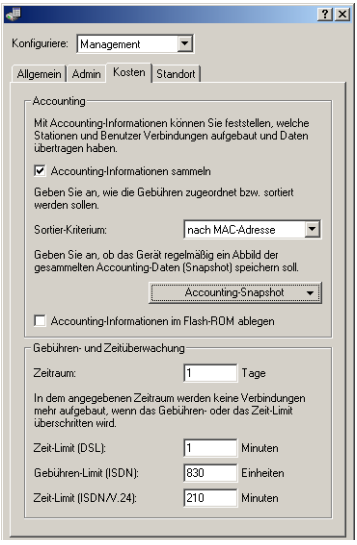
Bei Bedarf kann die Betriebsart jedoch auch fest auf UMTS/HSxPA oder GPRS eingestellt werden. Stellen Sie dazu im entsprechenden UMTS/HSxPA/GPRS- Profil in LANconfig im Konfigurationsbereich 'Interface' auf der Registerkarte 'WAN' unter der Schaltfläche **UMTS/HSxPA/GPRS- Profile** die gewünschte Betriebsart ein.



DE

8.3.4 Zeitlimit einrichten

Zum Schutz vor unerwarteten Kosten können Sie auch für die Verbindungen über die UMTS/HSxPA-Schnittstelle ein Zeitlimit einrichten, z.B. unter LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Kosten'.



9 Rat & Hilfe

In diesem Kapitel finden Sie Ratschläge und Hilfestellungen für die erste Hilfe bei einigen typischen Problemen.

9.1 Es wird keine DSL-Verbindung aufgebaut

Nach dem Start versucht der Router automatisch, Kontakt zum DSL-Anbieter aufzunehmen. Im Erfolgsfall wechselt diese LED dann auf dauerhaftes Grün. In der Regel ist eine der folgenden Ursachen:

Probleme an der Verkabelung?

Verwenden Sie für den DSL-Anschluss ausschließlich das mitgelieferte Anschlusskabel. Dieses Kabel muss mit dem Ethernet-Ausgang des DSL-Modems verbunden sein.

Stimmt das gewählte Übertragungsprotokoll?

Das Übertragungsprotokoll wird bei der Grundeinstellung gesetzt. Dabei setzt der Grundeinstellungs-Assistent für zahlreiche DSL-Anbieter selbstständig das korrekte Übertragungsprotokoll. Nur wenn Ihr DSL-Anbieter dem Assistenten unbekannt ist, müssen Sie das verwendete Protokoll selber angeben. In jedem Fall sollte das Protokoll funktionieren, das Ihnen Ihr DSL-Anbieter angibt.

Die Protokoll-Einstellung kontrollieren und korrigieren Sie unter:

Konfigurationstool	Aufruf
LANconfig	Kommunikation ▶ allgemein ▶ Kommunikations-Layer
WEBconfig	Expertenkonfiguration ▶ Setup ▶ WAN-Modul ▶ Layer-Liste

9.2 DSL-Übertragung langsam

Die Übertragungsgeschwindigkeit einer (Internet-) DSL-Verbindung hängt von zahlreichen Faktoren ab, von denen die meisten außerhalb des eigenen Einflussbereiches liegen: Entscheidend sind neben der Bandbreite der eigenen Internet-Anbindung beispielsweise auch die Internet-Anbindung und Auslastung des angesprochenen Ziels. Außerdem können zahlreiche Faktoren im Internet die Übertragungsleistung beeinflussen.

DE

Vergrößerung der TCP/IP-Windows-Size unter Windows

Wenn die tatsächliche Übertragungsleistung einer DSL-Verbindung deutlich unter den vom DSL-Anbieter angegebenen Maximalwerten liegt, gibt es außer diesen externen Einflussfaktoren nur wenige mögliche Fehlerquellen an den eigenen Geräten.

Ein übliches Problem tritt auf, wenn an einem Windows-PC über eine asynchrone Verbindung gleichzeitig große Datenmengen geladen und gesendet werden. In diesem Fall kann es zu einer starken Beeinträchtigung der Download-Geschwindigkeit kommen. Verantwortlich ist die sogenannte TCP/IP-Receive-Windows-Size im Windows-Betriebssystem, die standardmäßig auf einen für asynchrone Verbindungen zu kleinen Wert gesetzt ist.

Eine Anleitung zur Vergrößerung der Windows-Size finden Sie in der Wissensdatenbank im Support-Bereich der LANCOM Systems-Website (www.lancom.de).

9.3 Unerwünschte Verbindungen mit Windows XP

Windows-XP-Rechner versuchen beim Start, die eigene Uhrzeit mit einem Zeitserver im Internet abzugleichen. Deshalb kommt es beim Start eines Windows-XP-Rechners im WLAN zum Verbindungsaufbau des LANCOM mit dem Internet.

Zur Abhilfe schaltet man an den Windows-XP-Rechnern die automatische Zeitsynchronisation unter **Rechter Mausklick auf die Uhrzeit ▶ Datum ▶ Uhrzeit ändern ▶ Internetzeit** aus.

10 Anhang

10.1 Leistungs- und Kenndaten

		LANCOM 1751 UMTS
Anschlüsse	ETH1 bis ETH4	10/100Base-TX, Autosensing
	WAN bzw. ADSL	ADSL over ISDN nach ITU G.992.1 Annex B (kompatibel zum U-R2-Anschluss der Deutschen Telekom) oder ADSL over POTS nach ITU G.992.1 Annex A ADSL2+ over ISDN nach ITU G.992.3, ITU G.992.5 Annex B (ADSL2+) oder ADSL2+ over POTS nach ITU G.992.3 und ITU G.992.5 Annex A (ADSL2+)
	GSM/UMTS	UMTS-, HSxPA- GPRS- oder Edge mit intergriertem UMTS-Modem
	ISDN	ISDN-S_0-Bus
	Serielle Schnittstelle / COM Port	Serielle Konfigurationsschnittstelle / COM-Port (8-pol. Mini-DIN): 9.600-115.000 Baud
Stromversorgung		12V DC über externes Netzteil. Zulässiges Netzteil: ■ NEST 12V/1A DC/S Hohlstkr 2.1/5.5mm (RoHS) LANCOM Art.-Nr. 110524 Typenbezeichnung auf dem Netzteil „Type: 15.2230S“
Gehäuse		Abmessungen 210 mm x 143 mm x 45 mm (B x H x T), robustes Kunststoffgehäuse, stapelbar, für Wandmontage vorbereitet
Normen		CE-konform nach EN 60950
Zulassungen		Notifiziert in den Ländern Deutschland, Belgien, Niederlande, Luxemburg, Österreich, Schweiz, Großbritannien, Italien, Spanien, Frankreich, Portugal
FCC		Die Geräte mit der Artikelnummer 61626 (LANCOM 1751 UMTS FCC) entsprechen zusätzlich auch den Bedingungen der FCC. FCC-Kennzeichnungstext: Dieses Gerät entspricht dem Teil 15 der FCC-Regeln. Der Betrieb ist an die beiden folgenden Bedingungen geknüpft: 1) Dieses Gerät darf keine schädlichen Störungen verursachen 2) Dieses Gerät muss alle empfangenen Störungen tolerieren, inklusive solcher Störungen, die unerwünschtes Verhalten verursachen könnten. ■ FCC ID: N7NMC8781 ■ US: X1UDSNANLC1751
Umgebung/Temperatur		Temperaturbereich 5–35°C im Dauerbetrieb; Luftfeuchtigkeit 0–80 %; nicht kondensierend
Service		Garantie 3 Jahre

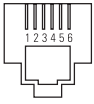
DE

		LANCOM 1751 UMTS
Support		Über Hotline und Internet
Zubehör		■ LANCOM Rack Mount Option (Art.-Nr. 61501) ■ LANCOM LCOS Referenzhandbuch (DE) (Art.-Nr. 61700) ■ LANCOM Advanced VPN Client für Windows® 2000, Windows® XP, Windows Vista™, 1er Lizenz, Art.-Nr. 61600 ■ LANCOM Advanced VPN Client für Windows® 2000, Windows® XP, Windows Vista™, 10er Lizenz, Art.-Nr. 61601 ■ LANCOM Advanced VPN Client für Windows® 2000, Windows® XP, Windows Vista™, 25er Lizenz, Art.-Nr. 61602
Optionen		■ LANCOM VPN-25 Option (25 Kanäle, inkl. Aktivierung VPN Hardware-Beschleuniger), Art.-Nr. 60083 ■ LANCOM Service Option (24h-Vorabaustausch innerhalb Deutschlands, 4 Jahre Garantie, nicht für PoE Power Injector), Art.-Nr. 61401

10.2 Anschlussbelegung

10.2.1 ADSL-Schnittstelle

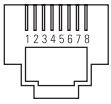
6-polige RJ11-Buchse

Steckverbindung	Pin	IAE
	1	–
	2	–
	3	a
	4	b
	5	–
	6	–

DE

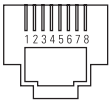
10.2.2 ISDN-S_0-Schnittstelle

8-polige RJ45-Buchse, entsprechend ISO 8877, EN 60603-7

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

10.2.3 Ethernet-Schnittstellen 10/100Base-T

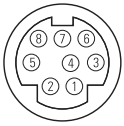
8-polige RJ45-Buchsen, entsprechend ISO 8877, EN 60603-7

Steckverbindung	Pin	Leitung
	1	T+
	2	T-
	3	R+
	4	–
	5	–
	6	R-
	7	–
	8	–

DE

10.2.4 Konfigurationsschnittstelle (Outband)

8-polige Mini-DIN-Buchse

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

10.3 CE-Konformitätserklärungen

CE Hiermit erklärt LANCOM Systems, dass sich die in dieser Dokumentation beschriebenen Geräte in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet.

Die CE-Konformitätserklärungen für Ihr Gerät finden Sie im jeweiligen Produktbereich der LANCOM-Website (www.lancom.de).

Index

DE