LANCOM 3850 UMTS

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom.de

Würselen, September 2007

110536/0907

DE

Ein Wort vorab

Vielen Dank für Ihr Vertrauen!

Die Verbindung aus UMTS/HSDPA, WLAN, DSL und VPN eröffnet völlig neue Möglichkeiten der Anbindung von Unternehmen – beispielsweise für mobile Konferenzräume, die mittels UMTS/HSDPA-Anbindung einen WLAN-Zugang zum Internet oder – in Verbindung mit VPN – einen Zugang zum Firmennetz bereitstellen.

Als Backupverbindung bei Standortkopplungen ist UMTS/HSDPA preiswerter und schneller als das üblicherweise dafür genutzte ISDN. Zudem ist es deutlich ausfallsicherer, da es ohne Kabel auch nicht durch Bauarbeiten gefährdet ist. Die Nutzung von VRRP im LANCOM 3850 UMTS bietet – auch herstellerübergreifend – höchste Verfügbarkeiten und vollkommen transparente sowie automatisierte Medienwechsel im Backupfall.

UMTS/HSDPA ist darüber hinaus als „Last-Mile"-Zugangstechnologie für Kunden geeignet, die nicht über eine äquivalente Breitbandanbindung verfügen. Die UMTS/HSDPA-Karte wird einfach im Cardbus-Erweiterungsslot des LANCOM 3850 UMTS betrieben. Die Umschaltung des Internetzugangs zwischen HSDPA, UMTS und GPRS erfolgt vollautomatisch je nach Verfügbarkeit.

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)
- Funknetzwerke (WLAN)
- Backup-Lösungen
- 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

1.1 Was ist ein Funk-LAN?

Die folgenden Abschnitte beschreiben allgemein die Funktionalität von Funknetzwerken. Welche Funktionen von Ihrem Gerät unterstützt werden, können Sie der weiter unten stehenden Tabelle 'Was kann Ihr LANCOM' entnehmen. Weitere Informationen zu diesem Thema finden Sie im Referenzhandbuch.

Ein Funk-LAN verbindet einzelne Endgeräte (PCs und mobile Rechner) zu einem lokalen Netzwerk (auch LAN – **L**ocal **A**rea **N**etwork). Im Unterschied zu einem herkömmlichen LAN findet die Kommunikation nicht über Netzwerkkabel, sondern über Funkverbindungen statt. Aus diesem Grund nennt man ein Funk-LAN auch **W**ireless **L**ocal **A**rea **N**etwork (WLAN).

In einem Funk-LAN stehen alle Funktionen eines kabelgebundenen Netzwerks zur Verfügung: Zugriff auf Dateien, Server, Drucker etc. ist ebenso möglich wie die Einbindung der einzelnen Stationen in ein firmeninternes Mailsystem oder der Zugang zum Internet.

Die Vorteile von Funk-LANs liegen auf der Hand: Notebooks und PCs können dort aufgestellt werden, wo es sinnvoll ist – Probleme mit fehlenden Anschlüssen oder baulichen Veränderungen gehören bei der drahtlosen Vernetzung der Vergangenheit an.

Funk-LANs sind außerdem einsetzbar für Verbindungen über größere Distanzen. Teure Mietleitungen und die damit verbundenen baulichen Maßnahmen können gespart werden.

1.1.1 Welche Hardware ist notwendig?

Jedes Endgerät im Funk-LAN benötigt einen Zugang zum Funk-LAN in Form einer Funk-Schnittstelle. Geräte, die nicht serienmäßig über eine Funk-Schnittstelle verfügen, können mit einer Erweiterungskarte oder einem Adapter nachgerüstet werden.

LANCOM Systems bietet Funkadapter in der Produktreihe AirLancer an. Mit einem AirLancer-Funkadapter rüsten Sie ein Endgerät (z. B. PC oder Notebook) für den Zugang zum Funk-LAN auf.

1.1.2 Betriebsarten von Funk-LANs und Access Points

Die Funk-LAN-Technologie und die Access Points in Funk-LANs werden in folgenden Betriebsarten eingesetzt:

- Einfache, direkte Verbindung zwischen Endgeräten ohne Access Point (Ad-hoc-Modus)
- Größere Funk-LANs, evtl. Anschluss an LAN mit einem oder mehreren Access Points (Infrastruktur-Netzwerk)
- Durchleiten von VPN-verschlüsselten Verbindungen mit VPN Pass-Through
- Schaffung eines Zugangs zum Internet
- Verbinden zweier LANs über eine Funkstrecke (Point-to-Point-Modus)
- Anbindung von Geräten mit Ethernet-Schnittstelle über einen Access Point (Client-Modus)
- Erweitern eines bestehenden Ethernet-Netzwerks um WLAN (Bridge-Modus)
- Relaisfunktion zur Verbindung von Netzwerken über mehrere Access Points
- Zentrale Verwaltung durch einen LANCOM WLAN Controller

1.2 Die Vorteile der UMTS/HSDPA-Lösung

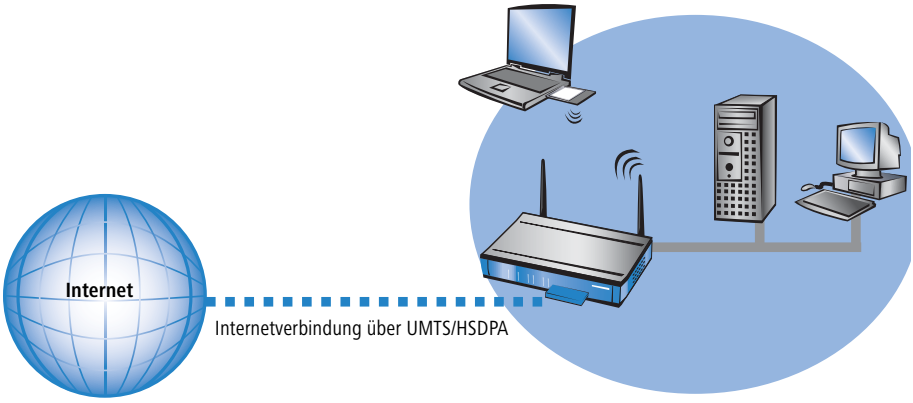
Die Verbindung aus UMTS/HSDPA, WLAN, DSL und VPN eröffnet völlig neue Möglichkeiten der Anbindung von Unternehmen: beispielsweise für mobile Konferenzräume, die mittels UMTS/HSDPA-Anbindung einen WLAN-Zugang zum Internet oder – in Verbindung mit VPN – einen Zugang zum Firmennetz bereitstellen. Als Backupverbindung bei Standortkopplungen ist UMTS/HSDPA preiswerter und/oder schneller als die üblicherweise dafür genutzten ISDN- oder Analogverbindungen. Zudem ist es deutlich ausfallsicherer, da es ohne Kabel auch nicht durch Bauarbeiten ausfallen kann. UMTS/HSDPA ist darüber hinaus als „Last-Mile"-Zugangstechnologie für Kunden geeignet, die nicht über eine äquivalente Breitbandanbindung verfügen.

Die UMTS/HSDPA-Karte wird einfach im Cardbus-Erweiterungsslot der entsprechenden LANCOM-Geräte betrieben. Die Umschaltung des Internetzugangs zwischen UMTS/HSDPA und GPRS erfolgt vollautomatisch je nach Verfügbarkeit.

DE

1.2.1 „Last Mile" via UMTS/HSDPA

Die Internetanbindung über UMTS/HSDPA bietet sich überall da an, wo kein breitbandiger Internetzugang angeboten wird. Mit dem UMTS/HSDPA-Internetzugang erreichen Sie wesentlich höhere Datenraten als mit einem ISDN-Anschluss.



Für den dauerhaften Internetzugang über UMTS/HSDPA bieten verschiedene Netzbetreiber einen so genannten „Homezone"-Tarif an. Dabei wird der Datenverkehr der UMTS/HSDPA-Karte in der „Homezone" – also in **der** Funkzelle, in der die UMTS/HSDPA-Karte üblicherweise eingebucht ist – deutlich günstiger abgerechnet als in einem normalen mobilen Tarif, bei dem die Datenkarte in wechselnden Funkzellen betrieben wird.

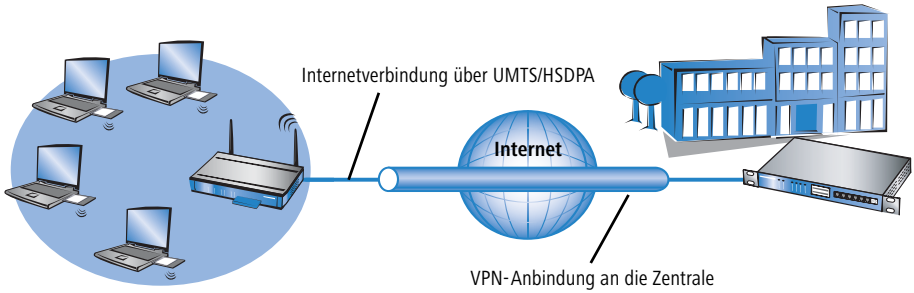
Als besondere Anwendung kann ein WLAN Access Point mit UMTS/HSDPA-Anbindung und LANCOM Public Spot Option als HotSpot an Orten ohne kabelgebundenen Internetzugang eingesetzt werden.

1.2.2 Mobiler Konferenzraum

Die moderne Arbeitswelt erfordert von immer mehr Mitarbeitern eine erhöhte Mobilität. Auf der anderen Seite wird die ständige Anbindung an E-Mail, Internet oder die Server in der Zentrale immer wichtiger.

Ein WLAN Access Point mit UMTS/HSDPA-Anbindung verschafft die nötige Flexibilität überall da, wo einzelne Mitarbeiter oder auch ganze Gruppen häufig an wechselnden Orten eingesetzt werden. Da fast alle modernen Notebooks heute über eine WLAN-Schnittstelle verfügen, fehlt zum mobilen

Internet- oder VPN-Zugang nur eine ebenso mobile WAN-Schnittstelle. Mit der drahtlosen Internetanbindung über UMTS/HSDPA oder GPRS können sehr komfortabel mobile Arbeitsräume eingerichtet werden, die den passenden Internetzugang einfach nur „in die Steckdose" stecken müssen.

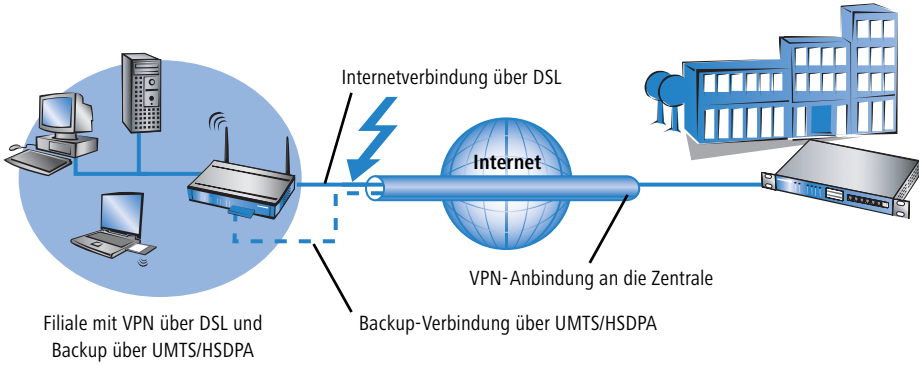


Mobiles WLAN, z.B. für einen „mobilen Konferenzraum".

Für eine Gruppe von Mitarbeitern, die z.B. häufig gemeinsam an Projekten bei Kunden arbeitet, wird so ein mobiler Konferenzraum eingerichtet. Der Access Point wird dabei vom Administrator einmal konfiguriert, die Mitarbeiter vor Ort müssen das Gerät nur mit Strom versorgen und die Datenkarte einstecken. Bei geeigneter Konfiguration stellt der Router dann automatisch eine Verbindung ins Internet her und alle erreichbaren Notebooks, in deren WLAN-Konfiguration eine passende Passphrase eingetragen ist, können sofort auf das Internet zugreifen. Sofern im Router eine VPN-Verbindung zur Zentrale konfiguriert ist, können die Aussendienstmitarbeiter aus dem mobilen Büro über die UMTS/HSDPA-Verbindung auch direkt auf alle Dienste im Netzwerk der Zentrale zugreifen (Fileserver, Mailserver, Datenbanken etc.).

1.2.3 UMTS/HSDPA Backup

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

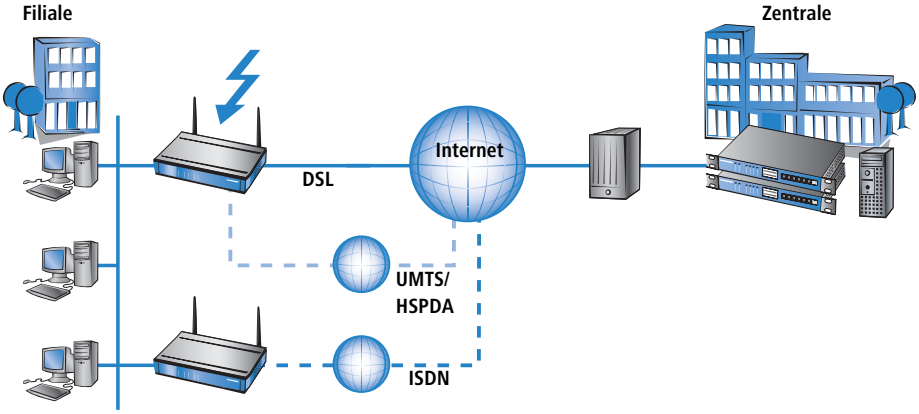


Als Alternative zu diesem ISDN/Analog-Backup-Verfahren kann auch eine UMTS/HSDPA-Verbindung die Verfügbarkeit der Datenverbindungen sicherstellen. Wenn die Anbindung an das Internet über einen UMTS/HSDPA-fähigen Router erfolgt, kann die UMTS/HSDPA-Verbindung sofort einspringen, wenn die DSL-Leitung gestört ist. Die Vorteile der UMTS/HSDPA-Backup-Lösung gegenüber der ISDN/Analog-Variante:

- Schneller als ISDN/Analog: Der Datendurchsatz liegt bei UMTS/HSDPA wesentlich höher.
- Sicherer als ISDN oder Analog: Wenn eine physikalische Beschädigung der DSL-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 UMTS/HSDPA liegen je nach Tarif deutlich unter den Gebühren für einen ISDN-Anschluss. Da die tatsächlichen Ausfallzeiten der DSL-Verbindung üblicherweise nur wenige Stunden im Jahr betragen, sind die ggf. höheren Verbindungskosten für UMTS/HSDPA oft nicht relevant.

Ein besonders ausgefeiltes Backup-System zum Schutz vor Hardware-Ausfällen der Router kann mit dem Virtual Router Redundncy Protocol (VRRP) realisiert werden. Dabei werden in einem Netzwerk zwei oder mehrere Router 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/HSPDA-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/HSPDA-Interface des Gerätes kann aber einen weiteren Platz in der Backup-Kette einnehmen, wenn auch der Backup-Router gestört ist.



Weitere Informationen zur Konfiguration von Backup-Lösungen finden Sie im LCOS-Referenzhandbuch.

1.3 Was kann Ihr LANCOM Wireless Router?

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

	LANCOM 3850 UMTS
Anwendungen	
Internet-Zugang	✔
IP-Router mit Stateful Inspection Firewall	✔
DHCP- und DNS-Server (für LAN und WAN)	✔
VPN-Gateway	✔
UMTS/HSPDA-Funktion zur Internetanbindung, als mobiler Konferenzraum oder als Backup-Lösung	✔
LAN-LAN-Kopplung über VPN	✔
RAS-Server (über VPN)	✔

DE

	LANCOM 3850 UMTS
WLAN	
Funkübertragung nach IEEE 802.11g / IEEE 802.11b, oder Funkübertragung nach IEEE 802.11a	✔
Dualbandbetrieb mit zusätzlicher Funkkarte möglich	✔
Point-to-Point-Funktion (pro WLAN-Schnittstelle sechs P2P-Strecken definierbar)	✔
Relais-Funktion zur Verbindung zweier P2P-Strecken untereinander (mit zweiter Funkkarte)	✔
Turbo Modus: Bandbreitenverdopplung im 2,4 GHz- und 5 GHz-Bereich	✔
Super AG inkl. Hardware-Compression und Bursting	✔
Multi SSID	✔
Roaming-Funktion	✔
802.11i / WPA mit Hardware-AES - Verschlüsselung	✔
WEP-Verschlüsselung (bis 128 Bit Schlüssellänge, WEP152)	✔
IEEE 802.1x/EAP	✔
MAC-Adressfilter (ACL)	✔
Individuelle Passphrases pro MAC-Adresse (LEPS)	✔
Closed-Network-Funktion	✔
Integrierter RADIUS-Server	✔
VLAN	✔
Intra-Cell-Blocking	✔
QoS für WLAN (IEEE 802.11e, WMM/WME)	✔
WLANmonitor zur Visualisierung von Access Points und Client in großen WLANs	✔
WLAN-Gruppenkonfiguration zur komfortablen Konfiguration mehrerer Geräte	✔
LAN-Anschluss	
Fast-Ethernet-Anschluss (10/100Base-TX)	✔
Power-over-Ethernet (PoE)	✔
DHCP- und DNS-Server	✔

	LANCOM 3850 UMTS
WAN-Anschluss	
WAN-Anschluss für DSL-/Kabelmodem	✔
UMTS/HSPDA-Anschluss über UMTS-Karte im Cardbus-Slot	✔
USB-Anschluss	
USB 2.0 Host Port (Fullspeed: 12 Mbit/s) zum Anschluss eines USB-Druckers und für zukünftige Erweiterungen	✔
Internet-Zugang (IP-Router)	
Stateful-Inspection Firewall	✔
Firewall-Filter (Adresse, Port)	✔
IP-Masquerading (NAT, PAT)	✔
Quality of Service	✔
Digitale Zertifikate (X.509) inkl. PKCS#12	✔
Advanced Routing and Forwarding (ARF-Netze)	8
N:N-Mapping zum Routen von Netzwerken mit den gleichen IP-Adresskreisen über VPN	✔
Policy-based Routing zur regelbasierten Auswahl der Zielroute	✔
Load-Balancing zur Bündelung von mehreren DSL-Kanälen	2 Kanäle
Backup-Lösungen und Load-Balancing mit VRRP	✔
PPPoE-Server	✔
WAN-RIP	✔
Rapid-Spanning-Tree-Protokoll	✔
Layer-2-QoS-Tagging	✔
802.1p	✔
NAT Traversal (NAT-T)	✔
DMZ mit konfigurierbarer IDS-Prüfung	✔
Stromversorgung	
12 V über separates Netzteil (DC)	✔
Power-over-Ethernet (PoE) nach IEEE 802.3af-Standard	✔

DE

	LANCOM 3850 UMTS
Konfiguration und Firmware	
Konfiguration mit LANconfig oder mit Webbrowser, zusätzlich Terminalmodus für Telnet oder andere Terminalprogramme, SNMP-Schnittstelle und TFTP-Serverfunktion, SSH-Zugang.	✔
Konfigurationsassistenten	✔
1-Click-VPN-Assistenten zur besonders komfotablen Einrichtung von RAS-Zugängen und LAN-Kopplungen über VPN	✔
Serielle Konfigurations-Schnittstelle	✔
FirmSafe zum Einspielen neuer Firmwareversionen ohne Risiko.	✔
Optionale Software-Erweiterungen	
LANCOM Public Spot Option	✔
LANCOM VPN Option mit 25 aktiven Tunneln zur Absicherung von Netzwerkkopplungen inkl. Aktivierung des Hardware-Beschleunigers	✔
LANCOM Service-Option	✔
Optionale Hardware-Erweiterungen	
AirLancer Extender Antennen zur Reichweitenerhöhung	✔
AirLancer MC-54 PC-Card zur Erweiterung auf eine zweite Funkzelle (Dual-Band)	✔
LANCOM ES-1108P PoE-Switch zur Ethernet-Verkabelung; gleichzeitig zur Spannungsversorgung über Ethernet	✔
Blitzschutzadapter SA-5 und SA-LAN	✔

2 Installation

2.1 Lieferumfang

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

	LANCOM 3850 UMTS
12 V DC Steckernetzteil	✔
Anschraubbare externe Dualband-Antennen mit Reverse SMA-Anschluss	2
PoE-LAN-Kabel (grüne Stecker)	✔
DSL-Anschlusskabel (dunkelblaue Stecker)	✔
Anschlusskabel für die Konfigurationsschnittstelle	✔
Abdeckung für den Cardbus-Slot	✔
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

2.2.1 Konfiguration der LANCOM-Geräte

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.
- Zugang zum LAN über das TCP/IP-Protokoll.

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

2.2.2 Betrieb der Access Points im Managed-Modus

LANCOM Wireless Router und LANCOM Access Points können entweder als autarke Access Points mit eigener Konfiguration betrieben werden („Access Point-Modus") oder als Teilnehmer in einer WLAN-Infrastruktur, die von einem zentralen WLAN Controller gesteuert wird („Managed-Modus").

Für den Betrieb im Managed-Modus benötigen die Access Points eine Firmware der Version 7.22 oder höher und einen aktuellen Loader (Version 1.86 oder höher).

2.3 Statusanzeigen, Schnittstellen und Installation der Hardware

2.3.1 Statusanzeigen

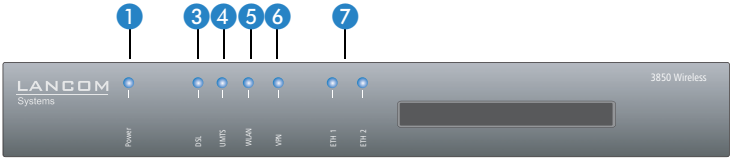
Bedeutung der LEDs

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

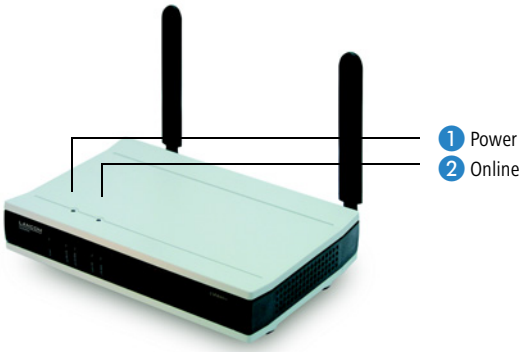
Die LANCOM Wireless Router verfügen über Statusanzeigen auf der Vorderseite.



DE

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

DE

orange/grün	Im Gehäusedeckel blinkend im Wechsel mit der Online-LED	Mindestens ein WLAN-Modul befindet sich im Managed-Modus und hat noch keinen WLAN Controller gefunden. Das bzw. die entsprechenden WLAN-Module sind ausgeschaltet, bis sie einen WLAN-Controller gefunden haben, von dem sie eine Konfiguration beziehen können bzw. bis sie manuell auf eine andere Betriebsart umgestellt werden.
orange/rot	Im Gehäusedeckel blinkend im Wechsel mit der Online-LED	Mindestens ein WLAN-Modul befindet sich im Managed-Modus und hat einen WLAN Controller gefunden. Der WLAN Controller kann dem WLAN-Modul jedoch keine Konfiguration zuweisen, da Firmware- und/oder Loader-Version des Geräts nicht mit dem WLAN Controller kompatibel sind.
rot	blinkend	Zeitlimit für Online-Verbindungen erreicht

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'.

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**.

DE

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
orange/ grün	Im Gehäuse-deckel blinkend im Wechsel mit der Power-LED	Mindestens ein WLAN-Modul befindet sich im Managed-Modus und hat noch keinen WLAN-Controller gefunden. Das bzw. die entsprechenden WLAN-Module sind ausgeschaltet, bis sie einen WLAN-Controller gefunden haben, von dem sie eine Konfiguration beziehen können bzw. bis sie manuell auf eine andere Betriebsart umgestellt werden.
orange/ rot	Im Gehäuse-deckel blinkend im Wechsel mit der Power-LED	Mindestens ein WLAN-Modul befindet sich im Managed-Modus und hat einen WLAN Controller gefunden. Der WLAN Controller kann dem WLAN-Modul jedoch keine Konfigura-tion zuweisen, da Firmware- und/oder Loader-Version des Geräts nicht mit dem WLAN Controller kompatibel sind.

3 DSL

Verbindungszustand für DSLoL:

aus		Keine DSL-Verbindung
grün	blinkend	Aufbau der ersten Verbindung
grün	blitzend	Aufbau einer weiteren Verbindung
grün	dauerhaft	mindestens eine logische Verbindung aufgebaut
grün	blinkend/blitzend	Datenverkehr (Versand oder Empfang)

4 UMTS

Verbindungszustand für UMTS:

aus		Keine UMTS-Verbindung
orange	blitzend	Einbuchung in das UMTS-Netz läuft
orange	dauerhaft an	Einbuchung in das UMTS-Netz erfolgreich
grün	blinkend	Aufbau der ersten Verbindung
grün	blitzend	Aufbau einer weiteren Verbindung
grün	dauerhaft	mindestens eine logische Verbindung aufgebaut

grün	blinkend/blitzend	Datenverkehr (Versand oder Empfang)
rot	flackernd	CRC-Fehler
rot/ orange	blinkend	Hardwarefehler

DE

5 WLAN

Gibt Informationen über die WLAN-Verbindungen der internen WLAN-Module aus. Die WLAN-Anzeige kann folgende Zustände annehmen:

aus		Kein WLAN-Netz definiert oder WLAN-Modul deaktiviert. Es werden keine Beacons vom WLAN-Modul gesendet.
grün	dauerhaft an	Mindestens ein WLAN-Netz definiert und WLAN-Modul aktiviert. Es werden Beacons vom WLAN-Modul gesendet.
grün	invers blitzend	Anzahl der Blitzer = Anzahl der verbundenen WLAN-Stationen und P2P-Funkstrecken, danach folgt eine Pause (Default). Alternativ kann die Frequenz der Blitzer die Eingangsempfindlichkeit anzeigen.
grün	blinkend	DFS Scanning oder anderer Scan-Vorgang.
grün	blitzend	WLAN-Modul ausgeschaltet wegen Unterschreitung der Betriebstemperatur.
rot	flackern	Fehler im WLAN (TX-Fehler, z.B. Sendefehler aufgrund schlechter Verbindung)
rot	blinkend	Hardwarefehler im WLAN-Modul

6 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

7 ETH

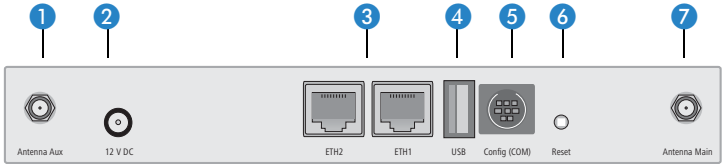
Zustand der LAN-Anschlüsse im integrierten Switch:

aus		kein Netzwerkgerät angeschlossen

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

2.4 Die Rückseite des Geräts

Auf der Rückseite befinden sich Anschlüsse und Schalter der LANCOM Wireless Router:



1. Anschluss für Diversity-Antenne.
2. Anschluss für das mitgelieferte Netzteil.
3. Switch mit 10/100Base-Tx-Anschlüssen

   Die LAN-Anschlüsse unterstützen den Power-over-Ethernet-Standard (PoE). Nähere Informationen zum Betrieb mit PoE finden Sie in der Info-Box 'Power-over-Ethernet – elegante Stromversorgung über die LAN-Verkabelung'.
4. USB-Anschluss (USB Host)
5. Serielle Konfigurationsschnittstelle (RS 232/V.24)
6. Reset-Taster

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

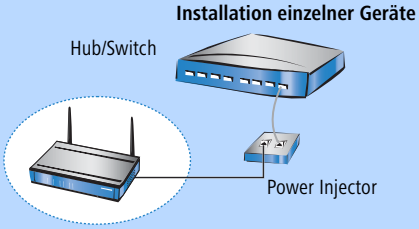
DE

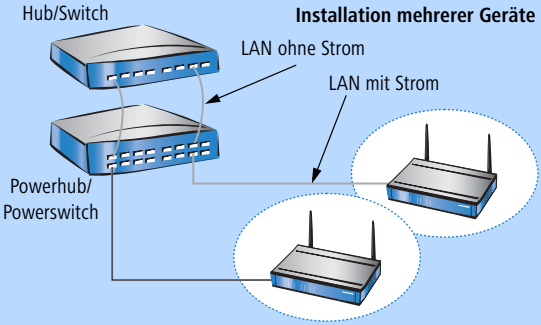
Power-over-Ethernet – elegante Stromversorgung über die LAN-Verkabelung

LANCOM Wireless Router sind für das PoE-Verfahren (Power-over-Ethernet) vorbereitet und entsprechen dem 802.3af-Standard. PoE-fähige Netzwerkgeräte können elegant über die LAN-Verkabelung mit Strom versorgt werden. Dadurch entfällt die Notwendigkeit eines eigenen Stromanschlusses für jede Basis-Station, wodurch der Installationsaufwand erheblich reduziert wird.

Die Stromeinspeisung in das LAN geschieht an zentraler Stelle, etwa über einen PoE-Injector oder einen Powerhub/Powerswitch. Bei der LAN-Verkabelung ist zu beachten, dass alle 8 Adern in den Kabeln durchgeführt werden. PoE speist den Strom über jene vier Adern ein, die normalerweise nicht für die Datenübertragung genutzt werden.

Die PoE-Versorgung funktioniert nur in solchen Netzwerksegmenten, in denen ausschließlich PoE-fähige Geräte betrieben werden. Der Schutz von Netzwerkgeräten ohne PoE-Unterstützung wird über einen intelligenten Mechanismus gewährleistet, der vor Einschalten der PoE-Stromversorgung das Netzwerksegment auf Geräte ohne PoE-Unterstützung untersucht. Die Spannung wird nur dann auf das LAN geschaltet, wenn sich dort ausschließlich Geräte mit PoE-Unterstützung befinden.





Verwenden Sie in einer PoE-Installation ausschließlich Geräte, die dem 802.3af-Standard entsprechen! Für Schäden, die durch unzulässige Geräte verursacht werden, besteht kein Gewährleistungsanspruch.

Beim LANCOM 3850 UMTS können zwei LAN-Buchsen zur redundanten Stromversorgung genutzt werden. Das Gerät wählt selbständig aus, welche Stromquelle genutzt wird. Wenn durch einen Ausfall der gerade aktiven Stromquelle eine andere Stromquelle die Stromversorgung des Gerätes übernimmt, bootet das Gerät ggf. neu, um die Stromspeisung neu zu aktivieren.

- **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 für zum Neustart, ein Druck von 5 Sekunden oder länger führt zum Neustart mit dem Rücksetzen der Konfiguration auf den Auslieferungszustand. Alle LEDs am Gerät leuchten dauerhaft auf. Sobald der Taster freigegeben wird, startet das Gerät mit Werkseinstellungen neu.

Bei einem harten Reset startet das Gerät mit Werkseinstellungen neu, alle bisherigen Einstellungen gehen dabei verloren!

Beachten Sie, dass bei einem Reset auch die im Gerät definierten WLAN-Verschlüsselungseinstellungen verloren gehen und auf den Standard-WEP-Schlüssel zurückgesetzt werden.

7 Anschluss für Hauptantenne (an diesem Anschluß werden ggf. AirLancer Extender Zusatzantennen angeschlossen).

2.5 Installation der Hardware

Die Installation der LANCOM Wireless Router erfolgt in folgenden Schritten:

① **Antennen** – Schrauben Sie die mitgelieferten Antennen auf der Rückseite des Access Points an.

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

Ein gleichzeitiger Betrieb des internen WLAN-Moduls und einer externen WLAN-Karte im Cardbus-Slot (z.b. AirLancer) im gleichen Frequenzband kann zur Beeinträchtigung der Übertragungsqualität führen, wenn dabei die direkt anschraubbaren Reverse-SMA-Antennen genutzt werden. An mindestens einem Funkmodul sollte in dem Fall eine externe Antenne genutzt werden.

② **LAN** – Sie können den Access Point zunächst an Ihr LAN anschließen. Stecken Sie dazu das mitgelieferte Netzwerkkabel (grüne Stecker) in einen LAN-Anschluss des Geräts 4 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 **DSLoL** – Wenn Sie den Access Point im DSLoL-Modus betreiben möchten, können Sie das Gerät entweder direkt an das DSL-Modem anschliessen (Exklusiv-Modus) oder über einen Hub bzw. Switch im kabelgebundenen LAN (Automatik-Modus).

- Stecken Sie im Exklusiv-Modus das mitgelieferte Netzwerkkabel (grüne Stecker) in den LAN-Anschluss des Geräts 4 und andererseits in die entsprechende Schnittstelle des DSL-Modems.
- Stecken Sie im Automatik-Modus zum gleichzeitigen LAN und DSLoL-Betrieb das mitgelieferte Netzwerkkabel (grüne Stecker) in den LAN-Anschluss des Geräts 4 und andererseits in eine freie Netzwerkanschlussdose Ihres lokalen Netzes (bzw. in eine freie Buchse eines Hubs/Switchs).

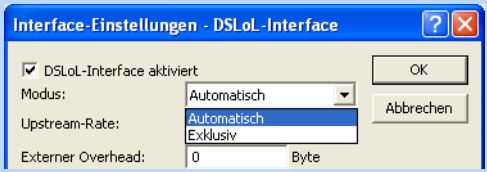
Informationen zur Nutzung einer LAN-Schnittstelle für DSLoL finden Sie in der Info-Box 'LAN-Schnittstelle: exklusiv oder parallel für DSLoL nutzen'.

④ **Mit Spannung versorgen** – versorgen Sie das Gerät an Buchse 2 über das mitgelieferte Netzteil mit Spannung.

DE

LAN-Schnittstelle: exklusiv oder parallel für DSLoL nutzen

Prinzipiell haben Sie zwei Möglichkeiten, den Access Point für den DSLoL-Betrieb zu nutzen. Den exklusiven Modus nutzen Sie, wenn Sie das Gerät direkt an das DSL-Modem anschliessen. Den automatischen Modus verwenden Sie, wenn Sie es an einen Hub oder Switch eines kabelgebundenen LANs anschliessen und diesen Hub wiederum mit dem DSL-Modem verbinden. Wenn der Access Point über DHCP als Gateway bekannt gemacht wird, können Rechner aus LAN und WLAN **gleichzeitig** über eine physikalische Schnittstelle den Internetzugang nutzen. Den gewünschten Modus stellen Sie im LANconfig bei den Interface-Einstellungen der DSLoL-Schnitt-stelle ein.



DSLoL unterstützt alle PPPoE-basierte Internetzugänge (z.B. T-DSL), sowie Internetzugänge, die über einen Router mit statischen IP-Adressen realisiert sind (z.B. CompanyConnect oder diverse SDSL-Geschäftskundenanschlüsse).

Verwenden Sie ausschließlich das mitgelieferte Netzteil! Die Verwendung eines ungeeigneten Netzteils kann zu Personen- oder Sachschäden führen.

Alternativ können Sie auf die PoE-Möglichkeiten zur Stromversorgung nutzen (siehe auch 'Power-over-Ethernet – elegante Stromversorgung über die LAN-Verkabelung').

Beim LANCOM 3850 UMTS können zwei LAN-Buchsen zur redundanten Stromversorgung genutzt werden. Das Gerät wählt selbständig aus, welche Stromquelle genutzt wird. Wenn durch einen Ausfall der gerade aktiven Stromquelle eine andere Stromquelle die Stromversorgung des Gerätes übernimmt, bootet das Gerät ggf. neu, um die Stromspeisung neu zu aktivieren.

⑤ **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.

DE

2.6

2.7 Installation der Software

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

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

2.7.1 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:

2.7.2 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 **WLANmonitor** erlaubt die Beobachtung und Überwachung der WLAN-Netze. Die mit den Access Points verbundenen Clients werden angezeigt, auch nicht authentifizierte Access Points und Clients können angezeigt werden (Rogue AP Detection und Rogue Client Detection).
- 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 den WLAN Controller einwandfrei funktioniert.

3.1 Welche Angaben sind notwendig?

Der Grundkonfigurations-Assistent nimmt die TCP/IP-Grundeinstellung des WLAN Controllers 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 Funk-LAN
- 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 WLAN Controller angeschlossen
- Neuaufbau eines Netzwerks

Wenn Sie den WLAN Controller 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 WLAN Controller erhält die IP-Adresse '172.23.56.254' (Netzmaske '255.255.255.0'). Außerdem wird der integrierte DHCP-Server aktiviert, so dass der WLAN Controller 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:

- **IP-Adresse und Netzwerkmaske für den WLAN Controller**
  Teilen Sie dem WLAN Controller eine freie IP-Adresse aus dem Adressbereich Ihres LAN zu, und geben Sie die Netzwerkmaske an.

3.1.2 Konfigurationsschutz

Mit dem Kennwort schützen Sie den Konfigurationszugang zum WLAN Controller 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 WLAN Controller können bis zu 16 verschiedene Administratoren eingerichtet werden. Weitere Informationen finden Sie im LCOS-Referenzhandbuch unter „Rechteverwaltung für verschiedene Administratoren".

Im Managed-Modus (siehe folgender Abschnitt) erhalten LANCOM Wireless Router und LANCOM Access Points automatisch das gleiche Root-Kennwort wie der WLAN Controller, wenn auf dem Gerät selbst noch kein Root-Kennwort gesetzt ist.

3.1.3 Einstellungen für das Funk-LAN

LANCOM Wireless Router und LANCOM Access Points können entweder als autarke Access Points mit eigener Konfiguration betrieben werden (WLAN-Module in der Betriebsart „Access Point-Modus") oder als Teilnehmer in einer WLAN-Infrastruktur, die von einem zentralen WLAN Controller gesteuert wird (Betriebsart „Managed-Modus").

Der Managed-Modus wird in den physikalischen WLAN-Einstellungen aktiviert. In dieser Betriebsart beziehen die WLAN-Module ihre Konfiguration vom WLAN Controller, die WLAN-Einstellungen in den LANCOM Wireless Router und LANCOM Access Points haben keine Auswirkungen.

Bei Geräten mit zwei WLAN-Modulen kann die Betriebsart für jedes Modul separat festgelegt werden, d.h. das eine WLAN-Modul kann im Managed-Modus, ein anderes z.B. als autarker Access Point betrieben werden.

Der Netzwerkname (SSID)

Der Grundkonfigurations-Assistent fragt nach dem Netzwerknamen des Access Points (häufig als SSID – **S**ervice **S**et **Id**entifier bezeichnet). Der Netzwerkname wird in den Access Point des Funk-LANs eingetragen. Der Name kann frei gewählt werden. Mehrere Access Points mit demselben Netzwerknamen bilden ein gemeinsames Funk-LAN.

Ab Werk ist für jeden unkonfigurierten LANCOM Wireless Router standardmäßig eine WEP128-Verschlüsselung aktiviert. Weitere Informationen finden Sie im LCOS-Referenzhandbuch unter „Standard-WEP-Verschlüsselung".

Offenes oder geschlossenes Funk-LAN?

Mobilfunkstationen wählen das gewünschte Funk-LAN durch Angabe des Netzwerknamens an. Erleichtert wird die Angabe des Netzwerknamens durch zwei Techniken:

- Mobilfunkstationen können die Umgebung nach Funk-LANs absuchen („scannen") und die gefundenen Funk-LANs in einer Liste zur Auswahl anbieten.
- Durch Verwendung des Netzwerknamens 'ANY' meldet sich die Mobilfunkstation im nächsten verfügbaren Funk-LAN an.

Um diese Vorgehensweise zu unterbinden kann das Funk-LAN „geschlossen" werden. In diesem Fall akzeptiert es keine Anmeldungen mit dem Netzwerknamen 'ANY'.

Standardmäßig sind LANCOM-Geräte unter dem Netzwerknamen 'LANCOM' ansprechbar. Die Grundkonfiguration eines Access Points über Funk erfolgt daher über diesen Netzwerknamen. Wird während der Grundkonfiguration ein anderer Netzwerkname gesetzt, so muss nach Abschluss der Grundkonfiguration der Funk-LAN-Zugang der konfigurierenden Mobilstation ebenfalls auf diesen neuen Netzwerknamen umgestellt werden.

DE

Auswahl eines Funkkanals

Der Access Point arbeitet in einem bestimmten Funkkanal. Der Funkkanal wird aus einer Liste von bis zu 13 Kanälen im 2,4 GHz Frequenzbereich, oder bis zu 19 Kanälen im 5 GHz Frequenzbereich ausgewählt (in verschiedenen Ländern sind einzelne Funkkanäle gesperrt, siehe Anhang).

Der verwendete Kanal und Frequenzbereich legt den Betrieb des gemeinsamen Funkstandards fest, wobei der 5 GHz Frequenzbereich dem IEEE 802.11a/h Standard entspricht und der 2,4 GHz Frequenzbereich den Betrieb im IEEE 802.11g und IEEE 802.11b Standard festlegt.

Wenn in Reichweite des Access Points keine weiteren Access Points arbeiten, so kann ein beliebiger Funkkanal eingestellt werden. Andernfalls müssen im 2,4 GHz-Band die Kanäle so gewählt werden, das sie sich möglichst nicht überdecken beziehungsweise möglichst weit auseinander liegen. Im 5 GHz-Band reicht normalerweise die automatische Einstellung, in welcher der Access Point über TPC (Transmission Power Control) und DFS (Dynamic Frequency Selection) selbst den besten Kanal einstellt.

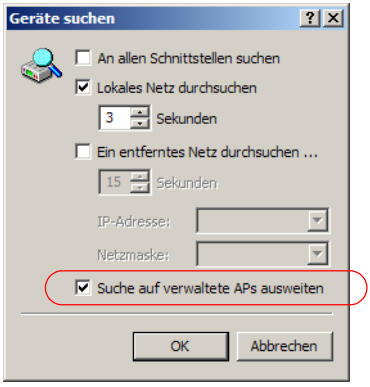
Weitere Informationen zu TPC und DFS finden Sie im LCOS-Referenzhandbuch.

3.2 Anleitung für LANconfig

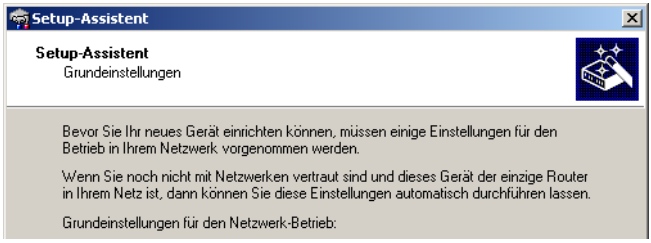
① Starten Sie LANconfig mit **Start** ▶ **Programme** ▶ **LANCOM** ▶ **LANconfig**. LANconfig erkennt neue LANCOM-Geräte im TCP/IP-Netz selbstständig.

② LANCOM Wireless Router und LANCOM Access Points im Managed-Modus werden standardmäßig bei der Suche mit LANconfig **nicht** ange-

zeigt. Zur Anzeige dieser Geräte aktivieren Sie bei der Suche die Option 'Suche auf verwaltete APs ausweiten'.



③ 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 Setup-Assistent nicht automatisch starten, so suchen Sie manuell nach neuen Geräten an allen Schnittstellen (falls der LANCOM Router über die serielle Konfigurationsschnittstelle angeschlossen ist) oder im Netzwerk (**Gerät ▶ Suchen**).

Sollte der Zugriff auf einen unkonfigurierten WLAN Controller 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.

④ Geben Sie dem LANCOM Router eine verfügbare Adresse aus einem geeigneten IP-Adressbereich. Bestätigen Sie mit **Weiter**.

⑤ 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.

⑥ Der Gebührenschutz beschränkt auf Wunsch die Kosten von WAN-Verbindungen auf ein festgesetztes Maß. Bestätigen Sie Ihre Angaben mit **Weiter**.

⑦ 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 WLAN Controller 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.

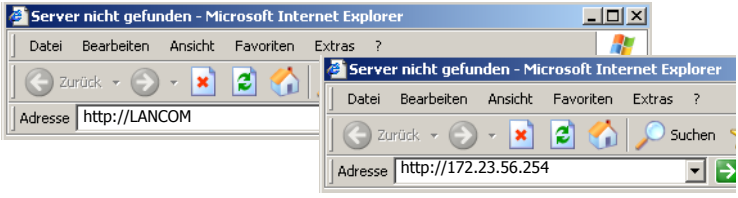
Wird ein LANCOM Wireless Router oder ein LANCOM Access Point von einem LANCOM WLAN Controller zentral verwaltet, dann wird beim

Zuweisen der WLAN-Konfiguration auch der DHCP-Server vom Auto-Modus in den Client-Modus umgeschaltet.

Netz ohne DHCP-Server

Nicht für zentral verwaltete LANCOM Wireless Router oder LANCOM Access Points

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).

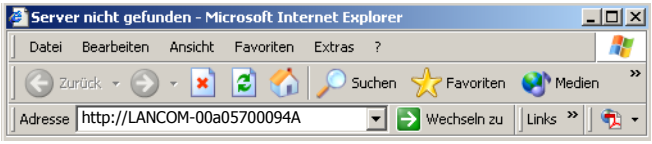
Netz mit DHCP-Server

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

DE

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.
  - Einen Rechner mit Terminalprogramm über die serielle Konfigurationsschnittstelle an das Gerät anschliessen.

Aufruf der Assistenten in WEBconfig

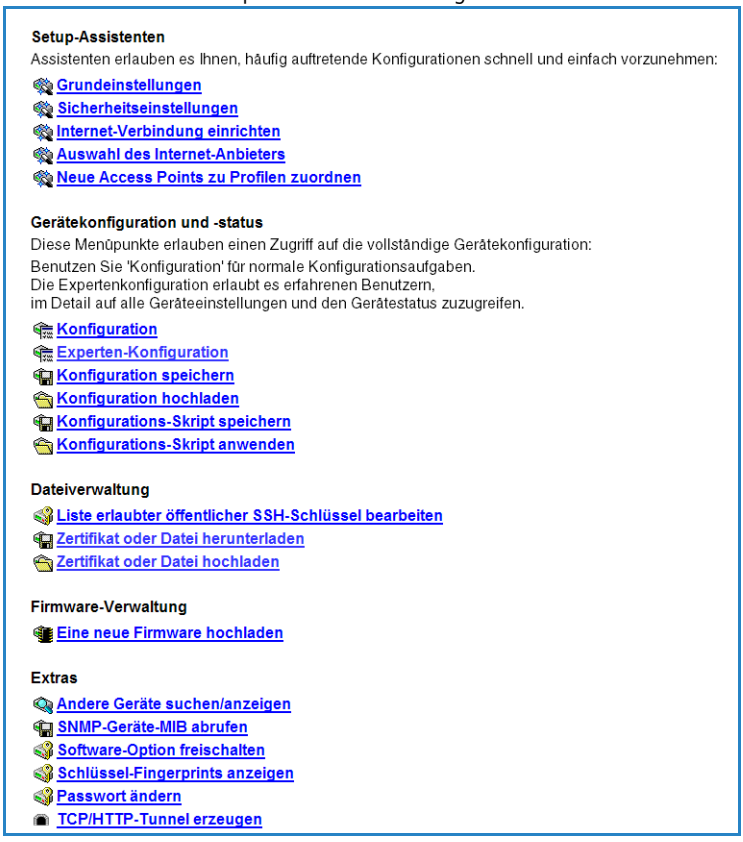
① Öffnen Sie also Ihren Web-Browser (z. B. Internet Explorer, Firefox, Opera) und rufen Sie dort den WLAN Controller auf:

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

(bzw. über beliebigen Namen)

Sollte der Zugriff auf einen unkonfigurierten WLAN Controller 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 LANCOM Router 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 Router 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**.

DE

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).

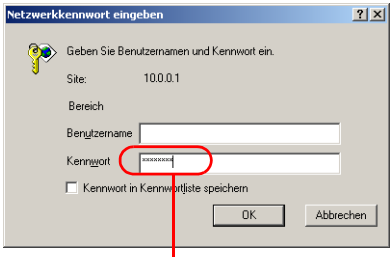
Legen Sie fest, ob das Gerät nur aus dem lokalen Netzwerk heraus konfiguriert werden darf, oder ob auch die Fernkonfiguration über das WAN (also aus einem entfernten Netzwerk) erlaubt ist.

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 WLAN Controller 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 den WLAN Controller**

  In dieser Betriebsart weist der WLAN Controller 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 LANCOM Router so zu hinterlegen, dass der DHCP-Server sie an die PCs im LAN als Standard-Gateway übermittelt. Außerdem sollte der DHCP-Server den LANCOM Router als DNS-Server angeben.

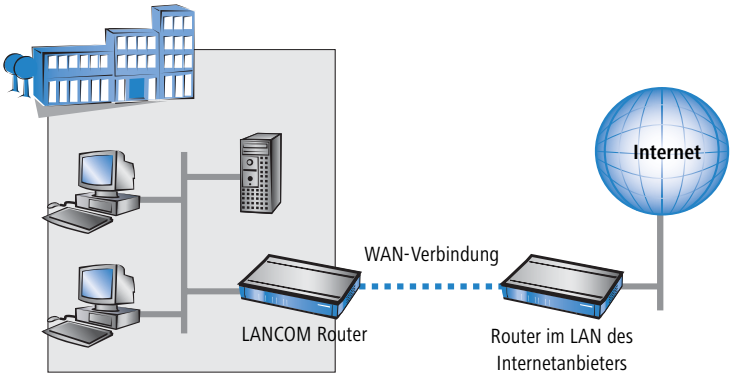
- **Manuelle Zuweisung der IP-Adressen**

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

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

4 Den Internet-Zugang einrichten

Über den zentralen Internet-Zugang des LANCOM erhalten alle Rechner im LAN Zugriff auf das Internet. Bei Modellen ohne WAN-Anschluss wird dazu eine LAN-Schnittstelle als DSLoL-Anschluss konfiguriert und mit einem geeigneten ADSL-Modem verbunden.



Kennt der Setup-Assistent Ihren Internet-Anbieter?

Die Einrichtung des Internet-Zugangs erfolgt über einen komfortablen Assistenten. Der Assistent kennt die Zugangsdaten der wichtigsten Internetanbieter 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 Router einstellen, dass bestehende Verbindungen automatisch abgebaut werden, wenn für eine bestimmte Dauer (die sogenannte Haltezeit) keine Daten mehr übertragen wurden.

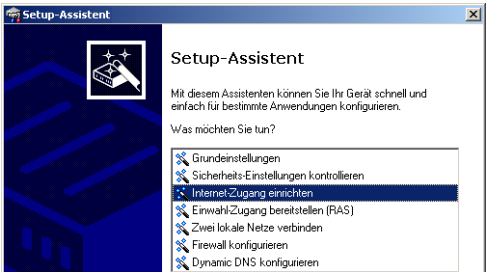
  Zusätzlich können Sie eine Leitungsüberwachung aktivieren, die inaktive Gegenstellen schneller erkennt und in diesem Fall die Verbindung schon vor Ablauf der Haltezeit abbaut.

- 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.

4.1 Anleitung für LANconfig

① Markieren Sie Ihr LANCOM 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**.

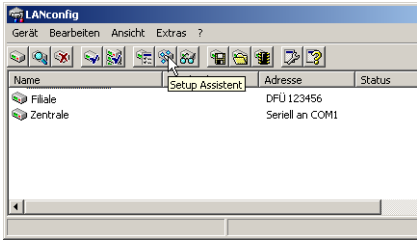
③ In den folgenden Fenstern wählen Sie Ihr Land, nach Möglichkeit Ihren Internetanbieter, und geben Sie die Zugangsdaten ein.

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

⑤ 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.



4.2 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.

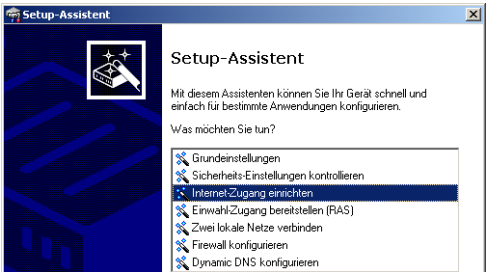
5 Einrichten der UMTS-Profile

5.1 Internetzugang

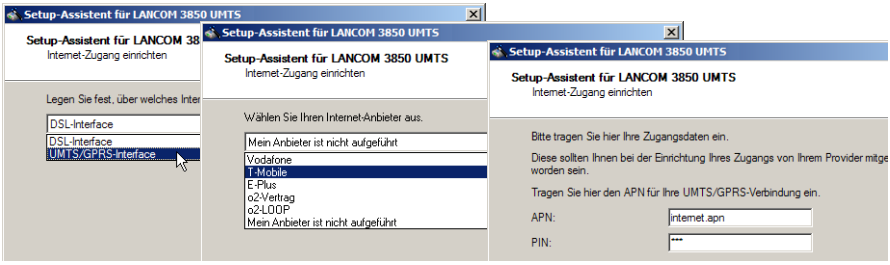
Das Einrichten des Internetzugangs über UMTS/HSDPA gelingt an schnellsten mit dem Internet-Assistenten von LANconfig.

DE

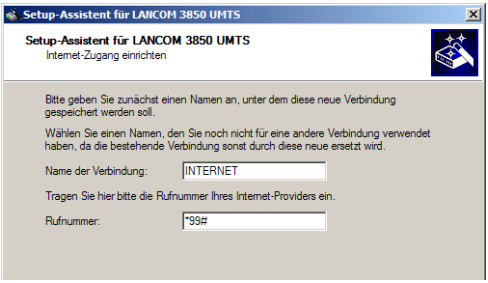
① Markieren Sie Ihren LANCOM Router im Auswahlfenster. Wählen Sie aus der Befehlsleiste den Punkt **Extras ▶ Setup Assistent**.



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.

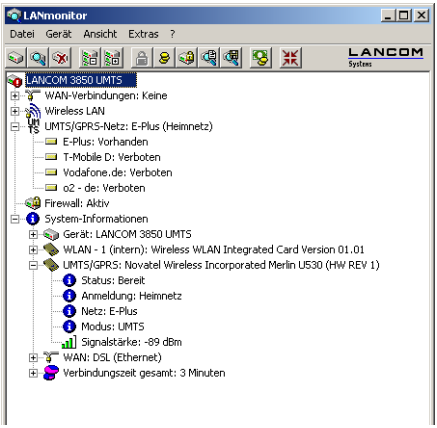
⑤ Zum Abschluss der Konfiguration des Internet-Zugangs können Sie für die UMTS/HSDPA-Verbindung die „Keep-Alive"-Option aktivieren. Damit wird die UMTS/HSDPA-Verbindung so eingerichtet, dass Sie nach dem Einschalten des Geräts automatisch aufgebaut wird und auch nach einer Trennung der Verbindung automatisch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

Mit dem Aktivieren der „Keep-Alive"-Funktion ermöglichen Sie z.B. sehr einfach die Einrichtung eines mobilen Konferenzraumes, der unabhängig vom Standort einen Internetzugang und ggf. den VPN-geschützten Zugang zum Netzwerk der Zentrale ermöglicht.

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/HSDPA-Tarifs bei Ihrem Mobilfunk-Provider.

⑥ Alternativ können Sie für die UMTS/HSDPA-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.

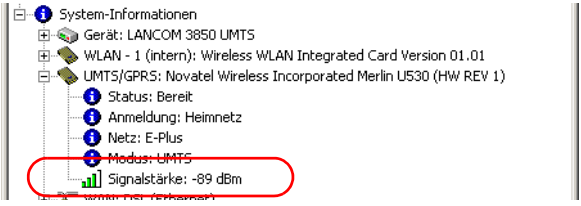
Im LANmonitor können Sie nach dem Einrichten des Internet-Zugangs prüfen, welche Mobilfunknetze verfügbar sind.



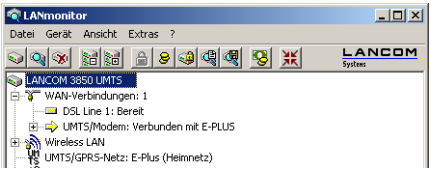
Auch ohne bestehende Verbindung sehen Sie im Bereich 'UMTS/GPRS-Netz' die gefundenen Netze. Darüber hinaus zeigt der LANmonitor hier an, welche Netze erlaubt sind und mit welchen Netzen sich die Karte nicht verbinden kann.

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.



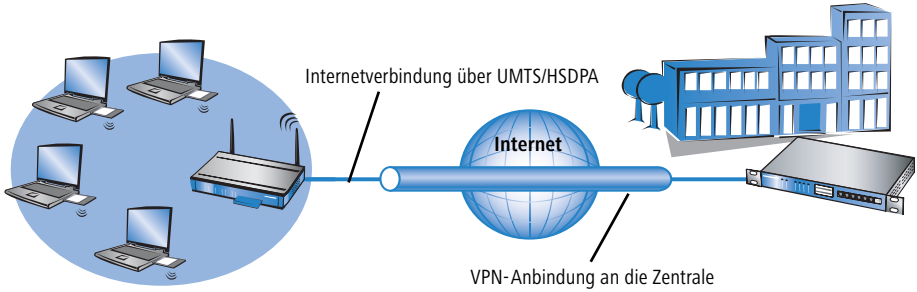
⑧ Sobald die Verbindung zum Internet hergestellt wurde, zeigt der LANmonitor im Bereich der WAN-Verbindungen an, mit welchem Netz die Verbindung hergestellt wurde.



Der Zustand der Datenkarte wird ebenfalls über die LEDs der Karte mit verschiedenen Blink-Codes angezeigt. Informieren Sie sich bitte in der Dokumentation zu Ihrer Datenkarte über die Bedeutung der LEDs.

5.2 VPN-Standort-Kopplung

Neben der Anbindung von einzelnen Arbeitsplatzrechnern an die Zentrale können über die UMTS/HSDPA-Schnittstelle auch vollständige Netzwerkkopplungen eingerichtet werden. Diese Variante kommt z.B. bei der Anbindung von „mobilen Konferenzräumen" zum Einsatz.



Mobiles WLAN, z.B. für einen „mobilen Konferenzraum".

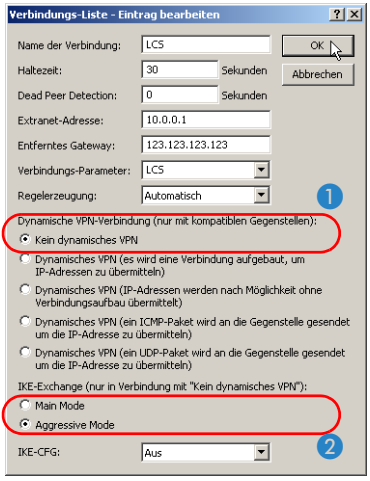
Für die Kopplung von zwei Netzwerken über ein UMTS-Interface wird zunächst beiden beteiligten VPN-Routern eine Netzwerkkopplung, z.B. mit dem Assistenten von LANconfig eingerichtet.

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

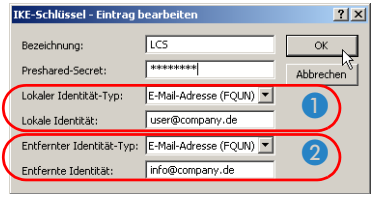
- Bei der Kopplung von Netzwerken über den Assistenten wird zunächst der sichere „Main Mode" für den Austausch der IKE-Schlüssel verwendet.

Einige Mobilfunkbetreiber unterstützen aber nur den „Aggressive Mode". 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!

DE

- Der UMTS/HSDPA-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.
- Da die UMTS/HSDPA-Karte eine dynamische IP-Adresse verfügt, aber nicht z.B. über einen ISDN-Anruf identifiziert werden kann (Dynamic VPN), muss die VPN-Verbindung immer vom VPN-Gateway mit der UMTS/HSDPA-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/HSDPA angebundenen Netzwerke jederzeit möglich (z.B. bei der Anbindung von Filialen per UMTS/HSDPA an Standorten ohne breitbandigen Internetanschluss).

  Für die Funktion des Keep Alive ist außerdem ein Eintrag in der Polling-Tabelle erforderlich. Erstellen Sie dazu unter LANconfig im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Gegenstellen' in der 'Polling-Tabelle' den Eintrag für die entsprechende Verbindung mit bis zu vier IP-Adressen im entfernten Netz und dem zugehörigen Ping-Interval sowie der Anzahl der Wiederholungen.
- Wenn die VPN-Verbindung durch ein Polling überwacht werden soll, müssen die Einstellungen für das Polling ebenfalls vom VPN-Gateway mit der UMTS/HSDPA-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/HSDPA-Tarifs bei Ihrem Mobilfunk-Provider.

5.3 Weitere Einstellungen

5.3.1 Auswahl des Mobilfunknetzes

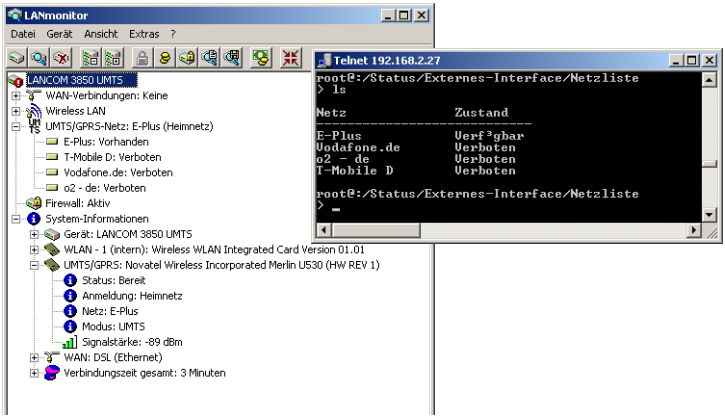
Solange sich eine Mobilfunkkarte im Bereich des eigenen Netzbetreibers befindet, ist sie normalerweise fest auf die Verwendung dieses Netzes gebunden – es ist keine freie Auswahl des Netzes möglich.

Sobald 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/HSDPA/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/HSDPA/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.

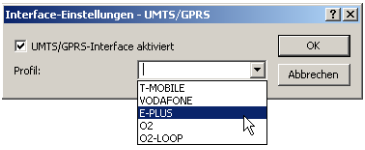


DE

5.3.2 UMTS/GPRS- Profil aktivieren

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

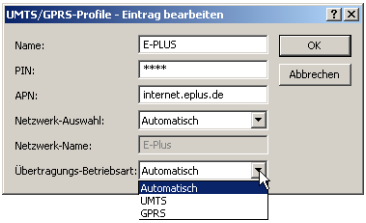
Die Aktivierung der UMTS/HSDPA- Schnittstelle und die Auswahl der Profile finden Sie im LANconfig im Konfigurationsbereich 'Interfaces' auf der Registerkarte 'WAN' unter der Schaltfläche **Interface- Einstellungen**.



5.3.3 Nur UMTS/HSDPA oder automatische UMTS/HSDPA/GPRS- Auswahl

In manchen Gebieten ist die Netzabdeckung der UMTS/HSDPA- Anbieter noch nicht vollständig abgeschlossen. Um in den Gebieten mit nicht ausreichendem UMTS/HSDPA- 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/HSDPA. Nur wenn das UMTS- Signal so schwach ist, das eine Datenübertragung in der erforderlichen Qualität nicht möglich ist, schaltet die Karte automatisch auf das GPRS- Netz um.

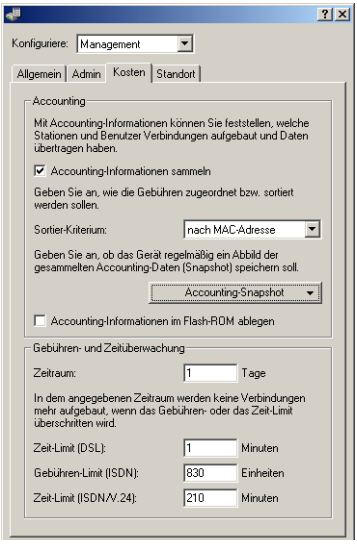
Bei Bedarf kann die Betriebsart jedoch auch fest auf UMTS/HSDPA oder GPRS eingestellt werden. Stellen Sie dazu im entsprechenden UMTS/HSDPA/GPRS- Profil in LANconfig im Konfigurationsbereich 'Interface' auf der Registerkarte 'WAN' unter der Schaltfläche **UMTS/HSDPA/GPRS- Profile** die gewünschte Betriebsart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



DE

5.3.4 Zeitlimit einrichten

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



DE

6 Punkt-zu-Punkt-Verbindungen

LANCOM Wireless Access Points können nicht nur als zentrale Station in einem Funknetzwerk arbeiten, sie können im Punkt-zu-Punkt-Betrieb auch Funkstrecken über größere Distanzen bilden. So können z. B. zwei Netzwerke über mehrere Kilometer hinweg sicher verbunden werden – ohne direkte Verkabelungen oder teure Standleitungen.

Das Verhalten eines Access Points beim Datenaustausch mit anderen Access Points wird in der „Punkt-zu-Punkt-Betriebsart" festegelegt:

- **Aus:** Der Access Point kann nur mit mobilen Clients kommunizieren
- **An:** Der Access Point kann mit anderen Basis-Stationen und mit mobilen Clients kommunizieren
- **Exklusiv:** Der Access Point kann nur mit anderen Basis-Stationen kommunizieren

Bei der automatischen Suche nach einem freien WLAN-Kanal kann es im 5 GHz-Band zu gleichzeitigen Sendeversuchen mehrerer Access Points kommen, die sich in der Folge gegenseitig nicht finden. Diese Pattsituationen kann mit dem geeigneten „Kanalwahlverfahren" verhindert werden:

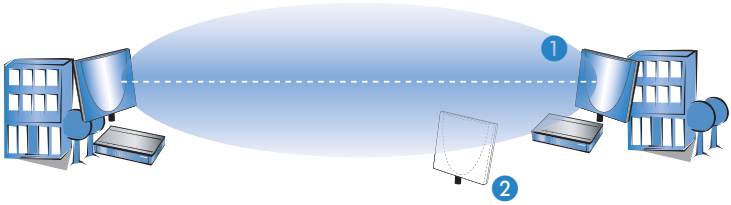
- **Master:** Dieser Access Point übernimmt die Führung bei der Auswahl eines freien WLAN-Kanals.
- **Slave:** Alle anderen Access Points suchen solange nach dem freien Kanal, bis sie einen sendenden Master gefunden haben.

Es ist daher empfehlenswert, im 5 GHz-Band jeweils einen zentralen Access Point als 'Master' und alle anderen Punkt-zu-Punkt-Partner als 'Slave' zu konfigurieren. Auch im 2,4 GHz-Band bei aktivierter automatischer Kanalsuche erleichtert diese Einstellung den Aufbau von Punkt-zu-Punkt-Verbindungen.

Für die Verschlüsselung von Punkt-zu-Punkt-Verbindungen mit 802.11i/WPA ist die korrekte Konfiguration der Kanalwahlverfahren zwingend erforderlich.

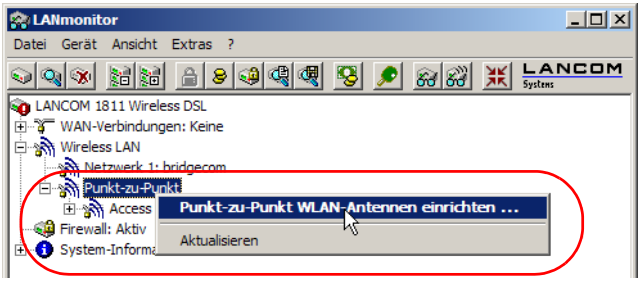
6.1 Ausrichten der Antennen für den P2P-Betrieb

Beim Aufbau von P2P-Strecken kommt der genauen Ausrichtung der Antennen eine große Bedeutung zu. Je besser die empfangende Antenne in der „Ideallinie" der sendenden Antenne liegt, desto besser ist die tatsächliche Leistung und damit die nutzbare Bandbreite (1). Liegt die empfangende Antenne jedoch deutlich neben dem idealen Bereich, sind deutliche Leistungsverluste zu erwarten (2).



Weitere Informationen zur geometrischen Auslegung von Funkstrecken und zur Ausrichtung der Antennen mit Hilfe der LANCOM-Software finden Sie im LCOS-Referenzhandbuch.

Um die Antennen möglichst gut ausrichten zu können, kann im LANmonitor die aktuelle Signalqualität von P2P-Verbindungen angezeigt werden. Die Anzeige der Verbindungsqualität kann über das Kontext-Menü im LANmonitor geöffnet werden. Ein Klick mit der rechten Maustaste auf den Eintrag 'Punkt-zu-Punkt' erlaubt den Aufruf 'Punkt-zu-Punkt WLAN-Antennen einrichten ...'



Der Eintrag 'Punkt-zu-Punkt' ist im LANmonitor nur sichtbar, wenn in dem überwachten Gerät mindestens eine Basisstation als Gegenstelle für eine P2P-Verbindung eingerichtet ist (LANconfig: **Wireless LAN ▶ Allgemein ▶ Physikalische WLAN-Einstellungen ▶ Punkt-zu-Punkt**).

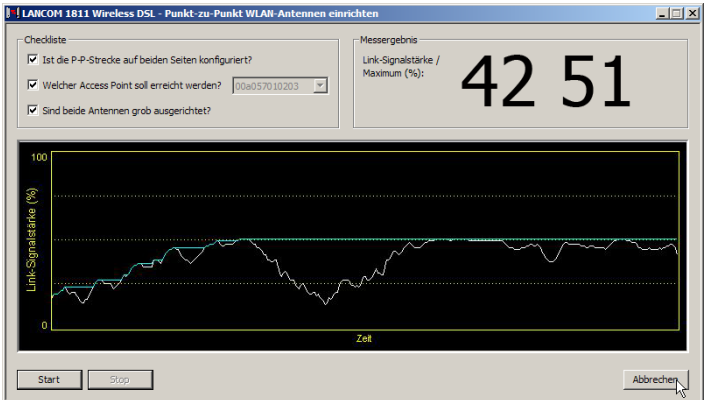
Im Dialog zur Einrichtung der Punkt-zu-Punkt-Verbindung fragt der LANmonitor die Voraussetzungen für den P2P-Verbindungsaufbau ab:

- Ist die P2P-Strecke auf beiden Seiten konfiguriert, ist also die jeweils gegenüberliegende Basisstation mit ihrer MAC-Adresse in der Konfiguration eingetragen, ist die Punkt-zu-Punkt-Betriebsart aktiviert?

DE

- Welcher Access Point soll überwacht werden? Hier können alle im jeweiligen Gerät als P2P-Gegenstelle eingetragenen Basis-Stationen ausgewählt werden.
- Sind beide Antennen grob ausgerichtet? Die Verbindung über die P2P-Strecke sollte schon grundsätzlich funktionieren, bevor die Einrichtung mit Hilfe des LANmonitor gestartet wird.

Der P2P-Dialog zeigt nach dem Start der Signalüberwachung jeweils die absoluten Werte für die aktuelle Signalstärke sowie den Maximalwert seit dem Start der Messung. Zusätzlich wird der zeitliche Verlauf mit dem Maximalwert in einem Diagramm angezeigt.



Bewegen Sie zunächst nur eine der beiden Antennen, bis sie den Maximalwert erreicht haben. Stellen Sie dann die erste Antenne fest und bewegen Sie auch die zweite Antenne in die Position, bei der Sie die höchste Signalqualität erzielen.

6.2 Konfiguration

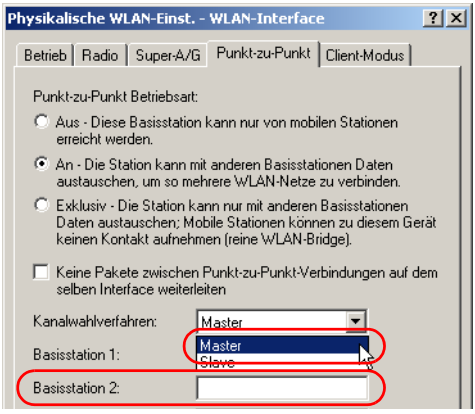
Bei der Konfiguration der Punkt-zu-Punkt-Verbindungen werden neben der Punkt-zu-Punkt-Betriebsart und dem Kanalwahlverfahren die MAC-Adressen der Gegenstellen eingetragen.

Konfiguration mit LANconfig

Bei der Konfiguration mit LANconfig finden Sie die Einstellungen für die P2P-Verbindungen im Konfigurationsbereich 'Interfaces' auf der Registerkarte 'Wireless LAN'.

① Öffnen Sie mit der Schaltfläche **Physikalische WLAN-Einst.** die Optionen für das entsprechende WLAN-Interface und wechseln Sie dort auf die Registerkarte 'Punkt-zu-Punkt'.

② Aktivieren Sie hier die geeignete Punkt-zu-Punkt-Betriebsart und stellen Sie als Kanalwahlverfahren entweder 'Master' oder 'Slave' ein. Tragen Sie dazu die jeweiligen MAC-Adressen der WLAN-Karte auf der Gegenseite ein (maximal 6).



Bitte beachten Sie, hier nur die MAC-Adressen der WLAN-Karten auf der anderen Seite der Verbindung einzutragen! Nicht die eigenen MAC-Adressen und nicht die MAC-Adressen von anderen Interfaces, die möglicherweise in den Basisstationen vorhanden sind.

Sie finden die WLAN-MAC-Adresse auf einem Aufkleber, der unterhalb des jeweileigen Antennenanschlusses angebracht ist. Verwenden Sie nur die als „WLAN-MAC" oder „MAC-ID" gekennzeichnete Zeichenkette. Bei den anderen ggf. angegebenen Adressen handelt es sich nicht um die WLAN-MAC-Adresse, sondern um die LAN-MAC-Adresse!

DE

Alternativ finden Sie die MAC-Adressen der WLAN-Karten in den Geräten unter WEBconfig oder Telnet bzw. Terminalprogramm auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ▶ Status ▶ WLAN-Statistik ▶ Interface-Statistiken
Terminal/Telnet	`Status/WLAN-Statistik/Interface-Statistiken`

Konfiguration mit WEBconfig oder Telnet

Unter WEBconfig oder Telnet finden Sie die Einstellungen für die Punkt-zu-Punkt-Verbindungen auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ▶ Setup ▶ Schnittstellen ▶ WLAN-Schnittstellen ▶ Interpoint-Einstellungen
Terminal/Telnet	`cd /Setup/Schnittstellen/WLAN-Schnittstellen/Interpoint-Einstellungen`

6.3 Access Points im Relais-Betrieb

Access Points mit zwei Funkmodulen können Funkbrücken über mehrere Stationen hinweg aufbauen. Dabei wird jeweils ein WLAN-Modul als 'Master', das zweite als 'Slave' konfiguriert.

Mit dem Einsatz von Relais-Stationen mit jeweils zwei WLAN-Modulen wird gleichzeitig das Problem der „hidden station“ gelöst, bei dem die MAC-Adressen der WLAN-Clients nicht über mehrere Stationen hinweg übertragen wird.

6.4 Sicherheit von Punkt-zu-Punkt-Verbindungen

Mit IEEE 802.11i kann auch die Sicherheit auf Punkt-zu-Punkt-Verbindungen im WLAN deutlich verbessert werden. Alle Vorteile von 802.11i wie die einfache Konfiguration und die starke Verschlüsselung mit AES stehen damit im P2P-Betrieb ebenso zur Verfügung wie die verbesserte Sicherheit der Passphrases durch LANCOM Enhanced Passphrase Security (LEPS).

6.4.1 Verschlüsselung mit 802.11i/WPA

Zum Aktivieren der 802.11i-Verschlüsselung auf einer korrekt konfigurierten P2P-Verbindung passen Sie die Einstellungen für das erste logische WLAN-

Netzwerk im verwendeten WLAN-Interface an (also WLAN-1, wenn Sie die erste WLAN-Karte für die P2P-Verbindung nutzen , WLAN-2 wenn Sie die zweite Karte z.B. bei einem Access Point mit zwei WLAN-Modulen nutzen).

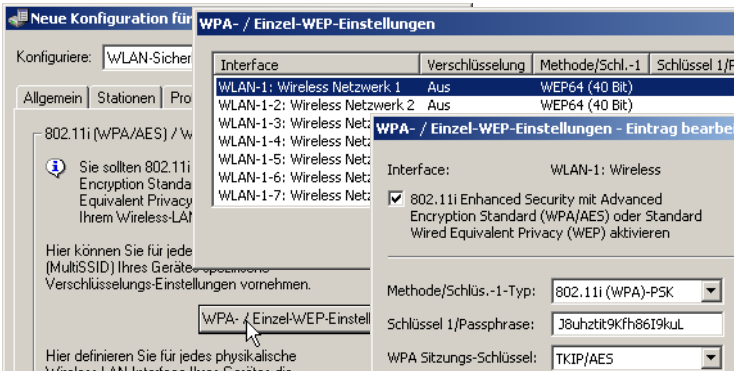
- Aktivieren Sie die 802.11i-Verschlüsselung.
- Wählen Sie als Methode '802.11i (WPA)-PSK' aus.
- Geben Sie die verwendete Passphrase ein.

Verwenden Sie als Passphrase zufällige Zeichenketten von mindestens 22 Zeichen Länge, was einer kryptographischen Stärke von 128 Bit entspricht.

In der Einstellung als P2P-Master wird die hier eingetragene Passphrase verwendet, um die Zugangsberechtigung der Slaves zu prüfen. In der Einstellung als P2P-Slave überträgt der Access Point diese Informationen an die Gegenseite, um sich dort anzumelden.

Konfiguration mit LANconfig

Bei der Konfiguration mit LANconfig finden Sie die Verschlüsselungs-Einstellungen im Konfigurationsbereich 'WLAN-Sicherheit' auf der Registerkarte '802.11i/WEP'.



Konfiguration mit WEBconfig oder Telnet

Die Verschlüsselungs-Einstellungen für die einzelnen logischen WLAN-Netzwerke finden Sie unter WEBconfig oder Telnet auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ▶ Setup ▶ Schnittstellen ▶ WLAN-Schnittstellen ▶ Verschluesselungs-Einstellungen
Terminal/Telnet	`/Setup/Schnittstellen/WLAN-Schnittstellen/Verschluesselungs-Einstellungen`

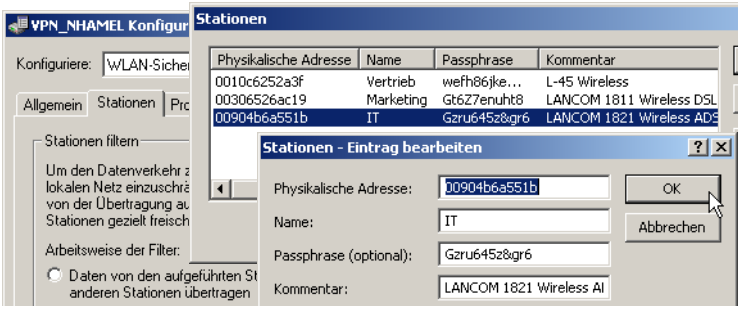
DE

6.4.2 LEPS für P2P-Verbindungen

Einen weiteren Sicherheitsgewinn erzielen Sie durch die zusätzliche Verwendung der LANCOM Enhanced Passphrase Security (LEPS), also der Verknüpfung der MAC-Adresse mit der Passphrase.

Mit LEPS können einzelne Punkt-zu-Punkt-Strecken (P2P) mit einer individuellen Passphrase abgesichert werden. Wenn bei einer P2P-Installation ein Access Point entwendet wird und dadurch Passphrase und MAC-Adresse bekannt werden, sind alle anderen per LEPS abgesicherten WLAN-Strecken weiterhin sicher, insbesondere wenn die ACL auf einem RADIUS-Server abgelegt ist.

Bei der Konfiguration mit LANconfig geben Sie die Passphrases der im WLAN zugelassenen Stationen (MAC-Adressen) im Konfigurationsbereich 'WLAN-Sicherheit' auf der Registerkarte 'Stationen' unter der Schaltfläche **Stationen** ein.



Konfiguration mit WEBconfig oder Telnet

Die Zugangs-Liste für die Zuordnung der MAC-Adressen zu den Passphrases (LEPS) finden Sie unter WEBconfig oder Telnet auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ▶ Setup ▶ WLAN-Modul ▶ Zugangs-Liste
Terminal/Telnet	`Setup/WLAN-Modul/Zugangs-Liste`

7 Sicherheits-Einstellungen

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

7.1 Sicherheit im Funk-LAN

Bei der Betrachtung von Funk-LANs entstehen oft erhebliche Sicherheitsbedenken. Vielfach wird angenommen, ein Datenmissbrauch der über Funk übertragenen Daten sei verhältnismäßig einfach.

Funk-LAN-Geräte von LANCOM Systems erlauben den Einsatz moderner Sicherungstechnologien:

- SSID Broadcast unterdrücken – geschlossenes Netzwerk (Closed Network)
- Zugangskontrolle über MAC-Adresse
- LANCOM Enhanced Passphrase Security (LEPS)
- Verschlüsselung des Datentransfers (802.11i/WPA oder WEP)
- 802.1x / EAP
- Optionales IPSec-over-WLAN VPN

7.1.1 SSID Broadcast unterdrücken – geschlossenes Netzwerk (Closed Network)

Jedes Funk-LAN nach IEEE 802.11 trägt einen eigenen Netzwerknamen (SSID). Dieser Netzwerkname dient der Identifizierung und Verwaltung von Funk-LANs.

Ein Funk-LAN kann so eingerichtet werden, dass jeder beliebige Benutzer Zugang zu diesem Netzwerk erhält. Solche Netzwerke werden als offene Netzwerke bezeichnet. Auf ein offenes Netzwerk kann ein Benutzer auch ohne Kenntnis des hierfür eigens reservierten Netzwerknamens zugreifen. Der Zugriff erfolgt mit der Eingabe des Netzwerknamens 'ANY'.

In einem geschlossenen Netzwerk (Closed Network) ist der Zugriff über 'ANY' ausgeschlossen. Hier muss der Benutzer den korrekten Netzwerknamen angeben. Unbekannte Netzwerke bleiben ihm verborgen.

DE

7.1.2 Zugangskontrolle über MAC-Adresse

Jedes Netzwerkgerät verfügt über eine unverwechselbare Identifizierungsnummer. Diese Identifizierungsnummer wird als MAC-Adresse (**M**edia **A**ccess **C**ontrol) bezeichnet und ist weltweit einmalig.

Die MAC-Adresse ist fest in die Hardware einprogrammiert. Auf einem Funk-LAN-Gerät von LANCOM Systems finden Sie die MAC-Adresse auf dem Gehäuse.

Der Zugriff auf ein Infrastruktur-Netzwerk kann unter Angabe von MAC-Adressen auf bestimmte Funk-LAN-Geräte beschränkt werden. Dazu gibt es in den Access Points Filter-Listen (ACL = Access Control List), in denen die zugriffsberechtigten MAC-Adressen hinterlegt werden können.

Im Ad-hoc-Netzwerk steht diese Methode der Zugangskontrolle nicht zur Verfügung.

7.1.3 LANCOM Enhanced Passphrase Security

Mit LEPS (**L**ANCOM **E**nhanced **P**assphrase **S**ecurity) hat LANCOM Systems ein effizientes Verfahren entwickelt, das die einfache Konfigurierbarkeit von IEEE 802.11i mit Passphrase nutzt und dabei die möglichen Fehlerquellen beim Verteilen der Passphrase vermeidet. Bei LEPS wird jeder MAC-Adresse in einer zusätzlichen Spalte der ACL eine individuelle Passphrase zugeordnet – eine beliebige Folge aus 4 bis 64 ASCII-Zeichen. Nur die Verbindung von Passphrase und MAC-Adresse erlaubt die Anmeldung am Access Point und die anschließende Verschlüsselung per IEEE 802.11i oder WPA.

LEPS kann sowohl lokal im Gerät genutzt werden als auch mit Hilfe eines RADIUS-Servers zentral verwaltet werden und funktioniert mit sämtlichen am Markt befindlichen WLAN-Client-Adaptern, ohne dass dort eine Änderung stattfinden muss. Da LEPS ausschließlich im Access Point konfiguriert wird, ist jederzeit die volle Kompatibilität zu Fremdprodukten gegeben.

Ein weiterer Sicherheitsaspekt: Mit LEPS können auch einzelne Point-to-Point-Strecken (P2P) mit einer individuellen Passphrase abgesichert werden. Wenn bei einer P2P-Installationen ein Access Point entwendet wird und dadurch Passphrase und MAC-Adresse bekannt werden, sind alle anderen per LEPS abgesicherten WLAN-Strecken weiterhin geschützt, insbesondere wenn die ACL auf einem RADIUS-Server abgelegt ist.

Gastzugang mit LEPS: LEPS kann auch zur Einrichtung eines Gast-Zugangs verwendet werden. Dabei werden alle Benutzer des internen WLAN-Netzes mit individuellen Passphrases ausgestattet. Für Gäste

steht eine eigene SSID mit einer globalen Passphrase zur Verfügung. Um Mißbrauch zu verhindern, kann die globale Passphrase regelmäßig – z.B. alle paar Tage – geändert werden.

7.1.4 Verschlüsselung des Datentransfers

Der Verschlüsselung des Datentransfers kommt bei Funk-LANs eine besondere Rolle zu. Für den Funktransfer nach IEEE 802.11 gibt es die ergänzenden Verschlüsselungsstandards 802.11i/WPA und WEP. Ziel dieser Verschlüsselungsverfahren ist, das Sicherheitsniveau kabelgebundener LANs auch im Funk-LAN zu gewährleisten.

- Verschlüsseln Sie die im WLAN übertragenen Daten. Aktivieren Sie dazu die maximal mögliche Verschlüsselung (802.11i mit AES, TKIP oder WEP) und tragen Sie entsprechenden Schlüssel bzw. Passphrases im Access Point und in den WLAN-Clients ein.
- Ändern Sie regelmäßig die WEP-Schlüssel in Ihrem Access Point. Die Passphrases für 802.11i oder WPA müssen nicht gewechselt werden, da bereits regelmäßig im Betrieb neue Schlüssel pro Verbindung verwendet werden. Nicht nur deswegen ist die Verschlüsselung per 802.11i/AES oder WPA/TKIP wesentlich sicherer als das veraltete WEP-Verfahren.
- Falls es sich bei den übertragenen Daten um extrem sicherheitsrelevante Informationen handelt, können Sie zusätzlich zur besseren Authentifizierung der Clients das 802.1x-Verfahren aktivieren (‘802.1x / EAP’ → Seite 66) oder aber eine zusätzliche Verschlüsselung der WLAN-Verbindung einrichten, wie sie auch für VPN-Tunnel verwendet wird (‘IPSec-over-WLAN’ → Seite 67). In Sonderfällen ist auch eine Kombination dieser beiden Mechanismen möglich.

Detaillierte Informationen zur WLAN-Sicherheit und zu den verwendeten Verschlüsselungsmethoden finden Sie im LCOS Referenzhandbuch.

Bitte beachten Sie auch die Informationen Im Kasten „Standard-WEP-Verschlüsselung“.

DE

Standard-WEP-Verschlüsselung

Ab Werk wird für jedes unkonfigurierte Gerät standardmäßig eine WEP128-Verschlüsselung aktiviert. Für WLAN-Interfaces, die von einem LANCOM WLAN Controller verwaltet werden, wird die WEP-Verschlüsselung durch die zentralen Verschlüsselungseinstellungen in den Profilen des WLAN Controllers überschrieben.

Der Schlüssel setzt sich aus dem Anfangsbuchstaben „L" gefolgt von der LAN-MAC-Adresse des Access Points in ASCII-Schreibsweise zusammen. Die LAN-MAC-Adressen der LANCOM-Geräte beginnen immer mit der Zeichenfolge „00A057". Sie finden Sie LAN-MAC-Adresse auf einem Aufkleber auf der Unterseite des Gerätes. Verwenden Sie **nur** die als „MAC-Address" gekennzeichnete Nummer, die mit „00A057" beginnt. Bei den anderen ggf. angegebenen Nummern handelt es sich **nicht** um die LAN-MAC-Adresse!

Für ein Gerät mit der LAN-MAC-Adresse „00A0570FB9BF" lautet der Standard-WEP-Schlüssel also „L00A0570FB9BF". Dieser Schlüssel wird in den 'Einzel-WEP-Einstellungen' des Gerätes für jedes logische WLAN-Netzwerk als 'Schlüssel 1' eingetragen.

Um mit einer WLAN-Karte eine Verbindung zu einem neuen LANCOM Access Point herzustellen, muss in der WLAN-Karte die WEP128-Verschlüsselung aktiviert und der 13-stellige Standard-WEP-Schlüssel eingetragen werden.

Ändern Sie das WEP-Passwort nach der ersten Anmeldung, um eine sichere Verbindung zu gewährleisten.

Beachten Sie, dass bei einem Reset auch die im Gerät definierten WLAN-Verschlüsselungseinstellungen verloren gehen und auf diesen Standard-WEP-Schlüssel zurückgesetzt werden. Der WLAN-Zugang gelingt nach dem Reset nur, wenn der Standard-WEP-Schlüssel in der WLAN-Karte eingetragen ist!

7.1.5 802.1x / EAP

Der internationale Industrie-Standard IEEE 802.1x und das **E**xtensible **A**uthentication **P**rotocol (EAP) ermöglichen Access Points die Durchführung einer zuverlässigen und sicheren Zugangskontrolle. Die Zugangsdaten können

zentral auf einem RADIUS-Server (integrierter RADIUS/EAP-Server im WLAN Controller oder externer RADIUS/EAP-Server) verwaltet und von dem Access Point bei Bedarf von dort abgerufen werden.

Diese Technologie ermöglicht außerdem den gesicherten Versand und den regelmäßigen automatischen Wechsel von WEP Schlüsseln. Auf diese Weise verbessert IEEE 802.1x die Sicherungswirkung von WEP.

In Windows XP ist die IEEE-802.1x-Technologie bereits fest integriert. Für andere Betriebssysteme existiert Client-Software. Die Treiber der LANCOM AirLancer-Funkkarten verfügen bereits über einen integrierten 802.1x Client.

7.1.6 IPSec-over-WLAN

Mittels IPSec-over-WLAN kann zusätzlich zu den bereits vorgestellten Sicherheitsmechanismen ein Funknetzwerk optimal abgesichert werden. Hierzu sind eine Basisstation mit VPN-Unterstützung und der LANCOM Advanced VPN Client erforderlich, welcher unter den Betriebssystemen Windows 2000, XP und Vista™ arbeitet. Für andere Betriebssysteme existiert Clientsoftware von Fremdherstellern.

7.2 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.

DE

7.3 Der Sicherheits-Assistent

Der Zugriff auf die Konfiguration des Geräts erlaubt nicht nur das Auslesen kritischer Informationen (z. B. WEP-Schlüssel, 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.

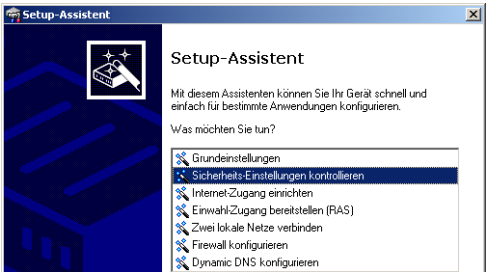
Ihr LANCOM verfügt über einen Kennwortschutz für den Konfigurationszugang. Dieser wird schon während der Grundkonfiguration durch Angabe eines Kennwortes aktiviert.

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.

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

⑤ Bei Geräten mit WLAN-Schnittstelle haben Sie nun die Möglichkeit, die Sicherheitsparameter für das Funknetzwerk einzustellen. Dazu gehören der Name des Funknetzwerks, die Closed-Network-Funktion und die Verschlüsselung mit 802.11i/WPA oder WEP. Bei einem Gerät mit der Option für eine zweite WLAN-Schnittstelle können Sie diese Parameter für beide Funknetzwerke separat eingeben.

⑥ Für die WLAN-Schnittstelle können Sie anschließend die Filterlisten für Stationen (ACL) und Protokolle definieren. Damit schränken Sie den Datenaustausch zwischen dem drahtlosen Netzwerk und dem lokalen Netzwerk ein.

⑦ Im Bereich der Firewall aktivieren Sie die Stateful-Inspection, das Ping-Blocking und den Stealth-Mode.

⑧ Der Assistent informiert Sie sobald die Eingaben vollständig sind. Schließen Sie die Konfiguration mit **Fertig stellen** ab.

7.3.2 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 Netzwerke
- Parameter der Konfigurationssperre (Anzahl der Fehllogins und Dauer der Sperre)
- Sicherheitsparameter wie WLAN-Name, Closed-Network-Funktion, WPA-Passphrase, WEP-Schlüssel, ACL-Liste und Protokoll-Filter

7.4 Der Firewall-Assistent

Ihr LANCOM verfügt über eine Stateful-Inspection-Firewall und Firewall-Filter zur wirksamen Absicherung Ihres WLAN 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.

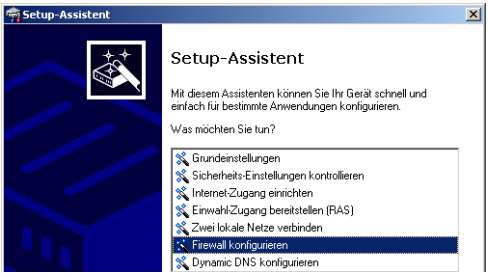
Der Firewall-Assistent hilft Ihnen, schnell und komfortabel neue Regeln für die Firewall zu erstellen.

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

DE

7.4.1 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.

7.4.2 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.

7.5 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'

- **Haben Sie die Konfiguration vom Funk-Netzwerk aus zugelassen?**

  Wenn Sie die Konfiguration vom Funk-Netzwerk aus nicht benötigen, so schalten Sie sie ab. Das Feld zur Abschaltung der Konfiguration vom Funk-Netzwerk aus finden Sie ebenfalls in LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Admin'. Wählen Sie hier unter 'Zugriffsrechte - Vom Wireless LAN' für alle Konfigurationsarten die Option 'nicht erlaubt'.

- **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'.

DE

- **Haben Sie die Firewall aktiviert?**

  Die Stateful-Inspection Firewall der LANCOM Router 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 LANCOM Router 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 den Router 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 den Router 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 das Funknetzwerk durch eine Verschlüsselung, ACL und LEPS abgesichert?**

  Mit Hilfe von 802.11i, WPA oder WEP verschlüsseln Sie die Daten im Funknetzwerk mit verschiedenen Verschlüsselungsmethoden wie AES, TKIP oder WEP. LANCOM Systems empfiehlt die stärkste mögliche Verschlüsselung mit 802.11i und AES. Wenn der eingesetzte WLAN Client Adapter diese nicht unterstützt, nutzen Sie TKIP oder zumindest WEP. Stellen Sie sicher, dass in Ihrem Gerät bei aktivierter Verschlüsselungs-Funktion mindestens eine Passphrase oder ein WEP-Schlüssel eingetragen und zur Verwendung ausgewählt ist.

Ab Werk wird für jedes unkonfigurierte Gerät standardmäßig eine WEP128-Verschlüsselung aktiviert. Für WLAN-Interfaces, die von einem LANCOM WLAN Controller verwaltet werden, wird die WEP-Verschlüsselung durch die zentralen Verschlüsselungseinstellungen in den Profilen des WLAN Controllers überschrieben.

Zur Kontrolle der WEP Einstellungen wählen Sie in LANconfig im Konfigurationsbereich 'WLAN-Sicherheit' auf der Registerkarte '802.11i/WEP' die Verschlüsselungseinstellungen für die logischen und physikalischen WLAN-Interfaces aus.

Ändern Sie das Default-WEP-Passwort gleich nach der Erstkonfiguration des Gerätes.

Mit der Access Control List (ACL) gewähren oder untersagen Sie einzelnen Funk-LAN-Clients den Zugriff auf Ihr Funk-LAN. Die Festlegung erfolgt anhand der fest programmierten MAC-Adressen der Funk-Netzwerkkarten. Zur Kontrolle der Access Control List wählen Sie in LANconfig im Konfigurationsbereich 'WLAN-Sicherheit' die Registerkarte 'Stationen'.

Mit der LANCOM Enhanced Passphrase Security (LEPS) ordnen Sie jeder MAC-Adresse in einer zusätzlichen Spalte der ACL eine individuelle Passphrase zu – eine beliebige Folge aus 4 bis 64 ASCII-Zeichen. Nur die Verbindung von Passphrase und MAC-Adresse erlaubt die Anmeldung am Access Point und die anschließende Verschlüsselung per IEEE 802.11i oder WPA.

- **Haben Sie für besonders sensiblen Datenaustausch auf dem Funknetzwerk die Funktionen von IEEE-802.1x eingerichtet?**

  Wenn Sie auf Ihrem Funk-LAN besonders sensible Daten austauschen, können Sie zur weiteren Absicherung die IEEE-802.1x-Technologie verwenden. Um die IEEE-802.1x-Einstellungen zu kontrollieren oder zu aktivieren, wählen Sie in LANconfig den Konfigurationsbereich 'Wireless-LAN'.

- **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 sie nach dem Wiedereinschalten oder beim Einschalten an einem anderen Ort nicht mehr verwendet werden kann.

  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).

Mit der Funktion des „Autarken Weiterbetriebs" wird die Konfiguration für ein WLAN-Interface, das von einem LANCOM WLAN Controller verwaltet wird, nur für eine bestimmte Zeit im Flash bzw. ausschließlich im RAM gespeichert. Die Konfiguration des Geräts wird gelöscht, wenn der Kontakt zum WLAN Controller oder die Stromversorgung länger als die eingestellte Zeit unterbrochen wird.

- **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.

DE

8 Optionen und Zubehör

Ihr LANCOM Wireless Router verfügt über zahlreiche Erweiterungsmöglichkeiten und die Möglichkeit das umfangreiche LANCOM Zubehör zu nutzen. In diesem Kapitel finden Sie Informationen darüber, welches Zubehör erhältlich ist und wie Sie es zusammen mit Ihrem Access Point verwenden können.

- Durch optionale Antennen der AirLancer-Serie lässt sich die Reichweite des Access Points erhöhen und an besondere Umgebungsbedingungen anpassen.
- Mit der LANCOM Public Spot Option lässt sich der LANCOM Wireless Router um zusätzliche Abrechnungsfunktionen erweitern und zu einem Wireless Public Spot aufrüsten.

8.1 Optionale AirLancer Extender Antennen

Um die Reichweite der LANCOM Wireless Router zu erhöhen, oder den Access Point an besondere Umgebungsbedingungen anzupassen, können Sie AirLancer Extender Antennen an das Gerät anschließen. Eine Übersicht, welche Antennen unterstützt werden und anschließbar sind, finden Sie jederzeit auf der LANCOM Webseite unter www.lancom.de.

Zur Berechnung der Konfiguration von AirLancer Extender Antennen und auch von Fremdantennen, die Sie an die LANCOM Wireless Router anschließen wollen, finden Sie weitere Informationen unter www.lancom.de.

Achten Sie bei der Installation von externen Antennen darauf, die Bestimmungen des Landes einzuhalten, in dem Sie das WLAN-Gerät betreiben. Dazu können Sie die Sendeleistung abzüglich der Kabeldämpfung in die LANCOM-Konfiguration eintragen. Mit diesen Daten berechnet LCOS selbständig die korrekte Sendeleistung für das gewählte Land.

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

8.1.1 Antenna Diversity

Bei der Übertragung von Funksignalen kommt es z. B. durch Reflektion und Streuung des Signals zu starken Qualitätsverlusten. An manchen Stellen über-

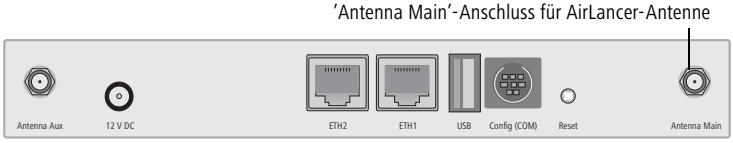
lagern sich die Schwingungen der reflektierten Signale so ungünstig, dass die Signalstärke zurückgeht bzw. vollständig ausgelöscht wird.

Zur Verbesserung der Übertragungsqualität gelangen sogenannte „Diversity"-Verfahren zum Einsatz. Das Prinzip eines „Diversity"-Verfahrens beruht darauf, dass am Empfangsort das Nachrichtensignal mehrfach (meistens zwei Mal) empfangen wird. Durch eine geeignete Weiterverarbeitung werden diese Nachrichtensignale wieder zu einem einzigen Signal zusammengeführt. Am bekanntesten sind Space- (Raum) und Polarisations-Diversity. LANCOM Systems bietet als Erweiterung der LANCOM Wireless Router verschiedene Polarisations-Diversity-Antennen an. Bei diesen Modellen werden in einer Antenne zwei senkrecht zueinander polarisierte Signale empfangen. Weitere Informationen zum Verfahren entnehmen Sie bitte unserem Techpaper „Polarisations-Diversity".

Polarisations-Diversity-Antennen von LANCOM Systems:

- AirLancer Extender O-D80g (2,4 GHz-Band), Art.Nr. 61221
- AirLancer Extender O-D60a (5 GHz Band), Art.Nr. 61222

Zur Installation einer optionalen AirLancer Antenne schalten Sie den LANCOM Wireless Router aus, indem sie das Kabel der Spannungsversorgung aus dem Gerät herausziehen. Entfernen Sie nun vorsichtig die beiden Diversity-Antennen auf der Rückseite, indem Sie diese abschrauben. Schliessen Sie die AirLancer Antenne an den mit 'Antenna Main' beschrifteten Antennenanschluss an.



8.2 LANCOM Public Spot Option

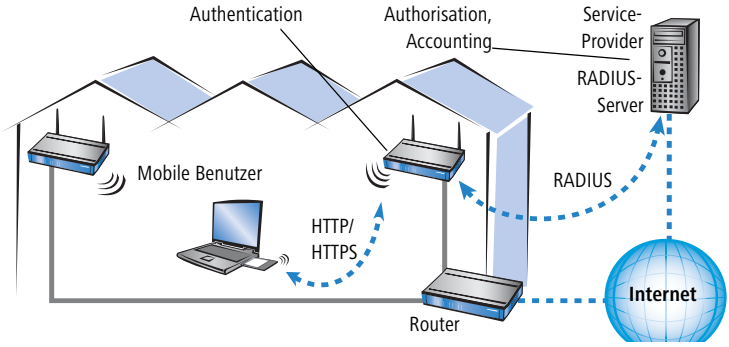
Wireless Public Spots sind öffentlich zugängliche Punkte, an denen sich Benutzer mit ihrem eigenen mobilen Rechner per Funk in ein Netzwerk (z.B. ein Firmen-LAN oder das Internet) einwählen können.

Die Wireless LAN Technologie ist ideal dafür geeignet, um an Plätzen wie Flughäfen, Hotels, Bahnhöfen, Restaurants oder Cafés (sogenannten Public Hot Spots) drahtlose Internet-Dienstleistungen für die Öffentlichkeit anzubieten. Die LANCOM Public Spot Option wendet sich dabei an alle Betreiber von

DE

öffentlichen Funknetzen und stellt für die LANCOM Router Access Points Zusatzfunktionen zur Authentifizierung und Abrechnung von öffentlichen Internet-Dienstleistungen zur Verfügung, und ermöglicht damit den einfachen Aufbau und Wartung von Public Hot Spots.

Die LANCOM Public Spot Option ist die optimale Lösung für öffentliche Funk-LANs. Denn Wireless LANs eignen sich sehr gut für Firmennetzwerke und zur Funkvernetzung zu Hause. Für öffentliche Access-Dienste fehlt es im Standard jedoch an Mechanismen zur Authentifizierung und Abrechnung von einzelnen Benutzern (AAA - Authentication / Authorisation / Accounting). Diesen Mangel behebt die LANCOM Systems Open User Authentication (OUA), der Kernbestandteil der LANCOM Public Spot Option. Das OUA-Verfahren realisiert die Authentifizierung aller Funk-Clients per User-Name und Passwort und prüft die Autorisierung einzelner Benutzer per RADIUS. Accounting-Daten (Online-Zeit und Datenvolumen) können pro Benutzer und pro Sitzung an den zentralen RADIUS-Server weitergegeben werden. Client-PCs benötigen lediglich eine Funkkarte (z. B. AirLancer), TCP/IP und einen Internet-Browser. Weitere Software wird nicht benötigt. Die Public Spot Option eignet sich daher optimal zur Einrichtung von drahtlosen Internet-Access-Dienstleistungen in Hotels, Restaurants, Cafés, Flughäfen, Bahnhöfen, Messegeländen oder Universitäten.



Mit der LANCOM Public Spot Option erweitern Sie einen Access Point nachträglich um diese Funktionen und rüsten sie zum Wireless Public Spot auf.

9 Rat & Hilfe

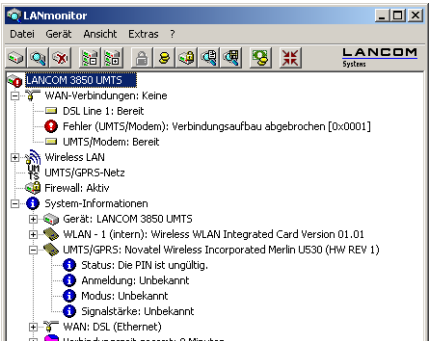
In diesem Kapitel finden Sie Ratschläge und Hilfestellungen für die erste Hilfe bei einigen typischen Problemen.

9.1 UMTS PIN-Handling

Je nach Konfiguration versucht ein LANCOM mit UMTS/HSDPA-Funktion und eingelegter Datenkarte direkt nach dem Einschalten automatisch eine Verbindung ins Internet aufzubauen. Dabei wird die in der Konfiguration des Geräts gespeicherte PIN an die SIM-Karte in der Datenkarte übertragen, um den Verbindungsaufbau in ein UMTS/HSDPA- oder GPRS-Netz zu ermöglichen.

Wenn die PIN in der Konfiguration nicht korrekt eingetragen ist, übermittelt das Gerät eine ungültige PIN an die SIM-Karte. Nach dem dritten Versuch, die SIM-Karte mit einer ungültigen PIN zu aktivieren, werden die meisten Karten automatisch gesperrt und können nur mit einer weiteren Kenn-Nummer (je nach Netzbetreiber z.B. PIN2 oder PUK) freigeschaltet werden.

Bei einem Gerät mit automatischem Verbindungsaufbau ins Internet würden diese drei Aktivierungsversuche mit ungültiger PIN möglicherweise vom Anwender unbemerkt und innerhalb weniger Sekunden ablaufen. Um die dadurch folgende Sperre der PIN zu verhindern, verhindert ein LANCOM mit UMTS/HSDPA-Funktion den Verbindungsaufbau über die Datenkarte automatisch, sobald die SIM-Karte einen Aktivierungsversuch mit einer falschen PIN meldet. Im LANmonitor wird dieser Zustand mit der Fehlermeldung 'Die PIN ist ungültig' angezeigt:



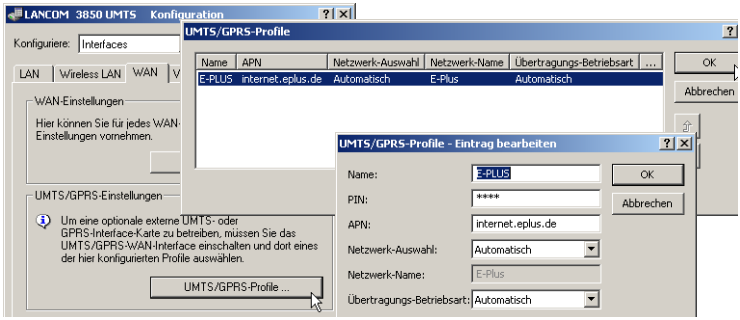
Um diese Sperre zu löschen, gehen Sie wie folgt vor:

① Ändern Sie die PIN in Ihrem UMTS/HSDPA-GPRS-Profil.

DE

Konfiguration mit LANconfig

Die UMTS/HSDPA-GPRS-Profile finden Sie in LANconfig im Konfigurationsbereich 'Interfaces' auf der Registerkarten 'WAN' unter der Schaltfläche UMTS/GPRS-Profile.



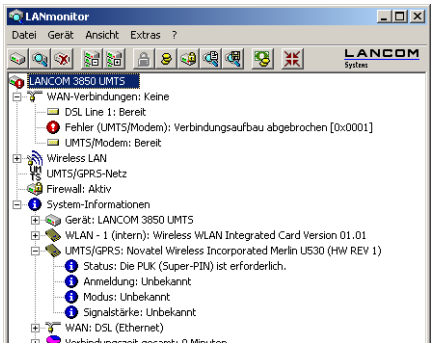
Konfiguration mit WEBconfig oder Telnet

Unter WEBconfig oder Telnet finden Sie die UMTS/HSDPA-GPRS-Profile auf folgenden Pfaden:

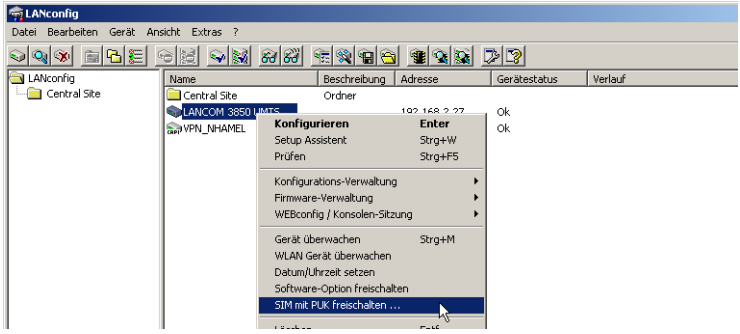
Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ▶ Setup ▶ Schnittstellen ▶ UMTS-GPRS-Parameter ▶ Profile
Terminal/Telnet	`Setup/Schnittstellen/Modem-Parameter/Schnittstelle/UMTS-GPRS-Parameter`

② Beim nächsten Aufbau mit der richtigen PIN wird die Verbindung ohne Fehler hergestellt.

Nach dem dritten Aktivierungsversuch mit einer falschen PIN wird die SIM-Karte gesperrt. Auch dieser Fehler wird im LANmonitor mit der Meldung 'Die PUK (Super-PIN) ist erforderlich' angezeigt.



In diesem Fall können Sie die SIM-Karte über das Kontext-Menü für das Gerät in LANconfig wieder freischalten.



Mit der Datenkarte wird üblicherweise auch eine Betriebssoftware des Netzbetreibers geliefert. Über diese Software können Sie bei Bedarf die PIN der SIM-Karte ändern.

9.2

9.3 Es wird keine DSL-Verbindung aufgebaut

Nach dem Start versucht der Router automatisch, Kontakt zum DSL-Anbieter aufzunehmen. Während dieser Phase blinkt die DSL-LED grün. Im Erfolgsfall wechselt diese LED dann auf dauerhaftes Grün. Schlägt die Kontaktaufnahme hingegen fehl, so leuchtet die DSL-LED nicht. In der Regel ist eine der folgenden Ursachen:

DE

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. Die DSL-LED muss zum Zeichen der physikalischen Verbindung grün leuchten.

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

9.4 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.

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).

9.5 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

DE

		LANCOM 3850 UMTS
Frequenzband		WLAN-Modul mit 2400 - 2483,5 MHz (ISM) oder 5150 - 5750 MHz
Anschlüsse	ETH1, ETH2	10/100Base-TX, Autosensing
	WLAN1	2x Reverse SMA-Buchse mit Antenna Diversity
	WLAN2	32-bit-Cardbus-Schnittstelle für eine optionale UMTS- oder zweite WLAN-Karte
Stromversorgung		12V DC über externes Netzteil, oder Power-over-Ethernet nach IEEE 802.3af
Antennen		Zwei Dualband Dipol-Antennen im Lieferumfang. Bitte berücksichtigen Sie die gesetzlichen Bestimmungen Ihres Landes für den Betrieb von Antennensystemen. Zur Berechnung einer konformen Antennen-Konfiguration finden Sie Informationen unter www.lancom.de
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 ETSI EN 300 328, ETSI EN 301 893, ETSI EN 301 489-1, ETSI EN 301 489-17, EN 60950 Funkzulassungen für alle Länder der EU inkl. Schweiz
Zulassungen		Notifiziert in den Ländern Deutschland, Belgien, Niederlande, Luxemburg, Österreich, Schweiz, Großbritannien, Italien, Spanien, Frankreich, Portugal
Umgebung/Temperatur		0 °C bis +50 °C bei 95 % max. Luftfeuchtigkeit (nicht kondensierend)
Service		Garantie 3 Jahre

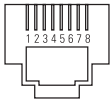
		LANCOM 3850 UMTS
Support		Über Hotline und Internet
Zubehör		■ LANCOM Modem Adapter Kit zum Anschluß von Modems (analog oder GSM) an die serielle Konfigurationsschnittstelle (Art.-Nr. 61500) ■ LANCOM Rack Mount Option (Art.-Nr. 61501) ■ LANCOM LCOS Referenzhandbuch (DE) (Art.-Nr. 61700) ■ LANCOM Advanced VPN Client für Windows 98SE-XP, 1er Lizenz, Art.-Nr. 61600 ■ LANCOM Advanced VPN Client für Windows 98SE-XP, 10er Lizenz, Art.-Nr. 61601 ■ LANCOM Advanced VPN Client für Windows 98SE-XP, 25er Lizenz, Art.-Nr. 61602 ■ LANCOM ES-1108P Kompakter, robuster 8-Port-Ethernetswitch mit 4 PoE-Schnittstellen, Art.-Nr. 61450 ■ Blitzschutzadapter SA-5 (2.4 und 5 GHz), Art.-Nr. 61212 ■ Blitzschutzadapter SA-LAN, Art.-Nr. 61213
Optionen		■ VPN-Option (25 Kanäle, 50 konfigurierbar) inkl. Aktivierung des Hardware-Beschleunigers (Art.-Nr. 60083) ■ LANCOM Service-Option (4 Jahre Garantie, Vorabaustausch) (Art.-Nr. 61401) ■ LANCOM Public Spot Option (Authentifizierungs- und Accounting-Software für Hotspots) (Art.-Nr. 60642)

DE

10.2 Anschlussbelegung

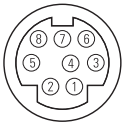
10.2.1 LAN/WAN-Schnittstelle 10/100Base-TX, DSL-Schnittstelle

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

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

10.2.2 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 Anforde-

rungen 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).

11 Zulassungen und Funkkanäle für WLANs

Informationen zu den Zulassungen und Notifizierungen in verschiedenen Ländern sowie zu den Funkkanälen und Nutzungsbeschränkungen finden Sie im Referenzhandbuch oder im Internet unter www.lancom.de.

Index

DE