

LANCOM OAP-54 Wireless

© 2007 LANCOM Systems GmbH, Würselen (Germany). Alle Rechte vorbehalten.

Alle Angaben in dieser Dokumentation sind nach sorgfältiger Prüfung zusammengestellt worden, gelten jedoch nicht als Zusicherung von Produkteigenschaften. LANCOM Systems haftet ausschließlich in dem Umfang, der in den Verkaufs- und Lieferbedingungen festgelegt ist.

Weitergabe und Vervielfältigung der zu diesem Produkt gehörenden Dokumentation und Software und die Verwendung ihres Inhalts sind nur mit schriftlicher Erlaubnis von LANCOM Systems gestattet. Änderungen, die dem technischen Fortschritt dienen, bleiben vorbehalten.

Windows®, Windows Vista™, Windows NT® und Microsoft® sind eingetragene Marken von Microsoft, Corp.

Das LANCOM Systems-Logo, LCOS und die Bezeichnung LANCOM sind eingetragene Marken der LANCOM Systems GmbH. Alle übrigen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein.

LANCOM Systems behält sich vor, die genannten Daten ohne Ankündigung zu ändern, und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Produkte von LANCOM Systems enthalten Software, die vom „OpenSSL Project“ für die Verwendung im „OpenSSL Toolkit“ entwickelt wurden (<http://www.openssl.org/>).

Produkte von LANCOM Systems enthalten kryptographische Software, die von Eric Young (eay@cryptsoft.com) geschrieben wurde.

Produkte von LANCOM Systems enthalten Software, die von der NetBSD Foundation, Inc. und ihren Mitarbeitern entwickelt wurden.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom.de

Würselen, Juni 2007

Ein Wort vorab

Vielen Dank für Ihr Vertrauen!

Das LANCOM OAP-54 Wireless ist designt für den anspruchsvollen Einsatz von Wireless LAN in rauen Umgebungen. Durch sein IP66-festes Gehäuse und die stabile Wand- und Mastmontagemöglichkeit ist er überall dort einsetzbar, wo höchste Ansprüche an Stabilität und Robustheit gestellt werden. Mit integrierter Heizung und Kühlung erlaubt er einen Betrieb bei Temperaturen von -30° bis +70°C.

Mit den zwei integrierten 108 MBit/s Funkmodulen nach den WLAN Standards IEEE 802.11a oder IEEE 802.11b/g arbeitet ein LANCOM OAP-54 Wireless auch gleichzeitig im 2,4 und/oder 5 GHz Frequenzbereich. Egal ob in Infrastruktur-Netzwerken oder zur Netzwerkkopplung als WLAN Bridge, es sind den Einsatzmöglichkeiten des LANCOM OAP-54 Wireless keine Grenzen gesetzt.

Sicherheitseinstellungen

Für einen sicheren Umgang mit Ihrem Produkt empfehlen wir Ihnen, sämtliche Sicherheitseinstellungen (z.B. Firewall, Verschlüsselung, Zugriffsschutz, Gebührensperrre) 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 drei Teilen: Dem Installation Guide, dem Benutzerhandbuch und dem Referenzhandbuch.

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:

■ Ein Wort vorab

DE

- 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
- LANC API
- 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.

Inhalt

1 Einleitung	9
1.1 Was ist ein Funk-LAN?	9
1.1.1 Welche Hardware ist notwendig?	9
1.1.2 Betriebsarten von Funk-LANs und Access Points	10
1.2 Was kann Ihr LANCOM Wireless Router?	10
2 Installation	14
2.1 Lieferumfang	14
2.2 Systemvoraussetzungen	15
2.3 Statusanzeigen, Schnittstellen und Installation der Hardware	15
2.3.1 Bedeutung der LEDs	15
2.3.2 LEDs beim LANCOM OAP-54 Wireless	16
2.3.3 Anschlüsse beim LANCOM OAP-54 Wireless	18
2.3.4 Montage und Anschluss des LANCOM OAP-54 Wireless	
21	
2.4 Installation der Software	24
2.4.1 Software-Setup starten	24
2.4.2 Welche Software installieren?	25
3 Grundkonfiguration	26
3.1 Welche Angaben sind notwendig?	26
3.1.1 TCP/IP-Einstellungen	26
3.1.2 Konfigurationsschutz	28
3.1.3 Einstellungen für das Funk-LAN	28
3.1.4 Gebührenschutz	29
3.2 Anleitung für LANconfig	30
3.3 Anleitung für WEBconfig	31
3.4 TCP/IP-Einstellungen an den Arbeitsplatz-PCs	36

4 Punkt-zu-Punkt-Verbindungen	37
4.1 Ausrichten der Antennen für den P2P-Betrieb	38
4.2 Konfiguration	40
4.3 Access Points im Relais-Betrieb	42
4.4 Sicherheit von Punkt-zu-Punkt-Verbindungen	42
4.4.1 Verschlüsselung mit 802.11i/WPA	42
4.4.2 LEPS für P2P-Verbindungen	44
5 Client-Modus	46
5.1 Grundkonfiguration	46
5.1.1 Betriebsart einstellen	46
5.1.2 Client-Einstellungen	48
5.1.3 Radio-Einstellungen	48
5.1.4 SSID der verfügbaren Netzwerke einstellen	49
5.1.5 Verschlüsselungseinstellungen	50
5.2 Erweiterte Konfiguration	51
5.2.1 Roaming	51
5.2.2 Weitere optionale Parameter	53
6 Den Internet-Zugang einrichten	56
6.1 Anleitung für LANconfig	57
6.2 Anleitung für WEBconfig	58

7 Sicherheits-Einstellungen	59
7.1 Sicherheit im Funk-LAN	59
7.1.1 Geschlossenes Netzwerk (Closed Network)	59
7.1.2 Zugangskontrolle über MAC-Adresse	59
7.1.3 LANCOM Enhanced Passphrase Security	60
7.1.4 Verschlüsselung des Datentransfers	61
7.1.5 802.1x / EAP	63
7.1.6 IPSec-over-WLAN	63
7.2 Tipps für den richtigen Umgang mit Schlüsseln und Passphrases	63
7.3 Der Sicherheits-Assistent	64
7.3.1 Assistent für LANconfig	64
7.3.2 Assistent für WEBconfig	65
7.4 Der Firewall-Assistent	65
7.4.1 Assistent für LANconfig	66
7.4.2 Konfiguration unter WEBconfig	66
7.5 Die Sicherheits-Checkliste	67
8 Optionen und Zubehör	72
8.1 Optionale AirLancer Extender Antennen	72
8.1.1 Antenna Diversity	72
8.2 LANCOM Public Spot Option	74
9 Rat & Hilfe	77
9.1 Es wird keine DSL-Verbindung aufgebaut	77
9.2 DSL-Übertragung langsam	77
9.3 Unerwünschte Verbindungen mit Windows XP	78
10 Anhang	79
10.1 Leistungs- und Kenndaten	79
10.2 Anschlussbelegung	80
10.2.1 LAN-Schnittstelle 10/100Base-TX, DSL-Schnittstelle	80
10.3 CE-Konformitätserklärungen	80
11 Index	81

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 – Local Area Network**). 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 **Wireless Local Area Network (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

1.2 Was kann Ihr LANCOM Wireless Router?

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

LANCOM OAP-54 Wireless	
Anwendungen	
WLAN über Point-to-Point und Relais-Modus (2 Funkmodule)	✓
Outdoor-Betrieb in rauen Umgebungen mit schwankenden Temperaturen (hohe Temperaturfestigkeit)	✓
Internet-Zugang	✓
IP-Router mit Stateful Inspection Firewall	✓
NetBIOS-Proxy zur Kopplung von Microsoft-Peer-to-Peer-Netzwerken über ISDN	✓
DHCP- und DNS-Server (für LAN und WAN)	✓

LANCOM OAP-54 Wireless	
N:N-Mapping zum Routen von Netzwerken mit den gleichen IP-Adresskreisen über VPN	✓
Policy-based Routing zur regelbasierten Auswahl der Zielroute	✓
Backup-Lösungen und Load-Balancing mit VRRP	✓
PPPoE-Server	✓
WAN- RIP	✓
Spanning-Tree-Protokoll	✓
Layer-2-QoS-Tagging	✓
VPN-Gateway (optional)	✓
WLAN	
Funkübertragung nach IEEE 802.11g und IEEE 802.11b	✓
Funkübertragung nach IEEE 802.11a und IEEE 802.11h	✓
Point-to-Point-Funktion (pro WLAN-Schnittstelle sechs P2P-Strecken definierbar)	✓
Relais-Funktion zur Verbindung zweier P2P-Strecken untereinander	✓
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	✓

■ Kapitel 1: Einleitung

LANCOM OAP-54 Wireless	
Integrierter RADIUS-Server	✓
VLAN	✓
Intra-Cell-Blocking	✓
QoS für WLAN (IEEE 802.11e, WMM/WME)	✓
Anschluss ans LAN	
Fast-Ethernet-Anschluss (10/100Base-TX)	✓
Power-over-Ethernet (PoE)	✓
DHCP- und DNS-Server	✓
WAN-Anschlüsse	
Anschluss für DSL- oder Kabelmodem	✓
Internet-Zugang (IP-Router)	
Stateful-Inspection Firewall	✓
Firewall-Filter (Adresse, Port)	✓
IP-Masquerading (NAT, PAT)	✓
Quality of Service	✓
VPN-Gateway mit VPN-Hardware-Verschlüsselung (optional)	✓
Stromversorgung	
Power-over-Ethernet (PoE) IEEE 802.3af	✓
Konfiguration und Firmware	
Konfiguration mit LANconfig oder mit Webbrowser, zusätzlich Terminalmodus für Telnet oder andere Terminalprogramme, SNMP-Schnittstelle und TFTP-Serverfunktion, SSH-Zugang.	✓
Konfigurationsassistenten	✓
FirmSafe zum Einspielen neuer Firmwareversionen ohne Risiko.	✓
Überwachung und Management Ihres WLAN mit Rogue AP Detection	
Optionale Software-Erweiterungen	
LANCOM Public Spot Option	✓

LANCOM OAP-54 Wireless	
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	✓
Gehäuse	
IP66-geschütztes Gehäuse für den Einsatz unter extremen äußereren Bedingungen	✓

2 Installation

Dieses Kapitel hilft Ihnen, möglichst schnell Hard- und Software zu installieren. Zunächst überprüfen Sie Lieferumfang und Systemvoraussetzungen. Sind alle Voraussetzungen erfüllt, gelingen Anschluss und Inbetriebnahme schnell und ohne Mühe.

2.1 Lieferumfang

Bitte prüfen Sie den Inhalt der Verpackung auf Vollständigkeit, bevor Sie mit der Installation beginnen. Neben des Access Points sollte der Karton folgendes Zubehör für Sie bereithalten:

LANCOM OAP-54 Wireless	
LAN-Anschlusskabel zum Anschluss an PoE-Injektor mit wasserdichten Verschraubungen, 15 m	✓
Anschraubbare externe 360° Dualband-Antennen mit Reverse N-plug	2
1 Adapterkabel Reverse N-jack nach N-plug, 1,5 m	✓
2 Adapterkabel Reverse N-jack nach N-plug, 10 cm	✓
Montagematerial für Wand und Mast	✓
1 PoE Port Injektor	✓
1 Stromkabel für PoE Power Injektor	✓
1 Erdungskabel mit Schrauben	✓
1 Terminator 50Ω zum Abschluß eines freien Antennenanschlusses	✓
LANCOM-CD	✓
Gedruckte Dokumentation	✓

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

2.2 Systemvoraussetzungen

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

- Betriebssystem mit TCP/IP-Unterstützung, z.B. Windows VistaTM, Windows XP, Windows Millennium Edition (Me), Windows 2000, Windows 98, Linux, BSD Unix, Apple Mac OS, OS/2.
- Funk-LAN-Adapter oder Zugang zum LAN (falls der Access Point ans LAN angeschlossen wird).



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

2.3 Statusanzeigen, Schnittstellen und Installation der Hardware

In diesem Abschnitt stellen wir Ihnen Ihr Gerät vor. Sie erhalten einen Überblick über alle Statusanzeigen, Anschlüsse und Schalter.



2.3.1 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.

2.3.2 LEDs beim LANCOM OAP-54 Wireless

Auf der Vorderseite des Geräts befinden sich Leuchtdioden (LEDs), die Informationen über den Status des Geräts geben.



1 Power

Diese LED gibt Auskunft über die Betriebsbereitschaft des Geräts. Sobald das Gerät mit Strom versorgt ist, leuchtet die LED konstant grün.

2 LAN

Zustand der LAN-Schnittstelle:

aus		kein Netzwerkgerät angeschlossen
gelb	dauerhaft an	Netzwerkgerät angeschlossen; Übertragungsrate 10 oder 100 Mbit/s
gelb	invers blitzend	Daten werden übertragen

3 WLAN1

Gibt Informationen über den WLAN-Zugang des ersten internen WLAN-Moduls des Access Points aus. Die WLAN-Link-Anzeige kann drei Zustände annehmen:

aus		WLAN-Modul defekt oder in der Konfiguration deaktiviert
gelb		WLAN-Modul in Betrieb
gelb	invers blitzend	Anzahl der Blitzer = Anzahl der verbundenen WLAN-Stationen und P2P-Funkstrecken, danach folgt eine Pause

4 WLAN2 Gibt Informationen über den WLAN-Zugang des zweiten internen WLAN-Moduls des Access Points aus. Bedeutung wie WLAN1.

5 WAN Zustand der WAN-Schnittstelle. Die WAN-Link-Anzeige kann drei Zustände annehmen:

aus		keine WAN-Verbindung angeschlossen
grün		Verbindung zum WAN hergestellt
grün	invers blitzend	Datentransfer über das WAN

6 Message Gibt Informationen über den allgemeinen Zustand des Gerätes aus.

Blinkende Message-LED und keine Verbindung möglich?

Blinkt die Message-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.



Signal für ein erreichtes Zeit- oder Gebührenlimit

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**.

aus		Ihr LANCOM OAP-54 Wireless arbeitet korrekt
rot	blinkend (langsam)	Gebührensperr aktiv (s. Kasten weiter unten)
rot	blinkend (schnell)	unsichere Konfiguration (kein Passwort gesetzt)
rot	blitzend	defektes WLAN-Modul



Eine blinkende Message-LED zeigt beim LANCOM OAP-54 Wireless das Erreichen eines Gebührenlimits an ('Blinkende Message-LED und keine Verbindung möglich?' → Seite 17).

2.3.3 Anschlüsse beim LANCOM OAP-54 Wireless

Beim LANCOM OAP-54 Wireless befinden sich sowohl auf der Ober- als auch auf der Unterseite Anschlüsse und Schalter der Basisstation.

Auf der Oberseite des LANCOM OAP-54 Wireless befinden sich zwei Anschlüsse für das erste WLAN-Modul. Auf der Unterseite befinden sich die LAN- und WAN-Anschlüsse, der Reset-Taster und der Antennenanschluss für das zweite WLAN-Modul.



- 7 Main-Anschluss für das erste WLAN-Modul.
- 8 Aux-Anschluss für das erste WLAN-Modul.
- 9 Anschluss für Erdungskabel.
- 10 10/100Base-Tx für den Anschluss an das LAN. Unterstützt werden 10-Mbit- oder 100-Mbit-Anschlüsse. Die verwendete Übertragungsgeschwindigkeit wird automatisch erkannt (Autosensing). Der LAN-Anschluss verfügt über eine automatische MDI/MDIX-Erkennung, so dass unabhängig von der Gegenstelle kein Crossover-Kabel benötigt wird.
- 11 10/100Base-Tx für den Anschluss an das WAN.
- 12 Antennenanschluss für das zweite WLAN-Modul.
- 13 Erdungskabel-Anschluss.

Der LAN-Anschluss des LANCOM Router Access Points unterstützt den Power-over-Ethernet-Standard (PoE).

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

Der LANCOM OAP-54 Wireless wird per Power over Ethernet mit Spannung versorgt. Dazu muss der im Lieferumfang befindliche Power Injektor benutzt werden.



Die Verwendung eines anderen PoE-Injektors etwa nach dem IEEE 802.3af-Standard ist nicht zulässig und kann zu Beschädigungen der Geräte führen. Der LANCOM OAP-54 Wireless hat bei voller Heiz- bzw. Kühlleistung eine Leistungsaufnahme von bis zu 25 Watt. Der dadurch entstehende höhere Stromfluß im PoE-Kabel begrenzt die mögliche Kabellänge.

Aufgrund der hohen Leistungsaufnahme des LANCOM OAP-54 Wireless ist eine störungsfreie Spannungsversorgung nur mit PoE-Kabellängen bis 50m gewährleistet.

Aus gleichem Grund ist darauf zu achten, daß auch die maximale Kabellänge zum nächsten Ethernet-Switch nicht länger als 50m sein darf, auch wenn die PoE-Einspeisung mit kürzerer Kabellänge (z.B. bei Nutzung des 15m-Kabels) geschieht.



Maximal 50 Meter zwischen Access Point und Power-Injektor/Ethernet-Switch!

Das im Lieferumfang des LANCOM OAP-54 Wireless beiliegende 15m PoE-Kabel mit wasserdichter Verschraubung kann dazu per Kupplung einfach verlängert werden. Eine Ethernet-Kabelkupplung und Cat.5 Ethernet-Kabel erhält man im Fachhandel.



Achten Sie bei allen Kabeln darauf, eine Kabelqualität von mindestens Cat. 5 zu verwenden. Die Kabel müssen dabei alle 4 Aderpaare durchkontaktieren.



Der beim LANCOM OAP-54 Wireless mitgelieferte 1 Port Power Injektor entspricht nicht dem IEEE 802.3af Standard. Er ist ausschließlich für die Speisung des LANCOM OAP-54 Wireless über den LAN-Port geeignet. Wollen Sie andere Geräte auf sichere Weise per IEEE 802.3af speisen, bietet Ihnen LANCOM einen eigenen PoE Power Injector an.

- 11 Anschluss für die WAN-Verbindung, die alternativ als LAN-Verbindung konfiguriert werden kann (ebenfalls Autosensing für 10/100 MBit/s und automatische MDI/MDIX-Erkennung).
- 12 Reset-Taster (siehe 'Die Funktion des Reset-Tasters')
- 13 Antennenanschluss für das zweite WLAN-Modul.

Reset-Taster beim LANCOM OAP-54 Wireless

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

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

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

■ Reset-Taster

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

- Ignorieren: Der Taster wird ignoriert.
- 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!



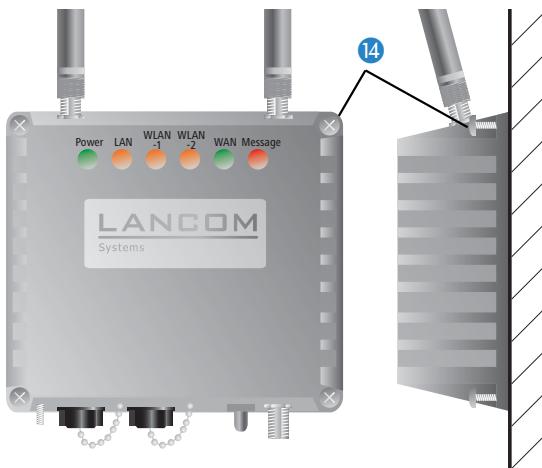
Beachten Sie, dass bei einem Reset auch die im Gerät definierten WLAN-Verschlüsselungseinstellungen verloren gehen und auf den Standard-WEP-Schlüssel zurückgesetzt werden ('Standard-WEP-Verschlüsselung' → Seite 62).

2.3.4 Montage und Anschluss des LANCOM OAP-54 Wireless

Wandmontage

- ① Montieren Sie Ihr LANCOM OAP-54 Wireless mit geeigneten Schrauben 14 in der gewünschten Position an der Wand. Die Schrauben zur Wandmontage sind nicht im Lieferumfang enthalten.

Wandmontage

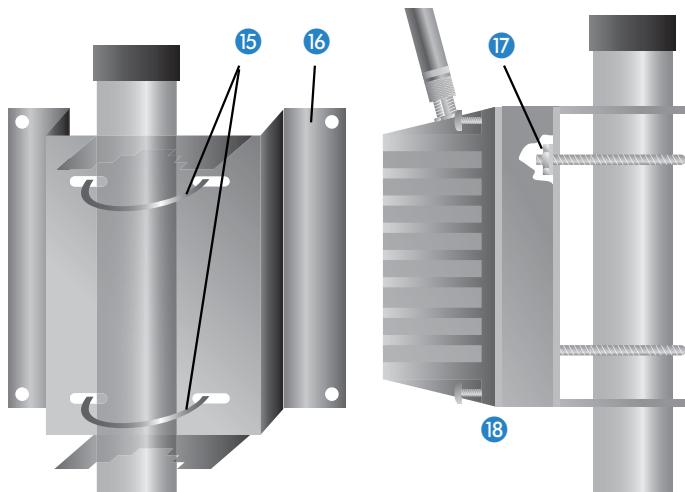


DE

Pfostenmontage

- ① Legen Sie die beiden U-förmigen Gewindestangen 15 um den Pfosten und verschrauben Sie die Gewindestangen mit den mitgelieferten Unterlegscheiben und Muttern 16 an der Montageplatte 17. Im Lieferumfang sind zwei Montageschellen für unterschiedliche Pfostendurchmesser enthalten.

Pfostenmontage



- ② Befestigen Sie anschließend Ihr LANCOM OAP-54 Wireless mit den beiden Schrauben ⑯ an der Montageplatte.

Anschluss des LANCOM OAP-54 Wireless

Die Installation der LANCOM OAP-54 Wireless-Geräte erfolgt in folgenden Schritten:

- ① Erdanschluss (falls notwendig) – Befestigen Sie das Erdungskabel an der Erdungsschraube ⑨ des LANCOM OAP-54 Wireless und an einem geeigneten Erdleiter.



Bei der Montage des LANCOM OAP-54 Wireless an Masten oder Wänden kann es notwendig sein, das Gehäuse zusätzlich mit einer Erdung zu versehen, um gefährliche Potentialunterschiede zu vermeiden. Außerdem empfiehlt LANCOM Systems, die Antennen und das PoE-Kabel jeweils mit Blitzschutzadapters zu versehen, um den LANCOM OAP-54 Wireless und das dahinter liegende LAN vor Beschädigung bei Blitzeinschlag zu schützen. Bitte konsultieren Sie bei jeder Installation in blitzeinschlaggefährdeten Bereichen einen zertifizierten Fachmann.

- ② Antennen – Schrauben Sie die beiden mitgelieferten Diversity Antennen an die beiden Reverse-N-Anschlüsse auf der Oberseite des LANCOM OAP-54 Wireless an ⑦ und ⑧. Eine zusätzliche Antenne für das zweite WLAN-

Modul können Sie an den Reverse-N-Anschluss auf der Unterseite des Geräts 13 anschliessen.



Zum Anschluss einer externe Antenne an einen Reverse-N-Anschluss nutzen Sie eines der beiliegenden Adapterkabel von „Reverse-N“ auf „N“.



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

- ③ LAN – Mit dem LAN-Anschluss wird ein LANCOM OAP-54 Wireless auch gleichzeitig mit Strom versorgt. Stecken Sie dazu das mitgelieferte wasser-tische Netzwerkkabel in den LAN-Anschluss an der Unterseite des Geräts 10 und verschließen Sie die Verschraubung sorgfältig. Verbinden Sie das andere Ende des Netzwerkkabels mit dem 'Power-Out'-Anschluss des mitgelieferten PoE-Injektors.
- ④ PoE – Verbinden Sie den 'LAN-In'-Anschluss des mitgelieferten PoE-Injektors über ein normales Ethernet-Kabel mit einer freien Netzwerkan-schlussdose Ihres lokalen Netzwerkes (bzw. einer freien Buchse eines Hubs/Switchs), und versorgen Sie den PoE-Injektor mit Spannung.

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

Bitte beachten Sie auch die mit dem PoE-Injektor gelieferte Dokumenta-tion.



Verwenden Sie den mitgelieferten PoE-Injektor nur für die Stromver-sorgung des LANCOM OAP-54 Wireless. Verbinden Sie den PoE-Injek-tor insbesondere nicht mit normalen Ethernet-Geräten!

- ⑤ WAN – Falls Sie den integrierten DSL-Router für eine direkte WAN-Ver-bindung nutzen möchten, stecken Sie das mitgelieferte WAN-Kabel in den WAN-Anschluss an der Unterseite des Gerätes 11 und verschließen Sie die Verschraubung sorgfältig. Verbinden Sie das andere Ende des WAN-Kabels mit einem ADSL- oder Kabel-Modem.



Wasser-tische WAN-Kabel von LANCOM Systems können bei Bedarf über den Fachhandel bestellt werden.

- ⑥ Betriebsbereit? – Sobald das Gerät mit Strom versorgt wird, leuchtet die Power-LED permanent grün. Nach dem Einschalten führt das Gerät einen Selbsttest durch, während dem die Message-LED blinkt. Danach zeigen die LEDs den Betriebszustand an.

DE

2.4 Installation der Software

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

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

2.4.1 Software-Setup starten

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

i 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:



2.4.2 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).
- 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 Router einwandfrei funktioniert.

3.1 Welche Angaben sind notwendig?

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

- TCP/IP-Einstellungen
- Schutz der Konfiguration
- Angaben zum Funk-LAN
- Einstellung des Gebührenschutzes
- Sicherheitseinstellungen

3.1.1 TCP/IP-Einstellungen

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

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

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

Neues LAN – vollautomatische Konfiguration möglich

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

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

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

Das Ergebnis der vollautomatischen TCP/IP-Konfiguration: Der Router erhält die IP-Adresse '172.23.56.1' (Netzmaske '255.255.255.0'). Außerdem wird der integrierte DHCP-Server aktiviert, so dass der LANCOM Router den Geräten im LAN automatisch IP-Adressen zuweist.

Trotzdem manuell konfigurieren?

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

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

Notwendige Angaben für die manuelle TCP/IP-Konfiguration

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

■ IP-Adresse und Netzwerkmaske für den LANCOM Router

Teilen Sie dem LANCOM Router 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 LANCOM 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 ein LANCOM können bis zu 16 verschiedene Administratoren eingerichtet werden. Weitere Informationen finden Sie im LCOS-Referenzhandbuch unter „Rechteverwaltung“ für verschiedene Administratoren“.

3.1.3 Einstellungen für das Funk-LAN

Der Netzwerkname (SSID)

Der Grundkonfigurations-Assistent fragt nach dem Netzwerknamen des Access Points (häufig als SSID – **S**ervice **S**et **I**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 jedes unkonfigurierte Gerät 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 Router Access Points 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.

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, dass sie sich möglichst nicht überdecken beziehungsweise möglichst weit auseinander liegen. Im 5 GHz-Band reicht normalerweise die automatische Einstellung, in der der LANCOM Router Access Point über TPC und DFS selbst den besten Kanal einstellt.

3.1.4 Gebührenschutz

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

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

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

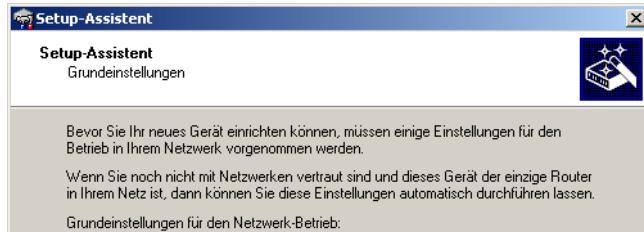


In der Grundeinstellung ist der Gebührenschutz auf maximal 600 Minuten innerhalb von sieben Tagen eingestellt. Passen Sie diese Einstellung an Ihre persönlichen Bedürfnisse an oder deaktivieren Sie den Gebührenschutz, wenn Sie mit Ihrem Provider einen Pauschal-Tarif (Flatrate) vereinbart haben.

3.2 Anleitung für LANconfig

- ① Starten Sie LANconfig mit **Start ▶ Programme ▶ LANCOM ▶ LANconfig**.

LANconfig erkennt den neuen LANCOM Router im TCP/IP-Netz selbstständig. Daraufhin 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 im Netzwerk (**Gerät ▶ Suchen**).



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

Wenn Sie die automatische TCP/IP-Konfiguration wählen, fahren Sie mit Schritt ④ fort.

- ② Geben Sie dem LANCOM Router eine verfügbare Adresse aus einem geeigneten IP-Adressbereich. Bestätigen Sie mit **Weiter**.
- ③ 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.

- ④ Geben Sie die Funk-Parameter ein. Wählen Sie einen Netzwerk-Namen (SSID) und einen Funkkanal aus. Schalten Sie ggf. die Funktion für ein 'geschlossenes Netzwerk' ein. Bestätigen Sie Ihre Angaben mit **Weiter**.
- ⑤ Der Gebührentschutz beschränkt auf Wunsch die Kosten von WAN-Verbindungen auf ein festgesetztes Maß. Bestätigen Sie Ihre Angaben mit **Weiter**.
- ⑥ Schließen Sie die Konfiguration mit **Fertig stellen** ab.

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

3.3 Anleitung für WEBconfig

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

Nach dem Einschalten prüfen unkonfigurierte LANCOM-Geräte zunächst, ob im LAN schon ein DHCP-Server aktiv ist. Je nach Situation kann das Gerät dann den eigenen DHCP-Server einschalten oder alternativ den DHCP-Client-

Modus aktivieren. In dieser zweiten Betriebsart kann das Gerät selbst eine IP-Adresse von einem im LAN schon vorhandenen DHCP-Server beziehen.

Netz ohne DHCP-Server

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



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

Netz mit DHCP-Server

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

- Ist im LAN auch ein DNS-Server zur Auflösung der Namen vorhanden und tauscht dieser die Zuordnung von IP-Adressen zu den Namen mit dem

DHCP-Server aus, kann das Gerät unter dem Namen "LANCOM-<MAC-Adresse>" (z.B. "LANCOM-00a057xxxxx") 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 Konfigurationschnittstelle an das Gerät anschliessen.

Aufruf der Assistenten in WEBconfig

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

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

(bzw. über beliebigen Namen)



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

Es erscheint das Hauptmenü von WEBconfig:

Setup-Assistenten

Assistenten erlauben es Ihnen, häufig auftretende Konfigurationen schnell und einfach vorzunehmen:

 [Grundeinstellungen](#)

 [Sicherheitseinstellungen](#)

 [Internet-Zugang einrichten](#)

 [Auswahl des Internet-Providers](#)

 [Einwahl-Zugang bereitstellen \(RAS\)](#)

 [Zwei lokale Netze verbinden](#)

Gerätekonfiguration und -status

Diese Menüpunkte erlauben einen Zugriff auf die vollständige Gerätekonfiguration:

 [Experten-Konfiguration](#)

 [Konfiguration speichern](#)

 [Konfiguration laden](#)

Firmware-Verwaltung

 [Eine neue Firmware hochladen](#)

Extras

 [Andere Geräte suchen/anzeigen](#)

 [SNMP-Geräte-MIB abrufen](#)



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**.
- ③ Geben Sie die Funk-Parameter ein. Wählen Sie einen Netzwerknamen (SSID) und einen Funkkanal aus. Schalten Sie ggf. die 'Closed Network' Funktion ein. Bestätigen Sie Ihre Eingabe mit **Setzen**.
- ④ 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.

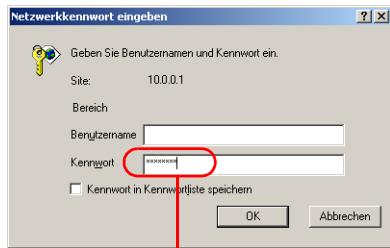


Bitte beachten Sie, dass mit dieser Freigabe auch die Fernkonfiguration über das Internet ermöglicht wird. Sie sollten in jedem Fall darauf achten, dass der Konfigurationszugriff geeignet abgesichert ist, z.B. durch ein Kennwort.

Eingabe des Kennworts im Web-Browser

Wenn Sie beim Zugriff auf das Gerät von Ihrem Web-Browser zur Eingabe von Benutzernamen 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

- ⑤ 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'.

- ⑥ Der Gebührenschutz beschränkt auf Wunsch die Kosten von WAN-Verbindungen auf ein festgesetztes Maß. Bestätigen Sie Ihre Angaben mit **Setzen**.
- ⑦ Der Grundeinrichtungs-Assistent meldet, dass alle notwendigen Angaben vorliegen. Mit **Weiter** schließen Sie ihn ab.

3.4 TCP/IP-Einstellungen an den Arbeitsplatz-PCs

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

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

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

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

■ IP-Adressvergabe über den LANCOM Router (Normalfall)

In dieser Betriebsart weist der LANCOM Router 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

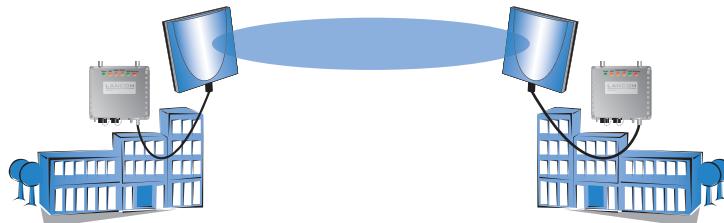
Werden die IP-Adressen im Netzwerk statisch vergeben, so sind bei jedem PC im LAN die IP-Adresse des LANCOM Router als Standard-Gateway und als DNS-Server in der TCP/IP-Konfiguration einzustellen.



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

4 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.

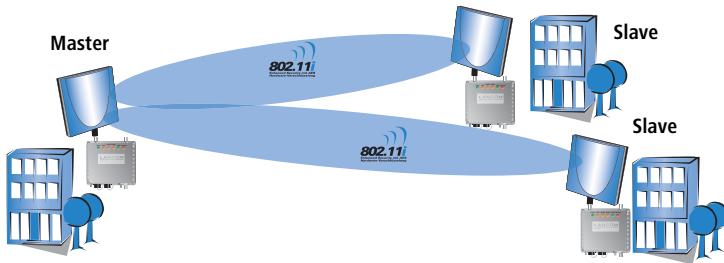


Das Verhalten eines Access Points beim Datenaustausch mit anderen Access Points wird in der „Punkt-zu-Punkt-Betriebsart“ festgelegt:

- **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 Sendever suchen 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.



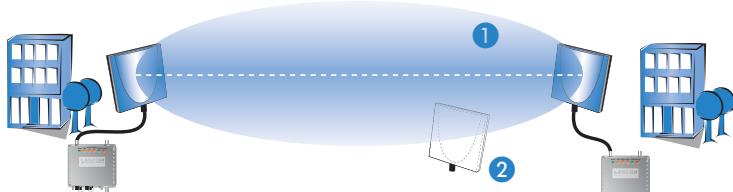
DE

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 aktiver automatischer Kanalsuche erleichtert diese Einstellung den Aufbau von Punkt-zu-Punkt-Verbindungen.

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

4.1 Ausrichten der Antennen für den P2P-Betrieb

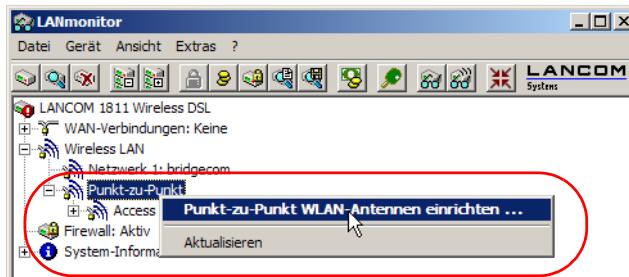
Beim Aufbau von P2P-Strecken kommt der genauen Ausrichtung der Antennen eine große Bedeutung zu. Je besser die empfangende Antenne in der „Ideallinie“ der sendenden Antenne liegt, desto besser ist die tatsächliche Leistung und damit die nutzbare Bandbreite ①. Liegt die empfangende Antenne jedoch deutlich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



(i) 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 ...'.

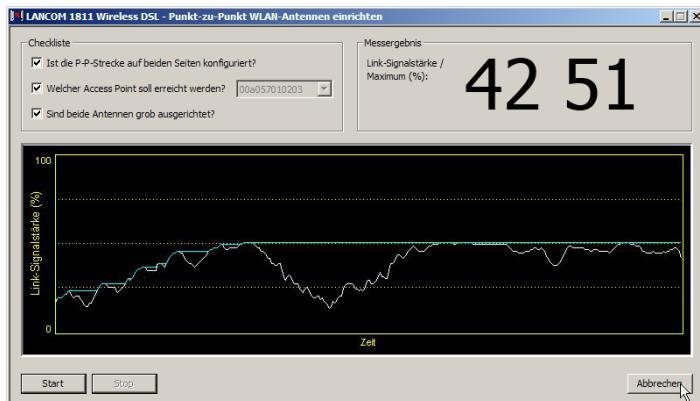


Der Eintrag 'Punkt-zu-Punkt' ist im LANmonitor nur sichtbar, wenn in dem überwachten Gerät mindestens eine Basisstation als Gegenstelle für eine P2P-Verbindung eingerichtet ist (LANconfig: **Wireless LAN** ▶ **Allgemein** ▶ **Physikalische WLAN-Einstellungen** ▶ **Punkt-zu-Punkt**).

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?
- 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.

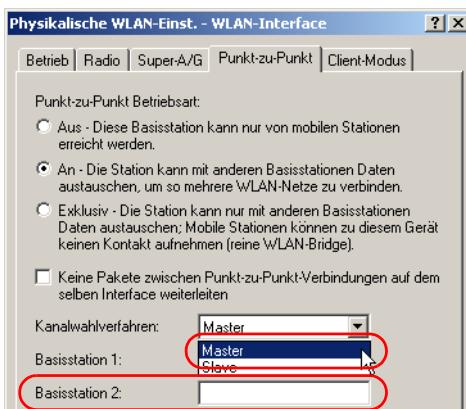
4.2 Konfiguration

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!



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

■ Kapitel 4: Punkt- zu- Punkt- Verbindungen

Konfiguration mit
WEBconfig oder
Telnet

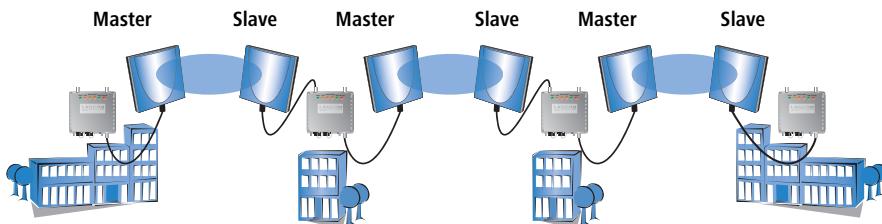
Unter WEBconfig oder Telnet finden Sie die Einstellungen für die Punkt-zu-Punkt-Verbindungen auf folgenden Pfaden:

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

DE

4.3 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.

4.4 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).

4.4.1 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

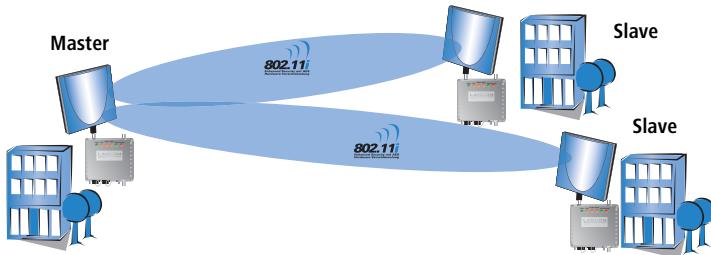
erste WLAN-Karte für die P2P-Verbindung nutzen , WLAN-2 wenn Sie die zweite Karte z.B. bei einem Access Point mit zwei WLAN-Modulen nutzen).

- 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.

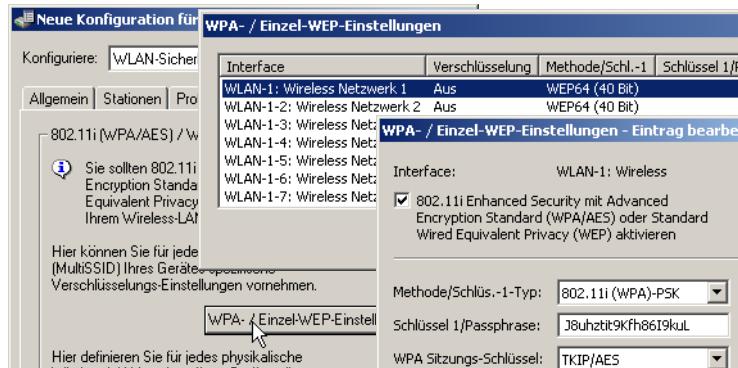
In der Einstellung als P2P-Master wird die hier eingetragene Passphrase verwendet, um die Zugangsberechtigung der Slaves zu prüfen. In der Einstellung als P2P-Slave überträgt der Access Point diese Informationen an die Gegenseite, um sich dort anzumelden.



■ Kapitel 4: Punkt- zu- Punkt- Verbindungen

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 ▶ Verschlüsselungs-Einstellungen
Terminal/Telnet	/Setup/Schnittstellen/WLAN-Schnittstellen/Verschlüsselungs-Einstellungen

4.4.2 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.



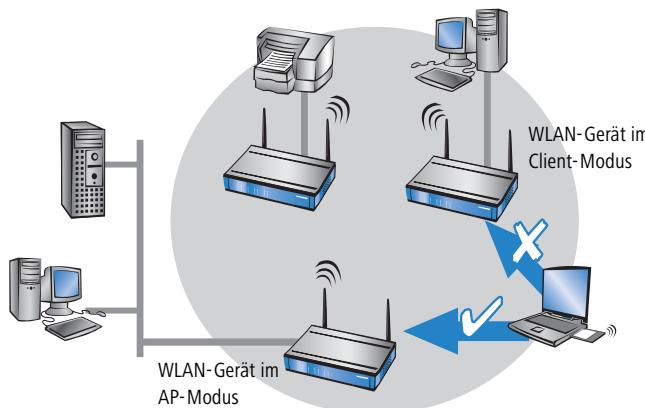
Konfiguration mit
WEBconfig oder
Telnet

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

5 Client-Modus

Zur Anbindung von einzelnen Geräten mit einer Ethernet-Schnittstelle in ein Funk-LAN können LANCOM-Geräte mit WLAN-Modul in den sogenannten Client-Modus versetzt werden, in dem sie sich wie ein herkömmlicher Funk-LAN-Adapter verhalten und nicht wie ein Access Point (AP). Über den Client-Modus ist es also möglich, auch Geräte wie PCs oder Drucker, die ausschließlich über eine Ethernet-Schnittstelle verfügen, in ein Funk-LAN einzubinden.



i Bei einem WLAN-Gerät im AP-Modus können sich weitere WLAN-Clients anmelden, bei einem WLAN-Gerät im Client-Modus jedoch nicht.

5.1 Grundkonfiguration

5.1.1 Betriebsart einstellen

LANCOM Wireless Router können grundsätzlich in zwei verschiedenen Betriebsarten arbeiten:

- Als Basisstation (Access Point) stellt es für die WLAN-Clients die Verbindung zu einem kabelgebundenen LAN her.
- Als Client sucht das Gerät selbst die Verbindung zu einem anderen Access Point und versucht sich in einem Funknetzwerk anzumelden. In diesem Fall dient das Gerät also dazu, ein kabelgebundenes Gerät über eine Funkstrecke an eine Basisstation anzubinden.



Manche Modelle können ausschließlich in der Betriebsart als WLAN-Client arbeiten. Bei diesen Geräten entfällt die Einstellung der Betriebsart.

- ① Zum Aktivieren des Client-Modus wechseln Sie unter LANconfig im Konfigurationsbereich 'Wireless LAN' auf die Registerkarte 'Allgemein'. Im Abschnitt 'Interfaces' können Sie aus der Liste der die physikalischen WLAN-Einstellungen für das gewünschte WLAN-Interface auswählen.



Je nach Modell verfügen die Geräte über ein oder mehrere WLAN-Interfaces.

- ② Auf der Registerkarte 'Betrieb' wird das WLAN-Interface aktiviert. Zusätzlich wird die WLAN-Betriebsart auf 'Client' eingestellt.



Ein WLAN-Interface kann nur auf eine der beiden Betriebsarten eingestellt werden. Der gleichzeitige Betrieb eines WLAN-Interfaces als Basisstation und Client ist nicht möglich.

Manche Modelle können nicht als Basis-Station betrieben werden, in diesem Fall ist die WLAN-Betriebsart fest auf 'Client' eingestellt.

Unter WEBconfig oder Telnet finden Sie die Einstellung der Betriebsart der physikalischen WLAN-Interfaces auf folgenden Pfaden:

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

5.1.2 Client-Einstellungen

Für LANCOM Wireless Router im Client-Modus können auf der Registerkarte 'Client-Modus' bei den Einstellungen für die physikalischen Interfaces weitere Einstellungen bzgl. des Verhaltens als Client vorgenommen werden.



- ① Zum Bearbeiten der Einstellungen für den Client-Modus wechseln Sie unter LANconfig bei den physikalischen WLAN-Einstellungen für das gewünschte WLAN-Interface auf die Registerkarte 'Client-Modus'.
- ② Stellen Sie unter 'Durchsuchte Bänder' ein, ob die Clientstation nur das 2,4 GHz-, nur das 5 GHz-Band oder alle verfügbaren Bänder absuchen soll, um eine Basisstation zu finden.

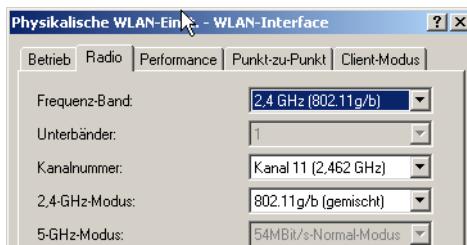
Unter WEBconfig oder Telnet finden Sie die Einstellungen für den Client-Modus auf folgenden Pfaden:

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

5.1.3 Radio-Einstellungen

Damit der WLAN-Client eine Verbindung zu einem Access Point aufbauen kann, muss er geeignete Frequenzbänder bzw. Kanäle verwenden.

- ① Zum Bearbeiten der Radio-Einstellungen wechseln Sie unter LANconfig bei den physikalischen WLAN-Einstellungen für das gewünschte WLAN-Interface auf die Registerkarte 'Radio'.



- ② Stellen Sie das Frequenz-Band, die Kanäle und den 2,4 GHz- bzw. 5 GHz-Modus passend zu den Einstellungen des Access Points ein.

i Je nach Modell entfällt die Auswahl des Frequenzbandes und der Kanäle, z.B. wenn das Gerät nur ein Frequenzband unterstützt.

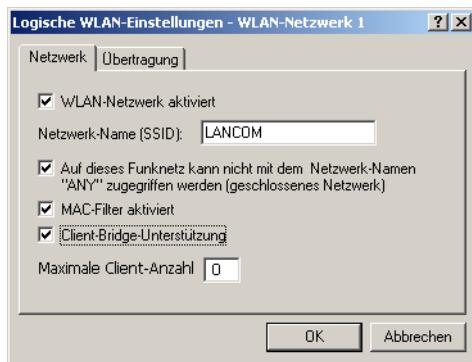
Unter WEBconfig oder Telnet finden Sie die Einstellungen für den Client-Modus auf folgenden Pfaden:

Konfigurationstool	Aufruf
LANconfig	WLAN-Interfaces ► Physikalische WLAN-Einstellungen ► Radio
WEBconfig, Telnet	Experten-Konfiguration > Setup > Schnittstellen > WLAN > Radio-Einstellungen

5.1.4 SSID der verfügbaren Netzwerke einstellen

In den WLAN-Clients müssen die SSIDs der Netzwerke eingetragen werden, zu denen sich die Clientstationen verbinden sollen.

- ① Zum Eintragen der SSIDs wechseln Sie unter LANconfig im Konfigurationsbereich 'Wireless LAN' auf die Registerkarte 'Allgemein'. Im Abschnitt 'Interfaces' wählen Sie aus der Liste der logischen WLAN-Einstellungen das **erste** WLAN-Interface aus.



- ② Aktivieren Sie das WLAN-Netzwerk und tragen Sie die SSID des Netzwerks ein, bei dem sich die Clientstation einbuchen soll.

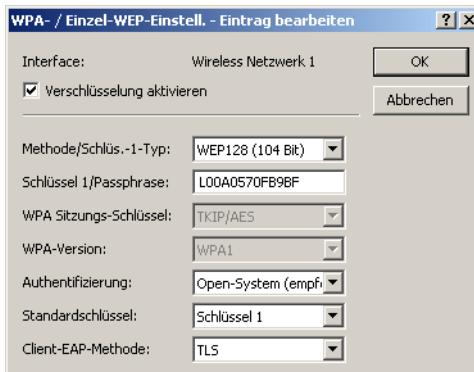
Unter WEBconfig oder Telnet finden Sie die Netzwerk-Einstellungen für die logischen WLAN-Interfaces auf folgenden Pfaden:

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

5.1.5 Verschlüsselungseinstellungen

Für den Zugriff auf ein WLAN müssen in der Clientstation die entsprechenden Verschlüsselungsmethoden und Schlüssel eingestellt werden.

- ① Zum Eintrage der Schlüssel wechseln Sie unter LANconfig im Konfigurationsbereich 'Wireless LAN' auf die Registerkarte '802.11i/WEP'. Im Abschnitt 'WPA- / Einzel-WEP-Einstellungen' wählen Sie aus der Liste der logischen WLAN-Einstellungen das **erste** WLAN-Interface aus



- ② Aktivieren Sie die Verschlüsselung und passen Sie die Verschlüsselungsmethode an die Einstellungen des Access Points an.
- ③ LANCOM Wireless Router in der Betriebsart als WLAN-Client können sich über EAP/802.1X bei einem anderen Access Point authentifizieren. Wählen Sie dazu hier die gewünschte Client-EAP-Methode aus. Beachten Sie, dass die gewählte Client-EAP-Methode zu den Einstellungen des Access Points passen muss, bei dem sich der LANCOM Wireless Router einbuchen will.

Unter WEBconfig oder Telnet finden Sie die Netzwerk-Einstellungen für die logischen WLAN-Interfaces auf folgenden Pfaden:

Konfigurationstool	Aufruf
WEBconfig, Telnet	Experten-Konfiguration > Setup > Schnittstellen > WLAN > Verschlüsselung > WLAN-1

5.2 Erweiterte Konfiguration

5.2.1 Roaming

Mit Roaming bezeichnet man den Übergang eines WLAN-Clients zu einem anderen Access Point, wenn er keine Verbindung zum bisherigen Access Point mehr aufrecht erhalten kann. Um das Roaming zu ermöglichen, muss sich mindestens ein weiterer Access Point in der Reichweite des Clients befinden, der ein Netzwerk mit der gleichen SSID und den passenden Radio- und Verschlüsselungs-Einstellungen anbietet.

Normalerweise würde der WLAN-Client sich nur dann bei einem anderen Access Point einbuchen, wenn er die Verbindung zu dem bisherigen Access Point vollständig verloren hat (Hard-Roaming). Das Soft-Roaming ermöglicht dem Client hingegen, anhand verfügbarer Scan-Informationen ein Roaming zu einem stärkeren Access Point durchzuführen. Mit der Funktion des Background-Scanning kann der LANCOM Wireless Router im Client-Modus schon vor Verbindungsverlust Informationen über andere verfügbare Access Points sammeln. Die Umschaltung auf einen anderen Access Point erfolgt dann nicht erst, wenn die bisherige Verbindung vollständig verloren wurde, sondern wenn ein anderer Access Point in Reichweite über ein stärkeres Signal verfügt.

- ① Zum Aktivieren des Soft-Roaming wechseln Sie unter WEBconfig oder Telnet in den Bereich Setup > Schnittstellen > WLAN > Roaming und wählen dort das physikalische WLAN-Interface.
- ② Schalten Sie das Soft-Roaming ein und stellen Sie ggf. die weiteren Parameter wie die Schwellwerte und Signalpegel ein. Weitere Informationen zu diesen Parametern finden Sie im Referenz-Handbuch.
- ③ Zur Konfiguration des Background-Scanning wechseln Sie unter LANconfig bei den physikalischen WLAN-Einstellungen für das gewünschte WLAN-Interface auf die Registerkarte 'Radio'.



- ④ Tragen Sie als Background-Scan-Intervall die Zeit ein, in welcher der LANCOM Wireless Router zyklisch die aktuell ungenutzten Frequenzen des aktiven Bandes nach erreichbaren Access Points absucht. Um ein schnelles Roaming zu erzielen, wird die Scan-Zeit auf z.B. mindestens 260 Sekunden (2,4 GHz) bzw. mindestens 720 Sekunden (5 GHz) beschränkt.

Unter WEBconfig oder Telnet finden Sie die Netzwerk-Einstellungen für die logischen WLAN-Interfaces auf folgenden Pfaden:

Konfigurationstool	Aufruf
LANconfig	WLAN-Interfaces ► Physikalische WLAN-Einstellungen ► Radio
WEBconfig, Telnet	Experten-Konfiguration > Setup > Schnittstellen > WLAN > Radio-Einstellungen

5.2.2 Weitere optionale Parameter

In den Einstellungen für den Client-Modus (unter LANconfig bei den physikalischen WLAN-Einstellungen für das gewünschte WLAN-Interface auf der Registerkarte 'Client-Modus') stellen Sie **optional** die folgenden Parameter ein:

■ Netzwerktypen

Mit der Auswahl der 'Netzwerktypen' wird festgelegt, ob sich die Station nur an Infrastruktur- oder auch in Adhoc-Netzwerken anmelden darf.



Manche Modelle können sich nicht bei Adhoc-Netzwerken anmelden, in diesem Fall ist die Auswahl der Netzwerktypen fest auf 'Infrastruktur' eingestellt.

■ IBBS erzeugen

Wenn diese Option aktiviert ist, kann das WLAN-Gerät selbst ein IBBS (Independent Basic Service Set), also ein Adhoc-Netzwerk aufbauen. Diese Option ist nur verfügbar, wenn die Verbindung zu Adhoc-Netzwerken erlaubt ist.

■ Client-Verbindung aufrecht erhalten

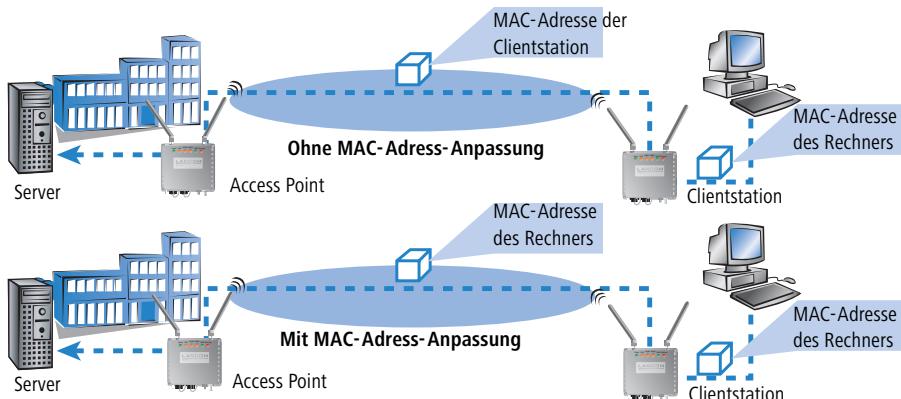
Mit dieser Option hält die Client-Station die Verbindung zur Basisstation aufrecht, auch wenn von den angeschlossenen Geräten keine Datenpakete gesendet werden. Ist diese Option ausgeschaltet, wird die Clientstation automatisch aus dem Funknetzwerk abgemeldet, wenn für eine bestimmte Zeit keine Pakete über die WLAN-Verbindung fließen.

■ Bevorzugte BSS-ID

Wenn sich die Clientstation nur bei einem bestimmten Access Point einbuchen soll, können Sie hier die MAC-Adresse der WLAN-Karte aus diesem Access Point eintragen.

■ Adress- Anpassung

Im Client-Modus ersetzt die Clientstation üblicherweise die MAC-Adressen in den Datenpaketen der an ihr angeschlossenen Geräte durch die eigene MAC-Adresse. Der Access-Point auf der anderen Seite der Verbindung „sieht“ also immer nur die MAC-Adresse der Clientstation, nicht jedoch die MAC-Adresse der oder des angeschlossenen Rechners.



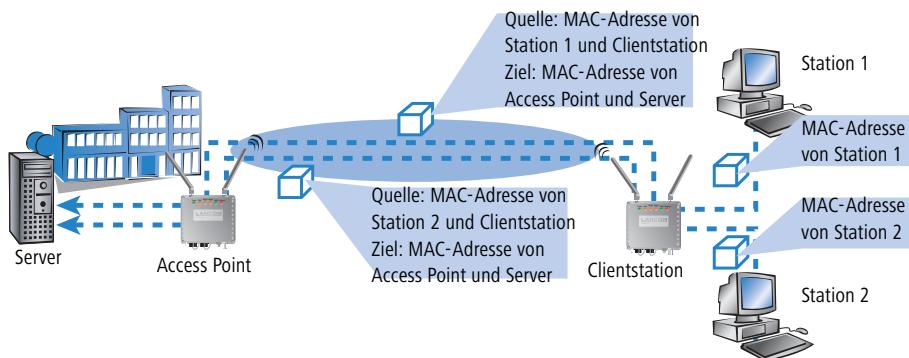
In manchen Installationen ist es jedoch gewünscht, dass die MAC-Adresse eines Rechners und nicht die der Clientstation an den Access Point übertragen wird. Mit der Option 'Adress- Anpassung' wird das Ersetzen der MAC-Adresse durch die Clientstation unterbunden, die Datenpakete werden mit der originalen MAC-Adresse übertragen.



Die Adress- Anpassung funktioniert nur, wenn an die Clientstation nur **ein** Rechner angeschlossen ist!

■ Client- Bridge- Unterstützung

Während mit der Adress- Anpassung nur die MAC-Adresse eines **einzigem** angeschlossenen Gerätes für den Access Point sichtbar gemacht werden kann, werden über die Client-Bridge-Unterstützung alle MAC-Adressen der Stationen im LAN hinter der Clientstationen transparent an den Access Point übertragen.



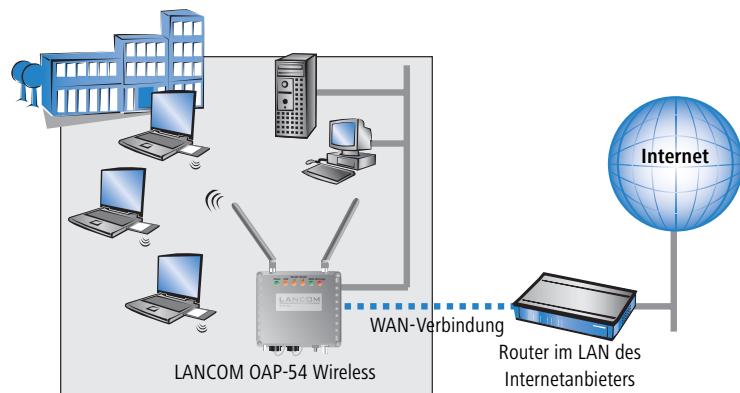
Dazu werden in dieser Betriebsart nicht die beim Client-Modus üblichen drei MAC-Adressen verwendet (in diesem Beispiel für Server, Access Point und Clientstation), sondern wie bei Punkt-zu-Punkt-Verbindungen vier Adressen (zusätzlich die MAC-Adresse der Station im LAN der Clientstation). Die voll-transparente Anbindung eines LANs an der Clientstation ermöglicht die gezielte Übertragung der Datenpakete im WLAN und damit Funktionen wie TFTP-Downloads, die über einen Broadcast angestoßen werden.



Der Client-Bridge-Modus kann ausschließlich zwischen zwei LANCOM-Geräten verwendet werden. Die Verwendung des Client-Bridge-Modus muss in den Einstellungen für das logische Netzwerk des Access Points ebenfalls aktiviert werden.

6 Den Internet-Zugang einrichten

Über den zentralen Internet-Zugang des LANCOM erhalten alle Rechner im LAN Zugriff auf das Internet. Die Verbindung zum Internetanbieter kann über den WAN-Anschluss aufgebaut werden, der an ein ADSL- oder Kabel-Modem angeschlossen wird.



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

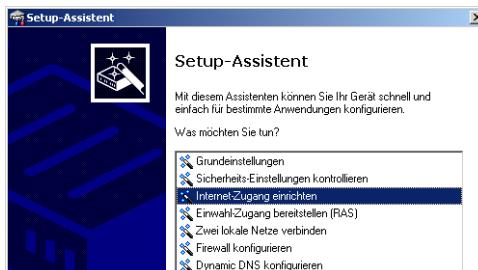
Zusätzlich können Sie (sofern von Ihrem Internetanbieter unterstützt) zusätzliche Optionen im Assistenten ein- oder ausschalten:

- 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.

6.1 Anleitung für LANconfig

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



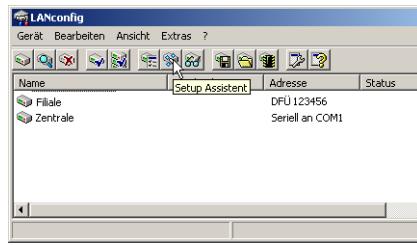
- ② Wählen Sie im Auswahlmenü den Setup-Assistenten **Internet-Zugang einrichten** und bestätigen Sie die Auswahl mit **Weiter**.
- ③ In den folgenden Fenstern wählen Sie Ihr Land, nach Möglichkeit Ihren Internetanbieter, und geben Sie die Zugangsdaten ein.
- ④ Je nach Verfügbarkeit bietet Ihnen der Assistent weitere Optionen für die Internetverbindung zur Auswahl an.

■ Kapitel 6: Den Internet-Zugang einrichten

- 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.



6.2 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.

7 Sicherheits- Einstellungen

Ihr LANCOM Router verfügt über zahlreiche Sicherheitsfunktionen. In diesem Kapitel finden Sie alle Informationen, die Sie für eine optimale Absicherung des Access Points 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:

- 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 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.

7.1.2 Zugangskontrolle über MAC-Adresse

Jedes Netzwerkgerät verfügt über eine unverwechselbare Identifizierungsnummer. Diese Identifizierungsnummer wird als MAC-Adresse (**Media Access Control**) 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 (LANCOM Enhanced Passphrase Security) 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-Adaptoren, 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, WPA 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 63) oder aber eine zusätzliche Verschlüsselung der WLAN-Verbindung einrichten, wie sie auch für VPN-Tunnel verwendet wird ('IPSec-over-WLAN' → Seite 63). 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“.

Standard-WEP-Verschlüsselung

Ab Werk wird für jedes unkonfigurierte Gerät standardmäßig eine WEP128-Verschlüsselung aktiviert.

Der Schlüssel setzt sich aus dem Anfangsbuchstaben „L“ gefolgt von der LAN-MAC-Adresse des Access Points in ASCII-Schreibweise 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 einge tragen 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 Extensible Authentication Protocol (EAP) ermöglichen Access Points die Durchführung einer zuverlässigen und sicheren Zugangskontrolle. Die Zugangsdaten können zentral auf einem RADIUS-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 ist eine Basisstation mit VPN-Unterstützung und der LANCOM Advanced VPN Client erforderlich, welcher unter den Betriebssystemen Windows 98ME, Windows 2000 und Windows XP 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.

■ Kapitel 7: Sicherheits- Einstellungen

■ 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.

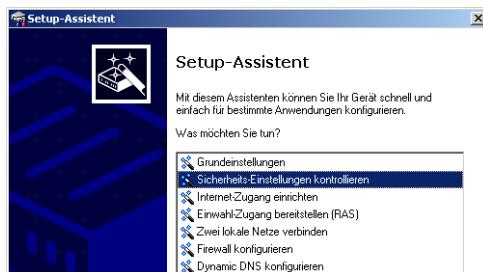
Ihr LANCOM Router verfügt über einen Kennwortschutz für den Konfigurationszugang. Dieser wird schon während der Grundkonfiguration durch Angabe eines Kennwertes aktiviert.

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 Fehlversuch 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 Router im Auswahlfenster. Wählen Sie aus der Befehlsleiste den Punkt **Extras ▶ Setup Assistant**.



- 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 Netzwerken
- 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

Der LANCOM Router verfügt über eine Stateful-Inspection-Firewall und Firewall-Filter zur wirksamen Absicherung Ihres WLAN gegenüber dem Internet.

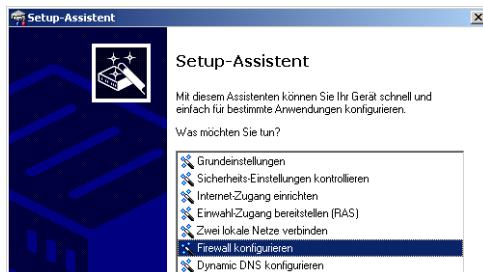
Kernidee der Stateful-Inspection-Firewall ist, dass nur selbstinitiiert Datentransfer als zulässig betrachtet wird. Alle Zugriffe, die unaufgefordert nicht aus dem lokalen Netz heraus erfolgen, sind unzulässig.

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

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

7.4.1 Assistent für LANconfig

- 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 **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 ▶ Regelabelle** 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 'Security'. 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'.

■ 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 aktiver 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

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 Routers.

■ Kapitel 7: Sicherheits- Einstellungen

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-Netzwerkarten. 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 sensible 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 'Benutzer-Anmeldung'.

■ 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 Gerät-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).

■ **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.

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:

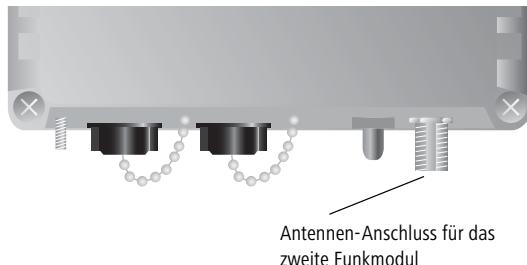
- AirLancer Extender O-D80g (2,4 GHz-Band), Art.Nr. 61221
- AirLancer Extender O-D60a (5 GHz Band), Art.Nr. 61222

Zur Installation von optionalen AirLancer Extender-Antennen schalten Sie den LANCOM Wireless Router aus, indem sie das LAN-Kabel der Spannungsversorgung aus dem Gerät herausziehen. Schrauben Sie dann vorsichtig die beiden Diversity-Antennen an der Oberseite des Gerätes ab (erstes Funkmodul). Schließen Sie die AirLancer Extender-Antenne an den 'Antenna Main'-Antennenanschluss an.



Zwischen die Anschlüsse des LANCOM OAP-54 Wireless und die anzuschließenden AirLancer Extender-Antennen muss in den meisten Fällen noch ein Adapterkabel von „Reverse-N“ auf „N“ geschraubt werden. Mit diesem Adapterkabel ist der Anschluss aller AirLancer Extender-Antennen und vieler Fremdprodukte möglich.

Außerdem können Sie eine zusätzliche Antenne auch an das zweite Funkmodul anschliessen.



Für den Relaisbetrieb schliessen Sie sowohl an das erste wie auch das zweite Funkmodul eine entsprechende AirLancer Extender-Antenne an.

Mit dem LANCOM OAP-54 Wireless können Sie die „Tx-Diversity“-Funktion auch über den AUX-Anschluss des ersten Funk-Moduls nutzen. Weitere Informationen finden Sie im LCOS-Referenzhandbuch.

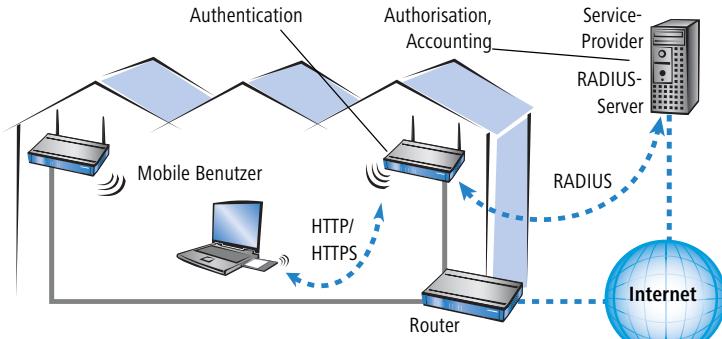
8.2 LANCOM Public Spot Option

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 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.



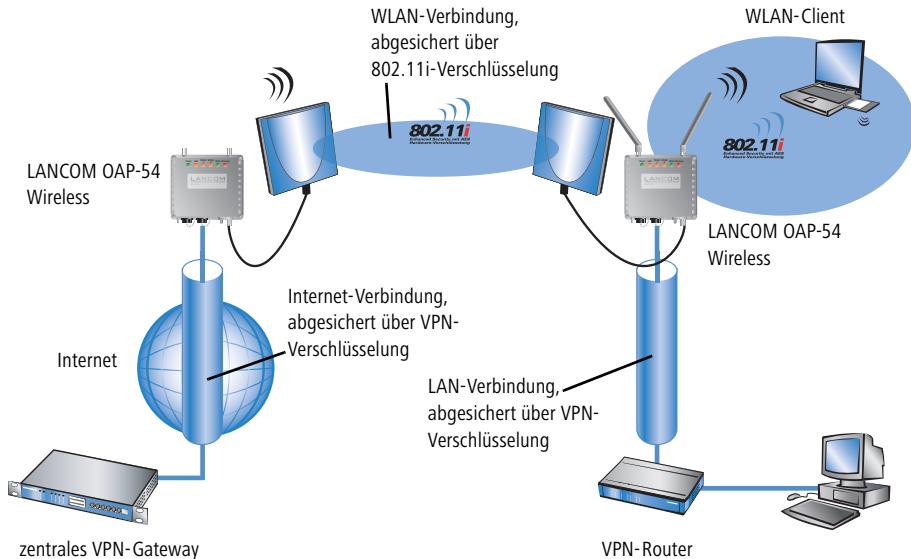
Mit der LANCOM Public Spot Option erweitern Sie einen Access Point nachträglich um diese Funktionen und rüsten sie zum Wireless Public Spot auf.

LANCOM VPN Option Mit der LANCOM VPN Option rüsten Sie Ihr Gerät nachträglich zum VPN-Gateway mit Hardwareverschlüsselung auf. In Verbindung mit der so möglichen VPN-Verschlüsselung können Sie für jede denkbare Verbindung die optimale Sicherheit einrichten:

- VPN-Verschlüsselung für WAN-Verbindungen, z. B. über das Internet
- VPN-Verschlüsselung auch für LAN-Verbindungen, um Daten auch gegen den Zugriff von Mithörern mit physikalischem Zugang zum Übertragungsmedium (z. B. zum LAN-Kabel) abzuschirmen
- 802.11i-Verschlüsselung für Punkt-zu-Punkt-WLAN-Strecken
- 802.11i-Verschlüsselung zur Anbindung von mobilen WLAN-Clients

Mit diesem Funktionen kann auch in einem Szenario mit hohen Sicherheitsanforderungen die komplette Datenstrecke über mehrere Zwischenpunkte hinweg zuverlässig abgesichert werden.

DE



Weitere Informationen über die VPN-Funktionen und die Konfiguration finden Sie in der Dokumentation zur LANCOM VPN Option und im LCOS Referenzhandbuch.

9 Rat & Hilfe

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

9.1 Es wird keine DSL-Verbindung aufgebaut

DE

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

Probleme an der Verkabelung?

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

9.2 DSL-Übertragung langsam

Die Übertragungsgeschwindigkeit einer (Internet-) DSL-Verbindung hängt von zahlreichen Faktoren ab, von denen die meisten außerhalb des eigenen Einflussbereiches liegen: Entscheidend sind neben der Bandbreite der eigenen Internet-Anbindung beispielsweise auch die Internet-Anbindung und Auslas-

tung 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).

9.3 Unerwünschte Verbindungen mit Windows XP

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

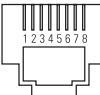
LANCOM OAP-54 Wireless		
Frequenzband		Zwei WLAN-Module mit jeweils 2400 - 2483,5 MHz (ISM) oder 5150 - 5750 MHz
Anschlüsse	LAN	10/100Base-TX, Autosensing, Auto Node-Hub
	WAN	10/100Base-TX, Autosensing, Auto Node-Hub
	WLAN1	2x Reverse N-Buchse mit Antenna Diversity
	WLAN2	1x Reverse N-Buchse
Stromversorgung		Ausschließlich über Power-over-Ethernet. Ein PoE Injector im Lieferumfang.
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
Adapterkabel		3 Reverse N to N Adapterkabel im Lieferumfang für den Anschluß aller AirLancer Extender Outdoor Antennen oder Antennen anderer Hersteller.
Gehäuse		235 mm x 210 mm x 80 mm (B x H x T), 3,4kg, robustes Metallgehäuse, IP66 Strahlwasserfest, für Wand-, Mast- und Hutschienenmontage vorbereitet, 6 LED zur Status-Signalisierung.
Normen		CE-konform nach ETSI EN 300 328, ETSI EN 301 893, ETSI EN 301 489-1, ETSI EN 301 489-17, EN 60950
Zulassungen		Notifiziert in den Ländern Deutschland, Belgien, Niederlande, Luxemburg, Österreich, Schweiz, Großbritannien, Italien, Frankreich, Tschechien, Dänemark
Umgebung/Temperatur		–30 °C bis +70 °C bei 95 % max. Luftfeuchtigkeit (nicht kondensierend). Mit interner Heizung/Kühlung. Einschaltverzögerung bei Temperaturen unter 0°C durch Aufheizung berücksichtigen.
Service		Garantie 3 Jahre
Support		Über Hotline und Internet

10.2 Anschlussbelegung

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

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

DE

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

10.3 CE-Konformitätserklärungen



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

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

Index

Numerics			
100-Mbit-Netz	18	Firewall	10, 12, 68
802.11i	11, 59, 60, 61, 65, 69	Stationen sperren	68
802.11i/	61	Firewall-Filter	65
802.1x	11, 59, 61, 63	FirmSafe	12
		Firmware	4
		Flatrate	56
A		Frequenz-Band	49
Access Control List	60	Funk-LANs	
ACL	60	Betriebsarten	10
AES	61		
Anschlussbelegung	80	G	
LAN-Schnittstelle	80	Gebührenschutz	29, 31, 35
Antennen		Gebührenschutz zurücksetzen	17
Dualband	14	Gebührensperrre	17
Autosensing	18		
B		H	
Background-Scanning	52	Hard-Roaming	52
		Hinweis-Symbole	5
C			
Client-Modus	46, 48	I	
Closed Network	59	IBBS	53
		ICMP	68
D		Installation	14
Default-Gateway	68	LANtools	24
DHCP	36	Internet-Anbieter	56
DHCP-Server	10, 27, 34, 36	Internet-Zugang	10, 56
DNS		Authentifizierungsdaten	56
DNS-Server	10, 36	Flatrate	56
Dokumentation	14		
Download	4	IP	
DSL-Übertragung zu langsam	77	Filter	68
DSL-Übertragungsprotokoll	35	Ports sperren	68
DSL-Verbindung		IP-Adresse	27, 28, 69
Probleme beim Aufbau	77	IP-Masquerading	12, 68
		IP-Router	10
E		IPSec-over-WLAN	59
EAP	11, 59, 63		
F		K	
Fernkonfiguration	31, 35	Kennwort	28, 31
		Konfigurationsdatei	69
		Konfigurationskennwort	67

■ Index

DE

Konfigurationsschutz	28	Reset-Schalter	20
Konfigurationszugriff	31, 35	Roaming	51
Konformitätserklärungen	80	Routing-Tabelle	68
L			
LAN		S	
Anschlusskabel	14	Internet-Zugriff	59
LANCOM Enhanced Passphrase Security	59	Schutz der Konfiguration	59
LANCOM Public Spot Option	74	Sicherheits-Checkliste	67
LANconfig	25, 30	Sicherheits-Einstellungen	77
Assistenten aufrufen	58	SNMP	
LANmonitor	25	Konfiguration schützen	67
LANtools		Soft-Roaming	52
Systemvoraussetzungen	15	Software-Installation	24
LEPS	11, 60, 69	SSID	28, 31, 34, 49
M			
MAC-Adresse	62	Standard-Gateway	36
MAC-Adressfilter	11	Stateful Inspection Firewall	10
Montagematerial	14	Stateful-Inspection-Firewall	65
Multi SSID	11	Statusanzeigen	
Multimode	35	Message	17
N			
NAT – siehe IP-Masquerading		Power	16
NetBIOS-Proxy	10	Wireless Link	16, 17
Netzmaske	27, 28, 69	Super AG	11
O			
Optionale Antennen	72	Support	4
Optionen und Zubehör	72	Systemvoraussetzungen	15
P			
P2P	60	T	
PAT – siehe IP-Masquerading		TCP	68
PoE Power Injector	14	TCP/IP	15
Point-to-Point	10, 60	Einstellungen	26, 34
Power-over-Ethernet	19	TCP/IP-Filter	12, 68
R			
RADIUS	63	TCP/IP-Konfiguration	
Relais-Modus	10	automatisch	34
Reset	62	manuell	26, 28
		vollautomatisch	26, 27
		TCP/IP-Windows-Size	78
		Technische Daten	79
		Telnet	69
		TFTP	69
		Turbo Modus	11

U			
Übertragungsprotokoll	77	Bevorzugte BSS-ID	54
UDP	68	Client-Bridge-Unterstützung	54
V		Client-Modus	48
Verschlüsselungsmethode	50	Client-Verbindung aufrecht erhalten	
		53	
W		Durchsuchte Bänder	48
WEBconfig	31	IBBS	53
Aufruf eines Assistenten	33	Netzwerktypen	53
Kennworteingabe	35	Radio-Einstellungen	48
Systemvoraussetzungen	15	WLAN-Betriebsart	47
WEP	11, 59, 61, 62, 63, 64, 65, 69	WPA	11, 59, 60, 61, 65, 69
WLAN			
Adress-Anpassung	54	Zugang zum Internet einrichten	56
z			