



. . . c o n n e c t i n g   y o u r   b u s i n e s s

# LANCOM IAP-54 Wireless LANCOM XAP-40-2 LANCOM XAC-40-1

- Handbuch
- Manual

**LANCOM IAP-54 Wireless**  
**LANCOM XAP-40-2**  
**LANCOM XAC-40-1**

© 2008 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 wurde (<http://www.openssl.org/>).

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

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

Produkte von LANCOM Systems enthalten das LZMA SDK, das von Igor Pavlov entwickelt wurde.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

[www.lancom.de](http://www.lancom.de)

Würselen, Juli 2008

# Ein Wort vorab

## Vielen Dank für Ihr Vertrauen!

Die Modelle LANCOM XAP-40-2, LANCOM XAC-40-1 und LANCOM IAP-54 Wireless bieten professionelle WLAN-Technologie und ein Maximum an Performance.

## Modellvarianten

Diese Dokumentation wendet sich an Anwender der folgenden LANCOM WLAN-Produkte:

- Das LANCOM IAP-54 Wireless arbeitet wahlweise nach dem 802.11g-Standard im 2,4 GHz-Band oder nach dem 802.11a-Standard im 5 GHz-Band. Es ist durch ein besonderes Gehäuse (IP50) für den Einsatz im industriellen Umfeld wie z.B. in Warenhäusern, Lagern oder Produktionshallen vorgesehen.
- Das LANCOM XAP-40-2 arbeitet mit zwei integrierten 108 MBit/s Funkmodulen nach den WLAN Standards IEEE 802.11a/h oder IEEE 802.11b/g auch gleichzeitig im 2,4 und/oder 5 GHz Frequenzbereich. Es ist in einem Industrie-Gehäuse für die Montage im Schaltschrank untergebracht und wird über eine 24 V-Spannung versorgt. Egal ob in Infrastruktur-Netzwerken oder zur Netzwerkkopplung als WLAN Bridge, es sind den Einsatzmöglichkeiten des LANCOM XAP-40-2 keine Grenzen gesetzt.
- Der Wireless LAN Client LANCOM XAC-40-1 ist die ideale Ergänzung zu den WLAN-Basisstationen von LANCOM. Der Client kann als Abschluss einer WLAN-Funkstrecke eingesetzt werden, beispielsweise um eine stationäre oder mobile Netzanbindung herzustellen. Er arbeitet dabei als transparenter WLAN-to-Ethernet-Umsetzer und ist für den Einsatz in rauen Umgebungsbedingungen geeignet. Der LANCOM XAC-40-1 bietet umfangreichste Sicherheits- und QoS-Funktionen sowie schnelle Roaming-Verfahren, um jederzeit eine verlässliche Verbindungsqualität zu gewährleisten.

Modell-  
Einschränkungen

Die Teile der Dokumentation, die nur für ein bestimmtes Modell gelten, sind entweder im Text selbst oder durch entsprechende seitliche Hinweise gekennzeichnet.

In den anderen Teilen der Dokumentation werden alle beschriebenen Modelle unter dem Sammelbegriff LANCOM zusammengefasst.

## Sicherheitseinstellungen

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

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

## Benutzerhandbuch und Referenzhandbuch

Die Dokumentation Ihres Gerätes besteht aus folgenden Teilen:

- Installation Guide
- Benutzerhandbuch
- Referenzhandbuch

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

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

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

## An der Erstellung dieser Dokumentation ...

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

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

<b>1 Einleitung</b>	<b>9</b>
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?	10
<b>2 Installation</b>	<b>14</b>
2.1 Lieferumfang	14
2.2 Systemvoraussetzungen	15
2.2.1 Konfiguration der LANCOM-Geräte	15
2.2.2 Betrieb der Access Points im Managed-Modus	15
2.3 Statusanzeigen, Schnittstellen und Installation der Hardware	15
2.3.1 LANCOM XAP-40-2 und LANCOM XAC-40-1	16
2.3.2 LANCOM IAP-54 Wireless	26
2.4 Installation der Software	31
2.4.1 Software-Setup starten	31
2.4.2 Welche Software installieren?	32
<b>3 Grundkonfiguration</b>	<b>33</b>
3.1 Welche Angaben sind notwendig?	33
3.1.1 TCP/IP-Einstellungen	34
3.1.2 Konfigurationsschutz	36
3.1.3 Einstellungen für das Funk-LAN	36
3.2 Anleitung für LANconfig	37
3.3 Anleitung für WEBconfig	39
3.4 TCP/IP-Einstellungen an den Arbeitsplatz-PCs	44
<b>4 Sicherheits-Einstellungen</b>	<b>45</b>
4.1 Sicherheit im Funk-LAN	45
4.1.1 SSID Broadcast unterdrücken – geschlossenes Netzwerk	

(Closed Network)	45
4.1.2 Zugangskontrolle über MAC-Adresse	46
4.1.3 LANCOM Enhanced Passphrase Security	46
4.1.4 Verschlüsselung des Datentransfers	47
4.1.5 802.1x / EAP	47
4.1.6 IPSec-over-WLAN	48
4.2 Tipps für den richtigen Umgang mit Schlüsseln und Passphrases	48
4.3 Der Sicherheits-Assistent	49
4.3.1 Assistent für LANconfig	49
4.3.2 Assistent für WEBconfig	50
4.4 Die Sicherheits-Checkliste	50
<b>5 Erweiterte WLAN-Konfiguration</b>	<b>55</b>
5.1 WLAN-Konfiguration mit dem Assistenten von LANconfig	55
5.2 Punkt-zu-Punkt-Verbindungen	57
5.2.1 Geometrische Auslegung von Outdoor-Funknetz-Strecken	58
5.2.2 Ausrichten der Antennen für den P2P-Betrieb	62
5.3 Konfiguration der P2P-Verbindungen	65
5.3.1 Access Points im Relais-Betrieb	67
5.3.2 Sicherheit von Punkt-zu-Punkt-Verbindungen	68
5.4 Client-Modus	70
5.4.1 Client-Einstellungen	72
5.4.2 SSID der verfügbaren Netzwerke einstellen	72
5.4.3 Verschlüsselungseinstellungen	73
<b>6 Den Internet-Zugang einrichten</b>	<b>75</b>
6.1 Der Internet-Assistent	76
6.1.1 Anleitung für LANconfig	76
6.1.2 Anleitung für WEBconfig	77
6.2 Der Firewall-Assistent	77
6.2.1 Assistent für LANconfig	78
6.2.2 Konfiguration unter WEBconfig	78



<b>7 Optionen und Zubehör</b>	<b>79</b>
7.1 Optionale AirLancer Extender Antennen	79
7.1.1 Antenna Diversity	80
7.1.2 Installation der AirLancer Extender Antennen	80
7.2 LANCOM Public Spot Option	82
<b>8 Rat &amp; Hilfe</b>	<b>83</b>
8.1 Es wird keine DSL-Verbindung aufgebaut	83
8.2 DSL-Übertragung langsam	83
8.3 Unerwünschte Verbindungen mit Windows XP	84
<b>9 Anhang</b>	<b>85</b>
9.1 Leistungs- und Kenndaten	85
9.2 Anschlussbelegung	86
9.2.1 LAN-Schnittstelle 10/100Base-TX, DSL-Schnittstelle	86
9.2.2 Konfigurationsschnittstelle (Outband)	87
9.3 CE-Konformitätserklärungen	87
<b>10 Index</b>	<b>88</b>

# 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)
- 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?

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

	LANCOM IAP-54 Wireless	LANCOM XAP-40-2	LANCOM XAC-40-1
<b>Betriebsarten</b>			
Point-to-Point-Modus (pro WLAN-Schnittstelle sechs P2P-Strecken definierbar)	✓	✓	
Access-Point-Modus	✓	✓	
Client-Modus	✓	✓	✓
Relais-Funktion zur Verbindung zweier P2P-Strecken untereinander		✓	
Managed-Modus zur zentralen Konfiguration der WLAN-Module durch einen WLAN-Controller	✓	✓	
IP-Router	✓	✓	

	LANCOM IAP-54 Wireless	LANCOM XAP-40-2	LANCOM XAC-40-1
<b>Anwendungen</b>			
Industrie-Betrieb im IP50-geschützten Gehäuse für Wand- Pfosten- oder Hutschienenmontage	✓		
Industrie-Betrieb im kompakten Gehäuse für Schaltschrank mit Hutschienenmontage und 24 V-Stromversorgung (erweiterter Temperaturbereich)		✓	✓
Internet-Zugang	✓	✓	
Stateful Inspection Firewall	✓	✓	
DHCP- und DNS-Server (für LAN)	✓	✓	✓
DHCP- und DNS-Client (für WAN)	✓	✓	
Advanced Routing and Forwarding (ARF-Netze)	8	8	
N:N-Mapping zum Routen von Netzwerken mit den gleichen IP-Adresskreisen	✓	✓	✓
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	✓	✓	✓
<b>WLAN</b>			
Funkübertragung nach IEEE 802.11g und IEEE 802.11b	✓	✓	✓
Funkübertragung nach IEEE 802.11a und IEEE 802.11h	✓	✓	✓
Turbo Modus: Bandbreitenverdopplung im 2,4 GHz- und 5 GHz-Bereich	✓	✓	✓
Super AG inkl. Hardware-Compression und Bursting	✓	✓	✓
Multi SSID	✓	✓	
Roaming-Funktion	✓	✓	Nur als Client

## ■ Kapitel 1: Einleitung

	LANCOM IAP-54 Wireless	LANCOM XAP-40-2	LANCOM XAC-40-1
802.11i / WPA mit Hardware-AES-Verschlüsselung	✓	✓	✓
WEP-Verschlüsselung (bis 128 Bit Schlüssellänge, WEP152)	✓	✓	✓
IEEE 802.1x/EAP Authenticator und Supplicant im Client Mode	✓	✓	
IEEE 802.1x/EAP nur Supplicant im Client Mode			✓
MAC-Adressfilter (ACL)	✓	✓	
Individuelle Passphrases pro MAC-Adresse (LEPS)	✓	✓	
Closed-Network-Funktion	✓	✓	
Integrierter RADIUS-Server	✓	✓	
VLAN	✓	✓	✓
Intra-Cell-Blocking	✓	✓	
QoS für WLAN (IEEE 802.11e, WMM/WME)	✓	✓	✓
<b>Anschluss ans LAN</b>			
Fast-Ethernet-Anschluss (10/100Base-TX)	✓	2	1
Power-over-Ethernet (PoE)	✓	2-fach	1-fach
DHCP- und DNS-Server	✓	✓	✓
<b>WAN-Anschlüsse</b>			
Anschluss für DSL-Modem (DSLolL)	✓	✓	✓
<b>Internet-Zugang (IP-Router)</b>			
Stateful-Inspection Firewall	✓	✓	✓
Firewall-Filter (Adresse, Port)	✓	✓	✓
IP-Masquerading (NAT, PAT)	✓	✓	✓
Quality of Service	✓	✓	✓
<b>Stromversorgung</b>			
Power-over-Ethernet (PoE) IEEE 802.3af	✓	2-fach, zueinander redundant	✓
12 V über separates Netzteil (DC)		✓	✓

	LANCOM IAP-54 Wireless	LANCOM XAP-40-2	LANCOM XAC-40-1
24 V (DC) über Industrieschnittstelle		2-fach, zueinander redundant	2-fach, zueinander redundant
Redundante Stromversorgung über PoE, 12 V oder 24 V		✓	✓
<b>Konfiguration und Firmware</b>			
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 des WLANs mit Rogue AP Detection	✓	✓	
<b>Optionale Software-Erweiterungen</b>			
LANCOM Public Spot Option	✓	✓	
LANCOM Service-Option	✓	✓	✓
<b>Optionale Hardware-Erweiterungen</b>			
AirLancer Extender Antennen zur Reichweitenerhöhung	✓	✓	✓
LANCOM Modem Adapter Kit zum Anschluss eines Analog- oder GSM-Modems an die serielle Schnittstelle		✓	✓
<b>Gehäuse</b>			
IP50-geschütztes Gehäuse für den industriellen Einsatz	✓		
IP40-geschütztes Gehäuse für den Einsatz im Schaltschrank		✓	✓

## 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 IAP-54 Wireless	LANCOM XAP-40-2	LANCOM XAC-40-1
12 V DC Steckernetzteil		✓	✓
Anschraubbare externe Dualband-Antennen	2	2	2
Reverse-SMA-Terminatoren zur Vermeidung von Einstrahlungen bei nicht genutzten Antennen-Anschlüssen		2	1
4-poliger 24 V-Stecker zur eigenen Konfektionierung		✓	✓
Anschlusskabel für die serielle Konfigurationsschnittstelle		✓	✓
Montagematerial für Wand und Mast	✓		
Montagematerial für Wand und Hutschiene	✓	✓	✓
PoE-LAN-Kabel (grüne Stecker)	✓	✓	✓
1 PoE Port Injektor (nicht in der Bulk-Version enthalten)	✓		
LANCOM-CD	✓	✓	✓
Gedruckte Dokumentation	✓	✓	✓

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

## 2.2 Systemvoraussetzungen

### 2.2.1 Konfiguration der LANCOM-Geräte

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

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

### 2.2.2 Betrieb der Access Points im Managed-Modus

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



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

## 2.3 Statusanzeigen, Schnittstellen und Installation der Hardware

### 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.

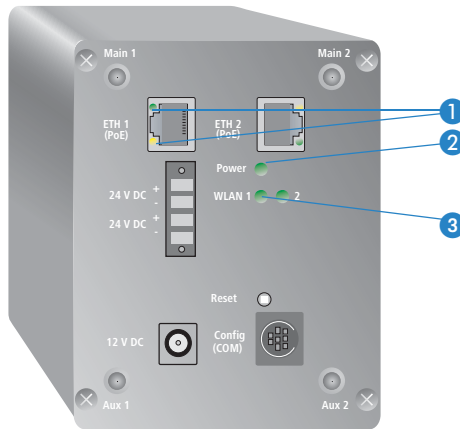


- **Invers Blitzen** bedeutet das Gegenteil. Hier leuchtet die LED in der jeweiligen Farbe dauerhaft und wird nur sehr kurz unterbrochen.
- **Flackern** bedeutet, dass die LED in unregelmäßigen Abständen ein- und ausgeschaltet wird.

### 2.3.1 LANCOM XAP-40-2 und LANCOM XAC-40-1

#### LEDs bei LANCOM XAP-40-2 und LANCOM XAC-40-1

Modellbeispiel:  
LANCOM XAP-40-2



- 1 ETH 1  
ETH 2 (nur  
LANCOM XAP-  
40-2)

Zustand der LAN-Schnittstellen, integriert in die RJ45-Ethernetbuchsen:

aus		kein Netzwerkgerät angeschlossen
grün	dauerhaft an	Ethernetverbindung aktiv
gelb	flackern	Datenverkehr

- 2 Power

Gibt Informationen über den allgemeinen Zustand des Gerätes aus.

grün	dauerhaft an	Gerät ist betriebsbereit.
rot	blinkend (langsam)	Gebührensperre aktiv (s. Kasten weiter unten)
grün/rot	blinkend (schnell)	unsichere Konfiguration (kein Passwort gesetzt)
rot	blinkend (schnell)	Hardwarefehler



Eine blinkende Power-LED zeigt beim LANCOM XAP-40-2 das Erreichen eines Gebührenlimits an (→ 'Blinkende Power-LED und keine Verbindung möglich?').

- 3 WLAN 1  
WLAN 2 (nur  
LANCOM XAP-  
40-2)

Geben Informationen über die WLAN-Verbindungen und den WLAN-Datenverkehr der internen WLAN-Module aus. Die WLAN-Anzeige kann folgende Zustände annehmen:

aus		Kein WLAN-Netz definiert oder WLAN-Modul deaktiviert. Es werden keine Beacons vom WLAN-Modul gesendet.
grün		Mindestens ein WLAN-Netz definiert und WLAN-Modul aktiviert. Es werden Beacons vom WLAN-Modul gesendet.
grün	invers blitzend	Anzahl der Blitzer = Anzahl der verbundenen WLAN-Stationen und P2P-Funkstrecken, danach folgt eine Pause.
grün	blinkend	DFS Scanning oder anderer Scan-Vorgang.
grün	flackernd	TX-Datenverkehr.
rot	flackern	Fehler im Funk-LAN (TX-Fehler, z.B. Sendefehler aufgrund schlechter Verbindung)
rot	blinkend	Hardwarefehler im WLAN-Modul

### Blinkende Power-LED und keine Verbindung möglich?

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

Es gibt drei Möglichkeiten die Sperre zu lösen:

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

Im LANmonitor wird Ihnen das Erreichen eines Zeit- oder Gebührenlimits angezeigt. Zum Reset des Gebührenschatzes 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 Gebührenschatz-Reset und alle Parameter unter **Experten-Konfiguration ▶ Setup ▶ Gebühren-Modul**.

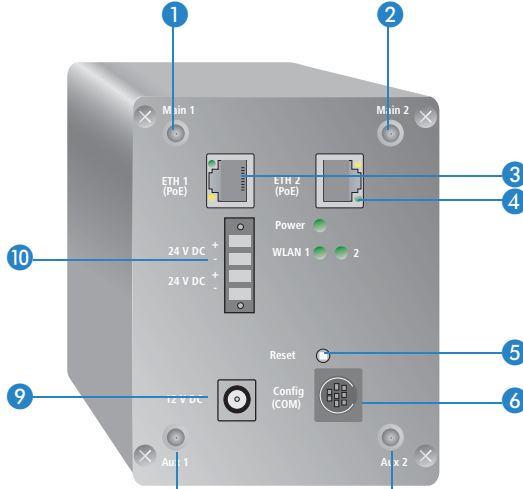


Signal für ein erreichtes Zeit- oder Gebührenlimit

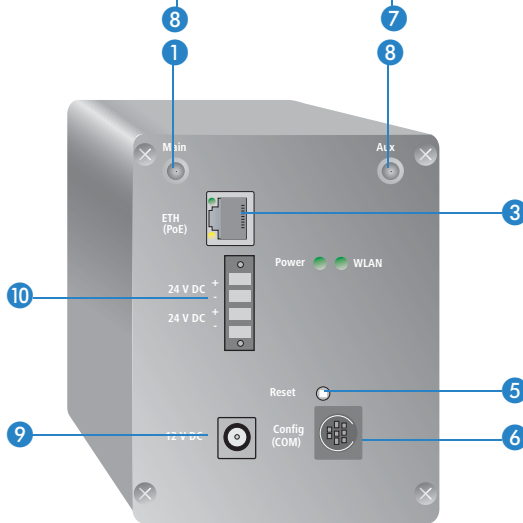
### Anschlüsse bei LANCOM XAP-40-2 und LANCOM XAC-40-1

Beim LANCOM XAP-40-2 befinden sich alle Anschlüsse auf der Frontseite des Gerätes.

LANCOM XAP-40-2



LANCOM XAC-40-1



- 1 Main-Anschluss für das erste WLAN-Modul.
- 2 Main-Anschluss für das zweite WLAN-Modul.

3 Erste Ethernet-Buchse (10/100Base-Tx) für den Anschluss an das LAN.

4 Zweite Ethernet-Buchse.

An beiden Ethernet-Buchsen werden 10-Mbit- oder 100-Mbit-Anschlüsse unterstützt. Die verwendete Übertragungsgeschwindigkeit wird automatisch erkannt (Autosensing).

Die LAN-Anschlüsse unterstützen den Power-over-Ethernet-Standard (PoE). Nähere Informationen zum Betrieb mit PoE finden Sie in der Info-Box 'Power-over-Ethernet – elegante Stromversorgung über die LAN-Verkabelung' → Seite 22.

Die LAN-Anschlüsse können bei aktivierter DSLoL-Option auch zum Anschluss des Access Points an ein DSL-Modem verwendet werden.

Die LAN-Anschlüsse verfügen über eine automatische MDI/MDIX-Erkennung, so dass unabhängig von der Gegenstelle kein Crossover-Kabel benötigt wird.

5 Reset-Schalter (siehe auch → 'Die Funktion des Reset-Tasters').

6 Anschluss für das serielle Konfigurationskabel.

7 Aux-Anschluss für das zweite WLAN-Modul.

8 Aux-Anschluss für das erste WLAN-Modul.

9 Anschluss für das mitgelieferte Netzteil.

10 Anschluss für 24 V DC über 4-poligen Stecker (Phoenix Contact, Combi-con RM 3,81mm). Die Stromversorgung ist redundant ausgelegt – hier können also zwei verschiedene 24 V-Spannungsquellen angeschlossen werden.



Der 24 V-Eingang ist besonders auf das industrielle Umfeld optimiert: Schwankungen der Eingangsspannung im Bereich von 20 V bis 28 V werden toleriert.

### Die Funktion des Reset-Tasters

Der Reset-Taster hat mit Booten (Neustart) und Reset (Rücksetzen auf Werks-einstellung) 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.



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

- Reset-oder-Booten (Standardeinstellung): Ein kurzer Druck auf den Taster führt zum Neustart, ein Druck von 5 Sekunden oder länger führt zum Neustart mit dem Zurücksetzen der Konfiguration auf den Auslieferungszustand. Alle LEDs am Gerät leuchten dauerhaft auf. Sobald der Taster freigegeben wird, startet das Gerät mit Werkseinstellungen neu.



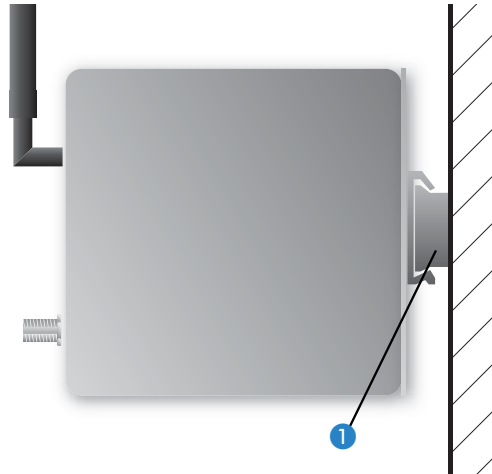
Das Gerät startet nach dem Reset neu im unkonfigurierten Zustand, **alle** Einstellungen gehen dabei verloren. Sichern Sie daher **vor** dem Reset nach Möglichkeit die aktuelle Konfiguration des Geräts!



Ein LANCOM Access Point befindet sich nach dem Reset wieder im „Managed-Modus“, in dem kein direkter Zugriff über die WLAN-Schnittstelle zur Konfiguration möglich ist!

### Hutschiennenmontage von LANCOM XAP-40-2 und LANCOM XAC-40-1

- ① Montieren Sie Ihr Gerät in der gewünschten Position auf der Hutschiene  
1.



DE

### Wandmontage

- ① Befestigen Sie die mitgelieferte Hutschiene für die Wandmontage mit den beiden Schrauben in der gewünschten Position an der Wand.
- ② Montieren Sie Ihr Gerät anschließend wie bei der Hutschiennenmontage beschrieben.

### Anschluss



Bitte beachten Sie bei der Montage des Geräts die Hinweise zum Blitzschutz im LANCOM Outdoor Wireless Guide (als Download auf [www.lancom.de](http://www.lancom.de)). Die Montage ohne ausreichenden Blitzschutz kann zu ernsthaften Schäden in den Access Points bzw. in der über das Netzwerk angeschlossenen Infrastruktur führen!

Der Anschluss des Geräts erfolgt in folgenden Schritten:

- ① **Antennen** – Schrauben Sie die mitgelieferten Antennen auf der Frontseite an:

- Verwenden Sie die jeweiligen Main-Anschlüsse der WLAN-Module, um separate Funk-Netze aufzubauen (z.B. für Point-to-Point-Anwendungen).
- Verwenden Sie die den Main- und den Aux-Anschluss eines WLAN-Moduls, wenn Sie die Diversity-Funktion nutzen möchten. Die Diversity-Funktion steigert die Verbindungsqualität, indem immer auf der Antenne gesendet oder empfangen wird, die den besten Kontakt zum Client bietet.



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



Beachten Sie bei der Montage von separat erworbenen Mobilfunk-Antennen, dass die im jeweiligen Land maximal zulässige Sendeleistung des WLAN-Systems nach EIRP nicht überschritten werden darf. Für die Einhaltung der Grenzwerte ist der Betreiber des Systems verantwortlich.

Für den inneren Blitzschutz ist der Überspannungsadapter AirLancer Extender SA-5L **immer erforderlich** – der AirLancer Extender SA-5L wird dabei zwischen dem Access Point und der Antenne montiert, dabei möglichst nah an der Antenne.



Bitte bestücken Sie die nicht genutzten Buchsen mit den mitgelieferten Terminatoren, um Einstreuungen von Funksignalen aus einem WLAN-Modul in das andere WLAN-Modul zu vermeiden.



Beim Einsatz des Gerätes in Schaltschränken beachten Sie bitte – für die Auswahl der verwendeten Antennen – die Dämpfung, die das Schaltschrankgehäuse verursacht. In diesen Anwendungen ist ggf. der Einsatz von externen Antennen zu empfehlen. Weitere Informationen zu externen Antennen und deren Montage finden Sie unter → 'Optionen und Zubehör'.

- ② **LAN** – Sie können das Gerät zunächst an Ihr LAN anschließen. Stecken Sie dazu das mitgelieferte Netzkabel (grüne Stecker) in einen LAN-Anschluss des Geräts ③ oder ④ und andererseits in eine freie Netzwerkanschlussdose Ihres lokalen Netzes (bzw. in eine freie Buchse eines Hubs/Switchs). Alternativ können Sie das Gerät auch einen einzelnen PC anschließen.

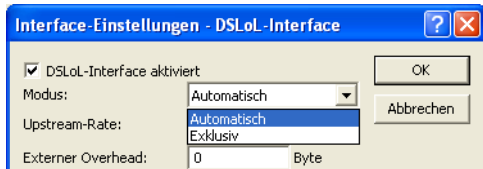
Der LAN-Anschluss erkennt die Übertragungsrate (10/100 Mbit) des angeschlossenen Netzwerkgerätes automatisch (Autosensing).

Informationen zur Installation von PoE finden Sie in der Info-Box 'Power-over-Ethernet – elegante Stromversorgung über die LAN-Verkabelung' → Seite 22.

- ③ **DSLol** – Wenn Sie das Gerät im DSLol-Modus betreiben möchten, können Sie das Gerät entweder direkt an das DSL-Modem anschliessen (Exklusiv-Modus) oder über einen Hub bzw. Switch im kabelgebundenen LAN (Automatik-Modus).

### LAN-Schnittstelle: exklusiv oder parallel für DSLol nutzen

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



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

- Stecken Sie im Exklusiv-Modus das mitgelieferte Netzwerkkabel (grüne Stecker) in den LAN-Anschluss des Geräts ③ oder ④ und andererseits in die entsprechende Schnittstelle des DSL-Modems.
- Stecken Sie im Automatik-Modus zum gleichzeitigen LAN und DSLol-Betrieb das mitgelieferte Netzwerkkabel (grüne Stecker) in den LAN-Anschluss des Geräts ③ oder ④ und andererseits in eine freie Netzwerkanschlussdose Ihres lokalen Netzes (bzw. in eine freie Buchse eines Hubs/Switches).



④ **Mit Spannung versorgen** – zur Spannungsversorgung des Gerätes haben Sie drei Möglichkeiten:

- Versorgen Sie das Gerät an Buchse 9 über das mitgelieferte Netzteil mit Spannung.



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

- Nutzen Sie die Stromversorgung über das Ethernetkabel (PoE) an den LAN-Anschlüssen des Geräts 3 oder 4. Informationen zur Installation von PoE finden Sie in der Info-Box → 'Power-over-Ethernet – elegante Stromversorgung über die LAN-Verkabelung'.



Die PoE-Versorgung für das LANCOM XAP-40-2 ist redundant ausgelegt, es können also beide LAN-Schnittstellen von separaten PoE-Injektoren versorgt werden.

- Versorgen Sie das Gerät über einen der 24 V-Anschlüsse 10 mit Spannung. Verwenden Sie dazu den mitgelieferten 24 V-Stecker (Anschlussbelegung im Anhang) oder einen anderen passenden 24 V-Stecker (Phoenix Contact, Combicon RM 3,81mm).



Die 24 V-Versorgung für LANCOM XAP-40-2 und LANCOM XAC-40-1 ist redundant ausgelegt, es können also beide 24 V-Schnittstellen von separaten Spannungsquellen versorgt werden.

Zur redundanten und ausfallsicheren Stromversorgung können mehrere Stromquellen in beliebigen Kombinationen gleichzeitig angeschlossen werden. Das Gerät wählt selbständig aus, welche Stromquelle genutzt wird. Wenn durch einen Ausfall der gerade aktiven Stromquelle eine andere Stromquelle die Stromversorgung des Gerätes übernimmt, bootet das Gerät ggf. neu, um die Stromspeisung neu zu aktivieren.

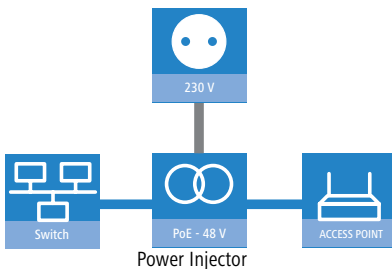
⑤ **Betriebsbereit?** – nach einem kurzen Selbsttest des Geräts leuchtet die Power-LED permanent grün bzw. blinkt abwechselnd rot und grün solange noch kein Konfigurationspasswort gesetzt ist.

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

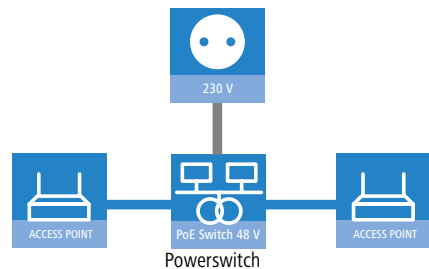
LANCOM Access Points sind für das PoE-Verfahren (Power-over-Ethernet) vorbereitet und entsprechen dem 802.3af-Standard. PoE-fähige Netzwerkgeräte können elegant über die LAN-Verkabelung mit Strom versorgt werden. Dadurch entfällt die Notwendigkeit eines eigenen Stromanschlusses für jede Basis-Station,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

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

### Installation einzelner Geräte



### Installation mehrerer Geräte



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



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

Beim LANCOM XAP-40-2 können zwei LAN-Buchsen zur redundanten Stromversorgung genutzt werden. Das Gerät wählt selbständig aus, welche Stromquelle genutzt wird. Wenn durch einen Ausfall der gerade aktiven Stromquelle eine andere Stromquelle die Stromversorgung des Gerätes übernimmt, bootet das Gerät ggf. neu, um die Stromspeisung neu zu aktivieren.

## 2.3.2 LANCOM IAP-54 Wireless

### LEDs beim LANCOM IAP-54 Wireless



#### 1 Power

Diese LED gibt Auskunft über die Betriebsbereitschaft des Geräts. Nach dem Einschalten blinkt sie für die Dauer des Selbsttests grün. Danach wird entweder ein festgestellter Fehler als roter Blinkcode ausgegeben, oder aber das Gerät geht in Betrieb, und die LED leuchtet konstant grün. Informationen zum Rücksetzen der Gebührensperrung finden Sie unter → 'Blinkende Power-LED und keine Verbindung möglich?'.

aus		Gerät abgeschaltet
grün	blinkend	Selbsttest nach dem Einschalten
grün		Gerät betriebsbereit
rot/grün	abwechselnd blinkend	Gerät unsicher: Kein Konfigurationskennwort gesetzt
rot	blinkend	Zeit- oder Gebührenlimit erreicht



Die Power-LED blinkt abwechselnd rot/grün, solange noch kein Konfigurationskennwort gesetzt wurde. Ohne Konfigurationskennwort sind die Konfigurationsdaten des LANCOM ungeschützt. Im Normalfall setzen Sie ein Konfigurationskennwort während der Grundkonfiguration.

#### 2 WLAN Link

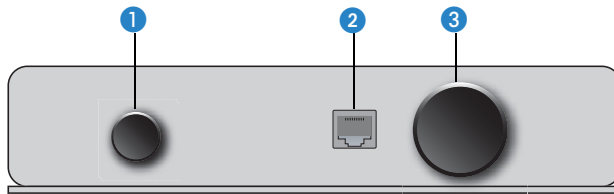
Gibt Informationen über den Funk-LAN-Zugang des internen Funk-Netzwerkadapters der Basis-Station aus.

Die WLAN-Link-Anzeige kann drei Zustände annehmen:

aus		kein Funk-LAN-Adapter gefunden
grün		Funk-LAN-Adapter betriebsbereit
grün	blinkend	Aktivität im Funk-LAN (Blinkfrequenz gibt die Anzahl angemeldeter Stationen an)

### Anschlüsse beim LANCOM IAP-54 Wireless

Beim LANCOM IAP-54 Wireless befinden sich Anschlüsse der Basis-Station an der Unterseite des Gerätes:



- 1 Spannungsanschluss für ein externes Netzteil (nicht im Lieferumfang enthalten), verdeckt mit einer IP50-geschützten Verschlusskappe.
- 2 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 des LANCOM IAP-54 Wireless unterstützt den Power-over-Ethernet-Standard (PoE). Nähere Informationen zum Betrieb mit PoE finden Sie in der Info-Box → 'Power-over-Ethernet – elegante Stromversorgung über die LAN-Verkabelung'.

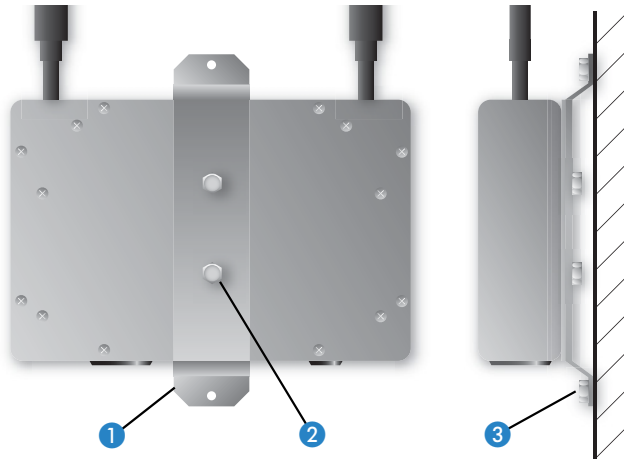
Der LAN-Anschluss kann bei aktivierter DSLoL-Option auch zum Anschluss der LANCOM Router Basis-Station an ein DSL-Modem verwendet werden (→ 'LAN-Schnittstelle: exklusiv oder parallel für DSLoL nutzen').

- 3 Anschluss für das serielle Konfigurationskabel (nicht im Lieferumfang enthalten) und Zugang zum Reset-Schalter, verdeckt mit einer IP50-geschützten Verschlusskappe (siehe auch → 'Die Funktion des Reset-Tasters').

## Wandmontage

- ① Befestigen Sie den Träger für die Wandmontage ① mit den beiden M6-Sechskantschrauben ② an der Rückseite des Gehäuses.
- ② Montieren Sie Ihr LANCOM IAP-54 Wireless anschließend mit geeigneten Schrauben ③ in der gewünschten Position an der Wand. Die Schrauben zur Wandmontage sind nicht im Lieferumfang enthalten.

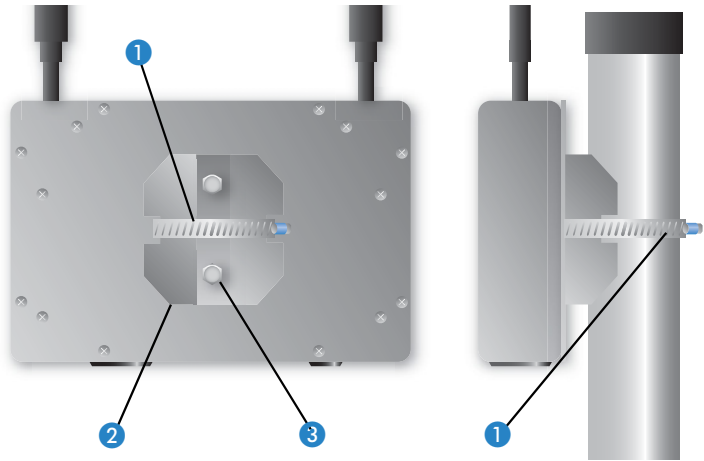
Wandmontage



## Pfostenmontage

- ① Legen Sie die für Ihren Pfostendurchmesser geeignete Montageschelle ① um den Halter für die Pfostenmontage ②. Im Lieferumfang sind zwei Montageschellen für unterschiedliche Pfostendurchmesser enthalten.
- ② Befestigen Sie den Halter für die Pfostenmontage ② mit den beiden M6-Sechskantschrauben ③ an der Rückseite des Gehäuses.
- ③ Montieren Sie Ihr LANCOM IAP-54 Wireless anschließend mit der Montageschelle ① in der gewünschten Position am Pfosten.

## Pfeostenmontage

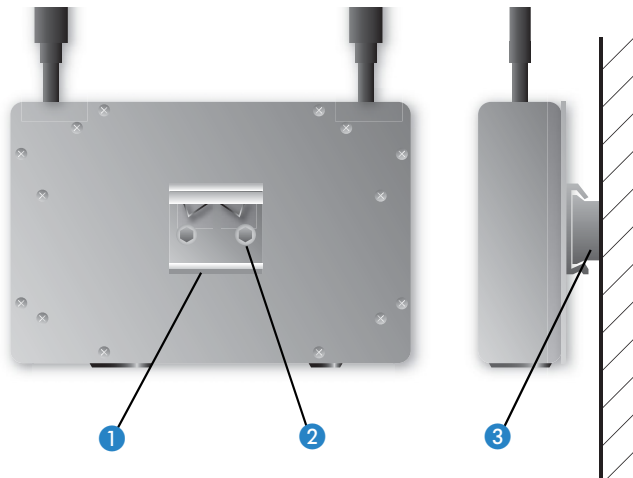


DE

**Hutschienenmontage**

- ① Befestigen Sie den Halter für die Hutschienenmontage ① mit den beiden M6-Innensechskantschrauben ② an der Rückseite des Gehäuses.
- ② Montieren Sie Ihr LANCOM IAP-54 Wireless anschließend in der gewünschten Position auf der Hutschiene ③.

## Hutschienenmontage



## Anschluss



Bitte beachten Sie bei der Montage des Geräts die Hinweise zum Blitzschutz im LANCOM Outdoor Wireless Guide (als Download auf [www.lancom.de](http://www.lancom.de)). Die Montage ohne ausreichenden Blitzschutz kann zu ernsthaften Schäden in den Access Points bzw. in der über das Netzwerk angeschlossenen Infrastruktur führen!

- ① Stecken Sie das mitgelieferte Netzkabel (grüne Stecker) in den LAN-Anschluss des LANCOM IAP-54 Wireless und in den 'Data/Power Out'-Ausgang des PoE-Power-Injectors.
- ② Verbinden Sie den 'Data In'-Eingang des PoE-Power-Injector mit einer freien Netzwerkanschlussdose Ihres lokalen Netzes (bzw. einer freie Buchse eines Hubs/Switchs). Das Kabel zur Verbindung des PoE-Power-Injector mit dem LAN ist nicht im Lieferumfang enthalten.



Wenn Sie den PoE-Power-Injector nicht an einen Switch oder Hub anschließen, sondern direkt an die Netzwerkschnittstelle eines Rechners, verwenden Sie dazu bitte ein geeignetes Crossover-Kabel.

- ③ Versorgen Sie den PoE-Power-Injector mit Spannung (wie in der entsprechenden Anleitung des PoE-Power-Injector beschrieben).
- ④ Nach einem kurzen Selbsttest des Geräts leuchtet die Power-LED am LANCOM IAP-54 Wireless permanent grün bzw. blinkt abwechselnd rot und grün, solange noch kein Konfigurationspasswort gesetzt ist.

### Öffnen der Verschlussstopfen für den seriellen Anschluss und den Resetschalter

Der Anschluss für das serielle Konfigurationskabel und der Resetschalter befinden sich geschützt im Gehäuse des Gerätes und sind durch zwei schwarze Kunststoffschrauben verschlossen.

Öffnen Sie bei Bedarf die Verschlusschrauben behutsam mit einem passenden Schraubendreher. Verschließen Sie das Gehäuse nach dem Reset bzw. nach der Konfiguration über das serielle Kabel wieder sorgfältig mit den Verschlussstopfen.

Information zur Funktion des Resetschalters finden Sie unter → 'Die Funktion des Reset-Tasters'.

## 2.4 Installation der Software

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



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

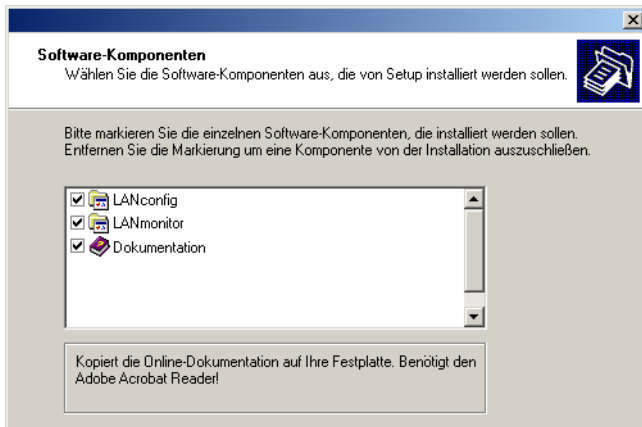
### 2.4.1 Software-Setup starten

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



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.



Unkonfigurierte LANCOM Access Points können im Auslieferungszustand nicht über die WLAN-Schnittstelle in Betrieb genommen werden.

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

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

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

Für unkonfigurierte LANCOM Access Points sind ab Werk die WLAN-Module ausgeschaltet und auf die Betriebsart „Managed“ eingestellt. Die WLAN-Module suchen im LAN nach einem LANCOM WLAN Controller, von dem sie eine Konfiguration für die WLAN-Schnittstellen beziehen können.

Mit dem Ausführen des Grundkonfigurations-Assistenten wird die Betriebsart der WLAN-Module automatisch auf „Access Point“ umgestellt – es ist dann eine manuelle Konfiguration der WLAN-Schnittstellen erforderlich.



Führen Sie den Grundkonfigurations-Assistenten nur dann aus, wenn der Access Point nicht von einem WLAN-Controller konfiguriert werden soll. Führen Sie danach den WLAN-Assistenten aus → WLAN-Konfiguration.

### 3.1 Welche Angaben sind notwendig?

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

## ■ Kapitel 3: Grundkonfiguration

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

### 3.1.1 TCP/IP-Einstellungen

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

Die vollautomatische TCP/IP-Konfiguration ist nur in bestimmten Netzwerkumgebungen möglich. Deshalb analysiert der Setup-Assistent das angeschlossene LAN daraufhin, ob die vollautomatische Konfiguration möglich ist oder nicht.

#### **Neues LAN – vollautomatische Konfiguration möglich**

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

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

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

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

#### **Trotzdem manuell konfigurieren?**

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

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

### Notwendige Angaben für die manuelle TCP/IP-Konfiguration

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

#### ■ DHCP-Betriebsart

- Aus: Die erforderlichen IP-Adressen müssen manuell eingetragen werden.
- Server: Der LANCOM arbeitet als DHCP-Server im Netzwerk, zumindest die eigene IP-Adresse und die Netzmaske müssen angegeben werden.
- Client: Der LANCOM bezieht als DHCP-Client die Adress-Informationen von einem anderen DHCP-Server, es müssen keine Adress-Informationen angegeben werden.

#### ■ IP-Adresse und Netzwerkmaske für den LANCOM

Teilen Sie dem LANCOM eine freie IP-Adresse aus dem Adressbereich Ihres LAN zu, und geben Sie die Netzwerkmaske an.

#### ■ Gateway-Adresse

Geben Sie die IP-Adresse des Gateways an, wenn Sie die DHCP-Betriebsart 'Aus' gewählt haben oder in der DHCP-Betriebsart 'Server' ein anderes Netzwerkgerät die Aufgabe des Gateways übernimmt.

#### ■ DNS-Server

Geben Sie die IP-Adresse eines DNS-Servers zur Auflösung der Domain-Namen an, wenn Sie die DHCP-Betriebsart 'Aus' gewählt haben oder in

der DHCP-Betriebsart 'Server' ein anderes Netzwerkgerät die Aufgabe des DNS-Servers übernimmt.

### 3.1.2 Konfigurationsschutz

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



In der Konfiguration des LANCOM können mehrere Administratoren angelegt werden, die über unterschiedliche Zugriffsrechte verfügen. Für einen LANCOM können bis zu 16 verschiedene Administratoren eingerichtet werden. Weitere Informationen finden Sie im LCOS-Referenzhandbuch unter „Rechteverwaltung für verschiedene Administratoren“.



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

### 3.1.3 Einstellungen für das Funk-LAN

#### Der Netzwerkname (SSID)

Der Grundkonfigurations-Assistent fragt nach dem Netzwerknamen des Access Points (häufig als SSID – **S**ervice **S**et **I**dentifier bezeichnet). Der Name kann frei gewählt werden. Mehrere Access Points mit demselben Netzwerknamen bilden ein gemeinsames Funk-LAN.

#### 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'.

### Auswahl eines Funkkanals

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

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

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



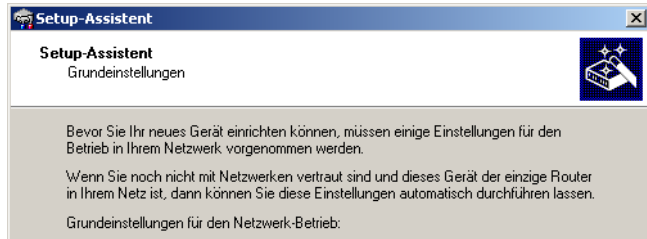
Weitere Informationen zu TPC und DFS finden sie im LCOS-Referenzhandbuch.

## 3.2 Anleitung für LANconfig

- ① Starten Sie LANconfig mit **Start ▶ Programme ▶ LANCOM ▶ LANconfig**. LANconfig erkennt neue LANCOM-Geräte im TCP/IP-Netz selbstständig.
- ② Wird bei der Suche ein unkonfiguriertes Gerät gefunden, startet der Setup-Assistent, der Ihnen bei der Grundeinstellung des Geräts behilflich

### ■ Kapitel 3: Grundkonfiguration

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

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

- ③ Geben Sie dem LANCOM eine verfügbare Adresse aus einem geeigneten IP-Adressbereich. Bestätigen Sie mit **Weiter**.
- ④ Im folgenden Fenster legen Sie zunächst das Kennwort für den Konfigurationszugriff fest. Achten Sie bei der Eingabe auf Groß- und Kleinschreibung, sowie auf eine ausreichende Länge (mindestens 6 Zeichen).

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



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

- ⑤ 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**.

- ⑥ Der Gehörenschtutz beschränkt auf Wunsch die Kosten von WAN-Verbindungen auf ein festgesetztes Maß. Bestätigen Sie Ihre Angaben mit **Weiter**.
- ⑦ Schließen Sie die Konfiguration mit **Fertig stellen** ab.



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

### 3.3 Anleitung für WEBconfig

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

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



Wird ein LANCOM Wireless Router oder ein LANCOM Access Point von einem LANCOM WLAN Controller zentral verwaltet, dann wird beim Zuweisen der WLAN-Konfiguration auch der DHCP-Server vom Auto-Modus in den Client-Modus umgeschaltet.

#### Netz ohne DHCP-Server

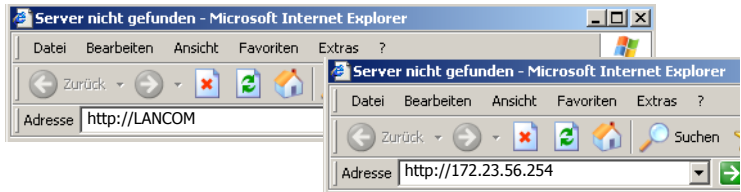
In einem Netz ohne DHCP-Server schalten unkonfigurierte LANCOM-Geräte nach dem Starten den eigenen DHCP-Serverdienst ein und weisen den anderen Rechnern im LAN die IP-Adressen sowie Informationen über Gateways etc. zu, sofern diese auf den automatischen Bezug der IP-Adressen eingestellt sind (Auto-DHCP).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

Nicht für zentral verwaltete LANCOM Wireless Router oder LANCOM Access Points



### ■ Kapitel 3: Grundkonfiguration

mit aktivierter Auto-DHCP-Funktion mit einem Webbrowser unter dem Namen **LANCOM** oder unter der IP-Adresse **172.23.56.254** erreicht werden.

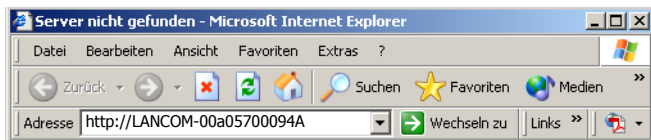



Falls der Konfigurations-Rechner seine IP-Adresse nicht vom LANCOM-DHCP-Server bezieht, ermitteln Sie die aktuelle IP-Adresse des Rechners (mit **Start ▶ Ausführen ▶ cmd** und dem Befehl **ipconfig** an der Eingabeaufforderung unter Windows 2000 oder Windows XP, mit **Start ▶ Ausführen ▶ cmd** und dem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

### Netz mit DHCP-Server

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

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

### Aufruf der Assistenten in WEBconfig

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

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

(bzw. über beliebigen Namen)








Sollte der Zugriff auf einen unkonfigurierten LANCOM 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-Verbindung einrichten](#)
-  [Auswahl des Internet-Anbieters](#)
-  [Neue Access Points zu Profilen zuordnen](#)

#### Gerätekonfiguration und -status




Diese Menüpunkte erlauben einen Zugriff auf die vollständige Gerätekonfiguration:

Benutzen Sie 'Konfiguration' für normale Konfigurationsaufgaben.

Die Expertenkonfiguration erlaubt es erfahrenen Benutzern, im Detail auf alle Geräteeinstellungen und den Gerätestatus zuzugreifen.

-  [Konfiguration](#)
-  [Experten-Konfiguration](#)
-  [Konfiguration speichern](#)
-  [Konfiguration hochladen](#)
-  [Konfigurations-Skript speichern](#)
-  [Konfigurations-Skript anwenden](#)







#### Dateiverwaltung

-  [Liste erlaubter öffentlicher SSH-Schlüssel bearbeiten](#)
-  [Zertifikat oder Datei herunterladen](#)
-  [Zertifikat oder Datei hochladen](#)

#### Firmware-Verwaltung

-  [Eine neue Firmware hochladen](#)

#### Extras

-  [Andere Geräte suchen/anzeigen](#)
-  [SNMP-Geräte-MIB abrufen](#)
-  [Software-Option freischalten](#)
-  [Schlüssel-Fingerprints anzeigen](#)
-  [Passwort ändern](#)
-  [TCP/HTTP-Tunnel erzeugen](#)




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

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

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

- ③ 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).

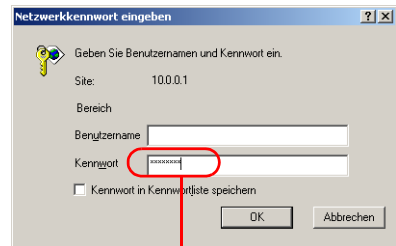
Legen Sie fest, ob das Gerät nur aus dem lokalen Netzwerk heraus konfiguriert werden darf, oder ob auch die Fernkonfiguration über das WAN (also aus einem entfernten Netzwerk) erlaubt ist.

-  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 Benutzername und Kennwort aufgefordert werden, tragen Sie Ihre persönlichen Werte in die entsprechenden Felder der Eingabemaske ein. Achten Sie dabei auf Groß- und Kleinschreibung.

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



Eingabe des Konfigurations-Kennworts

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

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

### ■ IP-Adressvergabe über ein LANCOM

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

### ■ IP-Adressvergabe über einen separaten DHCP-Server

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

### ■ Manuelle Zuweisung der IP-Adressen

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



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

## 4 Sicherheits- Einstellungen

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



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

### 4.1 Sicherheit im Funk-LAN

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

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

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

#### 4.1.1 SSID Broadcast unterdrücken – geschlossenes Netzwerk (Closed Network)

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

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

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

## 4.1.2 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.

## 4.1.3 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 verwendet 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.

#### 4.1.4 Verschlüsselung des Datentransfers

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

- Verschlüsseln Sie die im WLAN übertragenen Daten. Aktivieren Sie dazu die maximal mögliche Verschlüsselung (802.11i mit AES, TKIP oder WEP) und tragen Sie entsprechenden Schlüssel bzw. Passphrases im Access Point und in den WLAN-Clients ein.
- Ändern Sie regelmäßig die WEP-Schlüssel in Ihrem Access Point. Die Passphrases für 802.11i oder WPA müssen nicht gewechselt werden, da bereits regelmäßig im Betrieb neue Schlüssel pro Verbindung verwendet werden. Nicht nur deswegen ist die Verschlüsselung per 802.11i/AES oder WPA/TKIP wesentlich sicherer als das veraltete WEP-Verfahren.
- Falls es sich bei den übertragenen Daten um extrem sicherheitsrelevante Informationen handelt, können Sie zusätzlich zur besseren Authentifizierung der Clients das 802.1x-Verfahren aktivieren ('802.1x / EAP' → Seite 47) oder aber eine zusätzliche Verschlüsselung der WLAN-Verbindung einrichten, wie sie auch für VPN-Tunnel verwendet wird ('IPSec-over-WLAN' → Seite 48). 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.

#### 4.1.5 802.1x / 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 (integrierter RADIUS/EAP-Server im LANCOM oder externer RADIUS/EAP-Server) verwaltet und von dem Access Point bei Bedarf von dort abgerufen werden.



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

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

#### 4.1.6 IPSec-over-WLAN

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

## 4.2 Tipps für den richtigen Umgang mit Schlüsseln und Passphrasen

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

## 4.3 Der Sicherheits-Assistent

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

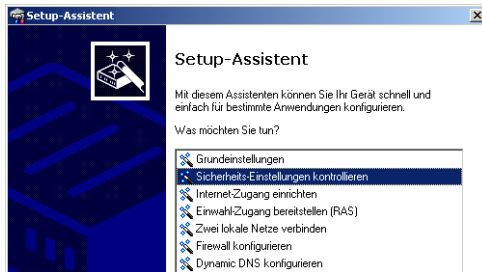
Ihr LANCOM verfügt über einen Kennwortschutz für den Konfigurationszugang. Dieser wird schon während der Grundkonfiguration durch Angabe eines Kennwortes aktiviert.

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

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

### 4.3.1 Assistent für LANconfig

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



- 2 Wählen Sie im Auswahlménú 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.

## ■ Kapitel 4: Sicherheits- Einstellungen

- 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.

### 4.3.2 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

## 4.4 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 das Funknetzwerk durch Verschlüsselung und Zugangs-kontrolllisten abgesichert?

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

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.

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

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

### ■ Haben Sie ein Kennwort für die Konfiguration vergeben?

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

**■ Haben Sie die Fernkonfiguration zugelassen?**

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

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

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

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

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

**■ Haben Sie die Firewall aktiviert?**

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

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

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

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

IP-Masquerading heißt das Versteck für alle lokalen Rechner beim Zugang ins Internet. Dabei wird nur das Router-Modul des Geräts mit seiner IP-Adresse im Internet bekannt gemacht. Die IP-Adresse kann fest vergeben

sein oder vom Provider dynamisch zugewiesen werden. Die Rechner im LAN nutzen den Router dann als Gateway und können selbst nicht erkannt werden. Der Router trennt Internet und Intranet wie eine Wand. Die Verwendung von IP-Masquerading wird für jede Route in der Routing-Tabelle einzeln festgelegt. Die Routing-Tabelle finden Sie in LANconfig im Konfigurationsbereich 'IP-Router' auf der Registerkarte 'Routing'.

#### ■ Haben Sie kritische Ports über Filter geschlossen?

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

#### ■ Haben Sie bestimmte Stationen von dem Zugriff auf das Gerät ausgeschlossen?

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

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

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

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

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

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

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

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

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

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

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

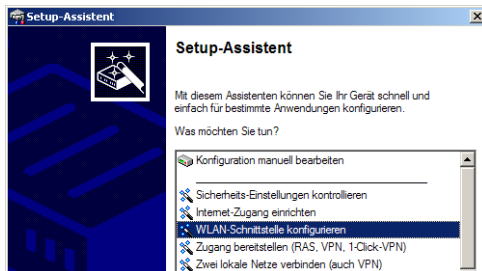
## 5 Erweiterte WLAN-Konfiguration

### 5.1 WLAN-Konfiguration mit dem Assistenten von LANconfig

Zur WLAN-Konfiguration der LANCOM Access Points stehen Ihnen komfortable Installations-Assistenten zur Verfügung.

Die Einstellungen betreffen sowohl allgemeine, übergreifende Parameter als auch die jeweiligen Einstellungen einer oder mehrerer logischer WLAN-Netzwerke (WLAN-Funkzellen oder SSIDs).

- ① Markieren Sie Ihren LANCOM Access Point im Auswahlfenster von LANconfig. Wählen Sie aus der Befehlsleiste den Punkt **Extras ▶ Setup Assistent**.



- ② Wählen Sie im Auswahlmenü den Setup-Assistenten **WLAN-Schnittstelle konfigurieren** und bestätigen Sie die Auswahl mit **Weiter**.
- ③ Nehmen Sie mit Hilfe des Assistenten die gewünschten Einstellungen vor wie in den folgenden Abschnitten beschrieben.

#### Ländereinstellungen

Der Betrieb von WLAN-Karten ist international nicht einheitlich geregelt. Die Verwendung von bestimmten Funkkanälen ist z.B. in manchen Ländern nicht erlaubt. Um den Betrieb der LANCOM Access Points auf die in dem jeweiligen Land zulässigen Parameter zu begrenzen, wird für alle physikalischen WLAN-Interfaces gemeinsam das Land eingestellt, in dem der Access Point betrieben wird.

#### Betriebsart der WLAN-Module

Die WLAN-Module können in verschiedenen Betriebsarten genutzt werden:



## ■ Kapitel 5: Erweiterte WLAN-Konfiguration

- Als Basisstation (Access Point-Modus) stellt das Gerät für die WLAN-Clients die Verbindung zu einem kabelgebundenen LAN her. Parallel dazu sind Punkt-zu-Punkt-Verbindungen möglich.
- Auch im Managed-Modus binden die Access Points WLAN-Clients in das Netzwerk ein – in dieser Betriebsart sind die Geräte allerdings Teilnehmer in einer WLAN-Infrastruktur, die von einem zentralen WLAN-Controller konfiguriert wird. In dieser Betriebsart ist keine weitere WLAN-Konfiguration erforderlich, alle WLAN-Parameter werden vom WLAN-Controller übermittelt.
- 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 z.B. dazu, ein kabelgebundenes Gerät über eine Funkstrecke an eine Basisstation anzubinden. In dieser Betriebsart sind parallele Punkt-zu-Punkt-Verbindungen **nicht** möglich.

Weitere Informationen finden Sie im Abschnitt → Client-Modus.



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

### Physikalische WLAN-Einstellungen

Neben dem verwendeten Funkkanal können Sie bei den physikalischen WLAN-Einstellungen Optionen wie die Bündelung von WLAN-Paketen (TX-Burst), die Hardwarekompression oder die Nutzung von QoS nach 802.11e aktivieren. Außerdem nehmen Sie hier die Einstellungen für das Diversity-Verhalten vor.

### Logische WLAN-Netzwerke

Jedes WLAN-Modul kann bis zu acht logische WLAN-Netzwerke aufspannen, in dem sich mobile WLAN-Clients anmelden können. Zur Konfiguration eines logischen WLAN-Netzwerks werden die folgenden Parameter abgefragt:

- Der Netzwerkname (SSID)
- Offenes oder geschlossenes Funk-LAN
- Verschlüsselungseinstellungen
- MAC-Filter
- Client-Bridge-Betrieb
- Filtereinstellungen

## Punkt-zu-Punkt-Einstellungen

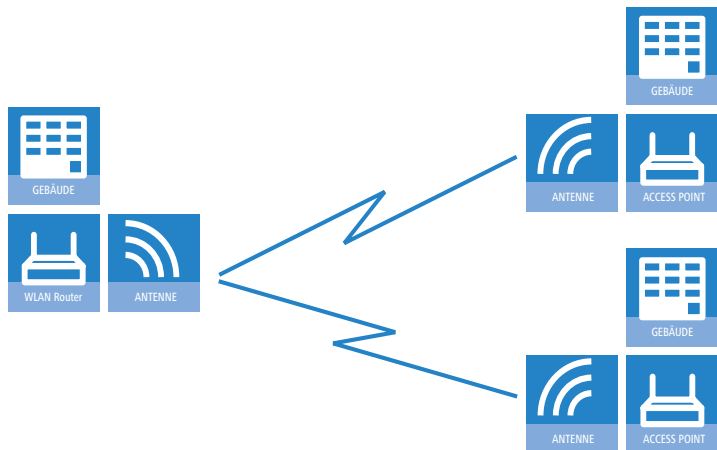
Bei der Konfiguration der P2P-Verbindungen wird neben der Betriebsart auch der Stationsname eingestellt, über den die Access Points eine Verbindung aufbauen können. Außerdem wird hier die Position als „Master“ oder „Slave“ festgelegt.

Neben den Einstellungen für den Access Point selbst wird auch definiert, zu welcher Gegenstelle der Access Point über die P2P-Verbindung Kontakt aufnehmen kann.

Weitere Informationen finden Sie im Abschnitt → Punkt-zu-Punkt-Verbindungen.

## 5.2 Punkt-zu-Punkt-Verbindungen

LANCOM 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:

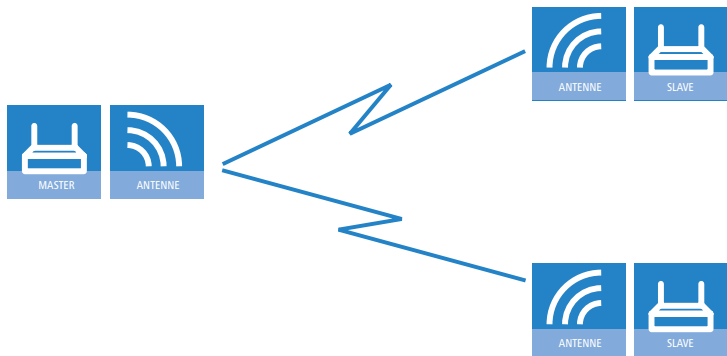
- **Aus:** Der Access Point kann nur mit mobilen Clients kommunizieren
- **An:** Der Access Point kann mit anderen Basis-Stationen und mit mobilen Clients kommunizieren

## ■ Kapitel 5: Erweiterte WLAN- Konfiguration

- **Exklusiv:** Der Access Point kann nur mit anderen Basis-Stationen kommunizieren

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

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



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



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

### 5.2.1 Geometrische Auslegung von Outdoor-Funknetz-Strecken

Bei der Auslegung der Funkstrecken sind im Wesentlichen folgende Fragen zu beantworten:

- Welche Antennen müssen für die gewünschte Anwendung eingesetzt werden?
- Wie müssen die Antennen positioniert werden, um eine einwandfreie Verbindung herzustellen?

- Welche Leistungen müssen die eingesetzten Antennen aufweisen, um einen ausreichenden Datendurchsatz innerhalb der gesetzlichen Grenzen zu gewährleisten?

### Auswahl der Antennen mit dem LANCOM Antennen-Kalkulator

Zur Berechnung der Ausgangsleistungen in den Access Points sowie der erreichbaren Distanzen und Datenraten können Sie den LANCOM Antennen-Kalkulator verwenden, den Sie zum Download auf unserer Webseite unter [www.lancom.de](http://www.lancom.de) finden.

Nach Auswahl der verwendeten Komponenten (Access Points, Antennen, Blitzschutz und Kabel) berechnet der Kalkulator neben Datenraten und Distanzen auch den Antennen-Gewinn, der in den Access Points eingestellt werden muss.



Bitte beachten Sie, dass bei der Verwendung von 5 GHz-Antennen je nach Einsatzland zusätzliche Techniken wie die dynamische Frequenzwahl (Dynamic Frequency Selection – DFS) vorgeschrieben sein können. Der Betreiber der WLAN-Anlage ist für die Einhaltung der jeweils geltenden Vorschriften verantwortlich.

■ Kapitel 5: Erweiterte WLAN- Konfiguration

**Antenna Distance Calculator**

LANCOM Systems

connecting your business

**Point A**

Accesspoint/Client Adapter: LANCOM IAP-54 Wireless

WLAN Module: Wltron OX12

Frequency Band: 802.11a (5 GHz)

Cable 1: ARCantor Cable 10/4P 3m

Surge Arrestor: Yes

Cable 2: 0-9a Cable 3m

Antenna: ARCantor Extender 0-9a

**Point B**

Accesspoint/Client Adapter: LANCOM IAP-54 Wireless

WLAN Module: Wltron OX12

Frequency Band: 802.11a (5 GHz)

Cable 1: ARCantor Cable 10/4P 3m

Surge Arrestor: Yes

Cable 2: 0-9a Cable 3m

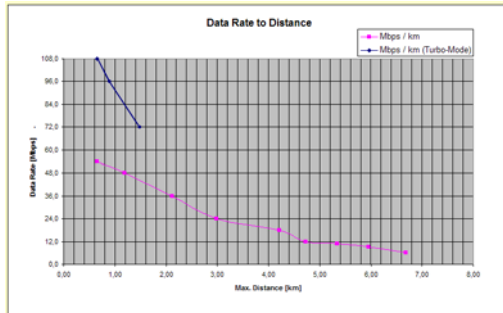
Antenna: ARCantor Extender 0-9a

Distance (km) : 6.68

Mast Height [m] : 13.52

Data Rate (Mbps) : 6.0

10 dB "bad weather" Reserve: Yes

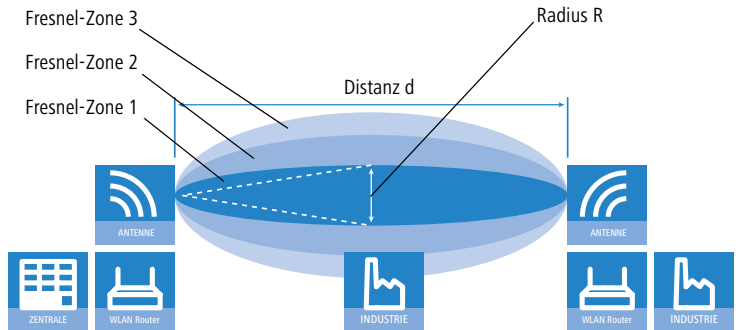


Calculator program: Distance between point A and point B by cables on maximum cable length 2000m (2 x 4 000m or 10 000m (100m) respectively)

Data Rate [Mbps]	Max. Distance [km]	POINT A Gain of Antenna System [dBi]	POINT B Gain of Antenna System [dBi]
1.0			
2.0	14.1		
3.0			
4.0	6.83		
5.0	5.957		
6.0			
7.0	4.752		
8.0	4.217		
9.0			
10.0	3.600		
11.0			
12.0	3.113		
13.0			
14.0	2.768		
15.0			
16.0	2.505		
17.0			
18.0	2.283		
19.0			
20.0	2.093		
21.0			
22.0	1.933		
23.0			
24.0	1.800		
25.0			
26.0	1.688		
27.0			
28.0	1.595		
29.0			
30.0	1.517		
31.0			
32.0	1.450		
33.0			
34.0	1.393		
35.0			
36.0	1.345		
37.0			
38.0	1.303		
39.0			
40.0	1.267		
41.0			
42.0	1.235		
43.0			
44.0	1.206		
45.0			
46.0	1.180		
47.0			
48.0	1.156		
49.0			
50.0	1.134		
51.0			
52.0	1.113		
53.0			
54.0	1.093		
55.0			
56.0	1.074		
57.0			
58.0	1.056		
59.0			
60.0	1.039		
61.0			
62.0	1.023		
63.0			
64.0	1.008		
65.0			
66.0	0.994		
67.0			
68.0	0.980		
69.0			
70.0	0.967		
71.0			
72.0	0.954		
73.0			
74.0	0.942		
75.0			
76.0	0.930		
77.0			
78.0	0.919		
79.0			
80.0	0.908		
81.0			
82.0	0.898		
83.0			
84.0	0.888		
85.0			
86.0	0.879		
87.0			
88.0	0.870		
89.0			
90.0	0.862		
91.0			
92.0	0.854		
93.0			
94.0	0.846		
95.0			
96.0	0.839		
97.0			
98.0	0.832		
99.0			
100.0	0.825		

**Positionierung der Antennen**

Die Antennen strahlen ihre Leistung nicht linear, sondern in einem modellabhängigen Winkel ab. Durch die kugelförmige Ausbreitung der Wellen kommt es in bestimmten Abständen von der direkten Verbindung zwischen Sender und Empfänger zur Verstärkung oder zu Auslöschungen der effektiven Leistung. Die Bereiche, in denen sich die Wellen verstärken oder auslöschen, werden als Fresnel-Zonen bezeichnet.



Um die von der Antenne abgestrahlte Leistung möglichst vollständig auf die empfangende Antenne abzubilden, muss die Fresnel-Zone 1 frei bleiben. Jedes störende Element, das in diese Zone hineinragt, beeinträchtigt die effektiv übertragene Leistung deutlich. Dabei schirmt das Objekt nicht nur einen Teil der Fresnel-Zone ab, sondern führt durch Reflexionen zusätzlich zu einer deutlichen Reduzierung der empfangenen Strahlung.

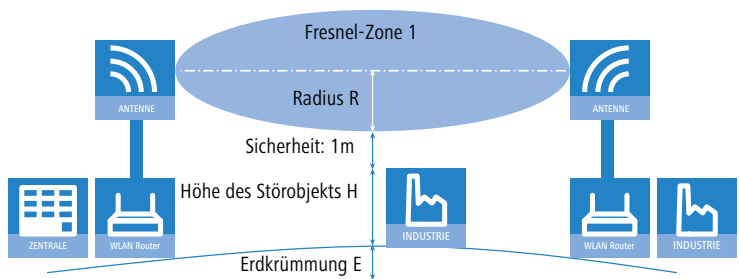
Der Radius (R) der Fresnel-Zone 1 berechnet sich bei gegebener Wellenlänge der Strahlung ( $\lambda$ ) und der Distanz zwischen Sender und Empfänger (d) nach folgender Formel:

$$R = 0,5 * \sqrt{(\lambda * d)}$$

Die Wellenlänge beträgt im 2,4 GHz-Band ca. 0,125 m, im 5 GHz-Band ca. 0,05 m.

**Beispiel:** Bei einer Distanz zwischen den beiden Antennen von 4 km ergibt sich im 2,4 GHz-Band der Radius der Fresnel-Zone 1 zu **11 m**, im 5 GHz-Band nur zu **7 m**.

Damit die Fresnel-Zone 1 frei und ungestört ist, müssen die Antennen das höchste Störobjekt um diesen Radius überragen. Die gesamte erforderliche Masthöhe (M) der Antennen ergibt sich nach folgendem Bild zu:



$$M = R + 1m + H + E \text{ (Erdkrümmung)}$$

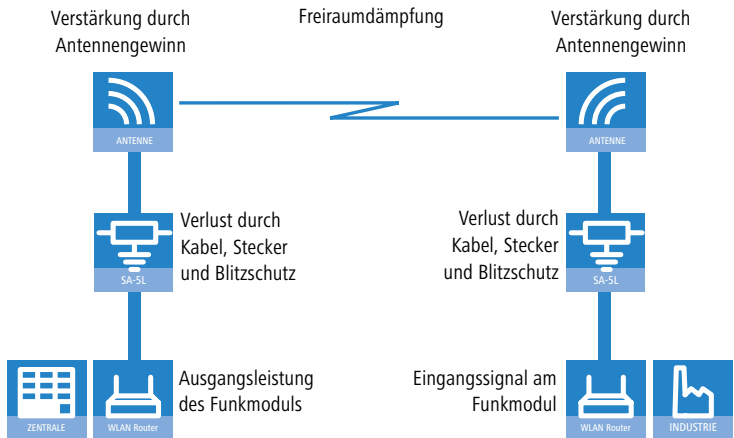
Die Höhe der Erdkrümmung (E) ergibt sich bei einer Distanz (d) zu  $E = d^2 * 0,0147$  – bei einer Distanz von 8 km also immerhin schon fast 1m!

**Beispiel:** Bei einer Distanz zwischen den beiden Antennen von 8 km ergibt sich im 2,4 GHz-Band die Masthöhe über dem höchsten Störobjekt von ca. **13 m**, im 5 GHz-Band zu **9 m**.

### Antennen-Leistungen

Die Leistungen der eingesetzten Antennen müssen so ausgelegt sein, dass eine ausreichende Datenübertragungsrate erreicht wird. Auf der anderen Seite dürfen die länderspezifischen gesetzlichen Vorgaben für die maximal abgestrahlten Leistungen nicht überschritten werden.

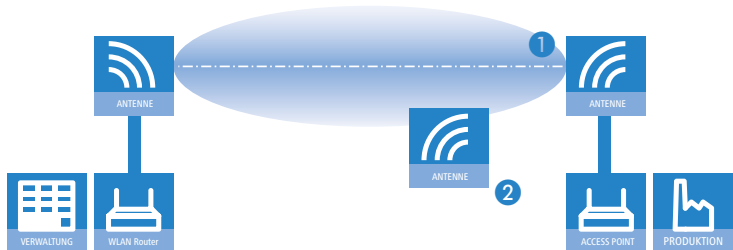
Die Berechnung der effektiven Leistungen führt dabei vom Funkmodul im sendenden Access Point bis zum Funkmodul im empfangenden Access Point. Dazwischen liegen dämpfende Elemente wie die Kabel, Steckverbindungen oder einfach die übertragende Luft und verstärkende Elemente wie die externen Antennen.



### 5.2.2 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

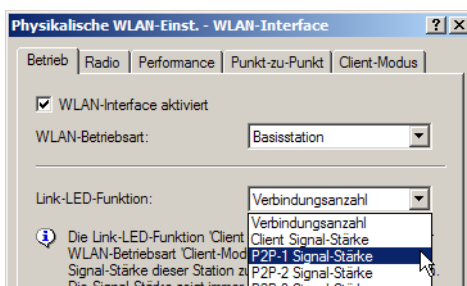
Antenne jedoch deutlich neben dem idealen Bereich, sind erhebliche Leistungsverluste zu erwarten **2**.



**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 die aktuelle Signalqualität von P2P-Verbindungen über die LEDs des Gerätes oder im LANmonitor angezeigt werden.

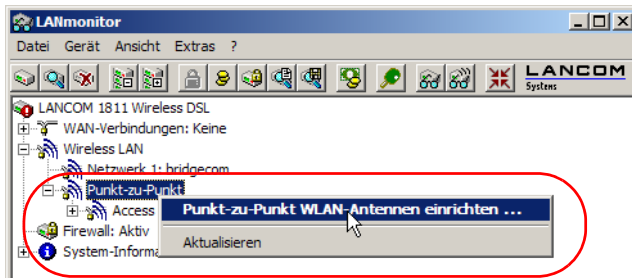
Die Anzeige der Signalqualität über die LEDs muss für die physikalische WLAN-Schnittstelle aktiviert werden (LANconfig: **Wireless LAN ► Allgemein ► Physikalische WLAN-Einstellungen ► Betrieb**). Je schneller die LED blinkt, umso besser ist die Verbindung (eine Blinkfrequenz von 1 Hz steht für eine Signalqualität von 10 dB, eine Verdoppelung der Frequenz zeigt die jeweils doppelte Signalstärke).



Im LANmonitor kann die Anzeige der Verbindungsqualität über das Kontextmenü geöffnet werden. Ein Klick mit der rechten Maustaste auf den Eintrag 'Punkt-zu-Punkt' erlaubt den Aufruf 'Punkt-zu-Punkt WLAN-Antennen einrichten ...'



## ■ Kapitel 5: Erweiterte WLAN-Konfiguration

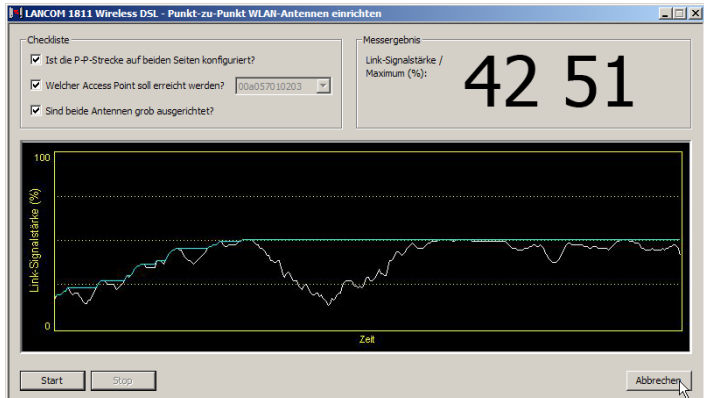


Der Eintrag 'Punkt-zu-Punkt' ist im LANmonitor nur sichtbar, wenn in dem überwachten Gerät mindestens eine Basisstation als Gegenstelle für eine P2P-Verbindung eingerichtet ist (LANconfig: **Wireless LAN** ► **Allgemein** ► **Physikalische WLAN-Einstellungen** ► **Punkt-zu-Punkt**).

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 (gegenüberliegende Basisstation mit MAC-Adresse oder Stations-Namen definiert)?
- 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 LANmonitors 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.

### 5.3 Konfiguration der P2P-Verbindungen

Bei der Konfiguration der Punkt-zu-Punkt-Verbindungen werden neben der Punkt-zu-Punkt-Betriebsart und dem Kanalwahlverfahren die MAC-Adressen oder die Stationsnamen 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'.



Die Konfiguration der P2P-Verbindungen kann auch mit dem WLAN-Assistenten von LANconfig erfolgen.

- 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. Wenn die Gegenstellen der P2P-Verbindungen über den Stationsnamen identifiziert werden sollen, tragen Sie einen eindeutigen Namen für diese WLAN-Station ein.



Bei Modellen mit mehreren WLAN-Modulen kann der Stationsname für jede physikalische WLAN-Schnittstelle separat eingetragen werden.

**Physikalische WLAN-Einst. - WLAN-Interface**

Betrieb | Radio | Performance | **Punkt-zu-Punkt** | Client-Modus

Punkt-zu-Punkt Betriebsart:

Aus - Diese Basisstation kann nur von mobilen Stationen erreicht werden.

An - Die Station kann mit anderen Basisstationen Daten austauschen, um so mehrere WLAN-Netze zu verbinden.

Exklusiv - Die Station kann nur mit anderen Basisstationen Daten austauschen; Mobile Stationen können zu diesem Gerät keinen Kontakt aufnehmen (reine WLAN-Bridge).

Stations-Name:

Konfigurieren Sie die Punkt-zu-Punkt-Partner ausserhalb dieses Dialogs in der entsprechenden Tabelle.

Keine Pakete zwischen Punkt-zu-Punkt-Verbindungen auf dem selben Interface weiterleiten

Kanalarwahlverfahren:

- ③ Schließen Sie die physikalischen WLAN-Einstellungen und öffnen Sie die Liste der **Punkt-zu-Punkt-Partner**. Tragen Sie zu jeder der maximal sechs P2P-Verbindungen entweder die jeweiligen MAC-Adressen der WLAN-Karte auf der Gegenseite ein oder den Namen der entsprechenden WLAN-Station (je nach Wahl der Identifizierung).

**Punkt-zu-Punkt-Partner - P2P-1-1: Punkt-zu-Punkt 1 - 1**

Diesen Punkt-zu-Punkt-Kanal aktivieren

Tragen Sie hier die WLAN-Basisstation ein, die über Punkt-zu-Punkt-Verbindung vernetzt werden sollen.

Identifikation durch:

MAC-Adresse

Stations-Name

Wenn Sie die Erkennung durch MAC-Adresse verwenden, dann tragen Sie hier die MAC-Adresse des WLAN-Adapters und nicht die des Gerätes selbst ein.

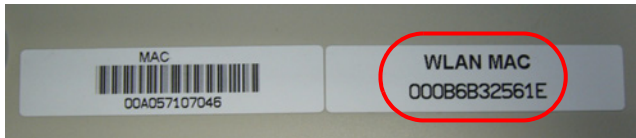
MAC-Adresse:

Stations-Name:



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 jeweiligen 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

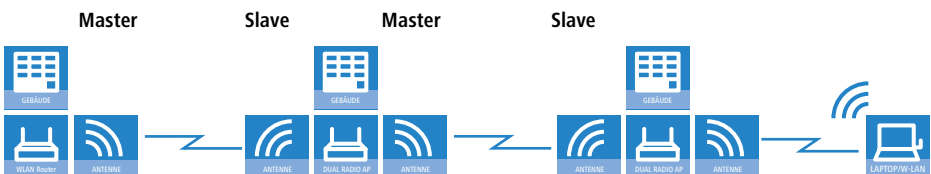
Konfiguration mit WEBconfig oder Telnet

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

### 5.3.1 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.

### 5.3.2 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).

#### Verschlüsselung mit 802.11i/WPA

Zum Aktivieren der 802.11i-Verschlüsselung auf einer korrekt konfigurierten P2P-Verbindung passen Sie die Einstellungen für das erste logische WLAN-Netzwerk im verwendeten WLAN-Interface an (also WLAN-1, wenn Sie die erste WLAN-Karte für die P2P-Verbindung nutzen, WLAN-2 wenn Sie die zweite Karte z.B. bei einem Access Point mit zwei WLAN-Modulen nutzen).

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

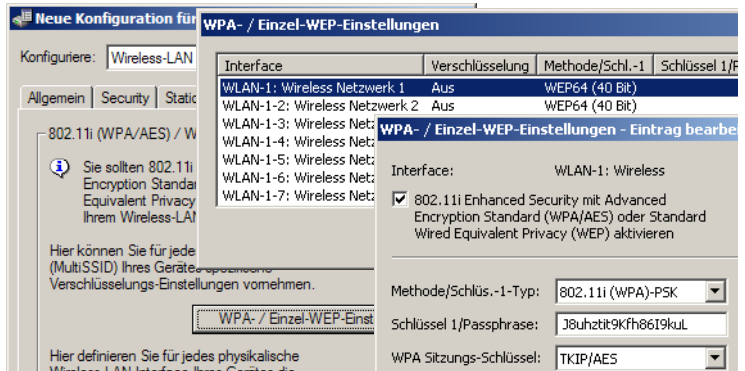


Verwenden Sie als Passphrase zufällige Zeichenketten von mindestens 22 Zeichen Länge, was einer kryptographischen Stärke von 128 Bit entspricht.

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

Konfiguration mit  
LANconfig

Bei der Konfiguration mit LANconfig finden Sie die Verschlüsselungs-Einstellungen im Konfigurationsbereich 'Wireless-LAN' 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

## LEPS für P2P-Verbindungen

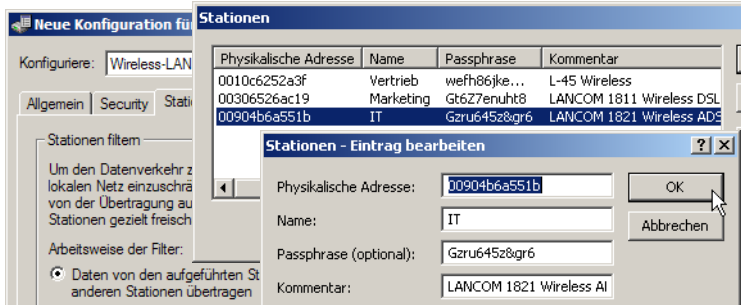
Einen weiteren Sicherheitsgewinn erzielen Sie durch die zusätzliche Verwendung der LANCOM Enhanced Passphrase Security (LEPS), also der Verknüpfung der MAC-Adresse mit der Passphrase.

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.

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

■ Kapitel 5: Erweiterte WLAN- Konfiguration

DE



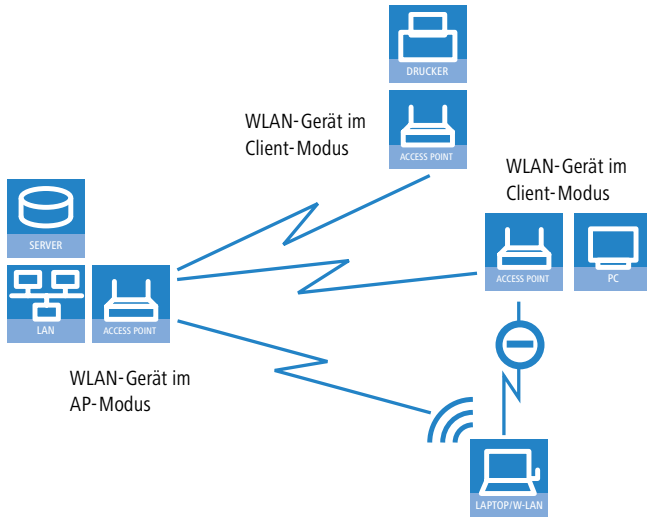
Konfiguration mit WEBconfig oder Telnet

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

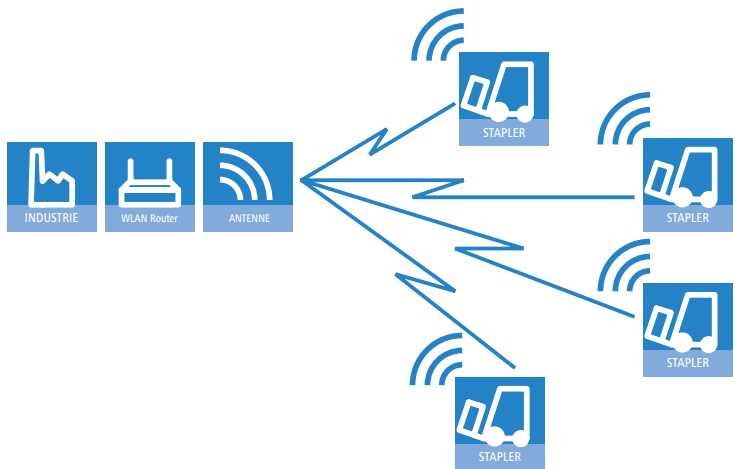
## 5.4 Client-Modus

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.

In industriellen Anwendungen können die WLAN-Clients auch mobil eingesetzt werden, z.B. auf einem Gabelstapler, der über die drahtlose Verbindung ständig Kontakt zu seiner Leitstelle hält.



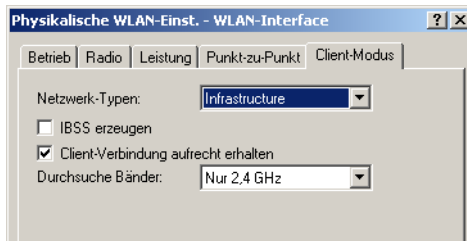


## 5.4.1 Client-Einstellungen

Für LANCOM Access Points und 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.



Die Konfiguration der Client-Einstellungen kann auch mit dem WLAN-Assistenten von LANconfig erfolgen.



- 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:

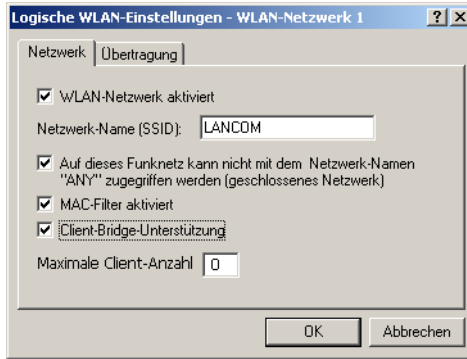
Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ▶ Setup ▶ Schnittstellen ▶ WLAN-Schnittstellen ▶ Client-Einstellungen
Terminal/Telnet	Setup/Schnittstellen/WLAN-Schnittstellen/Client-Einstellungen

## 5.4.2 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 einbuchten soll.

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

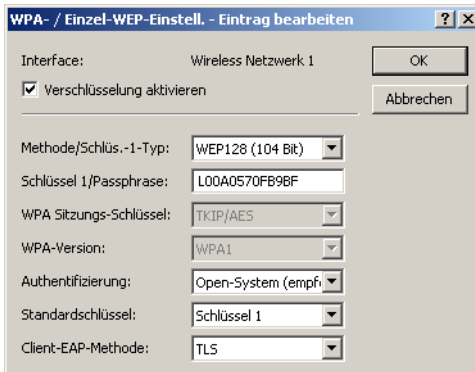
Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ▶ Setup ▶ Schnittstellen ▶ WLAN-Schnittstellen ▶ Netzwerk-Einstellungen
Terminal/Telnet	Setup/Schnittstellen/WLAN-Schnittstellen/Netzwerk-Einstellungen

### 5.4.3 Verschlüsselungseinstellungen


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

- ① Zum Eintragen 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

## Kapitel 5: Erweiterte WLAN- Konfiguration



- ② Aktivieren Sie die Verschlüsselung und passen Sie die Verschlüsselungsmethode an die Einstellungen des Access Points an.
- ③ LANCOM Access Point und 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 das Gerät einbuchten will.

 Je nach gewählter EAP-Methode müssen im Gerät die entsprechenden Zertifikate hinterlegt werden:

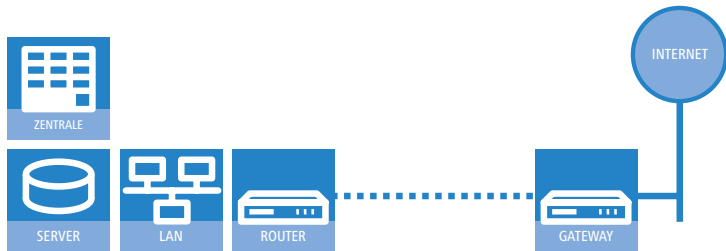
- Für TTLS und PEAP nur das EAP/TLS-Root-Zertifikat, als Schlüssel wird dabei die Kombination Benutzername:Kennwort eingetragen.
- Für TLS zusätzlich das EAP/TLS-Gerätezertifikat samt privatem Schlüssel.

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

## 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. Bei Modellen ohne WAN-Anschluss wird dazu eine LAN-Schnittstelle als DSLoL-Anschluss konfiguriert und mit einem geeigneten ADSL-Modem verbunden.



### Kennt der Setup-Assistent Ihren Internet-Anbieter?

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

### Zusätzlich Angaben bei unbekanntem Internet-Anbieter

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

### Weitere Verbindungsoptionen

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

- Zeitliche Abrechnung oder Flatrate – wählen Sie aus, nach welchem Modell Ihr Internetanbieter die Nutzung abrechnet.
  - Bei der zeitlichen Abrechnung können Sie am LANCOM einstellen, dass bestehende Verbindungen automatisch abgebaut werden, wenn

für eine bestimmte Dauer (die sogenannte Haltezeit) keine Daten mehr übertragen wurden.

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

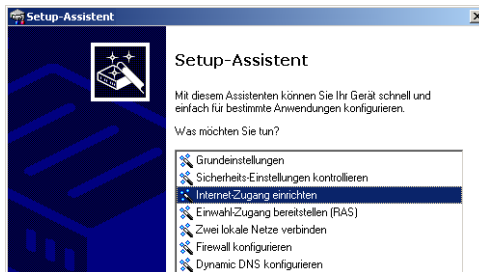
- Bei Flatrate-Abrechnung haben Sie ebenfalls die Möglichkeit der aktiven Leitungsüberwachung, und können so die Funktion der Gegenstelle ständig überprüfen.

Außerdem können Sie bei Flatrates Verbindungen dauerhaft aufrecht erhalten („Keep-alive“). Im Fall eines Verbindungsabbruchs wird diese automatisch wieder aufgebaut.

## 6.1 Der Internet-Assistent

### 6.1.1 Anleitung für LANconfig

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

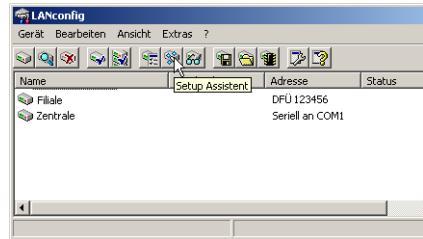


- ② Wählen Sie im Auswahlmenü den Setup-Assistenten **Internet-Zugang einrichten** und bestätigen Sie die Auswahl mit **Weiter**.
- ③ In den folgenden Fenstern wählen Sie Ihr Land, nach Möglichkeit Ihren Internetanbieter, und geben Sie die Zugangsdaten ein.
- ④ Je nach Verfügbarkeit bietet Ihnen der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

- ⑤ 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.



#### 6.1.2 Anleitung für WEBconfig

- ① Wählen Sie im Hauptmenü **Internet-Zugang einrichten**.
- ② In den folgenden Fenstern wählen Sie Ihr Land, nach Möglichkeit Ihren Internetanbieter, und geben Sie die Zugangsdaten ein.
- ③ Je nach Verfügbarkeit bietet Ihnen der Assistent weitere Optionen für die Internetverbindung zur Auswahl an.
- ④ Der Assistent informiert Sie sobald die Eingaben vollständig sind. Schließen Sie die Konfiguration mit **Weiter** ab.

#### 6.2 Der Firewall-Assistent

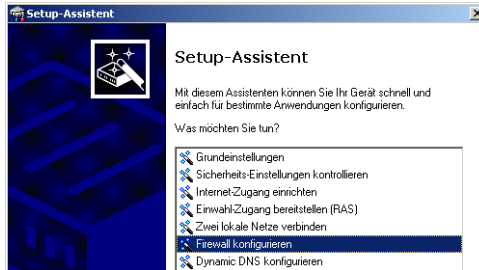
Ihr LANCOM verfügt über eine Stateful-Inspection-Firewall und Firewall-Filter zur wirksamen Absicherung Ihres WLAN gegenüber dem Internet. Kernidee der Stateful-Inspection-Firewall ist, dass nur selbstinitiiertes Datentransfer als zulässig betrachtet wird. Alle Zugriffe, die unaufgefordert nicht aus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

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

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

## 6.2.1 Assistent für LANconfig

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



- 2 Wählen Sie im Auswahlmenü den Setup-Assistenten **Firewall konfigurieren** und bestätigen Sie die Auswahl mit **Weiter**.
- 3 In den folgenden Fenstern wählen Sie aus, auf welche Dienste/Protokolle sich die Regel bezieht. Im nächsten Schritt legen Sie fest, für welche Quell- und Zielstationen die Regel gilt und welche Aktionen ausgeführt werden sollen, wenn die Regel auf ein Datenpaket zutrifft.
- 4 Zum Abschluss geben Sie der neuen Regel einen Namen, aktivieren sie und legen fest, ob weitere Regeln beachtet werden sollen, wenn die Regel auf ein Datenpaket zutrifft.
- 5 Der Assistent informiert Sie sobald die Eingaben vollständig sind. Schließen Sie die Konfiguration mit **Fertig stellen** ab.

## 6.2.2 Konfiguration unter WEBconfig

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

## 7 Optionen und Zubehör

Ihr Gerät 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 das Gerät um zusätzliche Abrechnungsfunktionen erweitern und zu einem Wireless Public Spot aufzurüsten.

### 7.1 Optionale AirLancer Extender Antennen

Um die Reichweite der Geräte 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](http://www.lancom.de).



Zur Berechnung der Konfiguration von AirLancer Extender Antennen und auch von Fremdanennen, die Sie an das LANCOM anschließen wollen, finden Sie weitere Informationen unter [www.lancom.de](http://www.lancom.de).



Beachten Sie bei der Montage von separat erworbenen Mobilfunk-Antennen, dass die im jeweiligen Land maximal zulässige Sendeleistung des WLAN-Systems nach EIRP nicht überschritten werden darf. Für die Einhaltung der Grenzwerte ist der Betreiber des Systems verantwortlich.



Für den inneren Blitzschutz ist der Überspannungsadapter AirLancer Extender SA-5L **immer erforderlich** – der AirLancer Extender SA-5L wird dabei zwischen dem Access Point und der Antenne montiert, dabei möglichst nah an der Antenne.



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



### 7.1.1 Antenna Diversity

Nur LANCOM IAP-54 Wireless

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

### 7.1.2 Installation der AirLancer Extender Antennen

Für die LANCOM sind folgende Diversityantennen als Zubehör erhältlich:

- AirLancer Extender O-D80g (2,4 GHz), Art.Nr. 61221
- AirLancer Extender O-D60a (5 GHz), Art.Nr. 61222
- AirLancer Extender O-D9a (5 GHz), Art.Nr. 61224



Bitte beachten Sie bei der Montage von externen Antennen die Hinweise zum Blitzschutz im LANCOM Outdoor Wireless Guide (mitgeliefert oder als Download auf [www.lancom.de](http://www.lancom.de)). Die Montage von Antennen ohne ausreichenden Blitzschutz kann zu ernsthaften Schäden in den Access Points bzw. in der über das Netzwerk angeschlossenen Infrastruktur führen!

Nur LANCOM XAP-40-2 und LANCOM XAC-40-1

Zur Installation von optionalen AirLancer Extender-Antenne schalten Sie den LANCOM aus, indem sie Spannungsversorgung (über 12 V-Netzteil, 24 V-Schnittstelle oder PoE) unterbrechen. Schrauben Sie dann vorsichtig die vorhandenen Antennen und falls erforderlich die Terminatoren ab. Schliessen Sie die AirLancer Extender-Antenne an den entsprechenden 'Antenna Main'-Antennenanschluss an.

Modellbeispiel:  
LANCOM XAP-40-2



Nur LANCOM XAP-40-2

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

Ausserdem können Sie mit dem LANCOM XAP-40-2 oder LANCOM XAC-40-1 die „Tx-Diversity“-Funktion über den Aux-Anschluss des jeweiligen WLAN-Moduls nutzen. Weitere Informationen finden Sie im LCOS-Referenzhandbuch.



Die AirLancer Extender O-D60a, O-D80g und O-D9a sind als Polarizationsdiversity-Antennen intern mit zwei um 90° versetzt polarisierenden Antennen ausgerüstet. Dadurch ergibt sich bei einer Ausleuchtung z.B. einer Lagerhalle oder eines Produktionsstandortes eine Verbesserung der Signalqualität von mindestens 3 dB. Bessere Verbindungen mit höherem Datendurchsatz werden möglich.

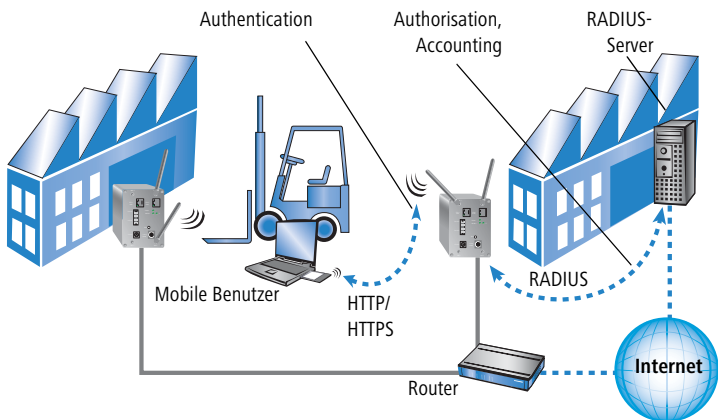
## 7.2 LANCOM Public Spot Option

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.



Bitte beachten Sie, dass der Betrieb eines LANCOMs mit LANCOM Public Spot Option (manchmal auch als HotSpot bezeichnet) in Ihrem Land rechtlichen Regulierungen unterliegen kann. Bitte informieren Sie sich vor der Einrichtung eines LANCOMs über die jeweils geltenden Vorschriften. Informationen zu diesem Thema finden Sie auch in unserem Whitepaper „Public Spot - Rechte und Pflichten eines Betreibers“, welches Sie als Download auf [www.lancom.de](http://www.lancom.de) finden.

Die LANCOM Public Spot Option ist ideal einsetzbar zur Authentifizierung von Mitarbeitern, die Zugang z.B. zu einer Maschine oder einem Netzwerk erhalten wollen. Die Zugangsberechtigungen wird dabei über einen zentralen Server (z.B. in der Produktion) gesteuert. Mitarbeiter müssen sich dann über den Browser jedesmal neu anmelden, sobald sie einen bestimmten IP-Adress-Bereich nutzen wollen.



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

## 8 Rat & Hilfe

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

### 8.1 Es wird keine DSL-Verbindung aufgebaut

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

### 8.2 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](http://www.lancom.de)).

## **8.3 Unerwünschte Verbindungen mit Windows XP**

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

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

## 9 Anhang

### 9.1 Leistungs- und Kenndaten

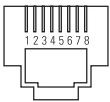
		LANCOM IAP-54 Wireless	LANCOM XAP-40-2	LANCOM XAC-40-1
Frequenzband		2400 - 2483,5 MHz (ISM) oder 5150 - 5750 MHz	Zwei WLAN-Module mit jeweils 2400 - 2483,5 MHz (ISM) oder 5150 - 5750 MHz	2400 - 2483,5 MHz (ISM) oder 5150 - 5750 MHz
Anschlüsse	LAN	10/100Base-TX, Auto-sensing, Auto Node-Hub	2x 10/100Base-TX, Auto-sensing, Auto Node-Hub	10/100Base-TX, Auto-sensing, Auto Node-Hub
	WAN	Verwendung eines LAN Anschlusses für gleichzeitiges DSL-over-LAN (DSLolL).		
	WLAN1	2x Reverse SMA-Buchse mit Antenna Diversity	2x Reverse SMA-Buchse mit Antenna Diversity	2x Reverse SMA-Buchse mit Antenna Diversity
	WLAN2		2x Reverse SMA-Buchse mit Antenna Diversity	
Stromversorgung		Ausschließlich über Power-over-Ethernet. Ein PoE Injector im Lieferumfang.	<ul style="list-style-type: none"> <li>■ 12V DC über externes Netzteil</li> <li>■ 2x Power-over-Ethernet nach IEEE 802.3af (redundant)</li> <li>■ 2x 24 V DC an Industriestecker (redundant)</li> </ul>	<ul style="list-style-type: none"> <li>■ 12V DC über externes Netzteil</li> <li>■ Power-over-Ethernet nach IEEE 802.3af (redundant)</li> <li>■ 2x 24 V DC an Industriestecker (redundant)</li> </ul>
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 <a href="http://www.lancom.de">www.lancom.de</a>		
Gehäuse		IP50-geschütztes Gehäuse, 225 mm x 145 mm x 45 mm (B x H x T), robustes Metallgehäuse, für Wand-, Mast- und Hutschienenmontage vorbereitet.	IP40-geschütztes Gehäuse, ca. 8 x 12 x 13 cm (B x H x T), robustes Metallgehäuse, für Wand- und Hutschienenmontage vorbereitet.	IP40-geschütztes Gehäuse, ca. 8 x 12 x 13 cm (B x H x T), robustes Metallgehäuse, für Wand- und Hutschienenmontage vorbereitet.
Normen		Das Gerät entspricht den Anforderungen folgender Normen: EN 300328, EN 301893, EN 301489-1, EN 301489-17, EN 61000-6-2, EN 60950		
Zulassungen		Notifiziert in den Ländern Deutschland, Belgien, Niederlande, Luxemburg, Österreich, Schweiz, Großbritannien, Italien, Frankreich, Tschechien, Dänemark, Spanien		

	LANCOM IAP-54 Wireless	LANCOM XAP-40-2	LANCOM XAC-40-1
Umgebung/Temperatur	0 °C bis +50 °C bei 95 % max. Luftfeuchtigkeit (nicht kondensierend)	-20 °C bis +50 °C bei 95 % max. Luftfeuchtigkeit (nicht kondensierend)	-20 °C bis +50 °C bei 95 % max. Luftfeuchtigkeit (nicht kondensierend)
Service	Garantie 3 Jahre		
Support	Über Hotline und Internet		

## 9.2 Anschlussbelegung


### 9.2.1 LAN-Schnittstelle 10/100Base-TX, DSL-Schnittstelle

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

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

## 9.2.2 Konfigurationsschnittstelle (Outband)

8-polige Mini-DIN-Buchse

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

DE

## 9.3 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](http://www.lancom.de)).



# Index

## Numerics

10/100Base-TX	19, 27
100-Mbit-Netz	19, 27
802.11i	12, 45, 46, 47, 50, 51
802.11i/	47
802.1x	12, 45, 47
802.3af-Standard	25

## A

Access Control List	46
Access Point-Modus	15
ACL	46
AES	47
Anschlussbelegung	86
Konfigurationsschnittstelle	87
LAN-Schnittstelle	86
Outband	87
Antennen	
Dualband	14
Antennen-Kalkulator	59
Antennen-Leistungen	62
autark	15
Autosensing	19, 23, 27

## C

Client-Modus	70, 72
Closed Network	45

## D

Default-Gateway	53
DFS	59
DHCP	44
DHCP-Server	11, 34, 42, 44
DNS	
DNS-Server	11, 44
Dokumentation	14
Download	5
DSLoL	19, 23, 27
DSL-Übertragung zu langsam	83

DSL-Übertragungsprotokoll	43
DSL-Verbindung	
Probleme beim Aufbau	83
Dynamic Frequency Selection	59
dynamische Frequenzwahl	59

## E

EAP	12, 45, 47
-----	------------

## F

Fernkonfiguration	38, 43
Firewall	11, 12, 53
Stationen sperren	53
Firewall-Filter	77
FirmSafe	13
Firmware	5
Flatrate	75
Fresnel-Zone	61
Funk-LANs	
Betriebsarten	10

## G

Gebührenschatz	39, 43
Gebührenschatz zurücksetzen	17
Gebührensperre	17

## H

Hinweis-Symbole	5
-----------------	---

## I

ICMP	53
Installation	14
Antennen	21
LAN	22
LANtools	31
Netzteil	24
Internet-Anbieter	75
Internet-Zugang	11, 75
Authentifizierungsdaten	75
Flatrate	75

IP			
Filter		53	
Ports sperren		53	
IP-Adresse	34, 35,	53	
IP-Masquerading		12, 52	
IPSec-over-WLAN		45	
<b>K</b>			
Kennwort		36, 38	
Konfigurationsdatei		53	
Konfigurationskabel	19, 27,	30	
Konfigurationskennwort		51	
Konfigurationsschutz		36	
Konfigurationszugriff		38, 43	
Konformitätserklärungen		87	
<b>L</b>			
LAN-Anschluss		19, 27	
LANCOM Enhanced Passphrase Security		45	
LANCOM Public Spot Option		82	
LANconfig		32, 37	
Assistenten aufrufen		77	
LANmonitor		32	
LANtools			
Systemvoraussetzungen		15	
LEPS		12, 46	
Loader		15	
<b>M</b>			
MAC-Adressfilter		12	
Managed-Modus		15	
Montagematerial		14	
Multi SSID		11	
Multimode		43	
<b>N</b>			
NAT – siehe IP-Masquerading			
Netzmaske	34, 35,	53	
Netzteil		19	
<b>O</b>			
Optionale Antennen		79	
Optionen und Zubehör			79
<b>P</b>			
P2P			46
PAT – siehe IP-Masquerading			
PoE Power Injector			14
Point-to-Point			46
Power-over-Ethernet			25
Punkt-zu-Punkt			57
<b>R</b>			
RADIUS			47
Routing-Tabelle			53
<b>S</b>			
serielles Konfigurationskabel	19, 27,	30	
Sicherheit			
Internet-Zugriff			45
Schutz der Konfiguration			45
Sicherheits-Checkliste			50
Sicherheits-Einstellungen			83
SNMP			
Konfiguration schützen			52
Software-Installation			31
SSID		36, 38, 43,	72
Standard-Gateway			44
Stateful Inspection Firewall			11
Stateful-Inspection-Firewall			77
Statusanzeigen			
Power			16, 17, 26
Wireless Link			17, 26
Super AG			11
Support			5
Systemvoraussetzungen			15
<b>T</b>			
TCP			53
TCP/IP			15
Einstellungen			34, 42
TCP/IP-Filter			12, 53
TCP/IP-Konfiguration			
automatisch			42

■ *Index*

manuell	34, 35
vollautomatisch	34
TCP/IP-Windows-Size	84
Technische Daten	85
Telnet	53
TFTP	53
Turbo Modus	11
<b>U</b>	
Übertragungsprotokoll	83
UDP	53
<b>V</b>	
Verschlüsselungsmethode	73

<b>W</b>	
WEBconfig	39
Aufruf eines Assistenten	41
Kennworteingabe	43
Systemvoraussetzungen	15
WEP	12, 45, 47, 48, 49, 50, 51
<b>WLAN</b>	
Client-Modus	72
Durchsuchte Bänder	72
WPA	12, 45, 46, 47, 50, 51
<b>Z</b>	
Zugang zum Internet einrichten	75