

LANCOM WLC-4006
LANCOM WLC-4025

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

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

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

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

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

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

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

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

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

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom.de

Würselen, September 2007

Ein Wort vorab

Vielen Dank für Ihr Vertrauen!

Die WLAN Controller LANCOM WLC-4025 und LANCOM WLC-4006 sind moderne Hardware-Komponenten für ein ebenso einfaches wie sicheres Management mittlerer WLAN-Installationen. Alle Einstellungen werden nur einmal als zentrales Profil im WLAN Controller definiert – der Rest ist echtes „Plug-and-Play“. Neue Access Points werden automatisch gefunden. Alle Konfigurationseinstellungen für die optimale Inbetriebnahme des Funknetzwerks, z. B. Kanaleinstellungen und Sicherheitsrichtlinien werden automatisch an alle Access Points übertragen. Ebenso erfolgt die Funktionsüberwachung des Betriebes (Monitoring inklusive Background-Scanning) zentral über den WLAN Controller.

Dieses deutlich vereinfachte WLAN-Management bietet erhebliche Kosteneinsparungen. So können vorhandene WLAN-Netzwerke durch das „Dazustechen“ eines neuen Access-Points einfach und sicher erweitert werden. Auch entfernte Außenstellen lassen sich – über eine beliebige IP-Verbindung – nahtlos integrieren. Für kleinere Standorte bieten die LANCOM WLAN Controller außerdem einen integrierten RADIUS/EAP-Server.

Gleichzeitig garantieren LANCOM WLAN Controller ein Maximum an Sicherheit, indem alle im Netzwerk vorhandenen LANCOM Access Points automatisch den firmenweiten Sicherheitsrichtlinien entsprechen. Eine permanente Überwachung – auch über Standortgrenzen hinweg – beseitigt vielfach vorhandene Sicherheitslücken.

Zu den besonderen Highlights der LANCOM WLAN Controller gehören u. a.:

- "Smart Controller" für anwendungs- oder benutzerbezogene WLAN-Netzwerke
- Keine separate Verkabelung notwendig - beliebige IP-Verbindung reicht aus
- "Split Management" für LANCOM WLAN Router
- Automatisches Finden und Inbetriebnehmen von Access Points und WLAN Routern
- Zentrale Administration von WLAN-Konfigurationsprofilen
- Überwachen und Sicherstellen der Verschlüsselungs- und QoS-Richtlinien
- Integrierte Funkfeldoptimierung
- Umfangreichste VLAN-, RADIUS- und 802.1x/EAP-Funktionen
- Router, Firewall und VPN-Gateway integriert

■ Ein Wort vorab

- Skalierbar bei Einsatz weiterer Controller, inklusive Redundanz
- Einzigartige Betriebssicherheit ohne "Single-Point-of-Failure"

Sicherheitseinstellungen

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

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

Benutzerhandbuch und Referenzhandbuch

Die Dokumentation Ihres Gerätes besteht aus folgenden Teilen:

- Installation Guide
- Benutzerhandbuch
- Referenzhandbuch

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

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

- Systemdesign des Betriebssystems LCOS
- Konfiguration
- Management
- Diagnose
- Sicherheit
- Routing- und WAN-Funktionen
- Firewall
- Quality-of-Service (QoS)
- Virtuelle Private Netzwerke (VPN)
- Virtuelle lokale Netzwerke (VLAN)

- Funknetzwerke (WLAN)
- Backup-Lösungen
- weitere Server-Dienste (DHCP, DNS, Gebührenmanagement)

An der Erstellung dieser Dokumentation ...

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

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

info@lancom.de



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

1 Einleitung	10
1.1 Zentrales WLAN-Management	10
1.1.1 Der CAPWAP-Standard	11
1.1.2 Die Smart-Controller-Technologie	11
1.1.3 Kommunikation zwischen Access Point und WLAN Controller	14
1.1.4 Zero-Touch-Management	17
1.1.5 Split-Management	17
1.2 Was kann Ihr LANCOM WLAN Controller?	18
2 Installation	21
2.1 Lieferumfang	21
2.2 Systemvoraussetzungen	21
2.2.1 Konfiguration der LANCOM-Geräte	21
2.2.2 Betrieb der Access Points im Managed-Modus	22
2.3 Ihr LANCOM WLAN Controller stellt sich vor	22
2.3.1 Statusanzeigen beim LANCOM WLAN Controller	22
2.3.2 LC-Display	27
2.3.3 Die Anschlüsse des Geräts	27
2.4 Installation der Hardware	30
2.5 Installation der Software	31
2.5.1 LANCOM-Setup starten	31
2.5.2 Welche Software installieren?	32
3 Grundkonfiguration	33
3.1 Welche Angaben sind notwendig?	33
3.1.1 TCP/IP-Einstellungen	33
3.1.2 Konfigurationsschutz	35
3.2 Anleitung für LANconfig	35
3.3 Anleitung für WEBconfig	37
3.4 TCP/IP-Einstellungen an den Arbeitsplatz-PCs	41

4 Konfiguration des WLAN Controllers	43
4.1 Grundeinstellung der LANCOM WLAN Controller	43
4.1.1 Zeitinformation für den LANCOM WLAN Controller einstellen	44
4.1.2 Default-Konfiguration erstellen	45
4.1.3 Zuweisung der Default-Konfiguration zu den neuen Access Points	48
4.2 Erweiterte Einstellungen	49
4.2.1 Allgemeine Einstellungen	49
4.2.2 Profile	50
4.2.3 Liste der Access Points	56
4.2.4 Optionen für den WLAN Controller	58
4.3 Weitere Konfigurations-Details	61
4.3.1 Neue Access Points manuell in die WLAN-Struktur aufnehmen	61
4.3.2 Access Points manuell aus der WLAN-Struktur entfernen	63
4.3.3 Vererbung von Parametern	64
4.3.4 Sicherung der Zertifikate	65
4.3.5 Sichern und Wiederherstellen weiterer Dateien der SCEP-CA	67
4.3.6 Backuplösungen	69
4.3.7 Load-Balancing zwischen den WLAN Controllern	74
4.3.8 Dynamische VLAN-Zuweisung	75
4.3.9 Prüfung der WLAN-Clients über RADIUS (MAC-Filter)	77
4.3.10 Access Point deaktivieren oder dauerhaft aus der WLAN-Struktur entfernen	78
4.4 Anzeigen und Aktionen im LANmonitor	79
4.5 Konfiguration der Access Points	81
5 Sicherheits-Einstellungen	83
5.1 Sicherheit im Funk-LAN	83
5.1.1 SSID Broadcast unterdrücken – geschlossenes Netzwerk	

	(Closed Network)	83
	5.1.2 Zugangskontrolle über MAC-Adresse	84
	5.1.3 LANCOM Enhanced Passphrase Security	84
	5.1.4 Verschlüsselung des Datentransfers	85
	5.1.5 802.1x / EAP	85
	5.1.6 IPSec-over-WLAN	86
	5.2 Tipps für den richtigen Umgang mit Schlüsseln und Passphrases	86
	5.3 Der Sicherheits-Assistent	86
	5.3.1 Assistent für LANconfig	87
	5.3.2 Assistent für WEBconfig	88
	5.4 Der Firewall-Assistent	88
	5.4.1 Assistent für LANconfig	89
	5.4.2 Konfiguration unter WEBconfig	89
	5.5 Die Sicherheits-Checkliste	89
6	Den Internet-Zugang einrichten	94
	6.1 Anleitung für LANconfig	95
	6.2 Anleitung für WEBconfig	96
7	Zwei Netzwerke verbinden	97
	7.1 Welche Angaben sind notwendig?	97
	7.1.1 Allgemeine Angaben	98
	7.1.2 Einstellungen für den TCP/IP-Router	99
	7.1.3 Einstellungen für NetBIOS-Routing	100
	7.2 Anleitung für LANconfig	101
	7.3 1-Click-VPN für Netzwerke (Site-to-Site)	102
	7.4 Anleitung für WEBconfig	103

8 Einwahl-Zugang bereitstellen	105
8.1 Welche Angaben sind notwendig?	105
8.1.1 Allgemeine Angaben	105
8.1.2 Einstellungen für TCP/IP	106
8.1.3 Einstellungen für NetBIOS-Routing	107
8.2 Einstellungen am Einwahl-Rechner	107
8.3 Anleitung für LANconfig	108
8.4 1-Click-VPN für LANCOM Advanced VPN Client	108
8.5 Anleitung für WEBconfig	110
9 Anhang	111
9.1 Leistungs- und Kenndaten	111
9.2 Anschlussbelegung	112
9.2.1 Ethernet-Schnittstellen 10/100Base-T	112
9.2.2 Konfigurationsschnittstelle (Outband)	112
9.3 CE-Konformitätserklärungen	112
10 Index	114

1 Einleitung

1.1 Zentrales WLAN-Management

Der weit verbreitete Einsatz von Wireless Access Points und Wireless Routern hat zu einem deutlich komfortableren und flexibleren Zugang zu Netzwerken in Firmen, Universitäten und anderen Organisationen geführt.

Bei allen Vorzügen der WLAN-Strukturen bleiben einige offene Aspekte:

- Alle Wireless Access Points benötigen eine Konfiguration und ein entsprechendes Monitoring zur Erkennung von unerwünschten WLAN-Clients etc. Die Administration der Access Points erfordert gerade bei größeren WLAN-Strukturen mit entsprechenden Sicherheitsmechanismen eine hohe Qualifikation und Erfahrung der Verantwortlichen und bindet erhebliche Ressourcen in den IT-Abteilungen.
- Die manuelle Anpassung der Konfigurationen in den Access Points bei Änderungen in der WLAN-Struktur zieht sich ggf. über einen längeren Zeitraum hinweg, sodass es zur gleichen Zeit unterschiedliche Konfigurationen im WLAN gibt.
- Durch die gemeinsame Nutzung des geteilten Übertragungsmediums (Luft) ist eine effektive Koordination der Access Points notwendig, um Frequenzüberlagerungen zu vermeiden und die Netzwerkperformance zu optimieren.
- Access Points an öffentlich zugänglichen Orten stellen ein potenzielles Sicherheitsrisiko dar, weil mit den Geräten auch die darin gespeicherten, sicherheitsrelevanten Daten wie Kennwörter etc. gestohlen werden können. Außerdem können ggf. unbemerkt fremde Access Points mit dem LAN verbunden werden und so die geltenden Sicherheitsrichtlinien umgehen.

Mit einem zentralen WLAN-Management werden diese Probleme gelöst. Die Konfiguration der Access Points wird dabei nicht mehr in den Geräten selbst vorgenommen, sondern in einer zentralen Instanz, dem WLAN Controller. Der WLAN Controller authentifiziert die Access Points und überträgt den zugelassenen Geräten eine passende Konfiguration. Dadurch kann die Konfiguration des WLANs komfortabel von einer zentralen Stelle übernommen werden und die Konfigurationsänderungen wirken sich zeitgleich auf alle Access Points aus. Da die vom WLAN Controller zugewiesene Konfiguration in den Access Points in der Regel **nicht** im Flash, sondern im RAM abgelegt wird, können bei einem Diebstahl der Geräte auch keine sicherheitsrelevanten Daten in

unbefugte Hände geraten. Nur im „autarken Weiterbetrieb“ (‘Autarker Weiterbetrieb’ → Seite 53) wird die Konfiguration für eine definierte Zeit optional im Flash gespeichert (in einem Bereich, der nicht mit LANconfig oder anderen Tools auszulesen ist).

1.1.1 Der CAPWAP-Standard

Mit dem CAPWAP-Protokoll (Control And Provisioning of Wireless Access Points) stellt die IETF (Internet Engineering Task Force) einen Draft-Standard für das zentrale Management großer WLAN-Strukturen vor.

CAPWAP verwendet zwei Kanäle für die Datenübertragung:

- Kontrollkanal, verschlüsselt mit DTLS. Über diesen Kanal werden die Verwaltungsinformationen zwischen dem WLAN Controller und dem Access Point ausgetauscht.



Das Datagram Transport Layer Security (DTLS) ist ein auf TLS basierendes Verschlüsselungsprotokoll, welches im Gegensatz zu TLS auch über unzuverlässige Transportprotokolle wie UDP übertragen werden kann. DTLS verbindet so die Vorteile der hohen Sicherheit von TLS mit der schnellen Übertragung über UDP. DTLS eignet sich damit – anders als TLS – auch für die Übertragung von VoIP-Paketen, da hier nach einem Paketverlust die folgenden Pakete wieder authentifiziert werden können.

- Datenkanal, optional ebenfalls verschlüsselt mit DTLS. Über diesen Kanal werden die Nutzdaten aus dem WLAN vom Access Point über den WLAN Controller ins LAN übertragen – gekapselt in das CAPWAP-Protokoll.

1.1.2 Die Smart-Controller-Technologie

In einer dezentralen WLAN-Struktur mit autonomen Access Points (Stand-Alone-Betrieb als so genannte „Rich Access Points“) sind alle Funktionen für die Datenübertragung auf dem PHY-Layer, die Kontroll-Funktionen auf dem MAC-Layer sowie die Management-Funktionen in den Access Points enthalten. Mit dem zentralen WLAN-Management werden diese Aufgaben auf zwei verschiedene Geräte aufgeteilt:

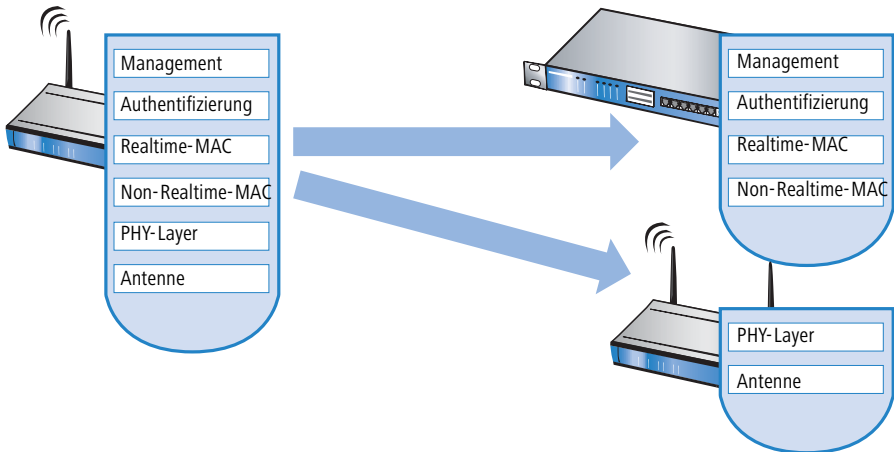
- Der zentrale WLAN Controller übernimmt die Verwaltungsaufgaben.
- Die verteilten Access Points übernehmen die Datenübertragung auf dem PHY-Layer und die MAC-Funktionen.

■ Kapitel 1: Einleitung

- Als dritte Komponente kommt ggf. ein RADIUS- oder EAP-Server zur Authentifizierung der WLAN-Clients hinzu (was in autonomen WLANs aber auch der Fall sein kann).

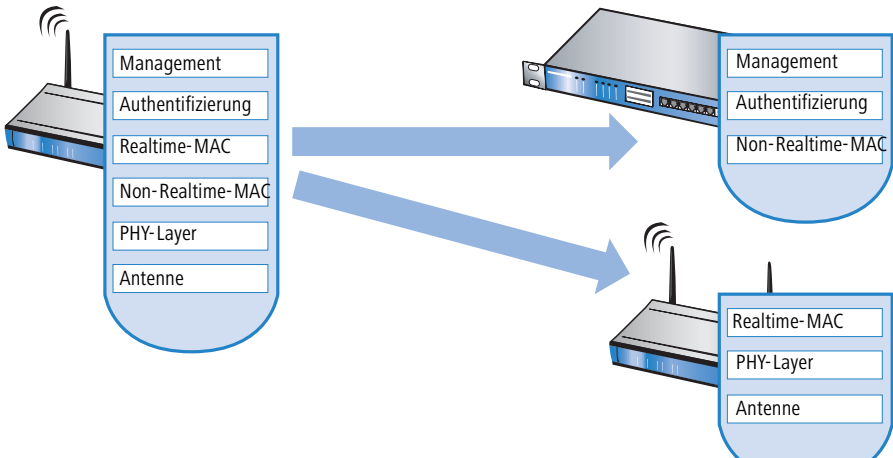
CAPWAP beschreibt drei unterschiedliche Szenarien für die Verlagerung von WLAN-Funktionen in den zentralen WLAN Controller.

- Remote-MAC: Hier werden alle WLAN-Funktionen vom Access Point an den WLAN Controller übertragen. Die Access Points dienen hier nur als „verlängerte Antennen“ ohne eigene Intelligenz.

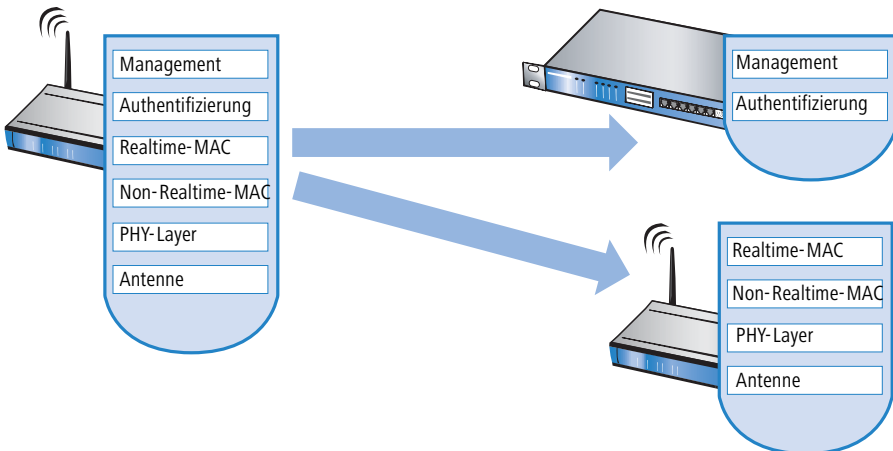


- Split-MAC: Bei dieser Variante wird nur ein Teil der WLAN-Funktionen an den WLAN Controller übertragen. Üblicherweise werden die zeitkritischen Anwendungen (Realtime-Applikationen) weiterhin auf dem Access Point

abgearbeitet, die nicht zeitkritischen Anwendungen (Non-Realtime-Applikationen) werden über den zentralen WLAN Controller abgewickelt.



- **Local-Mac:** Die dritte Möglichkeit sieht eine vollständige Verwaltung und Überwachung des WLAN-Datenverkehrs direkt in den Access Points vor. Zwischen dem Access Point und dem WLAN Controller werden lediglich Nachrichten zur Sicherung einer einheitlichen Konfiguration der Access Points und zum Management des Netzwerks ausgetauscht.



Die Smart-Controller-Technologie von LANCOM Systems setzt das Local-MAC-Verfahren ein. Durch die Reduzierung der zentralisierten Aufgaben bieten die WLAN-Strukturen eine optimale Skalierbarkeit. Gleichzeitig wird der

WLAN Controller in einer solchen Struktur nicht zum zentralen Flaschenhals, der große Teile des gesamten Datenverkehrs verarbeiten muss. In Remote-MAC- und Split-MAC-Architekturen müssen immer **alle** Nutzdaten zentral über den WLAN Controller laufen. In Local-MAC-Architekturen können die Daten jedoch alternativ auch direkt von den Access Points in das LAN ausgekoppelt werden, sodass eine hochperformante Datenübertragung ermöglicht wird. WLAN Controller von LANCOM eignen sich daher auch für WLANs nach dem Standard IEEE 802.11n mit deutlich höheren Bandbreiten als in den bisher bekannten WLANs. Bei der Auskopplung in das LAN können die Daten auch direkt in spezielle VLANs geleitet werden, die Einrichtung von geschlossenen Netzwerken z. B. für Gast-Zugänge sind so leicht möglich.

CAPWAP-Tunneling und Layer-3-Roaming

In einer späteren LCOS-Version unterstützen die LANCOM WLAN Controller auch die Übertragung der Nutzdaten durch einen CAPWAP-Tunnel.

- Auf diese Weise können z.B. ausgewählte Applikationen wie VoIP über den zentralen WLAN Controller geleitet werden. Beim Wechsel der WLAN-Clients in eine andere Funkzelle bleibt so die zugrundeliegende IP-Verbindung ohne Unterbrechung, da sie fortlaufend vom zentralen WLAN Controller verwaltet wird (Layer-3-Roaming). Mobile SIP-Telefone können auf diese Weise auch während eines Gesprächs komfortabel „roamen“.
- Die zentrale Verwaltung der Datenströme kann in Umgebungen mit zahlreichen VLANs auch die Konfiguration der VLANs auf den Switch-Ports überflüssig machen, da alle CAPWAP-Tunnel zentral auf dem WLAN Controller verwaltet werden.

1.1.3 Kommunikation zwischen Access Point und WLAN Controller



Ab der Firmware-Version LCOS 7.20 unterscheiden sich LANCOM Access Points (z. B. LANCOM L-54ag) und LANCOM Wireless Router (z. B. LANCOM 1811 Wireless) bzgl. der Einstellung der WLAN-Module im Auslieferungszustand. In den folgenden Beschreibungen wird meistens der übergreifende Begriff „Access Point“ verwendet.

Die Kommunikation zwischen einem Access Point und dem WLAN Controller wird immer vom Access Point aus eingeleitet. Die Geräte suchen in folgenden Fällen nach einem WLAN Controller, der ihnen eine Konfiguration zuweisen kann:

- Ein LANCOM Access Point befindet sich im Auslieferungszustand und ist noch nicht konfiguriert. In diesem Zustand sind die WLAN-Module ausgeschaltet, der Access Point sucht im LAN nach einem WLAN Controller.

- Ein LANCOM Access Point ist bereits konfiguriert, für mindestens ein WLAN-Modul ist manuell die Betriebsart auf 'Managed' eingestellt ('Konfiguration der Access Points' → Seite 81). Der Access Point sucht für das oder die entsprechenden WLAN-Module im LAN nach einem WLAN Controller.
- Ein LANCOM Wireless Router ist bereits konfiguriert, für mindestens ein WLAN-Modul ist manuell die Betriebsart auf 'Managed' eingestellt. Der Wireless Router sucht für das oder die entsprechenden WLAN-Module im LAN nach einem WLAN Controller.

Der Access Point sendet zu Beginn der Kommunikation eine „Discovery Request Message“, um die verfügbaren WLAN Controller zu ermitteln. Dieser Request wird grundsätzlich als Broadcast versendet. Da in manchen Strukturen ein potenzieller WLAN Controller aber nicht über Broadcast zu erreichen ist, können auch spezielle Adressen von weiteren WLAN Controllern in die Konfiguration der Access Points eingetragen werden.



Außerdem können auch DNS-Namen von WLAN Controllern aufgelöst werden. Alle Access Points mit LCOS 7.22 oder höher haben den Standardnamen 'WLC-Address' bereits konfiguriert, sodass ein DNS-Server diesen Namen zu einem LANCOM WLAN Controller auflösen kann. Somit können auch WLAN Controller erreicht werden, die nicht im gleichen Netz stehen, ohne die Access Points konfigurieren zu müssen.

Aus den verfügbaren WLAN Controllern wählt der Access Point den Besten aus und fragt bei diesem nach dem Aufbau der DTLS-Verbindung an. Der „beste“ WLAN Controller ist für den Access Point derjenige mit der geringsten Auslastung, also dem kleinsten Verhältnis von gemanagten Access Points zu den maximal möglichen Access Points. Bei zwei oder mehreren gleich „guten“ WLAN Controllern wählt der Access Point den im Netzwerk nächsten, also den mit der geringsten Antwortzeit.

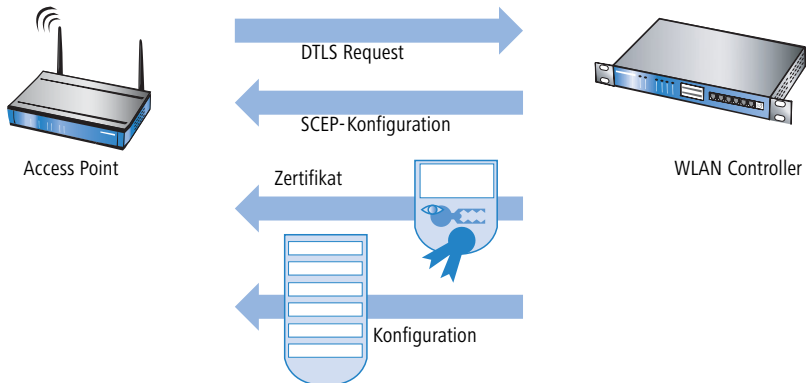
Der WLAN Controller ermittelt daraufhin mit einer internen Zufallszahl einen eindeutigen und sicheren Sitzungsschlüssel, mit dem er die Verbindung zum Access Point schützt. Außerdem erstellt der WLAN Controller automatisch ein selbst signiertes Zertifikat für den Access Point, über den sich dieser in der Folgezeit gegenüber dem WLAN Controller eindeutig authentifizieren kann.

Über die gesicherte DTLS-Verbindung wird dem Access Point die Konfiguration für den integrierten SCEP-Client mitgeteilt – der Access Point kann dann

über SCEP sein Zertifikat bei der SCEP-CA abholen. Anschließend wird die dem Access Point zugewiesene Konfiguration übertragen.

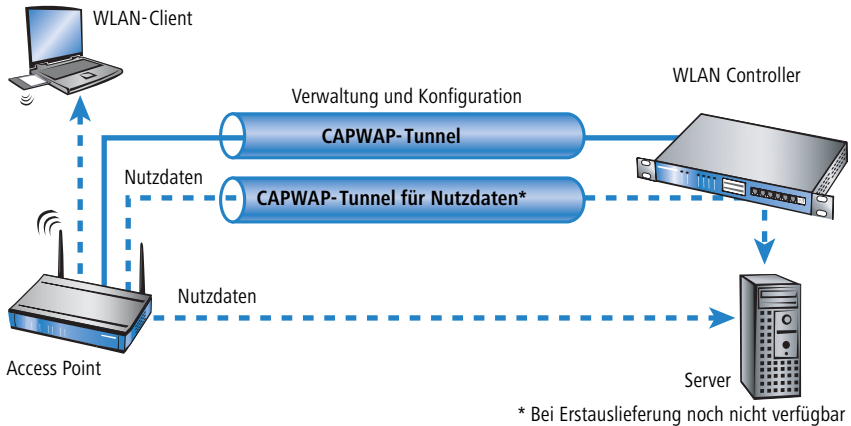


SCEP steht für Simple Certificate Encryption Protocol, CA für Certification Authority. Weitere Informationen über digitale Zertifikate, CAs und SCEP finden Sie im LCOS-Referenzhandbuch.



Sowohl Authentifizierung als auch Konfiguration können entweder automatisch vorgenommen werden oder nur bei passendem Eintrag der MAC-Adresse des Access Point in der AP-Tabelle des WLAN Controller. Sofern bei dem Access Point die WLAN-Module bei Beginn der DTLS-Kommunikation ausgeschaltet waren, werden diese nach erfolgreicher Übertragung von Zertifikat und Konfiguration eingeschaltet (sofern sie nicht in der Konfiguration explizit ausgeschaltet sind).

In der Folgezeit werden über den CAPWAP-Tunnel die Verwaltungs- und Konfigurationsdaten übertragen. Die Nutzdaten vom WLAN-Client werden im Access Point direkt in das LAN ausgekoppelt und z. B. an den Server übertragen.



1.1.4 Zero-Touch-Management

Mit der Möglichkeit, den anfragenden Access Points Zertifikat und Konfigurationen automatisch zuweisen zu lassen, realisieren die LANCOM WLAN Controller ein echtes „Zero-Touch-Management“. Neue Access Points müssen nur noch mit dem LAN verbunden werden, es sind keine weiteren Konfigurationsschritte erforderlich. Diese Reduzierung auf die reine Installation der Geräte entlastet die IT-Abteilungen gerade bei verteilten Strukturen, da in den entfernten Standorten kein spezielles IT- oder WLAN-Know-How zur Inbetriebnahme erforderlich ist.

1.1.5 Split-Management

LANCOM Access Point können ihren WLAN Controller auf in entfernten Netzen suchen – eine einfache IP-Verbindung z. B. über eine VPN-Strecke reicht aus. Da die WLAN Controller nur den WLAN-Teil der Konfiguration im Access Point beeinflussen, können alle anderen Funktionen separat verwaltet werden. Durch diese Aufteilung der Konfigurationsaufgaben können LANCOM WLAN Controller ideal für den Aufbau einer firmenweiten WLAN-Infrastruktur in der Zentrale inklusive aller angeschlossenen Niederlassungen und Home-Offices eingesetzt werden.

1.2 Was kann Ihr LANCOM WLAN Controller?

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

	LANCOM WLC- 4006	LANCOM WLC- 4025
WLAN-Controlling		
Anzahl gemanagter Geräte	6	25
Automatisches Finden der WLAN Controller durch die LANCOM Access Points oder WLAN Router	✓	✓
Automatische oder manuelle Authentifizierung der Access Points	✓	✓
Kommunikation zwischen Controller und Access Points über einfache IP-Verbindung mit CAPWAP	✓	✓
Verschlüsselung der Kontrolldaten mit DTLS, inklusive HW-Krypto-Beschleuniger	✓	✓
Vererbung von Konfigurationsprofilen, auch mehrstufig	✓	✓
Autarker Weiterbetrieb für den optionalen Weiterbetrieb auch bei Unterbrechung der Verbindung zum WLAN Controller	✓	✓
Advanced Routing and Forwarding (ARF) mit individuellen DHCP-, DNS-, Routing-, Firewall- und VPN-Funktionen für diese Netze, Zuordnung der Netze zu SSIDs im WLAN-Profil über VLAN-IDs.	16 Netze	16 Netze
Dynamische VLAN-Zuweisung für bestimmte Benutzergruppen anhand von MAC-Adressen, BSSID oder SSID mittels externem RADIUS-Server.	✓	✓
Integrierter RADIUS-Server zur Verwaltung von MAC-Adress-Listen	✓	✓
Integrierter EAP-Server zur Authentifizierung von 802.1x Clients mittels EAP-TLS, EAP-TTLS, PEAP, MSCHAP oder MSCHAPv2	✓	✓
Proxy-Betriebsart für externe RADIUS/EAP-Server (Forwarding und Realm Handling)	✓	✓
802.11e / WME: Automatisches VLAN-Tagging (802.1p) in den Access Points. Umsetzung auf DiffServ-Attribute im WLAN Controller, sofern dieser als Layer-3-Router zum Einsatz kommt	✓	✓
Fast Roaming über PMK-Caching und Pre-Authentication	✓	✓
Weitere Anwendungen		
Internet-Zugang	✓	✓
LAN-LAN-Kopplung über VPN	✓	✓
RAS-Server (über VPN)	✓	✓

	LANCOM WLC- 4006	LANCOM WLC- 4025
IP-Router	✓	✓
DHCP- und DNS-Server (für alle ARF-Netze getrennt)	✓	✓
N:N-Mapping zum Routen von Netzwerken mit den gleichen IP-Adresskreisen über VPN	✓	✓
Konfiguration eines LAN-Ports als WAN-Port	✓	✓
Policy-based Routing zur regelbasierten Auswahl der Zielroute	✓	✓
NAT Traversal (NAT-T)	✓	✓
PPPoE-Server	✓	✓
Layer-2-QoS-Tagging	✓	✓
802.1p	✓	✓
WAN-Anschlüsse		
Anschluss für DSL-Modem	✓	✓
LAN-Anschluss		
Uplink-Interface zum Anschluss an das LAN. Alternativ schaltbar als LAN-Interface oder als WAN-Interface zum Anschluss eines SDSL-Modems.	1	1
Individuelle Fast Ethernet LAN Ports, einzeln schaltbar, z.B. als LAN-Switch oder separate DMZ-Ports, Auto-Crossover. Alternativ schaltbar als WAN-Interface zum Anschluss eines SDSL-Modems.	4	4
Sicherheitsfunktionen		
IPSec-Verschlüsselung über externe Software (VPN-Client)	✓	✓
5 integrierte VPN-Tunnel zur Absicherung von Netzwerkverbindungen	✓	✓
DTLS- und IPSec-Verschlüsselung über Hardware	✓	✓
IP-Masquerading (NAT, PAT) zum Verstecken aller Arbeitsstationen im LAN hinter einer einheitlichen öffentlichen IP-Adresse.	✓	✓
Stateful-Inspection-Firewall	✓	✓
Firewall-Filter zur gezielten Sperrung von IP-Adressen, Protokollen und Ports	✓	✓
MAC-Adressfilter kontrolliert u.a. den Zugriff von Arbeitsstationen im LAN auf die IP-Routing-Funktion	✓	✓

■ Kapitel 1: Einleitung

	LANCOM WLC- 4006	LANCOM WLC- 4025
Konfigurationsschutz zur Abwehr von „Brute-Force-Angriffen“.	✓	✓
Konfiguration		
Konfiguration mit LANconfig oder mit Webbrowser, zusätzlich Terminalmodus für Telnet oder andere Terminalprogramme, SNMP-Schnittstelle und TFTP-Serverfunktion	✓	✓
Serielle Konfigurations-Schnittstelle	✓	✓
FirmSafe zum Einspielen neuer Firmwareversionen ohne Risiko	✓	✓
Optionale Software-Erweiterungen		
LANCOM WLAN Controller-12-Option zur Verwaltung von bis zu 12 Access Points	✓	
LANCOM WLAN Controller-50-Option zur Verwaltung von bis zu 50 Access Points		✓
LANCOM Service-Option	✓	✓

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 einfach.

2.1 Lieferumfang

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

	LANCOM WLC-4006	LANCOM WLC-4025
Kaltgerätekabel		✓
Netzteil	✓	
CAT5-LAN-Anschlusskabel (grüne Stecker)	✓	✓
RS232-Anschlusskabel für die Konfigurationsschnittstelle	✓	✓
GummifüÙe, 19"-Montagewinkel		✓
LANCOM-CD	✓	✓
Gedruckter Installation Guide	✓	✓
Gedrucktes Benutzerhandbuch	✓	✓
Gedrucktes Referenzhandbuch		✓

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

2.2 Systemvoraussetzungen

2.2.1 Konfiguration der LANCOM-Geräte

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

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



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

2.2.2 Betrieb der Access Points im Managed-Modus

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



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

2.3 Ihr LANCOM WLAN Controller stellt sich vor

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



Für die Installation des Gerätes ist dieser Abschnitt hilfreich aber nicht unbedingt erforderlich. Sie können diesen Abschnitt nach Belieben auch erst einmal überschlagen und direkt mit dem Abschnitt 'Installation der Hardware' auf Seite 30 fortfahren.

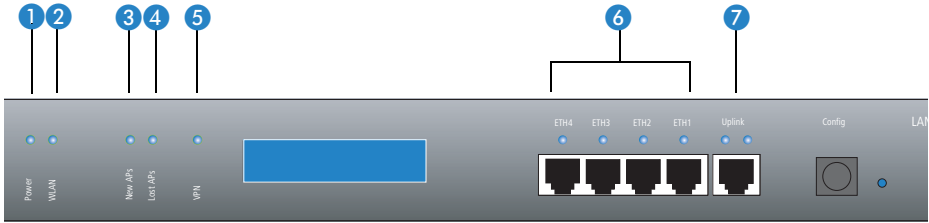
2.3.1 Statusanzeigen beim LANCOM WLAN Controller

Auf der Vorderseite des Geräts finden Sie eine Reihe von Leuchtdioden (LEDs), die Informationen über den Status des Geräts geben.

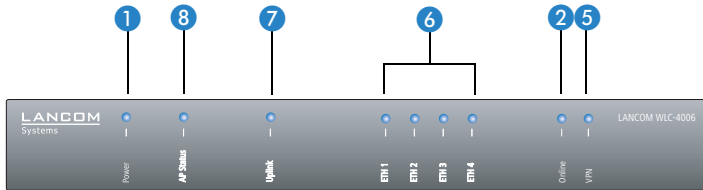
Vorderseite

Die verschiedenen LANCOM WLAN Controller-Modelle verfügen je nach Funktionsumfang über eine unterschiedliche Anzahl von Statusanzeigen auf der Vorderseite.

LANCOM WLC-4025



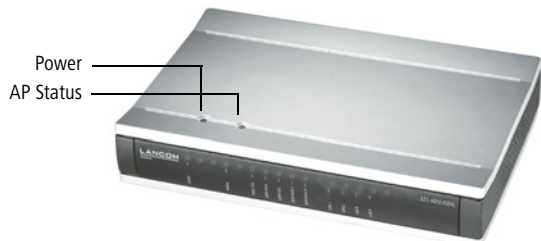
LANCOM WLC-4006



Oberseite

Nur LANCOM WLC-4006

Die beiden LEDs auf der Oberseite des LANCOM WLC-4006 ermöglichen ein bequemes Ablesen der wichtigsten Statusanzeigen auch bei vertikaler Befestigung des Gerätes.



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.

■ Kapitel 2: Installation

1 Power

- **Flackern** bedeutet, dass die LED in unregelmäßigen Abständen ein- und ausgeschaltet wird.

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

aus		Gerät abgeschaltet
grün	blinkend	Selbsttest nach dem Einschalten
grün	dauerhaft an	Gerät betriebsbereit
rot/grün	abwechselnd blinkend	Gerät unsicher: Kein Konfigurationskennwort gesetzt
rot	blinkend	Zeitlimit für Online-Verbindungen erreicht



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

2 WLAN (nur LANCOM WLC-4025)

Gibt Informationen über die Betriebsbereitschaft des Geräts und die verbundenen Access Points. Die WLAN-Anzeige kann folgende Zustände annehmen:

rot	dauerhaft an	Der LANCOM WLAN Controller ist noch nicht betriebsbereit, es fehlt eines der folgenden Elemente: <ul style="list-style-type: none"> ■ Root-Zertifikat ■ Geräte-Zertifikat ■ aktuelle Uhrzeit ■ Zufallszahl für die DTLS-Verschlüsselung
rot	blinkend	Das Gerät ist betriebsbereit, aber nicht mit einem aktiven Access Point verbunden.
grün	dauerhaft an	Mindestens ein aktiver Access Point verbunden und authentifiziert.



Der Grund für eine fehlende Betriebsbereitschaft wird im Display genauer angezeigt.

- 3 New APs
(nur LANCOM
WLC-4025)

Gibt Informationen über neue Access Points. Die New-AP-Anzeige kann folgende Zustände annehmen:

orange	blinkend	Mindestens ein neuer Access Point zur Authentifizierung gefunden.
--------	----------	---

- 4 Lost APs
(nur LANCOM
WLC-4025)

Gibt Informationen über verlorene Access Points. Die Lost-AP-Anzeige kann folgende Zustände annehmen:

rot	blinkend	Mindestens ein erwarteter Access Point wurde nicht gefunden.
-----	----------	--

- 5 VPN

Status einer VPN-Verbindung.

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

- 6 ETH

Zustand der LAN-Anschlüsse im integrierten Switch:

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

- 7 Uplink

Gibt Informationen über die Verbindung zum WAN und zum LAN. Die WAN-LED wird nur aktiv, wenn die Uplink-Schnittstelle als DSL-Interface konfiguriert ist. Die Uplink-Anzeige kann folgende Zustände annehmen:

		linke LED (WAN)	rechte LED
aus		keine aktive WAN-Verbindung aufgebaut	keine Verbindung
grün	blinkend	Verbindungsaufbau	
grün	blitzend	Verbindungsaufbau: erste Verbindung	

■ Kapitel 2: Installation

		linke LED (WAN)	rechte LED
grün	invers blitzend	Verbindungsaufbau: weitere Verbindungen	
grün	dauerhaft an	Verbindung aufgebaut	Verbindung aufgebaut
grün	flackernd		Datenverkehr (Versand oder Empfang)
rot	dauerhaft an	Letzter Verbindungsaufbauwunsch fehlgeschlagen. Fehlerstatus wird gelöscht, wenn Verbindung steht oder im LANmonitor gelöscht wird.	

8 AP-Status (nur LANCOM WLC-4006)

Gibt Informationen über die Betriebsbereitschaft des Geräts und die verbundenen Access Points. Die AP-Status-Anzeige kann folgende Zustände annehmen:

rot	dauerhaft an	Der LANCOM WLAN Controller ist noch nicht betriebsbereit, es fehlt eines der folgenden Elemente: <ul style="list-style-type: none"> ■ Root-Zertifikat ■ Geräte-Zertifikat ■ aktuelle Uhrzeit ■ Zufallszahl für die DTLS-Verschlüsselung
rot	blinkend	Mindestens ein erwarteter Access Point fehlt.
grün/ orange	blinkend	Mindestens ein neuer Access Point.
grün	dauerhaft an	Mindestens ein aktiver Access Point verbunden und authentifiziert, kein neuer und kein fehlender Access Point.

Statusanzeigen bei den Access Points

Die Access Points zeigen über die LEDs den Status der Verbindung zum LANCOM WLAN Controller an.

- Wenn sich ein Access Point im Managed-Modus befindet und nach einem WLAN Controller sucht, blinken die LEDs im Deckel des Geräts abwechselnd **grün** und **orange**.
- Findet der Access Point im Managed-Modus einen WLAN Controller, der ihm aufgrund einer ungeeigneten Firmware- bzw. Loader-Version keine Konfiguration zuweisen kann, blinken die LEDs im Deckel des Geräts abwechselnd **rot** und **orange**. Erst nach einem Update von Firmware

und/oder Loader kann der Access Point von einem WLAN Controller angenommen werden.

Sobald der Access Point die Verbindung mit dem WLAN Controller hergestellt hat, übernehmen die LEDs wieder ihre normale Aufgabe wie im Benutzerhandbuch zum jeweiligen Modell beschrieben.

2.3.2 LC-Display

Nur LANCOM WLC-4025

Das Display des LANCOM WLC-4025 zeigt in zwei Zeilen mit je 16 Zeichen folgende Informationen umlaufend im Wechsel an:

- ▶ Geräteame
- ▶ Firmwareversion
- ▶ Temperatur
- ▶ Datum und Zeit
- ▶ CPU-Auslastung
- ▶ Speicherauslastung
- ▶ Anzahl der VPN-Tunnel
- ▶ Anzahl der authentifizierten Access Points
- ▶ Anzahl der erwarteten Access Points (aktiv konfiguriert)
- ▶ Anzahl der neu gefundenen und noch nicht authentifizierten Access Points
- ▶ Anzahl der nicht vorhandenen erwarteten Access Points

Sofern die WLAN-LED dauerhaft rot leuchtet, zeigt das Display außerdem folgenden Informationen:

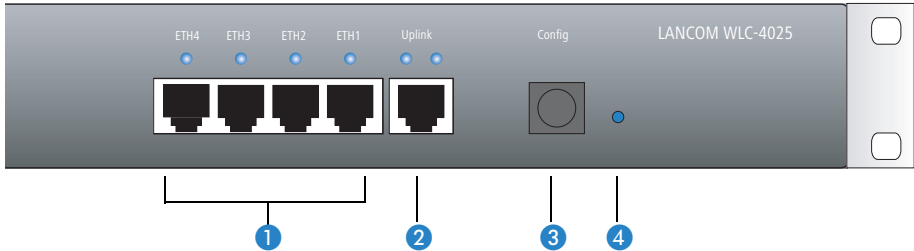
- ▶ Füllstand des Zufallszahlenspeichers
- ▶ SNTP-Status
- ▶ SCEP-Status

2.3.3 Die Anschlüsse des Geräts

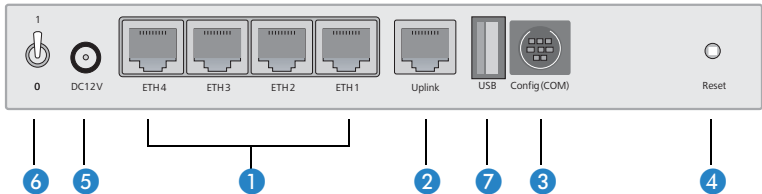
Die Anschlüsse und Schalter des Routers sind auf Vorder- und Rückseite verteilt:

■ Kapitel 2: Installation

LANCOM WLC-4025



LANCOM WLC-4006



Auf der Vorder- und Rückseite des LANCOM WLC-4025 bzw. auf der Rückseite des LANCOM WLC-4006 befinden sich die folgenden Anschlüsse:

- 1 Vier 10/100Base-Tx-Anschlüsse für lokale Netzwerke
- 2 Uplink-Anschluss
- 3 Serielle Konfigurationsschnittstelle
- 4 Reset-Taster
- 5 Anschluss für das Kaltgerätekabel (LANCOM WLC-4025) bzw. Netzteil (LANCOM WLC-4006)
- 6 Netzschalter
- 7 USB-Anschluss (nur LANCOM WLC-4006)

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.
- 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.



Bei einem harten Reset startet das Gerät mit Werkseinstellungen neu, alle bisherigen Einstellungen gehen dabei verloren! Dabei verlieren auch alle Access Points, die von diesem WLAN Controller verwaltet werden, je nach Einstellung des autarken Weiterbetriebes ('Autarker Weiterbetrieb' → Seite 53) ihre Konfiguration.




Bitte beachten Sie folgenden Hinweis: Mit den Einstellungen '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.

2.4 Installation der Hardware

Die Installation des LANCOM Router erfolgt in folgenden Schritten:

- ① **LAN** – schließen Sie Ihren LANCOM WLAN Controller zunächst ans LAN an. Stecken Sie das mitgelieferte Netzwerkkabel (grüne Stecker) einerseits in die Uplink-Buchse des Geräts ② und andererseits in eine freie Netzwerkanschlussdose Ihres lokalen Netzes, eine freie Buchse oder eines Switches/Hubs.


 In einem Netzwerksegment sollten sich niemals mehrere unkonfigurierte LANCOM gleichzeitig befinden. Alle unkonfigurierten LANCOM melden sich unter derselben IP-Adresse (mit den Endziffern '254'), es kommt daher zu Adresskonflikten. Zur Vermeidung von Problemen sollten mehrere LANCOM immer nacheinander konfiguriert und jeweils sofort mit einer eindeutigen IP-Adresse (die nicht auf '254' endet) versehen werden.

- ② **Weitere Netzwerkgeräte** – optional können Sie an die LAN-Schnittstellen ① weitere Netzwerkgeräte anschließen.

Die LAN-Anschlüsse erkennen sowohl die Übertragungsrates (10/100 Mbit) als auch den Typ (Node/Hub) angeschlossener Netzwerkgeräte automatisch (Autosensing). Der parallele Anschluss von Geräten unterschiedlicher Geschwindigkeit und Typen ist möglich.

- ③ **Konfigurations-Schnittstelle** – optional können Sie den Router direkt an die serielle Schnittstelle (RS-232, V.24) eines PC anschließen. Verwenden Sie dazu das mitgelieferte Anschlusskabel. Verbinden Sie die Konfigurations-Schnittstelle des LANCOM ③ mit einer freien seriellen Schnittstelle des PC.

- ④ **Mit Spannung versorgen** – versorgen Sie das Gerät an Buchse ⑤ über das mitgelieferte Netzteil mit Spannung.


 Verwenden Sie beim LANCOM WLC-4006 ausschließlich das mitgelieferte Netzteil! Die Verwendung eines ungeeigneten Netzteils kann zu Personen- oder Sachschäden führen.

- ⑤ **Mit Spannung versorgen und einschalten** – versorgen Sie das Gerät über das Kaltgeräte Kabel mit Spannung und schalten Sie es am Schalter ⑥ ein.

- ⑥ **Installation abgeschlossen** – Mit diesem Schritt ist die Hardware-Installation abgeschlossen. Als nächste Schritte stehen nun die Installation der Management-Software und die Konfiguration der LANCOM WLAN Controller an.


2.5 Installation der Software

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

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

2.5.1 LANCOM-Setup starten

Legen Sie die LANCOM-CD in Ihr Laufwerk ein. Daraufhin startet das LANCOM-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 **LANCOM Software installieren**. Es erscheint folgendes Auswahlmenü auf dem Bildschirm:



2.5.2 Welche Software installieren?

- **LANconfig** ist das Windows-Konfigurationsprogramm für alle LANCOM-Geräte. Alternativ (oder ergänzend) kann über einen Web-Browser WEBconfig verwendet werden.
- Mit **LANmonitor / WLANmonitor** überwachen Sie auf einem Windows-Rechner alle LANCOM Router und Access Points.
- Mit **LANCOM Dokumentation** kopieren Sie die Dokumentationsdateien auf Ihren PC.

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

3 Grundkonfiguration

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

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

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

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

3.1 Welche Angaben sind notwendig?

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

- TCP/IP-Einstellungen
- Schutz der Konfiguration
- 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 WLAN Controller angeschlossen
- Neuaufbau eines Netzwerks

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

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

Trotzdem manuell konfigurieren?

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

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

Notwendige Angaben für die manuelle TCP/IP-Konfiguration

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

■ IP-Adresse und Netzwerkmaske für den WLAN Controller

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

3.1.2 Konfigurationsschutz

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



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

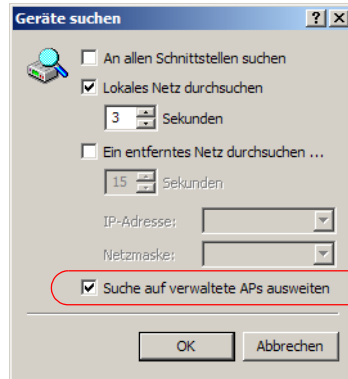


Im Managed-Modus erhalten LANCOM Wireless Router und LANCOM Access Points automatisch das gleiche Root-Kennwort wie der WLAN Controller, wenn auf dem Gerät selbst noch kein Root-Kennwort gesetzt ist.

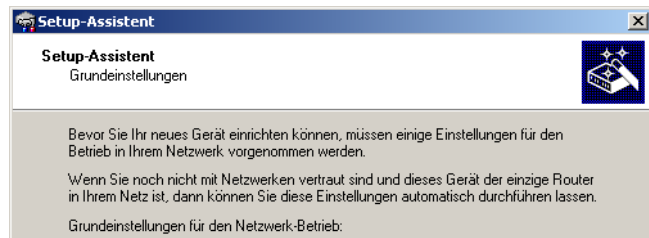
3.2 Anleitung für LANconfig

- ① Starten Sie LANconfig mit **Start ▶ Programme ▶ LANCOM ▶ LANconfig**. LANconfig erkennt neue LANCOM-Geräte im TCP/IP-Netz selbstständig.
- ② LANCOM Wireless Router und LANCOM Access Points im Managed-Modus werden standardmäßig bei der Suche mit LANconfig **nicht** ange-

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



- ③ Wird bei der Suche ein unkonfiguriertes Gerät gefunden, startet der Setup-Assistent, der Ihnen bei der Grundeinstellung des Geräts behilflich ist oder Ihnen (die passende Netzwerkumgebung vorausgesetzt) sogar die gesamte Arbeit abnimmt.




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

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

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


- ⑤ Im folgenden Fenster legen Sie zunächst das Kennwort für den Konfigurationszugriff fest. Achten Sie bei der Eingabe auf Groß- und Kleinschreibung, sowie auf eine ausreichende Länge (mindestens 6 Zeichen).

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

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

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


- ⑦ Schließen Sie die Konfiguration mit **Fertig stellen** ab.

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

3.3 Anleitung für WEBconfig

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

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

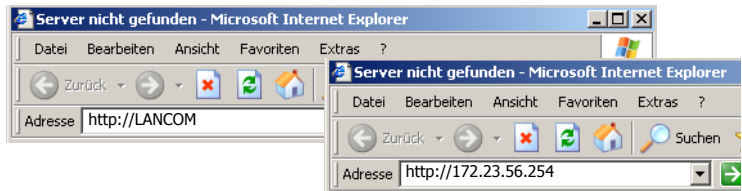
-  Wird ein LANCOM Wireless Router oder ein LANCOM Access Point von einem LANCOM WLAN Controller zentral verwaltet, dann wird beim Zuweisen der WLAN-Konfiguration auch der DHCP-Server vom Auto-Modus in den Client-Modus umgeschaltet.

Nicht für zentral
verwaltete
LANCOM Wireless
Router oder
LANCOM Access
Points

DE

Netz ohne DHCP-Server

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

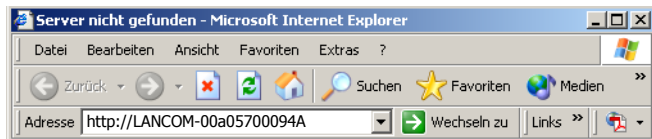


Falls der Konfigurations-Rechner seine IP-Adresse nicht vom LANCOM-DHCP-Server bezieht, ermitteln Sie die aktuelle IP-Adresse des Rechners (mit **Start ▶ Ausführen ▶ cmd** und dem Befehl **ipconfig** an der Eingabeaufforderung unter Windows 2000 oder Windows XP, mit **Start ▶ Ausführen ▶ cmd** und dem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

Netz mit DHCP-Server

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

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

DE

Aufruf der Assistenten in WEBconfig

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

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

(bzw. über beliebigen Namen)








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

Es erscheint das Hauptmenü von WEBconfig:







Setup-Assistenten

Assistenten erlauben es Ihnen, häufig auftretende Konfigurationen schnell und einfach

-  [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](#)



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

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

- ② Wenn Sie die TCP/IP-Einstellungen selbst vornehmen wollen, dann geben Sie dem LANCOM Router eine verfügbare Adresse aus einem geeigneten IP-Adressbereich. Stellen Sie außerdem ein, ob er als DHCP-Server arbeiten soll oder nicht. Bestätigen Sie Ihre Eingabe mit **Setzen**.
- ③ Im folgenden Fenster 'Sicherheitseinstellungen' vergeben Sie zunächst ein Kennwort für den Konfigurationszugriff. Achten Sie bei der Eingabe auf Groß- und Kleinschreibung, sowie auf eine ausreichende Länge (mindestens 6 Zeichen).

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

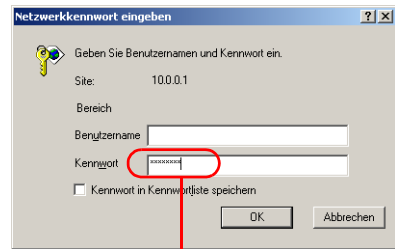


Bitte beachten Sie, dass mit dieser Freigabe auch die Fernkonfiguration über das Internet ermöglicht wird. Sie sollten in jedem Fall darauf achten, dass der Konfigurationszugriff geeignet abgesichert ist, z. B. durch ein Kennwort.

Eingabe des Kennworts im Web-Browser

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

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



Eingabe des Konfigurations-Kennworts

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

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

- ⑤ Der Gebührenschatz beschränkt auf Wunsch die Kosten von WAN-Verbindungen auf ein festgesetztes Maß. Bestätigen Sie Ihre Angaben mit **Setzen**.
- ⑥ Der Grundeinrichtungs-Assistent meldet, dass alle notwendigen Angaben vorliegen. Mit **Weiter** schließen Sie ihn ab.

3.4 TCP/IP-Einstellungen an den Arbeitsplatz-PCs

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

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

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

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

■ IP-Adressvergabe über den WLAN Controller

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

■ IP-Adressvergabe über einen separaten DHCP-Server

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

■ Manuelle Zuweisung der IP-Adressen

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



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

4 Konfiguration des WLAN Controllers

LANCOM WLAN Controller verwalten die Access Points in einer größeren WLAN-Infrastruktur. Die Konfigurationsdaten für die Access Points werden in den Profilen im WLAN Controller hinterlegt und von dort an die Access Points übertragen.



LANCOM WLAN Controller verwalten die Konfigurationen für LANCOM Wireless-Geräte, deren WLAN-Module auf die Betriebsart 'Managed' eingestellt sind.

- LANCOM Access Points (L-54g, L-54ag, L-54 dual, IAP, XAP, OAP) mit einer Firmware LCOS 7.20 oder höher sind im Auslieferungszustand auf den Managed-Modus eingestellt.
- LANCOM Wireless Router (18xx, 3x50) sind hingegen auf den Access Point-Modus eingestellt.

Hinweise zum Einstellen der Betriebsart für die WLAN-Module finden Sie unter 'Konfiguration der Access Points' → Seite 81.

4.1 Grundeinstellung der LANCOM WLAN Controller

Für den Start benötigt ein LANCOM WLAN Controller zur weitestgehend automatisierten Konfiguration der Access Points die beiden folgenden Informationen:

- Eine aktuelle Zeitinformation (Datum und Uhrzeit), damit die Gültigkeit der benötigten Zertifikate sichergestellt werden kann.
- Eine Default-Konfiguration, welche der WLAN Controller den Access Points zuweisen kann.



Die Beschreibungen in diesem Abschnitt ermöglichen eine grundlegende Konfiguration des WLAN Controllers für eine schnelle Inbetriebnahme, gehen aber nicht auf alle Möglichkeiten und Besonderheiten der einzelnen Parameter ein. Eine ausführliche Beschreibung der Konfigurationsparameter für die LANCOM WLAN Controller finden Sie unter 'Erweiterte Einstellungen' → Seite 49.

4.1.1 Zeitinformation für den LANCOM WLAN Controller einstellen

Die Verwaltung von Access Points in einer WLAN-Infrastruktur basiert auf der automatischen Verteilung von Zertifikaten über Simple Certificate Enrolment Protocol (SCEP).



Weitere Informationen über SCEP finden Sie im LCOS-Referenzhandbuch.

Der LANCOM WLAN Controller kann die Gültigkeit dieser zeitlich beschränkten Zertifikate nur dann prüfen, wenn er über eine aktuelle Zeitinformation verfügt. Solange der WLAN Controller nicht über eine aktuelle Zeitinformation verfügt, leuchtet die WLAN-LED dauerhaft rot, das Gerät ist nicht betriebsbereit.

Um dem Gerät eine Zeit zuzuweisen, klicken Sie in LANconfig mit der rechten Maustaste auf den Eintrag für den WLAN Controller und wählen im Kontext-Menü den Eintrag 'Datum/Zeit setzen'. Alternativ klicken Sie in WEBconfig am unteren Rand des Browserfensters den Link 'Datum/Zeit setzen'.



Die LANCOM WLAN Controller können die aktuelle Zeit alternativ auch automatisch über das Network Time Protocol (NTP) von einem Zeit-Server beziehen. Informationen über NTP und die entsprechende Konfiguration finden Sie im LCOS-Referenzhandbuch.

Sobald der WLAN Controller über eine gültige Zeitinformation verfügt, beginnen die Erstellung der Zertifikate (Root- und Geräte-Zertifikat) sowie die Ermittlung einer Zufallszahl. Wenn die Zufallszahl und die benötigten Zertifikate erfolgreich erzeugt wurden, meldet der LANCOM WLAN Controller Betriebsbereitschaft, die WLAN-LED blinkt dann rot.



Der WLAN Controller sollte mit dem LAN verbunden werden, um kryptografisch gute Zufallszahlen erzeugen zu können. Die Ermittlung der Zufallszahl kann je nach Netzwerkkonstellation einige Minuten dauern. Die Zufallszahlen müssen nur neu erstellt werden, wenn das Gerät mehrmals ein- und ausgeschaltet wurde, ansonsten sind genug Zufallszahlen gespeichert.



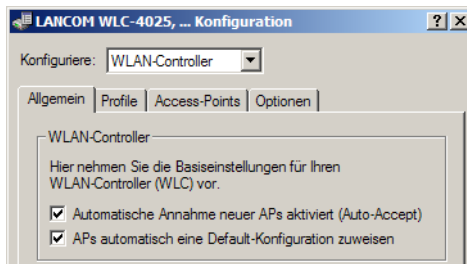
Nach Herstellung der Betriebsbereitschaft sollten Sie eine Sicherung der Zertifikate anlegen ('Sicherung der Zertifikate' → Seite 65).

4.1.2 Default-Konfiguration erstellen

Mit der Zeitinformation und den Zertifikaten ist der LANCOM WLAN Controller grundsätzlich betriebsbereit. Sofern sich im LAN Access Points im Managed-Modus befinden (Standardmodus für werksseitig ausgelieferte Access Points bzw. nach Reset mit LCOS 7.20 oder höher, manuelle Einstellung siehe 'Konfiguration der Access Points' → Seite 81), zeigt der WLAN Controller diese nach einer kurzen Zeit als „Neue Access Points“ an, die New-APs-LED blinkt entsprechend orange. Im Display des LANCOM WLC-4025 wird zusätzlich die Anzahl der neuen Access Points (New APs) aufgeführt.

Um diese neuen Access Points mit WLAN-Einstellungen zu bedienen, muss im LANCOM WLAN Controller zumindest eine Default-Konfiguration erstellt werden, welches den suchenden Access Points zugewiesen werden kann.

- ① Öffnen Sie die Konfiguration des WLAN Controllers durch einen Doppelklick auf den entsprechenden Eintrag in LANconfig.
- ② Aktivieren Sie im Konfigurationsbereich 'WLAN Controller' auf der Registerkarte 'Allgemein' die Optionen für die automatische Annahme neuer Access Points sowie die Zuweisung einer Default-Konfiguration.



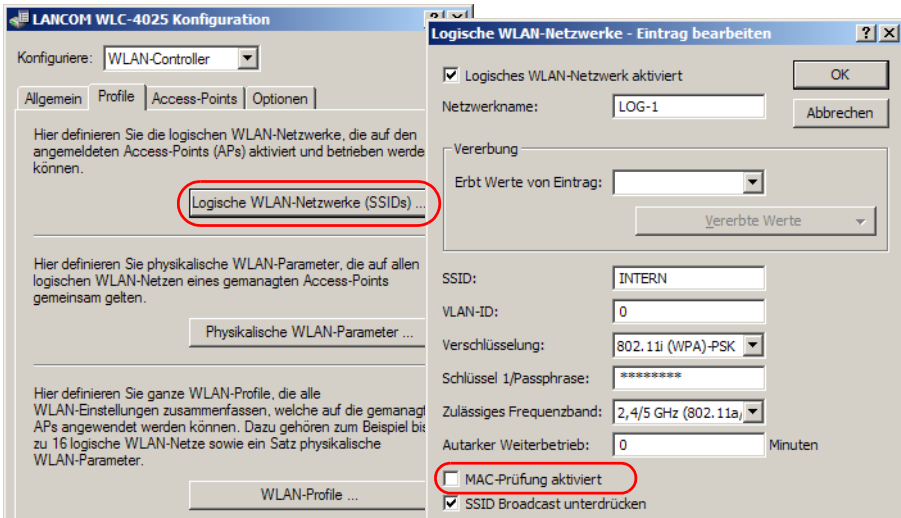
- Automatische Annahme neuer Access Points: Ermöglicht dem WLAN Controller, allen neuen Access Points **ohne** gültiges Zertifikat ein solches Zertifikat zuzuweisen. Dazu muss entweder für den Access Point eine Konfiguration in der AP-Tabelle eingetragen sein oder die 'Automatische Zuweisung der Default-Konfiguration' ist aktiviert.
- Automatische Zuweisung der Default-Konfiguration: Ermöglicht dem WLAN Controller, allen neuen Access Points eine Default-Konfiguration zuzuweisen, auch wenn für diese keine explizite Konfiguration hinterlegt wurde.

Durch die Kombination dieser beiden Optionen kann der LANCOM WLAN Controller alle im LAN gefundenen Access Points im Managed-Modus

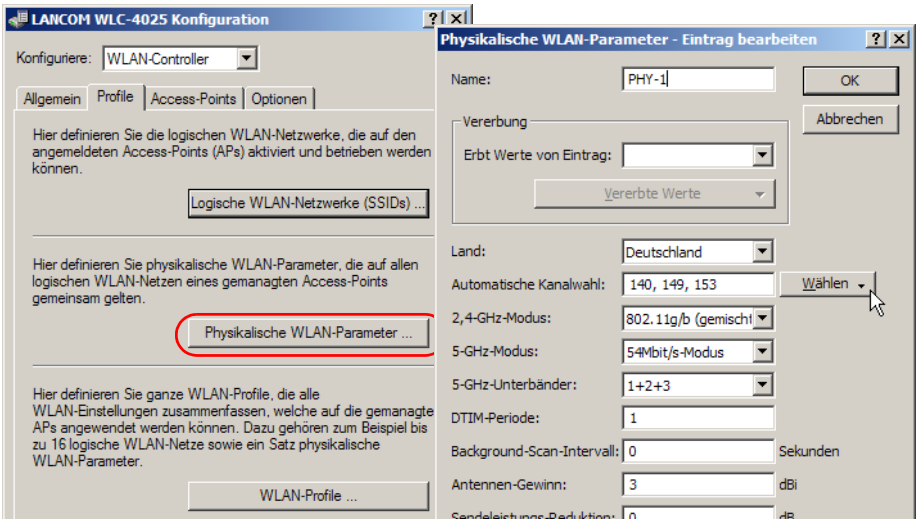
■ Kapitel 4: Konfiguration des WLAN Controllers

automatisch in die von ihm verwaltete WLAN-Struktur aufnehmen, z.B. temporär während der Rollout-Phase einer WLAN-Installation.

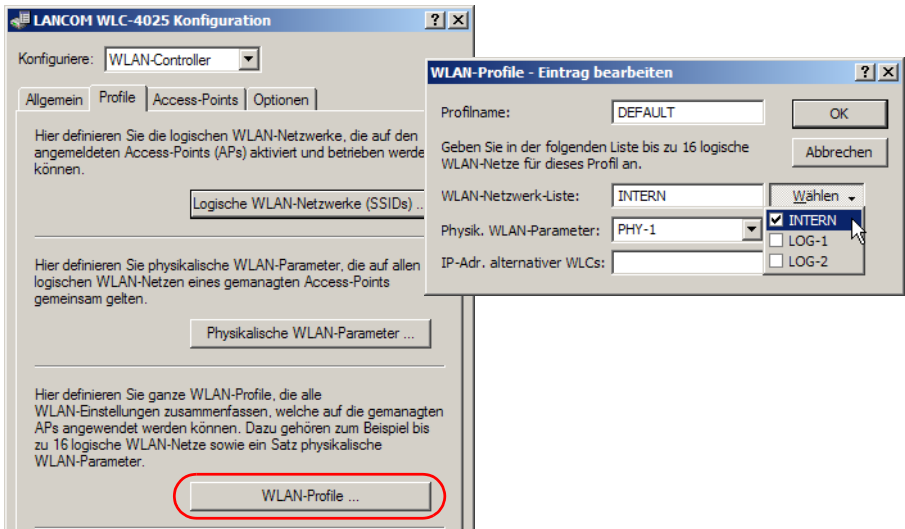
- ③ Wechseln Sie auf die Registerkarte 'Profile' in die logischen WLAN-Netzwerke. Erstellen Sie einen neuen Eintrag mit folgenden Werten:




- Netzwerkname: Geben Sie dem WLAN einen Namen. Dieser Name wird nur für die Verwaltung im LANCOM WLAN Controller verwendet.
 - SSID: Mit dieser SSID verbinden sich die WLAN-Clients.
 - Verschlüsselung: Wählen Sie die Verschlüsselung passend zu den Möglichkeiten der verwendeten WLAN-Clients und geben Sie ggf. einen Schlüssel bzw. eine Passphrase ein.
 - Deaktivieren Sie die MAC-Prüfung. Hinweise zur Nutzung der MAC-Filterlisten in gemanagten WLAN-Strukturen finden Sie unter 'Prüfung der WLAN-Clients über RADIUS (MAC-Filter)' → Seite 77.
- ④ Erstellen Sie auch bei den physikalischen WLAN-Parametern einen neuen Eintrag. Für die Default-Konfiguration reicht hier in vielen Fällen nur die Angabe eines Namens. Die restlichen Einstellungen können bei Bedarf angepasst werden.

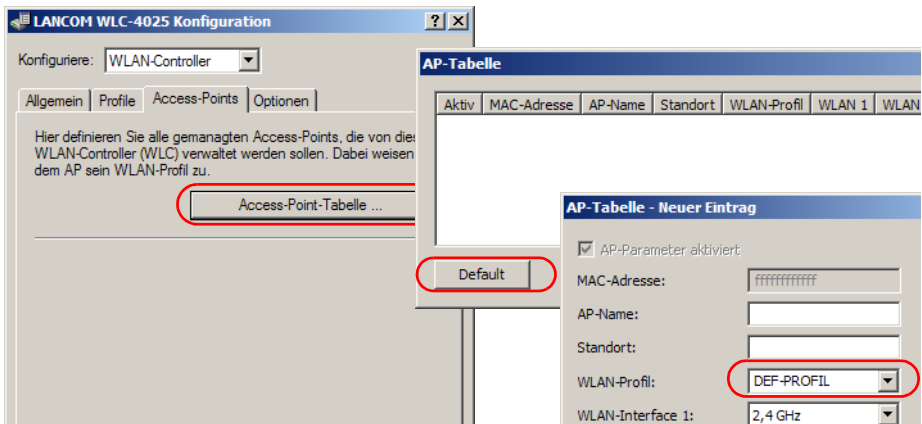


- ⑤ Erstellen Sie ein neues WLAN-Profil, geben Sie ihm einen eindeutigen Namen und weisen Sie ihm das eben erstellte logische WLAN-Netzwerk sowie die physikalischen WLAN-Parameter zu.



- ⑥ Wechseln Sie auf die Registerkarte 'Access Points' und erstellen Sie einen neuen Eintrag mit einem Klick auf die Schaltfläche **Default**. Weisen Sie dabei dem Eintrag das eben erstellte WLAN-Profil zu, 'AP-Name' und 'Standort' können frei bleiben.


 Die 'MAC-Adresse' wird für die Default-Konfiguration auf 'ffffffff' gesetzt und ist nicht editierbar. Damit gilt dieser Eintrag als Standard für alle Access Points, die nicht mit Ihrer MAC-Adresse explizit in dieser Tabelle eingetragen sind.



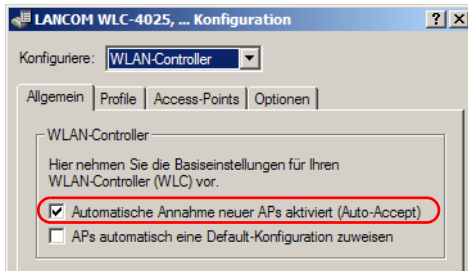
4.1.3 Zuweisung der Default-Konfiguration zu den neuen Access Points

Mit diesen Einstellungen haben Sie alle erforderlichen Werte definiert, damit der WLAN Controller den Access Points die erforderlichen WLAN-Parameter zuweisen kann. Mit dieser Konfigurations-Zuweisung ändern die Access Points in der Verwaltung des WLAN Controllers ihren Status von „Neuer Access Point“ auf „Erwarteter Access Point“, die im Display des Gerätes unter 'Exp. APs' aufgeführt werden. Sobald allen neuen Access Points die Default-Konfiguration zugewiesen wurde, erlischt die New-APs-LED.

In der Konfiguration des WLAN Controllers wird für jeden automatisch angenommenen Access Point ein Eintrag in der Access Point-Tabelle erstellt und aus der Default-Konfiguration gefüllt.

 Nach der ersten Startphase kann der die Option 'Automatische Zuweisung der Default-Konfiguration' wieder deaktiviert werden,

damit keine weiteren Access Points automatisch in das Netzwerk aufgenommen werden. Die 'Automatische Annahme neuer APs' kann aktiviert bleiben, damit der WLAN Controller den erwarteten Access Points – die in der AP-Tabelle eingetragen sind – z. B. nach einem Reset automatisch wieder ein gültiges Zertifikat zuweisen kann.



4.2 Erweiterte Einstellungen

Die meisten Parameter zur Konfiguration der LANCOM WLAN Controller entsprechen denen der Access Points. In dieser Dokumentation werden daher nicht alle WLAN-Parameter explizit beschrieben sondern nur die für den Betrieb der WLAN Controller erforderlichen Aspekte. Informationen zu den verfügbaren WLAN-Parametern finden sie im LCOS-Referenzhandbuch.

4.2.1 Allgemeine Einstellungen

In diesem Bereich nehmen sie die Basiseinstellungen für Ihren WLAN Controller vor.

■ Automatische Annahme neuer APs (Auto-Accept)

Ermöglicht dem WLAN Controller, allen neuen Access Points eine Konfiguration zuzuweisen, auch wenn diese nicht über ein gültiges Zertifikat verfügen.

Ermöglicht dem WLAN Controller, allen neuen Access Points **ohne** gültiges Zertifikat ein solches Zertifikat zuzuweisen. Dazu muss eine der beiden Bedingungen erfüllt sein:

- Für den Access Point ist unter seiner MAC-Adresse eine Konfiguration in der AP-Tabelle eingetragen.
- Die Option 'Automatische Zuweisung der Default-Konfiguration' ist aktiviert.

■ Automatische Zuweisung der Default-Konfiguration

Ermöglicht dem WLAN Controller, allen neuen Access Points (also **ohne** gültiges Zertifikat) eine Default-Konfiguration zuzuweisen, auch wenn für diese keine explizite Konfiguration hinterlegt wurde. Im Zusammenspiel mit dem Auto-Accept kann der LANCOM WLAN Controller alle im LAN gefundenen Access Points im Managed-Modus automatisch in die von ihm verwaltete WLAN-Struktur aufnehmen (bis zur maximalen Anzahl der auf einem WLAN Controller verwalteten Access Points).



Mit dieser Option können möglicherweise auch unbeabsichtigte Access Points in die WLAN-Struktur aufgenommen werden. Daher sollte diese Option nur während der Startphase bei der Einrichtung einer zentral verwalteten WLAN-Struktur aktiviert werden.

Mit der Kombination der Einstellungen für Auto-Accept und Default-Konfiguration können Sie verschiedene Situationen für die Einrichtung und den Betrieb der Access Points abdecken:

Auto-Accept	Default-Konfiguration	Geeignet für
Ein	Ein	Rollout-Phase: Verwenden Sie diese Kombination, wenn Sie sicherstellen können, dass keine Access Points unkontrolliert mit dem LAN verbunden werden und so unbeabsichtigt in die WLAN-Struktur aufgenommen werden.
Ein	Aus	Kontrollierte Rollout-Phase: Verwenden Sie diese Kombination, wenn Sie alle erlaubten Access Points mit ihrer MAC-Adresse in die AP-Tabelle eingetragen haben und diese automatisch in die WLAN-Struktur aufgenommen werden sollen.
Aus	Aus	Normalbetrieb: Es werden keine neuen Access Points ohne Zustimmung der Administratoren in die WLAN-Struktur aufgenommen.

4.2.2 Profile

Im Bereich der Profile definieren Sie die logischen WLAN-Netzwerke, die physikalischen WLAN-Parameter sowie die WLAN-Profile, die eine Kombination aus den beiden vorgenannten Elementen darstellen.

WLAN-Profil

In den WLAN-Profilen werden die Einstellungen zusammengefasst, die den Access Points zugewiesen werden. Die Zuordnung der WLAN-Profile zu den Access Points erfolgt in der AP-Tabelle.

Für jedes WLAN-Profil können Sie die folgenden Parameter definieren:

Konfigurationstool	Aufruf
LANconfig	WLAN Controller ► Profile ► WLAN-Profil
WEBconfig, Telnet	Experten-Konfiguration > Setup > WLAN-Management > Profile

■ Profil-Name

Name des Profils, unter dem die Einstellungen gespeichert werden.

- Maximal 31 ASCII-Zeichen.

■ WLAN-Netzwerk-Liste

Liste der logischen WLAN-Netzwerke, die über dieses Profil zugewiesen werden.

- Maximal 16 WLAN-Netzwerke, mehrere Werte durch Kommata getrennt bzw. in der Auswahlliste aktiviert.



Die Access Points nutzen aus dieser Liste nur die ersten acht Einträge, die mit der eigenen Hardware kompatibel sind. Somit können in einem Profil z. B. jeweils acht WLAN-Netzwerke für reinen 2,4 GHz-Betrieb und acht für reinen 5 GHz-Betrieb definiert werden. Für jeden LANCOM Access Point – sowohl Modelle mit 2,4 GHz- als auch die mit 5 GHz-Unterstützung – stehen damit die maximal möglichen acht logischen WLAN-Netzwerke zur Verfügung.

■ Physikalische WLAN-Parameter

Ein Satz von physikalischen Parametern, mit denen die WLAN-Module der Access Points arbeiten sollen.

■ IP-Adresse alternativer WLAN Controllers

Liste der WLAN Controller, bei denen der Access Point eine Verbindung versuchen soll. Der Access Point leitet die Suche nach einem WLAN Controller über einen Broadcast ein. Wenn nicht alle WLAN Controller

■ Kapitel 4: Konfiguration des WLAN Controllers

über einen solchen Broadcast erreicht werden können (WLAN Controller steht z. B. in einem anderen Netz), dann ist die Angabe von alternativen WLAN Controller sinnvoll.

- IP-Adressen, mehrere Werte getrennt durch Kommata. Maximal 159 Zeichen, also je nach Länge der IP-Adressen etwa 9 bis 10 Einträge.

Logische WLAN-Netzwerke

Hier werden die logischen WLAN-Netzwerke eingestellt, die den Access Points zugewiesen werden. Für jedes logische WLAN-Netzwerk können Sie die folgenden Parameter definieren:

Konfigurationstool	Aufruf
LANconfig	WLAN Controller ► Profile ► Logische WLAN-Netzwerke
WEBconfig, Telnet	Experten-Konfiguration > Setup > WLAN-Management > AP-Konfiguration > Netze

■ Netzwerkname

Name des logischen WLAN-Netzwerks, unter dem die Einstellungen gespeichert werden. Dieser Name wird nur für die interne Verwaltung der logischen Netze verwendet.

- Maximal 32 ASCII-Zeichen.

■ Vererbung

Auswahl eines schon definierten logischen WLAN-Netzwerks, von dem die Einstellungen übernommen werden sollen ('Vererbung von Parametern' → Seite 64).

■ SSID

Service Set Identifier – unter diesem Namen wird das logische WLAN-Netzwerk für die WLAN-Clients angeboten.

- Maximal 32 ASCII-Zeichen.

■ VLAN-ID

VLAN-ID für dieses logische WLAN-Netzwerk ('Dynamische VLAN-Zuweisung' → Seite 75).

- 0 bis 4094
- Default: 0
- Besondere Werte: 0 schaltet die Verwendung von VLAN für dieses WLAN-Netzwerk aus.



Bitte beachten Sie, dass für die Nutzung der VLAN-IDs in einem logischen WLAN-Netzwerk die Einstellung einer Management-VLAN-ID ('Management-VLAN-ID' → Seite 56) erforderlich ist!

■ Autarker Weiterbetrieb

Zeit in Minuten, für die der Access Point im Managed-Modus mit seiner aktuellen Konfiguration weiterarbeitet.

Die Konfiguration wird dem Access Point vom WLAN Controller zugewiesen und optional im Flash gespeichert (in einem Bereich, der nicht mit LANconfig oder anderen Tools auszulesen ist). Falls die Verbindung zum WLAN Controller unterbrochen wird, arbeitet der Access Point für die hier eingestellte Zeit mit seiner Konfiguration aus dem Flash weiter. Auch nach einem eigenen Stromausfall kann der Access Point mit der Konfiguration aus dem Flash weiterarbeiten.

Wenn die eingestellte Zeit abgelaufen ist und die Verbindung zum WLAN Controller noch nicht wiederhergestellt wurde, wird die Konfiguration im Flash gelöscht – der Access Point stellt seinen Betrieb ein. Sobald der WLAN Controller wieder erreichbar ist, wird die Konfiguration erneut vom WLAN Controller zum Access Point übertragen.

Durch diese Option kann der Access Point auch dann weiter arbeiten, wenn die Verbindung zum WLAN Controller kurzfristig unterbrochen wird.

Außerdem stellt diese Maßnahme einen wirksamen Schutz gegen Diebstahl dar, da die sicherheitsrelevanten Parameter der Konfiguration nach Ablauf der eingestellten Zeit automatisch gelöscht werden.



Stellt der Access Point im Backupfall eine Verbindung zu einem sekundären WLAN Controller her, so wird der Ablauf der Zeit für den autarken Weiterbetrieb unterbrochen ('Backup mit primären und sekundären WLAN Controllern' → Seite 71). Der Access Point bleibt also mit seinen WLAN-Netzwerken auch über diese eingestellte Zeit hinaus aktiv, solange er eine Verbindung zu einem WLAN Controller hat.



Bitte beachten sie, dass die Konfigurationsdaten im Flash erst nach Ablauf der eingestellten Zeit für den autarken Weiterbetrieb gelöscht werden, nicht jedoch durch die Trennung vom Stromnetz!

- 0 bis 9999
- Default: 0
- Besondere Werte:
 - ▶ 0: Schaltet das WLAN-Modul des Gerätes sofort aus, wenn die Verbindung zum Controller unterbrochen wird. Die vom WLAN Controller zugewiesene Konfiguration wird in diesem Fall nicht im Flash, sondern im RAM abgelegt und geht damit bei einer Trennung vom Stromnetz sofort verloren.
 - ▶ 9999: Arbeitet unbegrenzt mit der aktuellen Konfiguration weiter, auch wenn der WLAN Controller dauerhaft unerreichbar ist. Erst mit einem Reset wird die WLAN-Konfiguration im Flash gelöscht.



Alle weiteren Parameter der WLAN-Netzwerke entsprechen denen der üblichen Konfiguration für Access Points. Bitte schlagen Sie dazu ggf. im LCOS-Referenzhandbuch nach.

Physikalische WLAN-Parameter

Hier werden die physikalischen WLAN-Parameter eingestellt, die den Access Points zugewiesen werden. Für jeden Satz von physikalischen WLAN-Parametern können Sie die folgenden Parameter definieren:

Konfigurationstool	Aufruf
LANconfig	WLAN Controller ► Profile ► Physikalische WLAN-Parameter
WEBconfig, Telnet	Experten-Konfiguration > Setup > WLAN-Management > AP-Konfiguration > AP-Parameter

■ Name

Eindeutiger Name für diese Zusammenstellung von physikalischen WLAN-Parametern.

- Maximal 31 ASCII-Zeichen.

■ Vererbung

Auswahl eines schon definierten Satzes von physikalischen WLAN-Parametern, von dem die Einstellungen übernommen werden sollen ('Vererbung von Parametern' → Seite 64).

■ Land

Land, in dem die Access Points betrieben werden sollen. Aufgrund dieser Information werden landesspezifische Einstellungen wie die erlaubten Kanäle etc. festgelegt.

■ Kapitel 4: Konfiguration des WLAN Controllers

- Besondere Werte: 'Default' übernimmt die Ländereinstellung von der Definition im Bereich 'Optionen'.

■ Automatische Kanalwahl

Standardmäßig können die Access Points alle Kanäle nutzen, die aufgrund der Ländereinstellung erlaubt sind. Um die Auswahl auf bestimmte Kanäle zu beschränken, können hier die gewünschten Kanäle als kommaseparierte Liste eingetragen werden. Dabei ist auch die Angabe von Bereichen (z.B. '7-9') möglich.

- Maximal 16 Zeichen.

■ Management-VLAN-ID

Die VLAN-ID, die für das Management-Netz der Access Points verwendet wird.



Die Management-VLAN-ID **muss** auf einen Wert ungleich null eingestellt werden, um VLANs auf den WLAN-Netzwerken nutzen zu können. Das gilt auch dann, wenn das Management-Netz selbst nicht mit VLAN-IDs getaggt werden soll (Mgmt-VLAN-ID = 1).

- 0 bis 4094
- Default: 0
- Besondere Werte:
 - ▶ 0: Schaltet die Verwendung von VLAN **aus**.
 - ▶ 1: Schaltet die Verwendung von VLAN **ein**, das Management-Netz bleibt jedoch ungetaggt.
 - ▶ 2 bis 4094: Schaltet die Verwendung von VLAN **ein**, das Management-Netz verwendet die hier eingestellte VLAN-ID.



Die VLAN-Aktivierung gilt jeweils nur für diejenigen WLAN-Netzwerke, die mit diesen physikalischen WLAN-Parametern verbunden sind.



Alle weiteren physikalischen WLAN-Parameter entsprechen denen der üblichen Konfiguration für Access Points. Bitte schlagen Sie dazu ggf. im LCOS-Referenzhandbuch nach.

4.2.3 Liste der Access Points

Die AP-Tabelle ist ein zentraler Aspekt der Konfiguration für WLAN Controller. Hier werden den Access Points über ihre MAC-Adresse WLAN-Profile (also Kombinationen aus logischen und physikalischen WLAN-Parametern) zuge-

ordnet. Außerdem hat die reine Existenz eines Eintrags in der AP-Tabelle für einen bestimmten Access Point Auswirkungen auf die Möglichkeit, eine Verbindung zu einem WLAN Controller aufbauen zu können. Für jeden Access Point können Sie die folgenden Parameter definieren:

Konfigurationstool	Aufruf
LANconfig	WLAN Controller ▶ Access Points ▶ AP-Tabelle
WEBconfig, Telnet	Experten-Konfiguration > Setup > WLAN-Management > AP-Konfiguration > AP-Konfiguration

■ MAC-Adresse

MAC-Adresse des Access Points.

- Besondere Werte: FFFFFFFF definiert die Default-Konfiguration ('Automatische Zuweisung der Default-Konfiguration' → Seite 50).

■ AP-Name

Name des Access Point im Managed-Modus.

- Maximal 16 ASCII-Zeichen.

■ Standort

Standort des Access Point im Managed-Modus.

- Maximal 251 ASCII-Zeichen.

■ WLAN-Profil

WLAN-Profil aus der Liste der definierten Profile ('WLAN-Profile' → Seite 50).

■ WLAN-Interface 1

Frequenzband für das erste WLAN-Modul. Mit diesem Parameter kann das WLAN-Modul auch deaktiviert werden.

■ Kapitel 4: Konfiguration des WLAN Controllers

- Mögliche Werte: 2,4 GHz, 5 GHz, Aus, Default
- Besondere Werte: 'Default' übernimmt die Frequenzband-Einstellung von der Definition im Bereich 'Optionen'.

■ WLAN-Interface 2

Frequenzband für das zweite WLAN-Modul. Mit diesem Parameter kann das WLAN-Modul auch deaktiviert werden.

- Mögliche Werte: 2,4 GHz, 5 GHz, Aus, Default
- Besondere Werte: 'Default' übernimmt die Frequenzband-Einstellung von der Definition im Bereich 'Optionen'.

■ Verschlüsselung

Verschlüsselung für die Kommunikation über den Kontrollkanal. Ohne Verschlüsselung werden die Kontrolldaten im Klartext ausgetauscht. Eine Authentifizierung mittels Zertifikat findet in beiden Fällen statt.

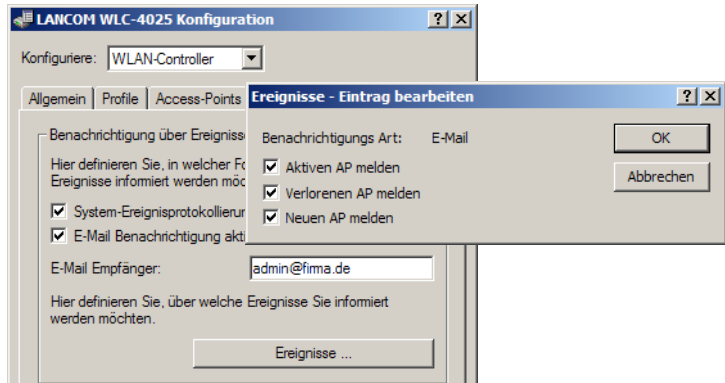
- Mögliche Werte: DTLS, keine, Default
- Besondere Werte: 'Default' übernimmt die Verschlüsselung von der Definition im Bereich 'Optionen'.

4.2.4 Optionen für den WLAN Controller

Im Bereich der 'Optionen' werden die Benachrichtigungen bei Ereignissen im WLAN Controller eingestellt sowie einige Defaultwerte definiert.

Benachrichtigungen über Ereignisse

Die Benachrichtigungen können über SYSLOG oder E-Mail erfolgen. Dazu können Sie die folgenden Parameter definieren:



Konfigurationstool	Aufruf
LANconfig	WLAN Controller ▶ Optionen ▶ Benachrichtigungen
WEBconfig, Telnet	Experten-Konfiguration > Setup > WLAN-Management > Benachrichtigung

■ SYSLOG

Aktiviert die Benachrichtigung über SYSLOG.

- Mögliche Werte: Ein/Aus.

■ E-Mail

Aktiviert die Benachrichtigung über E-Mail.

- Mögliche Werte: Ein/Aus.

■ Ereignisse

Wählt die Ereignisse, die über die eine Benachrichtigung erfolgen soll.

- Mögliche Werte:
 - ▶ Aktiven Access Point melden
 - ▶ Verlorenen Access Point melden
 - ▶ Neuen Access Point melden

Default-Parameter

Für einige Parameter können zentral Default-Werte definiert werden, die an anderen Stellen der Konfiguration als 'Default' referenziert werden können.

■ Kapitel 4: Konfiguration des WLAN Controllers

Default-Parameter

Bei den folgenden Parametern handelt es sich um Default-einstellungen, auf die an anderer Stelle innerhalb der WLC-Konfiguration über den Parameter 'Default' referenziert werden kann.

Land:

WLAN-Interface 1:

WLAN-Interface 2:

Verschlüsselung:

Konfigurationstool	Aufruf
LANconfig	WLAN Controller ▶ Optionen ▶ Benachrichtigungen
WEBconfig, Telnet	Experten-Konfiguration > Setup > WLAN-Management > Benachrichtigung

■ Land

Land, in dem die Access Points betrieben werden sollen. Aufgrund dieser Information werden landesspezifische Einstellungen wie die erlaubten Kanäle etc. festgelegt.

■ WLAN-Interface 1

Frequenzband für das erste WLAN-Modul. Mit diesem Parameter kann das WLAN-Modul auch deaktiviert werden.

- Mögliche Werte: 2,4 GHz, 5 GHz, Aus

■ WLAN-Interface 2

Frequenzband für das zweite WLAN-Modul. Mit diesem Parameter kann das WLAN-Modul auch deaktiviert werden.

- Mögliche Werte: 2,4 GHz, 5 GHz, Aus

■ Verschlüsselung

Verschlüsselung für die Kommunikation über den Kontrollkanal. Ohne Verschlüsselung werden die Kontrolldaten im Klartext ausgetauscht. Eine Authentifizierung mittels Zertifikat findet in beiden Fällen statt.

- Mögliche Werte: DTLS, keine

4.3 Weitere Konfigurations-Details

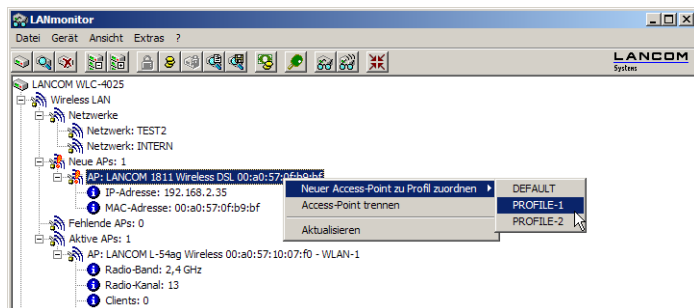
4.3.1 Neue Access Points manuell in die WLAN-Struktur aufnehmen

Wenn Sie die Access Points nicht automatisch in die WLAN-Struktur aufnehmen wollen (Auto-Accept, 'Automatische Annahme neuer APs (Auto-Accept)' → Seite 49), können sie die Access Points auch manuell akzeptieren.

Access Points akzeptieren über den LANmonitor

Neue Access Points können sehr komfortabel über den LANmonitor akzeptiert werden. Dabei wird eine Konfiguration ausgewählt, welche dem Access Point nach der Übertragung eines neuen Zertifikats zugewiesen wird.

Klicken Sie dazu im LANmonitor mit der rechten Maustaste auf den neuen Access Points, den Sie in die WLAN-Struktur aufnehmen möchten. Wählen Sie dann im Kontextmenü die Konfiguration, die Sie dem Gerät zuordnen wollen.



Mit dem Zuweisen der Konfiguration wird der Access Point in der AP-Tabelle des WLAN Controllers eingetragen. Es dauert jedoch einige Sekunden, bis der WLAN Controller dem Access Point auch ein Zertifikat zugewiesen hat und dieser ein aktives Element der zentralen WLAN-Struktur wird. Der neu aufgenommene Access Point wird also für eine kurze Zeit als „Lost AP“ mit der roten Lost-AP-LED, im Gerätedisplay und im LANmonitor angezeigt, bis die Zertifikatszuweisung abgeschlossen ist.

Access Points akzeptieren über WEBconfig mit Zuweisung eines Zertifikats

Neue Access Points, die kein gültiges Zertifikat haben, für die jedoch ein Eintrag in der AP-Tabelle vorliegt, können über eine Aktion in WEBconfig manuell akzeptiert werden.

- ① Öffnen Sie die Konfiguration des LANCOM WLAN Controller mit WEBconfig.
- ② Wählen Sie unter **Experten-Konfiguration** ► **Setup** ► **WLAN-Management** die Aktion **AP-einbinden**.
- ③ Geben sie als Parameter für die Aktion die MAC-Adresse des Access Points ein, den Sie akzeptieren möchten, und bestätigen Sie mit **Ausführen**.

The screenshot shows a web interface for 'Experten-Konfiguration'. Under 'Setup' > 'WLAN-Management', the 'AP-einbinden' action is selected. Below the title, there is a text prompt: 'Hier haben Sie die Möglichkeit, Parameter für das auszuführende Kommando einzugeben:'. A text input field labeled 'Parameter' contains the value '00a0571007f0'. Below the input field are two buttons: 'Ausführen' and 'Zurücksetzen'.

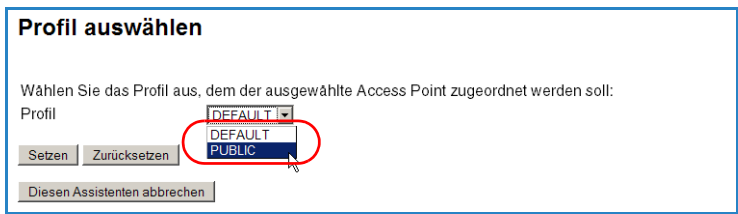
Access Points akzeptieren über WEBconfig mit Zuweisung von Zertifikat und Konfiguration

Neue Access Points, die kein gültiges Zertifikat haben und für die kein Eintrag in der AP-Tabelle vorliegt, können über einen Assistenten in WEBconfig manuell akzeptiert werden. Dabei wird eine Konfiguration ausgewählt, welche dem Access Point nach der Übertragung eines neuen Zertifikats zugewiesen wird.

- ① Öffnen Sie die Konfiguration des LANCOM WLAN Controller mit WEBconfig. Wenn neue Access Points gefunden wurden, zeigt WEBconfig das auf der Startseite mit einer entsprechenden Meldung an.



- ② Klicken Sie auf den Link, um den Assistenten zu starten. Wählen Sie den gewünschten Access Point anhand seiner MAC-Adresse aus und geben Sie die WLAN-Konfiguration an, die dem Access Point zugewiesen werden soll.



- ⓘ Mit dem Zuweisen der Konfiguration wird der Access Point in der AP-Tabelle des WLAN Controllers eingetragen. Es dauert jedoch einige Sekunden, bis der WLAN Controller dem Access Point auch ein Zertifikat zugewiesen hat und er damit aktives Element der zentralen WLAN-Struktur wird. Der neu aufgenommene Access Point wird also für eine kurze Zeit als „Lost AP“ mit der roten Lost-AP-LED, im Gerätedisplay und im LANmonitor angezeigt, bis die Zertifikatszuweisung abgeschlossen ist.

4.3.2 Access Points manuell aus der WLAN-Struktur entfernen

Um einen Access Point, der vom WLAN Controller verwaltet wird, aus der WLAN-Struktur zu entfernen, müssen Sie folgende Aktionen ausführen:

- ① Stellen Sie die WLAN-Betriebsart für die WLAN-Module von 'Managed' auf 'Client' oder 'Access-Point' um.
- ② Löschen Sie die Konfiguration für den Access Point bzw. deaktivieren Sie die 'Automatische Zuweisung der Default-Konfiguration'.

- ③ Trennen Sie die Verbindung zum Access Point unter WEBconfig im Bereich **Experten-Konfiguration ▶ Setup ▶ WLAN-Management** mit der Aktion **AP-Verbindung-trennen**.
- ④ Geben sie als Parameter für die Aktion die MAC-Adresse des Access Points ein, zu dem Sie die Verbindung trennen möchten, und bestätigen Sie mit **Ausführen**.

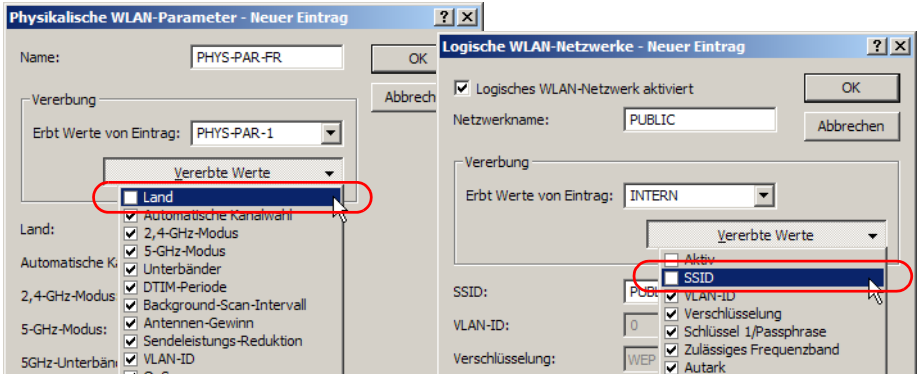
The screenshot shows a web interface with a breadcrumb trail: [Experten-Konfiguration](#) > [Status](#) > [WLAN-Management](#). Below this, the title **AP-Verbindung-trennen** is displayed. A text prompt reads: "Hier haben Sie die Möglichkeit, Parameter für das auszuführende Kommando einzugeben:". Below the prompt is a text input field labeled "Parameter" containing the value "00a057100710". At the bottom of the form are two buttons: "Ausführen" and "Zurücksetzen".

4.3.3 Vererbung von Parametern

Mit einem LANCOM WLAN Controller können sehr viele unterschiedliche Access Points an verschiedenen Standorten verwaltet werden. Nicht alle Einstellungen in einem WLAN-Profil eignen sich dabei für jeden der verwalteten Access Points gleichermaßen. Unterschiede gibt es z. B. in den Ländereinstellungen oder bei den Geräteeigenschaften.

Damit auch in komplexen Anwendungen die WLAN-Parameter nicht in mehreren Profilen redundant je nach Land oder Gerätetyp gepflegt werden müssen, können die logischen WLAN-Netzwerke und die physikalischen WLAN-Parameter ausgewählte Eigenschaften von anderen Einträgen „erben“.

- ① Erstellen Sie dazu zunächst die grundlegenden Einstellungen, die für die meisten verwalteten Access Points gültig sind.
- ② Erzeugen sie danach Einträge für die spezifischeren Werte, z. B. physikalische Einstellungen für ein bestimmtes Land oder ein logisches WLAN-Netzwerk für den öffentlichen Zugang von mobilen Clients.



- ③ Wählen Sie aus, von welchem Eintrag Werte geerbt werden sollen und markieren Sie die vererbten Werte. Die so übernommenen Parameter werden im Konfigurationsdialog grau dargestellt und können nicht verändert werden.
- ④ Die so zusammengestellten WLAN-Einstellungen werden dann je nach Verwendung zu separaten Profilen zusammengefasst, die wiederum gezielt den jeweiligen Access Points zugewiesen werden.



Bei der Vererbung sind grundsätzlich Ketten über mehrere Stufen (Kaskadierung) möglich. So können z. B. länder- und gerätespezifische Parameter komfortabel zusammengestellt werden.

Auch Rekursionen sind möglich – Profil A erbt von Profil B, gleichzeitig erbt B aber auch von A. Die verfügbaren Parameter für die Vererbung beschränken sich dabei aber auf eine „Vererbungsrichtung“ pro Parameter.

4.3.4 Sicherung der Zertifikate

Ein LANCOM WLAN Controller erzeugt beim ersten Systemstart die grundlegenden Zertifikate für die Zuweisung der Zertifikate an die Access Points – darunter die Root-Zertifikate für die CA (Certification Authority) und die RA (Registration Authority). Auf der Grundlage dieser beiden Zertifikate stellt der WLAN Controller die Geräte-Zertifikate für die Access Points aus.

Wenn mehrere WLAN Controller in der gleichen WLAN-Infrastruktur parallel eingesetzt werden (Load-Balancing) oder wenn ein Gerät ersetzt bzw. neu konfiguriert werden muss, sollten immer die gleichen Root-Zertifikate ver-

wendet werden, um einen reibungslosen Betrieb der verwalteten Access Points zu gewährleisten.

Backup der Zertifikate anlegen

Für die Wiederherstellung der CA bzw. der RA werden die jeweiligen Root-Zertifikate mit den privaten Schlüsseln benötigt, die beim Systemstart automatisch vom LANCOM WLAN Controller erzeugt werden. Außerdem sollten folgende noch weitere Dateien mit Informationen über die ausgestellten Geräte-Zertifikate gesichert werden ('Sichern und Wiederherstellen weiterer Dateien der SCEP-CA' → Seite 67). Damit diese vertraulichen Daten auch beim Export aus dem Gerät heraus geschützt bleiben, werden sie zunächst in einen PKCS12-Container gespeichert, der mit einer Passphrase geschützt ist.

- ① Öffnen Sie die Konfiguration des LANCOM WLAN Controller mit WEBconfig im Bereich **Experten-Konfiguration ▶ Setup ▶ Zertifikate ▶ SCEP-CA ▶ CA-Zertifikate**.
- ② Wählen Sie den Befehl **Erstelle-PKCS12-Backup-Dateien** und geben sie als Parameter die Passphrase für die PKCS12-Container an.

Experten-Konfiguration

- Setup
- Zertifikate
- SCEP-CA
- CA-Zertifikate

Erstelle-PKCS12-Backup-Dateien

Hier haben Sie die Möglichkeit, Parameter für das auszuführende Kommando einzugeben:

Parameter

Mit dieser Aktion werden die Zertifikate und privaten Schlüssel in die PKCS12-Dateien gespeichert und können dann aus dem Gerät heruntergeladen werden.

Zertifikats-Backup aus dem Gerät herunterladen

- ① Wählen Sie auf der Startseite von WEBconfig den Befehl **Zertifikat oder Datei herunterladen**.
- ② Wählen Sie dann als Dateityp nacheinander die beiden Einträge für die SCEP-CA und bestätigen Sie mit **Download starten**:
 - PKCS12-Container mit CA-Backup

- PKCS12-Container mit RA-Backup

Zertifikat oder Datei herunterladen

Wählen Sie aus, welche Datei Sie herunterladen wollen, dann klicken Sie auf 'Download starten':

Dateityp:

Die Backup-Datei wird damit auf Ihren Datenträger gespeichert. Die Passphrase wird erst beim Einspielen in einen LANCOM WLAN Controller wieder benötigt.

Zertifikats-Backup in das Gerät einspielen

- ① Wählen Sie auf der Startseite von WEBconfig den Befehl **Zertifikat oder Datei hochladen**.
- ② Wählen Sie dann als Dateityp nacheinander die beiden Einträge für die SCEP-CA:
 - PKCS12-Container mit CA-Backup
 - PKCS12-Container mit RA-Backup
- ③ Geben Sie dazu jeweils den Dateinamen mit Speicherort an und die Passphrase, die beim Erstellen der Sicherungsdateien definiert wurde. Bestätigen Sie mit **Upload starten**:

Zertifikat oder Datei hochladen

Wählen Sie aus, welche Datei Sie hochladen wollen sowie deren Namen, dann klicken Sie auf 'Upload starten':

Dateityp:
 Dateiname:
 Passphrase (falls benötigt):

Achtung: Beim Upload einer Datei (ggfs. mit falscher Passphrase) wird diese nicht auf inhaltliche Korrektheit überprüft. Diese Überprüfung findet später in den jeweiligen Modulen statt, die die Dateien verwenden. Beim Upload von Zertifikaten können Sie unmittelbar nach dem Upload entsprechende Fehlermeldungen im VPN-Status-Feld sehen.

4.3.5 Sicherung und Wiederherstellen weiterer Dateien der SCEP-CA

Um die SCEP-CA vollständig wiederherstellen zu können, sind auch die Informationen über die von der SCEP-CA ausgestellten – und ggf. später zurückgezogenen – Geräte-Zertifikate für die einzelnen Access Points wichtig.



Wenn nur die Root-Zertifikate gesichert werden, können die ausgestellten Geräte-Zertifikate nicht mehr zurückgerufen werden!

Daher müssen Sie neben den Zertifikaten selbst noch folgende Dateien sichern:

- SCEP-CRL-Datei: Liste der von der SCEP-CA ausgestellten und später zurückgezogenen Zertifikate.
- SCEP-Zertifikatsliste: Liste aller von der SCEP-CA jemals ausgestellten Zertifikate.
- SCEP-Seriennummern: Liste mit den Seriennummern der ausgestellten Zertifikate.

- ① Wählen Sie auf der Startseite von WEBconfig den Befehl **Zertifikat oder Datei herunterladen**.
- ② Wählen Sie dann als Dateityp nacheinander die oben aufgeführten Einträge und bestätigen Sie mit **Download starten**:

Zertifikat oder Datei herunterladen

Wählen Sie aus, welche Datei Sie herunterladen wollen, dann klicken Sie auf 'Download starten':

Dateityp: VPN - Container als PKCS#12-Datei (*.pfx; *.p12 [Passphrase erforderlich]) ▼

Download: VPN - Container als PKCS#12-Datei (*.pfx; *.p12 [Passphrase erforderlich])
EAP/TLS - Container als PKCS#12-Datei (*.pfx; *.p12 [Passphrase erforderlich])
SCEP-CA - CRL-Datei
SCEP-CA - Zertifikats-Liste
SCEP-CA - Seriennummer
SCEP-CA - PKCS12 Container mit CA Backup (Passphrase erforderlich)
SCEP-CA - PKCS12 Container mit RA Backup (Passphrase erforderlich)

① 13.09. [Vorherige](#) [Startseite](#)

[Meldung von Login \(einfacher Text\)](#)

- ③ Zum Einspielen dieser Dateien in das Gerät wählen Sie auf der Startseite von WEBconfig den Befehl **Zertifikat oder Datei hochladen**.

- ④ Wählen Sie dann als Dateityp nacheinander die oben aufgeführten Einträge, geben Sie dazu jeweils den Dateinamen mit Speicherort an und bestätigen Sie mit **Upload starten**:

Zertifikat oder Datei hochladen

Wählen Sie aus, welche Datei Sie hochladen wollen sowie deren Namen, dann klicken Sie auf 'Upload starten':

Dateityp:	SCEP-CA - CRL Datei
Dateiname:	SSL - Zertifikat (*.pem, *.crt, *.cer [BASE64])
Passphrase (falls benötigt):	SSL - Privater-Schlüssel (*.key [BASE64 unverschlüsselt]) SSH - RSA-Schlüssel (*.key [BASE64 unverschlüsselt]) SSH - DSA-Schlüssel (*.key [BASE64 unverschlüsselt])
Achtung: Beim Upload überprüft. Diese Überlappung von Zertifikat	SSH - akzeptierte öffentliche Schlüssel VPN - Root-CA-Zertifikat (*.pem, *.crt, *.cer [BASE64]) VPN - Geräte-Zertifikat (*.pem, *.crt, *.cer [BASE64]) VPN - Privater-Geräte-Schlüssel (*.key [BASE64 unverschlüsselt]) VPN-Status-Trace sende
Upload von Zertifikat	VPN - Container als PKCS#12-Datei (*.pfx, *.p12 [Passphrase erforderlich]) EAP/TLS - Root-CA-Zertifikat (*.pem, *.crt, *.cer [BASE64]) EAP/TLS - Geräte-Zertifikat (*.pem, *.crt, *.cer [BASE64]) EAP/TLS - Privater-Geräte-Schlüssel (*.key [BASE64 unverschlüsselt]) EAP/TLS - Container als PKCS#12-Datei (*.pfx, *.p12 [Passphrase erforderlich])
VPN-Status-Trace sende	SCEP-CA - CRL Datei
<input type="button" value="Upload starten"/>	SCEP-CA - Zertifikats-Liste SCEP-CA - Seriennummer SCEP-CA - PKCS12 Container mit CA Backup (Passphrase erforderlich) SCEP-CA - PKCS12 Container mit RA Backup (Passphrase erforderlich) Meldung von Login (einfacher Text)

🕒 13.09.2007 10:53

➔ [Vorherige Seite](#)

4.3.6 Backuplösungen

LANCOM WLAN Controller verwalten eine große Zahl von Access Points, bei denen wiederum zahlreiche WLAN-Clients eingebucht sein können. Die WLAN Controller haben daher eine zentrale Bedeutung für die Funktionsfähigkeit der gesamten WLAN-Struktur – die Einrichtung einer Backup-Lösung für den vorübergehenden Ausfall eines WLAN Controllers ist daher in vielen Fällen unverzichtbar.

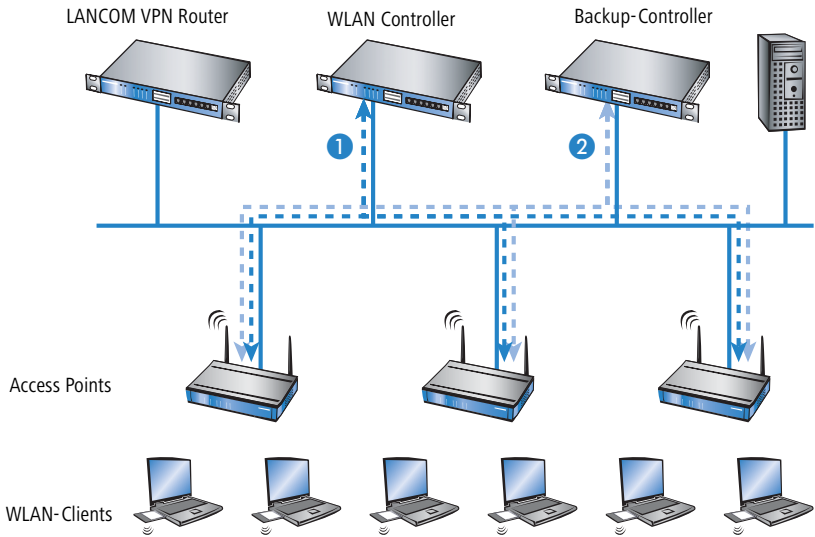
In einem Backup-Fall soll sich ein gemanagter Access Point mit einem anderen WLAN Controller verbinden. Da diese Verbindung nur gelingen kann, wenn das Zertifikat des Access Points von dem Backup-Controller authentifiziert wird, müssen alle WLAN Controller in einer Backup-Lösung auf jeden Fall identische Root-Zertifikate verwenden.

- Erstellen Sie daher auf einem der WLAN Controller ein Backup der Zertifikate und spielen Sie diese in die anderen WLAN Controller ein (siehe auch 'Sicherung der Zertifikate' → Seite 65).
- Damit die Prüfung der Zertifikate bzgl. der zeitlichen Gültigkeit zu gleichen Ergebnissen kommt, stellen Sie auf allen WLAN Controllern eine ähnliche Zeitinformation ein.

Neben diesen grundlegenden Einstellungen können sie aus zwei unterschiedlichen Backup-Szenarien wählen.

Backup mit redundanten WLAN Controllern

Diese Form des Backups bietet sich an, wenn Sie einen LANCOM WLAN Controller durch einen zweiten WLAN Controller absichern und dabei jederzeit die volle Kontrolle über alle gemanagten Access Points behalten möchten.



- ① Stellen Sie auf beiden LANCOM WLAN Controllern ① und ② die gleiche Uhrzeit ein.
- ② Übertragen Sie die CA- und RA-Zertifikate aus einem WLAN Controller ① in den zweiten, den „Backup-Controller“ ②.
- ③ Konfigurieren Sie den ersten WLAN Controller ① wie gewünscht mit allen Profilen und der zugehörigen AP-Tabelle. Die Access Points bauen dann die Verbindung zum ersten WLAN Controller auf. Die Access Points erhalten von diesem WLAN Controller ein gültiges Zertifikat und eine Konfiguration für die WLAN-Module.
- ④ Übertragen Sie die Konfiguration des ersten WLAN Controllers ① z. B. mit LANconfig auf den Backup-Controller ②. Dabei werden auch die Profile und die AP-Tabellen mit den MAC-Adressen der Access Points auf den Backup-Controller übertragen. Alle Access Points bleiben in diesem Zustand weiterhin beim ersten WLAN Controller angemeldet.

- ⑤ Fällt der erste WLAN Controller ① aus, suchen die Access Points automatisch nach einem anderen WLAN Controller und finden dabei den Backup-Controller ②. Da dieser über die gleichen Root-Zertifikate verfügt, kann er die Zertifikate der Access Points auf Gültigkeit überprüfen. Da die Access Points außerdem mit ihrer MAC-Adresse in der AP-Tabelle des Backup-Controllers eingetragen sind, übernimmt der Backup-Controller vollständig die Verwaltung der Access Points. Änderungen in den WLAN-Profilen des Backup-Controllers wirken sich direkt auf die gemanagten Access Points aus.



Die Access Points bleiben in diesem Szenario so lange in der Verwaltung des Backup-Controllers, bis dieser entweder selbst einmal nicht erreichbar ist oder bis sie manuell getrennt werden ('Access Point trennen' → Seite 80).



Mit der Einstellung des autarken Weiterbetriebs ('Autarker Weiterbetrieb' → Seite 53) können die Access Points auch während der Suche nach einem Backup-Controller mit der aktuellen WLAN-Konfiguration in Betrieb bleiben, und die WLAN-Clients bleiben eingebucht.

Backup mit primären und sekundären WLAN Controllern

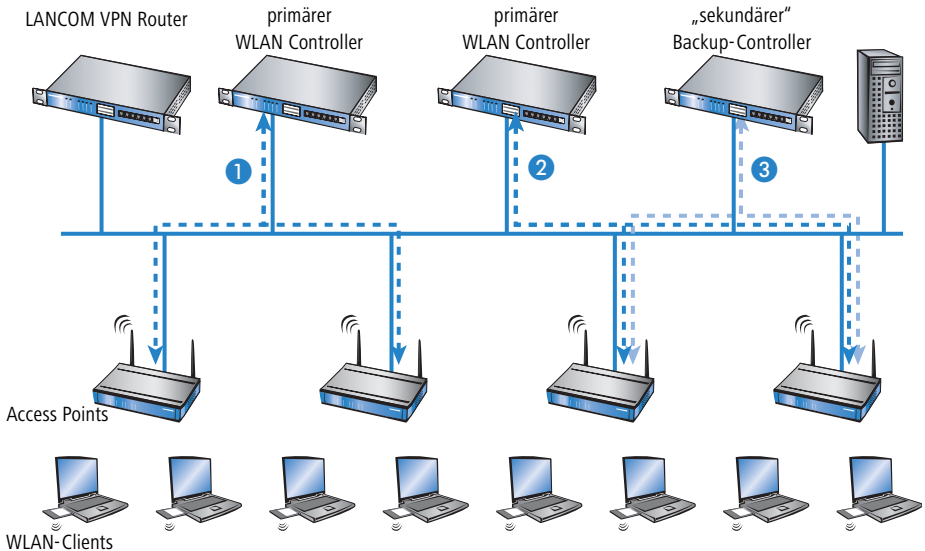
Mit einer zweiten Form des Backups können Sie für eine größere Anzahl von „primären“ WLAN Controllern einen gemeinsamen, „sekundären“ Backup-Controller bereitstellen. Beim Ausfall eines WLAN Controllers bleiben die Access Points zwar in Betrieb, arbeiten allerdings mit der aktuellen Konfiguration der WLAN-Module weiter. Der Backup-Controller kann als sekundärer Controller den Access Points keine veränderte Konfiguration zuweisen.

Primäre und sekundäre Controller

Der Verbindungsaufbau zwischen WLAN Controller und Access Point wird immer vom Access Point initiiert. Ein LANCOM Access Point im Managed-Modus sucht in einem LAN nach einem WLAN Controller, der ihm eine Konfiguration zuweisen kann. Bei dieser Suche kann der Access Point unterschiedliche geeignete WLAN Controller finden:

- Der WLAN Controller kann das **Zertifikat** des Access Points authentifizieren und hat für die MAC-Adresse des suchenden Access Points eine **Konfiguration** gespeichert. Einen solchen WLAN Controller bezeichnet man als „primären“ WLAN Controller.
- Ein WLAN Controller kann das **Zertifikat** des Access Points authentifizieren, hat aber für die MAC-Adresse des suchenden Access Points **keine Konfiguration** gespeichert und auch **keine Default-Konfiguration**. Einen solchen WLAN Controller bezeichnet man als „sekundären“ WLAN Controller.

Beispiel einer Backup-Lösung mit drei LANCOM WLC-4025 für 50 gemanagte Access Points: Zwei der WLAN Controller verwalten jeweils 25 Access Points, der dritte steht als Backup-Controller bereit:



- ① Stellen Sie auf allen LANCOM WLAN Controllern ① und ② und ③ die gleiche Uhrzeit ein.

- ② Übertragen Sie die CA- und RA-Zertifikate aus dem ersten primären WLAN Controller ① in den zweiten, primären ② und den sekundären „Backup-Controller“ ③.
- ③ Konfigurieren Sie den ersten WLAN Controller ① wie gewünscht mit den Profilen und der zugehörigen AP-Tabelle für eine Hälfte der Access Points. Dieses WLAN Controller wird somit zum primären Controller für die bei ihm eingetragenen Access Points.



Bei einer Backup-Lösung über einen sekundären WLAN Controller muss die Zeit für den autarken Weiterbetrieb auf jeden Fall so eingestellt werden, dass der Access Point während dieser Zeitspanne einen Backup-Controller findet, da der Backup-Controller dem Access Point keine neue Konfiguration zuweisen kann.

Sobald der Access Point eine Verbindung zu einem sekundären WLAN Controller hergestellt hat, wird der Ablauf der Zeit für den autarken Weiterbetrieb unterbrochen. Der Access Point bleibt also mit seinen WLAN-Netzwerken auch über diese eingestellte Zeit hinaus aktiv, solange er eine Verbindung zu einem WLAN Controller hat.

- ④ Konfigurieren Sie den zweiten WLAN Controller ② für die andere Hälfte der Access Points, welche dann diesen WLAN Controller als primären Controller betrachten.
- ⑤ Der Backup-Controller ③ bleibt bis auf die Uhrzeit und die Root-Zertifikate ohne weitere Konfiguration.
- ⑥ Die Access Points suchen nach dem Start über eine Discovery-Message nach einem WLAN Controller. In diesem Fall antworten alle drei LANCOM WLAN Controller auf diese Nachricht – die Access Points wählen jeweils „ihren“ primären Controller für die folgende DTLS-Verbindung. Die eine Hälfte der Access Points entscheidet sich für WLAN Controller ①, die andere Hälfte für WLAN Controller ②. Da WLAN Controller ③ für keinen der Access Points als primärer Controller fungiert, meldet sich kein Access Point bei ihm an.
- ⑦ Fällt z. B. der erste WLAN Controller ② aus, suchen die Access Points automatisch nach einem anderen WLAN Controller. Sie finden die WLAN Controller ① und ③, wobei ① schon mit seinen 25 Access Points vollständig ausgelastet ist. Backup-Controller ③ kann die Gültigkeit der Zertifikate prüfen, die Access Points also authentifizieren und als gemanagte Access Points annehmen. Da die Access Points jedoch **nicht** mit ihrer

MAC-Adresse in der AP-Tabelle des Backup-Controllers eingetragen sind, kann der Backup-Controller die Access Points nicht weiter verwalten, sie werden nur mit der jeweiligen aktuellen WLAN-Konfiguration weiterbetrieben.



Sollte WLAN Controller ① nicht ausgelastet sein, weil z. B. einige „seiner“ Access Points ausgeschaltet sind, so könnten sich auch einige der suchenden Access Points bei diesem anmelden. WLAN Controller ① bleibt für diese Access Points aber ein „sekundärer“ Controller, da er nicht über Konfigurationsprofile für diese Geräte verfügt. Wird in diesem Fall einer der Access Point wieder eingeschaltet, der über einen Eintrag in der AP-Tabelle von WLAN Controller ① verfügt, nimmt ① diesen reaktivierten Access Point wieder auf und trennt sich dafür von einem der Access Points im Backup-Fall.



Mit der Einstellung des autarken Weiterbetriebs ('Autarker Weiterbetrieb' → Seite 53) bleiben die Access Points auch während der Suche nach einem Backup-Controller mit der aktuellen WLAN-Konfiguration in Betrieb, die WLAN-Clients können weiterhin alle Funktionen nutzen.

4.3.7 Load-Balancing zwischen den WLAN Controllern

Wenn in einem Netzwerk mehrere WLAN Controller verfügbar sind, werden die Access Points automatisch gleichmäßig auf die WLAN Controller verteilt.

Der Access Point sendet zu Beginn der Kommunikation eine „Discovery Request Message“, um die verfügbaren WLAN Controller zu ermitteln.

- Wenn der Access Point Antworten von primären und sekundären WLAN Controllern erhält, werden primäre Controller bevorzugt.
- Aus den verfügbaren WLAN Controllern wählt der Access Point den mit der geringsten Auslastung, also dem kleinsten Verhältnis von gemanagten Access Points zu den maximal möglichen Access Points.
- Bei zwei oder mehreren gleich „guten“ WLAN Controllern wählt der Access Point den im Netzwerk nächsten, also den mit der geringsten Antwortzeit.

Auf diese Art und Weise können z. B. beim Aktivieren von mehreren WLAN Controllern über die automatische Zuweisung von Konfigurationen ('Automatische Zuweisung der Default-Konfiguration' → Seite 50) alle WLAN Controller gleichmäßig mit Konfigurationen für einen Teil der Access Points „gefüllt“ werden.

4.3.8 Dynamische VLAN-Zuweisung

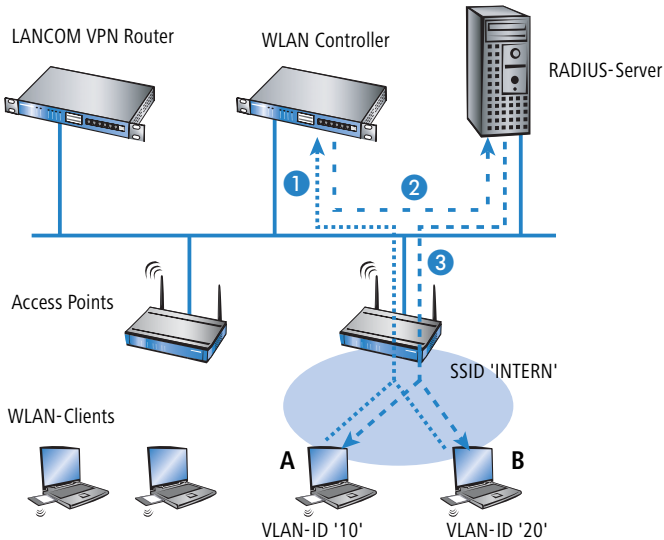
In einer größeren WLAN-Struktur ist es oft sinnvoll, den einzelnen WLAN-Clients ein bestimmtes Netzwerk zuzuweisen. Solange sich die WLAN-Clients immer in der Reichweite des gleichen Access Points befinden, kann diese Zuweisung über die SSID in Verbindung mit einem bestimmten IP-Netzwerk realisiert werden. Wechseln die WLAN-Clients hingegen häufig die Position und buchen sich dann bei unterschiedlichen Access Points ein, befinden sie sich je nach Konfiguration in einem anderen IP-Netzwerk.

Um die WLAN-Clients **unabhängig** von dem WLAN-Netzwerk, in dem sie sich gerade eingebucht haben, in ein bestimmtes Netzwerk zu leiten, können dynamisch zugewiesene VLANs genutzt werden. Anders als bei den statisch konfigurierten VLAN-IDs für eine bestimmte SSID ('VLAN-ID' → Seite 53) wird die VLAN-ID dabei dem WLAN-Client von einem RADIUS-Server direkt zugewiesen.

Beispiel: Zwei WLAN-Clients buchen sich über den gleichen Access Point in das WLAN mit der SSID 'INTERN' ein. Bei der Anmeldung werden die RADIUS-Anfragen der WLAN-Clients an den Access Point gestellt. Wenn sich das entsprechende WLAN-Interface in der Betriebsart 'Managed' befindet, werden die RADIUS-Anfragen automatisch an den WLAN Controller weitergereicht. Dieser leitet die Anfragen seinerseits an den konfigurierten RADIUS-Server weiter. Der RADIUS-Server kann die Zugangsberechtigung der WLAN-Clients prüfen. Darüber hinaus kann er allerdings auch z. B. anhand der MAC-Adresse eine bestimmte VLAN-ID zuweisen. Dabei erhält z. B. der WLAN-Client **A** die VLAN-ID '10' und WLAN-Client **B** die '20'.



Die Zuweisung der VLAN-ID kann im RADIUS-Server auch anhand von anderen Kriterien erfolgen, z. B. über die Kombination aus Benutzername und Kennwort. Auf diese Weise kann z. B. den unbekanntenen MAC-Adressen der Besucher in einer Firma eine VLAN-ID zugewiesen werden, die für den Gastzugang z. B. nur die Internetnutzung erlaubt, jedoch keinen Zugang zu anderen Netzwerkressourcen.



- ① Aktivieren Sie das VLAN-Tagging für den WLAN Controller. Tragen Sie dazu als Management-VLAN-ID in den physikalischen Parametern des Profils einen Wert größer als '0' ein ('Management-VLAN-ID' → Seite 56).
- ② Für eine Authentifizierung über 802.1x wählen Sie in den Verschlüsselungseinstellungen für das logische WLAN-Netzwerk des Profils eine Einstellung, die eine Authentifizierungsanfrage auslöst.
- ③ Für eine Prüfung der MAC-Adressen aktivieren Sie für das logische WLAN-Netzwerk des Profils die MAC-Prüfung.



Sowohl für die Authentifizierung über 802.1x als auch für die Prüfung der MAC-Adressen ist bei der Verwaltung von WLAN-Modulen über einen WLAN Controller ein RADIUS-Server erforderlich. Der WLAN Controller trägt sich dabei automatisch in den von ihm verwalteten Access Points als RADIUS-Server ein – alle RADIUS-Anfragen an die Access Points werden daher direkt an den WLAN Controller weitergeleitet, der die Anfragen entweder selbst bearbeitet oder sie alternativ an einen externen RADIUS-Server weiterleiten kann. Für eine automatische Zuweisung einer VLAN-ID aufgrund der Anmeldeinformationen wird ein externer RADIUS-Server benötigt.

- ④ Für eine Weiterleitung der RADIUS-Anfragen an einen anderen RADIUS-Server tragen Sie dessen Adresse über LANconfig in die Liste der Forwarding-Server im Konfigurationsbereich 'RADIUS-Server' auf der Registerkarte 'Forwarding' ein. Alternativ tragen Sie die externen RADIUS-Server über WEBconfig ein unter **Experten-Konfiguration ▶ Setup ▶ RADIUS ▶ Server ▶ Weiterleit-Server**.
- ⑤ Konfigurieren Sie die Einträge im RADIUS-Server entsprechend, damit den anfragenden WLAN-Clients anhand bestimmter Merkmale die richtigen VLAN-IDs zugewiesen werden.



Weitere Information zu RADIUS finden Sie im LCOS-Referenzhandbuch bzw. in der Dokumentation Ihres RADIUS-Servers.

4.3.9 Prüfung der WLAN-Clients über RADIUS (MAC-Filter)

Bei der Nutzung von RADIUS zur Authentifizierung der WLAN-Clients kann neben einem externen RADIUS-Server auch die interne Benutzertabelle der LANCOM WLAN Controller genutzt werden, um nur bestimmten WLAN-Clients anhand ihrer MAC-Adresse den Zugang zum WLAN zu erlauben.

Tragen Sie die zugelassenen MAC-Adressen über LANconfig in die RADIUS-Datenbank im Konfigurationsbereich 'RADIUS-Server' auf der Registerkarte 'Allgemein' ein. Verwenden Sie dabei die MAC-Adresse als 'Name' und ebenso als 'Passwort' und wählen Sie als Authentifizierungsmethode 'Alle'.

Alternativ tragen Sie die zugelassenen MAC-Adressen über WEBconfig ein unter **Experten-Konfiguration ▶ Setup ▶ RADIUS ▶ Server ▶ Benutzer**.



Als 'Benutzername' **und** 'Passwort' wird jeweils die MAC-Adresse in der Schreibweise 'AABBCC-DDEEFF' eingetragen.

Benutzer

Benutzername

Passwort

(Wiederholen)
Passwort

Limitiere-Auth-Methoden

- PAP
- CHAP
- MSCHAP
- MSCHAPv2
- EAP
- Alle

4.3.10 Access Point deaktivieren oder dauerhaft aus der WLAN-Struktur entfernen

In manchen Fällen ist es notwendig, einen vom WLAN Controller verwalteten Access Point entweder vorübergehend zu deaktivieren oder dauerhaft aus der WLAN-Struktur zu entfernen.

Access Point deaktivieren

Um eine Access Point zu deaktivieren, setzen Sie den entsprechenden Eintrag in der AP-Tabelle auf 'inaktiv' oder löschen Sie den Eintrag aus der Tabelle. Dadurch werden die WLAN-Module im Managed-Modus ausgeschaltet, die entsprechenden SSIDs werden im Access Point gelöscht.



Die WLAN-Module und die WLAN-Netzwerke (SSIDs) werden auch dann abgeschaltet, wenn der autarke Weiterbetrieb ('Autarker Weiterbetrieb' → Seite 53) aktiviert ist.

Ein so deaktivierter Access Point bleibt mit dem WLAN Controller verbunden, die Zertifikate bleiben erhalten. Der WLAN Controller kann also jederzeit durch das Aktivieren des Eintrags in der AP-Tabelle oder durch einen neuen Eintrag in der AP-Tabelle für die entsprechende MAC-Adresse den Access Point und seine WLAN-Module im Managed-Modus wieder einschalten.

Wird die Verbindung zu einem deaktivierten Access Point getrennt (unbeabsichtigt z. B. durch Störung im LAN oder gezielt durch den Administrator), dann beginnt der Access Point eine neue Suche nach einem passenden WLAN Controller. Der bisherige WLAN Controller kann zwar das Zertifikat auf Gültigkeit prüfen, hat aber keinen (aktiven) Eintrag in der AP-Tabelle – er wird also zum sekundären WLAN Controller für diesen Access Point. Findet der Access Point einen primären WLAN Controller, so wird er sich bei diesem anmelden.

Access Point dauerhaft aus der WLAN-Struktur entfernen

Damit ein Access Point auf Dauer nicht mehr Mitglied der zentral verwalteten WLAN-Struktur ist, müssen die Zertifikate im SCEP-Client gelöscht oder widerrufen werden.

- Wenn Sie Zugriff auf den Access Point haben, können Sie die Zertifikate am schnellsten durch einen Reset des Geräts löschen.
- Wurde das Gerät gestohlen und soll aus diesem Grund aus der WLAN-Struktur entfernt werden, so müssen die Zertifikate in der CA des WLAN Controllers widerrufen werden. Wechseln Sie dazu unter WEBconfig in den Bereich **Status ▶ Zertifikate ▶ SCEP-CA ▶ Zertifikate** in die **Zertifikatsstatus-Tabelle**. Löschen Sie dort das Zertifikat für die MAC-Adresse des Access Points, den Sie aus der WLAN-Struktur entfernen möchten. Die Zertifikate werden dabei nicht gelöscht, aber als abgelaufen markiert.

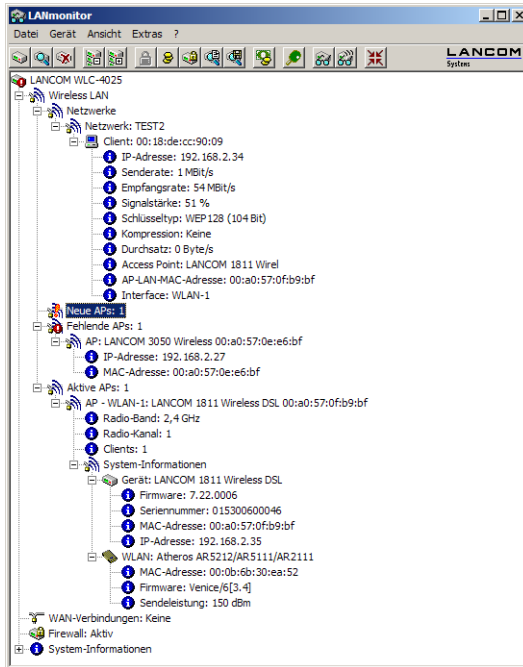


Bei einer Backup-Lösung mit redundanten WLAN Controllern müssen die Zertifikate in allen WLAN Controllern widerrufen werden!

4.4 Anzeigen und Aktionen im LANmonitor

Über den LANmonitor haben sie einen schnellen Überblick über die LANCOM WLAN Controller im Netzwerk und die Access Points in der WLAN-Struktur. LANmonitor zeigt dabei u. a. die folgenden Informationen:

■ Kapitel 4: Konfiguration des WLAN Controllers



- Aktive WLAN-Netzwerke mit den eingebuchten WLAN-Clients sowie der Bezeichnung des Access Points, bei dem der WLAN-Client eingebucht ist.
- Anzeige der neuen Access Points mit IP- und MAC-Adresse
- Anzeige der fehlenden Access Points mit IP- und MAC-Adresse
- Anzeige der gemanagten Access Points mit IP- und MAC-Adresse, verwendetem Frequenzband und Kanal

Über die rechte Maustaste kann auf den Access Points ein Kontext-Menü geöffnet werden, in dem folgende Aktionen zur Auswahl stehen:

■ Neuer Access Point zu Profil zuordnen

Bietet die Möglichkeit, einem neuen Access Point eine Konfiguration zuzuordnen und ihn so in die WLAN-Struktur aufzunehmen ('Access Points akzeptieren über den LANmonitor' → Seite 61).

■ Access Point trennen

Trennt die Verbindung zwischen Access Point und WLAN Controller. Der Access Point sucht dann erneut nach einem zuständigen WLAN Controller. Diese Aktion wird z. B. verwendet, um Access Points nach einem Backup-

Fall vom Backup-Controller zu trennen und wieder auf den eigentlichen WLAN Controller zu leiten.

■ Aktualisieren

Aktualisiert die Anzeige des LANmonitors.

4.5 Konfiguration der Access Points

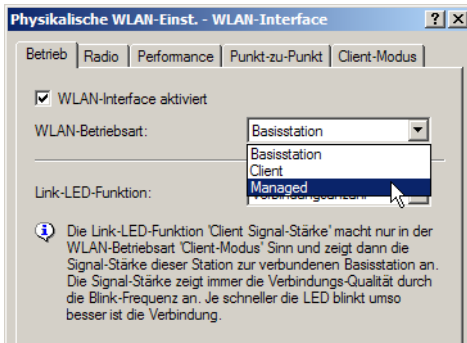
Ab der Firmware-Version LCOS 7.20 unterscheiden sich LANCOM Access Points (z. B. LANCOM L-54ag) und LANCOM Wireless Router (z. B. LANCOM 1811 Wireless) bzgl. der Einstellung der WLAN-Module im Auslieferungszustand.

- Bei LANCOM Access Points sind im Auslieferungszustand die WLAN-Module auf die Betriebsart 'Managed' eingestellt. In diesem Modus suchen die LANCOM Access Points nach einem zentralen WLAN Controller, der ihnen eine Konfiguration zuweisen kann, und bleiben so lange im „Such-Modus“, bis sie einen passenden WLAN Controller gefunden haben oder die Betriebsart für die WLAN-Module manuell geändert wird.
- Bei LANCOM Wireless Routern sind im Auslieferungszustand die WLAN-Module auf die Betriebsart 'Access-Point' eingestellt. In diesem Modus arbeiten die LANCOM Wireless Router als autarke Access Points mit einer im Gerät lokal gespeicherten Konfiguration. Um Teilnehmer einer zentral über WLAN Controller verwalteten WLAN-Struktur zu werden, muss die Betriebsart für die WLAN-Module in den gewünschten LANCOM Wireless Routern auf 'Managed' umgestellt werden.



Die Betriebsart kann für jedes WLAN-Modul separat eingestellt werden. Bei Modellen mit zwei WLAN-Modulen kann so ein Modul mit einer lokalen Konfiguration arbeiten, das zweite kann zentral über den WLAN Controller verwaltet werden.

Für einzelne Geräte finden Sie die Betriebsart der WLAN-Module in LANconfig über **Wireless LAN ► Allgemein ► Physikalische WLAN-Einstellungen ► Betrieb:**



Wenn Sie die Betriebsart für mehrere Geräte gleichzeitig umstellen möchten, können Sie auf die Geräte ein einfaches Script anwenden mit folgenden Zeilen:

- # Script (7.22 / 23.08.2007)
- lang English
- flash 0
- cd Setup/Interfaces/WLAN/Operational
- set WLAN-1 0 managed-AP 0
- # done
- exit



Weitere Informationen zu Scripten finden Sie im LCOS-Referenzhandbuch.

5 Sicherheits- Einstellungen

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

5.1 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

5.1.1 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.

5.1.2 Zugangskontrolle über MAC-Adresse

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

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

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

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

5.1.3 LANCOM Enhanced Passphrase Security

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

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

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

5.1.4 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 85) oder aber eine zusätzliche Verschlüsselung der WLAN-Verbindung einrichten, wie sie auch für VPN-Tunnel verwendet wird ('IPSec-over-WLAN' → Seite 86). 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.

5.1.5 802.1x / 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 WLAN Controller oder externer RADIUS/EAP-Server) erwaltes 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.

5.1.6 IPSec-over-WLAN

Mittels IPSec-over-WLAN kann zusätzlich zu den bereits vorgestellten Sicherheitsmechanismen ein Funknetzwerk optimal abgesichert werden. Hierzu sind in der Regel ein externes VPN-Gateway und der LANCOM Advanced VPN Client (für Windows 2000, XP und Vista™) erforderlich. Der LANCOM WLAN Controller bietet selbst nur einige wenige VPN-Tunnel z.B. zur Standortkopplung an. Für andere Betriebssysteme existiert Clientsoftware von Fremdherstellern.

5.2 Tipps für den richtigen Umgang mit Schlüsseln und Passphrases

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

■ Halten Sie Schlüssel so geheim wie möglich.

Notieren Sie niemals einen Schlüssel. 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 Passphrases.

Nutzen Sie deswegen LEPS, um eine individuelle Passphrase nutzen zu können.

5.3 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.

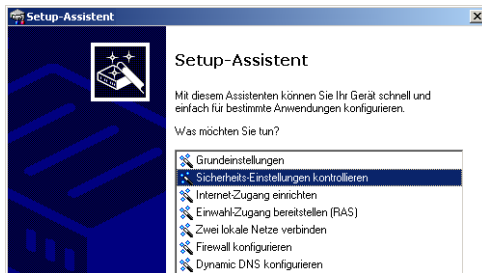
Ihr LANCOM verfügt über einen Kennwortschutz für den Konfigurationszugang. Dieser wird schon während der Grundkonfiguration durch Angabe eines Kennwortes aktiviert.

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 Fehlversuch für eine Dauer von fünf Minuten.

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

5.3.1 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.
- 4 In einem weiteren Schritt werden die Parameter der Konfigurationssperre wie Anzahl der Fehllogins und Dauer der Sperre eingestellt.
- 5 Der Assistent informiert Sie sobald die Eingaben vollständig sind. Schließen Sie die Konfiguration mit **Fertig stellen** ab.

5.3.2 Assistent für WEBconfig

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

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

5.4 Der Firewall-Assistent

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



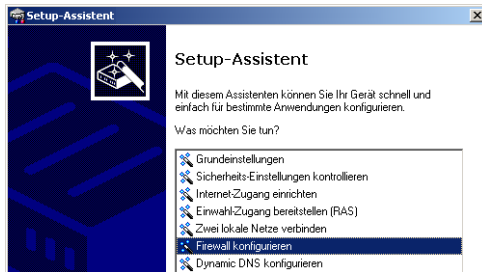
Stateful-Inspection-Firewall und Firewall-Filter im LANCOM WLAN Controller kommen dann zum Einsatz, wenn das Gerät gleichzeitig auch als Layer-3-Router betrieben wird. Damit können z.B. SSIDs oder VLANs auf kontrolliert auf bestimmte Gegenstellen abbilden. Weitere Informationen finden Sie dazu im LCOS Referenzhandbuch.

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

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

5.4.1 Assistent für LANconfig

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



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

5.4.2 Konfiguration unter WEBconfig

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

5.5 Die Sicherheits-Checkliste

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



Detaillierte Informationen zu den angesprochenen Sicherheitseinstellungen finden Sie im Referenzhandbuch.

■ Haben Sie ein Kennwort für die Konfiguration vergeben?

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

■ Haben Sie die Fernkonfiguration zugelassen?

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

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

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

■ Haben Sie die Firewall aktiviert?

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

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

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

■ Haben Sie IP-Masquerading aktiviert?

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

■ Haben Sie kritische Ports über Filter geschlossen?

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

■ Haben Sie bestimmte Stationen von dem Zugriff auf den Router ausgeschlossen?

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

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

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

■ Haben Sie das Funknetzwerk durch eine Verschlüsselung, ACL und LEPS abgesichert?

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

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

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

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

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

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

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

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

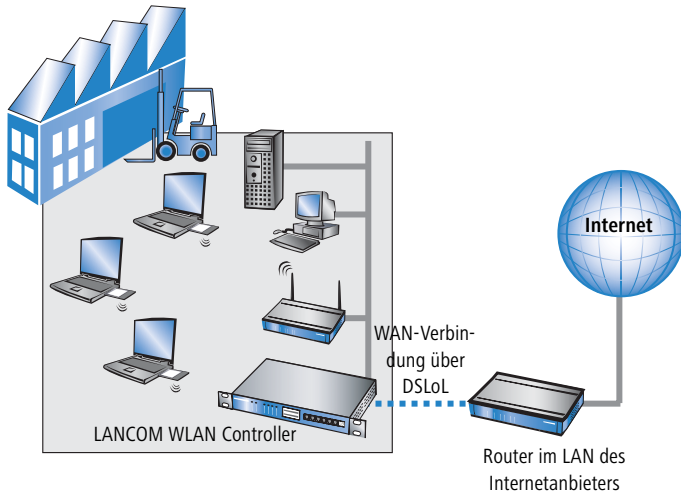
Mit der Funktion des „Autarken Weiterbetriebs“ wird die Konfiguration für ein WLAN-Interface, das von einem LANCOM WLAN Controller verwaltet wird, nur für eine bestimmte Zeit im Flash bzw. ausschließlich im RAM gespeichert. Die Konfiguration des Gerätes wird gelöscht, wenn der Kontakt zum WLAN Controller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

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

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

6 Den Internet-Zugang einrichten

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



Kennt der Setup-Assistent Ihren Internet-Anbieter?

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

Zusätzlich Angaben bei unbekanntem Internet-Anbieter

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

Weitere Verbindungsoptionen

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

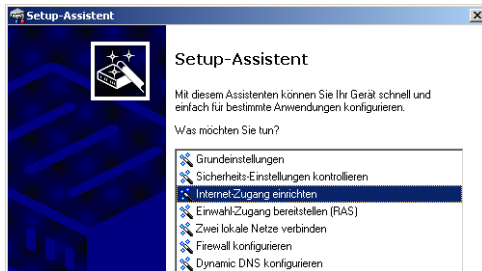
- Zeitliche Abrechnung oder Flatrate – wählen Sie aus, nach welchem Modell Ihr Internetanbieter die Nutzung abrechnet.
 - Bei der zeitlichen Abrechnung können Sie am LANCOM Router einstellen, dass bestehende Verbindungen automatisch abgebaut werden, wenn für eine bestimmte Dauer (die sogenannte Haltezeit)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

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

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

6.1 Anleitung für LANconfig

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



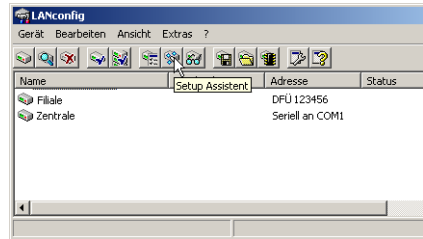
- ② Wählen Sie im Auswahlmenü den Setup-Assistenten **Internet-Zugang einrichten** und bestätigen Sie die Auswahl mit **Weiter**.
- ③ In den folgenden Fenstern wählen Sie Ihr Land, nach Möglichkeit Ihren Internetanbieter, und geben Sie die Zugangsdaten ein.
- ④ Je nach Verfügbarkeit bietet Ihnen der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

■ Kapitel 6: Den Internet-Zugang einrichten

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

LANconfig: Schneller Aufruf der Setup-Assistenten

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



6.2 Anleitung für WEBconfig

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

7 Zwei Netzwerke verbinden

Mit der Netzwerkkopplung (auch LAN-LAN-Kopplung) des LANCOM Router werden zwei lokale Netzwerke miteinander verbunden. Bei der Kopplung über VPN wird die Verbindung zwischen den beiden LANs über eine besonders geschützte Verbindung über das öffentliche Internet hergestellt. In beiden LANs wird dazu ein Router mit VPN-Unterstützung benötigt.

Die Einrichtung einer LAN-LAN-Kopplung erfolgt über einen Setup-Assistenten in bekannt komfortabler Art.

Immer beide Seiten konfigurieren

Beide an der Netzwerkkopplung beteiligten Router müssen konfiguriert werden. Dabei ist darauf zu achten, dass die Konfigurationsangaben auf beiden Seiten zueinander passen.



Die folgende Anleitung geht davon aus, dass auf beiden Seiten LANCOM Router-Router verwendet werden. Die Netzwerkkopplung ist zwar auch mit Routern anderer Hersteller möglich. Eine gemischte Konfiguration erfordert aber in aller Regel tiefer gehende Eingriffe an beiden Geräten. Ziehen Sie in einem solchen Fall das Referenzhandbuch zu Rate.

Sicherheitsaspekte

Der Zugang zu Ihrem LAN muss natürlich gegen unbefugten Zugriff geschützt sein. Ein LANCOM bietet daher eine ganze Reihe von Sicherheitsmechanismen an, bei deren Einsatz ein hervorragender Schutz gewährleistet ist: Bei Kopplungen über VPN werden die Daten mittels IPSec übertragen und dabei mit den Verfahren 3-DES, AES oder Blowfish verschlüsselt.

7.1 Welche Angaben sind notwendig?

Der Assistent fragt alle notwendigen Daten Schritt für Schritt ab. Nach Möglichkeit sollten Ihnen die erforderlichen Angaben schon vor Aufruf des Assistenten vorliegen.

Die Bedeutung aller Angaben, nach denen Sie der Assistent fragt, erklären wir Ihnen an Hand eines typischen Beispiels: der Kopplung einer Filiale an ihre Zentrale. Die beiden beteiligten Router tragen die Namen 'ZENTRALE' und 'FILIALE'.

Den folgenden Tabellen entnehmen Sie, welche Einträge an welchem der beiden Router vorzunehmen sind. Pfeile kennzeichnen die Abhängigkeiten zwischen den Einträgen.

7.1.1 Allgemeine Angaben

Die folgenden Angaben werden für die Einrichtung einer LAN-LAN-Kopplung benötigt.



Weitere Informationen zur Netzwerkkopplung über VPN-Verbindungen mit anderen Verfahren entnehmen Sie bitte dem LANCOM Referenzhandbuch.

Angabe	Gateway 1		Gateway 2
Typ der eigenen IP-Adresse	statisch/dynamisch		statisch/dynamisch
Typ IP-Adresse der Gegenstelle	statisch/dynamisch		statisch/dynamisch
Name des eigenen Gerätes	'ZENTRALE'		'FILIALE'
Name der Gegenstelle	'FILIALE'		'ZENTRALE'
Kennwort zur sicheren Übertragung der IP-Adresse	'Geheim'		'Geheim'
Shared Secret für Verschlüsselung	'Secret'		'Secret'
IP-Adresse der Gegenstelle	'10.0.2.100'		'10.0.1.100'
IP-Netzadresse des entfernten Netzes	'10.0.2.0'		'10.0.1.0'
Netzmaske des entfernten Netzwerks	255.255.255.0		255.255.255.0
Dömnänenbezeichnung im entfernten Netzwerk	'zentrale'		'filiale'
Eigene Stationen bei Zugriff auf entferntes Netz verstecken (Extranet-VPN)?	Ja/Nein		Ja/Nein
NetBIOS-Routing für Zugriff auf entferntes Netz?	Ja/Nein		Ja/Nein
Name einer lokalen Arbeitsgruppe (nur bei NetBIOS)	'workgroup1'		'workgroup2'

Hinweise zu den einzelnen Werten:

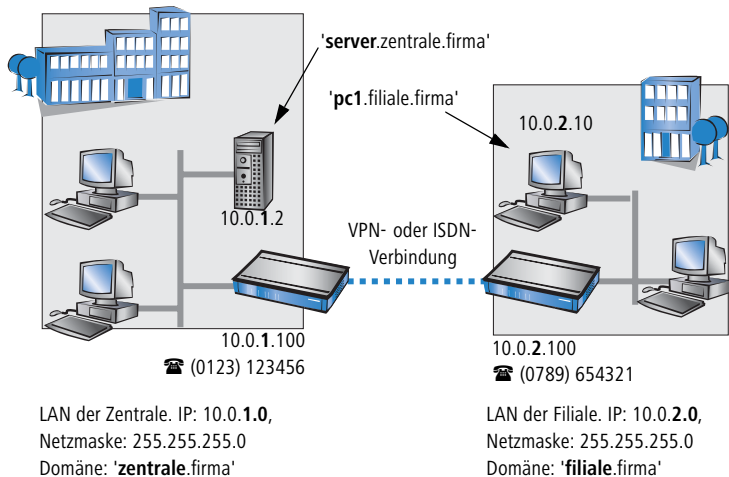
- Für VPN-Verbindungen über das Internet muss der Typ der IP-Adressen auf beiden Seiten angegeben werden. Es gibt zwei **Typen von IP-Adressen**: statische und dynamische. Eine Erklärung zum Unterschied der beiden IP-Adresstypen finden Sie im Referenzhandbuch.

Die Dynamic-VPN-Funktionalität erlaubt VPN-Verbindungen nicht nur zwischen Gateways mit statischen (festen) IP-Adressen, sondern auch bei Verwendung dynamischer IP-Adressen.

- Wenn Sie Ihr LANCOM noch nicht benannt haben, so fragt Sie der Assistent nach einem neuen **eigenen Gerätenamen**. Mit der Eingabe benennen Sie Ihr LANCOM neu. Achten Sie darauf, dass Sie beide Gegenstellen unterschiedlich benennen.
- Der **Name der Gegenstelle** wird für deren Identifikation benötigt.
- Das **Shared Secret** ist das zentrale Kennwort für die Sicherheit der VPN-Verbindung. Es muss auf beiden Seiten identisch eingegeben werden.

7.1.2 Einstellungen für den TCP/IP-Router

Im TCP/IP-Netzwerk kommt der korrekten Adressierung eine besondere Bedeutung zu. Bei einer Netzwerkkopplung ist zu beachten, dass beide Netzwerke logisch voneinander getrennt sind. Sie müssen daher jeweils über eine eigene Netzwerknummer verfügen (im Beispielfall '10.0.1.x' und '10.0.2.x'). Die beiden Netzwerknummern müssen unterschiedlich sein.



Im Gegensatz zum Internet-Zugang werden bei der Kopplung von Netzen alle IP-Adressen aus den beteiligten Netzen auch im entfernten LAN sichtbar, nicht nur die der Router. Der Rechner mit der IP-Adresse 10.0.2.10 im LAN der Filiale sieht den Server 10.0.1.2 in der Zentrale und kann (entsprechende Rechte vorausgesetzt) auch auf ihn zugreifen. Gleiches gilt umgekehrt.

DNS-Zugriffe ins entfernte LAN

Der Zugriff auf entfernte Rechner kann in einem TCP/IP-Netzwerk nicht nur über die Angabe der IP-Adresse erfolgen, sondern dank DNS auch über frei definierbare Namen.

Beispielsweise kann der Rechner mit dem Namen 'pc1.filiale.firma' (IP 10.0.2.10) auf den Server in der Zentrale nicht nur über dessen IP-Adresse zugreifen, sondern auch über dessen Namen 'server.zentrale.firma'. Einzige Voraussetzung: Die Domäne des entfernten Netzwerks muss im Assistenten angegeben werden.



Die Angabe der Domäne ist nur im LANconfig-Assistenten möglich. Bei WEBconfig nehmen Sie die entsprechenden Einstellungen später in der Expertenkonfiguration vor. Nähere Informationen finden Sie im LANCOM Router-Referenzhandbuch.

VPN-Extranet

Bei einer LAN-LAN-Kopplung über VPN können Sie die eigenen Stationen hinter einer anderen IP-Adresse maskieren. Bei dieser als 'Extranet-VPN' bezeichneten Betriebsart erscheinen die eigenen Rechner gegenüber dem entfernten LAN nicht mit ihrer eigenen IP-Adresse, sondern mit einer anderen frei wählbaren (z. B. der des VPN-Gateways).

Den Stationen im entfernten LAN wird dadurch der direkte Zugriff auf die Rechner im eigenen LAN verwehrt. Wurde beispielsweise im LAN der Filiale für den Zugriff auf die Zentrale der Extranet-VPN-Modus hinter der IP-Adresse '10.10.2.100' eingestellt, und greift der Rechner '10.10.2.10' auf den Server '10.10.1.2' zu, so erscheint bei diesem eine Anfrage von der IP '10.10.2.100'. Die tatsächliche IP-Adresse des Rechners bleibt verborgen.

Wenn ein LAN im Extranet-Modus gekoppelt wird, so wird auf der Gegenseite nicht dessen tatsächliche (verborgene) LAN-Adresse angegeben, sondern die IP-Adresse, mit der das LAN nach außen hin auftritt (im Beispiel '10.10.2.100'). Die Netzmaske lautet in diesem Fall '255.255.255.255'.

7.1.3 Einstellungen für NetBIOS-Routing

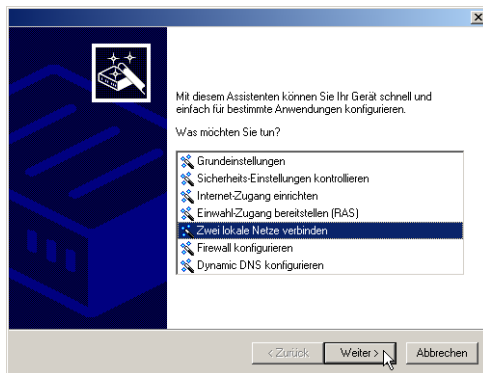
Das NetBIOS-Routing ist schnell eingerichtet: Zusätzlich zu den Angaben für das verwendete TCP/IP-Protokoll muss lediglich der Name einer Windows-Arbeitsgruppe aus dem eigenen LAN des Routers angegeben werden.

- i** Entfernte Windows-Arbeitsgruppen erscheinen nicht in der Windows-Netzwerkumgebung, sondern können nur direkt (z. B. über die Computer-Suche) angesprochen werden.

7.2 Anleitung für LANconfig

Führen Sie die Konfiguration nacheinander an beiden Routern durch.

- ① Rufen Sie den Assistenten 'Zwei lokale Netze verbinden' auf. Folgen Sie den Anweisungen des Assistenten und geben Sie notwendigen Daten ein.



- ② Der Assistent meldet, sobald ihm alle notwendigen Angaben vorliegen. Schließen Sie den Assistenten dann mit **Fertig stellen** ab.
- ③ Nach Abschluss der Einrichtung an beiden Routern können Sie die Netzwerkverbindung testen. Versuchen Sie dazu, einen Rechner im entfernten LAN (z. B. mit ping) anzusprechen. Der LANCOM Router sollte automa-

tisch eine Verbindung zur Gegenstelle aufbauen und den Kontakt zum gewünschten Rechner herstellen.

Ping – schneller Verbindungstest einer TCP/IP-Verbindung

Für den Test einer TCP/IP-Verbindung schicken Sie einfach ein `ping` von Ihrem Rechner an einen Rechner im entfernten Netz. Details zum Ping-Befehl finden Sie in der Dokumentation Ihres Betriebssystems.

IPX- und NetBIOS-Verbindungen testen Sie, indem Sie von Ihrem Rechner aus einen entfernten Novell-Server bzw. einen Rechner in der entfernten Windows-Arbeitsgruppe suchen.

```

Eingabeaufforderung
C:\>ping 10.0.1.2

Ping wird ausgeführt für 10.0.1.2 mit 32

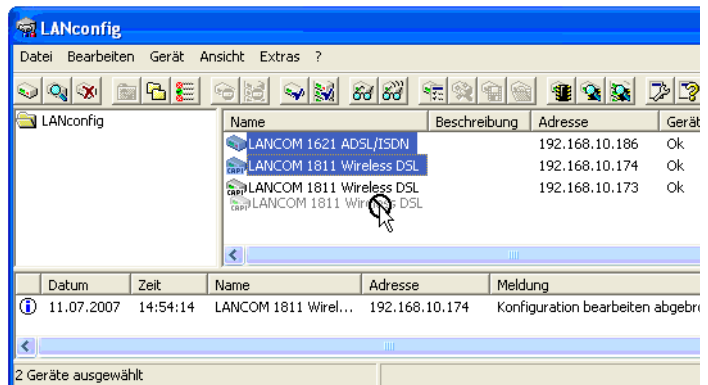
Antwort von 10.0.1.2: Bytes=32 Zeit=10ms
Antwort von 10.0.1.2: Bytes=32 Zeit=20ms
Antwort von 10.0.1.2: Bytes=32 Zeit=10ms
Antwort von 10.0.1.2: Bytes=32 Zeit<10ms

Ping-Statistik für 10.0.1.2:
    Pakete: Gesendet = 4, Empfangen = 4,
    Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum = 20ms, Mitte
  
```

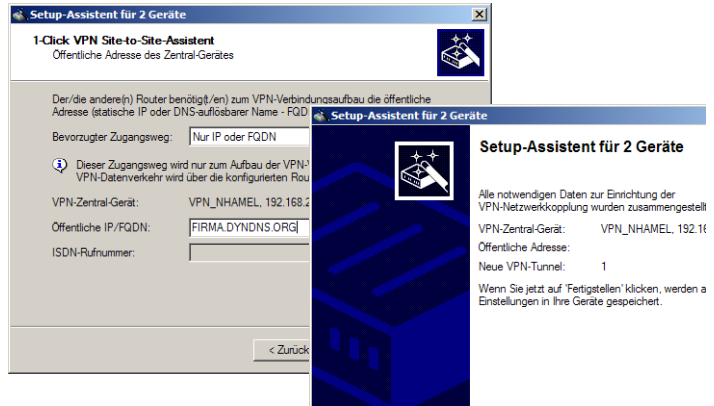
7.3 1-Click-VPN für Netzwerke (Site-to-Site)

Die Einstellungen für die Kopplung von Netzwerken können sehr komfortabel über den 1-Click-VPN-Assistenten vorgenommen werden. Dabei können sogar mehrere Router gleichzeitig an einen zentrales Netzwerk gekoppelt werden.

- ① Markieren Sie in LANconfig die Router der Filialen, für die Sie eine VPN-Kopplung zu einem zentralen Router einrichten möchten.
- ② Ziehen Sie die Geräte mit der Maus auf den Eintrag für den zentralen Router.



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



- ④ Geben Sie die Adresse bzw. den Namens des zentralen Routers an.
- ⑤ Im letzten Schritt legen Sie fest, wie die verbundenen Netzwerke untereinander kommunizieren können:
- Nur das INTRANET der Zentrale wird für die Außenstellen verfügbar gemacht werden.
 - Alle privaten Netze der Außenstellen können ebenfalls über die Zentrale untereinander verbunden werden.

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

7.4 Anleitung für WEBconfig

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

Führen Sie die Konfiguration nacheinander an beiden Routern durch.

- ① Rufen Sie im Hauptmenü den Assistenten 'Zwei lokale Netze verbinden' auf. Folgen Sie den Anweisungen des Assistenten und geben Sie die notwendigen Daten ein.

■ *Kapitel 7: Zwei Netzwerke verbinden*

- ② Der Assistent meldet, sobald ihm alle notwendigen Angaben vorliegen. Schließen Sie den Assistenten dann mit **Weiter** ab.
- ③ Nach Abschluss der Einrichtung an beiden Routern können Sie die Netzwerkverbindung testen. Versuchen Sie dazu, einen Rechner im entfernten LAN (z. B. mit `ping`) anzusprechen. Der LANCOM Router sollte automatisch eine Verbindung zur Gegenstelle aufbauen und den Kontakt zum gewünschten Rechner herstellen.

8 Einwahl-Zugang bereitstellen

An Ihrem LANCOM können Sie Einwahl-Zugänge einrichten, über die sich einzelne Rechner in Ihr LAN einwählen können und für die Dauer der Verbindung vollwertiger Teilnehmer des Netzwerks werden. Dieser Dienst wird auch als RAS (**R**emote **A**ccess **S**ervice) bezeichnet. Bei einem RAS-Zugang über VPN wird die Verbindung zwischen dem LAN und dem Einwahlrechner über eine besonders geschützte Verbindung über das öffentliche Internet hergestellt. Der Router im LAN benötigt eine VPN-Unterstützung, der Einwahlrechner einen beliebigen Zugang zum Internet und einen VPN Client.

Die Einrichtung eines Einwahl-Zugangs erfolgt über einen Setup-Assistenten in bekannt komfortabler Art.

Sicherheitsaspekte

Der Zugang zu Ihrem LAN muss natürlich gegen unbefugten Zugriff geschützt sein. Bei Kopplungen über VPN werden die Daten mittels IPSec übertragen und dabei mit den Verfahren 3-DES, AES oder Blowfish verschlüsselt.

8.1 Welche Angaben sind notwendig?

Der Assistent richtet den Einwahl-Zugang nur für einen Benutzer ein. Für jeden zusätzlichen Benutzer führen Sie den Assistenten ein weiteres Mal aus.

8.1.1 Allgemeine Angaben

Die folgenden Angaben werden für die Einrichtung eines RAS-Zugangs benötigt.



Weitere Informationen zu RAS-Zugängen über VPN-Verbindungen mit anderen Verfahren entnehmen Sie bitte dem LANCOM Referenzhandbuch.

Angabe

Benutzername

Passwort

Shared Secret für Verschlüsselung

Eigene Stationen bei Zugriff auf entferntes Netz verstecken (Extranet-VPN)?

Angabe

IP-Adresse(n) für den oder die Einwahlrechner: fest oder dynamisch aus einem Adressbereich (IP-Adress-Pool)

NetBIOS-Routing für Zugriff auf entferntes Netz?

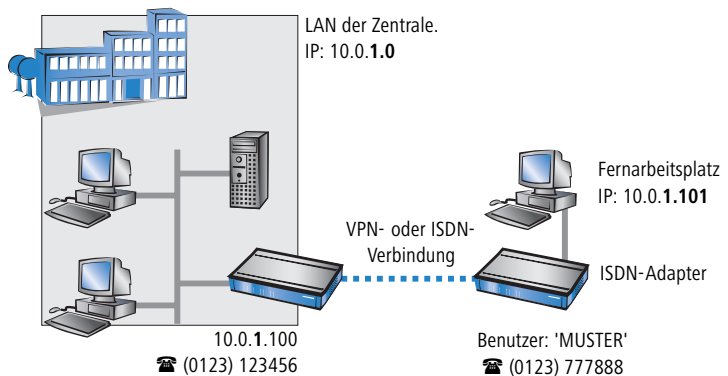
Name einer lokalen Arbeitsgruppe (nur bei NetBIOS)

Hinweise zu den einzelnen Werten:

- **Benutzername und Passwort:** Mit diesen Zugangsdaten weist sich der Benutzer bei der Einwahl aus.

8.1.2 Einstellungen für TCP/IP

Beim Protokoll TCP/IP muss jedem aktiven RAS-Benutzer eine eigene IP-Adresse zugewiesen werden.



Diese IP-Adresse können Sie entweder bei der Anlage eines Benutzers manuell festlegen. Einfacher ist es, den LANCOM Router einem Benutzer automatisch bei der Einwahl eine freie IP-Adresse zuteilen zu lassen. In diesem Fall legen Sie bei der Konfiguration nur den IP-Adressbereich fest, aus dem der LANCOM Router die Adresse für den RAS-Benutzer nehmen soll.

Achten Sie sowohl bei der manuellen als auch bei der automatischen IP-Adresszuteilung darauf, dass es sich um freie Adresse(n) aus dem Adressbereich Ihres lokalen Netzwerks handelt. Im Beispiel wird dem PC bei der Einwahl die IP-Adresse '10.0.1.101' zugewiesen.

Mit dieser IP-Adresse ist der Rechner ein vollwertiger Teilnehmer im LAN: Er kann (bei entsprechender Berechtigung) auf alle anderen Geräte im LAN

zugreifen. Umgekehrt gilt dieses Verhältnis auch: auf den entfernten Rechner kann auch aus dem LAN zugegriffen werden.

8.1.3 Einstellungen für NetBIOS-Routing

Für die Verwendung von NetBIOS muss lediglich der Name einer Windows-Arbeitsgruppe aus dem eigenen LAN des Routers angegeben werden.



Die Verbindung wird nicht automatisch aufgebaut. Der RAS-Benutzer muss bei Bedarf zunächst manuell eine Verbindung über das DFÜ-Netzwerk zum LANCOM Router herstellen. Bei bestehender Verbindung kann die Rechner im anderen Netz suchen und auf sie zugreifen (über **Suchen** ► **Computer**, nicht über die Netzwerkumgebung).

8.2 Einstellungen am Einwahl-Rechner

Für die Einwahl in ein Netzwerk über VPN benötigt ein Rechner:

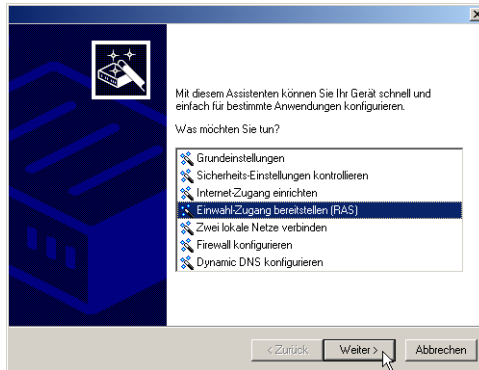
- Einen Zugang zum Internet
- Einen VPN-Client

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

Der Assistent fragt im folgenden die Werte ab, die beim Anlegen des RAS-Zugangs im LANCOM Router festgelegt wurden.

8.3 Anleitung für LANconfig

- ① Rufen Sie den Assistenten 'Zugang bereitstellen (RAS, VPN, IPsec über WLAN)' auf. Folgen Sie den Anweisungen des Assistenten und geben Sie die notwendigen Daten ein.



- ② Der Assistent meldet, sobald ihm alle notwendigen Angaben vorliegen. Schließen Sie den Assistenten dann mit **Fertig stellen** ab.
- ③ Konfigurieren Sie wie beschrieben den Zugang am Einwahl-PC. Anschließend können Sie die Verbindung testen (siehe Kasten 'Ping – schneller Verbindungstest einer TCP/IP-Verbindung').

8.4 1-Click-VPN für LANCOM Advanced VPN Client

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

- ① Starten Sie über LANconfig den Setup-Assistenten 'Zugang bereitstellen' und wählen Sie die 'VPN-Verbindung'.
- ② Aktivieren Sie die Optionen 'LANCOM Advanced VPN Client' und 'Beschleunigen Sie das Konfigurieren mit 1-Click-VPN'.

- ③ Geben Sie den Namen für diesen Zugang ein und wählen Sie aus, über welche Adresse der Router aus dem Internet erreichbar ist.
- ④ Im letzten Schritt können Sie wählen, wie die neuen Zugangsdaten ausgegeben werden sollen:
 - Profil als Importdatei für den LANCOM Advanced VPN Client speichern
 - Profil per E-Mail versenden
 - Profil ausdrucken



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

Zum Versenden der Profildatei per E-Mail muss in der Konfiguration des Geräts ein SMTP-Konto mit den erforderlichen Zugangsdaten eingerichtet sein. Außerdem muss auf dem Konfigurationsrechner ein E-Mail-Programm als Standard-Mail-Anwendung eingerichtet sein, über die auch andere Anwendungen E-Mails versenden dürfen.

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

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

8.5 Anleitung für WEBconfig

- ① Rufen Sie im Hauptmenü den Assistenten 'Einwahl-Zugang bereitstellen (RAS)' auf. Folgen Sie den Anweisungen des Assistenten und geben Sie die notwendigen Daten ein.
- ② Konfigurieren Sie wie beschrieben den Zugang am Einwahl-PC. Anschließend können Sie die Verbindung testen (siehe Kasten 'Ping – schneller Verbindungstest einer TCP/IP-Verbindung').

9 Anhang

9.1 Leistungs- und Kenndaten

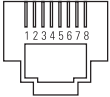
		LANCOM WLC-4006	LANCOM WLC-4025
Anschlüsse	Ethernet LAN	5x 10/100Base-TX, Autosensing, Switch mit Node/Hub Autosensing	
	WAN	Ein beliebiger Ethernet-Port kann als WAN-Anschluss geschaltet werden.	
	Konfiguration	Serielle V.24/RS-232 Outband Schnittstelle mit Mini-DIN8 Anschluss	
	Stromversorgung	12V DC über externes Netzteil	internes Netzteil (110-230 V)
Gehäuse		210 mm x 143 mm x 45 mm (B x H x T), robustes Kunststoffgehäuse, für Wandmontage vorbereitet	Robustes Metallgehäuse, 19" 1 HE, (435 x 45 x 207 mm) mit abschraubbaren Montagewinkeln, Netzwerkan-schlüsse auf der Frontseite
Zulassungen		EU (CE-Zertifizierung: EN 55022, EN 55024, EN 60950)	
Umgebung / Temperatur		5 °C bis +35 °C bei 80% max. Luftfeuchtigkeit (nicht kondensierend)	5 °C bis +40 °C bei 80% max. Luftfeuchtigkeit (nicht kondensierend)
Lieferumfang		LAN-Kabel (CAT.5, STP, 3 m), RS232-Kabel, externes Netzteil, gedrucktes Handbuch (Deutsch, Englisch), Software-CD	LAN-Kabel (CAT.5, STP, 3 m), RS232-Kabel, Kaltgerätekabel, gedrucktes Handbuch (Deutsch, Englisch), Software-CD
Optionen		<ul style="list-style-type: none"> ■ LANCOM WLAN Controller-12-Option zur Verwaltung von bis zu 12 Access Points ■ LANCOM Service-Option (4 Jahre Garantie, Vorabaustausch) (Art.-Nr. 61401) 	<ul style="list-style-type: none"> ■ LANCOM WLAN Controller-50-Option zur Verwaltung von bis zu 50 Access Points ■ LANCOM Service-Option (4 Jahre Garantie, Vorabaustausch) (Art.-Nr. 61401)
Zubehör		<ul style="list-style-type: none"> ■ LANCOM Modem Adapter Kit zum Anschluß von Modems (analog oder GSM) an die serielle Konfigurationsschnittstelle Art.Nr. 110288 ■ LANCOM LCOS Referenzhandbuch (DE) Art.-Nr. 110405 	

9.2 Anschlussbelegung

9.2.1 Ethernet-Schnittstellen 10/100Base-T


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

DE

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

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

9.3 CE-Konformitätserklärungen



Hiermit erklärt LANCOM Systems, dass sich die in dieser Dokumentation beschriebenen Geräte in Übereinstimmung mit den grundlegenden Anforder-

rungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet.

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

Index

Numerics

10/100Base-TX	28
3-DES	97, 105
802.11i	83, 84, 85, 92
802.11i/	85
802.1p	18
802.1x	3, 83, 85

A

Access Control List	84
Access Point	3, 10
Access Point-Modus	22
Access Points manuell akzeptieren	61
ACL	84
Advanced Routing and Forwarding	18
AES	85, 97, 105
Alternative WLAN- Controller	51
Anschlussbelegung	112
Ethernet-Schnittstelle	112
Konfigurationsschnittstelle	112
LAN-Schnittstelle	112
Outband	112
WAN-Schnittstelle	112
Anzahl der VPN-Tunnel	27
autark	22
Autarker Weiterbetrieb	18, 53
Authentifizierung	16, 18
Auto-Accept	49, 50
Automatische Annahme neuer Access Points	45
Automatische Annahme neuer APs	49
Automatische Kanalwahl	56
Automatische Zuweisung der Default-Konfiguration	45, 48, 49, 50, 63
Autosensing	30

B

Background-Scanning	3
Backup mit primären und sekundären	

WLAN- Controllern	71
Backup mit redundanten WLAN- Controllern	70
Backupslösungen	69
Blowfish	97, 105
Broadcast	52

C

CA	16
CAPWAP	11, 14, 16, 18
CAPWAP-Tunneling	14
Certification Authority	16
Closed Network	83
Control And Provisioning of Wireless Access Points	11
CPU-Auslastung	27

D

Datagram Transport Layer Security	11
Datenkanal	11
Datum	27
Default-Gateway	91
Default-Konfiguration	43, 45, 48, 57
DHCP	42
DHCP-Server	19, 34, 40, 42
DiffServ	18
Discovery Request Message	15, 74
DNS	15
DNS-Server	19, 42
Zugriffe ins entfernte LAN	100
Domäne	100
Download	5
DSL-Übertragungsprotokoll	41
DTLS	11, 15, 18, 24, 26
Dynamische VLAN-Zuweisung	18, 75

E

EAP	12, 18, 83, 85
Einwahl-Zugang	105

E-Mail	58	IPSec	97, 105
Erwarteter Access Point	48	IPSec-over-WLAN	83
F		IPX-Router	18
Fast Roaming	18	K	
Fernkonfiguration	37, 41	Kennwort	35, 37
Firewall	19, 91	Konfiguration	49
Stationen sperren	91	Konfigurationsdatei	92
Firewall-Filter	88	Konfigurationskennwort	90
FirmSafe	20	Konfigurations-Schnittstelle	20
Firmware	5	Anschlusskabel	21
Firmwareversion	27	Konfigurationsschnittstelle	28
Flash	11, 53	Konfigurationsschutz	20, 35
Flatrate	95	Konfigurationszugriff	37, 41
G		Konformitätserklärungen	112
Gebührenschatz	37, 41	Kontrollkanal	11
Gerätename	27	L	
H		LAN	
Hardware-Installation	30	Anschlusskabel	21
Hinweis-Symbole	5	LANCOM Enhanced Passphrase Security	83
I		LANCOM Online Dokumentation	32
ICMP	91	LANCOM-Setup	31
IEEE 802.11n	14	LANconfig	32, 35
IETF	11	Assistenten aufrufen	96
Installation	21	LAN-LAN-Kopplung	18, 97
Konfigurations-Schnittstelle	30	erforderliche Angaben	97
LAN	30	LANmonitor	32, 61, 79
LANtools	31	Access Point trennen	80
Netzteil	30	Neuer Access Point zu Profil zuordnen	80
Internet-Anbieter	94	LANtools	
Internet-Zugang	18, 94	Systemvoraussetzungen	22
Authentifizierungsdaten	94	Layer-3-Roaming	14
Flatrate	95	LCD-Display	27
IP		LED	
Filter	91	Lost-AP	25
Ports sperren	91	New-AP	25
IP-Adresse	30, 34, 35, 91	WLAN	24
IP-Masquerading	19, 91	LED-Anzeigen – siehe Statusanzeigen	
IP-Router	19	LEPS	84, 92

■ Index

Lieferumfang	21	R	
Load-Balancing	74	RADIUS	3, 12, 18, 77, 85
Loader	22	RAM	54
Local-Mac	13	Remote-Access-Service (RAS)	
Lost AP-LED	25	Benutzername	106
Lost-AP-LED	61, 63	einrichten	105
M		Einwahl-Rechner konfigurieren	107
MAC-Adressfilter	19	NetBIOS	107
MAC-Filter	77	Server	18
MAC-Funktionen	11	TCP/IP	106
MAC-Prüfung	46	Windows-Arbeitsgruppe suchen	107
Managed-Modus	22	Remote-MAC	12
Management-VLAN-ID	56	Reset-Schalter	28
Multimode	41	Reset-Taster	29
N		Routing-Tabelle	91
NAT – siehe IP-Masquerading		S	
NetBIOS	100	SCEP	15, 44
Network Time Protocol	44	SCEP-Status	27
Netzmaske	34, 35, 91	SDSL-Modem	19
Netzschalter	28	Sekundäre Controller	72
Netzwerkkopplung	97	Sicherheit	
Sicherheitsaspekte	97, 105	Internet-Zugriff	83
Netzwerkname	46	Schutz der Konfiguration	83
Netzwerksegment	30	Sicherheits-Checkliste	89
Neuer Access Point	48	Simple Certificate Encryption Protocol	16,
New AP-LED	25	44	
NTP	44	SIP-Telefon	14
P		Skalierbarkeit	13
P2P	84	Smart Controller	3
PAT – siehe IP-Masquerading		Smart-Controller	11, 13
PCKS12-Container	66	SNMP	
PHY-Layer	11	Konfiguration schützen	90
Ping	102	SNTP-Status	27
PMK-Caching	18	Software-Installation	31
Point-to-Point	84	Speicherauslastung	27
Pre-Authentication	18	Split Management	3
Primäre Controller	72	Split-MAC	12
		Split-Management	17
		SSID	46, 53

Standard-Gateway	42	Verschlüsselung	18, 46, 58, 60, 97, 105
Stateful-Inspection-Firewall	88	Virtual Private Network (VPN)	18
Statusanzeigen	22	VLAN	3
Power	23	VLAN-ID	53, 75
Support	5	VPN-Client	107
SYSLOG	58	W	
Systemvoraussetzungen	21	WEBconfig	37
T		Aufruf eines Assistenten	39
TCP	91	Kennworteingabe	41
TCP/IP	22	Systemvoraussetzungen	22
Einstellungen	33, 40	WEP	83, 85, 86, 92
Verbindung testen	102	Windows-Arbeitsgruppen suchen	101
TCP/IP-Filter	19, 91	WLAN- Controller	3, 10
TCP/IP-Konfiguration		WLAN-LED	24, 44
automatisch	40	WLAN-Profil	50, 57
manuell	33, 35	WME	18
vollautomatisch	33, 34	WPA	83, 84, 85, 92
TCP/IP-Router		Z	
Einstellungen	99	Zeit	27
Telnet	91	Zeitinformation	43
Temperatur	27	Zero-Touch-Management	17
TFTP	91	Zertifikat	43, 44, 49, 61, 62, 65
TLS	11	Zertifikate	
U		Sichern	65
UDP	91	Zufallszahl	15, 44
V		Zugang zum Internet einrichten	94
Vererbung	18, 53, 55, 64		

