



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

LANCOM WLC-4006 LANCOM WLC-4025+ LANCOM WLC-4100

- Handbuch
- Manual

LANCOM WLC-4006
LANCOM WLC-4025+
LANCOM WLC-4100

© 2010 LANCOM Systems GmbH, Würselen (Germany). Alle Rechte vorbehalten.

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

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

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

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

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

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

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

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

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

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom.de

Würselen, Januar 2010

Ein Wort vorab

Vielen Dank für Ihr Vertrauen!

Die WLAN Controller LANCOM WLC-4006, LANCOM WLC-4025+ und LANCOM WLC-4100 sind moderne Hardware-Komponenten für ein ebenso einfaches wie sicheres Management mittlerer und großer 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
- Betriebssicherheit durch den autarken Weiterbetrieb
- 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

■ *Ein Wort vorab*

- Router, Firewall und VPN-Gateway integriert
- 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 'Sicherheitseinstellungen'.

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.

Bestandteile der Dokumentation

Die Dokumentation Ihres Gerätes besteht aus folgenden Teilen:

- Installation Guide
- Benutzerhandbuch
- Referenzhandbuch
- Menü-Referenz

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) unter www.lancom.de/download oder auf der beiliegenden 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)

Die Menü-Referenz (ebenfalls unter www.lancom.de/download oder auf der beiliegenden CD) beschreibt alle Parameter von LCOS, dem Betriebssystem der LANCOM-Geräte. Diese Beschreibung unterstützt den Anwender bei der Konfiguration der Geräte mit WEBconfig bzw. über die Konsole (Telnet).

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	Zentrales WLAN-Management	10
1.1	Einleitung	10
1.2	Technische Konzepte	11
1.2.1	Der CAPWAP-Standard	11
1.2.2	Die Smart-Controller-Technologie	11
1.2.3	Kommunikation zwischen Access Point und WLAN Controller	13
1.2.4	Zero-Touch-Management	16
1.2.5	Split-Management	16
1.3	Was kann Ihr LANCOM WLAN Controller?	17
2	Installation	20
2.1	Lieferumfang	20
2.2	Systemvoraussetzungen	20
2.2.1	Konfiguration der LANCOM-Geräte	20
2.2.2	Betrieb der Access Points im Managed-Modus	21
2.3	Statusanzeigen und Schnittstellen	21
2.3.1	Statusanzeigen	22
2.3.2	Schnittstellen	26
2.4	Installation der Hardware	29
2.5	Installation der Software	30
2.5.1	Software-Setup starten	30
2.5.2	Welche Software installieren?	31
3	Grundkonfiguration	32
3.1	Welche Angaben sind notwendig?	32
3.1.1	TCP/IP-Einstellungen	32
3.1.2	Konfigurationsschutz	34
3.2	Anleitung für LANconfig	35
3.3	Anleitung für WEBconfig	36
3.4	TCP/IP-Einstellungen der Access Points	41
3.5	TCP/IP-Einstellungen an den Arbeitsplatz-PCs	41

4 Konfiguration des WLAN Controllers	43
4.1 Grundkonfiguration der LANCOM WLAN Controller	43
4.1.1 Zeitinformation für den LANCOM WLAN Controller ein- stellen	43
4.1.2 Default-Konfiguration erstellen	44
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	51
4.2.3 Access Point Konfiguration	59
4.2.4 AP-Update	66
4.2.5 Stationen	72
4.2.6 RADIUS-Server	75
4.2.7 Optionen für den WLAN Controller	76
4.2.8 Vererbung von Parametern	78
4.3 Konkrete Konfigurationsbeispiele	80
4.3.1 Neue Access Points manuell in die WLAN-Struktur auf- nehmen	80
4.3.2 Access Point deaktivieren oder dauerhaft aus der WLAN- Struktur entfernen	83
4.3.3 Sicherung der Zertifikate	84
4.3.4 Sichern und Wiederherstellen weiterer Dateien der SCEP- CA	86
4.3.5 Backup von LANCOM WLAN Controllern	88
4.3.6 Load-Balancing zwischen den WLAN Controllern	91
4.3.7 Dynamische VLAN-Zuweisung	92
4.3.8 Virtualisierung und Gastzugang über LANCOM WLAN Controller	95
4.3.9 Prüfung der WLAN-Clients über RADIUS (MAC-Filter)	108
4.3.10 Interner und externer RADIUS-Server kombiniert	109
4.4 Anzeigen und Aktionen im LANmonitor	113
4.5 Automatische Funkfeldoptimierung mit LANCOM WLAN Controllern	115
4.6 Konfiguration der Access Points	117

5 Sicherheits-Einstellungen	119
5.1 Sicherheit im Funk-LAN	119
5.1.1 Verschlüsselung des Datentransfers	119
5.1.2 802.1x / EAP	120
5.1.3 LANCOM Enhanced Passphrase Security	120
5.1.4 Zugangskontrolle über MAC-Adresse	121
5.1.5 IPSec-over-WLAN	121
5.2 Tipps für den richtigen Umgang mit Schlüsseln und Passphrasen	121
5.3 Der Sicherheits-Assistent	122
5.3.1 Assistent für LANconfig	123
5.3.2 Assistent für WEBconfig	123
5.4 Die Sicherheits-Checkliste	124
6 Den Internet-Zugang einrichten	128
6.1 Der Internet-Assistent	128
6.1.1 Anleitung für LANconfig	128
6.1.2 Anleitung für WEBconfig	129
7 Zwei Netzwerke verbinden	130
7.1 Welche Angaben sind notwendig?	130
7.1.1 Allgemeine Angaben	131
7.1.2 Einstellungen für den TCP/IP-Router	132
7.1.3 Einstellungen für NetBIOS-Routing	133
7.2 Anleitung für LANconfig	134
7.3 1-Click-VPN für Netzwerke (Site-to-Site)	135
7.4 Anleitung für WEBconfig	136

8 Einwahl-Zugang bereitstellen	138
8.1 Welche Angaben sind notwendig?	138
8.1.1 Allgemeine Angaben	138
8.1.2 Einstellungen für TCP/IP	139
8.1.3 Einstellungen für NetBIOS-Routing	140
8.2 Einstellungen am Einwahl-Rechner	140
8.3 Anleitung für LANconfig	141
8.4 1-Click-VPN für LANCOM Advanced VPN Client	141
8.5 Anleitung für WEBconfig	143
9 Anhang	144
9.1 Leistungs- und Kenndaten	144
9.2 Anschlussbelegung	145
9.2.1 Ethernet-Schnittstelle 10/100/1000Base-TX, DSL-Schnittstelle	145
9.2.2 Konfigurationsschnittstelle (Outband)	145
9.3 CE-Konformitätserklärungen	146
10 Index	147

1 Zentrales WLAN-Management

1.1 Einleitung

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. Evtl. werden auch einige Access Points bei den Aktualisierungen ausgelassen, die Konfigurationen sind dann nicht mehr konsistent.
- 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 optional **nicht** im Flash, sondern im RAM abgelegt wird, können in

besonders sicherheitskritischen Netzen bei einem Diebstahl der Geräte auch keine sicherheitsrelevanten Daten in unbefugte Hände geraten. Nur im „autarken Weiterbetrieb“ wird die Konfiguration für eine definierte Zeit optional im Flash gespeichert (in einem Bereich, der nicht mit LANconfig oder anderen Tools auszulesen ist).

1.2 Technische Konzepte

1.2.1 Der CAPWAP-Standard

Mit dem CAPWAP-Protokoll (Control And Provisioning of Wireless Access Points) hat die IETF (Internet Engineering Task Force) im März 2009 einen Standard für das zentrale Management großer WLAN-Strukturen verabschiedet.

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 verbindungslose, ungesicherte 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.

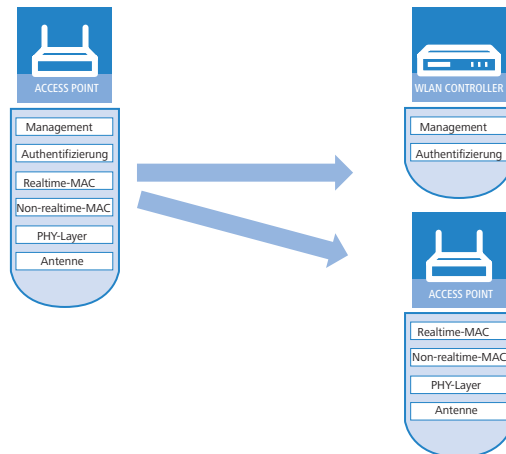
1.2.2 Die Smart-Controller-Technologie

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

Die Smart-Controller-Technologie von LANCOM Systems setzt das Local-MAC-Verfahren ein. Dieses Verfahren 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.



Durch die Reduzierung der zentralisierten Aufgaben bieten die WLAN-Strukturen eine optimale Skalierbarkeit. Gleichzeitig wird der WLAN Controller, der große Teile des gesamten Datenverkehrs verarbeiten muss, in einer solchen Struktur nicht zum zentralen Flaschenhals. 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 früheren

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“ – über die Subnetzgrenzen im Ethernet hinweg.
- 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.

1.2.3 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 1811n Wireless) bzgl. der Einstellung der WLAN-Module im Auslieferungszustand. In den folgenden Beschreibungen wird meistens der übergreifende Begriff „Access Point“ verwendet.

Für eine erfolgreiche Inbetriebnahme der Access Points müssen folgende Voraussetzungen erfüllt sein:

- Der Access Point verfügt über eine IP-Adresse (statisch oder über DHCP zugewiesen)
- Der Access Point kann einen WLAN Controller im LAN über einen Broadcast erreichen
- Alternativ: Der Access Point kann die Adresse eines WLAN Controllers im WAN über einen DNS-Server auflösen (die „WLC-Address“ wird ggf. über „company.intern“ aufgelöst).
- Für einen über WAN erreichbaren WLAN Controller wird in der Firewall die Kommunikation für DNS, CAPWAP auf UDP Port 1027 sowie HTTP für SCEP erlaubt.

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'). Der Access Point sucht für das oder die entsprechenden WLAN-Module im Netz 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 Netz 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. Gleiches gilt auch für die über DHCP gelernten DNS-Suffixe: ein DNS-Server kann so den Standardnamen des Controllers automatisch zu 'WLC-Address.company.intern' ergänzen. Somit können auch WLAN Controller erreicht werden, die nicht im gleichen Netz stehen, ohne die Access Points konfigurieren zu müssen.

Bitte beachten Sie, dass die Access Points über eine IP-Adresse verfügen müssen, um mit dem WLAN Controller in Kontakt zu treten. Die IP-Adresse kann entweder fest im Access Point eingetragen sein oder über einen DHCP-Server zugewiesen werden.



Wenn der Access Point die IP-Adresse von einem DHCP-Server bezieht und dieser DHCP-Server nicht erreichbar ist, hat der Access Point nach einem Neustart evtl. keine IP-Adresse mehr und kann nicht mit dem WLAN Controller kommunizieren.

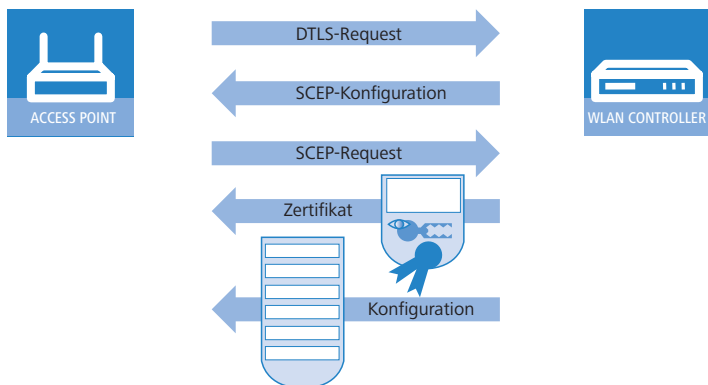
Aus den verfügbaren WLAN Controllern wählt der Access Point den Besten aus und fragt bei diesem nach dem Aufbau der DTLS-Verbindung an. Der „beste“ WLAN Controller ist für den Access Point derjenige mit der geringsten Auslastung, also dem kleinsten Verhältnis von gemanagten Access Points zu den maximal 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.

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 Enrollment Protocol, CA für Certification Authority.

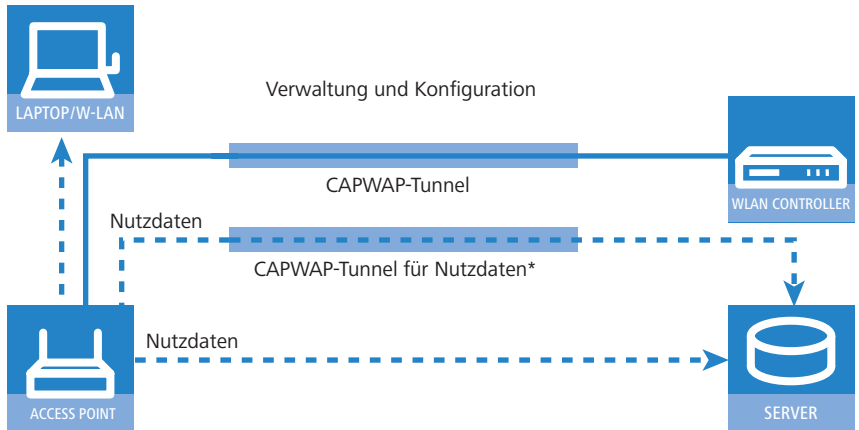
Der WLAN Controller ermittelt daraufhin mit einer internen Zufallszahl einen eindeutigen und sicheren Sitzungsschlüssel, mit dem er die Verbindung zum Access Point schützt. Die CA im WLAN Controller stellt dem Access Point ein Zertifikat mittels SCEP aus. Der Bezug des Zertifikats ist mit einem Kennwort für einmalige Verwendung als „Challenge“ gesichert, der Access Point kann sich mit diesem Zertifikat gegenüber dem WLAN Controller für die Abholung des Zertifikats authentifizieren.



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.



* wird in einer späteren Version bereitgestellt

1.2.4 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.

1.2.5 Split-Management

LANCOM Access Points können ihren WLAN Controller 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.

1.3 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+	LANCOM WLC- 4100
WLAN-Controlling			
Anzahl gemanagter Geräte (Auslieferungszustand / optional erweiterbar auf Maximalwert)	6 / 12	25 / 100	100 / 1000
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	64 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	✓	✓	✓

	LANCOM WLC- 4006	LANCOM WLC- 4025+	LANCOM WLC- 4100
Fast Roaming über PMK-Caching und Pre-Authentication	✓	✓	✓
Weitere Anwendungen			
Internet-Zugang	✓	✓	✓
LAN-LAN-Kopplung über VPN	✓	✓	✓
RAS-Server (über VPN)	✓	✓	✓
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	✓	✓	✓
Spanning-Tree-Protokoll	✓	✓	✓
802.1p	✓	✓	✓
LAN-Anschluss			
Uplink-Interface zum Anschluss an das LAN. Alternativ schaltbar als LAN-Interface oder als WAN-Interface zum Anschluss eines SDSL-Modems.	1		
Individuelle Gigabit Ethernet LAN Ports, Auto-Crossover, einzeln schaltbar, z. B. als LAN- oder DMZ-Ports. Alternativ schaltbar als WAN-Interface zum Anschluss eines externen DSL-Modems/Routers.	4	4	4
USB-Anschluss			
USB 2.0 Host Port (Highspeed: 480Mbit/s) zum Anschluss eines USB-Druckers und für zukünftige Erweiterungen	✓	✓	✓
Sicherheitsfunktionen			
5 integrierte VPN-Tunnel zur Absicherung von Netzwerkverbindungen	✓	✓	✓
DTLS- und IPsec-Verschlüsselung über Hardware	✓	✓	✓

	LANCOM WLC- 4006	LANCOM WLC- 4025+	LANCOM WLC- 4100
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	✓	✓	✓
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 WLC-PSPOT Option für die Einrichtung von Gastzugängen und kostenpflichtigen WLAN-Zugängen auf den verwalteten Access Points	integriert	✓	✓
LANCOM 2-Year Warranty Extension	✓	✓	✓
LANCOM Next Business Day Service Extension	✓	✓	✓

2 Installation

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

2.1 Lieferumfang

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

	LANCOM WLC-4006	LANCOM WLC-4025+	LANCOM WLC-4100
Kaltgerätekabel		✓	✓
Netzteil	✓		
CAT5-LAN-Anschlusskabel (grüne Stecker)	✓	✓	✓
RS232-Anschlusskabel für die Konfigurationsschnittstelle	✓	✓	✓
GummifüÙe, 19"-Montagewinkel		✓	✓
LANCOM-CD	✓	✓	✓
Gedruckter Installation Guide	✓	✓	✓
Gedrucktes Benutzerhandbuch	✓	✓	✓
LANCOM Configuration Service Ticket	✓	✓	✓

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

2.2 Systemvoraussetzungen

2.2.1 Konfiguration der LANCOM-Geräte

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

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



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

2.2.2 Betrieb der Access Points im Managed-Modus

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



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

2.3 Statusanzeigen und Schnittstellen

Bedeutung der LEDs

In den folgenden Abschnitten wird das Verhalten der LEDs beschrieben.



Bitte beachten Sie, dass der LANmonitor über die Anzeige der LEDs hinaus weitere wichtige Informationen über den Status der Geräte anzeigt '→ LANCOM mit LANmonitor überwachen'.

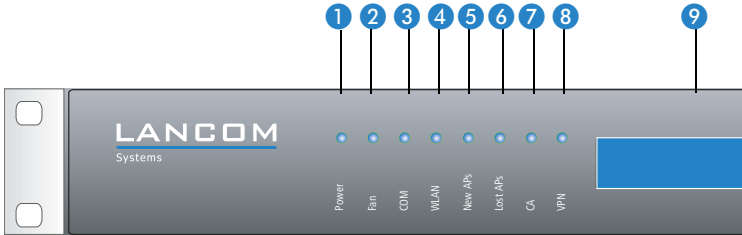
In den folgenden Abschnitten verwenden wir verschiedene Begriffe, um das Verhalten der LEDs zu beschreiben:

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

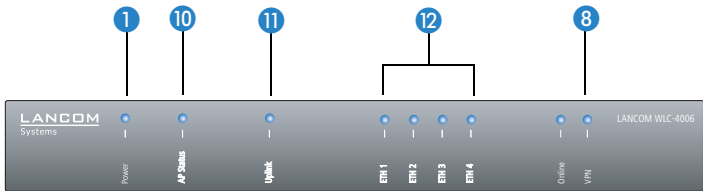
2.3.1 Statusanzeigen

Die LANCOM WLAN Controller verfügen über folgende Statusanzeigen:

LANCOM WLC-4025+
LANCOM WLC-4100

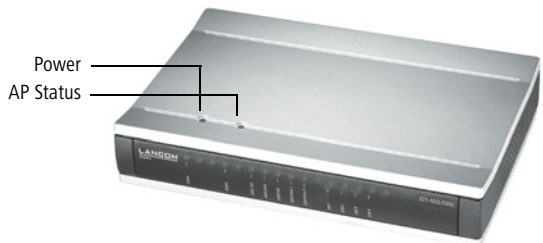


LANCOM WLC-4006



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.



1 Power

Diese LED gibt Auskunft über die Betriebsbereitschaft des Geräts.

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 Fan

Die Fan-LED zeigt den Status des Lüfters an:

grün	dauerhaft an	CPU-Temperatur OK
orange	dauerhaft an	CPU-Temperatur > 55°
rot	blinkend	Hardwarefehler des Lüfters oder CPU-Temperatur > 60°, zusätzlich akustisches Signal

Um Schäden an der Hardware zu vermeiden, wird diese LED mit einem akustischen Signal unterstützt: Wenn der Lüfter blockiert oder die Temperatur der CPU über 60° steigt, wird ein pulsierendes akustisches Signal ausgegeben.

3 COM

Verbindungszustand der seriellen Konfigurationsschnittstelle:

aus		keine Sitzung eingebucht
grün	dauerhaft an	seriell eingebuchte Konfigurationssitzung
orange	flackernd	Datenübertragung während der Konfigurationssitzung

■ Kapitel 2: Installation

4 WLAN

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
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.

5 New APs

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

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

6 Lost APs

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

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

7 CA

Status der internen CA.

aus		CA aus
grün	dauerhaft an	CA an und bereit
rot	dauerhaft an	CA an, ein Fehler ist aufgetreten
orange	dauerhaft an	CA an und bereit, eine Anfrage steht an (Request pending)

8 VPN

Status einer VPN-Verbindung.

aus		kein VPN-Tunnel aufgebaut
grün	blinkend	Verbindungsaufbau

grün	blitzend	erste Verbindung
grün	invers blitzend	weitere Verbindungen
grün	dauerhaft an	VPN-Tunnel sind aufgebaut

9 LCD-Display

Das LCD-Display zeigt in zwei Zeilen mit je 16 Zeichen folgende Informationen umlaufend im Wechsel an:

- ▶ Gerätename
- ▶ Firmwareversion
- ▶ Geräte-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:

- ▶ SNTP-Status
- ▶ SCEP-Status

10 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.

11 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	
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.	

12 ETH

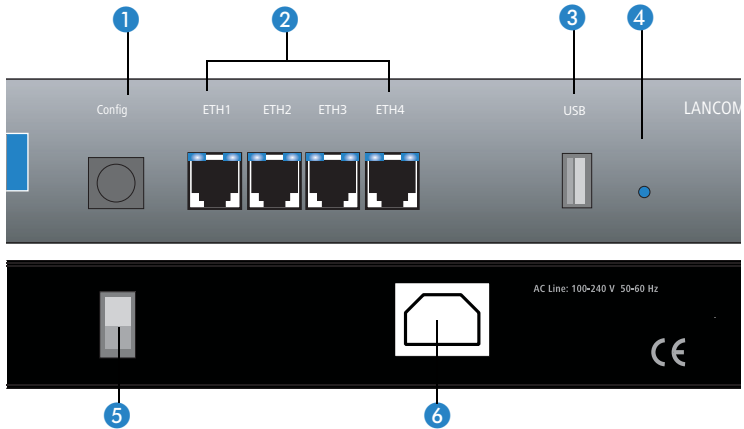
Zustand der LAN-Anschlüsse im integrierten Switch:

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

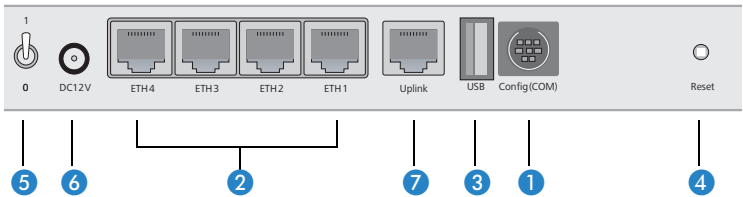
2.3.2 Schnittstellen

Die LANCOM WLAN Controller verfügen über folgende Schnittstellen:

LANCOM WLC-4025+
LANCOM WLC-4100



LANCOM WLC-4006



- 1 COM
- 2 ETH 1 bis 4

Anschluss für das serielle Konfigurationskabel.

Ethernet-Buchsen (10/100/1000Base-Tx) für den Anschluss an das LAN. Unterstützt werden 10-Mbit, 100-Mbit und Gigabit-Anschlüsse. Die verwendete Übertragungsgeschwindigkeit wird automatisch erkannt (Autosensing). Jede Ethernetbuchse verfügt über zwei LEDs (grün und gelb):

grün	aus	kein Netzwerkgerät angeschlossen
grün	dauerhaft an	Verbindung zu Netzwerkgerät betriebsbereit, kein Datenverkehr
grün	flackernd	Datenverkehr
gelb	aus	1000 MBit/s
gelb	dauerhaft an	10/100 MBit/s

- 3 USB

USB-Anschluss (USB Host)

■ Kapitel 2: Installation

- 4 Reset Reset-Taster (siehe 'Die Funktion des Reset-Tasters')
- 5 Ein/
Ausschalter Schalter zur Trennung des Gerätes vom Stromnetz.



Bitte beachten Sie folgenden Hinweis:

Zur vollständigen Trennung vom Netz ziehen Sie bitte immer den Netzstecker aus der Steckdose!

- 6 Netzanschluss Anschluss für Kaltgerätekabel zur Stromversorgung (LANCOM WLC-4025+, LANCOM WLC-4100), Anschluss für das Netzteil (LANCOM WLC-4006)
- 7 Uplink Uplink-Anschluss

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 über WEBconfig (LCOS-Menübaum ► Setup ► Config) kann das Verhalten des Reset-Tasters gesteuert werden:

■ 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.



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') ihre Konfiguration.



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

- Reset-oder-Booten (Standardeinstellung): Ein kurzer Druck auf den Taster führt zum Neustart, ein Druck von 5 Sekunden oder länger führt zum Neustart mit dem Zurücksetzen der Konfiguration auf den Auslieferungszustand.

Alle LEDs am Gerät leuchten dauerhaft auf.

Sobald der Taster freigegeben wird, startet das Gerät mit Werkseinstellungen neu.



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

2.4 Installation der Hardware

Die Installation des LANCOM WLAN Controller erfolgt in folgenden Schritten:

LANCOM WLC-4025+
LANCOM WLC-4100

- ① **Montage** – montieren Sie das Gerät in einem freien 19"-Einschub in einem entsprechenden Serverschrank. Bringen Sie ggf. die Gummifüße auf der Unterseite des Gerätes an, um Kratzer auf den Oberflächen anderer Geräte zu vermeiden.

LANCOM WLC-4025+
LANCOM WLC-4100

- ② **LAN** – schließen Sie Ihren LANCOM WLAN Controller zunächst ans LAN an. Stecken Sie das mitgelieferte Netzwerkkabel (grüne Stecker) einerseits in einen Ethernet-Port des Geräts ② und andererseits in eine freie Netzwerkanschlussdose Ihres lokalen Netzes.

LANCOM WLC-4006

- 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 ⑦ und andererseits in eine freie Netz-

werkanschlussdose Ihres lokalen Netzes, eine freie Buchse oder eines Switches.

Die Ethernet-Ports erkennen sowohl die Übertragungsrate (10/100/1000 Mbit) als auch den Typ (Node/Hub) angeschlossener Netzwerkgeräte automatisch (Autosensing). Der parallele Anschluss von Geräten unterschiedlicher Geschwindigkeit und Typen ist möglich.

- ③ **Weitere Netzwerkgeräte** – optional können Sie an die LAN-Schnittstellen ② weitere Netzwerkgeräte anschließen.
- ④ **Konfigurations-Schnittstelle** – optional können Sie das Gerät direkt an die serielle Schnittstelle (RS-232, V.24) eines PCs anschließen. Verwenden Sie dazu das mitgelieferte Anschlusskabel. Verbinden Sie die Konfigurations-Schnittstelle des LANCOM ① mit einer freien seriellen Schnittstelle des PCs.
- ⑤ **Mit Spannung versorgen und einschalten** – versorgen Sie das Gerät über den Netzanschluss mit Spannung ⑥ und schalten Sie es am Schalter ⑤ auf der Rückseite ein.

2.5 Installation der Software

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



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

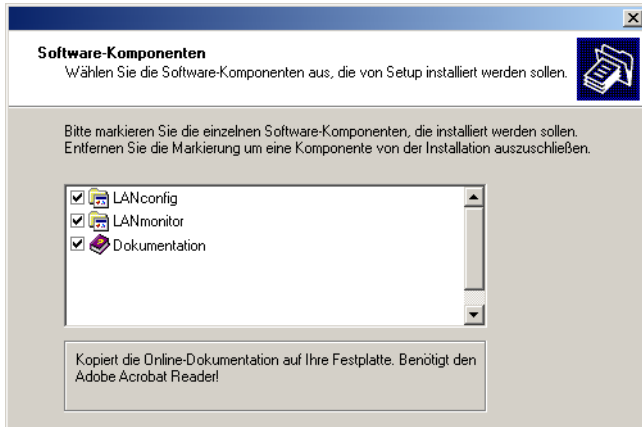
2.5.1 Software-Setup starten

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



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

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



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** überwachen Sie auf einem Windows-Rechner alle LANCOM-Geräte.
- Der **WLANmonitor** erlaubt die Beobachtung und Überwachung der WLAN-Netze. WLAN-Controller, Access Points und die mit den Access Points verbundenen Clients werden angezeigt, auch nicht authentifizierte Access Points und Clients können angezeigt werden (Rogue AP Detection und Rogue Client Detection).
- Mit **Dokumentation** kopieren Sie die Dokumentationsdateien auf Ihren PC.

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

3 Grundkonfiguration

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

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

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

Zum Abschluss dieses Kapitels zeigen wir Ihnen, welche Einstellungen an den Arbeitsplatzrechnern im LAN notwendig sind, damit der Zugriff auf das Gerät 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 Sie die IP-Adresse für den Router selbst festlegen möchten (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).

Notwendige Angaben für die manuelle TCP/IP-Konfiguration

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

- **DHCP-Betriebsart**
 - Aus: Die erforderlichen IP-Adressen müssen manuell eingetragen werden.

- Server: Der WLAN Controller arbeitet als DHCP-Server im Netzwerk, zumindest die eigene IP-Adresse und die Netzmaske müssen angegeben werden.
- Client: Der WLAN Controller bezieht als DHCP-Client die Adress-Informationen von einem anderen DHCP-Server, es müssen keine Adress-Informationen angegeben werden.

■ IP-Adresse und Netzwerkmaste für den WLAN Controller

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

■ Gateway-Adresse

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

■ DNS-Server

Geben Sie die IP-Adresse eines DNS-Servers zur Auflösung der Domain-Namen an, wenn Sie die DHCP-Betriebsart 'Aus' gewählt haben oder in der DHCP-Betriebsart 'Server' ein anderes Netzwerkgerät die Aufgabe des DNS-Servers übernimmt.

3.1.2 Konfigurationsschutz

Mit dem Kennwort schützen Sie den Konfigurationszugang zum 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.



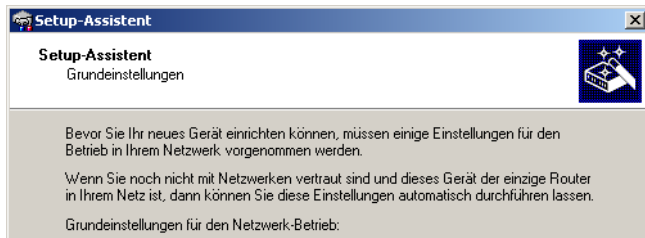
In der Konfiguration des LANCOM können mehrere Administratoren angelegt werden, die über unterschiedliche Zugriffsrechte verfügen. Für einen WLAN Controller können bis zu 16 verschiedene Administratoren eingerichtet werden. Weitere Informationen finden Sie im LCOS-Referenzhandbuch unter „Rechteverwaltung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




- ③  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 oder ein DHCP-Server im Netz aktiv ist.

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

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

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

- ③  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.

Solange kein Hauptgerätepasswort gesetzt ist blinkt die Power-LED und es ist keine WAN-Konfiguration möglich, auch wenn die WAN-Konfiguration eigentlich aktiviert ist!

- ⑤ Der Gebührenschatz beschränkt auf Wunsch die Kosten von WAN-Verbindungen auf ein festgesetztes Maß. Bestätigen Sie Ihre Angaben mit **Weiter**.
- ⑥ Schließen Sie die Konfiguration mit **Fertig stellen** ab.



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

3.3 Anleitung für WEBconfig

Sie können die Einstellungen des Gerätes über einen beliebigen Webbrowser vornehmen. Im LANCOM ist die Konfigurationssoftware WEBconfig integriert. Sie benötigen lediglich einen Webbrowser, um auf WEBconfig zuzugreifen. WEBconfig bietet ähnliche Setup-Assistenten wie LANconfig an und bietet damit optimale Voraussetzungen für eine komfortable Konfiguration des LANCOM – im Unterschied zu LANconfig aber unter allen Betriebssystemen, für die es einen Webbrowser gibt.

Sicher mit HTTPS

WEBconfig bietet zur sicheren (Fern-) Konfiguration die Möglichkeit der verschlüsselten Übertragung der Konfigurationsdaten über HTTPS.

`https://<IP-Adresse oder Gerätename>`



Für maximale Sicherheit sollten Sie stets die neueste Version Ihres Browsers verwenden.

Zugang zum Gerät mit WEBconfig

Für die Konfiguration mit WEBconfig müssen Sie wissen, wie sich das Gerät 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. Der Zugriff mit WEBconfig erfolgt entweder über die IP-Adresse des LANCOM, über den Namen des Gerätes (sofern bereits zugewiesen) bzw. sogar über einen beliebigen Namen, falls das Gerät noch nicht konfiguriert wurde und sich selbst als DNS Server zugewiesen hat.

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 bzw. eine vorgegebene IP-Adresse fest zugewiesen.

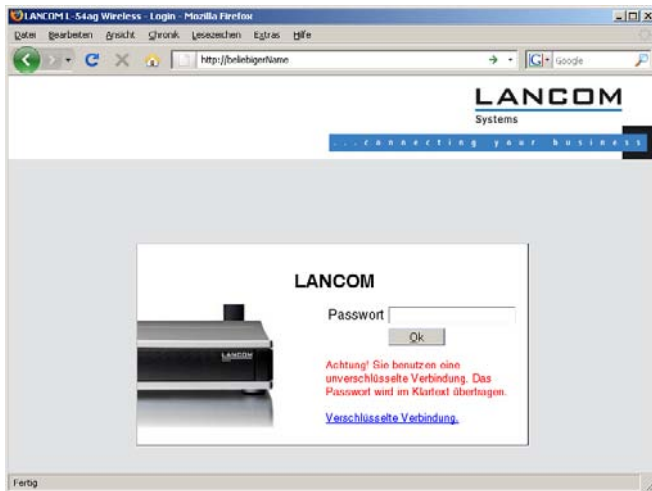
Netz ohne DHCP-Server

Nicht für zentral
verwaltete
LANCOM Wireless
Router oder
LANCOM Access
Points

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



Im werksseitigen Auslieferungszustand mit aktiviertem DHCP-Server leitet das Gerät alle eingehenden DNS-Anfragen an den internen Webserver weiter. Dadurch können unkonfigurierte LANCOMs einfach durch Eingabe eines beliebigen Names mittels eines Webbrowsers angesprochen und in Betrieb genommen werden.



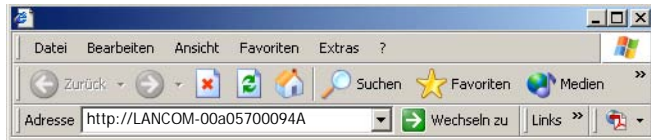
Falls der Konfigurations-Rechner seine IP-Adresse nicht vom LANCOM-DHCP-Server bezieht, ermitteln Sie die aktuelle IP-Adresse des Rechners (mit **Start ▶ Ausführen ▶ cmd** und dem Befehl **ipconfig** an der Eingabeaufforderung unter Windows 2000, Windows XP oder Windows Vista, mit **Start ▶ Ausführen ▶ 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 Gerätes 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:
 - Sie nutzen die Funktion "Geräte suchen" in LANconfig oder die Gerätesuche unter WEBconfig von einem anderen erreichbaren LANCOM.
 - Die per DHCP an das LANCOM-Gerät zugewiesene IP-Adresse über geeignete Tools ausfindig machen und das Gerät mit dieser IP-Adresse direkt erreichen.
 - Einen Rechner mit Terminalprogramm über die serielle Konfigurationsschnittstelle an das Gerät anschließen.

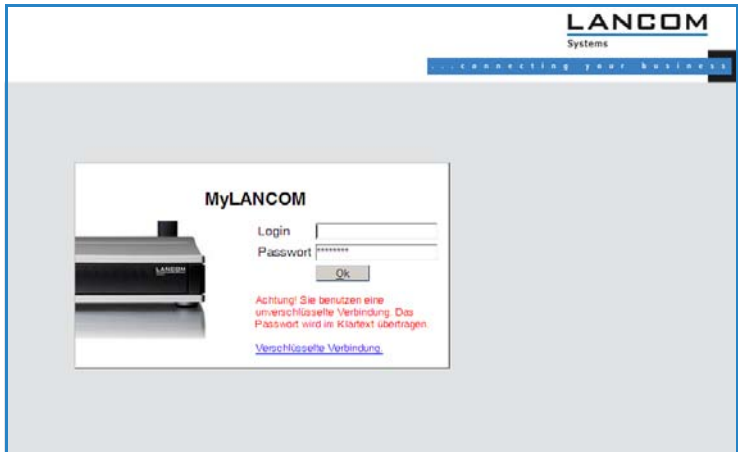
Login

Wenn Sie beim Zugriff auf das Gerät 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.

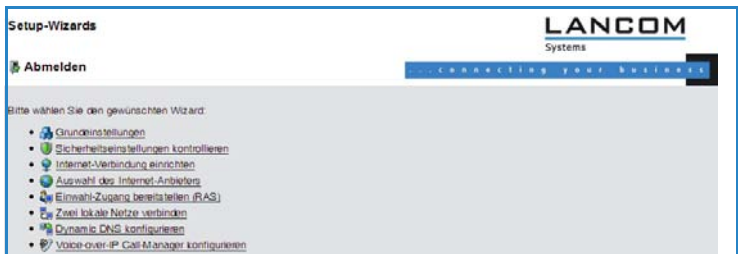


Der Login-Dialog bietet alternativ einen Link für eine verschlüsselte Verbindung über HTTPS. Nutzen Sie nach Möglichkeit immer die HTTPS-Verbindung mit erhöhter Sicherheit.



Setup Wizards

Mit den Setup-Wizards können Sie schnell und komfortabel die häufigsten Einstellungen für ein Gerät vornehmen. Wählen Sie dazu den gewünschten Assistenten aus und geben Sie auf den folgenden Seiten die benötigten Daten ein.



Die Einstellungen werden erst dann in das Gerät gespeichert, wenn Sie die Eingaben auf der letzten Seite des Assistenten bestätigen.

3.4 TCP/IP-Einstellungen der Access Points

Bitte beachten Sie, dass die Access Points über ein IP-Adresse verfügen müssen, um mit dem WLAN Controller in Kontakt zu treten. Die IP-Adresse kann entweder fest im Access Point eingetragen sein oder über einen DHCP-Server zugewiesen werden.



Wenn der Access Point die IP-Adresse von einem DHCP-Server bezieht und dieser DHCP-Server nicht erreichbar ist, hat der Access Point nach einem Neustart evtl. keine IP-Adresse mehr und kann nicht mit dem WLAN Controller kommunizieren.

3.5 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 ein LANCOM

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

■ IP-Adressvergabe über einen separaten DHCP-Server

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

LAN als Standard-Gateway übermittelt. Außerdem sollte der DHCP-Server den LANCOM als DNS-Server angeben.

■ **Manuelle Zuweisung der IP-Adressen**

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



Weitere Informationen und Hilfe zu den TCP/IP-Einstellungen Ihres 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-315agn dual, L-310agn, L-305agn, 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 117.

4.1 Grundkonfiguration 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.
- Ein WLAN-Profil, welches der WLAN Controller den Access Points zuweisen kann.

Weiterführende, optionale Konfigurationsbeispiele schließen das Einrichten von redundanten WLAN-Controllern, das manuelle Trennen und Verbinden von Access-Points sowie das Durchführen eines Backups der notwendigen Zertifikate ein.

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 Enrollment 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 im Bereich 'Extras' den Link 'Datum und Uhrzeit einstellen'.



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.

Für die Modelle vom Typ LANCOM WLC-4006 **muß** die Zeitinformation von einem Zeit-Server bezogen werden, da die Geräte nicht über eine batteriegepufferte Echtzeituhr verfügen.

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



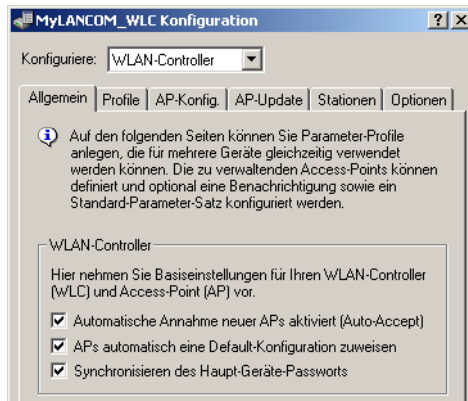
Nach Herstellung der Betriebsbereitschaft sollten Sie eine Sicherung der Zertifikate anlegen ('Sicherung der Zertifikate' → Seite 84).

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 117), zeigt der WLAN Controller diese nach einer kurzen Zeit als „Neue Access Points“ an, die New-APs-LED blinkt entsprechend orange. Im LANmonitor und im Display des Gerätes 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, welche den suchenden Access Points zugewiesen werden kann.

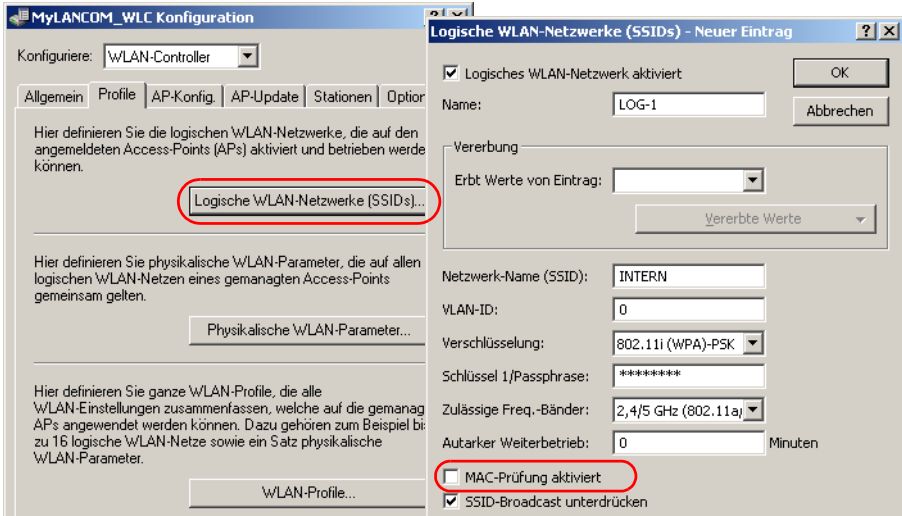
- ① Öffnen Sie die Konfiguration des WLAN Controllers durch einen Doppelklick auf den entsprechenden Eintrag in LANconfig.
- ② Aktivieren Sie im Konfigurationsbereich 'WLAN Controller' auf der Registerkarte 'Allgemein' die Optionen für die automatische Annahme neuer Access Points sowie die Zuweisung 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 automatisch in die von ihm verwaltete WLAN-Struktur aufnehmen, z. B. temporär während der Rollout-Phase einer WLAN-Installation.

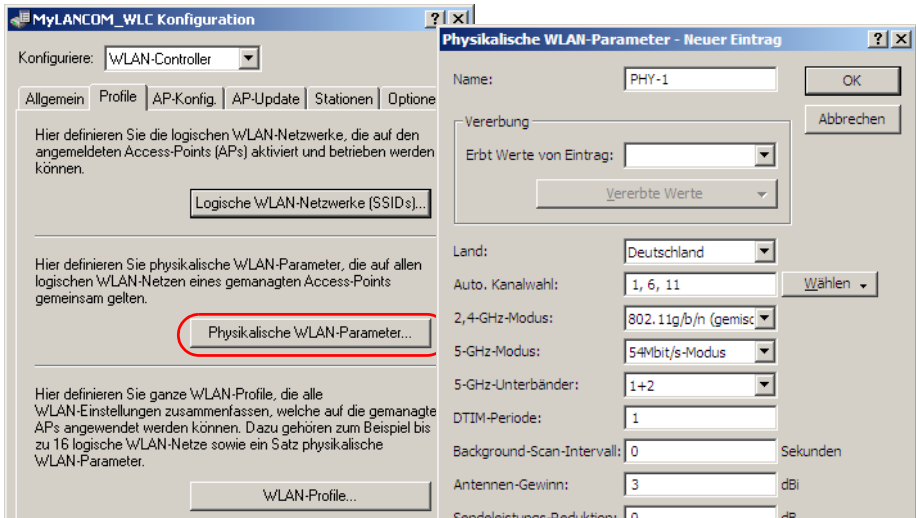
- ③ Wechseln Sie auf die Registerkarte 'Profile' in die logischen WLAN-Netzwerke. Erstellen Sie einen neuen Eintrag mit folgenden Werten:



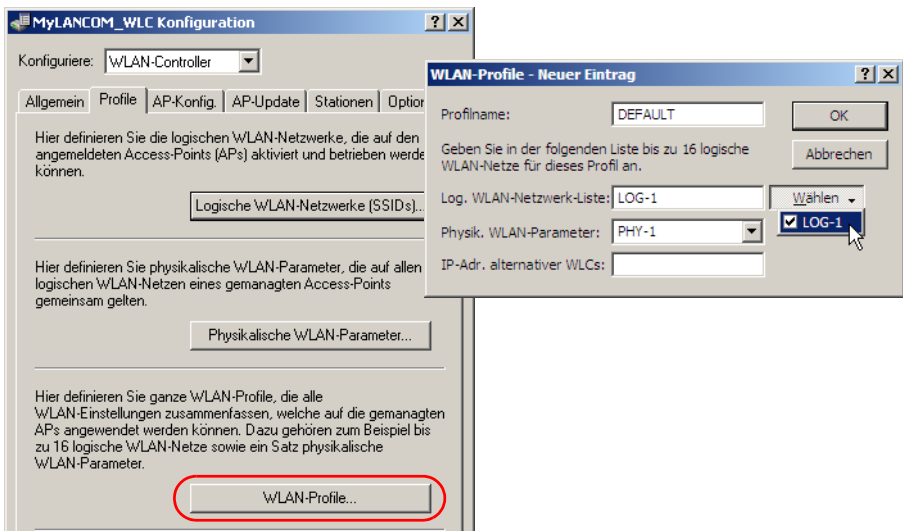
- Netzwerkname: Geben Sie dem WLAN einen Namen. Dieser Name wird nur für die Verwaltung im LANCOM WLAN Controller verwendet.
 - SSID: Mit dieser SSID verbinden sich die WLAN-Clients.
 - Verschlüsselung: Wählen Sie die Verschlüsselung passend zu den Möglichkeiten der verwendeten WLAN-Clients und geben 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 108.
- 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.



In normalen Access-Point-Anwendungen sollten Sie nur die 5-GHz-Unterbänder 1 und 2 verwenden. Das Unterband 3 steht nur für besondere Anwendungen zur Verfügung (z. B. BFWA – Broadband Fixed Wireless Access).



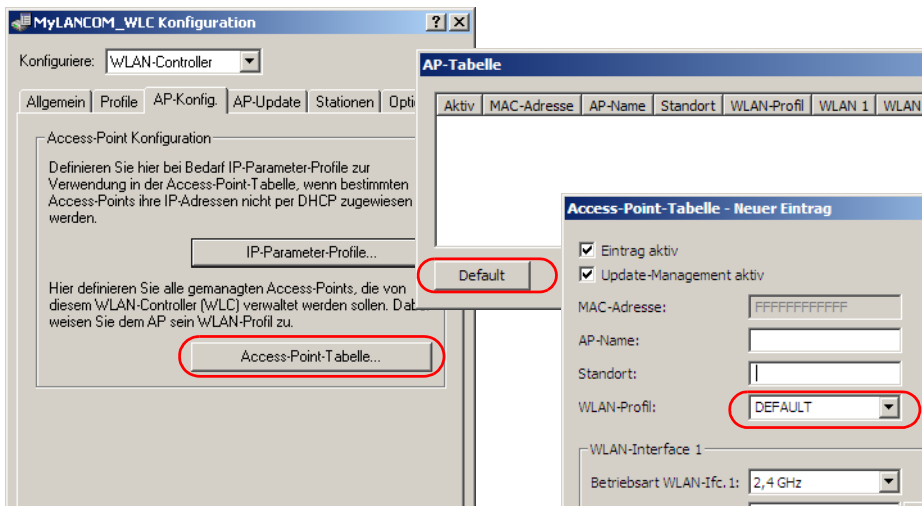
- ⑤ Erstellen Sie ein neues WLAN-Profil, geben Sie ihm einen eindeutigen Namen und weisen Sie ihm das eben erstellte logische WLAN-Netzwerk sowie die physikalischen WLAN-Parameter zu.



- ⑥ Wechseln Sie auf die Registerkarte 'AP-Konfig.' 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.



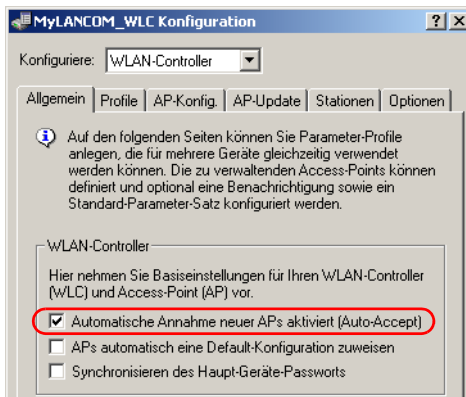
4.1.3 Zuweisung der Default-Konfiguration zu den neuen Access Points

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 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.

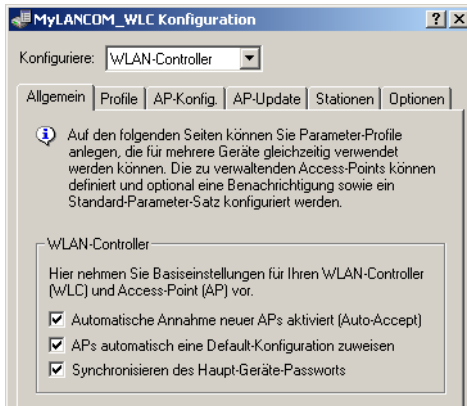


4.2 Erweiterte Einstellungen

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.



LANconfig: WLAN Controller ▶ Allgemein ▶ WLAN-Profile

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WLAN-Management

■ Automatische Annahme neuer APs (Auto-Accept)

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 eine Default-Konfiguration zuzuweisen, 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). Per Default aufgenommene Access Points werden auch in die MAC-Liste aufgenommen.



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 nur dann, wenn keine Access Points unkontrolliert mit dem LAN verbunden werden können 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.

■ Synchronisieren des Haupt-Geräte-Passworts

Bei Aktivierung dieser Funktion, wird das Haupt-Geräte-Passwort der Access-Points bei jeder Anmeldung gesetzt, um dies synchron zum Passwort des WLAN-Controllers zu halten.

Ist die Funktion deaktiviert, wird das Haupt-Geräte-Passwort nur dann gesetzt, wenn der Access-Point bei der Anmeldung kein Passwort gesetzt hat. Ein einmal gesetztes Passwort wird niemals überschrieben und wird bei Änderung des WLC-Passwortes von diesem abweichen.

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.

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:

Logische WLAN-Netzwerke (SSIDs) - Neuer Eintrag

Logisches WLAN-Netzwerk aktiviert OK

Name: Abbrechen

Vererbung

Erbt Werte von Eintrag:

Netzwerk-Name (SSID):

VLAN-ID:

Verschlüsselung:

Schlüssel 1/Passphrase:

Zulässige Freq.-Bänder:

Autarker Weiterbetrieb: Minuten

MAC-Prüfung aktiviert

SSID-Broadcast unterdrücken

WPA-Version:

WPA1 Sitzungsschl.-Typ:

WPA2 Sitzungsschl.-Typ:

Broadcastgeschwindigk.:

Client-Bridge-Unterst.:

Maximalzahl der Clients:

Lange Präambel bei 802.11n verwenden

802.11n

Anzahl Spatial-Streams:

Kurzes Guard-Intervall zulassen

Frame-Aggregation verwenden

LANconfig: WLAN Controller ▶ Profile ▶ Logische WLAN-Netzwerke

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WLAN-Management ▶ AP-Konfiguration ▶ Netzwerkprofile

■ Name

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

Mögliche Werte:

- Maximal 32 ASCII-Zeichen.

Default:

- leer

■ Vererbung

Auswahl eines schon definierten logischen WLAN-Netzwerks, von dem die Einstellungen übernommen werden sollen ('Vererbung von Parametern' → Seite 78).

■ Netzwerkname (SSID)

Stellen Sie für jedes logische WLAN-Netzwerk eine eindeutige SSID (den Netzwerknamen) ein. Nur solche WLAN-Clients, die über die gleiche SSID verfügen, können sich in diesem WLAN-Netzwerk anmelden.

Mögliche Werte:

- Maximal 32 ASCII-Zeichen.

Default:

- leer

■ VLAN-ID

VLAN-ID für dieses logische WLAN.

Mögliche Werte:

- 1 bis 4096

Default:

- 0

Besondere Werte:

- 1: logisches WLAN arbeitet ungetaggt (ohne VLAN-Tag).
- 2 bis 4096: logisches WLAN verwendet VLAN mit der angegebenen ID, sofern die Management-VLAN-ID ungleich 0 ist.



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! Mit der Definition einer VLAN-ID für ein WLAN-Profil wird dann auf den damit verwalteten Access Points automatisch das VLAN-Modul eingeschaltet.

■ 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 der Daten bei einem Diebstahl dar, da die sicherheitsrelevanten Parameter der Konfiguration nach Ablauf der eingestellten Zeit automatisch gelöscht werden.

Mögliche Werte:

- 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.



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!



Alle weiteren Parameter der WLAN-Netzwerke entsprechen denen der üblichen Konfiguration für Access Points.

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:



In normalen Access-Point-Anwendungen sollten Sie nur die 5-GHz-Unterbänder 1 und 2 verwenden. Das Unterband 3 steht nur für besondere Anwendungen zur Verfügung (z. B. BFWA – Broadband Fixed Wireless Access).

LANconfig: WLAN Controller ► Profile ► Physikalische WLAN-Parameter
 WEBconfig: LCOS-Menübaum ► Setup ► WLAN-Management ► AP-Konfiguration ► Radioprofile

■ Name

Eindeutiger Name für diese Zusammenstellung von physikalischen WLAN-Parametern.

Mögliche Werte:

- Maximal 31 ASCII-Zeichen.

Default:

leer

■ Vererbung

Auswahl eines schon definierten logischen WLAN-Netzwerks, von dem die Einstellungen übernommen werden sollen ('Vererbung von Parametern' → Seite 78).

■ Land

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

Mögliche Werte:

Auswahl aus der Liste der angebotenen Länder.

Default:

leer

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 (z. B. '1,6,11'). Dabei ist auch die Angabe von Bereichen möglich.

Mögliche Werte:

Maximal 16 Zeichen.

Default:

leer

■ Management-VLAN-ID

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

Mögliche Werte:

0 bis 4094

Default:

0

Besondere Werte:

- 0: Schaltet die Verwendung von VLAN generell aus – auch für alle logischen WLANs (SSIDs), unabhängig von deren VLAN-Konfiguration.
- 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.

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:

LANconfig: WLAN Controller ► Profile ► WLAN-Profile

WEBconfig: LCOS-Menübaum ► Setup ► WLAN-Management ► AP-Konfiguration ► Gesamtprofile

■ Profil-Name

Name des Profils, unter dem die Einstellungen gespeichert werden.

Mögliche Werte:

- Maximal 31 ASCII-Zeichen.

Default:

- leer

■ WLAN-Netzwerk-Liste

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

Mögliche Werte:

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

Default:

- leer



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.

Mögliche Werte:

- Auswahl aus der Liste der physikalischen WLAN-Netzwerke

Default:

- leer

■ IP-Adresse alternativer WLAN Controller

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 oder DNS ein. Wenn nicht alle WLAN Controller über einen solchen Broadcast erreicht werden können (WLAN Controller steht z. B. in einem anderen Netz), dann ist die Angabe von alternativen WLAN Controllern sinnvoll.

Mögliche Werte:

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

Default:

- leer

4.2.3 Access Point Konfiguration

In diesem Bereich finden Sie eine Liste aller verfügbaren Access Points sowie die IP-Parameter-Profile. Diese Profile können Sie verwenden, sollten Sie bestimmten Access Points ihre IP-Adressen nicht per DHCP zuweisen wollen.

IP-Parameter-Profile

Sie können hier bestimmte Profile definieren, die Sie dann Access Points zuweisen können, wenn Sie sie nicht mittels DHCP mit einer IP-Adresse versehen wollen. Damit können Sie gezielt festlegen, welche IP-Parameter ein Access Point nutzt.

LANconfig: WLAN Controller ► AP-Konfig. ► IP-Parameter-Profile

WEBconfig: LCOS-Menübaum ► Setup ► WLAN-Management ► AP-Konfiguration ► AP-Intranets

■ Name

Name des IP-Parameter-Profils

Mögliche Werte:

Maximal 31 Zeichen

Default:

leer

■ Vererbung

Auswahl eines schon definierten IP-Parameter-Profils, von dem die Einstellungen übernommen werden sollen ('Vererbung von Parametern' → Seite 78).

■ Domänen-Name

Name der Domäne (DNS-Suffix), die dieses Profil nutzen soll.

Mögliche Werte:

- max. 63 Zeichen

Default:

- leer

■ Netzmaske

Netzmaske des Profils

Mögliche Werte:

- gültige Netzmaske

Default:

- leer

■ Standard-Gateway

Das Standard-Gateway, dass das Profil verwendet.

Mögliche Werte:

- gültige IP-Adresse

Default:

- leer

■ Erster DNS

Der DNS (Domain Name System), den das Profil verwenden soll.

Mögliche Werte:

- gültige IP-Adresse

Default:

- leer

■ Zweiter DNS

Zweiter, alternativer DNS, sollte der erste nicht erreichbar sein.

Mögliche Werte:

- gültige IP-Adresse

Default:

- leer

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-Profil (also Kombinationen aus logischen und physikalischen WLAN-Parametern) zugeordnet. 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:

LANconfig: WLAN Controller ► AP-Konfig. ► Access-Point-Tabelle

WEBconfig: LCOS-Menübaum ► Setup ► WLAN-Management ► AP-Konfiguration ► Basisstationen

■ Update-Management aktiv

Wenn Sie für den Access-Point das Update-Management aktivieren, können neue Firmware- oder Script-Versionen automatisch geladen werden. Nehmen Sie alle weiteren Einstellungen unter AP-Update vor.

Mögliche Werte:

- Ja, Nein

Default:

- Ja

■ **MAC-Adresse**

MAC-Adresse des Ethernet-Interfaces des Access Points.

Mögliche Werte:

- 12 Hexadezimal-Zeichen.

Besondere Werte:

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

Default:

- Leer

■ **AP-Name**

Name des Access Point im Managed-Modus.

Mögliche Werte:

- Maximal 16 ASCII-Zeichen.

Default:

- Leer

■ **Standort**

Standort des Access Point im Managed-Modus.

Mögliche Werte:

- Maximal 251 ASCII-Zeichen.

Default:

- Leer

■ **WLAN-Profil**

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

Mögliche Werte:

- Auswahl aus der Liste der definierten WLAN-Profile, max. 31 ASCII-Zeichen.

Default:

- Leer

■ **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, Default

Besondere Werte:

- 'Default' übernimmt die Frequenzband-Einstellung von der Definition im Bereich 'Optionen'.

■ **Auto. Kanalwahl Ifc 1**

Die Kanalauswahl erfolgt vom Access-Point grundsätzlich automatisch für das Frequenzband des eingestellten Landes, wenn hier kein Eintrag erfolgt.

Tragen Sie hier die Kanäle ein, auf die sich die automatische Auswahl für das erste WLAN-Modul beschränken soll. Wird hier nur ein Kanal angegeben, so wird nur dieser verwendet und es findet keine automatische Auswahl statt. Achten Sie deshalb darauf, dass die angegebenen Kanäle wirklich im Frequenzband des eingestellten Landes zur Verfügung stehen. Für das jeweilige Frequenzband ungültige Kanäle werden ignoriert.

Auch die automatische Kanaloptimierung nutzt diesen Wert, um den Kanal dem Access Point fest zuzuweisen.

Mögliche Werte:

- Kommaseparierte Liste mit max. 48 Zeichen

Default:

- Leer

■ **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

Default:

- Leer

Besondere Werte:

- 'Default' übernimmt die Frequenzband-Einstellung von der Definition im Bereich 'Optionen'.

■ **Auto. Kanalwahl Ifc 2**

Automatische Kanalwahl für das zweite WLAN-Modul.



Die Einstellungen für das zweite WLAN-Modul werden ignoriert, wenn das verwaltete Gerät nur über ein WLAN-Modul verfügt.

■ 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

Default:

- DTLS

Besondere Werte:

- 'Default' übernimmt die Verschlüsselung von der Definition im Bereich 'Optionen'.

■ Doppelte Bandbreite

Für LANCOM Access Points nach IEEE 802.11n kann hier die Nutzung der doppelten Bandbreite aktiviert werden.

Normalerweise nutzt das WLAN-Modul einen Frequenzbereich von 20 MHz, in dem die zu übertragenen Daten auf die Trägersignale aufmoduliert werden. 802.11a/b/g nutzen 48 Trägersignale in einem 20 MHz-Kanal. Durch die Nutzung des doppelten Frequenzbereiches von 40 MHz können 96 Trägersignale eingesetzt werden, was zu einer Verdoppelung des Datendurchsatzes führt.

802.11n kann in einem 20 MHz-Kanal 52, in einem 40 MHz-Kanal sogar 108 Trägersignale zur Modulation nutzen. Für 802.11n bedeutet die Nutzung der 40 MHz-Option also einen Performance-Gewinn auf mehr als das Doppelte.

Mögliche Werte:

- Auto, Nein

Default:

- Auto

■ Antennengruppierung

LANCOM Access Points mit 802.11-Unterstützung können bis zu drei Antennen zum Senden und Empfangen der Daten einsetzen. Je nach Anwendung kann die Nutzung der Antennen eingestellt werden.

Mögliche Werte:

- 1+2+3: Beim Einsatz des Geräts im Access-Point-Modus zur Anbindung von WLAN-Clients ist in der Regel die parallele Nutzung aller drei Antennen zu empfehlen um eine gute Netzabdeckung zu erzielen.
- 1+3: Für die Nutzung von zwei parallelen Datenströmen z. B. bei Point-to-Point-Verbindungen mit einer entsprechenden Dual-Slant-Antenne werden die Antennen-Anschlüsse 1 und 3 verwendet. Der dritte Antennen-Anschluss wird dabei deaktiviert.
- 1: Bei Anwendungen mit nur einer Antenne (z. B. Outdoor-Anwendung mit einer Antenne) wird die Antennen an den Anschluss 1 angeschlossen die Anschlüsse 2 und 3 werden deaktiviert.
- Auto: automatische Auswahl der Antennen

Default:

- Auto

Besondere Werte:

- Auto: Mit der Einstellung 'Auto' werden alle verfügbaren Antennen genutzt.

■ IP-Adresse

Statische IP-Adresse für den AP, wenn kein DHCP genutzt werden kann/soll.

Mögliche Werte:

- Gültige IP-Adresse.

Default:

- Leer

■ IP-Parameterprofil

Geben Sie hier den Profilnamen an, über den die IP-Einstellungen für den Access-Point referenziert werden. Wenn Sie den Standardwert DHCP beibehalten, wird die Angabe der festen IP-Adresse ignoriert, so dass der Access-Point seine IP-Adresse über DHCP beziehen muss.

Mögliche Werte:

- Auswahl aus der Liste der definierten IP-Parameter-Profile, max. 31 ASCII-Zeichen.

Default:

- DHCP

4.2.4 AP-Update

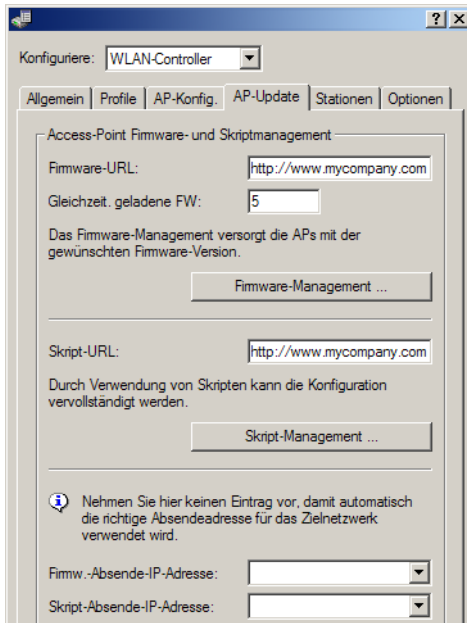
Mit einem LANCOM WLAN Controller kann die Konfiguration von mehreren LANCOM Access Points von einer Stelle aus komfortabel und konsistent verwaltet werden. Mit dem zentralen Firmware- und Skript-Management können auch Firmware- und Skript-Uploads auf allen verwalteten WLAN-Geräten automatisch ausgeführt werden.

Dazu werden die Firmware- und Skript-Dateien auf einem Web-Server abgelegt (Firmware als *.UPX, Skripte als *.LCS). Der WLAN Controller prüft einmal täglich oder aufgrund einer entsprechenden Benutzeraktion den Bestand und vergleicht die verfügbaren Dateien mit den Versionen in den Geräten – alternativ kann dieser Vorgang auch über einen Cron-Job z. B. nachts erledigt werden. Wenn ein Update durchgeführt werden kann oder nicht die gewünschte Version auf dem Access Point läuft, lädt der WLAN Controller diese vom Web-Server herunter und spielt sie in die entsprechenden Access Points ein.

Mit der Konfiguration des Firmware- und Skript-Managements kann die Distribution der Dateien gezielt gesteuert werden. So kann die Nutzung von bestimmten Firmware-Versionen z. B. auf bestimmte Gerätetypen oder MAC-Adressen beschränkt werden.

Das Update kann in zwei möglichen Zuständen ausgeführt werden:

- Beim Verbindungsaufbau, danach startet der Access Point automatisch neu.
- Wenn der Access Point schon verbunden ist, startet das Gerät danach **nicht** automatisch neu. In diesem Fall wird der Access Point manuell über die Menüaktion `"/Setup/WLAN-Management/Central-Firmware-Management/Reboot-updated-APs"` oder zeitgesteuert per Cron-Job neu gestartet.
- Mit der Aktion `"/Setup/WLAN-Management/Central-Firmware-Management/Update-Firmware-and-Script-Information"` können Skript- und Firmwareverzeichnisse aktualisiert werden.



LANconfig: WAN-Controller ► AP-Update

WEBconfig: Setup ► WLAN-Management ► Zentrales-Firmware-Management

Allgemeine Einstellungen für das Firmware-Management

■ Firmware-URL

Pfad zum Verzeichnis mit den Firmware-Dateien.

Mögliche Werte:

- URL in der Form Server/Verzeichnis oder http://Server/Verzeichnis

Default:

- leer

■ Gleichzeitig geladene FW

Anzahl der gleichzeitig im Arbeitsspeicher des WLAN Controllers vorgehaltenen Firmware-Versionen.



Die hier vorgehaltenen Firmware-Versionen werden nur einmal vom Server geladen und anschließend für alle passenden Update-Prozesse genutzt.

Mögliche Werte:

- 1 bis 10

Default:

- 5

■ Firmware-Absende-IP-Adresse

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

Mögliche Werte:

- Name eines definierten IP-Netzwerks.
- 'INT' für die IP-Adresse im ersten Netzwerk mit der Einstellung 'Intranet'.
- 'DMZ' für die IP-Adresse im ersten Netzwerk mit der Einstellung 'DMZ'.
- Name einer Loopback-Adresse.
- Beliebige andere IP-Adresse, die auf dem WLAN Controller gültig ist.

Default:

- leer



Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'INT' oder 'DMZ' vorhanden ist, wird die IP-Adresse des IP-Netzwerks bzw. der Loopback-Adresse mit dem Namen 'INT' bzw. 'DMZ' verwendet.

Firmware-Management-Tabelle

Tabelle mit Gerätetyp, MAC-Adresse und Firmware-Version zur gezielten Steuerung der verwendeten Firmware-Dateien.



Die Einträge in der Firmware-Management-Tabelle werden nur benötigt, wenn gezielt bestimmte Firmware-Versionen (z. B. Downgrades) eingespielt werden sollen. Wenn die Geräte immer die aktuelle Firmware verwenden sollen, sind hier keine Einträge notwendig.

■ Gerätetypen

Wählen Sie hier aus, für welchen Gerätetyp die in diesem Eintrag spezifizierte Firmware-Version verwendet werden soll.

Mögliche Werte:

- Alle bzw. Auswahl aus der Liste der verfügbaren Gerätetypen.

Default:

- Alle

■ MAC-Adresse

Wählen Sie hier aus, für welches Gerät (identifiziert anhand der MAC-Adresse) die in diesem Eintrag spezifizierte Firmware-Version verwendet werden soll.

Mögliche Werte:

- Gültige MAC-Adresse.

Default:

- Leer

■ Version

Firmware-Version, welche für die in diesem Eintrag spezifizierten Geräte oder Gerätetypen verwendet werden soll.

Mögliche Werte:

- Firmware-Version in der Form X.XX

Default:

- Leer

Allgemeine Einstellungen für das Skript-Management

■ Skript-URL

Pfad zum Verzeichnis mit den Skript-Dateien.

Mögliche Werte:

- URL in der Form `Server/Verzeichnis` oder `http://Server/Verzeichnis`

Default:

- Leer

■ Skript-Absende-IP-Adresse

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

Mögliche Werte:

- Name eines definierten IP-Netzwerks.
- 'INT' für die IP-Adresse im ersten Netzwerk mit der Einstellung 'Intranet'.
- 'DMZ' für die IP-Adresse im ersten Netzwerk mit der Einstellung 'DMZ'.
- Name einer Loopback-Adresse.
- Beliebige andere IP-Adresse, die auf dem WLAN Controller gültig ist.

Default:

- leer



Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'INT' oder 'DMZ' vorhanden ist, wird die IP-Adresse des IP-Netzwerks bzw. der Loopback-Adresse mit dem Namen 'INT' bzw. 'DMZ' verwendet.

Skript- Management-Tabelle

Tabelle mit Skript-Dateiname und WLAN-Profil zur Zuordnung der Skripte zu einem WLAN-Profil.

Die Konfiguration eines Access Points in der Betriebsart "Managed" erfolgt über WLAN-Profile. Mit einem Skript können auch diejenigen Detail-Parameter der gemanagten Geräte eingestellt werden, die nicht im Rahmen der vorgegebenen Parameter eines WLAN-Profiles verwaltet werden. Dabei erfolgt die Zuordnung ebenfalls über die WLAN-Profile, um für die Access Points mit gleicher WLC-Konfiguration auch das gleiche Skript zu verwenden.

Da für jedes WLAN-Profil nur eine Skript-Datei angegeben werden kann, ist hier keine Versionierung möglich. Bei der Zuweisung eines Skripts zu einem Access Point wird allerdings eine MD5-Prüfsumme der Skript-Datei gespeichert. Über diese Prüfsumme kann der WLAN Controller bei einer neuen oder geänderten Skript-Datei mit gleichem Dateinamen feststellen, ob die Skript-Datei erneut übertragen werden muss.

■ Skript-Dateiname

Name der zu verwendenden Skript-Datei.

Mögliche Werte:

- Dateiname in der Form *.lcs

Default:

- leer

■ WLAN-Profil

Wählen Sie hier aus, für welches WLAN-Profil die in diesem Eintrag spezifizierte Skript-Datei verwendet werden soll.

Mögliche Werte:

- Auswahl aus der Liste der definierten WLAN-Profile.

Default:

- Leer

Interner Skript-Speicher (Skript-Management ohne HTTP-Server)

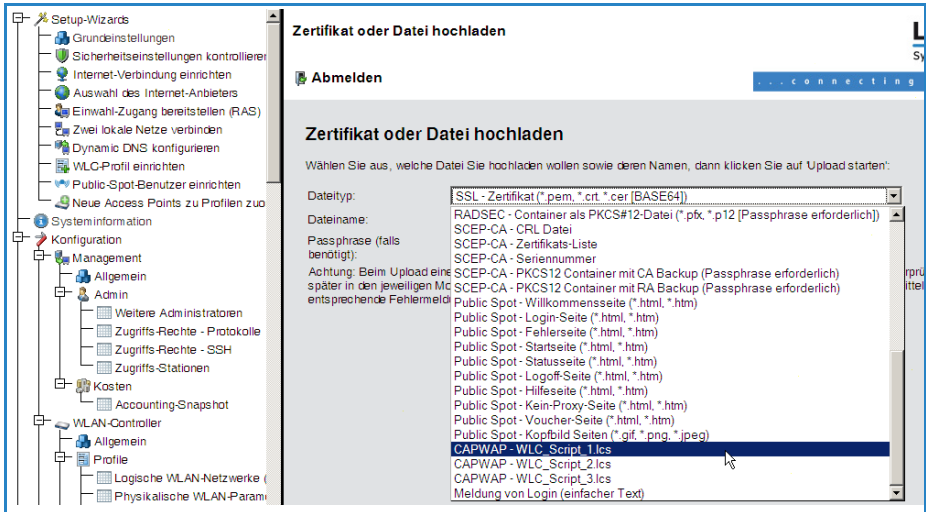
Skripte haben im Gegensatz zu Firmware-Dateien oft nur ein geringes Datenvolumen. Im internen Skript-Speicher der WLAN Controller können drei Skripte mit maximal je 64kB Größe gespeichert werden. Wenn der Bedarf für Skripte nicht über dieses Volumen hinausgeht, kann die Einrichtung eines HTTP-Servers für diesen Zweck entfallen.

Die Skript-Dateien werden dazu einfach über WEBconfig auf den vorgesehenen Speicherplatz geladen. Nach dem Upload muss die Liste der verfügbaren Skripte mit der Aktion Setup/WLAN-Management/Zentrales-Firmware-Management/Aktualisiere-Firmware-und-Skript-Information aktualisiert werden.

Aus der Skript-Management-Tabelle können diese internen Skripte den entsprechenden Namen referenziert werden (WLC_Script_1.lcs, WLC_Script_2.lcs oder WLC_Script_3.lcs).



Bitte beachten Sie bei der Angabe der Script-Namen die Groß- und Kleinschreibung!



4.2.5 Stationen

Mit Hilfe der Stationstabelle legen Sie fest, welche WLAN-Clients sich in den WLAN-Netzwerken der LANCOM Access Points anmelden können, die durch den WLAN Controller zentral verwaltet werden. Außerdem können sie den einzelnen WLAN-Clients auf diesem Wege sehr komfortabel eine individuelle Passphrase zur Authentifizierung und eine VLAN-ID zuweisen.

Zur Nutzung der Stationstabelle muss grundsätzlich der RADIUS-Server im WLAN Controller aktiviert sein. Alternativ kann auch eine Weiterleitung zu einem anderen RADIUS-Server konfiguriert werden. Weitere Information zu RADIUS finden Sie unter 'RADIUS'.

Für jedes logische WLAN-Netzwerk, in dem die WLAN-Clients über RADIUS geprüft werden sollen, muss die MAC-Prüfung aktiviert werden.

The screenshot shows a dialog box titled "Stationen - Neuer Eintrag". It contains the following fields and values:

- MAC-Adresse: 00A057010203
- Name: CLIENT01
- Passphrase (optional):
- TX Bandbr.-Begrenzung: 0 kbit/s
- RX Bandbr.-Begrenzung: 0 kbit/s
- Kommentar:
- VLAN-ID: 0

Buttons: OK, Abbrechen

LANconfig: WLAN Controller ► Stationen ► Stationen

WEBconfig: LCOS-Menübaum ► Setup ► WLAN Management ► Zugangs-Liste

■ MAC-Adresse

MAC-Adresse des WLAN-Clients, für den dieser Eintrag gilt.

Mögliche Werte:

- Gültige MAC-Adresse

Default:

- Leer

■ Name

Sie können zu jedem WLAN-Client einen beliebigen Namen und einen Kommentar eingeben.

Dies ermöglicht Ihnen eine einfachere Zuordnung der MAC-Adressen zu bestimmten Stationen oder Benutzern.

Mögliche Werte:

- max. 32 Zeichen

Default:

- Leer

■ Passphrase

Hier können Sie optional für jede physikalische Adresse (MAC) eine separate Passphrase eintragen, die in den 802.11i/WPA/AES-PSK gesicherten Netzwerken benutzt wird. Ohne die Angabe einer gesonderten Passphrase für diese MAC-Adresse werden die im Bereich '802.11i/WEP' (beim WLAN Controller in der Definition der logischen WLAN-Netzwerke (SSIDs)) für jedes logische Wireless-LAN-Netzwerk hinterlegten Passphrasen verwendet.

Mögliche Werte:

- ASCII-Zeichenkette mit einer Länge von 8 bis 63 Zeichen

Default:

- Leer

■ TX Bandbreitenbegrenzung

Bandbreiten-Begrenzung für die sich einbuchenden WLAN-Clients. Ein LANCOM WLAN-Gerät im Client-Modus übermittelt seine eigene Einstellung bei der Anmeldung an den Access Point. Diese bildet daraus zusammen mit dem hier eingestellten Wert das Bandbreiten-Minimum.

Mögliche Werte:

- 0 bis 65535 kbit/s

Default:

- 0

Besondere Werte:

- 0: keine Begrenzung

■ RX Bandbreitenbegrenzung

Bandbreiten-Begrenzung für die sich einbuchenden WLAN-Clients. Ein Client übermittelt seine eigene Einstellung bei der Anmeldung an die Basisstation. Diese bildet daraus zusammen mit dem hier eingestellten Wert das Bandbreiten-Minimum.

Mögliche Werte:

- 0 bis 65535 kbit/s

Default:

- 0

Besondere Werte:

- 0: keine Begrenzung



Die RX-Bandbreiten-Begrenzung ist nur aktiv für LANCOM WLAN-Geräte im Client-Modus. Für normale WLAN-Clients wird dieser Wert nicht verwendet.

■ VLAN-ID

Diese VLAN-ID wird Paketen zugewiesen, die von dem Client mit der eingetragenen MAC-Adresse empfangen wurden.

Mögliche Werte:

- 0 bis 4096

Default:

- 0

Besondere Werte:

- Bei der VLAN-ID 0 wird der Station keine spezielle VLAN-ID zugewiesen, es gilt die VLAN-ID der Funkzelle (SSID).

4.2.6 RADIUS-Server

Standardmäßig übernimmt der WLAN Controller die Weiterleitung von Anfragen für die Konto- bzw. Zugangsverwaltung an einen RADIUS-Server. Damit die Access Points den RADIUS-Server direkt ansprechen können, müssen entsprechenden Server-Informationen hier definiert werden. Somit funktioniert die RADIUS-Anwendung auch dann noch, wenn der WLAN Controller nicht erreichbar ist. Allerdings müssen dafür Einstellungen für jeden einzelnen Access Point im adressierten RADIUS-Server vorgenommen werden und die managed Access Points müssen den RADIUS-Server aus ihrem Management-Netz heraus erreichen können. Ist der RADIUS-Server in einem anderen IP-Netz, muss über das IP-Parameter-Profil insbesondere das Gateway definiert werden.

LANconfig: WLAN Controller ▶ Stationen ▶ RADIUS-Server

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WLAN Management ▶ RADIUS-Server

■ Typ

Type der RADIUS Anwendung.

Mögliche Werte:

- Konto oder Zugang

Default:

- Die Einträge Konto, Zugang, Backup-Konto und Backup-Zugang sind fest eingestellt und können nicht verändert werden.

■ IP-Adresse

IP-Adresse des Radius Servers, die den AP mitgeteilt wird, um den RADIUS Server zu erreichen. Wird hier kein Wert angegeben, wird automatisch die IP-Adresse des Controllers genommen.

Mögliche Werte:

- Gültige IP-Adresse.

Default:

- Leer

■ Port

Port-Nummer, die den AP mitgeteilt wird, um den RADIUS Server zu erreichen. Der Port muss mit dem im RADIUS-Server konfigurierten Wert übereinstimmen. Dieser Wert wird ignoriert, wenn keine IP-Adresse konfiguriert ist, da dann der Controller selbst als RADIUS-Server benutzt wird.

Mögliche Werte:

- Gültige Port-Nummer, im Allgemeinen 1812 für Zugangs- und 1813 für Kontoverwaltung.

Default:

- 0

■ Secret

Passwort für den RADIUS Dienst. Der Schlüssel (Secret) muss mit dem im RADIUS-Server konfigurierten Wert übereinstimmen. Dieser Wert wird ignoriert, wenn keine IP-Adresse konfiguriert ist, da dann der Controller selbst als RADIUS-Server benutzt wird.

Mögliche Werte:

- max. 31 ASCII-Zeichen.

Default:

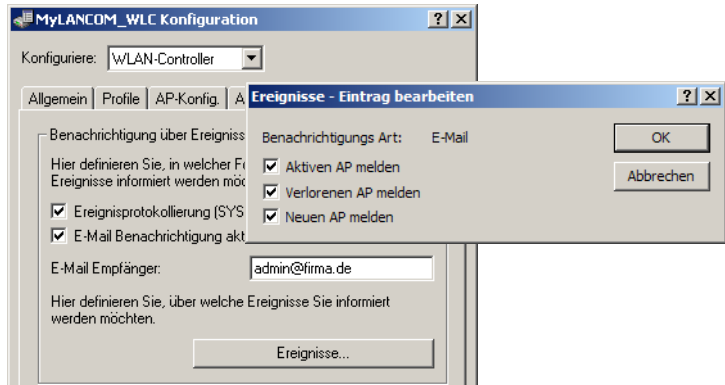
- Leer

4.2.7 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:



LANconfig: WLAN Controller ▶ Optionen ▶ Benachrichtigungen

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WLAN-Management ▶ Benachrichtigung

■ SYSLOG

Aktiviert die Benachrichtigung über SYSLOG.

Mögliche Werte:

Ein oder Aus

Default:

Aus

■ E-Mail

Aktiviert die Benachrichtigung über E-Mail.

Mögliche Werte:

Ein oder Aus

Default:

Aus

■ Ereignisse

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

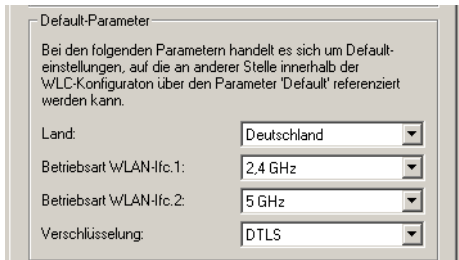
Mögliche Werte:

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.



Default-Parameter

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

Land: Deutschland

Betriebsart WLAN-Ifc.1: 2,4 GHz

Betriebsart WLAN-Ifc.2: 5 GHz

Verschlüsselung: DTLS

LANconfig: WLAN Controller ▶ Optionen ▶ Default-Parameter

WEBconfig: LCOS-Menübaum ▶ Setup ▶ WLAN-Management ▶ AP-Konfiguration

■ 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.

■ WLAN-Interface 2

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

■ 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.

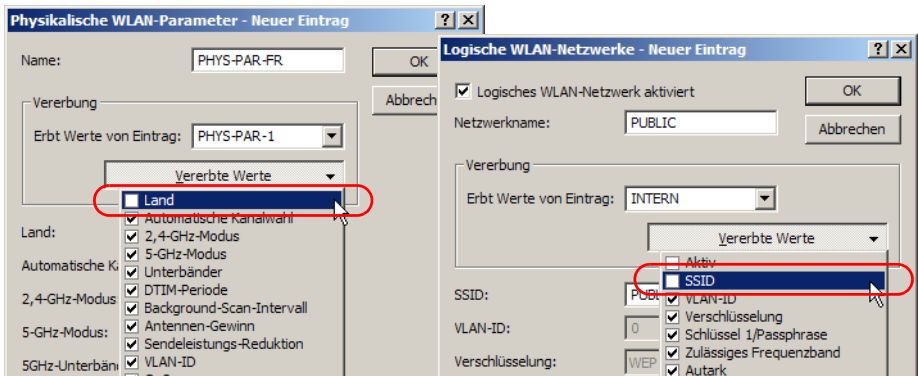
4.2.8 Vererbung von Parametern

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 Verer-

bung beschränken sich dabei aber auf eine „Vererbungsrichtung“ pro Parameter.



Änderungen an Eltern-Einträgen haben unmittelbare Auswirkung auf alle von ihm ererbenden Einträge. Der Eltern-Eintrag kann und darf seinerseits ebenfalls Werte von anderen Einträgen erben. Derartig komplexe Vererbung sollte jedoch mit Bedacht eingesetzt werden, da dies leicht zu unüberschaubaren Konfigurationen und Konfigurations-Fehlern führen kann.



Wenn ein Eltern-Eintrag aus der Konfiguration gelöscht wird, werden alle von diesem Eintrag ererbenden Einträge ungültig.

4.3 Konkrete Konfigurationsbeispiele

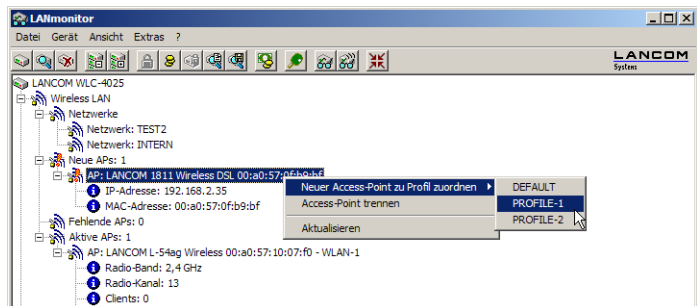
4.3.1 Neue Access Points manuell in die WLAN-Struktur aufnehmen

Wenn Sie die Access Points nicht automatisch in die WLAN-Struktur aufnehmen wollen (Auto-Accept, 'Automatische Annahme neuer APs (Auto-Accept)), 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 Controllers mit WEBconfig.
- 2 Wählen Sie unter **LCOS-Menübaum ▶ Setup ▶ WLAN-Management** die Aktion **AP-einbinden**.
- 3 Geben Sie als Parameter für die Aktion die Ethernet-MAC-Adresse des Access Points ein, den Sie akzeptieren möchten, und bestätigen Sie mit **Ausführen**.

AP-einbinden

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

Parameter

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 Controllers mit WEBconfig. Wenn neue Access Points gefunden wurden, zeigt WEBconfig das im Gerätestatus mit einer entsprechenden Meldung an.

Systemdaten	Gerätestatus	Syslog
SCEP-GA	GA-Status: Aktiv Wartende-Anfragen: 0	
WLAN-Controller	Controller-Status: Bereit Erwartete-AP: 1 Verbundene-erwartete-AP: 0 Verbundene-neue-AP: 1	Neue Access Points zu Profilen zuordnen
Uhrzeit	22.07.2009 15:06	

- 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.

192.168.2.34 - Neue Access Points zu Profilen zuordnen

LANCOM
Systems
... connecting your

Schritt 3 von 4

Wählen Sie das Profil aus, dem der ausgewählte Access Point zugeordnet werden soll:

Profil

- ⓘ 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.

- ⓘ Für die Konfiguration der LANCOM-Geräte können mehrere Administratoren mit unterschiedlichen Rechten eingerichtet werden. Für einen WLAN Controller kann ein Administratorkonto sinnvoll sein, mit dem nur neue Access Points aufgenommen werden können, das aber keine anderen Änderungen an der Konfiguration erlaubt. Hinweise zum Anlegen von Administratoren finden Sie im LCOS-Referenzhandbuch.

4.3.2 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 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 im Access Point die WLAN-Betriebsart für die WLAN-Module von 'Managed' auf 'Client' oder 'Access-Point' um.
- ② Löschen Sie im WLAN Controller 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 **LCOS-Menübaum ▶ Setup ▶ WLAN-Management** mit der Aktion **AP-Verbindung-trennen** oder alternativ im LANmonitor.
- 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**.

AP-Verbindung-trennen

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

Parameter:

Access Point deaktivieren

Um einen 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') 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 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.

4.3.3 Sicherung der Zertifikate

Ein LANCOM WLAN Controller erzeugt beim ersten Systemstart die grundlegenden eigenen 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, müssen immer die gleichen Root-Zertifikate verwendet 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'). 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 **LCOS-Menübaum ▶ 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.

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 von 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'.
Bei PKCS12-Dateien kann eine Passphrase erforderlich sein.

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-Trace sehen.

- ④ Nach dem Einspielen der CA Sicherung muss die Datei controller_rootcert im Verzeichnis /Status/File-System/Contents gelöscht werden. Geben Sie dazu an der Konsole die folgenden Befehle ein:


```
cd /Status/File-System/Contents
del controller_rootcert
```
- ⑤ Danach muss im Verzeichnis /Setup/Certificates/SCEP-Client der Befehl Reinit aufgerufen werden:


```
cd /Setup/Certificates/SCEP-Client
do Reinit
```

4.3.4 Sichern 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 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-CA-Zertifikatsliste: Liste aller von der SCEP-CA jemals ausgestellten Zertifikate.
- SCEP-CA-Seriennummer: Enthält die nächste freie Seriennummer für das nächste Zertifikat.

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:

- RADIUS-Server - Summarisches Accounting (*.csv)
- SCEP-CA - CRL-Datei
- SCEP-CA - Zertifikats-Liste**
- SCEP-CA - Seriennummer
- SCEP-CA - PKCS12 Container mit CA Backup
- SCEP-CA - PKCS12 Container mit RA Backup
- Public Spot - Willkommenseite (*.html, *.htm)
- Public Spot - Login-Seite (*.html, *.htm)
- Public Spot - Fehlersseite (*.html, *.htm)
- Public Spot - Startseite (*.html, *.htm)
- Public Spot - Statusseite (*.html, *.htm)

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'.
Bei PKCS12-Dateien kann eine Passphrase erforderlich sein.

Dateityp:

Dateiname:

Passphrase (falls benötigt):

Achtung: Beim Upload von Dateien ist die Passphrase erforderlich.

Korrektur: Beim Upload von Dateien ist die Passphrase erforderlich.

Fehlermeldungen:



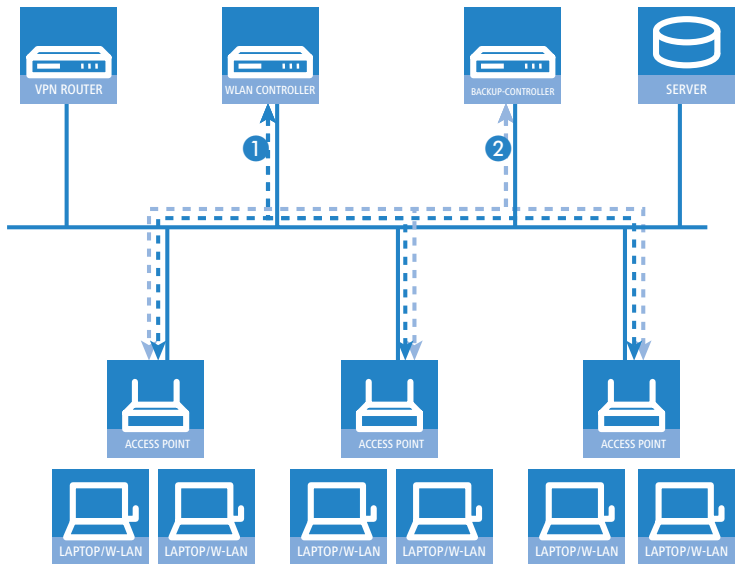
Nach dem Einspielen einer neuen Zertifikatsliste werden abgelaufene Zertifikate entfernt und eine neue CRL erstellt. Weiterhin reinitialisiert sich die CA automatisch, wenn nach dem Einspielen der Zertifikatsbackups erfolgreich Zertifikate und Schlüssel extrahiert wurden.

4.3.5 Backup von LANCOM WLAN Controllern

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 84).
- Damit die Prüfung der Zertifikate bzgl. der zeitlichen Gültigkeit zu gleichen Ergebnissen kommt, stellen Sie auf allen WLAN Controllern die gleiche Zeitinformation ein.



- 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 Speichern Sie die Konfiguration des ersten WLAN Controllers ① z. B. mit LANconfig als Datei. Weisen Sie dieser Konfiguration die passende IP-Adresse für den Backup-Controller zu.
- ⑤ Übertragen Sie die angepasste Konfiguration 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.
- ⑥ 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.

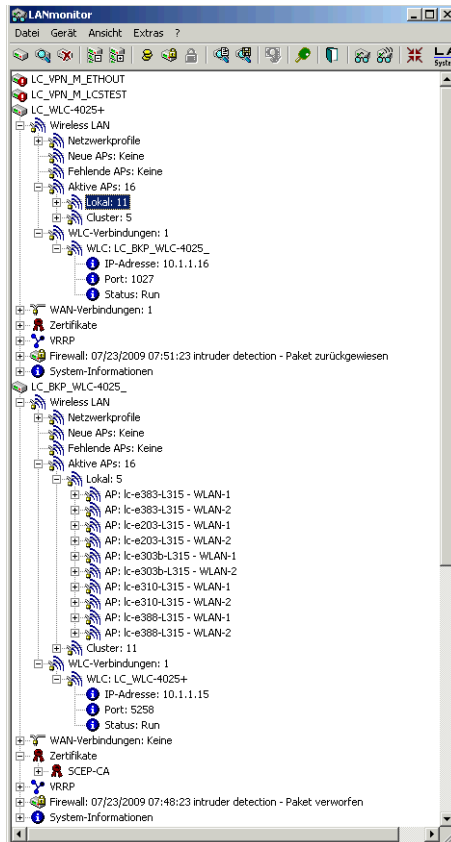


Die Access Points bleiben in diesem Szenario so lange in der Verwaltung des Backup-Controllers, bis dieser entweder selbst einmal nicht erreichbar ist oder bis sie manuell getrennt werden ('Access Point trennen' → Seite 114).



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.

- ⑦ Im LANmonitor werden die Verbindungen der Access Points zu den Controllern angezeigt: Lokale Access Points werden von dem jeweiligen Controller zu diesem Zeitpunkt selbst verwaltet, Access Points im "Cluster" werden von einem anderen Controller verwaltet, könnten aber auch von diesem Controller übernommen werden.



4.3.6 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.

- 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') alle WLAN Controller gleichmäßig mit Konfigurationen für einen Teil der Access Points „gefüllt“ werden.

Wenn nachträglich zu einem vorhandenen WLAN Controller ein zweiter WLAN Controller im Netzwerk integriert wird, sind die Access Points zunächst alle beim bisherigen Controller angemeldet. Um die Access Points komfortabel auf die beiden Controller zu verteilen, können Sie folgendermaßen vorgehen:

- ① Stellen Sie bei dem zweiten Controller die gleiche Zeit ein wie bei dem bisher genutzten Gerät.
- ② Übertragen Sie die CA- und RA-Zertifikate aus dem bisherigen WLAN Controller in das neue Gerät.
- ③ Aktivieren Sie im neuen Controller die 'Automatische Annahme neuer APs (Auto-Accept)'.
- ④ Speichern Sie die Konfiguration des bisherigen WLAN Controllers z. B. mit LANconfig als Datei. Weisen Sie dieser Konfiguration die passende IP-Adresse für den neuen Controller zu.
- ⑤ Übertragen Sie die angepasste Konfiguration auf den neuen Controller. Dabei werden auch die Profile und die AP-Tabellen mit den MAC-Adressen der Access Points auf den neuen Controller übertragen.
- ⑥ Schalten Sie den bisherigen Controller aus. Die Access Points suchen nun nach einem verfügbaren Controller und finden das neue Gerät, das auch über die passenden CA-Zertifikate und WLAN-Profile verfügt. Der neue Controller kann auf die Anfrage der Access Points neue Geräte-Zertifikate ausstellen und die Verwaltung übernehmen.
- ⑦ Schalten Sie den bisherigen Controller wieder ein. Die Access Points bleiben so lange in der Verwaltung des neuen Controllers. Durch das manuelle Trennen kann dann ein Teil der Access Points wieder vom neuen Controller gelöst werden. Bei der neuerlichen Suche nach einem freien Controller verbinden sich diese Access Points dann mit dem bisherigen Controller, da dieser über eine geringere Auslastung verfügt.

4.3.7 Dynamische VLAN-Zuweisung

In einer größeren WLAN-Struktur ist es oft sinnvoll, den einzelnen WLAN-Clients ein bestimmtes Netzwerk zuzuweisen. Prinzipiell kann diese Zuweisung über die SSID in Verbindung mit einem bestimmten IP-Netzwerk realisiert

werden. In größeren Organisationen macht es jedoch ggf. keinen Sinn, für jede Abteilung o.ä. eine separate SSID zu verwenden. Um die WLAN-Clients **unabhängig** von dem WLAN-Netzwerk, in dem sie sich gerade eingebucht haben, in ein bestimmtes Netzwerk zu leiten und logisch von anderen Teilnehmern zu trennen, können dynamisch zugewiesene VLANs genutzt werden. Anders als bei den statisch konfigurierten VLAN-IDs für eine bestimmte SSID ('VLAN-ID') wird die VLAN-ID dabei dem WLAN-Client von einem RADIUS-Server direkt zugewiesen.

Beispiel:

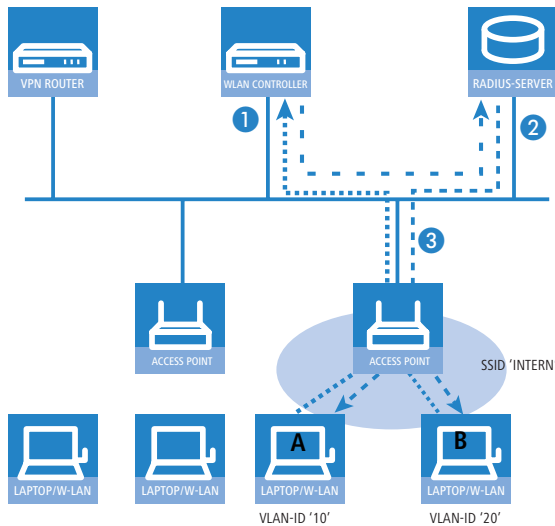
- Die WLAN-Clients der Mitarbeiter buchen sich über einen Access Point in das WPA-gesicherte WLAN mit der SSID 'INTERN' ein. Bei der Anmeldung werden die RADIUS-Anfragen der WLAN-Clients an den Access Point gestellt. Wenn sich das entsprechende WLAN-Interface in der Betriebsart 'Managed' befindet, werden 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 oder bei der Verwendung von 802.1x anhand des Benutzernamens eine bestimmte VLAN-ID für die jeweilige Abteilung zuweisen. Dabei erhält z. B. der WLAN-Client aus dem Marketing die VLAN-ID '10' und WLAN-Client aus der Entwicklung die '20'. Wenn für den Benutzer keine VLAN-ID definiert ist, wird die Haupt-VLAN-ID der SSID verwendet.
- Die WLAN-Clients der Gäste buchen sich über den gleichen Access Point in das nicht gesicherte WLAN mit der SSID 'PUBLIC' ein. Diese SSID ist statisch auf die VLAN-ID '99' gebunden und leitet die Gäste so in ein bestimmtes Netzwerk. Statische und dynamische VLAN-Zuweisung können also sehr elegant parallel genutzt werden.



Die Zuweisung der VLAN-ID kann im RADIUS-Server auch anhand von anderen Kriterien erfolgen, z. B. über die Kombination aus Benutzername und Kennwort.



Alternativ zu einem externen RADIUS-Server kann den WLAN-Clients auch über den internen RADIUS-Server oder die Stationstabelle im LANCOM WLAN Controller eine VLAN-ID zugewiesen werden ('Stationstabelle (ACL-Tabelle)').



- 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').
- ② Für eine Authentifizierung über RADIUS wählen Sie in den Verschlüsselungseinstellungen für das logische WLAN-Netzwerk des Profils eine Einstellung, die eine Authentifizierungsanfrage über IEEE 802.1x auslöst, idealerweise '802.11i (WPA)-802.1x'.
- 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. Alternativ können die Access Points auch direkt mit dem RADIUS-Server kommunizieren, wenn die Informationen über die RADIUS-Server entsprechend konfiguriert wurden ('RADIUS-Server' → Seite 75).

- 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 **LCOS-Menübaum ▶ Setup ▶ RADIUS ▶ Server ▶ Weiterleit-Server**. Stellen Sie außerdem den Standard-Realm sowie den leeren Realm ein, um auf unterschiedliche Benutzerinformationen (mit unbekanntem oder ganz ohne Realm) gezielt reagieren zu können ('Konfiguration für das RADIUS-Forwarding' → Seite 111).
- 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 in der Dokumentation Ihres RADIUS-Servers.

4.3.8 Virtualisierung und Gastzugang über LANCOM WLAN Controller

In vielen Unternehmen ist es erwünscht, den Besuchern für die mitgebrachten Notebooks o. ä. einen Internetzugang über WLAN anzubieten. In einem größeren Netzwerk mit mehreren Access Points kann die Konfiguration der nötigen Einstellungen zentral im WLAN Controller erfolgen.

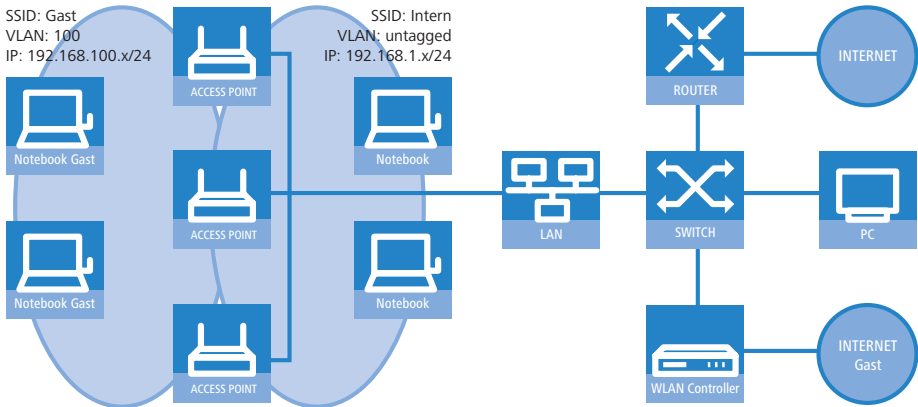
Ziele

- Nutzung der WLAN-Infrastruktur für interne Mitarbeiter und Gäste
- Nutzung der gleichen physikalischen Komponenten (Kabel, Switche, Access Points)
- Trennung der Netzwerke über VLAN und ARF
- Auskopplung der Datenströme zu bestimmten Zielnetzwerken:
 - Gäste: nur Internet
 - Interne Mitarbeiter: Internet sowie alle lokalen Geräte und Dienste
- Gäste melden sich über ein Webformular am WLAN an.
- Interne Mitarbeiter nutzen die WLAN-Verschlüsselung zur Authentifizierung.

Aufbau

- Die Verwaltung der Access Points erfolgt zentral über den LANCOM WLC.

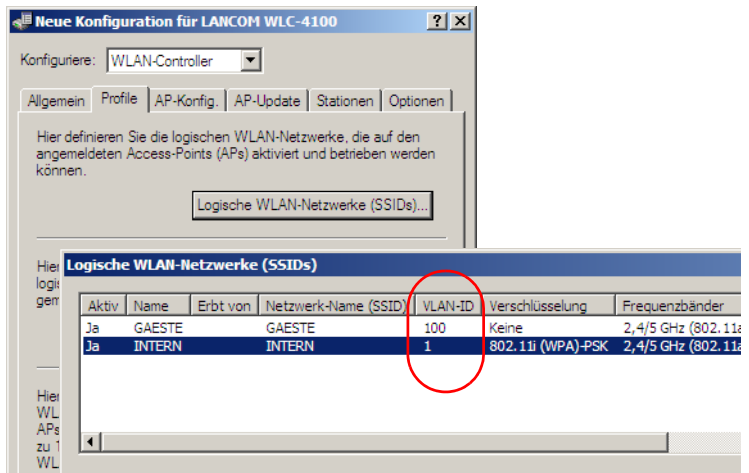
- Der LANCOM WLC dient als DHCP Server für die WLAN-Clients des Gastnetzes.
- Für das Gastnetz wird der Internetzugang vom LANCOM WLC (z. B. separater DSL Zugang oder Internetzugang über Firmen DMZ) bereitgestellt.
- Die kabelgebundene Infrastruktur basiert auf gemanagten VLAN fähigen Switches:
 - Das VLAN-Management der Access Points erfolgt über den LANCOM WLC.
 - Das VLAN-Management der Switches erfolgt separat über die Switch Konfiguration.
- Die Access Points werden innerhalb des internen VLANs betrieben.



WLAN-Konfiguration des WLAN Controllers

Bei der WLAN-Konfiguration werden die benötigten WLAN-Netzwerke definiert und zusammen mit den physikalischen WLAN-Einstellungen den vom Controller verwalteten Access Points zugewiesen.

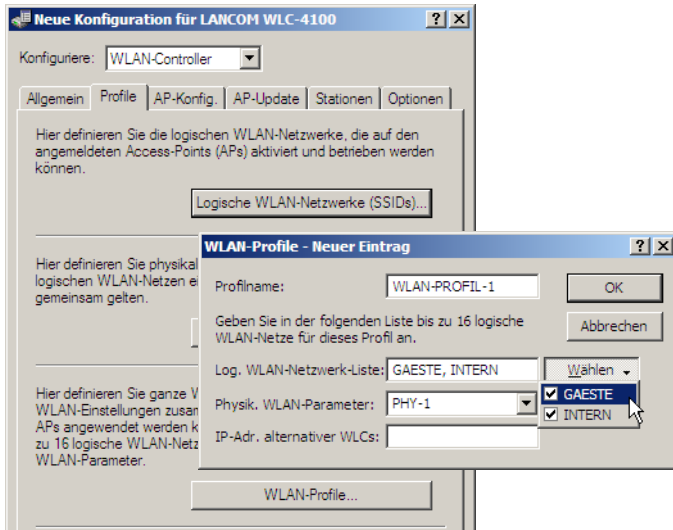
- ① Erstellen Sie ein logisches WLAN für die Gäste und eins für die internen Mitarbeiter:
 - Das WLAN mit der SSID 'GAESTE' nutzt die VLAN-ID '100', hier wird keine Verschlüsselung verwendet.
 - Das WLAN mit der SSID 'INTERN' nutzt die VLAN-ID '1' (wird ohne VLAN-Tag in das Ethernet übertragen), hier wird eine Verschlüsselung nach WPA verwendet.



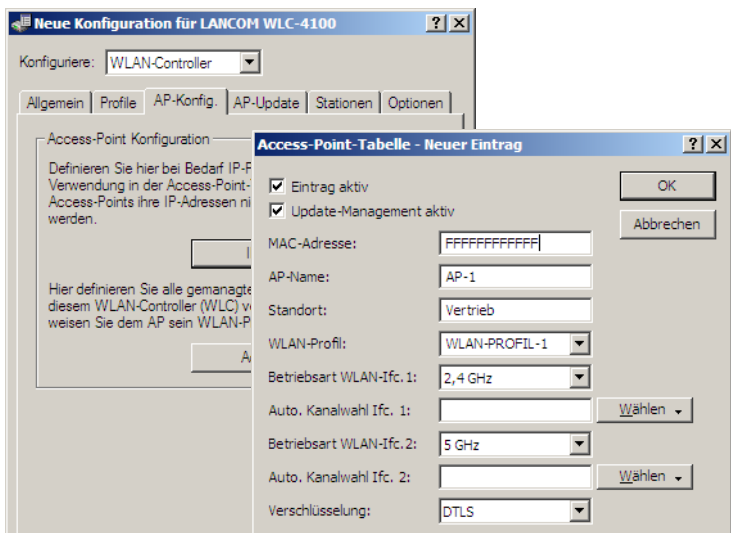
- ② Erstellen Sie einen Satz von physikalischen Parametern für die verwendeten Access Points. Dabei wird die Management-VLAN-ID auf '1' gesetzt, um die VLAN-Nutzung generell zu aktivieren (jedoch ohne separates Management-VLAN für das Gerät, der Management-Datenverkehr wird untagged übertragen).



- ③ Erstellen Sie ein WLAN-Profil, das den Access Points zugewiesen werden kann. In diesem WLAN-Profil werden die beiden zuvor erstellten logischen WLAN-Netzwerke und der zuvor erstellte Satz von physikalischen Parametern zusammengefasst.



- ④ Ordnen Sie das WLAN-Profil den vom Controller verwalteten Access Points zu. Tragen Sie dazu entweder die einzelnen Access Points mit der MAC-Adresse ein oder nutzen Sie alternativ das Default-Profil.



Konfiguration des Switches

Die Konfiguration des Switches wird am Beispiel des LANCOM ES-2126+ vorgestellt.

- ① Stellen Sie den VLAN-Modus auf 'Tag-based' ein, da die Zuweisung der VLAN-Tags durch die Access Points erfolgt.

VLAN Mode

VLAN Mode	Tag-based
Symmetric Vlan	Enable
SVL	Disable
Double Tag	Disable
Up-Link Port	26 Port

Apply

- ② Zur Unterscheidung der VLANs im Switch werden zwei Gruppen verwendet. Das interne Netz für die Mitarbeiter wird in der Default-Gruppe abgebildet, für die Gäste wird eine eigene Gruppe eingerichtet. Dabei werden jeweils die VLAN-IDs verwendet, die auch schon bei der Konfiguration der VLANs im Controller eingetragen wurden.

Tag-based Group

No	VLAN NAME	VID
1	default	1
2	Gaeste	100

- ③ Das Default-VLAN gilt dabei auf allen Ports und wird ungetaggt betrieben, d. h. die VLAN-Tags werden aus den ausgehenden Datenpaketen dieser Gruppe entfernt.

Tag-based Group

No	VLAN NAME	VID
1	default	1
2	Gaeste	100

VLAN name: default
 VID: 1
 GVRP Propagation: Enable

Member	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

- ④ Die VLAN-Gruppe für die Gäste verwendet die VLAN-ID '100' und gilt nur auf den Ports, an denen der WLAN-Controller und die Access Points angeschlossen sind (in diesem Beispiel die Ports 10 bis 16). Bei ausgehenden Datenpaketen werden die Tags nicht entfernt.

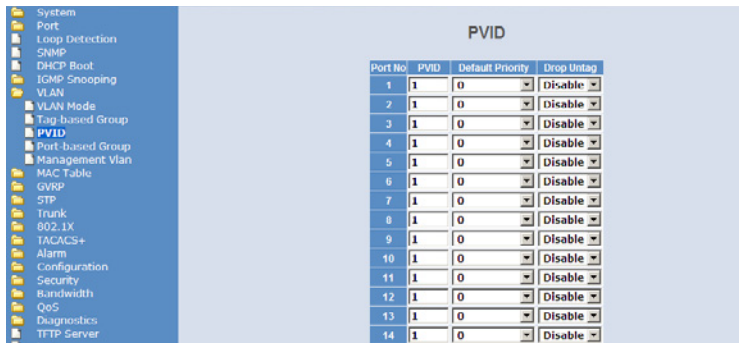
Tag-based Group

No	VLAN NAME	VID
1	default	1
2	Gaeste	100

VLAN name: Gaeste
 VID: 100
 GVRP Propagation: Disable

Member	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

- ⑤ Die Port VLAN ID (PVID) wird für alle Ports auf '1' gestellt, um die Ports dem internen Netz zuzuordnen. Ungetaggt eingehende Pakete werden auf diesen Ports also mit der VLAN-ID '1' weitergeleitet.



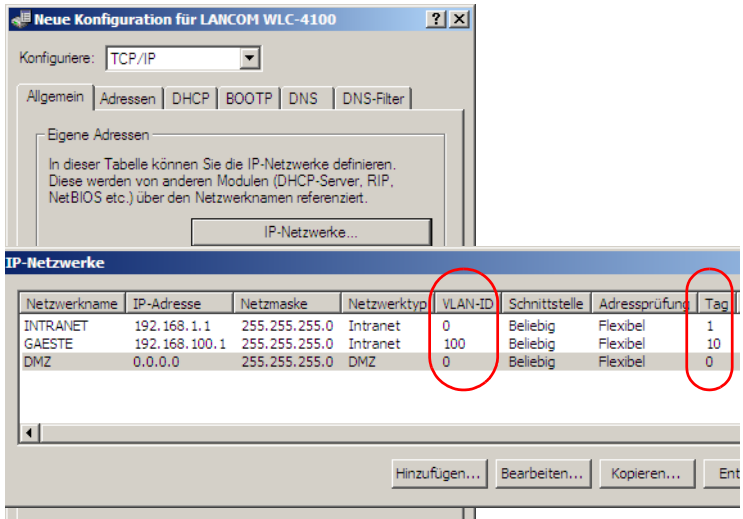
The screenshot shows the configuration interface for a LANCOM WLAN Controller. On the left is a navigation tree with categories like System, Port, Loop Detection, SWMP, DHCP, IGMP Snooping, VLAN, VLAN Mode, Tag-based Group, PVID, Port-based Group, Management VLAN, MAC Table, GVRP, STP, Trunk, 802.1X, TAGS+, Alarm, Configuration, Security, Bandwidth, QoS, Diagnostics, and TFTP Server. The 'PVID' category is selected, and the configuration table is displayed on the right.

Port No	PVID	Default Priority	Drop Untag
1	1	0	Disable
2	1	0	Disable
3	1	0	Disable
4	1	0	Disable
5	1	0	Disable
6	1	0	Disable
7	1	0	Disable
8	1	0	Disable
9	1	0	Disable
10	1	0	Disable
11	1	0	Disable
12	1	0	Disable
13	1	0	Disable
14	1	0	Disable

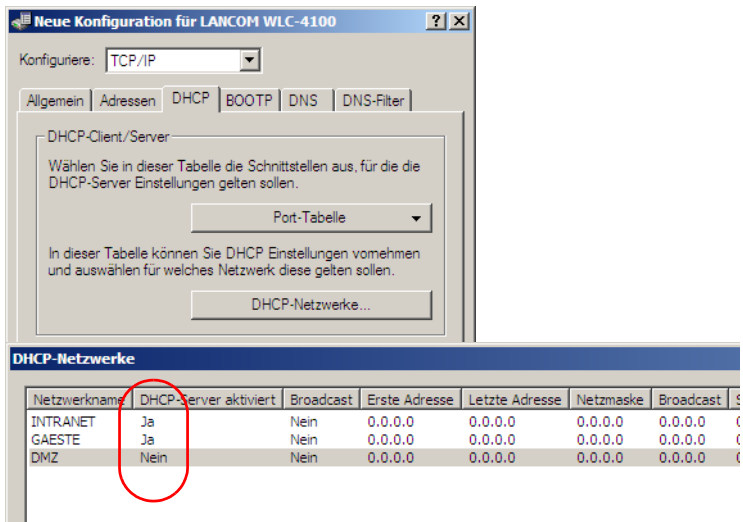
Konfiguration der IP-Netzwerke im WLAN Controller

Für die Trennung der Datenströme auf Layer 3 werden zwei verschiedene IP-Netzwerke verwendet (ARF – Advanced Routing and Forwarding).

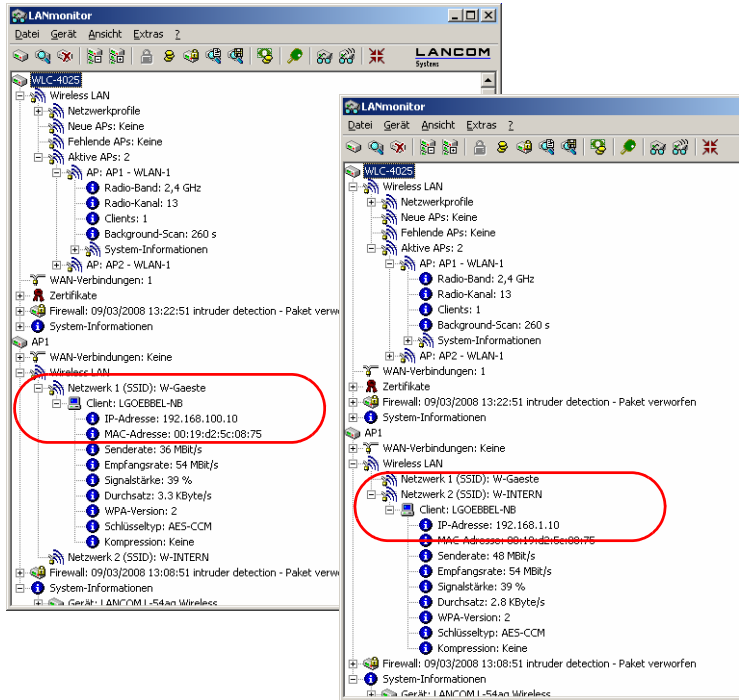
- ① Im ersten Schritt werden die benötigten IP-Netzwerke definiert.
 - Stellen Sie für das interne Netzwerk das 'Intranet' auf die Adresse '192.168.1.1' ein. Dieses IP-Netzwerk verwendet die VLAN-ID '0', damit werden alle ungetaggten Datenpakete diesem Netzwerk zugeordnet (das VLAN-Modul des Controllers selbst muss dazu deaktiviert sein). Das Schnittstellen-Tag '1' wird für die spätere Auskopplung der Daten im virtuellen Router verwendet.
 - Legen Sie für die Gäste ein neues IP-Netzwerk mit der Adresse '192.168.100.1' an. Dieses Netzwerk verwendet die VLAN-ID '100', damit werden alle Datenpakete mit dieser ID dem Gäste-Netzwerk zugeordnet. Auch hier dient das Schnittstellen-Tag '10' der späteren Verwendung im virtuellen Router.



- ② Für beide IP-Netzwerke wird ein Eintrag bei den DHCP-Netzwerken angelegt, mit dem der DHCP-Server fest eingeschaltet wird.



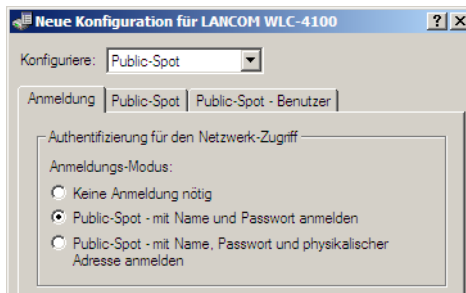
- ③ Mit diesen Einstellungen können die WLAN-Clients der internen Mitarbeiter und der Gäste gezielt den jeweiligen Netzwerken zugeordnet werden.



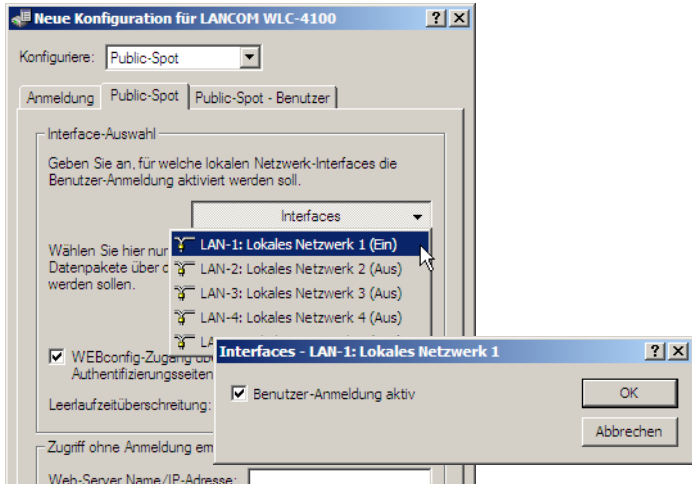
Konfiguration der Public-Spot-Zugänge

Mit dem Public Spot bieten Sie einen kontrollierten Zugriffspunkt auf Ihr WLAN. Die Authentifizierung erfolgt über ein Webinterface mittels Benutzerabfrage. Bei Bedarf kann der Zugang zeitlich begrenzt werden.

- ① Aktivieren Sie die Authentifizierung für den Netzwerk-Zugriff mit Benutzername und Passwort.



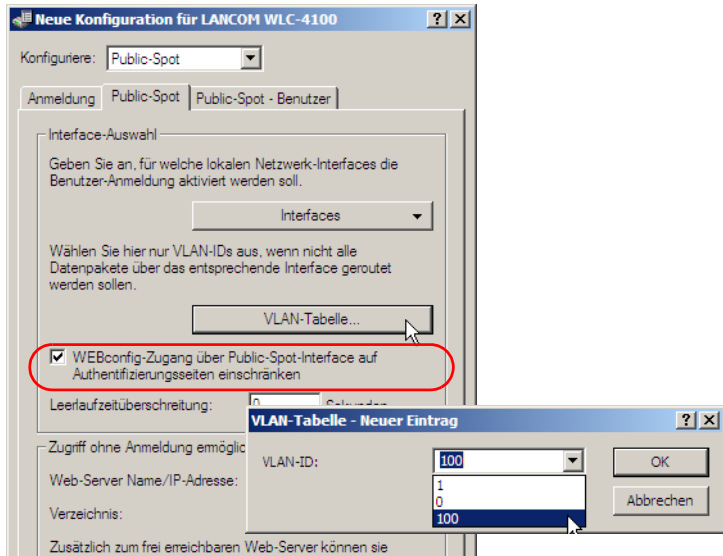
- ② Schalten Sie die Benutzeranmeldung für das Interface des Controllers ein, über das er mit dem Switch verbunden ist.



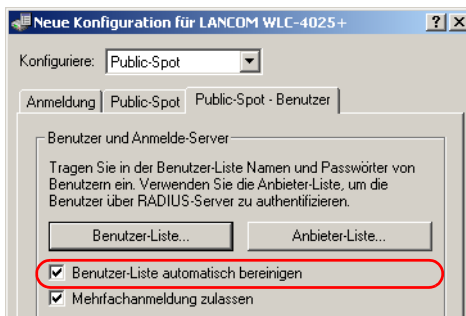
- ③ Mit dem Eintrag der VLAN-ID '100' für das Gästernetzwerk in der VLAN-Tabelle wird die Public-Spot-Verwendung auf Datenpakete aus diesem virtuellen LAN eingeschränkt. Alle Datenpakete aus anderen VLANs werden ohne Anmeldung am Public Spot weitergeleitet. Achten Sie dabei auch darauf, dass der WEBconfig-Zugang über das Public-Spot-Interface auf die Authentifizierungsseiten beschränkt ist und das HTTP in den Konfigurationsprotokollen aktiviert ist.



Ohne die Einschränkung des Interfaces auf die VLAN-ID ist der Controller auf dem angegebenen physikalischen Ethernet-Port nicht mehr erreichbar!



- ④ Aktivieren Sie im Public-Spot-Modul die Option zum Bereinigen der Benutzer-Liste, damit die nicht mehr benötigten Einträge automatisch gelöscht werden können.

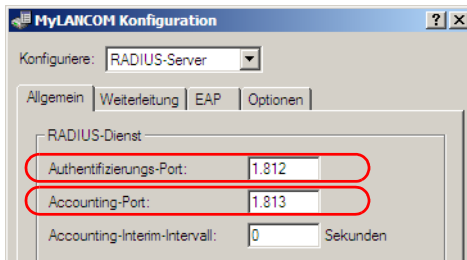


RADIUS-Server für Public-Spot-Nutzung konfigurieren

In den LCOS-Versionen vor 7.70 wurden Public-Spot-Zugänge über den Assistenten in der Benutzer-Liste des Public-Spot-Moduls eingetragen. Ab der LCOS-Version 7.70 speichert der Assistent die Public-Spot-Zugänge nicht mehr in dieser Liste, sondern in der Benutzerdatenbank des internen RADIUS-Servers. Um diese Public-Spot-Zugänge nutzen zu können, **muss** der RADIUS-

Server konfiguriert und das Public-Spot-Modul auf die Nutzung des RADIUS-Servers eingestellt sein.

- ① Damit die Benutzer-Datenbank im internen RADIUS-Server genutzt werden kann, muss der RADIUS-Server im LANCOM zunächst eingeschaltet werden. Aktivieren Sie den RADIUS-Server durch das Eintragen von Authentifizierungs- und Accounting-Port. Verwenden Sie den Authentifizierungs-Port 1.812 und den Accounting-Port 1.813.



- ② Damit die Public-Spot-Zugänge am internen RADIUS-Server des LANCOMs authentifiziert werden können, muss der Public-Spot die Adresse des RADIUS-Servers kennen. Erstellen Sie dazu für den internen RADIUS-Server einen neuen Eintrag als "Anbieter". Tragen Sie die IP-Adresse des LANCOMs, in dem der RADIUS-Server aktiviert wurde, als Authentifizierungs- und Accounting-Server ein.

! Wenn der Public-Spot und der RADIUS-Server vom gleichen LANCOM bereitgestellt werden, tragen Sie hier die interne Loopback-Adresse des Geräts (127.0.0.1) ein.

- ③ Übernehmen Sie Authentifizierungs- und Accounting-Port von der Einstellung im RADIUS-Server (1.812 und 1.813).

The screenshot shows a configuration window titled "Anbieter-Liste - Neuer Eintrag". It contains the following fields and values:

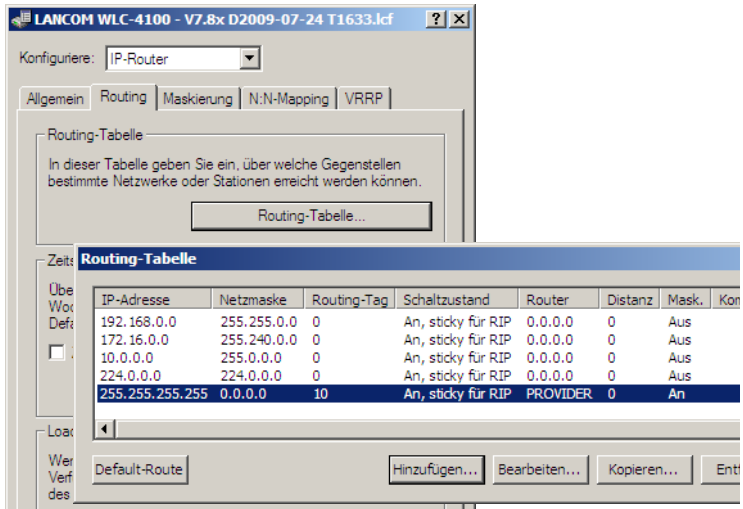
- Anbieter: RADIUS-INTERN
- Backup-Anbieter: (empty)
- Authentifizierungs-Server:
 - Auth.-Server IP-Adresse: 127.0.0.1
 - Auth.-Server Port: 1.812
 - Auth.-Server Schlüssel: (empty)
 - Absende-IP-Adresse: (empty)
- Accounting-Server:
 - Acc.-Server IP-Adresse: 127.0.0.1
 - Acc.-Server Port: 1.813
 - Acc.-Server Schlüssel: (empty)
 - Absende-IP-Adresse: (empty)



Nach einem Update auf LCOS 7.70 sind die mit der vorherigen LCOS-Version angelegten Benutzerkonten in der Benutzer-Liste des Public-Spot-Moduls weiterhin gültig.

Konfiguration des Internetzugangs für das Gästernetzwerk

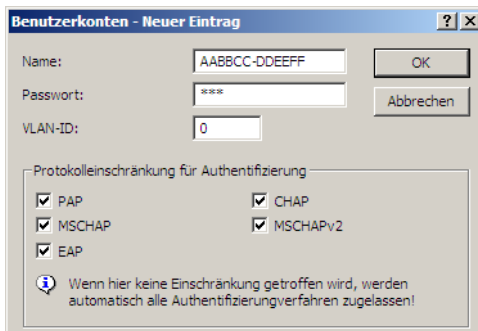
- ① Um den Benutzern des Gast-Netzes einen Internetzugang bereitzustellen, wird z. B. über den Assistenten ein Zugang zum Providernetz angelegt.
- ② Damit dieser Zugang nur für die Benutzer im Gästernetzwerk zur Verfügung steht, wird die entsprechende Route auf das Routing-Tag '10' eingestellt. Damit können nur Datenpakete aus dem IP-Netzwerk 'GAESTE' mit dem Schnittstellen-Tag '10' in das Netz des Providers übertragen werden. Das Routing zwischen dem Gäste-Netzwerk und dem internen Netzwerk ist aufgrund der unterschiedlichen Routing-Tags ausgeschlossen.



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 **LCOS-Menübaum ▶ Setup ▶ RADIUS ▶ Server ▶ Benutzer**.



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

Benutzer	
Benutzername	AABBCC-DDEEFF (max. 48 Zeichen)
Rufende-Station-Id-Maske	(max. 64 Zeichen)
Gerufene-Station-Id-Maske	(max. 64 Zeichen)
Passwort	(max. 32 Zeichen)
(Wiederholen) Passwort	(max. 32 Zeichen)
Mehrfach-Logins	ja
Ablauf-Typ	<input type="checkbox"/> absolut <input type="checkbox"/> relativ
Abs.-Ablauf	(max. 20 Zeichen)
Rel.-Ablauf	0 (max. 10 Zeichen)
Zeit-Risicet	0 (max. 10 Zeichen)

4.3.10 Interner und externer RADIUS-Server kombiniert

Für die Authentifizierung der internen WLAN-Benutzer mit IEEE 802.1x wird in manchen Unternehmen ein externer RADIUS-Server eingesetzt. In einer Anwendung mit einem WLAN Controller und mehreren Access Points fungiert zunächst der WLAN Controller als RADIUS-Server für alle Access Points. Im WLAN Controller wird dazu die entsprechende Weiterleitung der RADIUS-Anfragen an den externen RADIUS-Server definiert.



Die im folgenden beschriebenen Einstellungen sind nur dann notwendig, wenn Sie neben dem Public Spot im LANCOM einen externen RADIUS-Server nutzen.

Im Zusammenhang mit einem Public Spot für Gast-Zugänge sind weitere Einstellungen notwendig:

- Die Authentifizierungsanfragen der internen Mitarbeiter sollen an den externen RADIUS-Server weitergeleitet werden.
- Die Authentifizierungsanfragen der Public-Spot-Zugänge sollen vom internen RADIUS-Server geprüft werden.

Realm-Tagging für das RADIUS-Forwarding

Die Authentifizierungsanfragen der beiden Benutzergruppen müssen separat behandelt werden. Damit der WLAN Controller diese beiden Gruppen unterscheiden kann, werden so genannte "Realms" eingesetzt. Realms dienen der Adressierung von Domänen, innerhalb derer Benutzeraccounts gültig sind. Die Realms können mit der Authentifizierungsanfrage an den RADIUS-Server

im WLAN Controller übermittelt werden. Alternativ kann der RADIUS-Server nach folgenden Regeln die Realms der Benutzernamen verändern, um das RADIUS-Forwarding zu steuern:

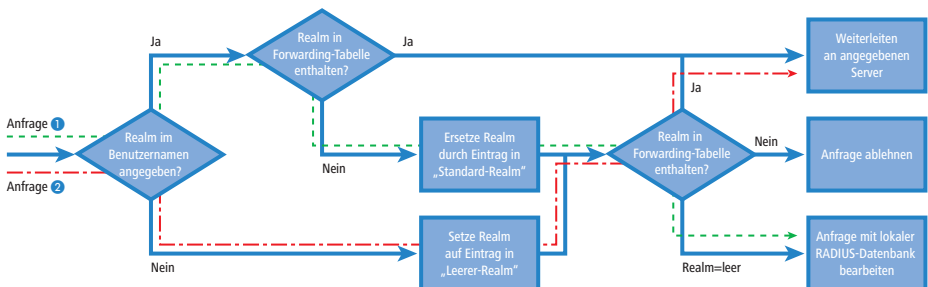
- Der als "Standard-Realm" definierte Wert ersetzt einen vorhandenen Realm einer eingehenden Anfrage, wenn für diesen Realm keine Weiterleitung definiert ist.
- Der unter "Leerer-Realm" definierte Wert wird **nur dann** verwendet, wenn der eingehende Benutzername **noch keinen** Realm enthält.

Über einen Eintrag in der Weiterleitungstabelle können alle Authentifizierungsanfragen mit einem bestimmten Realm an einen RADIUS-Server weitergeleitet werden. Wenn in der Weiterleitungstabelle kein passender Eintrag vorhanden ist, wird die Anfrage abgelehnt.



Wenn nach der Ermittlung eines Realms ein leerer Realm festgestellt wird, so wird die Authentifizierungsanfrage **immer** mit der internen RADIUS-Datenbank des LANCOMs geprüft.

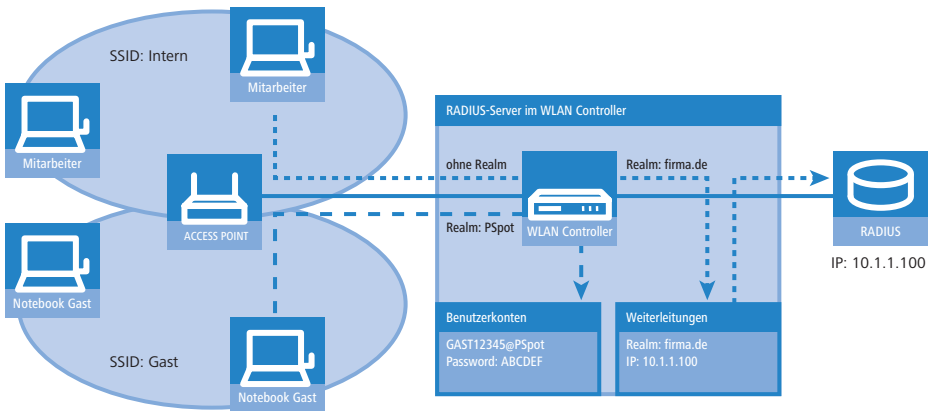
Das folgende Flussdiagramm zeigt schematisch die Arbeitsweise des RADIUS-Server bei der Verarbeitung von Realms:



Durch ein unterschiedliches Realm-Tagging können somit verschiedene RADIUS-Server angesprochen werden. Den Entscheidungsweg im RADIUS-Server des LANCOMs können Sie im Diagramm für die beiden Anfragen verfolgen:

- 1 Da die Benutzernamen für die Gastzugänge automatisch erzeugt werden, wird für diese Benutzernamen der Realm "PSpot" verwendet. Da in der Weiterleitungstabelle kein entsprechender Eintrag vorhanden ist und der Standard-Realm leer ist, werden alle Authentifizierungsanfragen mit diesem Realm an den internen RADIUS-Server weitergeleitet.

- 2 Um den Konfigurationsaufwand zu begrenzen, werden die internen Benutzer weiterhin ohne Realm geführt. Der RADIUS-Server im LANCOM kann einen leeren Realm automatisch durch einen anderen Realm ersetzen, mit dem die internen Benutzer identifiziert werden. In diesem Beispiel wird der leere Realm durch die Domäne der Firma "firma.de" ersetzt. Mit den Angaben in der Weiterleitungstabelle können alle Authentifizierungsanfragen mit diesem Realm an den externen RADIUS-Server weitergeleitet werden.



Konfiguration für das RADIUS-Forwarding

Mit den folgenden Konfigurationsschritten können Sie die separate Behandlung der internen Benutzer und der Gastzugänge definieren.

- 1 Passen Sie im Public Spot das Muster für die Benutzernamen so an, dass ein eindeutiger Realm verwendet wird. Mit dem Muster "GAST%n@Pspot" werden z. B. Benutzernamen der Form "GAST12345@Pspot" erzeugt.

Neue Konfiguration für LANCOM WLC-4025+

Konfigurieren: Public-Spot

Anmeldung | Public-Spot | Public-Spot - Benutzer

Benutzer und Anmelde-Server

Tragen Sie in der Benutzer-Liste Namen und Passwörter von Benutzern ein. Verwenden Sie die Anbieter-Liste, um die Benutzer über RADIUS-Server zu authentifizieren.

Benutzer-Liste... Anbieter-Liste...

Benutzer-Liste automatisch bereinigen
 Mehrfachanmeldung zulassen

Accounting

Update-Zyklus: 0 Sekunden

Benutzer-Erstellungs-Assistent

Public-Spot Benutzerkonten können mit Hilfe des WEBconfig Assistenten auf einfache Weise angelegt werden. Benutzername und Passwort werden automatisch generiert und es folgt eine Seite zum Ausdrucken aller notwendigen Zugangsdaten.

Standard-Laufzeiten...

Muster für Benutzernamen: GAST%n@Pspot

Passwort-Länge: 6

SSID:

- ② Tragen Sie im RADIUS-Server des WLAN Controllers einen "leeren Realm" ein (z. B. "FIRMA.DE"). Dieser Realm wird für alle Benutzernamen verwendet, die ohne Realm eine Authentifizierungsanfrage bei dem WLAN Controller stellen. Das sind in dieser Anwendung die internen Benutzer, für die kein Realm definiert ist. Damit der RADIUS-Server des WLAN Controllers für diese Benutzernamen auch keinen Realm einsetzt, muss der "Standard-Realm" unbedingt leer bleiben.

Neue Konfiguration für LANCOM WLC-4025+

Konfigurieren: RADIUS-Server

Allgemein | Weiterleitung | EAP | Optionen

RADIUS-Weiterleitungs-Server

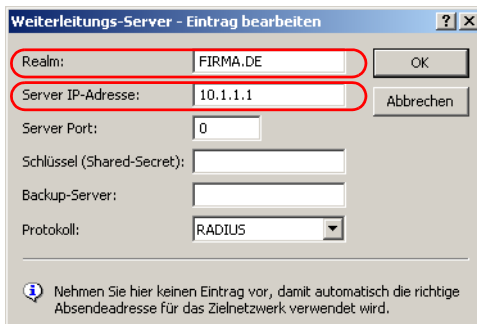
Wenn Sie RADIUS-Weiterleitung nutzen möchten, müssen Sie hier weitere Angaben machen.

Weiterleitungs-Server...

Standard-Realm:

Leerer Realm: FIRMA.DE

- ③ Damit die Authentifizierungsanfragen der internen Benutzer an den externen RADIUS-Server weitergeleitet werden, legen Sie einen passenden Eintrag bei den Weiterleitungen an. Mit dem Realm "FIRMA.DE" werden alle eingehenden RADIUS-Anfragen an die angegebene IP-Adresse weitergeleitet, die über diesen Realm verfügen.



Weiterleitungs-Server - Eintrag bearbeiten

Realm: FIRMA.DE OK


Server IP-Adresse: 10.1.1.1 Abbrechen

Server Port: 0

Schlüssel (Shared-Secret):

Backup-Server:

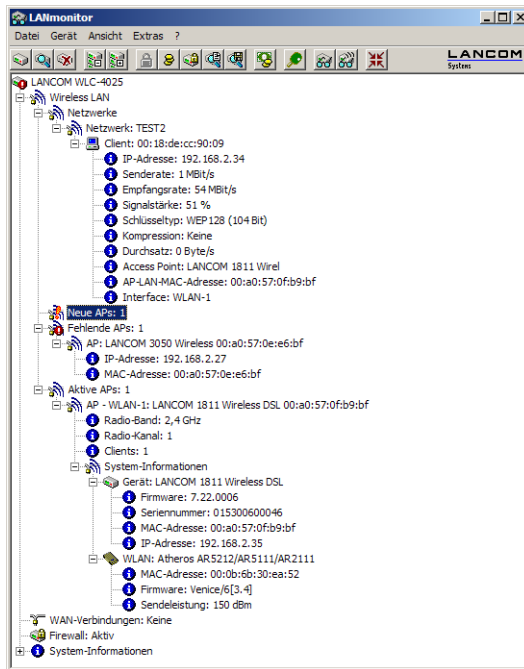
Protokoll: RADIUS

 Nehmen Sie hier keinen Eintrag vor, damit automatisch die richtige Absendeadresse für das Zielnetzwerk verwendet wird.

- ④ Die Authentifizierungsanfragen der Public-Spot-Benutzer gehen mit dem Realm "@PSpot" beim WLAN Controller ein. Da für diesen Realm keine Weiterleitung definiert ist, werden die Benutzernamen automatisch in der internen RADIUS-Datenbank geprüft. Da die über den Assistenten angelegten Public-Spot-Zugänge in dieser Datenbank gespeichert werden, können diese Anfragen wie gewünscht authentifiziert 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:



- 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:

■ **Neuen 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').

■ **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 Automatische Funkfeldoptimierung mit LANCOM WLAN Controllern

DE

Mit der Auswahl des Kanals in der Kanal-Liste wird der Teil des Frequenzbandes festgelegt, den ein Access Point für seine physikalischen WLANs verwendet. Alle WLAN-Clients, die sich mit einem Access Point verbinden wollen, müssen den gleichen Kanal im gleichen Frequenzband verwenden. Im 2.4 GHz-Band stehen je nach Land die Kanäle 1 bis 13, im 5 GHz-Band die Kanäle 36 bis 64 zur Verfügung. Auf einem Kanal kann dabei zeitgleich jeweils nur ein Access Point Daten übertragen. Um in der Funkreichweite eines anderen Access Points ein WLAN mit maximaler Bandbreite betreiben zu können, muss jeder Access Point einen separaten Kanal nutzen – anderenfalls müssen sich die WLANs die Bandbreite des Kanals teilen.



Bei einer völlig offenen Kanalliste werden die Access Points möglicherweise automatisch Kanäle wählen, die sich gegenseitig teilweise überlappen und so die Signalqualität reduzieren. Außerdem könnten die Access Point evtl. Kanäle wählen, welche die WLAN-Clients aufgrund der Ländereinstellung nicht nutzen können. Um die Access Points gezielt auf bestimmte Kanäle zu leiten, können z. B. die überlappungsfreien Kanäle 1, 6, 11 in der Kanalliste aktiviert werden.

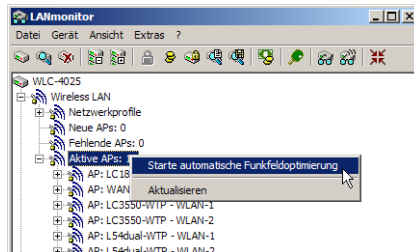
In größeren Installationen mit mehreren Access Points ist es manchmal schwierig, für jeden Access Point einen geeigneten Kanal einzustellen. Mit der automatischen Funkfeldoptimierung bieten die LANCOM WLAN Controller ein Verfahren, um die optimalen Kanäle der Access Points für das 2.4 GHz-Band automatisch einzustellen.

WEBconfig: **Setup ▶ WLAN-Management ▶ Start-automatic-radio-field-optimization**



Die Optimierung kann auch gezielt für einen einzelnen Access Point gestartet werden, indem die MAC-Adresse als Parameter für die Aktion eingetragen wird.

LANmonitor: Klick mit der rechten Maustaste auf die Liste der aktiven Access Points oder auf ein bestimmtes Gerät, dann im Kontextmenü **Starte automatische Funkfeldoptimierung** wählen.



Die Optimierung läuft dann in den folgenden Schritten ab:

- ① Der WLAN Controller löscht die AP-Kanalliste aller Access Points im 2.4 GHz-Bereich. Da die Kanalliste der Access Points dann leer ist, wird ihnen über ein Konfigurations-Update die Kanalliste ihres Profils zugewiesen.
- ② Der WLAN Controller schaltet alle Funkmodule im 2.4 GHz-Bereich aus.
- ③ Die Access Points werden nacheinander eingeschaltet. Dabei werden sie in der Reihenfolge bearbeitet, in der sie sich beim WLAN Controller angemeldet haben.
- ④ Automatische Einmessung: Nach dem Einschalten sucht sich der Access Point selbständig den für ihn besten Kanal aus der Kanalliste. Zur Bestimmung des am besten geeigneten Kanals führt der Access Point jeweils eine Interferenz-Messung durch, so dass die Signalstärken und Kanäle anderer Access Points entsprechend berücksichtigt werden. Da die bisherige Liste in der Konfiguration des WLAN Controllers gelöscht wurde, ist dies nun die Profilkannalliste. Wenn die Profilkannalliste leer ist, hat der Access Point die freie Auswahl aus den nicht durch andere Funk-Module belegten Kanälen.
- ⑤ Der gefundene Kanal wird zurück an den WLAN Controller gesendet und dort in der AP-Kanalliste gespeichert. Deswegen erhält der Access Point beim nächsten Verbindungsaufbau wieder diesen Kanal. Die AP-Kanalliste hat so gesehen ein höheres Gewicht als die Profilkannalliste.



Verfügt ein Access Point über mehrere WLAN-Module, so wird dieser Vorgang für jedes WLAN-Modul nacheinander ausgeführt.

4.6 Konfiguration der Access Points

Bitte beachten Sie, dass die Access Points über eine IP-Adresse verfügen müssen, um mit dem WLAN Controller in Kontakt zu treten. Die IP-Adresse kann entweder fest im Access Point eingetragen sein oder über einen DHCP-Server zugewiesen werden.



Wenn der Access Point die IP-Adresse von einem DHCP-Server bezieht und dieser DHCP-Server nicht erreichbar ist, hat der Access Point nach einem Neustart evtl. keine IP-Adresse mehr und kann nicht mit dem WLAN Controller kommunizieren.

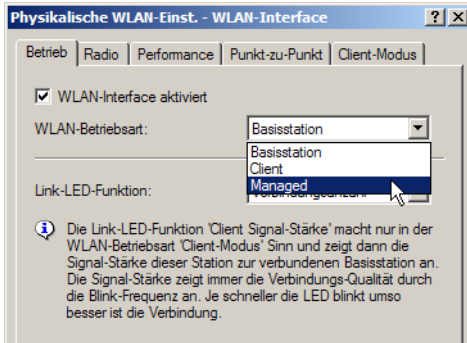
Ab der Firmware-Version LCOS 7.20 unterscheiden sich LANCOM Access Points (z. B. LANCOM L-54ag) und LANCOM Wireless Router (z. B. LANCOM 1811 Wireless) bzgl. der Einstellung der WLAN-Module im Auslieferungszustand.

- 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

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.



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

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:

- Verschlüsselung des Datentransfers (802.11i/WPA)
- 802.1x / EAP
- LANCOM Enhanced Passphrase Security (LEPS)
- Zugangskontrolle über MAC-Adresse
- Optionales IPSec-over-WLAN VPN

5.1.1 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.



LANCOM Systems empfiehlt für den Passphrase-Betrieb den Einsatz von 802.11i (WPA2) in Verbindung mit AES als sicherste Passphrase-Variante. Der Schlüssel sollte zufällig aus einem großen Zeichenbereich gewählt und möglichst lang (32 bis 63 Zeichen) sein. Hiermit können Wörterbuchattacken vermieden werden.

- 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.

- Die Passphrases für 802.11i oder WPA müssen nicht so häufig 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 Sie aus Gründen der Kompatibilität zu älteren WLAN-Clients WEP verwenden, ändern Sie regelmäßig die WEP-Schlüssel in Ihrem Access Point und schränken Sie diese Clients wenn möglich auf eine separate SSID mit Zuweisung eines VLANs ein, für das niedrige Sicherheitsansprüche ausreichen.
- 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 120) oder aber eine zusätzliche Verschlüsselung der WLAN-Verbindung einrichten, wie sie auch für VPN-Tunnel verwendet wird ('IPSec-over-WLAN' → Seite 121). 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.

5.1.2 802.1x / 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) verwaltet und von dem Access Point bei Bedarf von dort abgerufen werden. Das dynamisch erzeugte und kryptografisch sichere Schlüsselmaterial für 802.11i (WPA1/2) ersetzt dabei die manuelle Schlüsselverwaltung.

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

5.1.3 LANCOM Enhanced Passphrase Security

Mit LEPS (**LANCOM Enhanced Passphrase Security**) hat LANCOM Systems ein effizientes Verfahren entwickelt, das die einfache Konfigurierbarkeit von IEEE

802.11i mit Passphrase nutzt und dabei die möglichen Fehlerquellen beim Verteilen der Passphrase vermeidet. Bei LEPS wird jeder MAC-Adresse in einer zusätzlichen Spalte der ACL eine individuelle Passphrase zugeordnet – eine beliebige Folge aus 4 bis 64 ASCII-Zeichen. Nur die Verbindung von Passphrase und MAC-Adresse erlaubt die Anmeldung am Access Point und die anschließende Verschlüsselung per IEEE 802.11i oder WPA.

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

5.1.4 Zugangskontrolle über MAC-Adresse

Jedes Netzwerkgerät verfügt über eine unverwechselbare Identifizierungsnummer. Diese Identifizierungsnummer wird als MAC-Adresse (**Media Access Control**) bezeichnet und ist weltweit einmalig.

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

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

5.1.5 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 Standortkoppelung an. Für andere Betriebssysteme existiert Clientsoftware von Fremdherstellern.

5.2 Tipps für den richtigen Umgang mit Schlüsseln und Passphrasen

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

■ Halten Sie Schlüssel so geheim wie möglich.

Notieren Sie niemals einen Schlüssel. Liebt, aber völlig ungeeignet sind beispielsweise: Notizbücher, Brieftaschen und Textdateien im Computer. Verraten Sie einen Schlüssel nicht unnötig weiter.

■ Wählen Sie einen zufälligen Schlüssel.

Verwenden Sie zufällige, lange Buchstaben- und Ziffernfolgen (min. 32 bis zu den maximal möglichen 63 Zeichen). 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. Alternativ ermöglicht auch 802.1x die benutzerbezogenen Zugriffsbeschränkungen und das Sperren von kompromittierten Zugangsdaten.

5.3 Der Sicherheits-Assistent

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

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

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

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

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 Auswahlmenü den Setup-Assistenten **Sicherheitseinstellungen kontrollieren** und bestätigen Sie die Auswahl mit **Weiter**.
- ③ In den folgenden Fenstern stellen Sie das Passwort ein und wählen die zulässigen Protokolle für den Konfigurationszugriff von lokalen und entfernten Netzwerken aus.
- ④ In einem weiteren Schritt werden die Parameter der Konfigurationssperre wie Anzahl der Fehllogins und Dauer der Sperre eingestellt.
- ⑤ 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 Netzwerken
- Parameter der Konfigurationssperre (Anzahl der Fehllogins und Dauer der Sperre)

5.4 Die Sicherheits-Checkliste

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



Detaillierte Informationen zu den angesprochenen Sicherheitseinstellungen finden Sie im Referenzhandbuch.

■ Haben Sie das Funknetzwerk durch Verschlüsselung und Zugangskontrolllisten 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.



LANCOM Systems rät aus Sicherheitsgründen von der Verwendung von WEP ab! Setzen Sie WEP nur in begründeten Ausnahmefällen ein und ergänzen Sie die WEP-Verschlüsselung nach Möglichkeit mit anderen Schutzmechanismen!

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 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 Firewall im LANCOM WLAN Controller wird nur genutzt, wenn der WLAN Controller als Public Spot betrieben wird und einen direkten Internetzugang bereitstellt. In der Betriebsart als rein zentrales WLAN-Management wird die Firewall im WLAN Controller nicht genutzt.

Nur für WLAN
Controller als Public
Spot

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



Beachten Sie, dass alle Sicherheitsaspekte der Firewall (inkl. IP-Masquerading, Port-Filter und Zugriffs-Liste) nur für Datenverbindungen aktiv sind, die über den IP-Router geführt werden. Direkte Datenverbindungen über die Bridge werden nicht von der Firewall geschützt!

Nur für WLAN
Controller als Public
Spot

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

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

■ Haben Sie IP-Masquerading aktiviert?

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

■ Haben Sie kritische Ports über Filter geschlossen?

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

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

Mit einer speziellen Filter-Liste kann der Zugriff auf die internen Funktionen der Geräte über TCP/IP eingeschränkt werden. Mit den internen Funktionen werden hierbei Konfigurationssitzungen über LANconfig, WEBconfig, Telnet oder TFTP bezeichnet. Standardmäßig enthält diese Tabelle keine Einträge, damit kann also von Rechnern mit beliebigen IP-Adressen aus über TCP/IP mit Telnet oder TFTP ein Zugriff auf das Gerät gestartet werden. Mit dem ersten Eintrag einer IP-Adresse sowie der zugehörigen Netzmaske wird der Filter aktiviert, und nur noch die in diesem Eintrag enthaltenen IP-Adressen werden berechtigt, die internen

Nur für WLAN
Controller als Public
Spot

Nur für WLAN
Controller als Public
Spot

Funktionen zu nutzen. Mit weiteren Einträgen kann der Kreis der Berechtigten erweitert werden. Die Filter-Einträge können sowohl einzelne Rechner als auch ganze Netze bezeichnen. Die Zugangsliste finden Sie in LANconfig im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Allgemein'.

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

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

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

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

■ **Haben Sie die Speicherung der Konfigurationsdaten Ihren Sicherheitsanforderungen angepasst?**

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

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

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

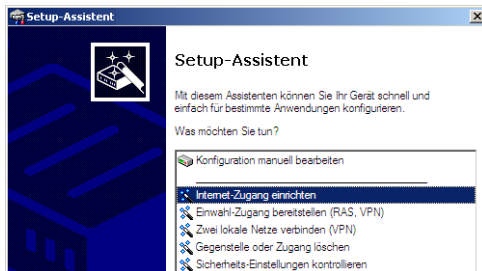
6 Den Internet-Zugang einrichten

LANCOM WLAN Controller enthalten auch Routing- und Firewall-Funktionen, so dass diese auf Wunsch ebenfalls als Internetzugangsroutern eingesetzt werden können.

6.1 Der Internet-Assistent

6.1.1 Anleitung für LANconfig

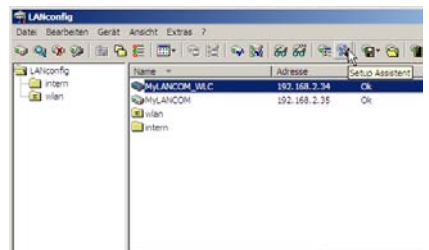
- 1 Markieren Sie Ihr Gerät im Auswahlfenster. Wählen Sie aus der Befehlsleiste den Punkt **Extras ▶ Setup Assistent**.



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

LANconfig: Schneller Aufruf der Setup-Assistenten

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



6.1.2 Anleitung für WEBconfig

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

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 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:

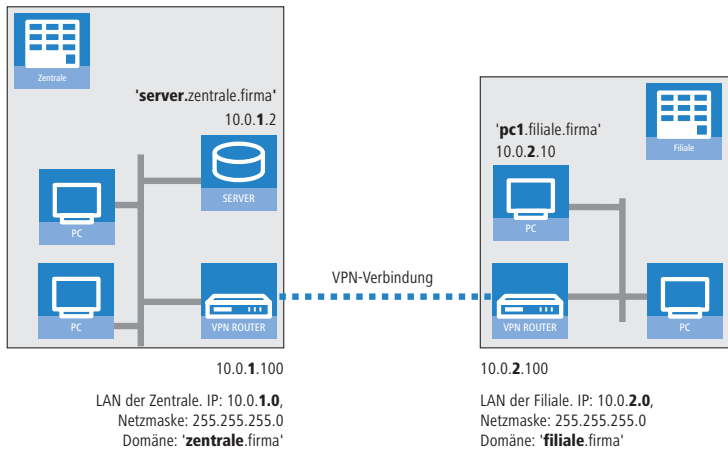
- Für VPN-Verbindungen über das Internet muss der Typ der IP-Adressen auf beiden Seiten angegeben werden. Es gibt zwei **Typen von IP-Adressen**: statische und dynamische. Eine Erklärung zum Unterschied der beiden IP-Adresstypen finden Sie im Referenzhandbuch.

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.

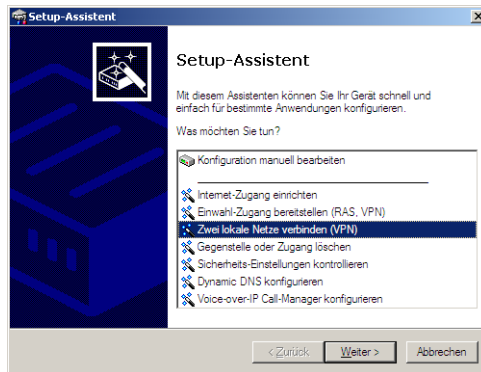


Entfernte Windows-Arbeitsgruppen erscheinen nicht in der Windows-Netzwerkumgebung, sondern können nur direkt (z. B. über die Computer-Suche) angesprochen werden.

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 die 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.

```

C:\>ping 10.0.1.2

Ping wird ausgeführt für 10.0.1.2 mit 32

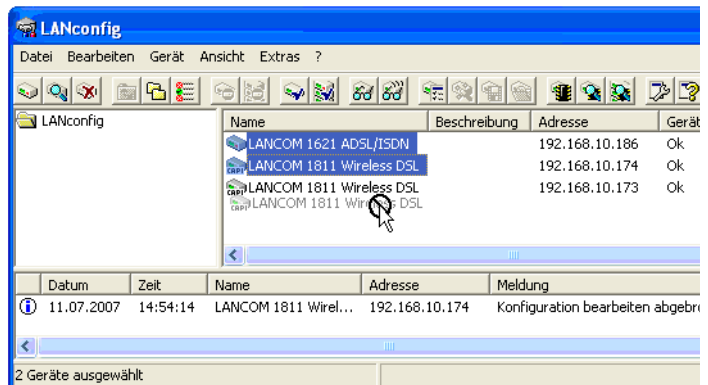
Antwort von 10.0.1.2: Bytes=32 Zeit=10ms
Antwort von 10.0.1.2: Bytes=32 Zeit=20ms
Antwort von 10.0.1.2: Bytes=32 Zeit=10ms
Antwort von 10.0.1.2: Bytes=32 Zeit<10ms

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)

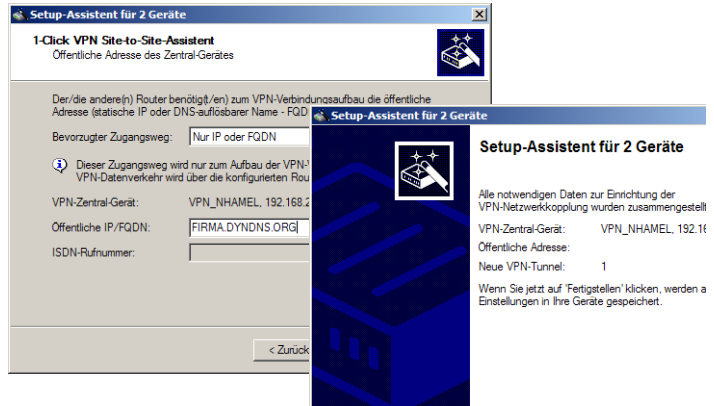
Die Einstellungen für die Kopplung von Netzwerken können sehr komfortabel über den 1-Click-VPN-Assistenten vorgenommen werden. Dabei können sogar mehrere Router gleichzeitig an einen zentralen Netzwerk gekoppelt werden.

- 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.



Kapitel 7: Zwei Netzwerke verbinden

- 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 Namen 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.

- 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?

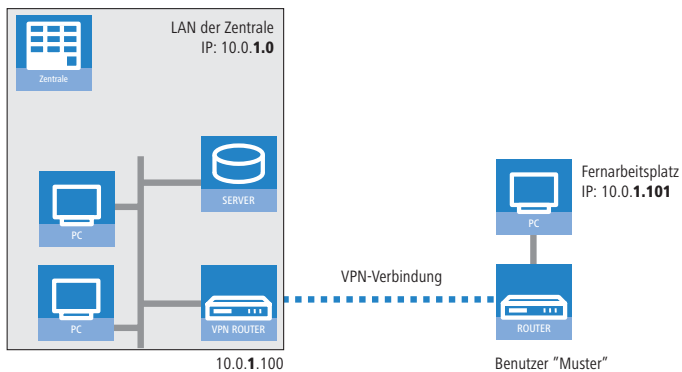
Name einer lokalen Arbeitsgruppe (nur bei NetBIOS)

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:

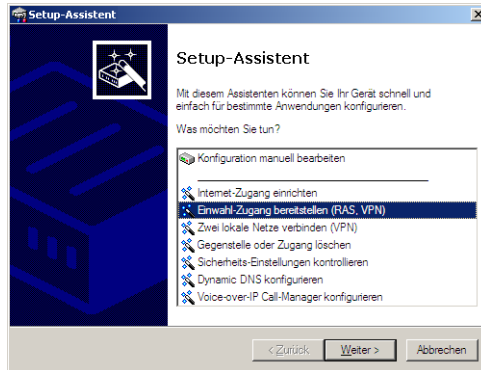
- Einen Zugang zum Internet
- Einen VPN-Client

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 over 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'.

■ Kapitel 8: Einwahl-Zugang bereitstellen

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



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

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

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

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

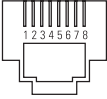
9.1 Leistungs- und Kenndaten

	LANCOM WLC-4006		LANCOM WLC-4025+	LANCOM WLC-4100
Anschlüsse	Ethernet LAN	5x 10/100Base-TX, Auto-sensing, Switch mit Node/Hub Autosensing	4x 10/100/1000Base-TX, Autosensing, Node/Hub Autosensing	
	WAN	Ethernet-Ports können optional als WAN-Anschluss geschaltet werden.		
	USB	USB 2.0 Host Port (Highspeed: 480Mbit/s) zum Anschluss eines USB-Druckers und für zukünftige Erweiterungen		
	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, Netzwerkanschlüsse 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)	
Optionen	<ul style="list-style-type: none"> ■ Erweiterungsoptionen für bis zu 12 gemanagte Access Points 		<ul style="list-style-type: none"> ■ Erweiterungsoptionen für bis zu 100 gemanagte Access Points 	<ul style="list-style-type: none"> ■ Erweiterungsoptionen für bis zu 1000 gemanagte Access Points
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 			
	<ul style="list-style-type: none"> ■ LANCOM Next Business Day Service Extension CPE Art.-Nr. 61411 ■ LANCOM 2-Year Warranty Extension CPE Art.-Nr. 61414 		<ul style="list-style-type: none"> ■ LANCOM Next Business Day Service Extension Central Site Art.-Nr. 61413 ■ LANCOM 2-Year Warranty Extension Central Site Art.-Nr. 61416 	

9.2 Anschlussbelegung

9.2.1 Ethernet-Schnittstelle 10/100/1000Base-TX, DSL-Schnittstelle

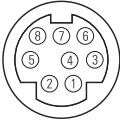
8-polige RJ45-Buchsen, entsprechend ISO 8877, EN 60603-7

Steckverbindung	Pin	Fast Ethernet	Gigabit Ethernet
	1	T+	BI_DA+*
	2	T-	BI_DA-
	3	R+	BI_DB+
	4		BI_DC+
	5		BI_DC-
	6	R-	BI_DB-
	7		BI_DD+
	8		BI_DD-

*BI_DA+ steht für „Bi-directional pair +A“

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

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

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

Index

Numerics

10/100Base-TX	27
100-Mbit-Netz	27
3-DES	130, 138
802.11i	119, 121, 124
802.11i/	120
802.1p	17
802.1x	3, 119, 120

A

Access Control List	121
Access Point	3, 10
Access Point-Modus	21
Access Points manuell akzeptieren	80
ACL	121
Advanced Routing and Forwarding	17
AES	119, 130, 138
Alternative WLAN- Controller	58
Anschlussbelegung	145
LAN-Schnittstelle	145
Outband	145
Anzahl der VPN-Tunnel	25
autark	21
Autarker Weiterbetrieb	17, 53
Authentifizierung	15, 17
Auto-Accept	50
Automatische Annahme neuer Access Points	45
Automatische Annahme neuer APs	49, 50
Automatische Kanalwahl	56
Automatische Zuweisung der Default-Konfiguration	45, 49, 50, 83
Autosensing	27, 30

B

Background-Scanning	3
Blowfish	130, 138
Broadcast	58

C

CA	15
CAPWAP	11, 13, 16, 17
CAPWAP-Tunneling	13
Certification Authority	15
Control And Provisioning of Wireless Access Points	11
CPU-Auslastung	25
Cron-Job	66

D

Datagram Transport Layer Security	11
Datenkanal	11
Datum	25
Default-Gateway	126
Default-Konfiguration	45, 48, 62
DHCP	41
DHCP-Server	18, 33, 41
DiffServ	17
Discovery Request Message	14, 91
DNS	14
DNS-Server	18, 41
Zugriffe ins entfernte LAN	133
Domäne	133
Download	5
DTLS	11, 15, 17, 25
Dynamische VLAN-Zuweisung	17, 92

E

EAP	12, 17, 119, 120
Einwahl-Zugang	138
E-Mail	77
Erwarteter Access Point	48

F

Fast Roaming	18
Fernkonfiguration	35
Firewall	19, 126
Stationen sperren	126

■ Index

FirmSafe	19	Konfigurationszugriff	36
Firmware	5	Konformitätserklärungen	146
zentrale Verwaltung	66	Kontrollkanal	11
Firmwareversion	25	L	
Flash	11, 54	LAN	
G		Anschlusskabel	20
Gebührenschutz	36	LAN-Anschluss	27
Gerätename	25	LANCOM Enhanced Passphrase Security	119
H		LANconfig	31, 35
Hardware-Installation	29	Assistenten aufrufen	128
Hinweis-Symbole	5	LAN-LAN-Kopplung	18, 130
HTTPS	36	erforderliche Angaben	130
I		LANmonitor	31, 80, 113
ICMP	126	Access Point trennen	114
IEEE 802.11n	12	Neuer Access Point zu Profil zuordnen	114
IETF	11	LANtools	
Installation	20	Systemvoraussetzungen	21
Konfigurations-Schnittstelle	30	Layer-3-Roaming	13
LAN	29	LCD-Display	25
Internet-Zugang	18, 128	LED	
IP		Lost-AP	24
Filter	126	New-AP	24
Ports sperren	126	WLAN	24
IP-Adresse	33, 34, 126	LEPS	120
IP-Masquerading	19, 126	Load-Balancing	91
IP-Router	18	Loader	21
IPSec	130, 138	Lost AP-LED	24
IPSec-over-WLAN	119	Lost-AP-LED	81, 82
IPX-Router	17	M	
K		MAC-Filter	108
Kennwort	34, 35	MAC-Funktionen	12
Konfiguration	50	MAC-Prüfung	46
Konfigurationsdatei	127	Managed-Modus	21
Konfigurationskabel	27	Management-VLAN-ID	56
Konfigurationskennwort	125	N	
Konfigurations-Schnittstelle	19	NAT – siehe IP-Masquerading	
Anschlusskabel	20		
Konfigurationsschutz	19, 34		

NetBIOS	133	SIP-Telefon	13
Network Time Protocol	44	Skalierbarkeit	12
Netzmaske	33, 34, 126	Skript	
Netzwerkkopplung	130	zentrale Verwaltung	66
Sicherheitsaspekte	130, 138	Smart Controller	3
Netzwerkname	46	Smart-Controller	11, 12
Neuer Access Point	48	SNMP	
New AP-LED	24	Konfiguration schützen	125
NTP	44	SNTP-Status	25
P		Software-Installation	30
PAT – siehe IP-Masquerading		Speicherauslastung	25
PCKS12-Container	85	Split Management	3
PHY-Layer	12	Split-Management	16
Ping	135	SSID	46, 53
PMK-Caching	18	Standard-Gateway	41
Pre-Authentication	18	Statusanzeigen	
R		Power	22
RADIUS	3, 12, 17, 108, 120	Support	5
RAM	54	SYSLOG	77
Remote-Access-Service (RAS)		Systemvoraussetzungen	20
Benutzername	139	T	
einrichten	138	TCP	126
Einwahl-Rechner konfigurieren	140	TCP/IP	21
NetBIOS	140	Einstellungen	32
Server	18	Verbindung testen	135
TCP/IP	139	TCP/IP-Filter	19, 126
Windows-Arbeitsgruppe suchen	140	TCP/IP-Konfiguration	
Routing-Tabelle	126	manuell	32, 33
S		vollautomatisch	32, 33
SCEP	15, 43	TCP/IP-Router	
SCEP-Status	25	Einstellungen	132
SDSL-Modem	18	Telnet	126
serielles Konfigurationskabel	27	Temperatur	25
Sicherheit		TFTP	126
Schutz der Konfiguration	119	TLS	11
Sicherheits-Checkliste	124	U	
Simple Certificate Encryption Protocol	15,	UDP	126
43		USB-Anschluss	27

■ Index

V

Vererbung	17, 53, 56, 59, 83
Verschlüsselung	17, 46, 64, 78, 130, 138
Virtual Private Network (VPN)	18
VLAN	3
VLAN-ID	53, 93
VPN-Client	140

W

WEBconfig	36
HTTPS	36
Systemvoraussetzungen	21
WEP	119, 122, 124
Windows-Arbeitsgruppen suchen	134
WLAN Controller	
Firmware-Management	66

Skript-Management

66

WLAN- Controller	3, 10
WLAN-LED	24, 44
WLAN-Profil	57, 62
WME	17
WPA	119, 121, 124

Z

Zeit	25
Zeitinformation	43
Zero-Touch-Management	16
Zertifikat	43, 44, 50, 81, 84
Zertifikate	
Sichern	84
Zufallszahl	15
Zugang zum Internet einrichten	128

