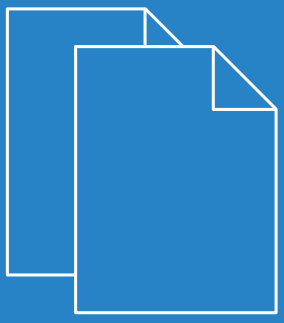
SICHER. **VERNETZT.**

LCOS 10.42

WLAN-Management



01/2021

LANCOM Systems

Inhalt

1 WLAN-Management....5
1.1 Ausgangslage....5
1.2 Technische Konzepte....5
1.2.1 WLC-Funktionen im LANCOM vRouter....5
1.2.2 Der CAPWAP-Standard....6
1.2.3 Die Smart-Controller-Technologie....6
1.2.4 Kommunikation zwischen Access Point und WLAN-Controller....8
1.2.5 Zero-Touch-Management....10
1.2.6 Split-Management....10
1.2.7 Schutz vor unberechtigtem CAPWAP-Zugriff aus dem WAN....10
1.3 Grundkonfiguration der WLAN-Controller-Funktion....11
1.3.1 Zeitinformation für den WLAN-Controller einstellen....11
1.3.2 Beispiel einer Default-Konfiguration....11
1.3.3 Zuweisung der Default-Konfiguration zu den neuen Access Points....15
1.3.4 Konfiguration der Access Points....16
1.4 Konfiguration....17
1.4.1 Allgemeine Einstellungen....17
1.4.2 Profile....17
1.4.3 Access Point Konfiguration....34
1.4.4 IP-abhängige Autokonfiguration und Tagging von APs....69
1.5 Access Point Verwaltung....71
1.5.1 Neue Access Points manuell in die WLAN-Struktur aufnehmen....71
1.5.2 Access Points manuell aus der WLAN-Struktur entfernen....74
1.5.3 Access Point deaktivieren oder dauerhaft aus der WLAN-Struktur entfernen....74
1.6 AutoWDS – Kabellose Integration von APs über P2P-Verbindungen....75
1.6.1 Hinweise zur Nutzung von AutoWDS....77
1.6.2 Funktionsweise....79
1.6.3 Einrichtung mittels vorkonfigurierter Integration....86
1.6.4 Vorkonfigurierte Integration durch Pairing beschleunigen....88
1.6.5 Einrichtung mittels Express-Integration....88
1.6.6 Umschalten von Express- zu vorkonfigurierter Integration....90
1.6.7 Manuelles Topologie-Mangement....90
1.6.8 Redundante Strecken mittels RSTP....93
1.7 Zentrales Firmware- und Skript-Management....94
1.7.1 Allgemeine Einstellungen für das Firmware-Management....95
1.8 RADIUS....98
1.8.1 Prüfung der WLAN-Clients über RADIUS (MAC-Filter)....99
1.8.2 Externer RADIUS-Server....100
1.8.3 Dynamische VLAN-Zuweisung....102
1.8.4 RADIUS-Accounting im WLAN-Controller für logische WLANs aktivieren....103

1.9 Anzeigen und Aktionen im LANmonitor....105
1.10 Funkfeldoptimierung....106
1.10.1 Gruppenbezogene Funkfeldoptimierung....107
1.11 Client Steering über den WLC....109
1.11.1 Konfiguration....110
1.12 Kanallastanzeige im WLC-Betrieb....113
1.13 Sicherung der Zertifikate....113
1.13.1 Backup der Zertifikate anlegen....113
1.13.2 Zertifikats-Backup in das Gerät einspielen....114
1.13.3 Sichern und Wiederherstellen weiterer Dateien der SCEP-CA....115
1.13.4 One Click Backup der SCEP-CA....116
1.13.5 Backup und Einspielen der Zertifikate über LANconfig....117
1.14 Backuplösungen....118
1.14.1 WLC-Cluster....118
1.14.2 Backup mit redundanten WLAN-Controllern....122
1.14.3 Backup mit primären und sekundären WLAN-Controllern....124
1.14.4 Primäre und sekundäre Controller....124
1.14.5 Automatische Suche nach alternativen WLCs....125
1.14.6 One Click Backup der SCEP-CA....125
1.15 Automatischer Konfigurationsabgleich (Config-Sync) mit der LANCOM WLC High Availability Clustering XL Option....126
1.15.1 Spezielles LANconfig-Icon für Cluster-Geräte oder mit Config-Sync....127
1.15.2 Spezielles LANmonitor-Icon für Cluster-Geräte oder mit Config-Sync....129
2 Anhang....130
2.1 Übersicht der capwap-Parameter im show-Befehl....130

Copyright

© 2021 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® und Microsoft® sind eingetragene Marken von Microsoft, Corp.

LANCOM, LANCOM Systems, LCOS, LANcommunity und Hyper Integration sind eingetragene Marken. Alle anderen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein. Dieses Dokument enthält zukunftsbezogene Aussagen zu Produkten und Produkteigenschaften. LANCOM Systems behält sich vor, diese jederzeit ohne Angaben von Gründen zu ändern. Keine Gewähr für technische Ungenauigkeiten und / oder Auslassungen.

Das Produkt enthält separate Komponenten, die als sogenannte Open Source Software eigenen Lizenzen, insbesondere der General Public License (GPL), unterliegen. Die Lizenzinformationen zur Geräte-Firmware (LCOS) finden Sie auf der WEBconfig des Geräts unter dem Menüpunkt „Extras > Lizenzinformationen“. Sofern die jeweilige Lizenz dies verlangt, werden Quelldateien zu den betroffenen Software-Komponenten auf Anfrage über einen Download-Server bereitgestellt.

Produkte von LANCOM Systems enthalten Software, die vom „OpenSSL Project“ für die Verwendung im „OpenSSL Toolkit“ entwickelt wurde (*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-systems.de

1 WLAN-Management

1.1 Ausgangslage

Der weit verbreitete Einsatz von Wireless Access Points (APs) 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 APs benötigen eine Konfiguration und ein entsprechendes Monitoring zur Erkennung von unerwünschten WLAN-Clients etc. Die Administration der APs 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 APs bei Änderungen in der WLAN-Struktur zieht sich ggf. über einen längeren Zeitraum hinweg, sodass es zur gleichen Zeit unterschiedliche Konfigurationen im WLAN gibt.
- Durch die gemeinsame Nutzung des geteilten Übertragungsmediums (Luft) ist eine effektive Koordination der APs notwendig, um Frequenzüberlagerungen zu vermeiden und die Netzwerkperformance zu optimieren.
- APs 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 APs mit dem LAN verbunden werden und so die geltenden Sicherheitsrichtlinien umgehen.

1.2 Technische Konzepte

Mit einem zentralen WLAN-Management lassen sich diese Probleme lösen. Die Konfiguration der APs wird dabei nicht mehr in den Geräten selbst vorgenommen, sondern in einer zentralen Instanz, dem WLAN-Controller (WLC). Der WLC authentifiziert die APs 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 APs aus. Da die vom WLC zugewiesene Konfiguration in den APs 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).

1.2.1 WLC-Funktionen im LANCOM vRouter

Ab LCOS 10.30 unterstützt der LANCOM vRouter zusätzlich die Funktionen eines WLAN-Controllers. Entscheiden Sie selbst und flexibel, welche Rolle Ihr LANCOM vRouter übernehmen soll: VPN-Gateway oder WLAN-Controller. Der LANCOM vRouter unterstützt ab sofort die Rolle eines virtuellen WLCs (vWLC) und kann somit Access Points verwalten. Damit können die WLAN-Controller-Funktionalitäten vollständig auf einer Virtualisierungsplattform wie VMWare ESXi oder Microsoft Hyper-V virtualisiert werden. Die Anzahl der verwalteten Access Points ist abhängig von der Lizenzkategorie des vRouters. Alle vRouter-Lizenzen, die ab dem Release von LCOS 10.30 ausgestellt wurden, enthalten eine vWLC-Option.

Produkt	VPN-Lizenzen	AP-Lizenzen
vRouter 50	10	10
vRouter 250	50	50
vRouter 500	100	100

Produkt	VPN-Lizenzen	AP-Lizenzen
vRouter 1000	200	200
vRouter unlimited	1000	1000

LANCOM Systems GmbH empfiehlt den Betrieb einer vRouter-Instanz entweder hauptsächlich als VPN-Gateway / Router oder als WLAN-Controller. Die empfohlene Nutzung kann auch anteilig erfolgen; zum Beispiel bei der Lizenzstufe „vRouter 1000“ (200 VPN-Lizenzen und 200 AP-Lizenzen):

- 100 gleichzeitige VPN-Verbindungen und 100 verwaltete APs oder
- 150 gleichzeitige VPN-Verbindungen und 50 verwaltete APs.

1.2.2 Der CAPWAP-Standard

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

CAPWAP verwendet zwei Kanäle für die Datenübertragung:

- Kontrollkanal, verschlüsselt mit Datagram Transport Layer Security (DTLS). Über diesen Kanal werden die Verwaltungsinformationen zwischen dem WLC und dem AP ausgetauscht.

  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.
- Über diesen Datenkanal werden die Nutzdaten aus dem WLAN vom AP über den WLC ins LAN übertragen – gekapselt in das CAPWAP-Protokoll.

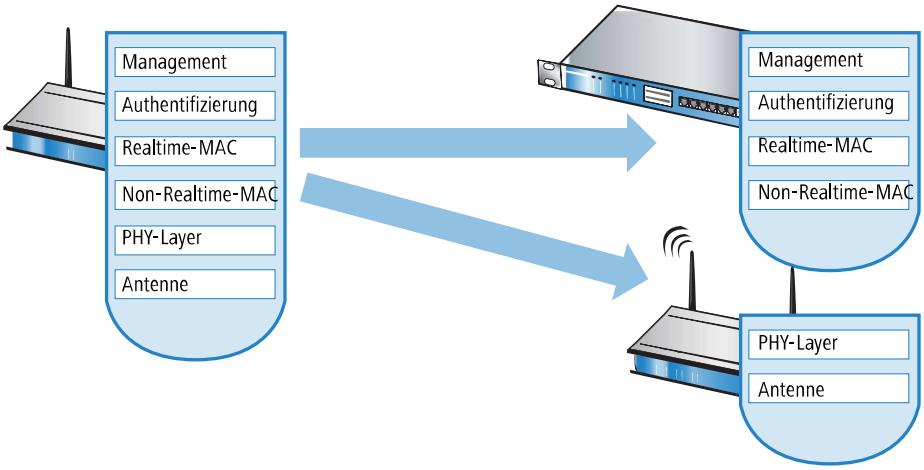
1.2.3 Die Smart-Controller-Technologie

In einer dezentralen WLAN-Struktur mit autonomen APs (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 APs enthalten. Mit dem zentralen WLAN-Management werden diese Aufgaben auf zwei verschiedene Geräte aufgeteilt:

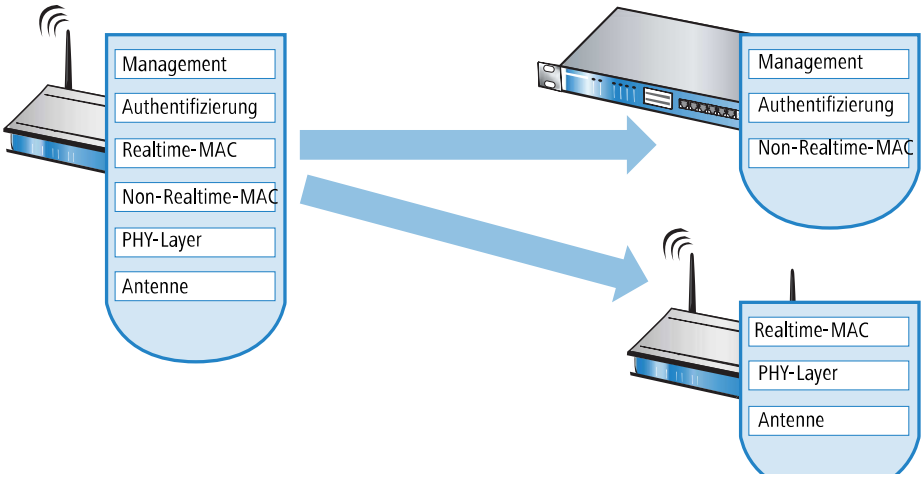
- Der zentrale WLC übernimmt die Verwaltungsaufgaben.
- Die verteilten APs übernehmen die Datenübertragung auf dem PHY-Layer und die MAC-Funktionen.
- Als dritte Komponenten kommt ggf. ein RADIUS- oder EAP-Server zur Authentifizierung der WLAN-Clients hinzu (was in autonomen WLANs aber auch der Fall sein kann).

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

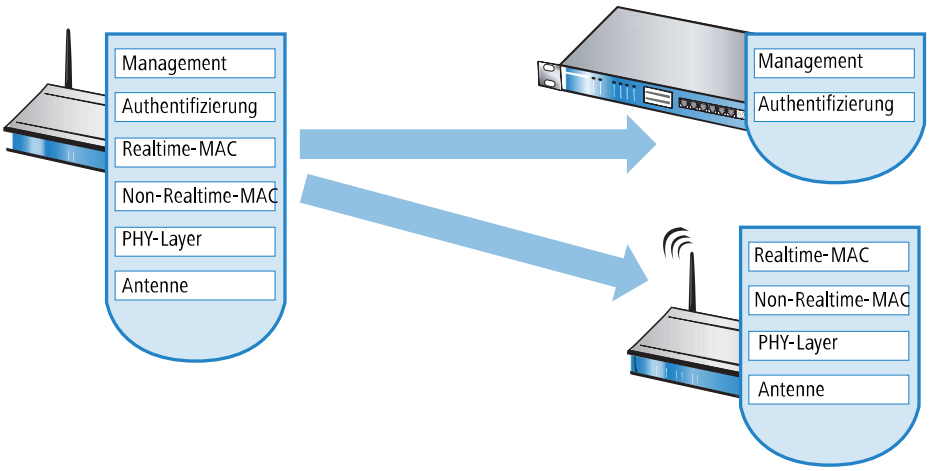
- Remote-MAC: Hier werden alle WLAN-Funktionen vom AP an den WLC übertragen. Die APs dienen hier nur als "verlängerte Antennen" ohne eigene Intelligenz.



- Split-MAC: Bei dieser Variante wird nur ein Teil der WLAN-Funktionen an den WLC übertragen. Üblicherweise werden die zeitkritischen Anwendungen (Realtime-Applikationen) weiterhin auf dem AP abgearbeitet, die nicht zeitkritischen Anwendungen (Non-Realtime-Applikationen) werden über den zentralen WLC abgewickelt.



- Local-MAC: Die dritte Möglichkeit sieht eine vollständige Verwaltung und Überwachung des WLAN-Datenverkehrs direkt in den APs vor. Zwischen dem AP und dem WLC werden lediglich Nachrichten zur Sicherung einer einheitlichen Konfiguration der APs und zum Management des Netzwerks ausgetauscht.



Die Smart-Controller-Technologie von LANCOM setzt das Local-MAC-Verfahren ein. Durch die Reduzierung der zentralisierten Aufgaben bieten die WLAN-Strukturen eine optimale Skalierbarkeit. Gleichzeitig wird der WLC in einer solchen Struktur nicht zum zentralen Flaschenhals, der große Teile des gesamten Datenverkehrs verarbeiten muss. In Remote-MAC- und Split-MAC-Architekturen müssen immer **alle** Nutzdaten zentral über den WLC laufen. In Local-MAC-Architekturen können die Daten jedoch alternativ auch direkt von den APs in das LAN ausgekoppelt werden, sodass eine hochperformante Datenübertragung ermöglicht wird. 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.

Layer-3-Tunneling und Layer-3-Roaming

WLCs mit LCOS unterstützen ebenfalls die Übertragung der Nutzdaten durch einen CAPWAP-Tunnel. Auf diese Weise können z. B. ausgewählte Applikationen wie VoIP über den zentralen WLC geleitet werden. Beim Wechsel der WLAN-Clients in eine andere Funkzelle bleibt so die zugrundeliegende IP-Verbindung ohne Unterbrechung, da sie fortlaufend vom zentralen WLC 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 WLC verwaltet werden.

1.2.4 Kommunikation zwischen Access Point und WLAN-Controller

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

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

Der AP sendet zu Beginn der Kommunikation eine "Discovery Request Message", um die verfügbaren WLCs zu ermitteln. Dieser Request wird grundsätzlich als Broadcast versendet. Da in manchen Strukturen ein potenzieller WLC aber nicht

über Broadcast zu erreichen ist, können auch spezielle Adressen von weiteren WLCs in die Konfiguration der APs eingetragen werden.

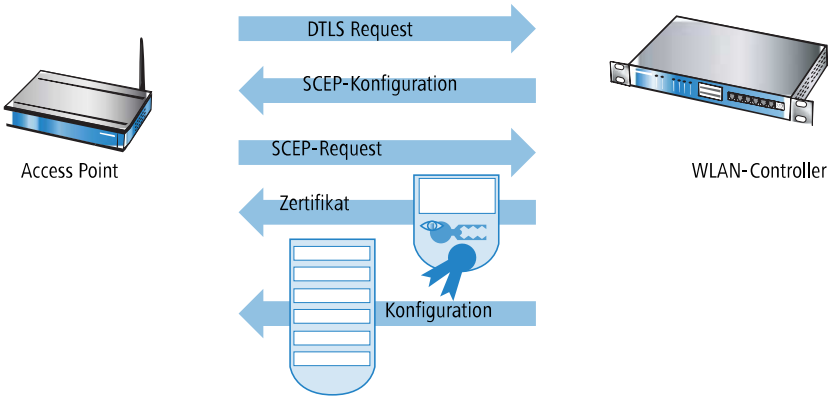
Außerdem können auch DNS-Namen von WLCs aufgelöst werden. Alle APs mit LCOS 7.22 oder höher haben den Standardnamen 'WLC-Address' bereits konfiguriert, sodass ein DNS-Server diesen Namen zu einem WLC auflösen kann. Gleiches gilt auch für die über DHCP gelernten DHCP-Suffixe. Somit können auch WLCs erreicht werden, die nicht im gleichen Netz stehen, ohne die APs konfigurieren zu müssen.

Aus den verfügbaren WLCs wählt der AP den besten aus und fragt bei diesem nach dem Aufbau der DTLS-Verbindung an. Der "beste" WLC ist für den AP derjenige mit der geringsten Auslastung, also dem kleinsten Verhältnis von gemanagten APs zu den maximal möglichen APs. Bei zwei oder mehreren gleich "guten" WLCs wählt der AP den im Netzwerk nächsten, also den mit der geringsten Antwortzeit.

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

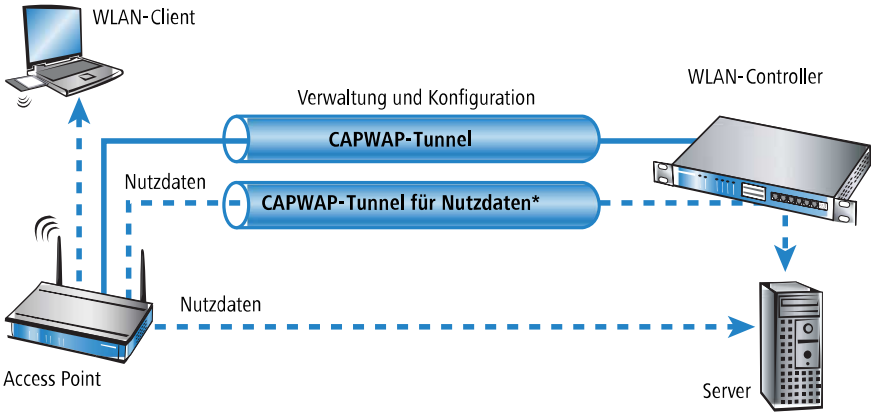
Über die gesicherte DTLS-Verbindung wird dem AP die Konfiguration für den integrierten SCEP-Client mitgeteilt – der AP kann dann über SCEP sein Zertifikat bei der SCEP-CA abholen. Anschließend wird die dem AP zugewiesene Konfiguration übertragen.

SCEP steht für Simple Certificate Encryption Protocol, CA für Certification Authority.



Sowohl Authentifizierung als auch Konfiguration können entweder automatisch vorgenommen werden oder nur bei passendem Eintrag der MAC-Adresse des AP in der AP-Tabelle des WLC. Sofern bei dem AP 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 AP direkt in das LAN ausgekoppelt und z. B. an den Server übertragen.



1.2.5 Zero-Touch-Management

Mit der Möglichkeit, einem anfragenden AP ein Zertifikat und eine Konfiguration automatisch zuzuweisen, realisieren WLCs ein echtes "Zero-Touch-Management". Neue APs brauchen nur noch mit dem LAN verbunden werden; weitere Konfigurationsschritte sind 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.

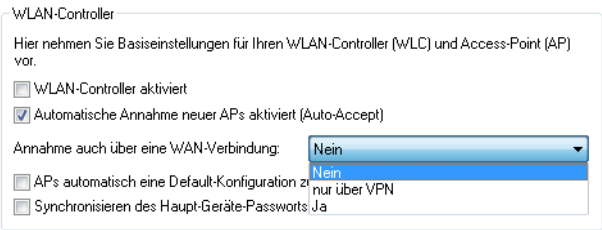
1.2.6 Split-Management

APs sind fähig, ihren WLC auch in entfernten Netzen zu suchen – eine einfache IP-Verbindung z. B. über eine VPN-Strecke reicht aus. Da die WLCs ausschließlich den WLAN-Teil der Konfiguration im AP beeinflussen, lassen sich alle anderen Funktionen separat verwalten. Durch diese Aufteilung der Konfigurationsaufgaben eignen sich WLCs ideal für den Aufbau einer firmenweiten WLAN-Infrastruktur in der Zentrale inklusive aller angeschlossenen Niederlassungen und Home-Offices.

1.2.7 Schutz vor unberechtigtem CAPWAP-Zugriff aus dem WAN

Der WLC oder LANCOM Router mit aktiver WLC-Option behandelt CAPWAP-Anfragen aus dem LAN und dem WAN identisch. Bei von WAN-Gegenstellen stammenden Anfragen übernimmt er die APs in seine AP-Verwaltung und übergibt ggf. eine Default-Konfiguration. Entsprechend konfiguriert wird der CAPWAP-Dienst auf WAN-Gegenstellen nicht mehr angeboten, so dass keine Annahme von APs und Konfigurationsvergabe auf WAN-Gegenstellen mehr stattfindet.

Die Konfiguration erfolgt unter **WLAN-Controller** > **Allgemein** im Bereich **WLAN-Controller**. Ist die automatische Annahme neuer APs aktiviert, können Sie unter **Annahme auch über eine WAN-Verbindung** wählen, ob der CAPWAP-Dienst auch auf WAN-Gegenstellen angeboten wird.



Nein

Das Gerät nimmt keine neuen APs über die WAN-Verbindung an.

Nur über VPN

Das Gerät nimmt nur neue APs an, wenn die WAN-Verbindung über VPN erfolgt.

Ja

Das Gerät nimmt alle neuen APs über die WAN-Verbindung an.

1.3 Grundkonfiguration der WLAN-Controller-Funktion

Für den Start benötigt ein WLC zur weitestgehend automatisierten Konfiguration der APs die beiden folgenden Informationen:

- Eine aktuelle Zeitinformation (Datum und Uhrzeit), damit die Gültigkeit der benötigten Zertifikate sichergestellt werden kann.
- Ein WLAN-Profil, welches der WLC den APs zuweisen kann.

Weiterführende, optionale Konfigurationsbeispiele schließen das Einrichten von redundanten WLCs, das manuelle Trennen und Verbinden von APs sowie das Durchführen eines Backups der notwendigen Zertifikate ein.

Standardmäßig wartet der WLC auf Port 1027 (konfigurierbar) auf Verbindungen. Die Verteilung der Zertifikate erfolgt über SCEP, welches Port 80 (HTTP) nutzt.

1.3.1 Zeitinformation für den WLAN-Controller einstellen

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

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

Router mit WLC-Option verfügen über keine WLAN-LED.

Um dem Gerät eine Zeit zuzuweisen, klicken Sie in LANconfig mit der rechten Maustaste auf den Eintrag für den WLC 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 WLCs können die aktuelle Zeit alternativ auch automatisch über das Network Time Protocol (NTP) von einem Zeit-Server beziehen. Informationen über NTP und die entsprechende Konfiguration finden Sie im LCOS-Referenzhandbuch.

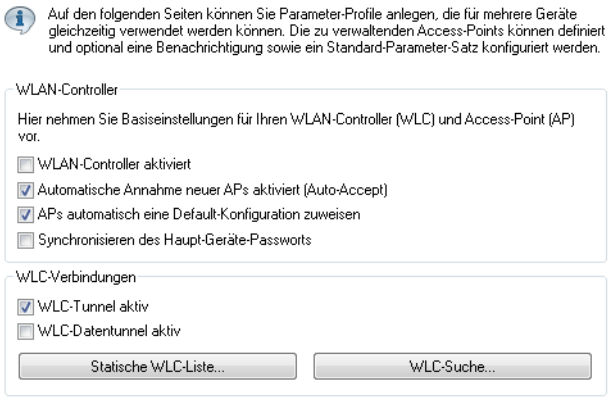
Sobald der WLC über eine gültige Zeitinformation verfügt, beginnt die Erstellung der Zertifikate (Root- und Geräte-Zertifikat). Wenn die Zertifikate erfolgreich erzeugt wurden, meldet der WLC Betriebsbereitschaft, die WLAN-LED blinkt dann rot.

Nach Herstellung der Betriebsbereitschaft sollten Sie eine Sicherung der Zertifikate anlegen (*Sicherung der Zertifikate*)

1.3.2 Beispiel einer Default-Konfiguration

1. Öffnen Sie die Konfiguration des WLCs durch einen Doppelklick auf den entsprechenden Eintrag in LANconfig.

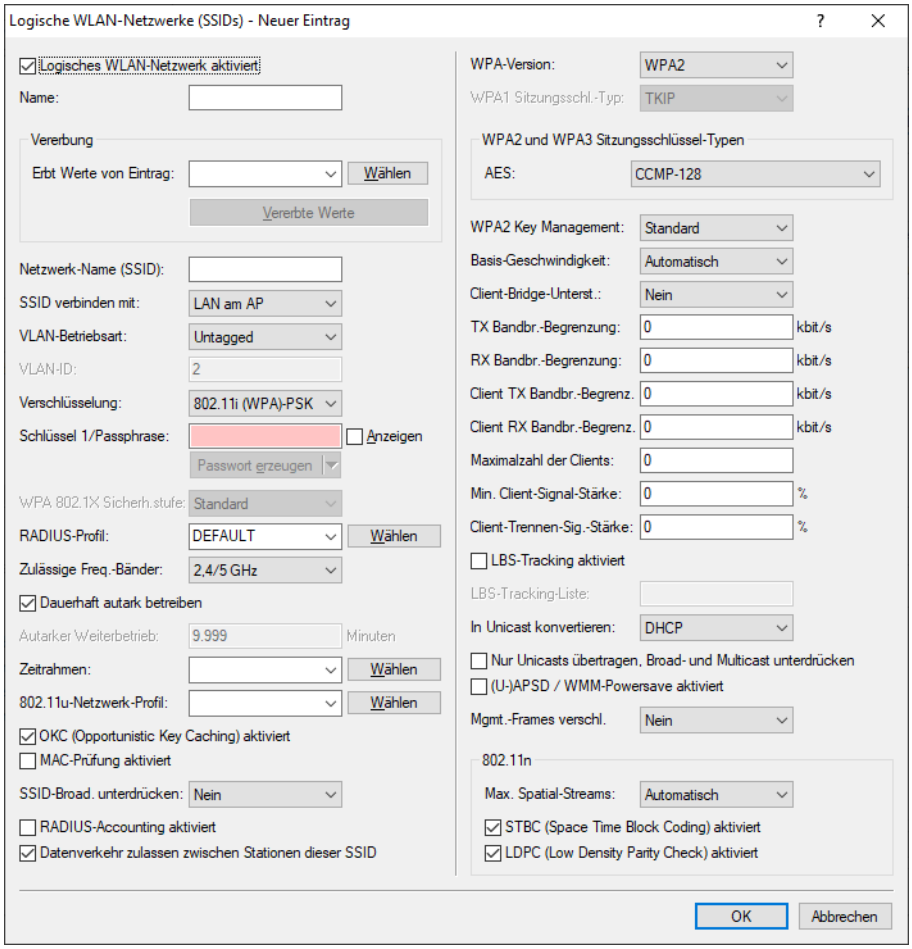
2. Aktivieren Sie unter **WLAN-Controller** > **Allgemein** die Optionen für die automatische Annahme neuer APs sowie die Zuweisung einer Default-Konfiguration.



- **Automatische Annahme neuer APs aktiviert (Auto-Accept)**: Ermöglicht dem WLC, allen neuen APs ohne gültiges Zertifikat ein solches Zertifikat zuzuweisen. Dazu muss entweder für den AP eine Konfiguration in der AP-Tabelle eingetragen sein oder die Automatische Zuweisung der Default-Konfiguration ist aktiviert.
- **APs automatisch eine Default-Konfiguration zuweisen** : Ermöglicht dem WLC, allen neuen APs eine Default-Konfiguration zuzuweisen, auch wenn für diese keine explizite Konfiguration hinterlegt wurde.

Durch die Kombination dieser beiden Optionen kann der WLC alle im LAN gefundenen APs im Managed-Modus automatisch in die von ihm verwaltete WLAN-Struktur aufnehmen, z. B. temporär während der Rollout-Phase einer WLAN-Installation.

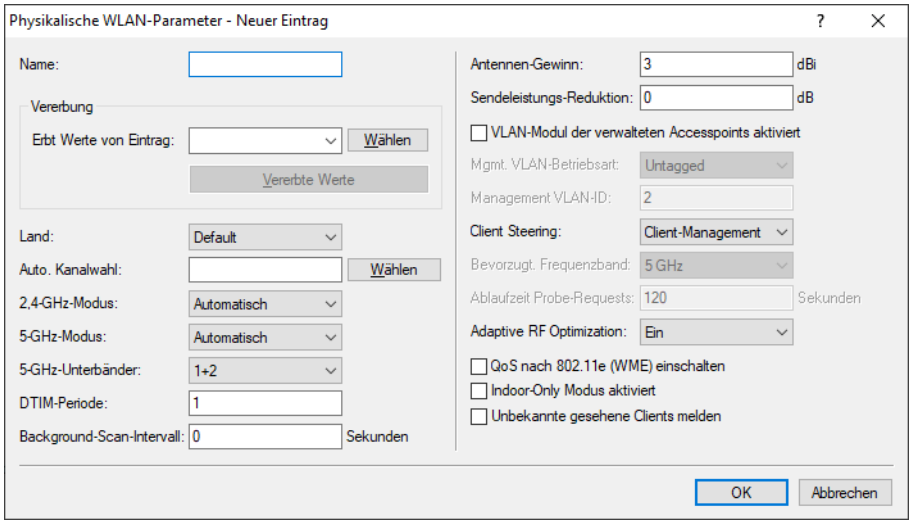
3. Wechseln Sie in der Ansicht **Profile** in die logischen WLAN-Netzwerke. Erstellen Sie einen neuen Eintrag mit folgenden Werten:



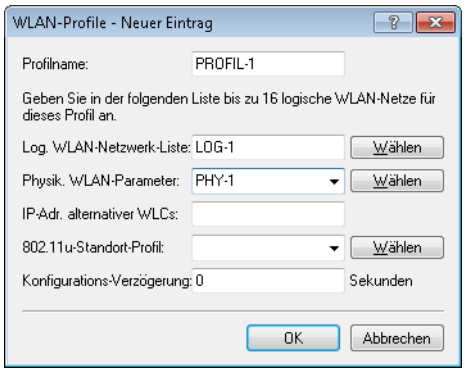
- **Netzwerkname**: Geben Sie dem WLAN einen Namen. Dieser Name wird nur für die Verwaltung im WLC verwendet.
- **SSID**: Mit dieser SSID verbinden sich die WLAN-Clients.
- **Verschlüsselung**: Wählen Sie die Verschlüsselung passend zu den Möglichkeiten der verwendeten WLAN-Clients und geben Sie ggf.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

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 AP-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).

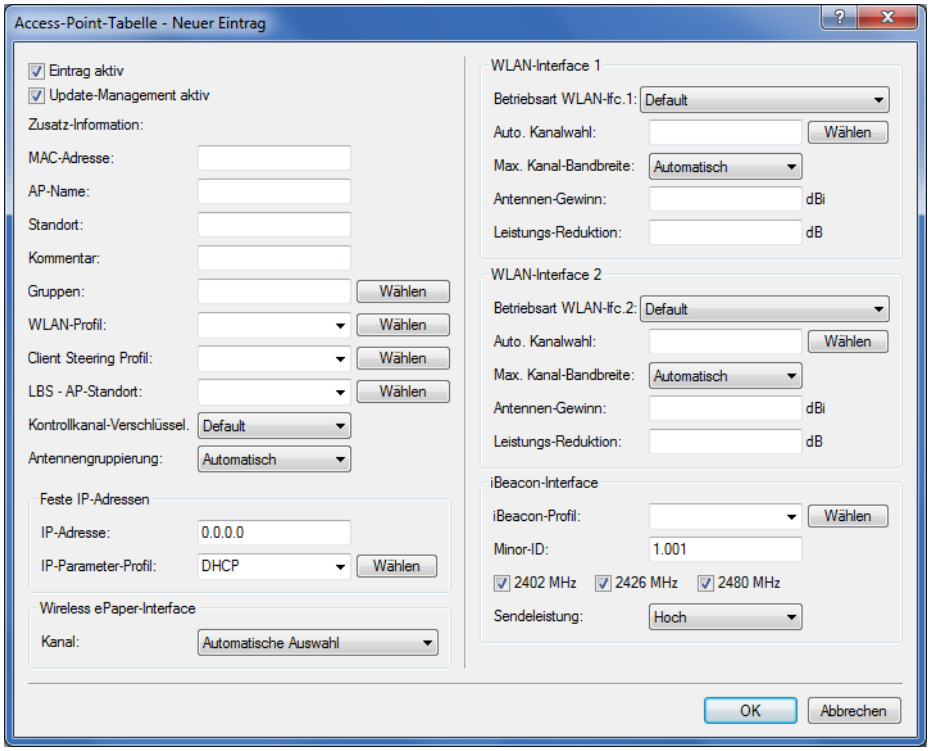


5. Erstellen Sie ein neues WLAN-Profil, geben Sie ihm einen eindeutigen Namen und weisen Sie ihm das eben erstellte logische WLAN-Netzwerk sowie die physikalischen WLAN-Parameter zu.



6. Wechseln Sie auf in Ansicht **AP-Konfiguration**, öffnen Sie die **Access-Point-Tabelle** 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** sollten frei bleiben.

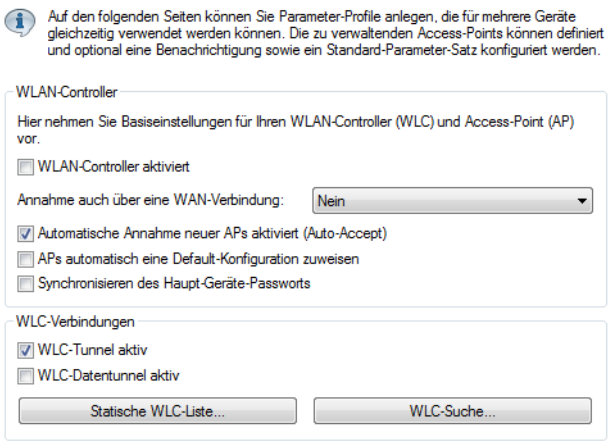
Die **MAC-Adresse** wird für die Default-Konfiguration auf 'ffffffffffff' gesetzt und ist nicht editierbar. Damit gilt dieser Eintrag als Standard für alle APs, die nicht mit ihrer MAC-Adresse explizit in dieser Tabelle eingetragen sind.



1.3.3 Zuweisung der Default-Konfiguration zu den neuen Access Points

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

Nach der ersten Startphase kann die Option **Automatische Annahme neuer APs** wieder deaktiviert werden, damit keine weiteren APs automatisch in das Netzwerk aufgenommen werden.



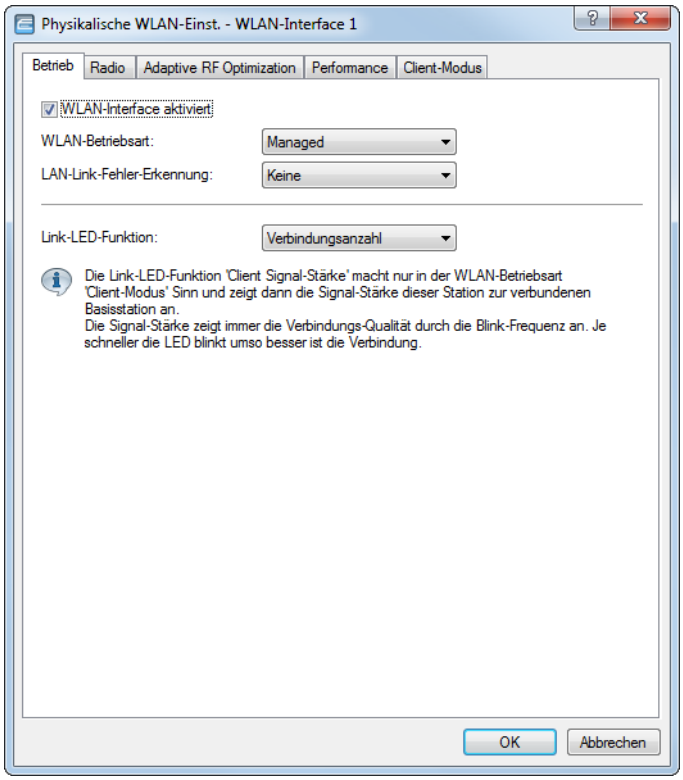
1.3.4 Konfiguration der Access Points

LANCOM Access Points und LANCOM Wireless Router unterscheiden sich bzgl. der Einstellung der WLAN-Module im Auslieferungszustand.

- Bei APs sind im Auslieferungszustand die WLAN-Module auf die Betriebsart 'Managed' eingestellt. In diesem Modus suchen die APs nach einem zentralen WLC, der ihnen eine Konfiguration zuweisen kann, und bleiben so lange im "Such-Modus", bis sie einen passenden WLC gefunden haben oder die Betriebsart für die WLAN-Module manuell geändert wird.
- Bei Wireless Routern sind im Auslieferungszustand die WLAN-Module auf die Betriebsart 'Access-Point' eingestellt. In diesem Modus arbeiten die Wireless Router als autarke APs mit einer im Gerät lokal gespeicherten Konfiguration. Um Teilnehmer einer zentral über WLC verwalteten WLAN-Struktur zu werden, muss die Betriebsart für die WLAN-Module in den gewünschten 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 WLC 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
lang English
flash 0
cd Setup/Interfaces/WLAN/Operational
set WLAN-1 0 managed-AP 0
# done
exit
```

1.4 Konfiguration

Die meisten Parameter zur Konfiguration der WLAN-Controller entsprechen denen der Access Points. In diesem Abschnitt werden daher nicht alle WLAN-Parameter explizit beschrieben sondern nur die für den Betrieb der WLAN-Controller erforderlichen Aspekte.

1.4.1 Allgemeine Einstellungen

In diesem Bereich nehmen Sie die Basiseinstellungen für Ihren WLC vor.

- Automatische Annahme neuer APs (Auto-Accept)

  Ermöglicht dem WLC, allen neuen APs eine Konfiguration zuzuweisen, auch wenn diese nicht über ein gültiges Zertifikat verfügen.

  Ermöglicht dem WLC, allen neuen APs **ohne** gültiges Zertifikat ein solches Zertifikat zuzuweisen. Dazu muss eine der beiden Bedingungen erfüllt sein:

  - Für den AP 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 WLC, allen neuen APs (also **ohne** gültiges Zertifikat) eine Default-Konfiguration zuzuweisen, auch wenn für diese keine explizite Konfiguration hinterlegt wurde. Im Zusammenspiel mit dem Auto-Accept kann der WLC alle im LAN gefundenen APs im Managed-Modus automatisch in die von ihm verwaltete WLAN-Struktur aufnehmen (bis zur maximalen Anzahl der auf einem WLC verwalteten APs). Per Default aufgenommene APs werden auch in die MAC-Liste aufgenommen.

  Mit dieser Option können möglicherweise auch unbeabsichtigte APs 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 APs abdecken:

Auto-Accept	Default-Konfiguration	Geeignet für
Ein	Ein	Rollout-Phase: Verwenden Sie diese Kombination nur dann, wenn **keine APs 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 APs 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 APs ohne Zustimmung der Administratoren in die WLAN-Struktur aufgenommen.

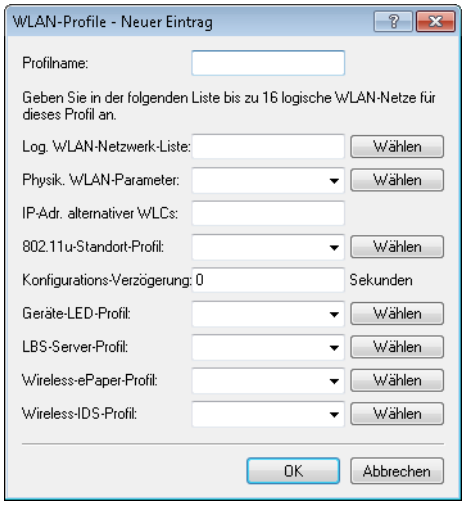
1.4.2 Profile

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

WLAN-Profile

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

Für jedes WLAN-Profil können Sie unter **WLAN-Controller** > **Profile** > **WLAN-Profile** die folgenden Parameter definieren:



Profil-Name

Name des Profils, unter dem die Einstellungen gespeichert werden.

Log. WLAN-Netzwerk-Liste

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

Die APs nutzen aus dieser Liste nur die ersten 16 Einträge, die mit der eigenen Hardware kompatibel sind. Somit können in einem Profil z. B. jeweils 16 WLAN-Netzwerke für reinen 2,4 GHz-Betrieb und 16 für reinen 5 GHz-Betrieb definiert werden. Für jeden AP – sowohl Modelle mit 2,4 GHz- als auch die mit 5 GHz-Unterstützung – stehen damit die maximal möglichen 16 logischen WLAN-Netzwerke zur Verfügung.

Physik. WLAN-Parameter

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

IP-Adr. alternativer WLCs

Liste der WLCs, bei denen der AP eine Verbindung versuchen soll. Der AP leitet die Suche nach einem WLC über einen Broadcast ein. Wenn nicht alle WLCs über einen solchen Broadcast erreicht werden können (WLC steht z. B. in einem anderen Netz), dann ist die Angabe von alternativen WLCs sinnvoll.

802.11u-Standort-Profil

Wählen Sie aus der Liste ein Hotspot-2.0-Profil aus. Hotspot-2.0-Profile legen Sie im Konfigurationsmenü über die gleichnamige Schaltfläche an.

Konfigurations-Verzögerung

Geben Sie hier die Verzögerung an, nach der ein vom WLAN-Controller gemanagter AP die übertragene Konfiguration übernimmt.

Dies ist insbesondere in AutoWDS-Szenarien sinnvoll, in denen mehrere gemanagte APs über Punkt-zu-Punkt-Strecken hintereinander verbunden sind. Durch eine vorzeitige Konfigurations-Änderung auf einem AP, welcher die Verbindung zu einem entfernteren AP herstellt, könnte sonst die Verbindung zu dem entfernteren AP abgeschnitten werden.

Eine grobe Regel für die Berechnung der Verzögerung ist (unabhängig von der Topologie): Eine Sekunde pro gemanagtem AP, also z. B. 200 Sekunden bei 200 APs.

Die Verzögerung gilt nicht für übertragene Skripte.

Geräte-LED-Profil

Wählen Sie aus der Liste der Geräte-LED-Profile das Profil aus, das im WLAN-Profil gelten soll. Die Geräte-LED-Profile verwalten Sie unter **WLAN-Controller** > **Profile** > **Geräte-LED-Profile**.

LBS-Allgemein-Profil

Wählen Sie hier aus der Liste der allgemeinen LBS-Profile das Profil aus, das im WLAN-Profil gelten soll. Die allgemeinen LBS-Profile verwalten Sie unter **WLAN-Controller** > **Profile** > **Erweiterte Profile** mit der Schaltfläche **LBS - Allgemein**.

Wireless-ePaper-Profil

Wählen Sie hier aus der Liste der Wireless-ePaper-Profile das Profil aus, das im WLAN-Profil gelten soll. Die Wireless-ePaper-Profile verwalten Sie unter **WLAN-Controller** > **AP-Konfiguration** > **Erweiterte Einstellungen** mit der Schaltfläche **Wireless-ePaper-Profile**.

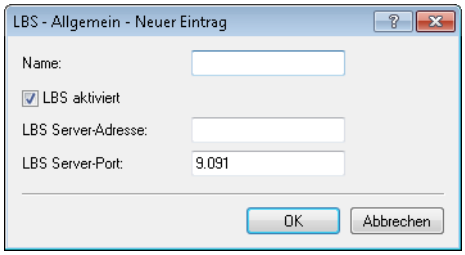
Wireless-IDS-Profil

Wählen Sie hier aus der Liste der Wireless-IDS-Profile das Profil aus, das im WLAN-Profil gelten soll. Die Wireless-IDS-Profile verwalten Sie unter **WLAN-Controller** > **AP-Konfiguration** > **Erweiterte Einstellungen** mit der Schaltfläche **Wireless-IDS-Profile**.

Allgemeines LBS-Profil und Gerätestandort-Profil

Um die Einstellungen von Location Based Services-Servern (LBS-Servern) und AP-Standorten komfortabel über einen WLC zu verwalten, erstellen Sie über **WLAN-Controller** > **Profile** mit der Schaltfläche **Erweiterte Profile** das entsprechende Profil für den LBS-Server.

Mit der Schaltfläche **LBS – Server** erstellen Sie ein allgemeines LBS-Server-Profil.



Name

Vergeben Sie einen aussagekräftigen Namen für das Profil.

LBS aktiviert

Aktivieren oder deaktivieren Sie LBS.

LBS Server-Adresse

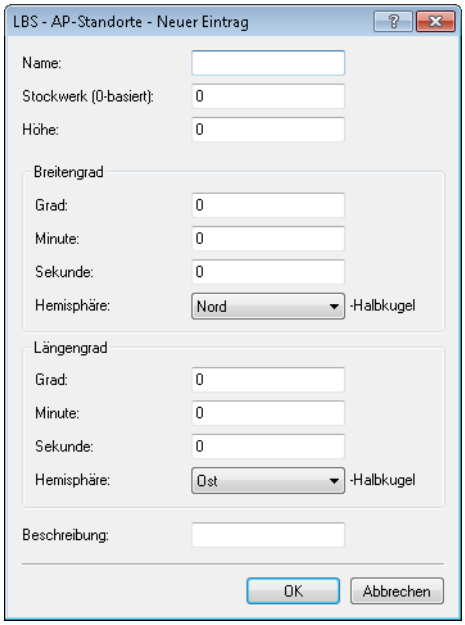
Geben Sie hier die Adresse des LBS-Servers ein.

LBS Server-Port

Geben Sie hier den Port des LBS-Servers ein (Default: 9091).

Sie erstellen das entsprechende Profil für Standorte der LBS APs über **WLAN-Controller** > **AP-Konfiguration** mit der Schaltfläche **Erweiterte Einstellungen**.

Mit der Schaltfläche **LBS-AP-Standorte** erstellen Sie ein Standort-Profil der LBS-APs.



Name

Vergeben Sie einen aussagekräftigen Namen für das Profil.

Stockwerk (0-basiert)

Geben Sie hier die Etage ein, auf der sich das Gerät befindet. So differenzieren Sie z. B. zwischen Ober- und Untergeschoss.

Höhe

Geben Sie hier die Höhe ein, auf der sich das Gerät befindet. Die Angabe eines negativen Wertes ist möglich, so dass Sie zwischen einer Position über und unter dem Meeresspiegel differenzieren können.

Grad (Breitengrad)

Dieses Feld gibt den Winkel in Grad des geographischen Koordinatensystems an.

Minute (Breitengrad)

Dieses Feld gibt die Minute des geographischen Koordinatensystems an.

Sekunde (Breitengrad)

Dieses Feld gibt die Sekunde des geographischen Koordinatensystems an.

Hemisphäre (Breitengrad)

Dieses Feld gibt die Orientierung des geographischen Koordinatensystems an. Für die geographische Breite (Latitude) sind folgende Werte möglich:

- Nord: nördliche Breite
- Süd: südliche Breite

Grad (Längengrad)

Dieses Feld gibt den Winkel in Grad des geographischen Koordinatensystems an.

Minute (Längengrad)

Dieses Feld gibt die Minute des geographischen Koordinatensystems an.

Sekunde (Längengrad)

Dieses Feld gibt die Sekunde des geographischen Koordinatensystems an.

Hemisphäre (Längengrad)

Dieses Feld gibt die Orientierung des geographischen Koordinatensystems an. Für die geographische Länge (Longitude) sind folgende Werte möglich:

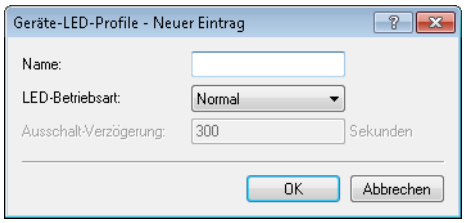
- Ost: östliche Länge
- West: westliche Länge

Beschreibung

Geben Sie hier eine Beschreibung des Gerätes ein.

Geräte-LED-Profile

Die Geräte-LEDs lassen sich am Gerät konfigurieren, um den AP unauffällig betreiben zu können. Um diese Konfiguration auch über einen WLC durchzuführen, erstellen Sie unter **WLAN-Controller** > **Profile** > **Geräte-LED-Profile** entsprechende Profile, die Sie anschließend einem WLAN-Profil zuordnen.



Name

Vergeben Sie hier einen Namen für das Geräte-LED-Profil.

LED-Betriebsart

Die folgenden Optionen stehen zur Auswahl:

- **Normal**: Die LEDs sind immer aktiviert, auch nach einem Neustart des Gerätes.
- **Verzögert aus**: Nach einem Neustart sind die LEDs für einen bestimmten Zeitraum aktiviert, danach schalten sie sich aus. Das ist dann hilfreich, wenn die LEDs während des Neustartes auf kritische Fehler hinweisen.
- **Alle aus**: Die LEDs sind alle deaktiviert. Auch nach einem Neustart des Gerätes bleiben die LEDs deaktiviert.

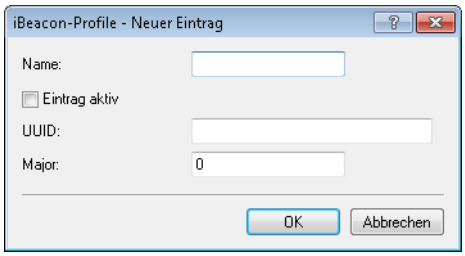
Ausschalt-Verzögerung

In der Betriebsart **Verzögert aus** können Sie im Feld **LED-Ausschalt-Verzögerung** die Dauer in Sekunden festlegen, nach der das Gerät die LEDs bei einem Neustart deaktivieren soll.

ESL- und iBeacon-Profile

Um die Einstellungen von Wireless-ePaper-Informationen und iBeacon-Informationen der einzelnen APs komfortabel über einen WLC zu verwalten, erstellen Sie über **WLAN-Controller** > **AP-Konfiguration** mit der Schaltfläche **Erweiterte Einstellungen** die entsprechenden Profile für Wireless-ePapaper und iBeacon.

Mit der Schaltfläche **iBeacon-Profile** erstellen Sie iBeacon-Profile für die Zuweisungsgruppen und die AP-Tabelle, die festlegen, welche iBeacon-Informationen die einzelnen APs ausstrahlen.



Name

Name des Profils

Eintrag aktiv

Aktiviert oder deaktiviert dieses Profil.

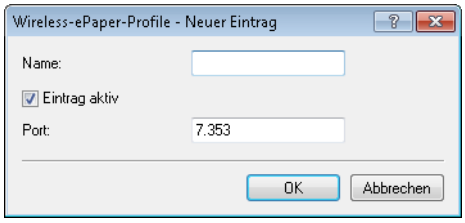
UUID

Eindeutige Kennzeichnung des Senders

Major

Gibt den Major-Wert des iBeacons an.

Mit der Schaltfläche **Wireless-ePaper-Profile** erstellen Sie Wireless-ePaper-Profile für die WLAN-Profile-Tabelle, die festlegen, welche Wireless-ePaper-Informationen die einzelnen APs ausstrahlen.



Name

Name des Profils

Eintrag aktiv

Aktiviert oder deaktiviert dieses Profil.

Port

Gibt den Port an.

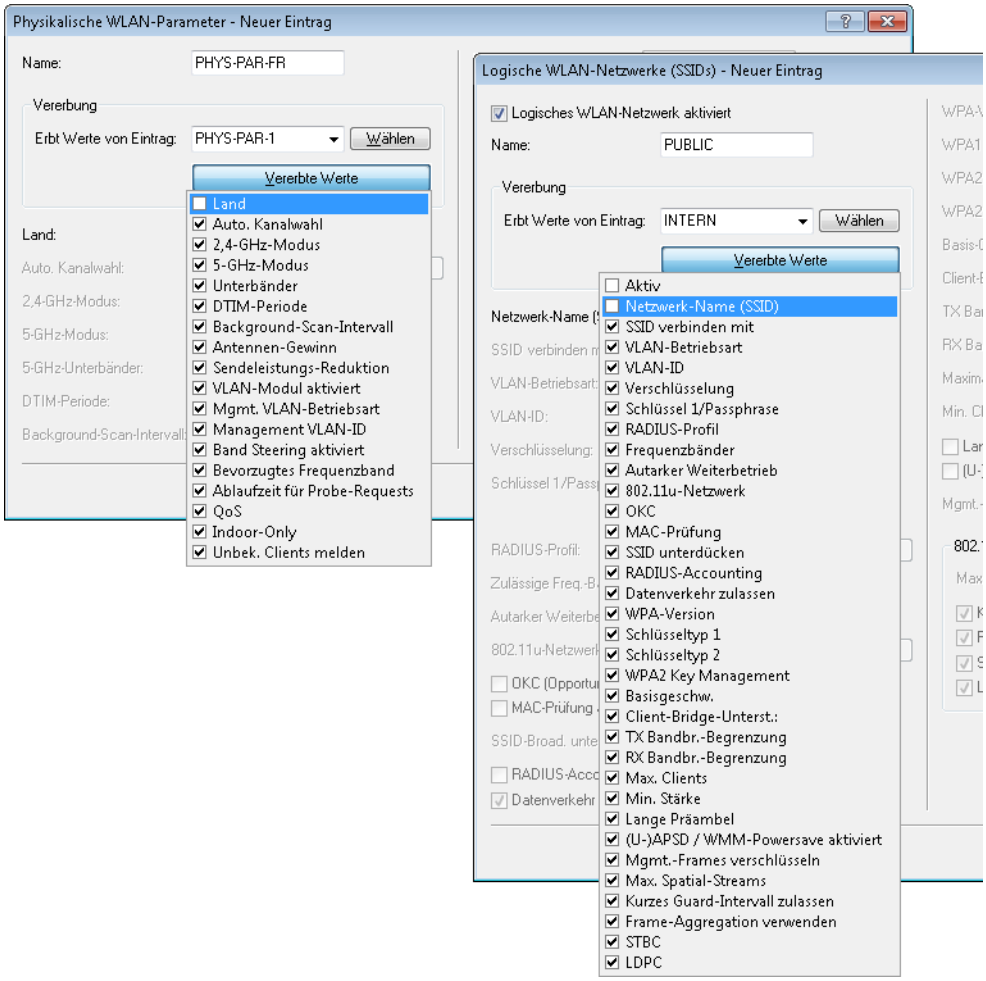
Vererbung von Parametern

Mit einem WLC können sehr viele unterschiedliche APs an verschiedenen Standorten verwaltet werden. Nicht alle Einstellungen in einem WLAN-Profil eignen sich dabei für jeden der verwalteten APs 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 APs gültig sind.

2. Erzeugen Sie danach Einträge für die spezifischeren Werte, z. B. physikalische Einstellungen für ein bestimmtes Land oder ein logisches WLAN-Netzwerk für den öffentlichen Zugang von mobilen Clients.



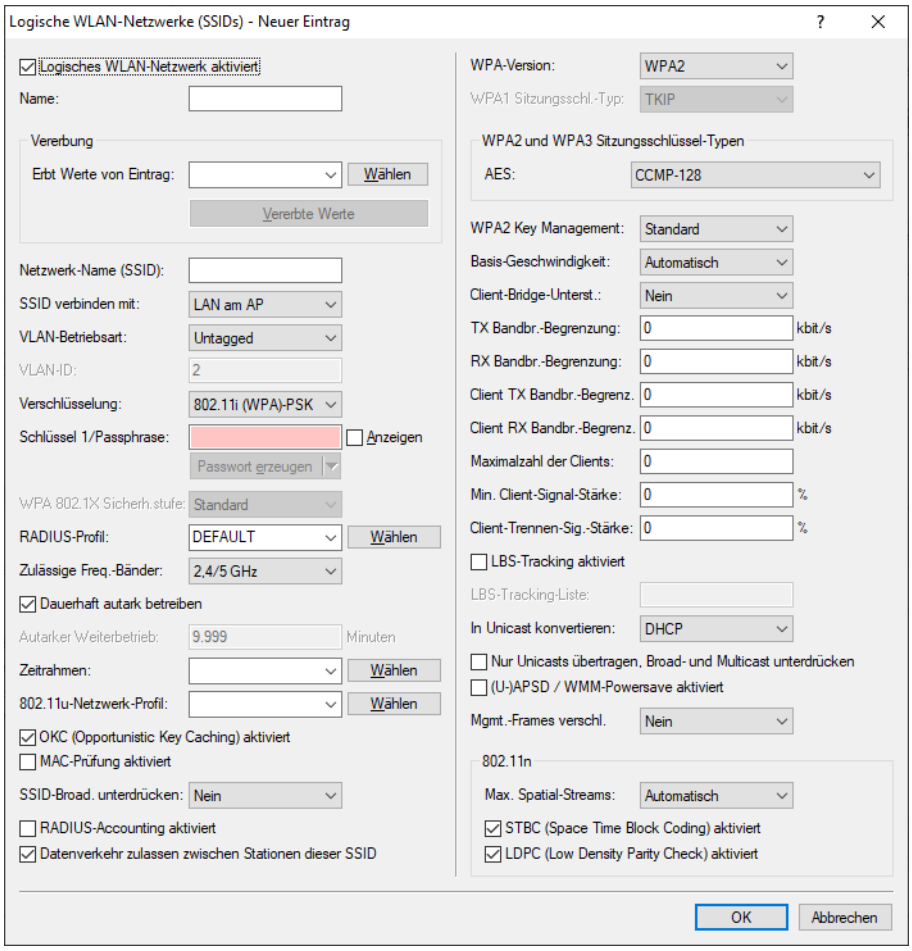
3. Wählen Sie aus, von welchem Eintrag Werte geerbt werden sollen und markieren Sie die vererbten Werte. Die so übernommenen Parameter werden im Konfigurationsdialog grau dargestellt und können nicht verändert werden.
4. Die so zusammengestellten WLAN-Einstellungen werden dann je nach Verwendung zu separaten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

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

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

Logische WLAN-Netzwerke

Unter **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke** können Sie die Parameter für die logischen WLAN-Netzwerke einstellen, die der WLC den APs zuweisen soll. Für jedes logische WLAN-Netzwerk können Sie die folgenden Parameter definieren:



Logisches WLAN-Netzwerk aktiviert

Aktivieren Sie das logische WLAN-Netzwerk, indem Sie diese Option anklicken.

Name

Geben Sie hier einen Namen an, der das logische WLAN-Netzwerk eindeutig kennzeichnet.

Vererbung

Möchten Sie Einträge erzeugen, die sich nur in wenigen Werten von vorhandenen Einträgen unterscheiden, können Sie einen "Eltern"-Eintrag sowie die zu übernehmenden Einträge hier gezielt auswählen.

Auch ein "Eltern"-Eintrag kann selber geerbte Einträge enthalten. Achten Sie darauf, dass die Konstruktionen für geerbte Einträge nicht zu komplex und damit schwer nachvollziehbar und konfigurierbar sind.

Netzwerk-Name (SSID)

Geben Sie hier die SSID des WLAN-Netzwerkes an. Alle Stationen, die zu diesem WLAN-Netz gehören, müssen dieselbe SSID verwenden.

SSID verbinden mit

Wählen Sie hier aus, mit welcher logischen Schnittstelle des APs die SSID verknüpft sein soll bzw. wohin der AP Datenpakete dieser SSID leiten soll.

- "LAN": Der AP lädt die Datenpakete standardmäßig lokal ins LAN weiter (LAN-1). Dazu muss er entsprechend konfiguriert sein.
- "WLC-Tunnel-x": Die SSID ist mit einem WLC-Bridge-Layer-3-Tunnel verbunden. Der AP liefert alle Datenpakete in diesen Tunnel und damit zum WLC. Dieser Tunnel muss auf dem WLC konfiguriert sein.

Beachten Sie, dass Sie bei Weiterleitung aller Datenpakete zum WLC zwar zentrale Routen und Filter definieren können, dieses jedoch eine hohe Last auf dem WLC erzeugt. Dafür müssen dort entsprechend hohe Bandbreiten zur Verfügung stehen, um den gesamten Datenverkehr dieser und ggf. weiterer über WLC-Tunnel mit diesem WLC verbundenen SSIDs übertragen zu können.

VLAN-Betriebsart

Stellen Sie hier die VLAN-Betriebsart des APs für Pakete dieses WLAN-Netzwerkes (SSID) ein. Die Verwendung von VLAN-IDs ist abhängig davon, ob das VLAN-Modul in den physikalischen WLAN-Parametern des APs aktiviert ist. Ansonsten ignoriert der AP alle VLAN-Einstellungen in den logischen Netzwerken. Es ist möglich, das Netzwerk trotz aktiviertem VLAN auch ungetagged zu betreiben:

- "Untagged": Der AP markiert Datenpakete dieser SSID nicht mit einer VLAN-ID.

  Es ist möglich ein WLAN-Netzwerk trotz aktiviertem VLAN auch ungetagged zu betreiben. Intern ist dafür die VLAN-ID "1" reserviert.
- "Tagged": Der AP markiert die Datenpakete mit der nachfolgend bestimmten VLAN-ID.

VLAN-ID

VLAN-ID für dieses logische WLAN-Netzwerk.

Bitte beachten Sie, dass für die Nutzung der VLAN-IDs in einem logischen WLAN-Netzwerk die Einstellung einer Management-VLAN-ID erforderlich ist (siehe Physikalische WLAN Parameter)!

Verschlüsselung

Bestimmen Sie hier das Verschlüsselungsverfahren bzw. bei WEP die Schlüssellänge für die Verschlüsselung von Datenpaketen in diesem WLAN.

Schlüssel 1 / Passphrase

Sie können die Schlüssel oder Passphrasen als ASCII-Zeichenkette eingeben. Bei WEP ist alternativ die Eingabe einer Hexadezimalzahl durch ein vorangestelltes "0x" möglich. Folgende Zeichenkettenlängen ergeben sich für die verwendeten Formate:

- WPA-PSK: 8 bis 63 ASCII-Zeichen
- WEP128 (104 Bit): 13 ASCII- oder 26 Hexadezimal-Zeichen
- WEP64 (40 Bit): 5 ASCII- oder 10 Hexadezimal-Zeichen

RADIUS-Profil

Geben Sie an, welches RADIUS-Profil der AP für dieses Netzwerk erhalten soll, damit dieser bei Bedarf eine direkte Verbindung zum RADIUS-Server aufbauen kann. Lassen Sie dieses Feld leer, wenn der WLC RADIUS-Anfragen abwickeln soll.

Die RADIUS-Profile müssen Sie in der entsprechenden Tabelle konfigurieren.

Zulässige Freq.-Bänder

Bestimmen Sie das Frequenzband, das die Netzwerkteilnehmer zur Übertragung von Daten im WLAN verwenden sollen. Sie können sowohl das 2,4 GHz-Band, das 5 GHz-Band als auch beide Bänder auswählen.

Dauerhaft autark betreiben

Ist am WLC der autarke Weiterbetrieb für WLAN-Netwerke so konfiguriert, dass Netzwerke dauerhaft ausgestrahlt werden (Wert: 9999), so gilt dies gleichermaßen für lokal am LAN ausgekoppelte Netzwerke, als auch für via WLC-Tunnel verbundene Netzwerke. Im Falle eines Ausfalls des WLC werden beide Arten von Netzen somit weiter ausgestrahlt; sinnvoll ist dies aber nur für via LAN ausgekoppelte Netzwerke, da via WLC-Tunnel angebundenen Netzwerken ihr Endpunkt in Form des WLCs fehlt und diese damit nicht einsatzfähig sind.

Mit diesem Schalter können die beiden Arten von Netzwerken getrennt behandelt werden.

- Ist der Schalter gesetzt, werden lokal ausgekoppelte Netzwerke dauerhaft autark weiterbetrieben. Über einen WLC-Tunnel ausgekoppelte Netzwerke werden hingegen nur ausgestrahlt, wenn der WLC erreichbar ist.
- Ist der Schalter nicht gesetzt, wird weiterhin die unter **Autarker Weiterbetrieb** angegebene Zeit verwendet.

Autarker Weiterbetrieb

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

Der WLC weist dem AP die Konfiguration zu, der sie optional im Flash speichert (in einem Bereich, der nicht mit LANconfig oder anderen Tools auszulesen ist). Falls die Verbindung zum WLC abbricht, arbeitet der AP für die hier eingestellte Zeit mit seiner Konfiguration aus dem Flash weiter. Auch nach einem eigenen Stromausfall kann der AP mit der Konfiguration aus dem Flash weiterarbeiten.

Wenn die eingestellte Zeit abgelaufen ist, bevor die Verbindung zum WLC wiederhergestellt ist, löscht der AP die Konfiguration im Flash – der AP stellt seinen Betrieb ein. Sobald der WLC wieder erreichbar ist, überträgt der WLC die Konfiguration erneut zum AP.

Diese Maßnahme stellt einen wirksamen Schutz gegen Diebstahl dar, da der AP die sicherheitsrelevanten Parameter der Konfiguration nach Ablauf der eingestellten Zeit automatisch löscht.

Stellt der AP im Backup-Fall eine Verbindung zu einem sekundären WLC her, so unterbricht der AP den Count-Down für den autarken Weiterbetrieb. Der AP bleibt also mit seinen WLAN-Netzwerken auch über diese eingestellte Zeit hinaus aktiv, solange er eine Verbindung zu einem WLC hat.

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

Zeitrahmen

Wählen Sie hier einen der in **WLAN-Controller** > **Allgemein** > **Zeitrahmen** definierten Zeitrahmen aus. Über diesen kann die Ausstrahlung dieser SSID auf die dort definierten Zeiten eingeschränkt werden. Somit lässt sich z. B. in einer Schule ein WLAN nur während der Unterrichtszeiten aktivieren.

802.11u-Netzwerk-Profil

Wählen Sie aus der Liste ein Hotspot-2.0-Profil aus.

OKC aktiviert

Mit dieser Option aktivieren Sie das opportunistische Schlüssel-Caching (Opportunistic Key Caching). Das OKC ermöglicht es WLAN-Clients, schnell und komfortabel in WLAN-Umgebungen mit WPA2-Enterprise-Verschlüsselung zwischen WLAN-Zellen zu wechseln (Roaming).

MAC-Prüfung aktiviert

In der MAC-Filterliste (**Wireless-LAN** > **Stationen/LEPS** > **LEPS-MAC** > **Stationsregeln**) sind die MAC-Adressen der Clients hinterlegt, die sich bei einem AP einbuchen dürfen. Mit dem Schalter **MAC-Filter aktiviert** können Sie die Verwendung der MAC-Filterliste gezielt für einzelne logische Netzwerke ausschalten.

SSID-Broad. unterdrücken

Sie können Ihr Funk-LAN entweder in einem öffentlichen oder in einem privaten Modus betreiben. Ein Funk-LAN im öffentlichen Modus kann von Mobilstationen in der Umgebung ohne weiteres kontaktiert werden. Durch

Aktivieren der Closed-Network-Funktion versetzen Sie Ihr Funk-LAN in einen privaten Modus. In dieser Betriebsart sind Mobilstationen ohne Kenntnis des Netzwerknamens (SSID) von der Teilnahme am Funk-LAN ausgeschlossen.

Schalten Sie den "Closed-Network-Modus" ein, wenn Sie verhindern möchten, dass sich WLAN-Clients mit der SSID "Any" oder einer leeren SSID in Ihrem Funknetzwerk anmelden.

Die Option **SSID-Broadcast unterdrücken** ermöglicht folgende Einstellungen:

- **Nein**: Der AP veröffentlicht die SSID der Funkzelle. Sendet ein Client einen Probe Request mit leerer oder falscher SSID, antwortet der AP mit der SSID der Funkzelle (öffentliches WLAN).
- **Ja**: Der AP veröffentlicht die SSID der Funkzelle nicht. Sendet ein Client einen Probe Request mit leerer SSID, antwortet der AP ebenfalls mit einer leeren SSID.
- **Verschärft**: Der AP veröffentlicht die SSID der Funkzelle nicht. Sendet ein Client einen Probe Request mit leerer oder falscher SSID, antwortet der AP überhaupt nicht.

Das einfache Unterdrücken der SSID bietet keinen ausreichenden Zugriffsschutz, da der AP diese bei der Anmeldung berechtigter WLAN-Clients im Klartext überträgt und sie somit für alle im WLAN-Netz befindlichen WLAN-Clients kurzfristig sichtbar ist.

RADIUS-Accounting aktiviert

Aktivieren Sie diese Option, wenn Sie das RADIUS-Accounting in diesem logischen WLAN-Netzwerkm aktivieren wollen.

Datenverkehr zulassen zwischen Stationen dieser SSID

Aktivieren Sie diese Option, wenn alle Stationen, die an dieser SSID angemeldet sind, untereinander kommunizieren dürfen.

WPA-Version

Wählen Sie hier die WPA-Version aus, die der AP den WLAN-Clients zur Verschlüsselung anbieten soll.

- WPA1: Nur WPA1
- WPA2: Nur WPA2
- WPA3: Nur WPA3
- WPA1/2: Sowohl WPA1 als auch WPA2 in einer SSID (Funkzelle)
- WPA2/3: Sowohl WPA2 als auch WPA3 in einer SSID (Funkzelle)
- WPA1/2/3: WPA1, WPA2 und WPA3 in einer SSID (Funkzelle)

WPA1 Sitzungsschl.-Typ

Wenn Sie als Verschlüsselungsmethode "802.11i (WPA)-PSK" nutzen, können Sie hier das Verfahren zur Generierung des Sitzungs- bzw. Gruppenschlüssels für WPA1 auswählen:

- AES: Der AP verwendet das AES-Verfahren.
- TKIP: Der AP verwendet das TKIP-Verfahren.
- AES/TKIP: Der AP verwendet das AES-Verfahren. Falls die Client-Hardware das AES-Verfahren nicht unterstützt, wechselt der AP zum TKIP-Verfahren.

WPA2 und WPA3 Sitzungsschlüssel-Typen

Wählen Sie hier das Verfahren zur Generierung des Sitzungs- bzw. Gruppenschlüssels für WPA2 und WPA3 aus.

Basis-Geschwindigkeit

Die eingestellte Basis-Geschwindigkeit sollte es auch unter ungünstigen Bedingungen erlauben, die langsamsten Clients im WLAN zu erreichen. Stellen Sie hier nur dann eine höhere Geschwindigkeit ein, wenn alle Clients in diesem logischen WLAN auch "schneller" zu erreichen sind. Bei automatischer Festlegung der Übertragungsrate sammelt der AP die Informationen über die Übertragungsraten der einzelnen WLAN-Clients.

Die Rate teilen die Clients dem AP automatisch bei jeder Unicast-Kommunikation mit. Aus der Liste der angemeldeten Clients wählt der AP nun ständig die jeweils niedrigste Übertragungsrate aus und überträgt damit die Multicast- und Broadcast-Sendungen.

Client-Bridge-Unterst.

Aktivieren Sie diese Option für einen AP, wenn Sie im WLAN-Client-Modus für eine Client-Station die Client-Bridge-Unterstützung aktiviert haben.

Der Client-Bridge-Modus ist ausschließlich zwischen zwei LANCOM-Geräten verwendbar.

TX Bandbr.-Begrenzung

Über diese Einstellung definieren Sie die zur Verfügung stehende Gesamtbandbreite in Senderichtung für die betreffende SSID. Der Wert 0 deaktiviert die Begrenzung.

RX Bandbr.-Begrenzung

Über diese Einstellung definieren Sie die zur Verfügung stehende Gesamtbandbreite in Empfangsrichtung für die betreffende SSID. Der Wert 0 deaktiviert die Begrenzung.

Client TX Bandbr.-Begrenzung

Hier begrenzen Sie die Bandbreite (Limit in kBit/s) in Senderichtung, die jedem WLAN-Client auf dieser SSID zur Verfügung steht. Der Wert 0 deaktiviert die Begrenzung.

Client RX Bandbr.-Begrenzung

Hier begrenzen Sie die Bandbreite (Limit in kBit/s) in Empfangsrichtung, die jedem WLAN-Client auf dieser SSID zur Verfügung steht. Der Wert 0 deaktiviert die Begrenzung.

Maximalzahl der Clients

Legen Sie hier die maximale Anzahl der Clients fest, die sich bei diesem AP einbuchen dürfen. Weitere Clients, die sich über diese Anzahl hinaus anmelden wollen, lehnt der AP ab.

Min. Client-Signal-Stärke

Mit diesem Eintrag bestimmen Sie den Schwellwert in Prozent für die minimale Signalstärke für Clients beim Einbuchen. Unterschreitet ein Client diesen Wert, sendet der AP keine Probe-Responses mehr an diesen Client und verwirft die entsprechenden Anfragen.

Ein Client mit schlechter Signalstärke findet den AP somit nicht und kann sich nicht darauf einbuchen. Das sorgt beim Client für eine optimierte Liste an verfügbaren APs, da keine APs aufgeführt werden, mit denen der Client an der aktuellen Position nur eine schwache Verbindung aufbauen könnte.

Client-Trennen-Signal-Stärke

Wenn dieser Schwellenwert unterschritten wird, dann wird der Client disassoziiert. Dadurch lässt sich vermeiden, dass der Client an einer aufgrund der geringen Signalstärke de facto bereits unbrauchbaren WLAN-Verbindung hängen bleibt anstatt auf eine am Client oft ebenfalls verfügbare Mobiltelefon-Verbindung umzuschalten – ein Verhalten, welches sich bei Mobiltelefonen immer wieder beobachten lässt und für den Benutzer ärgerlich ist.

Dieser Schwellenwert funktioniert nur, wenn auch der Wert **Minimale Client-Signal-Stärke** gesetzt ist und außerdem **Client-Trennen-Signal-Stärke** kleiner als dieser Wert ist.

LBS-Tracking aktiviert

Diese Option gibt an, ob der LBS-Server die Client-Informationen nachverfolgen darf.

Diese Option konfiguriert das Tracking aller Clients einer SSID. Im Public Spot-Modul bestimmen Sie, ob der LBS-Server die am Public Spot angemeldeten Benutzer tracken darf.

LBS-Tracking-Liste

Mit diesem Eintrag legen Sie den Listennamen für das LBS-Tracking fest. Bei einem erfolgreichen Einbuchen eines Clients in diese SSID überträgt der AP den angegebenen Listennamen, die MAC-Adresse des Clients und die eigene MAC-Adresse an den LBS-Server.

Lange Präambel bei 802.11b verwenden

Normalerweise handeln die Clients im 802.11b-Modus die Länge der zu verwendenden Präambel mit dem AP selbst aus. Stellen Sie hier die "lange Präambel" nur dann fest ein, wenn die Clients diese feste Einstellung verlangen.

(U-)APSD / WMM-Powersave aktiviert

Aktivieren Sie diese Option, um Stationen die Unterstützung für den Stromsparmechanismus (U-)APSD ([Unscheduled] Automatic Power Save Delivery) zu signalisieren.

(U-)APSD ist im Standard 802.11e verankert und hilft VoWLAN-Geräten dabei, ihre Akkulaufzeit zu erhöhen. Die betreffenden Geräte schalten dafür nach der Anmeldung an einem (U-)APSD-fähigen AP in den Energiesparmodus um. Erhält der AP nun Datenpakete für das betreffende Gerät, speichert es die Daten kurz zwischen und wartet, bis das VoWLAN-Gerät wieder verfügbar ist. Erst dann leitet er die Daten weiter. (U-)APSD erhöht demnach die Latenzzeit des Funkmoduls, wodurch es letztlich weniger Strom verbraucht. Die einzelnen Ruhezeiten können dabei so kurz ausfallen, dass ein VoWLAN-Gerät selbst im Gesprächszustand noch den Stromsparmechanismus benutzen kann. Die betreffenden Geräte müssen (U-)APSD allerdings ebenfalls unterstützen.

Bei WWM (Wi-Fi Multimedia) Power Save handelt es sich um einen Stromsparmechanismus der Wi-Fi Alliance, welcher auf U-APSD basiert. Bestimmte LANCOM APs sind von der Wi-Fi Alliance WMM® Power Save CERTIFIED.

Max. Spatial-Streams

Mit der Funktion des Spatial-Multiplexing kann der AP mehrere separate Datenströme über separate Antennen übertragen, um so den Datendurchsatz zu verbessern. Der Einsatz dieser Funktion ist nur dann zu empfehlen, wenn die Gegenstelle die Datenströme mit entsprechenden Antennen verarbeiten kann.

In der Einstellung 'Automatisch' nutzt der AP alle Spatial-Streams, die das jeweilige WLAN-Modul unterstützt.

Kurzes Guard-Intervall zulassen

Dieser Option reduziert die Sendepause zwischen zwei Signalen von 0,8 s (Standard) auf 0,4 s (Short Guard Interval). Dadurch steigt die effektiv für die Datenübertragung genutzte Zeit und damit der Datendurchsatz. Auf der anderen Seite ist das WLAN-System damit anfälliger für Störungen, welche durch die Interferenzen zwischen zwei aufeinanderfolgenden Signalen auftreten können.

Im Automatik-Modus wird das kurze Guard-Intervall aktiviert, sofern die jeweilige Gegenstelle diese Betriebsart unterstützt. Alternativ kann die Nutzung des kurzen Guard-Intervalls auch ausgeschaltet werden.

Frame-Aggregation verwenden

Bei der Frame-Aggregation werden mehrere Datenpakete (Frames) zu einem größeren Paket zusammengefasst und gemeinsam versendet. Dieses Verfahren reduziert den Overhead der Pakete, der Datendurchsatz steigt.

Die Frame-Aggregation eignet sich weniger gut bei schnell bewegten Empfängern oder für zeitkritische Datenübertragungen wie Voice over IP.

STBC (Space Time Block Coding) aktiviert

Aktivieren Sie hier das Space Time Block Coding.

Die Funktion 'STBC' variiert den Versand von Datenpaketen zusätzlich über die Zeit, um auch zeitliche Einflüsse auf die Daten zu minimieren. Durch den zeitlichen Versatz der Sendungen besteht für den Empfänger eine noch bessere Chance, fehlerfreie Datenpakete zu erhalten, unabhängig von der Anzahl der Antennen.

LDPC (Low Density Parity Check) aktiviert

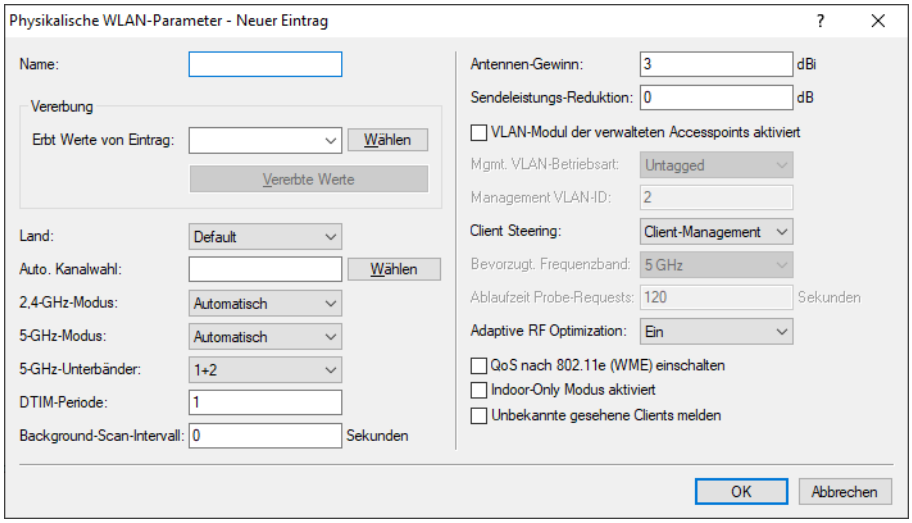
Aktivieren Sie hier den Low Density Parity Check.

Bevor der Sender die Datenpakete abschickt, erweitert er den Datenstrom abhängig von der Modulationsrate um Checksummen-Bits, um dem Empfänger damit die Korrektur von Übertragungsfehlern zu ermöglichen. Standardmäßig nutzt der Übertragungsstandard IEEE 802.11n das bereits aus den Standards 802.11a und 802.11g bekannte 'Convolution Coding' (CC) zur Fehlerkorrektur, ermöglicht jedoch auch eine Fehlerkorrektur nach der LDPC-Methode (Low Density Parity Check).

Im Unterschied zur CC-Kodierung nutzt die LDPC-Kodierung größere Datenpakete zur Checksummenberechnung und kann zusätzlich mehr Bit-Fehler erkennen. Die LDPC-Kodierung ermöglicht also bereits durch ein besseres Verhältnis von Nutz- zu Checksummen-Daten eine höhere Datenübertragungsrate.

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 unter **WLAN-Controller** > **Profile** > **Physikalische WLAN-Parameter** die folgenden Parameter definieren:



Name

Eindeutiger Name für diese Zusammenstellung von physikalischen WLAN-Parametern.

Vererbung

Auswahl eines schon definierten Satzes von physikalischen WLAN-Parametern, von dem die Einstellungen übernommen werden sollen.

Land

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

Automatische Kanalwahl

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

Tragen Sie hier die Kanäle als kommaseparierte Liste ein, auf die sich die automatische Auswahl 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.

Dabei ist auch die Angabe von Bereichen möglich. Z. B. würde die Angabe „1,7-9,13“ bei der automatischen Kanalsuche nur die Kanäle 1, 7 bis 9 und 13 berücksichtigen.

Solange die Radarerkennung eingeschaltet ist, handelt es sich lediglich um eine Bevorzugung der hier eingetragenen Kanäle. Werden diese durch Radarimpulse beeinflusst, wird versucht auf weitere Kanäle auszuweichen, die hier nicht aufgeführt sind. Erst wenn die Radarerkennung durch Einschalten des Indoor-Only-Modus abgeschaltet ist, findet die Auswahl der Kanäle exklusiv statt.

Die hier getroffene Kanaleinstellung wird auch zur Funkfeldoptimierung des Access Points herangezogen, falls diese aktiviert ist. Ist die Kanalanzahl hier eingeschränkt worden, kann auch nur innerhalb dieser Kanäle optimiert werden.

DTIM-Periode

Sobald mindestens ein mobiles Endgerät (Client) Stromsparmechanismen verwendet, werden Broad- und Multicasts nicht mehr unmittelbar in die Funkzelle gesendet, sondern gesammelt nach den regelmäßig von dem Access Point ausgestrahlten Beacon. Da den Clients das nächste relevante Beacon bekannt gegeben wird und sie sich daher auf die Aussendung der Broad- und Multicasts synchronisieren können, ermöglicht ihnen dies, ihr Funkmodul die meiste Zeit ausgeschaltet zu lassen und es nur zu diesen Zeitpunkten zu aktivieren.

Die DTIM-Periode gibt an, nach jeweils wievielen Beacons gesammelte Broad- und Multicasts ausgestrahlt werden. Höhere Werte erlauben Clients, mehr Energie zu sparen, erhöhen aber auch die Latenz bei der Zustellung dieser Pakete.

Der Standard-Wert ist 1, d .h. gesammelte Broad- und Multicasts werden nach jedem Beacon ausgestrahlt.

Management VLAN-ID

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

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

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

Client Steering

Dieser Eintrag bestimmt die Art des Client Steerings und ob der AP das Band-Steering aktivieren soll. In diesem Fall kann ein Dual-Port-Access-Point einen WLAN-Client auf ein bevorzugtes Frequenzband umleiten.

Das Client-Steering ermöglicht den APs, die im Sendebereich befindlichen WLAN-Clients anhand bestimmter Kriterien zu veranlassen, sich immer mit dem für sie idealen AP zu verbinden. Die Kriterien sind zentral im WLAN-Controller definiert. Die verwalteten Access Point melden ständig die aktuellen Werte an den WLAN-Controller, der aufgrund der Kriterien entscheidet, welche Access Points die Anfragen von WLAN-Clients beantworten dürfen. Deshalb ist das Client-Steering auch nur mit Access Points möglich, die ein WLAN-Controller zentral verwaltet.

Aus

Das Client-Steering ist deaktiviert.

Ein

Der AP lässt das Client-Steering vom WLC durchführen.

Client Management

Das Client Steering wird dezentral von den APs durchgeführt.

AP-basiertes Band-Steering

Der AP leitet den WLAN-Client eigenständig auf ein bevorzugtes Frequenzband.

Unbekannte gesehene Clients melden

Der Access-Point meldet standardmäßig nur bekannte (also assoziierte) Clients an den WLC. Sollen darüber hinaus auch alle übrigen gesehenen (also unbekannte und nicht assoziierte) Clients gemeldet werden, so können Sie diesen Schalter aktivieren. Dies erhöht natürlich den Datenverkehr im Netz. Sie sollten diesen Schalter daher nur vorübergehend oder zu Testzwecken aktivieren.

Wenn mit einer Vielzahl von unbekannten Clients zu rechnen ist (z. B. bei einem Public Spot oder in Bereichen mit regem Publikumsverkehr), sollten Sie diesen Schalter nicht aktivieren, da Sie ansonsten von den eingehenden Meldungen überflutet werden.

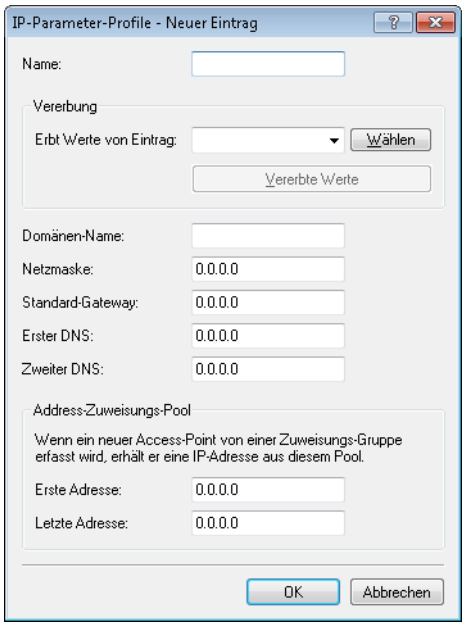
Alle weiteren physikalischen WLAN-Parameter entsprechen denen der üblichen Konfiguration für APs.

Für den erfolgreichen Profilbezug ist es erforderlich, dass der HTTP-Zugriff auf den WLC aus dem lokalen Netz erlaubt ist.

1.4.3 Access Point Konfiguration

IP-Parameter-Profile

In dieser Tabelle definieren Sie bestimmte Netzprofile, welche sich einem AP zuweisen lassen, den der WLC nicht automatisch via DHCP konfigurieren soll. Auf diese Weise legen Sie gezielt fest, welche IP-Parameter ein AP nutzt.



Name

Name des IP-Parameter-Profils.

Vererbung

Auswahl eines schon definierten IP-Parameter-Profils, von dem die Einstellungen übernommen werden sollen (siehe *Vererbung von Parametern* auf Seite 24).

Domänen-Name

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

Netzmaske

Netzmaske des Profils.

Standard-Gateway

Standard-Gateway, welches das Profil verwendet.

Erster DNS

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

Zweiter DNS

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

Erste Adresse

Anfang des IPv4-Adressbereichs, aus dem ein neuer AP eine IP-Adresse erhält, wenn der WLC den AP einer Zuweisungs-Gruppe zuordnen kann und Sie für den betreffenden AP in der AP-Tabelle keine konkrete IP-Adresse definiert haben.

Letzte Adresse

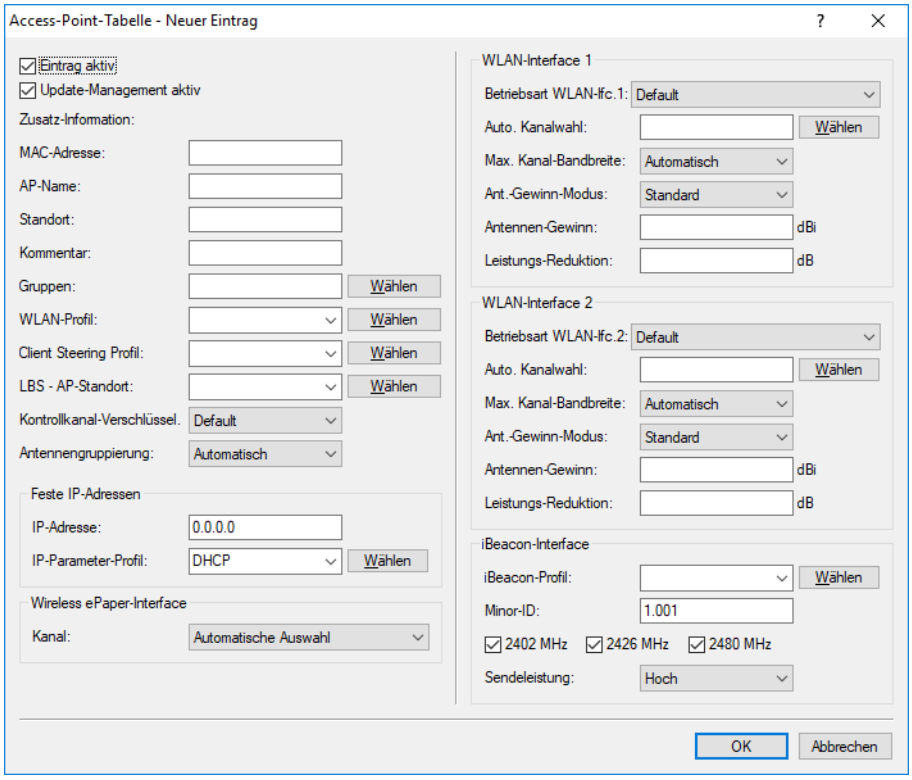
Ende des IPv4-Adressbereichs, aus dem ein neuer AP eine IP-Adresse erhält, wenn der WLC den AP einer Zuweisungs-Gruppe zuordnen kann und Sie für den betreffenden AP in der AP-Tabelle keine konkrete IP-Adresse definiert haben.

Weitere Informationen zu den Zuweisungs-Gruppen finden Sie im Abschnitt *IP-abhängige Autokonfiguration und Tagging von APs* auf Seite 69.

Liste der Access Points

Die Access Point-Tabelle ist ein zentraler Aspekt der Konfiguration für WLCs. Hier ordnet der WLC den Access Points über WLAN-Profile (also Kombinationen aus logischen und physikalischen WLAN-Parametern) ihre MAC-Adresse zu. Außerdem hat die reine Existenz eines Eintrages in der Access Point-Tabelle für einen bestimmten Access Point Auswirkungen auf

die Möglichkeit, eine Verbindung zu einem WLC aufbauen zu können. Für jeden Access Point können Sie unter **WLAN-Controller** > **AP-Konfiguration** > **Access-Point-Tabelle** die folgenden Parameter definieren:



Eintrag aktiv

Aktiviert bzw. deaktiviert diesen Eintrag.

Update-Management aktiv

Wenn Sie für diesen Access Point das Update-Management aktivieren, kann er neue Firmware- oder Script-Versionen automatisch laden. Nehmen Sie alle weiteren Einstellungen unter Access Point-Update vor (*Zentrales Firmware- und Skript-Management*).

MAC-Adresse

MAC-Adresse des Access Points.

AP-Name

Name des Access Points im Managed-Modus.

Standort

Standort des Access Points im Managed-Modus.

Gruppen

Ordnet den Access Point einer oder mehrerer Gruppen zu

WLAN-Profil

WLAN-Profil aus der Liste der definierten Profile.

Client Steering Profil

Client Steering-Profile legen die Bedingungen fest, nach denen der WLC entscheidet, welche Access Points beim nächsten Anmeldeversuch einen Client annehmen.

LBS-AP-Standort-Profil

LBS-Standort-Profil aus der Liste der definierten Profile.

Kontrollkanal-Verschlüsselung

Verschlüsselung für die Kommunikation über den Kontrollkanal. Ohne Verschlüsselung tauschen Access Point und WLC die Kontrolldaten im Klartext aus. Eine Authentifizierung mittels Zertifikat findet in beiden Fällen statt.

Antennengruppierung

Um den Gewinn durch Spatial-Multiplexing zu optimieren, kann die Antennengruppierung konfiguriert werden.

IP-Adresse

Spezifizieren Sie hier eine feste IP-Adresse des Access Points.

IP-Parameter-Profil

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

Kanal (Wireless ePaper-Interface)

Bestimmen Sie hier, wie die Kanalwahl der Wireless ePaper-Schnittstelle erfolgen soll.

Betriebsart WLAN-Ifc. 1

Über diese Einstellung konfigurieren Sie das Frequenzband, in dem der Access Point die 1. physikalische WLAN-Schnittstelle betreibt. In der Einstellung **Default** wählt der Access Point das Frequenzband für die physikalische WLAN-Schnittstelle selbstständig aus. Dabei behandelt der Access Point das 2,4-GHz-Band bevorzugt, sofern dieses verfügbar ist.

Betriebsart WLAN-Ifc. 2

Über diese Einstellung konfigurieren Sie das Frequenzband, in dem der Access Point die 2. physikalische WLAN-Schnittstelle betreibt. In der Einstellung **Default** wählt der Access Point das Frequenzband für die physikalische WLAN-Schnittstelle selbstständig aus. Dabei behandelt der Access Point das 5-GHz-Band bevorzugt, sofern dieses verfügbar ist.

Sofern ein verwalteter Access Point lediglich über eine physikalische WLAN-Schnittstelle verfügt, ignoriert der Access Point die Einstellungen für die 2. physikalische WLAN-Schnittstelle.

Auto. Kanalwahl

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. Geben Sie hier nur einen Kanal an, so verwendet der Access Point nur diesen 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 ignoriert der Access Point.

Max. Kanal-Bandbreite

Geben Sie an, wie und in welchem Umfang der Access Point die Kanal-Bandbreite für die physikalische(n) WLAN-Schnittstelle(n) festlegt. Folgende Werte sind möglich:

- **Automatisch**: Der Access Point ermittelt automatisch die maximale Kanal-Bandbreite (Default).
- **20 MHz**: Der Access Point benutzt auf 20 MHz gebündelte Kanäle.
- **40 MHz**: Der Access Point benutzt auf 40 MHz gebündelte Kanäle.
- **80 MHz**: Der Access Point benutzt auf 80 MHz gebündelte Kanäle.

Standardmäßig bestimmt die physikalische WLAN-Schnittstelle den Frequenzbereich, in dem die zu übertragenen Daten auf die Trägersignale aufmoduliert werden, automatisch. 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.

Ant.-Gewinn-Modus

Bei der Inbetriebnahme von Access Points an einem WLAN-Controller wurden diese bisher immer mit einem Antennengewinn von 3 dBi je Modul eingerichtet, da dieser Wert für die meisten Indoor-Access Points mit Standardantennen passend ist. Insbesondere für Outdoor-Access Points mit integrierten Antennen musste der Wert aber in der Vergangenheit manuell angepasst werden, die hier häufig interne Antennen mit einem hohen Antennengewinn zum Einsatz kommen. Ab LCOS 10.30 wird der Standard-Antennengewinn eines verwalteten Access Points an den WLAN-Controller übertragen und dort automatisch verwendet. Für diese Funktion müssen sowohl der Access Point als auch der WLAN-Controller, mindestens den Firmware-Stand 10.30 aufweisen. Mit dieser Einstellung für den Modus des Antennengewinns wird verhindert, dass man nach einem Rollout einige Access Points noch manuell korrigieren muss.

Mögliche Werte:

Standard

Der im Access Point voreingestellte Wert für den Antennengewinn wird verwendet.

Benutzerdefiniert

Der im Feld **Antennen-Gewinn** eingestellte Wert wird verwendet.

Antennen-Gewinn

Mit diesem Eintrag können Sie den Antennen-Verstärkungsfaktor (Gewinn in dBi) abzüglich der Dämpfungen für Kabel und ggf. Blitzschutz angeben. Hieraus errechnet der Access Point die im jeweiligen Land und für das jeweilige Frequenzband maximal zulässige Sendeleistung.

Wenn Sie das Feld leer lassen, verwendet der Access Point die Default-Einstellung der Konfigurationsgruppe im verwendeten WLAN-Profil.

Sie können die Sendeleistung auf minimal 0,5 dBm im 2,4-GHz-Band bzw. 6,5 dBm im 5-GHz-Band reduzieren. Das begrenzt den maximal einzutragenden Wert im 2,4-GHz-Band auf 17,5 dBi, im 5-GHz-Band auf 11,5 dBi.

Achten Sie darauf, dass Ihr Antennen-, Kabel- und Blitzschutz-Aufbau unter diesen Bedingungen den Regulierungsanforderungen des Landes entspricht, in dem Sie das System einsetzen.

Die Empfindlichkeit des Empfängers bleibt hiervon unbeeinflusst.

Die aktuelle Sendeleistung können Sie mit Hilfe von WEBconfig bzw. Telnet unter **Status** > **WLAN-Statistik** > **WLAN-Parameter** > **Sendeleistung** oder per LANmonitor unter **System-Informationen** > **WLAN-Karte** > **Sendeleistung** einsehen.

Leistungs-Reduktion

Wenn Sie eine Antenne mit einem hohen Verstärkungsfaktor verwenden, können Sie mit diesem Eintrag die Sendeleistung des Access Points auf die in verwendeten Land und die im jeweiligen Frequenzband zulässige Sendeleistung herunterdämpfen.

Wenn Sie das Feld leer lassen, verwendet der Access Point die Default-Einstellung der Konfigurationsgruppe im verwendeten WLAN-Profil.

Es gelten dieselben Werte und Einschränkungen wie im Feld **Antennen-Gewinn**.

iBeacon-Profil (iBeacon-Interface)

Wählen Sie ein iBeacon-Profil aus der Liste der angelegten Profile aus.

iBeacon-Profile erstellen Sie unter **WLAN-Controller** > **AP-Konfiguration** > **Erweiterte Einstellungen** > **iBeacon-Profile**.

Minor

Legen Sie eine Minor-ID für das iBeacon-Modul fest.

2402 MHz, 2426 MHz, 2480 MHz

Definieren Sie hier, welche Sendekanäle das iBeacon-Modul verwenden soll.

Sendeleistung

Geben Sie an, Mit welcher Leistung das iBeacon-Modul senden soll. Folgende Werte sind möglich:

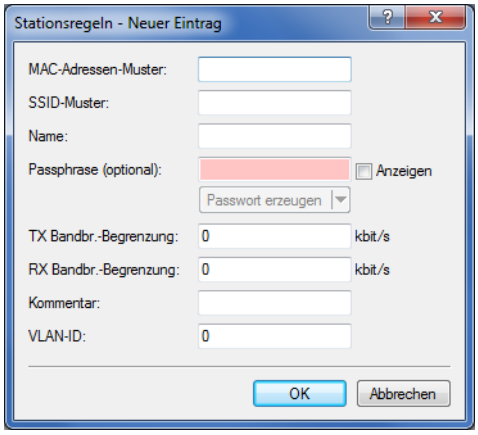
- **Hoch**: Das Modul sendet mit maximaler Leistung (Default).
- **Mittel**: Das Modul sendet mit durchschnittlicher Leistung.
- **Gering**: Das Modul sendet mit minimaler Leistung.

Stationen

Mit Hilfe der Stationsregeln legen Sie fest, welche WLAN-Clients sich in den WLAN-Netzwerken der APs anmelden können, die durch den WLC 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 Stationsregeln unter **WLAN-Controller** > **Stationen/LEPS** > **LEPS-MAC** > **Stationsregeln** muss grundsätzlich der RADIUS-Server im WLC 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.



MAC-Adresse

MAC-Adresse des WLAN-Clients, für den dieser Eintrag gilt. Die folgenden Eingaben sind möglich:

einzelne MAC-Adresse

Eine MAC-Adresse im Format `00a057112233`, `00-a0-57-11-22-33` oder `00:a0:57:11:22:33`.

Wildcards

Wildcards '*' und '?' für die Angabe von MAC-Adressbereichen, z. B. `00a057*`, `00-a0-57-11-??-??` oder `00:a0:??:11:*`.

Vendor-ID

Das Gerät hat eine Liste der gängigen Hersteller-OUIs (Organizationally Unique Identifier) gespeichert. Der MAC-Adressbereich ist gültig, wenn dieser Eintrag den ersten drei Bytes der MAC-Adresse des WLAN-Clients entspricht.

Die Verwendung von Wildcards ist möglich.

SSID-Muster

Dieser Eintrag begrenzt den Zugriff der WLAN-Clients mit den entsprechenden MAC-Adressen auf diese SSID.

Die Verwendung von Wildcards ist möglich, um den Zugriff auf mehrere SSIDs zu erlauben.

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.

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** für jedes logische Wireless-LAN-Netzwerk hinterlegten Passphrasen verwendet.

TX Bandbreitenbegrenzung

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

RX Bandbreitenbegrenzung

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

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

Kommentar

Hier können Sie einen Kommentar eintragen.

VLAN-ID

Die ID des VLANs, zu welchem dieser Client gehört. Das heißt, der Client kann nur von Paketen erreicht werden, die dem selben VLAN entstammen. Pakete, welche der Client selbst versendet, werden mit dieser VLAN-ID markiert. Sie brauchen diesen Wert nur zu setzen, wenn dieser Client zu einem anderen VLAN gehören soll, als das logische WLAN-Netzwerk (SSID), mit dem er verbunden ist. Gültige VLAN-IDs liegen im Bereich 0 bis 4094. Eine 0 bedeutet, dass der Client zu dem VLAN seines logischen WLAN-Netzwerks (SSID) gehört, sofern dieses überhaupt einem VLAN angehört.

Nutzen Sie IPv6 oder wird in einem VLAN auch Multicast verwendet, müssen den verschiedenen VLANs einer SSID zwingend verschiedene Gruppenschlüssel zugeordnet werden. Ansonsten können die

verschiedenen Multicasts nicht den richtigen Clients zugeordnet werden. Dies führt zum Beispiel bei Nutzung von IPv6 dazu, dass den Clients auch IPv6-Präfixe bekannt gegeben werden, die auf der genutzten VLAN-ID nicht funktionieren! Die Gruppenschlüssel können Sie unter **WLAN** > **Verschlüsselung** > **VLAN-Gruppenschlüssel** konfigurieren.

Falls sich Filterregeln widersprechen, hat die individuellere Regel eine höhere Priorität: Eine Regel ohne Wildcards in der MAC-Adresse oder SSID hat Vorrang vor einer Regel mit Wildcards. Ansonsten hat der Anwender beim Anlegen von Einträgen darauf zu achten, dass sich die Filterregeln nicht widersprechen. Mit dem Trace-Aufruf `trace WLAN-ACL` in einer Telnet-Sitzung lassen sich die Filterangaben kontrollieren.

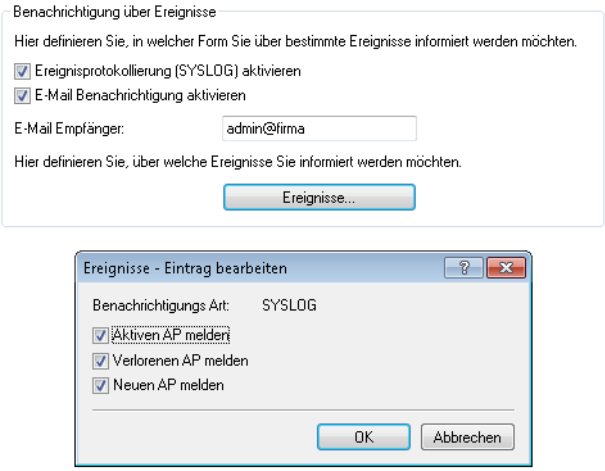
Die Filterkriterien in der Stationsliste erlauben oder verweigern den Zugriff von WLAN-Clients auf das WLAN-Netzwerk. Die Einträge **Name**, **Bandbreiten-Begrenzung**, **VLAN-ID** und **Passphrase** sind bedeutungslos, wenn das Gerät bei gültigen Filterkriterien den WLAN-Zugriff verweigert.

Optionen für den WLAN-Controller

Im Bereich der **Optionen** werden die Benachrichtigungen bei Ereignissen im WLC 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**

Ereignisprotokollierung (SYSLOG) aktivieren

Aktiviert die Benachrichtigung über SYSLOG.

E-Mail-Benachrichtigung aktivieren

Aktiviert die Benachrichtigung über E-Mail.

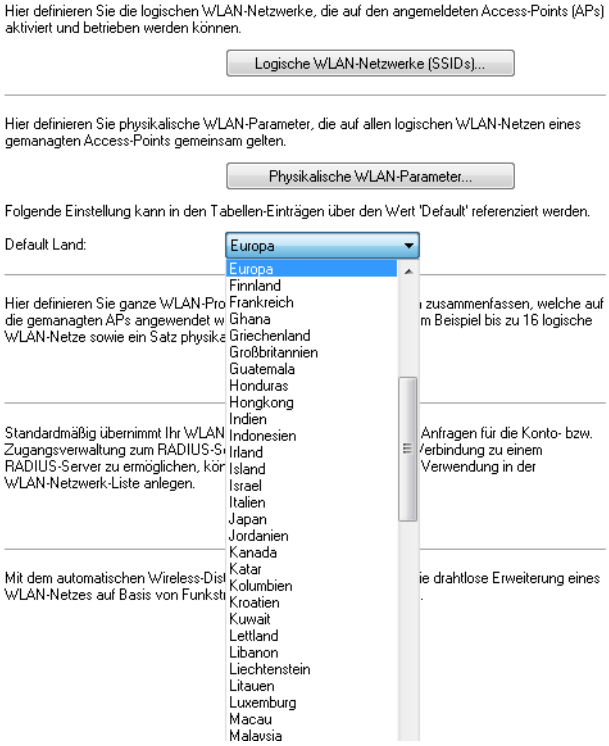
Ereignisse

Wählt die Ereignisse, die über die eine Benachrichtigung erfolgen soll. Mögliche Werte:

- Aktiven AP melden
- Verlorenen AP melden
- Neuen AP melden

Default-Parameter

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

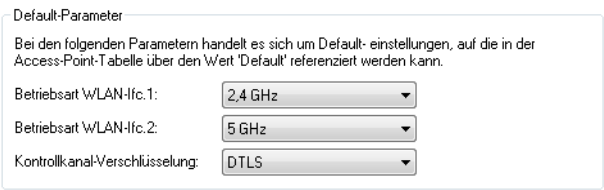


LANconfig: **WLAN-Controller** > **Profile** > **Default Land**

- **Default Land**

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

  - Mögliche Werte:
    - Auswahl aus den verfügbaren Ländern
  - Default:
    - Europa



LANconfig: **WLAN-Controller** > **AP-Konfig** >

WEBconfig: **LCOS-Menübaum** > **Setup** > **WLAN-Management** > **AP-Konfiguration**

- **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.

Virtualisierung und Gastzugang über WLAN Controller mit VLAN

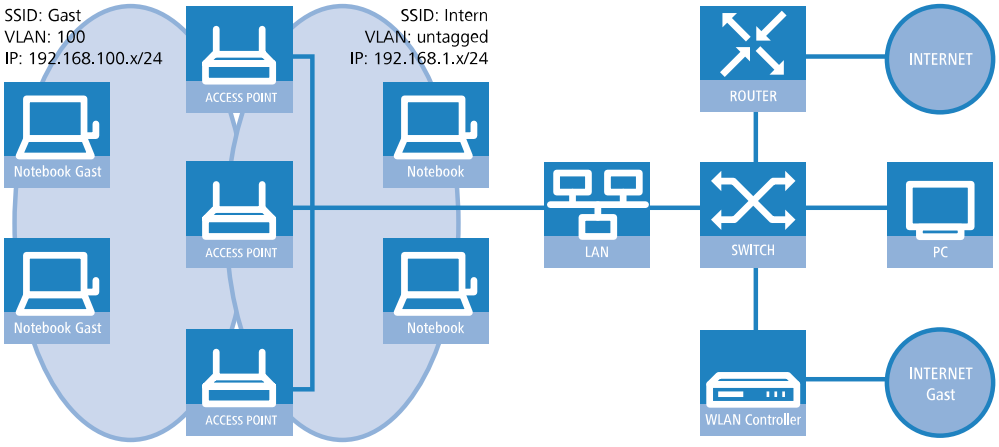
In vielen Unternehmen ist es erwünscht, den Besuchern für die mitgebrachten Notebooks o. ä. einen Internetzugang über WLAN anzubieten. In einem größeren Netzwerk mit mehreren Access Points kann die Konfiguration der nötigen Einstellungen zentral im WLAN Controller erfolgen.

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 WLC.
- Der WLC dient als DHCP-Server für die WLAN-Clients des Gastnetzes.
- Für das Gastnetz wird der Internetzugang vom 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 WLC.
  - Das VLAN-Management der Switches erfolgt separat über die Switch-Konfiguration.
- Die Access Points werden innerhalb des internen VLANs betrieben.

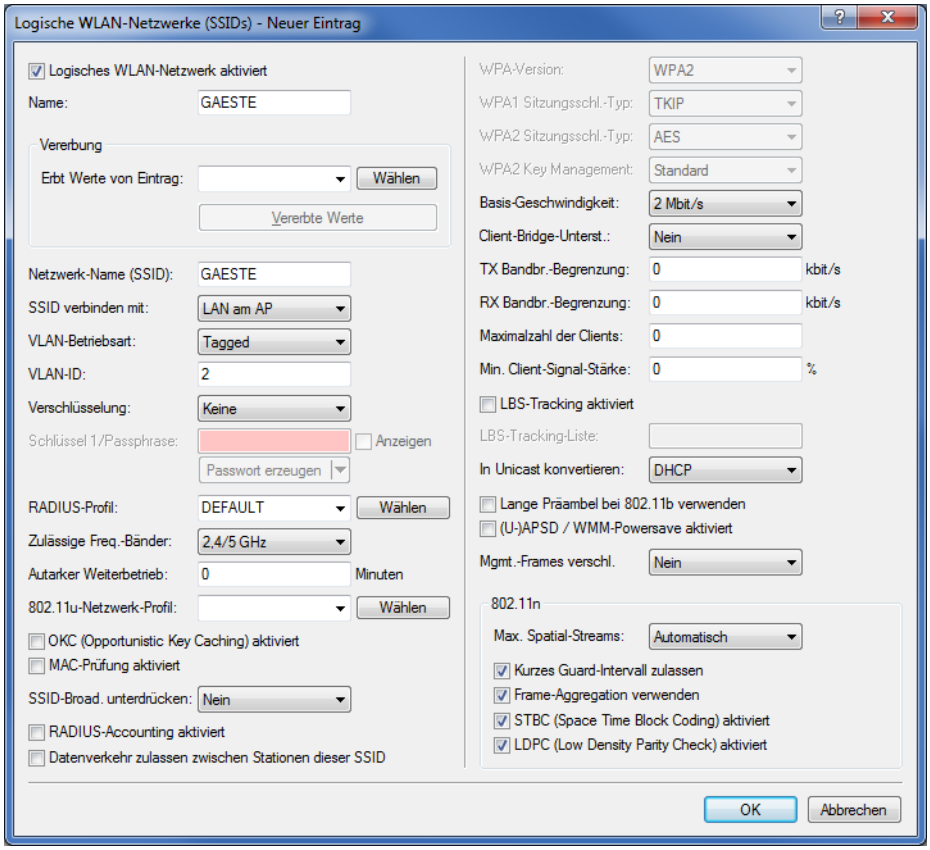


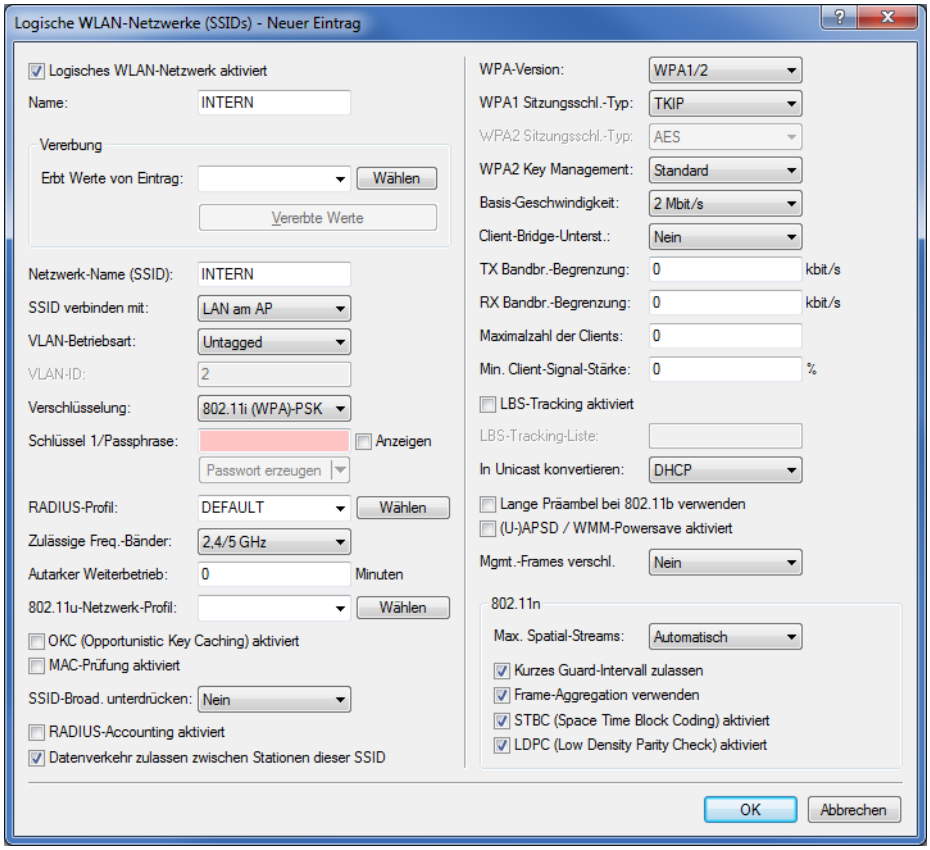
WLAN-Konfiguration des WLAN Controllers

Bei der WLAN-Konfiguration definieren Sie die benötigten WLAN-Netzwerke und weisen sie zusammen mit den physikalischen WLAN-Einstellungen den vom Controller verwalteten Access Points zu.

1. Erstellen Sie ein logisches WLAN für die Gäste und eines für die internen Mitarbeiter.
   - Das WLAN mit der SSID `GAESTE` erhält die VLAN-ID `100` (VLAN-Betriebsart **Tagged**) und verwendet **Keine** Verschlüsselung.
   - Das WLAN mit der SSID `INTERN` erhält keine VLAN-ID (VLAN-Betriebsart **Untagged**, d. h. Datenpakete werden ohne VLAN-Tag in das Ethernet übertragen) und verwendet eine Verschlüsselung nach WPA, z. B. **802.11i (WPA)-PSK**.

› LANconfig: **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke (SSIDs)**

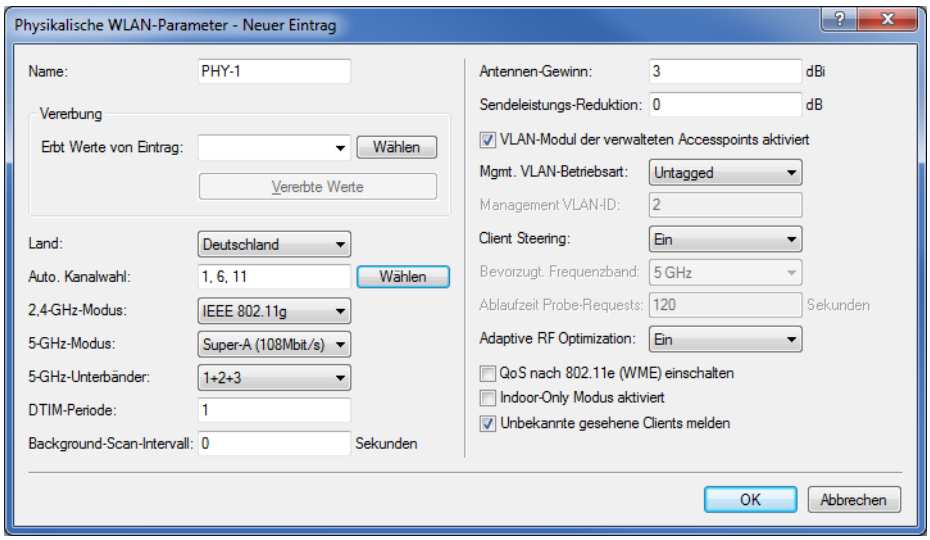




Wenn Sie die **VLAN-Betriebsart** auf **Untagged** stellen, graut LANconfig das Eingabefeld **VLAN-ID** im oben gezeigten Hinzufügen-/Bearbeiten-Dialog aus. Die dazugehörige Tabelle **Logische WLAN-Netzwerke (SSIDs)** zeigt als zugewiesene VLAN aber trotzdem den im ausgegrauten Feld ausgewiesenen Wert an. Dieser Eintrag ist lediglich programmintern, da der zulässige Wertebereich zwischen 2 und 4094 liegt. Letztlich entscheidend ist die VLAN-Betriebsart: Wenn diese auf **Untagged** steht, wird in keinem Fall eine VLAN-ID übertragen.

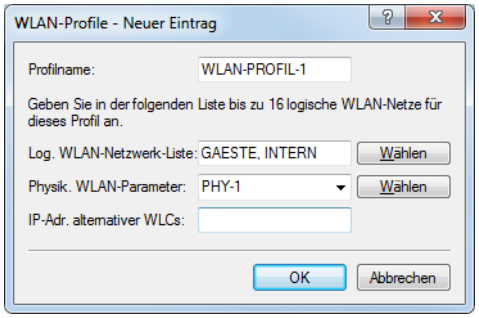
2. Erstellen Sie einen Satz von physikalischen Parametern für die verwendeten Access Points.
Dabei wird die Management-VLAN-ID auf `1` gesetzt, um die VLAN-Nutzung generell zu aktivieren (jedoch ohne separates Management-VLAN für das Gerät; der Management-Datenverkehr wird ungetagged übertragen).

› LANconfig: **WLAN-Controller** > **Profile** > **Physikalische WLAN-Parameter**



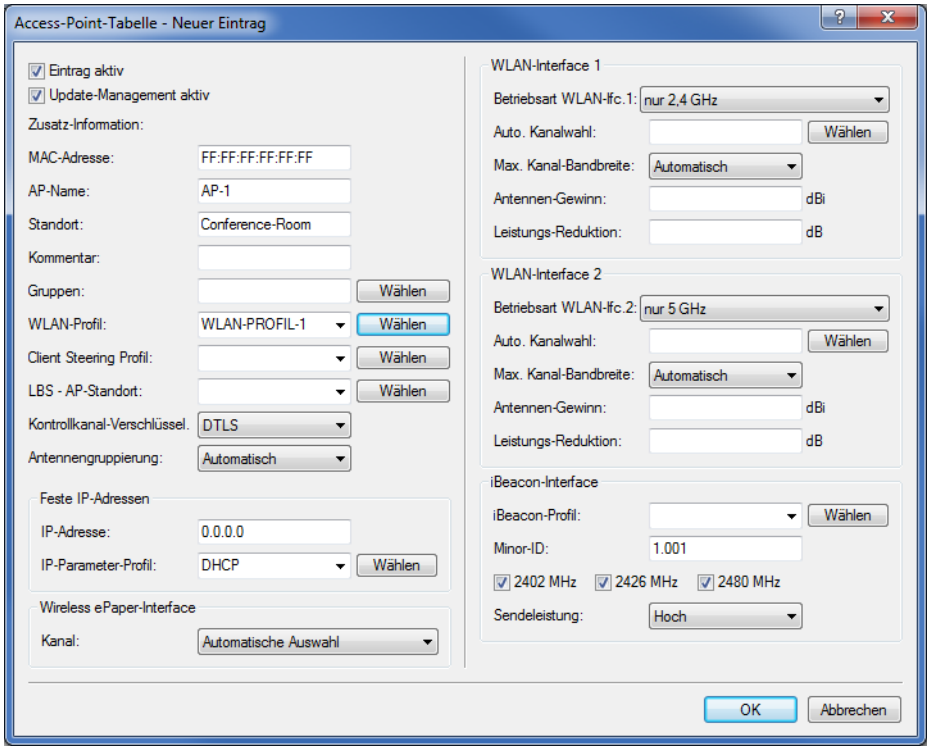
3. Erstellen Sie ein WLAN-Profil, welches Sie den Access Points zuweisen.
   Unter diesem WLAN-Profil vereinen Sie die beiden zuvor erstellten logischen WLAN-Netzwerke und den zuvor erstellten Satz von physikalischen Parametern.

   › LANconfig: **WLAN-Controller** > **Profile** > **WLAN-Profile**



4. Ordnen Sie das WLAN-Profil den vom Controller verwalteten Access Points zu.
   Tragen Sie dazu die einzelnen Access Points mit der MAC-Adresse in die Access-Point-Tabelle ein. Alternativ können Sie über die Schaltfläche **Default** auch ein Standardprofil anlegen, das für alle Access Points gilt.

   › LANconfig: **WLAN-Controller** > **AP-Konfig.** > **Access-Point-Tabelle**



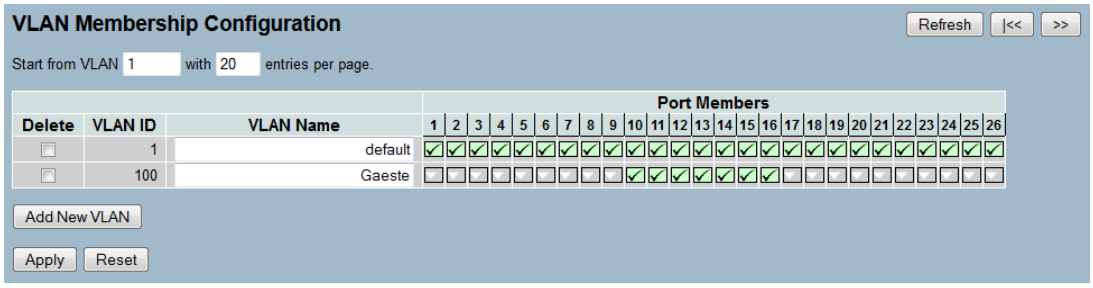
Konfiguration des Switches (LANCOM GS-2326P)

In diesem Kapitel beschreiben die Konfiguration des Switches am Beispiel eines LANCOM GS-2326P.

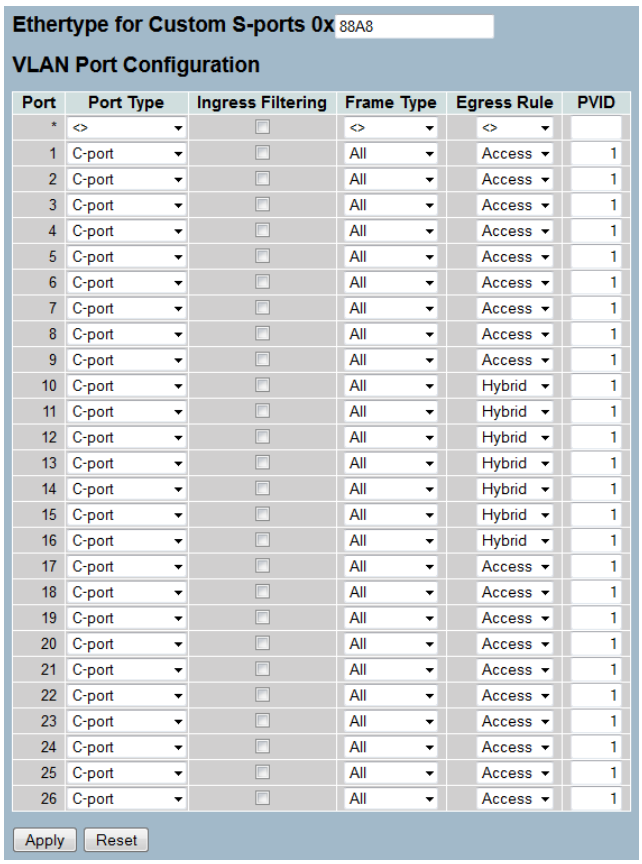
1. Legen Sie unter **Configuration** > **VLAN** > **VLAN-Membership** für das eingerichtete Gäste-Netz eine weitere VLAN-Gruppe an.

   Zur Unterscheidung der VLANs im Switch werden zwei Gruppen verwendet. Das interne Netz für die Mitarbeiter wird in der Gruppe `default` abgebildet, das der Gäste in der Gruppe `Gaeste`.

- Die VLAN-Gruppe für die internen Mitarbeiter verwendet die Default-VLAN-ID `1`. Diese zur internen Verwaltung eingesetzte VLAN-ID gilt auf allen Ports und wird ungetagged betrieben; d. h. alle ungetaggt eingehenden Datenpakete erhalten für das interne Routing die VLAN-ID 1, welche bei ausgehenden Datenpaketen wieder entfernt wird (siehe auch "PVID" im nächsten Schritt).
- Die VLAN-Gruppe für die Gäste verwendet die VLAN-ID `100`, die Sie bereits bei der Konfiguration der WLANs im Controller eingetragen haben. Sie gilt nur auf den Ports, an denen der WLAN-Controller und die Access Points angeschlossen sind (in diesem Beispiel: Port 10 bis 16, grüner Haken unter **Port Members**). Bei ausgehenden Datenpaketen entfernt der Switch die Tags nicht; d. h. alle getaggt eingehenden Datenpakete mit der VLAN-ID 100 behalten diesen Tag und werden nur an die Ports geroutet, die Mitglied der entsprechenden Gruppe sind.



2. Stellen Sie unter **Configuration** > **VLAN** > **Ports** den **Port Type** alle Ports auf **C-port**. Details zu dieser Einstellung finden Sie in der Switch-Dokumentation.
3. Konfigurieren Sie die **Egress Rule** für die einzelnen Ports.
   - Alle Ports außer Port 10 bis 16 erhalten die Regel **Access**. Dadurch leiten diese Ports nur ungetaggte Datenpakete weiter, alle anderen werden verworfen.
   - Die Ports 10 bis 16 erhalten die Regel **Hybrid**. Dadurch leiten diese Ports sowohl ungetaggte als auch getaggte Datenpakete weiter.



Achten Sie darauf, dass die **PVID** (Port-VLAN-ID) für jeden Port den Wert `1` besitzt. Die PVID ist die VLAN-ID, die ein Port eingehenden Datenpaketen ohne VLAN-Tag zuweist; daher entspricht die PVID der VLAN-ID der `default`-Gruppe.

4. OPTIONAL: Sofern Sie den Zugang zum Gäste-Netz auch über Ethernet erlauben möchten, stellen Sie unter **Configuration** > **VLAN** > **Ports** z. B. für die Ports 17 bis 20 die **PVID** auf `100`, und weisen unter **Configuration** > **VLAN** > **VLAN-Membership** diese Ports der Gruppe `Gaeste` zu. Dadurch erhalten alle über diese Ports ungetaggt eingehenden Datenpakete die VLAN-ID 100.

Beachten Sie, dass die betreffenden Datenpakete den Switch dann lediglich über die Ports des Gäste-Netzes wieder verlassen können!

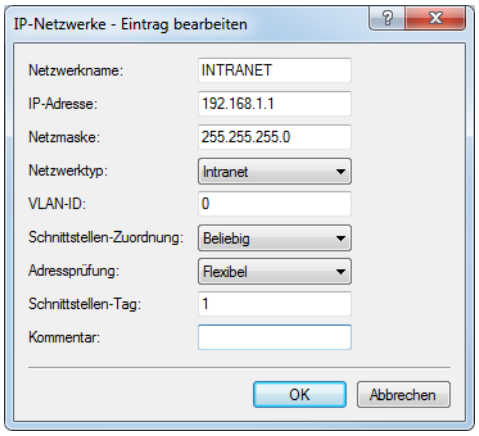
Konfiguration der IP-Netzwerke im WLAN Controller

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

1. 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.

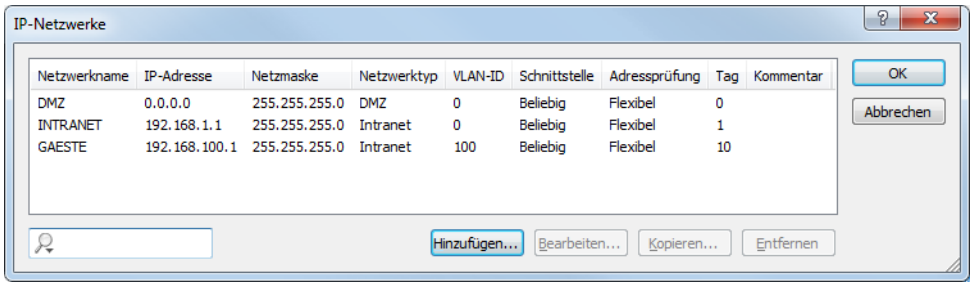
   › LANconfig: **TCP/IP** > **Allgemein** > **IP-Netzwerke**



2. Legen Sie für die Gäste ein neues IP-Netzwerk mit der Adresse `192.168.100.1` an.

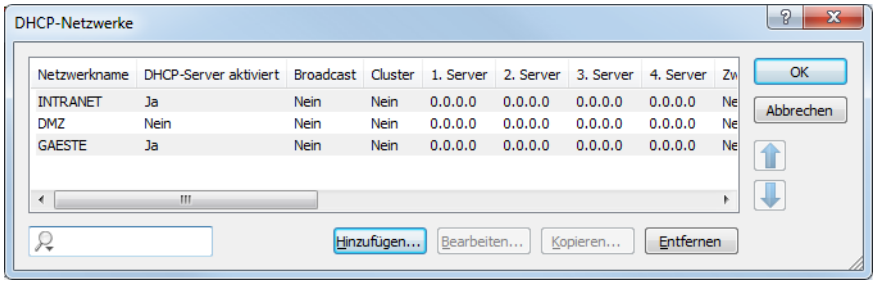
   Dieses Netzwerk verwendet die **VLAN-ID** `100`. Damit werden alle Datenpakete mit dieser ID dem Gäste-Netzwerk zugeordnet. Auch hier dient das **Schnittstellen-Tag** `10` der späteren Verwendung im virtuellen Router.

   › LANconfig: **TCP/IP** > **Allgemein** > **IP-Netzwerke**

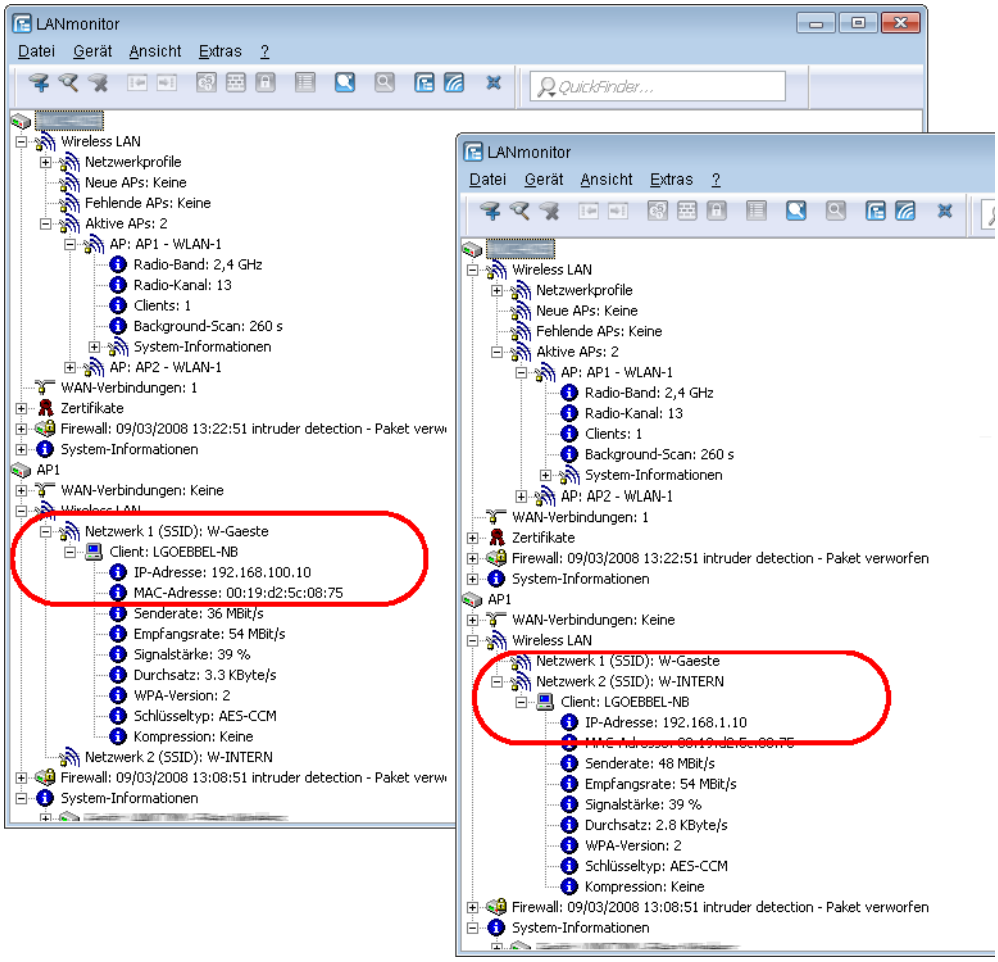


3. Aktivieren Sie für die beiden IP-Netzwerke den DHCP-Server.

› LANconfig: **TCP/IP** > **Allgemein** > **IP-Netzwerke**



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

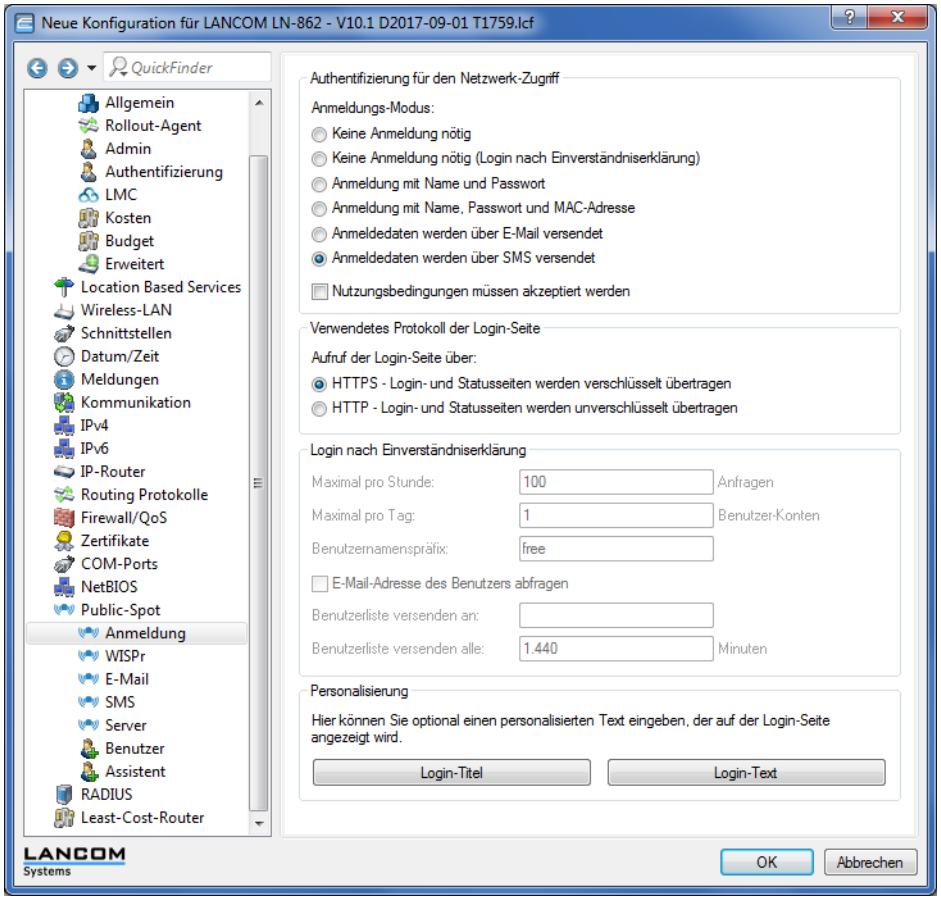


Konfiguration der Public Spot-Zugänge

Mit dem Public Spot bieten Sie einen kontrollierten Zugriffspunkt auf Ihr WLAN. Die Authentifizierung erfolgt durch Benutzerabfrage über ein Webinterface. Bei Bedarf können Sie den Zugang zeitlich begrenzen.

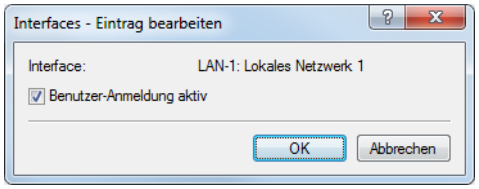
1. Aktivieren Sie die Authentifizierung für den Netzwerk-Zugriff mit Benutzername und Passwort.

> LANconfig: **Public-Spot** > **Anmeldung** > **Authentifizierung für den Netzwerk-Zugriff**



2. Aktivieren Sie die Benutzeranmeldung für das Controller-Interface, über das er mit dem Switch verbunden ist.

   > LANconfig: **Public-Spot** > **Server** > **Betriebseinstellungen** > **Interfaces**

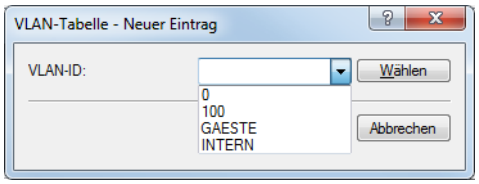


3. Regulieren Sie den Zugang zum Public Spot.

   Mit dem Eintrag der VLAN-ID "100" für das Gäste-Netzwerk in der VLAN-Tabelle beschränken Sie die Public Spot-Verwendung auf Datenpakete aus diesem virtuellen LAN. Alle Datenpakete aus anderen VLANs werden ohne Anmeldung am Public Spot weitergeleitet.

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

   > LANconfig: **Public-Spot** > **Server** > **VLAN-Tabelle**



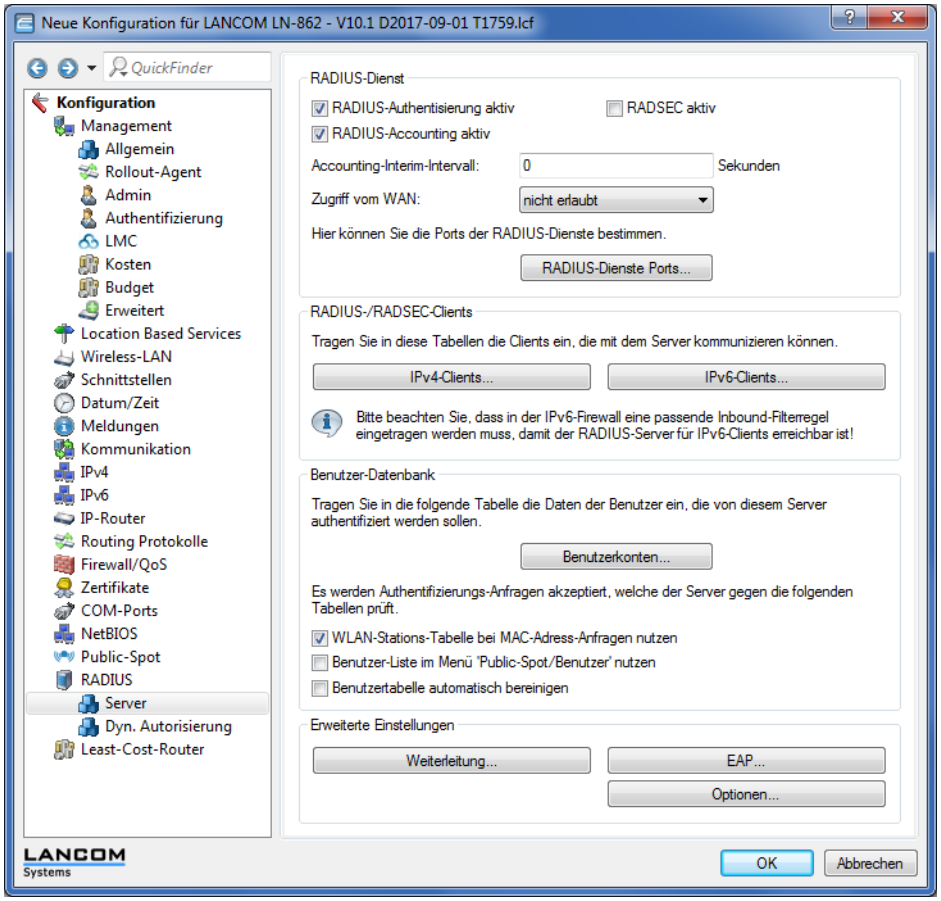
4. Aktivieren Sie die Option zum Bereinigen der Benutzertabelle, damit das Gerät nicht mehr benötigte Einträge automatisch löscht.

   › LANconfig: **RADIUS** > **Server** > **Benutzer-Datenbank** > **Benutzertabelle automatisch bereinigen**

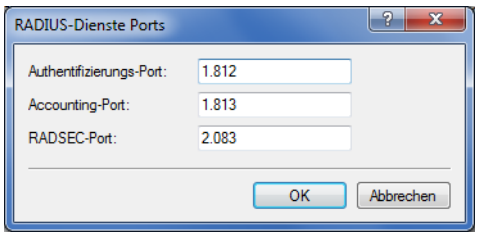
Internen RADIUS-Server für Public Spot-Nutzung konfigurieren

Der Assistent speichert die Public Spot-Zugänge in der Benutzerdatenbank des internen RADIUS-Servers. Damit Sie diese Public Spot-Zugänge nutzen können, wurde der interne RADIUS-Server standardmäßig vorkonfiguriert. Dies können Sie in **LANconfig** wie folgt einsehen:

1. Navigieren Sie zu **RADIUS** > **Server** > **RADIUS-Dienst**.
2. Stellen Sie sicher, dass die Häkchen für **RADIUS-Authentisierung aktiv** und **RADIUS-Accounting aktiv** gesetzt sind.



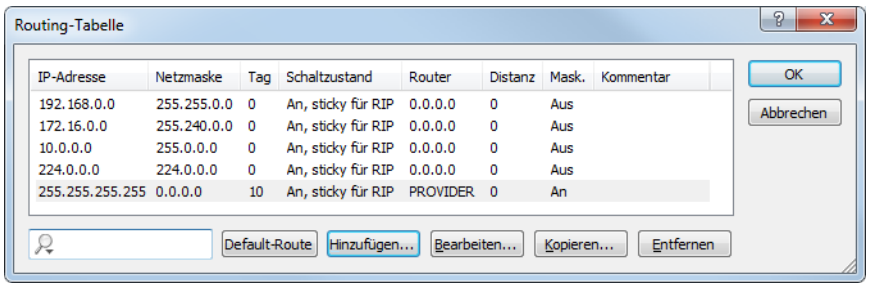
3. Klicken Sie die Schaltfläche **RADIUS-Dienste Ports**.



Hier sehen Sie die Default-Einstellungen.

Konfiguration des Internetzugangs für das Gästenetzwerk

1. Um den Benutzern des Gast-Netzes einen Internetzugang bereitzustellen, nutzen Sie z. B. den Assistenten für die Einrichtung eines Zugangs zum Providernetz.
2. Beschränken Sie den Zugang zum Providernetz.
   Damit dieser Zugang nur für die Benutzer im Gästenetzwerk zur Verfügung steht, vergeben Sie der entsprechenden Route das Routing-Tag "10". 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.
   - LANconfig: **IP-Router** > **Routing** > **Routing-Tabelle**



3. Optional: Laden Sie im LANconfig ggf. über **Gerät** > **Konfigurations-Verwaltung** > **Zertifikat oder Datei hochladen** eine HTML-Vorlage und ein Bild als Vorlage für die Ausgabe der Vouchers in das Gerät.
   Das Bild kann als GIF, JPEG oder PNG vorliegen und darf maximal 64 KB groß sein.

WLAN Layer-3 Tunneling

Einleitung

Der CAPWAP-Standard für das zentrale WLAN-Management bietet zwei verschiedene Übertragungskanäle an:

- Der obligatorische Kontrollkanal überträgt Verwaltungsdaten zwischen dem verwalteten AP und dem WLC.
- Der optionale Datenkanal überträgt die Nutzdaten aus den jeweiligen WLAN-Netzwerken (SSID) zwischen dem verwalteten AP und dem WLC.

Die optionale Nutzung des Datenkanals zwischen dem verwalteten AP und dem WLC entscheidet über den Weg der Nutzdaten:

- Wenn Sie den Datenkanal deaktivieren, leitet der AP die Nutzdaten direkt in das LAN weiter. In diesem Fall steuern Sie die Zuordnung von WLAN-Clients zu bestimmten LAN-Segmenten z. B. über die Zuweisung von VLAN-IDs. Der Vorteil dieser Anwendung liegt vor allem in der geringen Belastung des WLCs und des gesamten Netzwerks, weil der AP ausschließlich die Verwaltungsdaten über den CAPWAP-Tunnel überträgt, während er die Nutzdaten auf dem kürzesten Weg überträgt.
- Wenn Sie den Datenkanal aktivieren, leitet der AP auch die Nutzdaten an den zentralen WLC weiter. Dieser Ansatz hat folgende Vorteile:
  - Die APs können Netzwerke anbieten, die nur auf dem WLC verfügbar sind, z. B. einen zentralen Internetzugang für einen Public Spot.
  - Die von den APs angebotenen WLANs (SSIDs) sind auch ohne die Nutzung von VLAN voneinander separiert verfügbar. Der Verzicht auf VLAN reduziert den Aufwand für die Konfiguration der anderen Netzwerkkomponenten wie Switches etc.
  - Die an den APs in verschiedenen IP-Netzwerken angemeldeten WLAN-Clients können ohne Unterbrechung der IP-Verbindung zu einem anderen AP roamen, weil die Verbindung fortlaufen vom zentralen WLC verwaltet wird und nicht vom AP (Layer-3-Roaming).

Mit der Nutzung des Datenkanals entstehen auf der Basis der vorhandenen, physikalischen Netzwerkstruktur zusätzliche logische Netzwerke, die so genannten Overlay-Netzwerke.

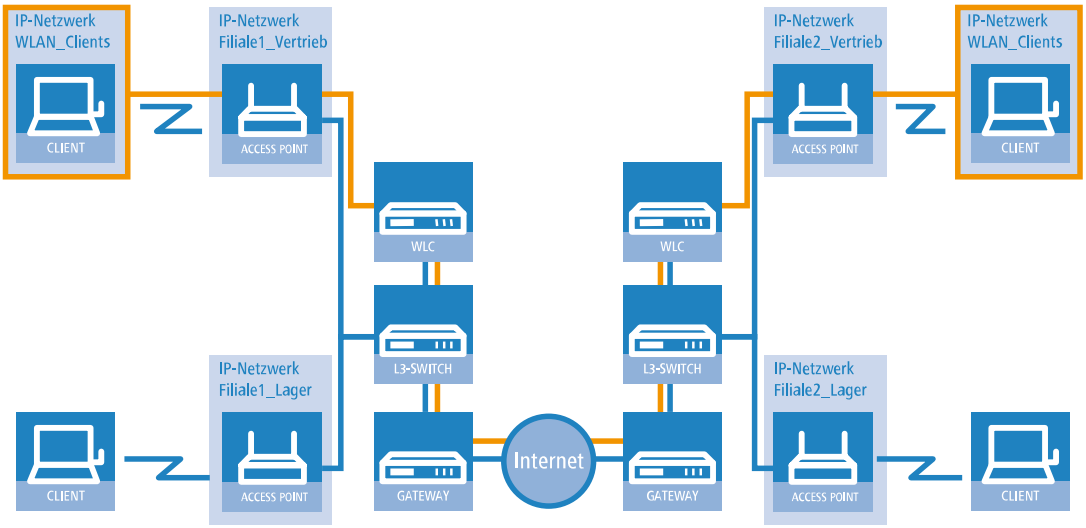


Abbildung 1: Overlay-Netzwerk über mehrere IP-Netzwerke hinweg

Über den Datenkanal können Sie so sogar über mehrere WLCs hinweg logische Overlay-Netzwerke aufspannen.

Mehrere WLCs innerhalb einer Broadcast-Domäne können das gleiche Overlay-Netzwerk unterstützen. Deaktivieren Sie den WLC-Datenkanal zwischen diesen WLCs (WEBconfig: LCOS-Menübaum > Setup > WLAN-Management > WLC-Cluster > WLC-Daten-Tunnel-aktiviert). Der mehrfache Empfang der Broadcast-Nachrichten führt ansonsten zu Schleifen. Da Router die Broadcast-Nachrichten verwerfen, haben Sie für WLC in getrennten Netzen die Möglichkeit, den CAPWAP-Datenkanal zu aktivieren.

Die APs nutzen virtuelle WLC-Schnittstellen (WLC-Tunnel), um die Datenkanäle der jeweiligen SSIDs zwischen dem AP und dem WLC zu verwalten. Jeder WLC bietet je nach Modell 16 bis 32 WLC-Tunnel an, die Sie bei der Konfiguration der logischen WLANs nutzen können.

Die Geräte bieten die virtuellen WLC-Schnittstellen in allen Dialogen zur Auswahl von logischen Schnittstellen an (LAN oder WLAN), z. B. in den Port-Tabellen der LAN- und VLAN-Einstellungen oder bei der Definition von IP-Netzwerken.

Tutorials

In den folgenden Abschnitten finden Sie konkrete Szenarien mit Schritt-für-Schritt Anleitungen für eine Reihe von Standard-Szenarien beim Einsatz von WLCs.

"Overlay Netzwerk": Netzwerke für Access Points trennen ohne VLAN

Die Trennung von Netzwerken in einer gemeinsam genutzten physikalischen Infrastruktur basiert in vielen Fällen auf dem Einsatz von VLANs. Dieses Verfahren setzt allerdings voraus, dass die eingesetzten Switches VLAN-fähig sind und dass in allen Switches die entsprechenden VLAN-Konfigurationen durchgeführt werden. Der Administrator rollt die VLAN-Konfiguration in diesem Beispiel also über das gesamte Netzwerk aus.

Mit einem WLC können Sie die Netze auch mit minimalem Einsatz von VLANs trennen. Über einen CAPWAP-Datentunnel leiten die APs die Nutzdaten der angeschlossenen WLAN-Clients direkt zum WLC, der die Daten den entsprechenden VLANs zuordnet. Die VLAN-Konfiguration beschränkt sich dabei auf den WLC und einen einzigen zentralen Switch. Alle anderen Switches arbeiten in diesem Beispiel ohne VLAN-Konfiguration.

Mit dieser Konfiguration reduzieren Sie das VLAN auf den Kern der Netzstruktur (in der Grafik blau hinterlegt dargestellt). Darüber hinaus erfordern lediglich 3 der genutzten Switch-Ports eine VLAN-Konfiguration.

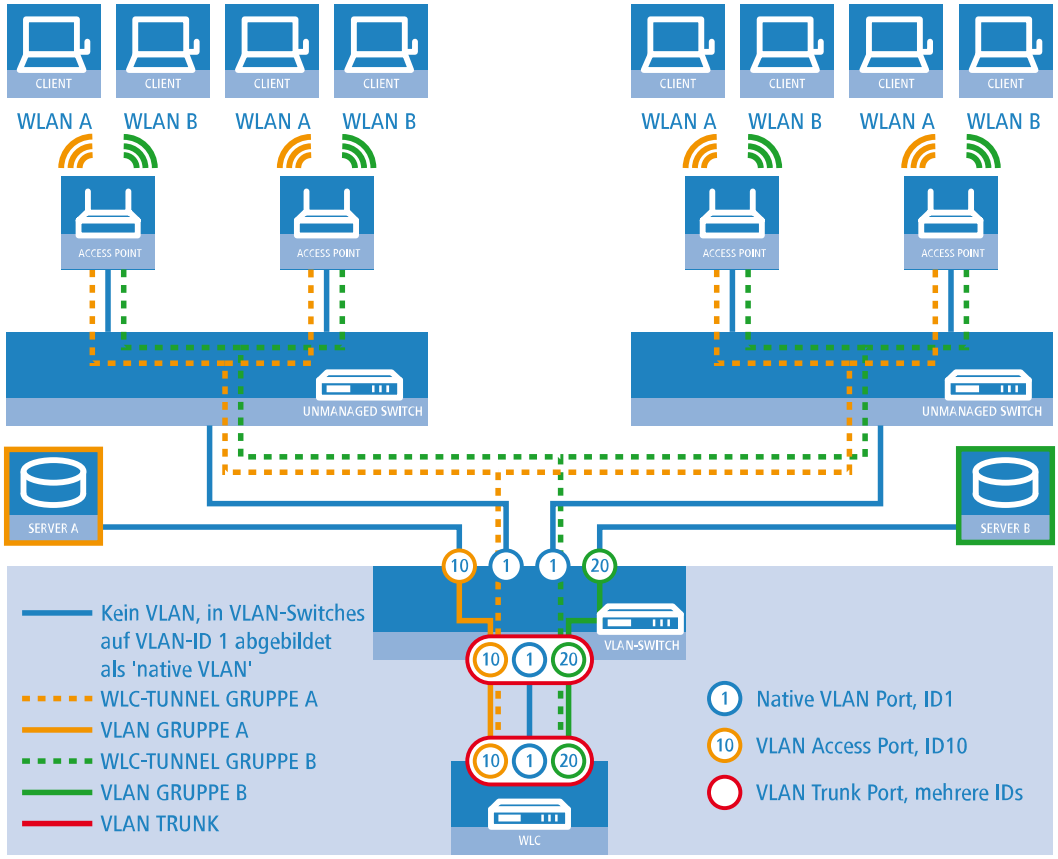


Abbildung 2: Anwendungsbeispiel Overlay-Netz

Die Grafik zeigt ein Anwendungsbeispiel mit den folgenden Komponenten:

- Das Netz besteht aus zwei Segmenten mit jeweils einem eigenen (nicht unbedingt VLAN-fähigen) Switch.
- In jedem Segment stehen mehrere APs, angeschlossen an den jeweiligen Switch.
- Jeder AP bietet zwei SSIDs für die WLAN-Clients aus verschiedenen Benutzergruppen an, in der Grafik dargestellt in Grün und Orange.
- Jede der Benutzergruppen hat Zugang zu einem eigenen Server, der vor dem Zugriff aus anderen Benutzergruppen getrennt ist. Die Server sind nur durch die auf dem Switch konfigurierten Access-Ports über die entsprechenden VLANs erreichbar.
- Ein WLC verwaltet alle APs in Netz.
- Ein zentraler, VLAN-fähiger Switch verbindet die Switches der Segmente, die gruppenbezogenen Server und den WLC.

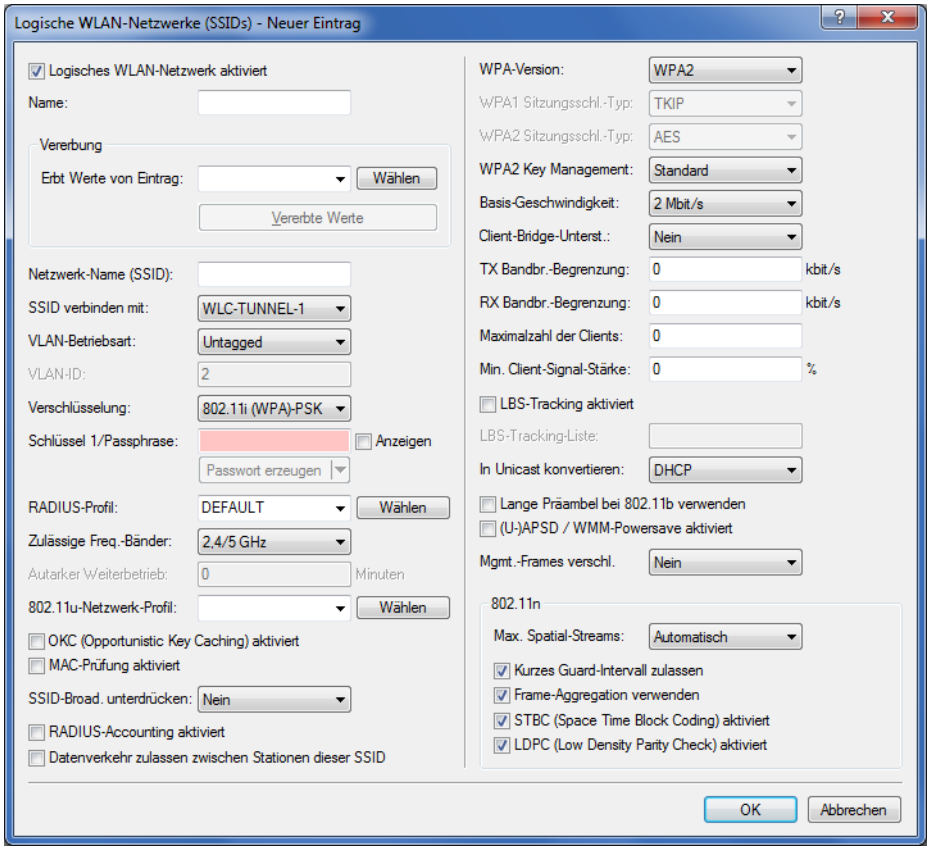
Das Ziel der Konfiguration: Ein WLAN-Client, der sich an einer bestimmten SSID anmeldet, soll Zugang zu "seinem" Server haben – unabhängig vom verwendeten AP und unabhängig vom Segment, in dem er sich gerade befindet.

Die folgende Beschreibung basiert auf einer funktionsfähigen Grundkonfiguration des WLCs. Die Konfiguration des VLAN-Switches ist nicht Bestandteil dieser Beschreibung.

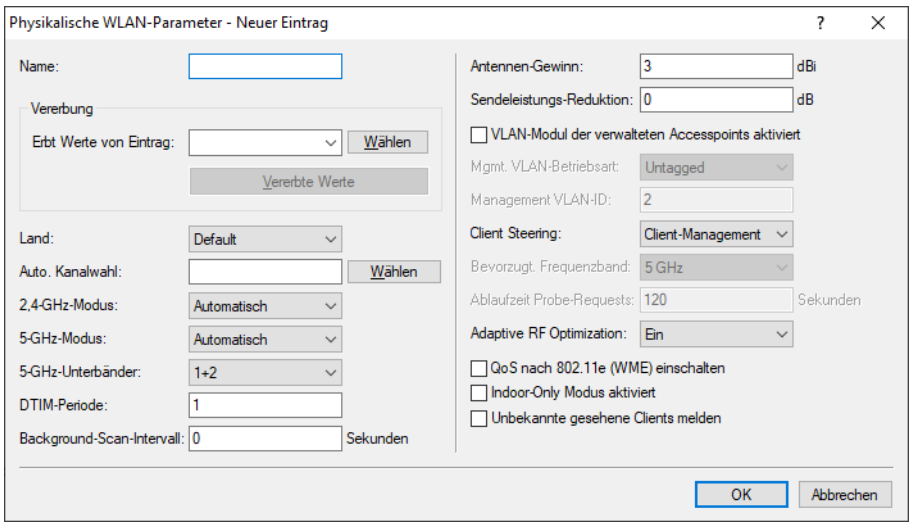
Konfiguration der WLAN-Einstellungen

1. Erstellen Sie für jede SSID einen Eintrag in der Liste der logischen Netzwerke mit einem passenden Namen und der zugehörigen SSID. Verbinden Sie diese SSID mit einem WLC-Tunnel, die erste SSID z. B. mit 'WLC-TUNNEL-1' und die zweite mit 'WLC-TUNNEL-2'. Stellen Sie die VLAN-Betriebsart jeweils auf 'Tagged' mit der VLAN-ID '10' für das

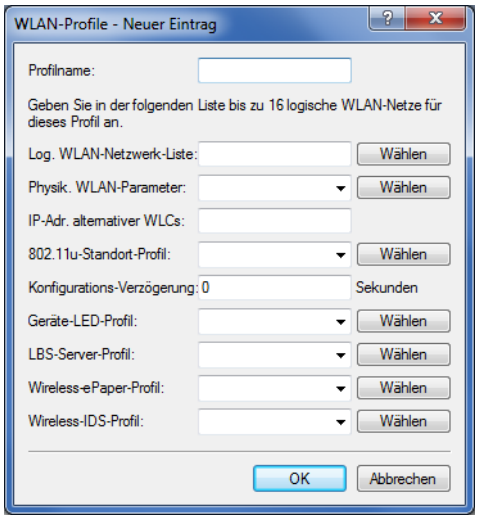
erste logischen Netz und der VLAN-ID '20' für das zweite logischen Netz. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke (SSIDs)**.



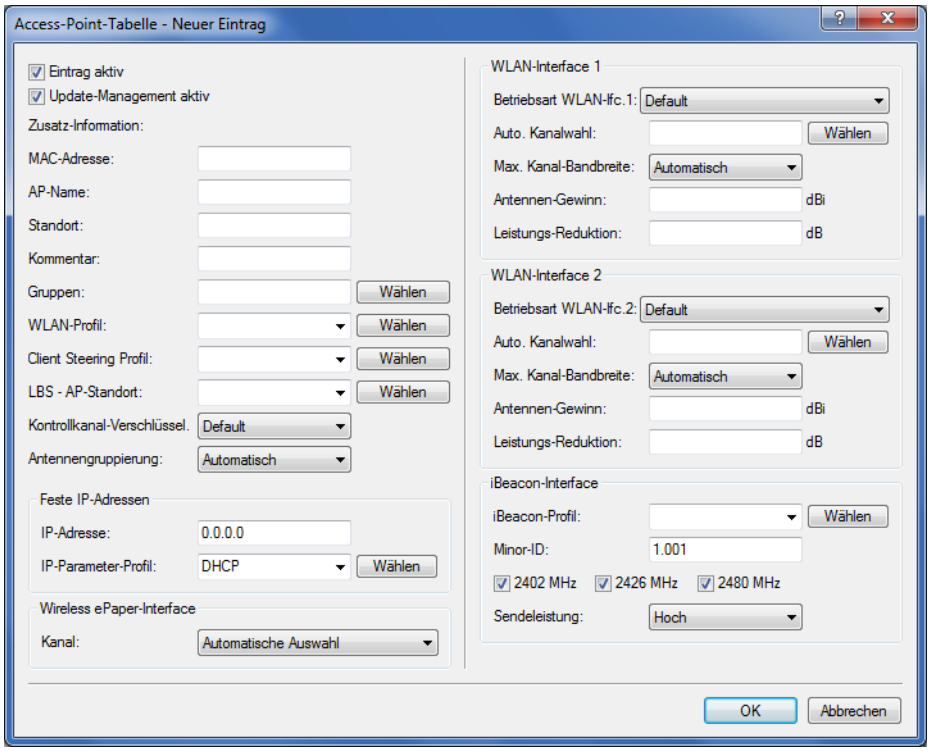
2. Erstellen Sie einen Eintrag in der Liste der physikalischen WLAN-Parameter mit den passenden Einstellungen für Ihre APs, z. B. für das Land 'Europa' mit den Kanälen 1, 6 und 11 im 802.11g/b/n und 802.11a/n gemischten Modus. Aktivieren Sie für dieses Profil der physikalischen WLAN-Parameter die Option, das VLAN-Modul auf den APs einzuschalten. Stellen Sie die Betriebsart für das Management-VLAN in den APs auf 'Ungetagged' ein. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **WLAN-Controller** > **Profile** > **Physikalische WLAN-Parameter**.



3. Erstellen Sie ein WLAN-Profil mit einem passenden Namen und ordnen Sie diesem WLAN-Profil die zuvor erstellten logischen WLAN-Netzwerke und die physikalischen WLAN-Parameter zu. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **WLAN-Controller** > **Profile** > **WLAN-Profile**.

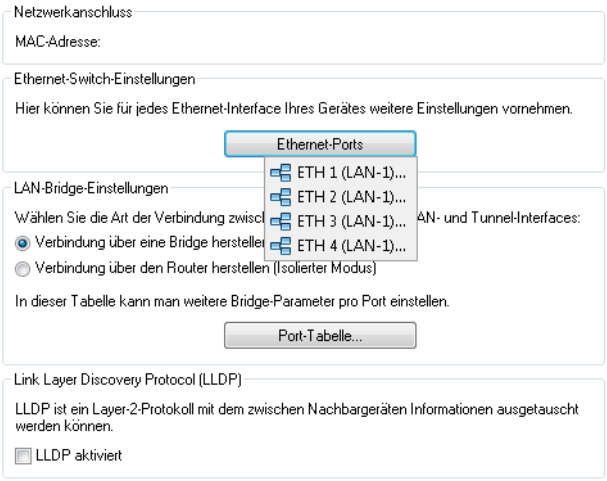


4. Erstellen Sie für jeden verwalteten AP einen Eintrag in der AP-Tabelle mit einem passenden Namen und der zugehörigen MAC-Adresse. Ordnen Sie diesem AP das zuvor erstellte WLAN-Profil zu. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **WLAN-Controller** > **AP-Konfig.** > **Access-Point-Tabelle**.

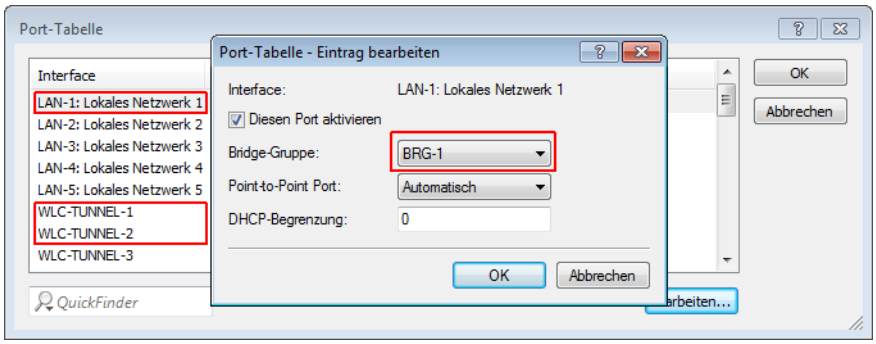


Konfiguration der Schnittstellen am WLC

5. Ordnen Sie jedem physikalischen Ethernet-Port eine separate logische LAN-Schnittstelle zu, z. B. 'LAN-1'. Stellen Sie sicher, dass die anderen Ethernet-Ports nicht der gleichen LAN-Schnittstelle zugeordnet sind. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **Schnittstellen** > **LAN** > **Ethernet-Ports**.

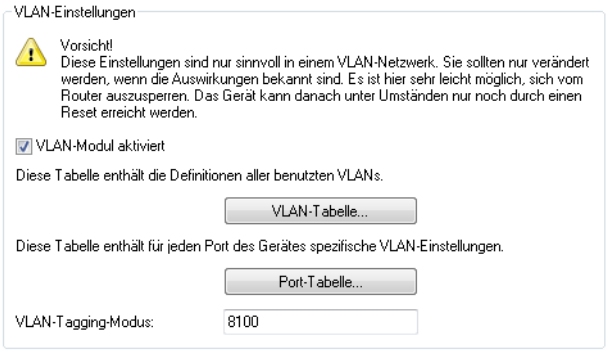


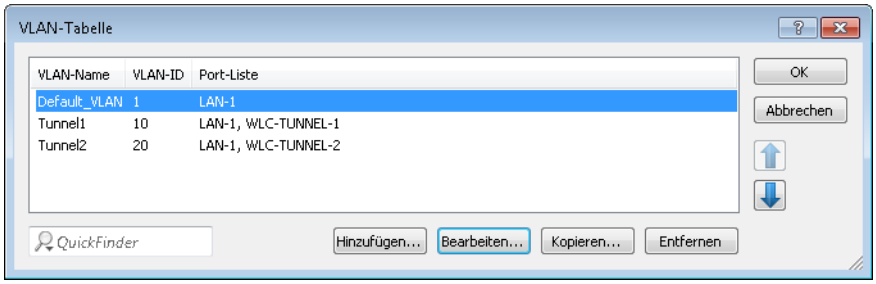
6. Ordnen Sie die logische LAN-Schnittstelle 'LAN-1' und die WLC-Tunnel 'WLC-Tunnel-1' und 'WLC-Tunnel-2' der Bridge-Gruppe 'BRG-1' zu. Stellen Sie sicher, dass die anderen LAN-Schnittstellen nicht der gleichen Bridge-Gruppe zugeordnet sind. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **Schnittstellen** > **LAN** > **Port-Tabelle**.



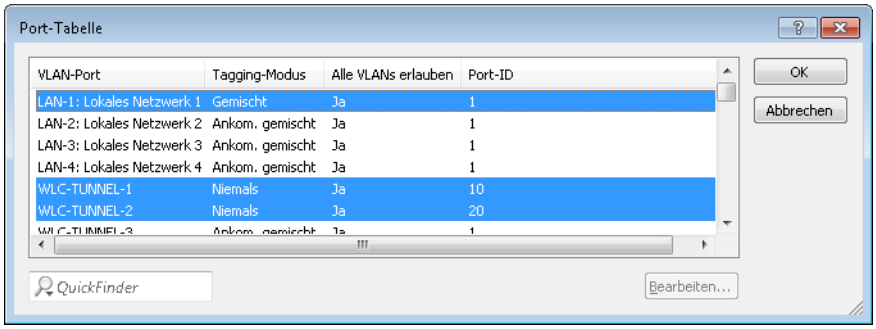
Die LAN-Schnittstellen und WLC-Tunnel gehören standardmäßig keiner Bridge-Gruppe an. Indem Sie die LAN-Schnittstelle 'LAN-1' sowie die beiden WLC-Tunnel 'WLC-Tunnel-1' und 'WLC-Tunnel-2' der Bridge-Gruppe 'BRG-1' zuordnen, leitet das Gerät alle Datenpakete zwischen LAN-1 und den WLC-Tunneln über die Bridge weiter.

7. Aktivieren Sie unter **Schnittstellen** > **VLAN** das VLAN-Modul des WLC und ordnen Sie unter **VLAN-Tabelle** dem gewünschten VLAN den oben gewählten LAN-Port (LAN-1) sowie den passenden WLC-Tunnel zu.





8. Stellen Sie unter **Schnittstellen** > **VLAN** > **Port-Tabelle** den Tagging-Modus der Tunnel-Interfaces sowie des LAN-Interfaces korrekt ein und setzen Sie die passende Port-VLAN-ID.



Je nach Schaltung des Switches konfigurieren Sie den Tagging-Modus des LAN-Interfaces auf 'Gemischt' oder 'Immer'.

Im Normalfall betreibt man die Tunnel-Interfaces im Modus 'Niemals', da Pakete hier (aus dem WLAN) immer ungetaggt ankommen und der WLC sie mit der Port-VLAN-ID versieht.

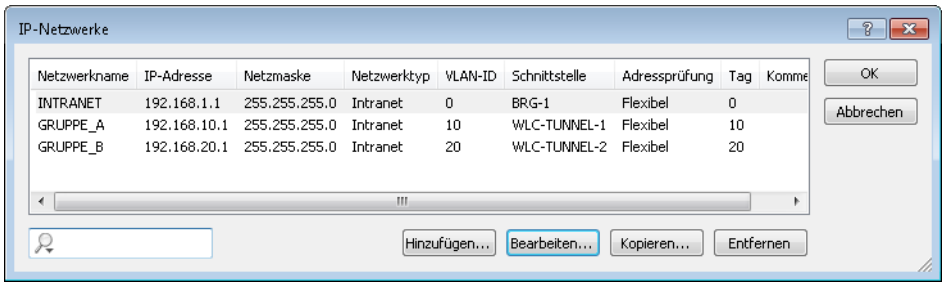
Bitte beachten Sie, dass bei Aktivierung des VLAN-Moduls die auf dem WLC angelegten ARF-Netze eine VLAN-ID erhalten müssen. Soll der WLC das Netz ohne VLAN-Tag erreichen, setzen Sie bei oben stehender VLAN-Konfiguration die '1' als VLAN-ID für das IP-Netz.

Eine ähnliche Konfiguration ist möglich, indem Sie schon am Access Point ein VLAN-Tag für die durch den Tunnel zu leitenden Pakete setzen und das VLAN-Modul des WLC nicht nutzen.

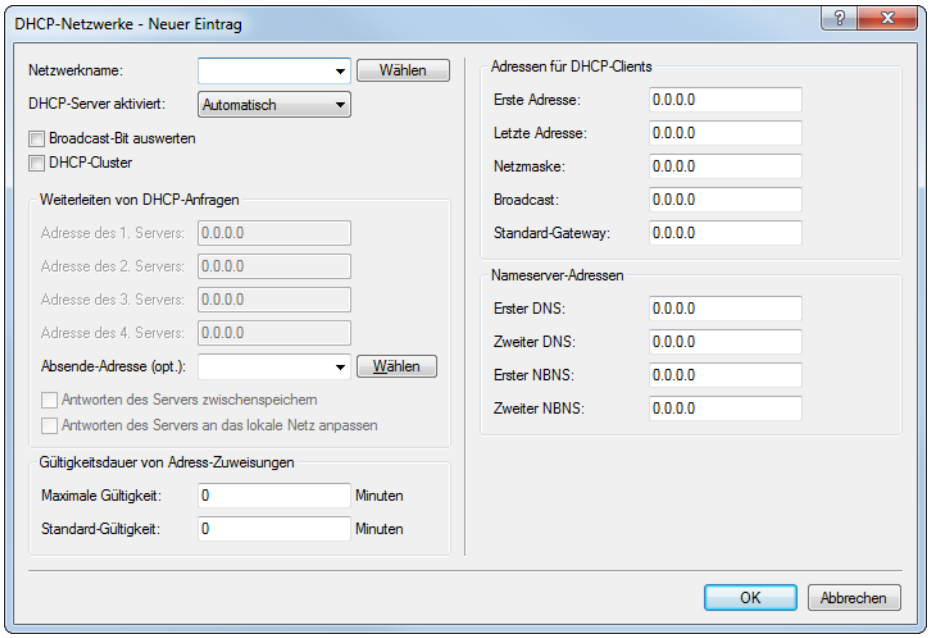
Dabei würde der WLC allerdings durch das Bridgen der verschiedenen WLC-Tunnel untereinander auch Broadcasts in alle Tunnel weiterleiten, was ab einer bestimmten Menge von Tunneln/SSIDs und APs zu Lastproblemen im Netz und auf dem WLC führen kann. Die vorliegende Konfiguration des VLAN-Moduls verhindert das.

9. Ergänzend konfigurieren Sie unter **IPv4** > **Allgemein** > **IP-Netzwerke** für die auf Layer 2 getrennten Netzwerke die IP-Einstellungen.

Damit das Gerät die Netzwerke nicht wieder auf Layer 3 verbindet, ist auch eine Trennung auf Layer 3 erforderlich, z. B. durch ein Schnittstellen-Tag oder durch die Firewall.



10. Der WLC kann optional als DHCP-Server für die APs fungieren. Aktivieren Sie dazu den DHCP-Server für das 'INTRANET'. In LANconfig finden Sie diese Einstellungen unter **IPv4** > **DHCPv4** > **DHCP-Netzwerke**.



"Layer-3-Roaming"

Die Durchleitung der Nutzdaten aus den WLANs über WLC-Tunnel bis zum WLC ermöglicht das Roaming auch über die Grenzen von Broadcast-Domänen hinweg. In diesem Anwendungsbeispiel verhindert ein Layer-3-Switch zwischen den Etagen die Weiterleitung der Broadcasts und trennt so die Broadcast-Domänen.

In diesem Beispiel haben zwei Benutzergruppen A und B jeweils Zugang zu einem eigenen WLAN (SSID). Die APs in mehreren Etagen des Gebäudes bieten die beiden SSIDs 'GRUPPE_A' und 'GRUPPE_B' an.

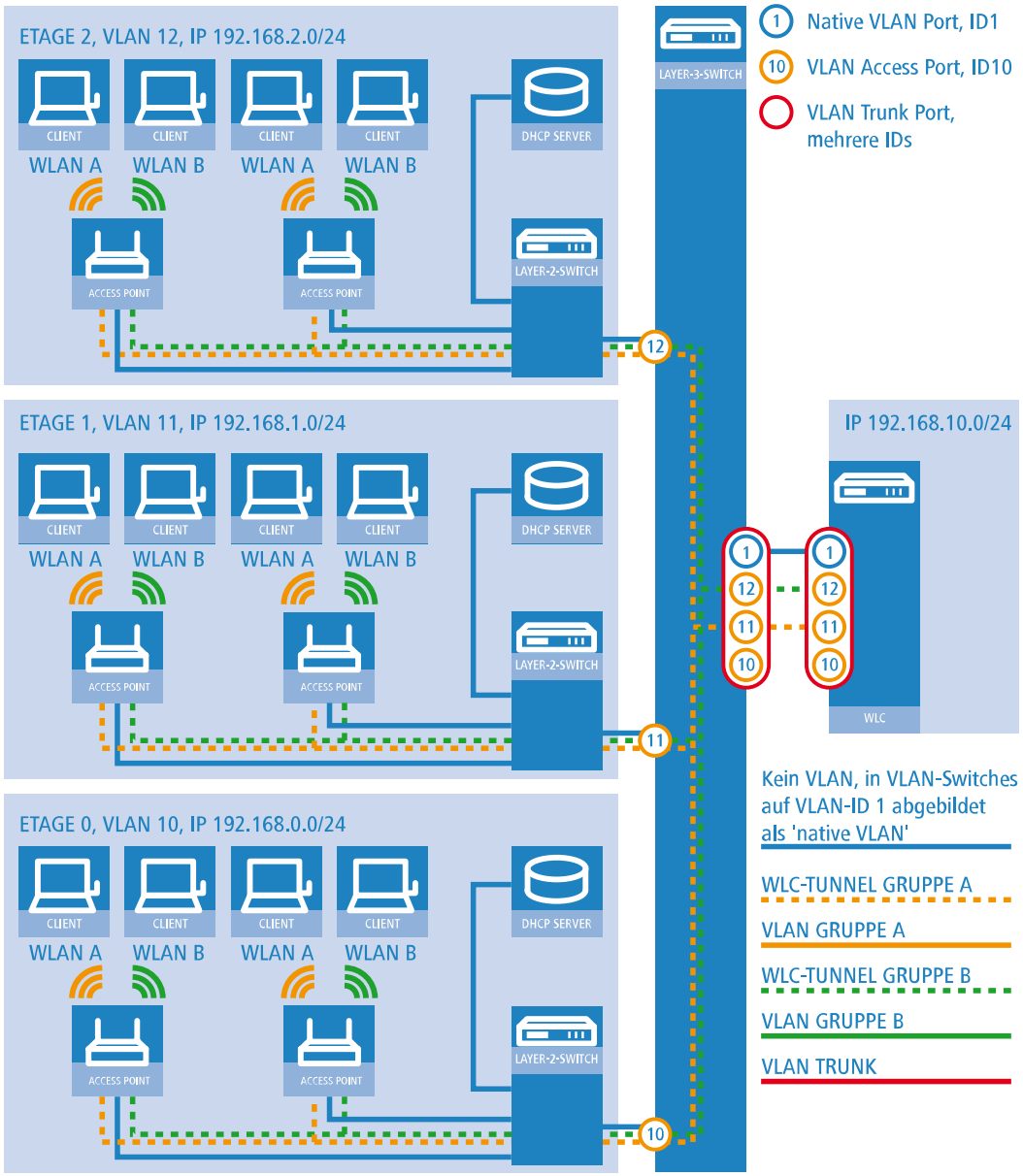


Abbildung 3: Anwendungsbeispiel Layer-3-Roaming

Die Grafik zeigt ein Anwendungsbeispiel mit den folgenden Komponenten:

- Das Netz besteht aus 3 Segmenten in separaten Etagen eines Gebäudes.
- Ein zentraler Layer-3-Switch verbindet die Segmente und teilt das Netzwerk in 3 Broadcast-Domänen auf.
- Jedes Segment nutzt einen eigenen IP-Adressbereich und ein eigenes VLAN.
- In jedem Segment arbeitet ein lokaler DHCP-Server, der den APs die folgenden Informationen übermittelt:
  - IP-Adresse des Gateways
  - IP-Adresse des DNS-Servers
  - Domänen-Suffix

Die Bereitstellung dieser Informationen ermöglicht es den APs, Kontakt mit dem WLC in einer anderen Broadcast-Domäne aufzunehmen.

Das Ziel der Konfiguration: Ein WLAN-Client, der sich an einer bestimmten SSID anmeldet, soll beim Wechsel der Etage nahtlos Zugang zu "seinem" WLAN behalten – unabhängig vom verwendeten AP und unabhängig vom Segment, in dem er sich gerade befindet. Da die Segmente in diesem Beispiel unterschiedliche IP-Adresskreise nutzen, gelingt das nur durch die Verwaltung der APs auf Layer 3 direkt über den zentralen WLC über die Grenzen der VLANs hinweg.

Die Konfiguration entspricht dem Beispiel *"Overlay Netzwerk": Netzwerke für Access Points trennen ohne VLAN* auf Seite 54.

WLAN-Controller mit Public Spot

Dieses Szenario basiert auf dem ersten Szenario (Overlay-Netzwerk) und erweitert es um spezifische Einstellungen für eine Benutzer-Authentifizierung.

Die Durchleitung der Nutzdaten aus den WLANs über WLC-Tunnel bis zum WLC ermöglicht eine besonders einfache Konfiguration von Public Spots z. B. für Gäste parallel zu einem intern genutzten WLAN.

In diesem Beispiel haben die Mitarbeiter einer Firma Zugang zu einem eigenen WLAN (SSID), die Gäste erhalten über einen Public Spot ebenfalls Zugang zum Internet. Die APs in allen Bereichen des Gebäudes bieten die beiden SSIDs 'FIRMA' und 'GAESTE' an.

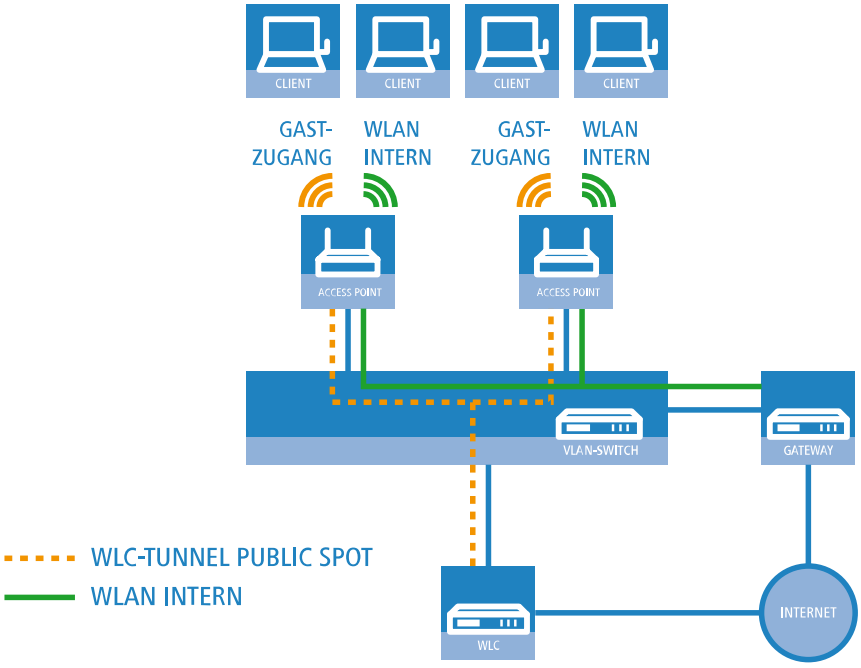
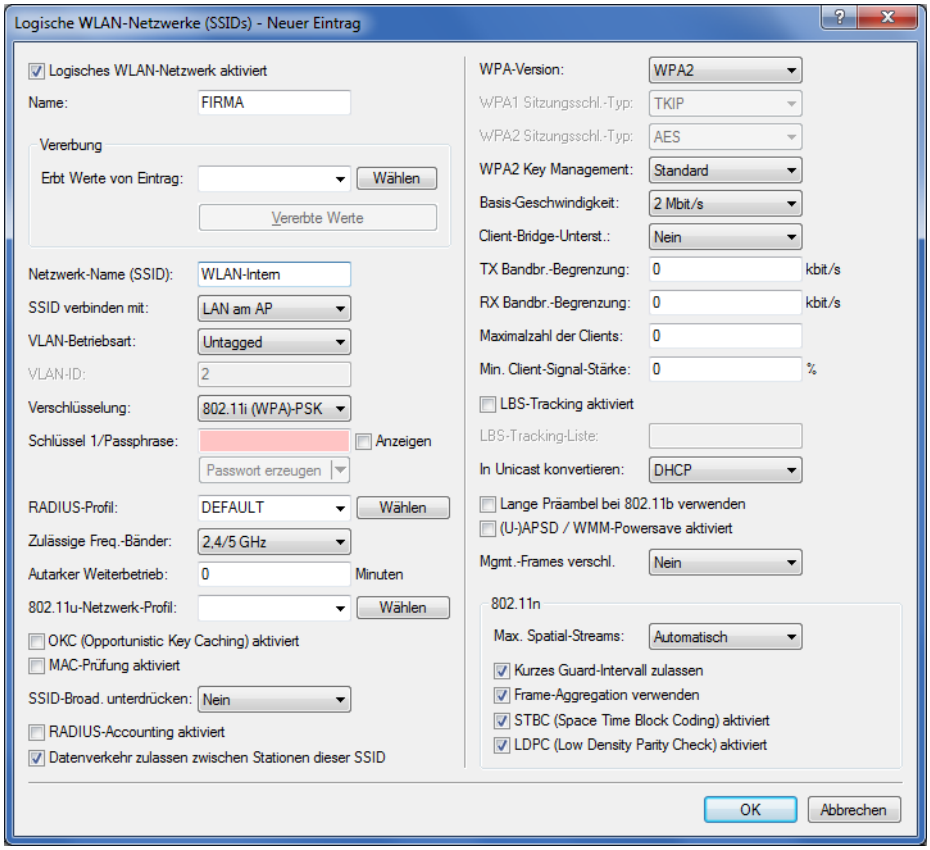


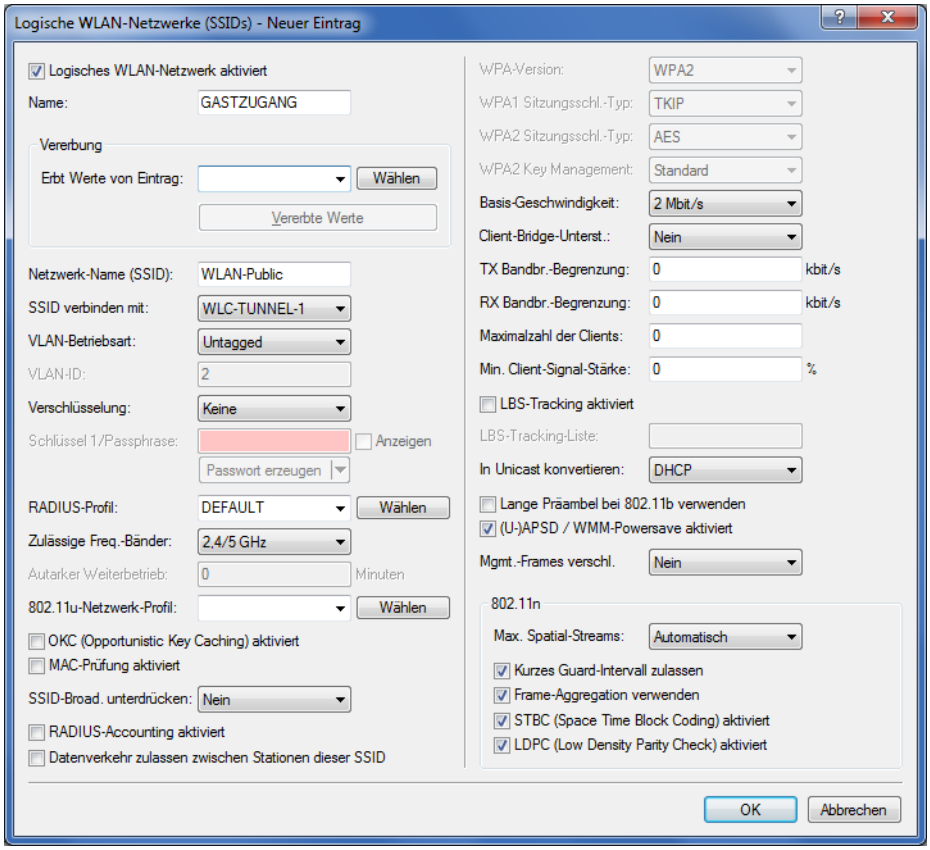
Abbildung 4: Anwendungsbeispiel WLAN-Controller mit Public Spot

Das Ziel der Konfiguration: Ein WLAN-Client, der sich an der internen SSID anmeldet, soll Zugang zu allen internen Ressourcen und zum Internet über das zentrale Gateway erhalten. Die APs koppeln die Nutzdaten der internen Clients lokal aus und leiten sie direkt in das LAN weiter. Die WLAN-Clients der Gäste melden sich am Public Spot an. Die APs leiten die Nutzdaten der Gäste-Clients über einen WLC-Tunnel direkt zum WLC, der über eine separate WAN-Schnittstelle Zugang zum Internet ermöglicht.

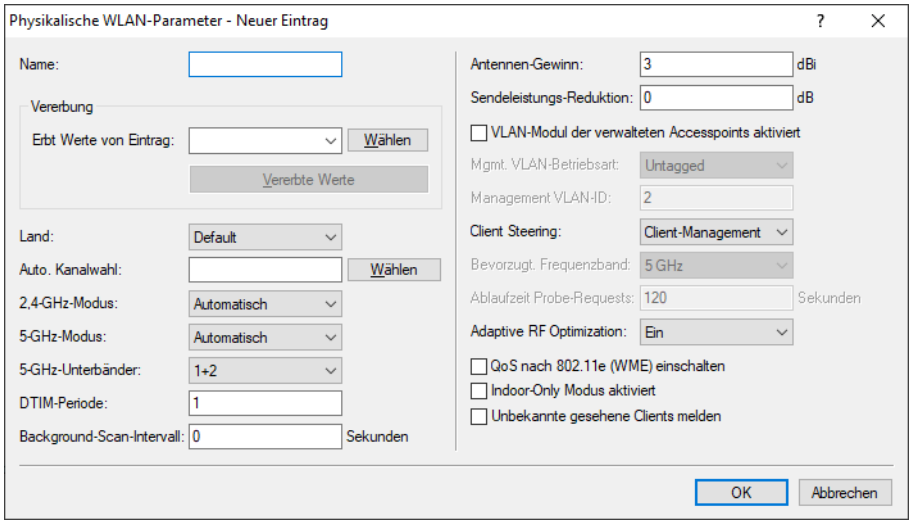
1. Erstellen Sie für das interne WLAN und das Gäste-WLAN jeweils einen Eintrag in der Liste der logischen Netzwerke mit einem passenden Namen und der zugehörigen SSID. Verbinden Sie die SSID für die interne Nutzung mit dem 'LAN am AP', die SSID für die Gäste z. B. mit 'WLC-TUNNEL-1'. Deaktivieren Sie bei der SSID für das Gästenetzwerk die Verschlüsselung, damit sich die WLAN-Clients der Gäste beim Public Spot anmelden können. Unterbinden Sie

für diese SSID außerdem den Datenverkehr der Stationen untereinander (Interstation-Traffic). In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke (SSIDs)**.

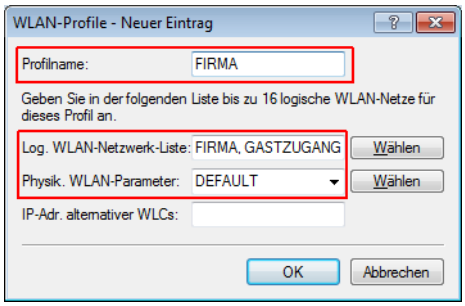




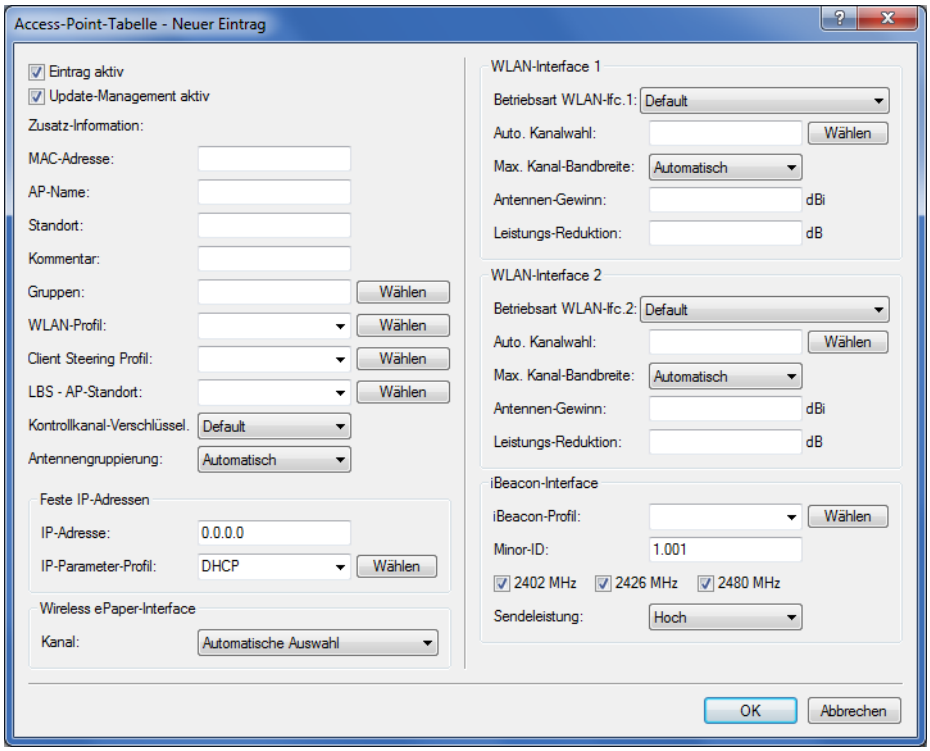
2. Erstellen Sie einen Eintrag in der Liste der physikalischen WLAN-Parameter mit den passenden Einstellungen für Ihre APs, z. B. für das Land 'Europa' mit den Kanälen 1, 6 und 11 im 802.11g/b/n und 802.11a/n gemischten Modus. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **WLAN-Controller** > **Profile** > **Physikalische WLAN-Parameter**.



3. Erstellen Sie ein WLAN-Profil mit einem passenden Namen und ordnen Sie diesem WLAN-Profil die zuvor erstellten logischen WLAN-Netzwerke und die physikalischen WLAN-Parameter zu. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **WLAN-Controller** > **Profile** > **WLAN-Profile**.

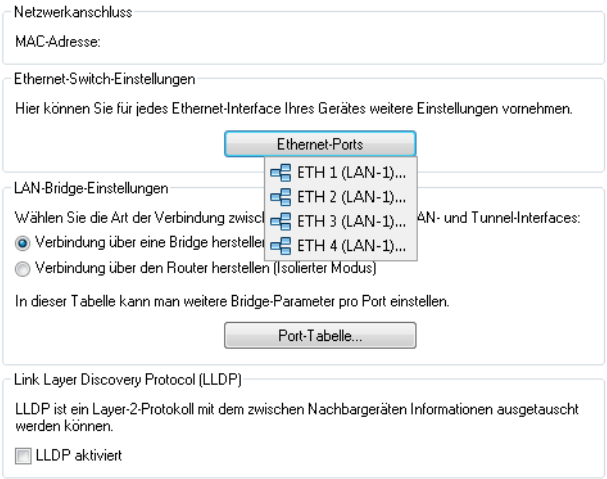


4. Erstellen Sie für jeden verwalteten AP einen Eintrag in der AP-Tabelle mit einem passenden Namen und der zugehörigen MAC-Adresse. Ordnen Sie diesem AP das zuvor erstellte WLAN-Profil zu. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **WLAN-Controller** > **AP-Konfig** > **Access-Point-Tabelle**.

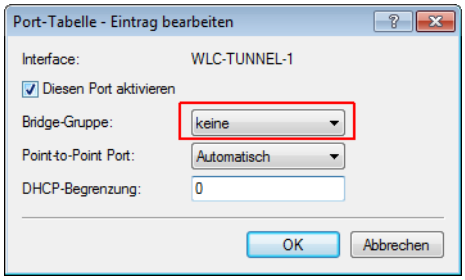


5. Ordnen Sie jedem physikalischen Ethernet-Port eine separate logische LAN-Schnittstelle zu, z. B. 'LAN-1'. Stellen Sie den 4. Ethernet-Port auf die logische LAN-Schnittstelle 'DSL-1' ein. Der WLC verwendet diese LAN-Schnittstelle später

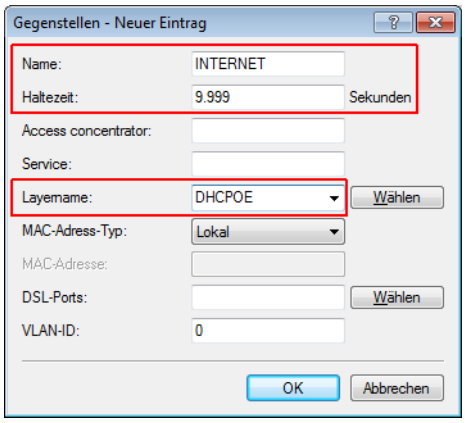
für den Internetzugang des Gästenetzes. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **Schnittstellen** > **LAN** > **Ethernet-Ports**.



6. Überprüfen Sie, dass die logische LAN-Schnittstelle 'WLC-Tunnel 1' keiner Bridge-Gruppe zugeordnet ist. So stellen Sie sicher, dass die anderen LAN-Schnittstellen keine Daten zum Public Spot-Netzwerk übertragen. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **Schnittstellen** > **LAN** > **Port-Tabelle**.

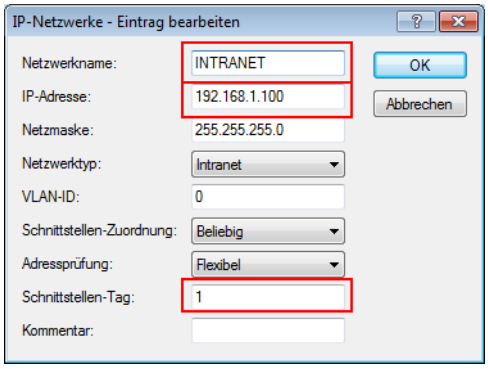


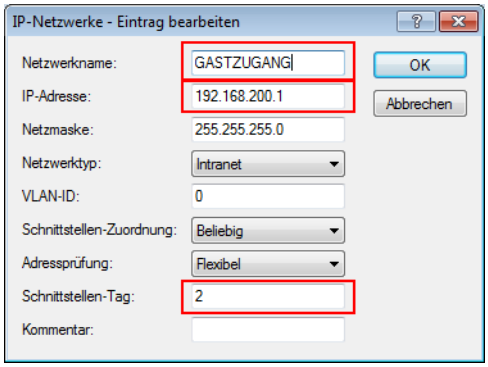
7. Erstellen Sie für den Internetzugang der Gäste einen Eintrag in der Liste der DSL-Gegenstellen mit der Haltezeit '9999' und dem vordefinierten Layer 'DHCPOE'. Dieses Beispiel setzt voraus, dass ein Router mit aktiviertem DHCP-Server den Internetzugang bereitstellt. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **Kommunikation** > **Gegenstellen** > **Gegenstellen**.



8. Erstellen Sie für die interne Nutzung das IP-Netzwerk 'INTRANET' z. B. mit der IP-Adresse '192.168.1.100' und mit dem Schnittstellen-Tag '1', für die Gäste das IP-Netzwerk 'GASTZUGANG' z. B. mit der IP-Adresse '192.168.200.1' und mit dem Schnittstellen-Tag '2'. Der virtuelle Router im WLC nutzt die Schnittstellen-Tags, um die Routen für die

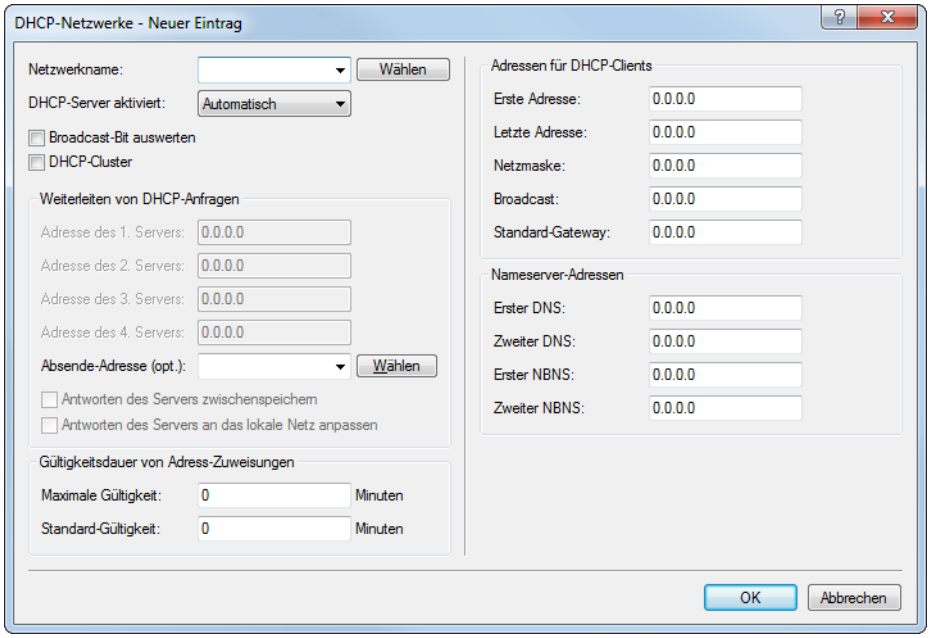
beiden Netzwerke zu trennen. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **TCP/IP** > **Allgemein** > **IP-Netzwerke**.



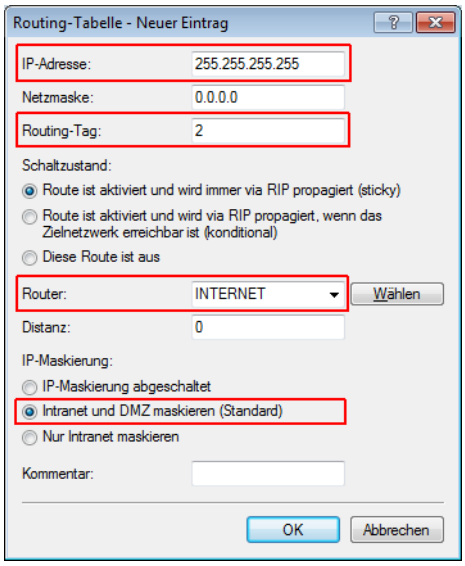


9. Der WLC kann als DHCP-Server für die APs und die angemeldeten WLAN-Clients fungieren. Aktivieren Sie dazu den DHCP-Server für das 'INTRANET' und den 'GASTZUGANG. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **TCP/IP** > **DHCP** > **DHCP-Netzwerke**.

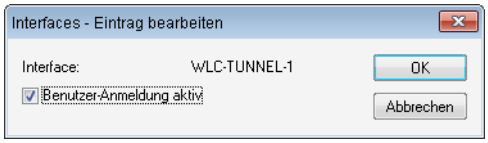
Die Aktivierung des DHCP-Servers ist für das Gästenetz zwingend, für das interne Netz optional. Für das interne Netz können Sie den DHCP Server auch anders realisieren.



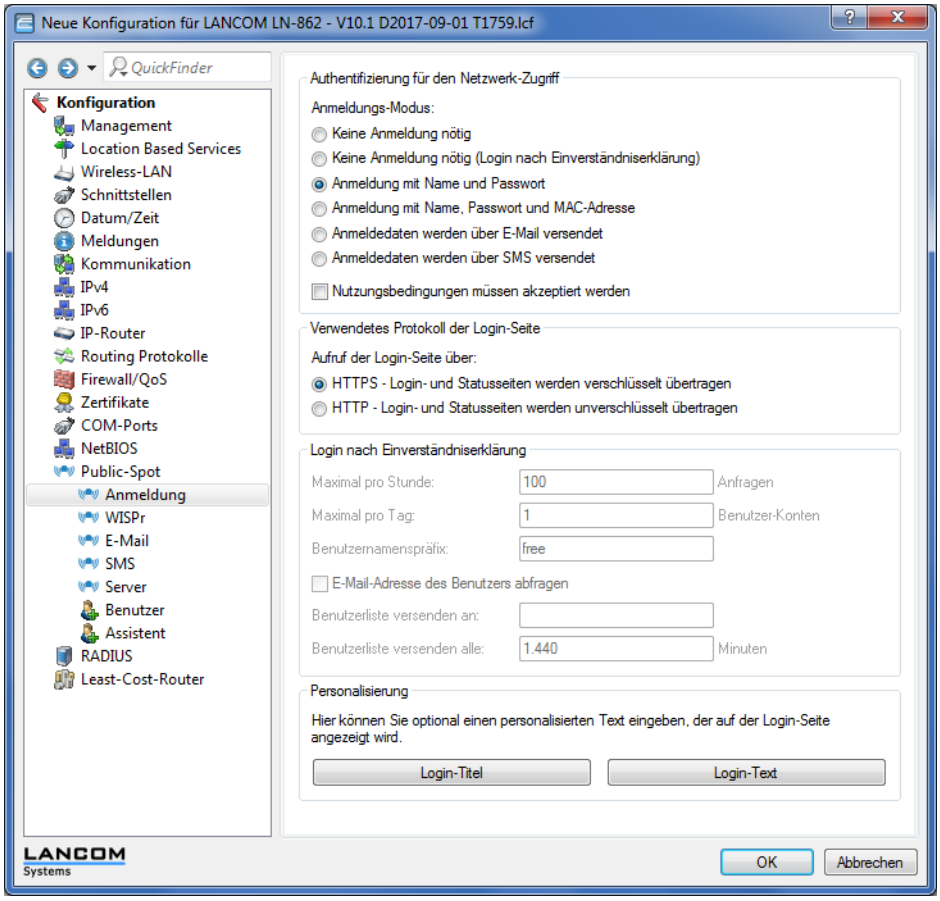
10. Erstellen Sie eine neue Standard-Route in der Routing-Tabelle, welche die Daten aus dem Gästenetzwerk auf den Internet-Zugang des WLCs leitet. Wählen Sie dazu das Routing-Tag '2' und den Router 'Internet'. Aktivieren Sie außerdem die Option 'Intranet und DMZ maskieren (Standard)'. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **IP-Router** > **Routing** > **Routing-Tabelle**.



11. Aktivieren Sie die Public Spot-Anmeldung für die logische LAN-Schnittstelle 'WLC-Tunnel 1'. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **Public-Spot** > **Server** > **Betriebseinstellungen** > **Interfaces**.



12. Aktivieren Sie im letzten Schritt die Anmeldung über den Public-Spot für den WLC. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **Public-Spot** > **Anmeldung**.



Neben der Konfiguration des WLCs konfigurieren Sie den Public Spot nach Ihren Wünschen entweder für die interne Benutzerliste oder für die Verwendung eines RADIUS-Servers.

1.4.4 IP-abhängige Autokonfiguration und Tagging von APs

Sämtliche APs, die Sie einem gemanagten Netz hinzufügen, verwalten Sie im einfachsten Falle in einer flachen Hierarchie. In größeren Installationen mit Hunderten von APs über mehrere Standorte hinweg wird diese Form der Organisation jedoch schnell unübersichtlich und erzeugt einen hohen Administrationsaufwand. Über die Einrichtung von **Zuweisungs-Gruppen** haben Sie daher die Möglichkeit, das Management verteilter APs zu vereinfachen. Hierbei lassen Sie neue APs in Abhängigkeit von der erhaltenen IP-Adresse automatisch vom WLC konfigurieren. Dadurch entfällt die manuelle Zuweisung eines IP-Parameter-Profils, eines WLAN-Profils und eines Client Steering-Profils durch einen Administrator.

Die Anwendung einer Zuweisungs-Gruppe bei Anmeldung eines neuen APs an einem zentralen WLC läuft nach folgendem Schema ab: Nachdem die neuen APs am gewünschten Einsatzort (z. B. einem Firmen- bzw. Filialnetz) installiert sind, versuchen diese, eine Verbindung zum eingetragenen WLC aufzubauen und via CAPWAP eine Konfiguration zu beziehen. Der WLC erkennt die Verbindungsanfragen und prüft für jeden neuen AP, ob in der AP-Tabelle ein geeignetes AP-Profil (z. B. das Default-Profil) vorliegt oder/und eine geeignete Zuweisungs-Gruppe definiert ist. Liegen eine oder mehrere Konfigurationsmöglichkeiten vor, prüft der WLC diese auf folgende Zustände:

1. Für einen neuen AP existiert eine Zuweisungs-Gruppe, jedoch kein AP-Profil. In diesem Fall weist der WLC dem neuen AP die innerhalb der Zuweisungs-Gruppe definierten Profile zu.
2. Für einen neuen AP existiert sowohl eine Zuweisungs-Gruppe als auch ein AP-Profil. In diesem Fall ignoriert der WLC die Zuweisungs-Gruppe und weist dem neuen AP die innerhalb des AP-Profils definierten Profile zu.

3. Für einen neuen AP existiert ein AP-Profil, aber keine Zuweisungs-Gruppe. Das Verhalten entspricht dem von Punkt (2).

Existieren für einen neuen AP weder ein AP-Profil, noch eine Zuweisungs-Gruppe, gibt der WLC eine Warnung aus, welche den Administrator auf die Fehlkonfiguration hinweist.

Nach der erfolgreichen Gruppenzuweisung legt der WLC in der Access-Point-Tabelle automatisch ein AP-Profil für jeden neuen AP an. Im Feld **Gruppen** referenziert der WLC die Zuweisungs-Gruppen, die er beim Hinzufügen des neuen AP angewandt hat.

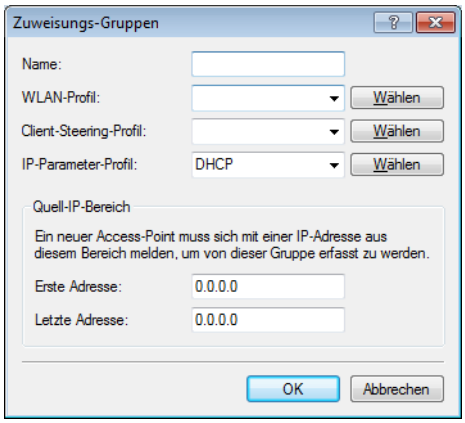
Ein AP darf immer nur eine Zuweisungsgruppe erhalten. Sobald sich Anwendungsbereiche von Zuweisungsgruppen überschneiden, erkennt LCOS derartige Konfigurationsfehler und schreibt die Meldungen in die entsprechende Status-Tabelle unter **Status** > **WLAN-Management** > **AP-Konfiguration**.

Über das Gruppen-Feld haben Sie ebenfalls die Möglichkeit, einen AP mit individuell definierbaren Tags zu versehen. Diese **Tag-Gruppen** lassen sich z. B. beim Ausführen von Aktionen auf dem WLC als Filterkriterien einsetzen, um eine Aktion auf eine Auswahl von APs zu beschränken.

Einrichten von Zuweisungs-Gruppen für die IP-abhängige Autokonfiguration

Das nachfolgende Tutorial zeigt Ihnen, wie Sie auf einem WLC Zuweisungs-Gruppen für die IP-abhängige Autokonfiguration neuer APs einrichten.

1. Öffnen Sie den Konfigurationsdialog für Ihr Gerät und wählen Sie **WLAN-Controller** > **AP-Konfiguration** > **Zuweisungs-Gruppen**.
2. Klicken Sie **Hinzufügen**, um eine neue Gruppe anzulegen.



3. Geben Sie als **Name** eine eindeutige Bezeichnung für die Zuweisungs-Gruppe an, z. B. `Filiale_Berlin`.
4. Wählen Sie das **WLAN-Profil** aus, welches der WLC einem neuen AP automatisch zuweist, wenn die IP-Adresse des neuen APs innerhalb des Quell-IP-Bereichs liegt.
5. Geben Sie ein **IP-Parameter-Profil** an, sofern der neue AP eine manuelle Netzkonfiguration erhalten soll. Andernfalls belassen Sie den Einzelwert **DHCP**; hierbei erhält der AP eine automatische Netzkonfiguration vom DHCP-Server. Der DHCP-Server muss dazu entsprechend konfiguriert sein.

   Sofern Sie eine manuelle Netzkonfiguration zuweisen wollen, bei der ein neuer AP eine abweichende IP-Adresse erhält, so geben Sie den entsprechenden Adressbereich im **IP-Parameter-Profil** unter **Address-Zuweisungs-Pool** an.
6. **Optional**: Geben Sie ein **Client Steering-Profil** an, um bei mehreren neuen APs die sich im Sendebereich befindlichen, künftigen WLAN-Clients auf den für sie idealen AP umzuleiten.

   Sofern Sie Client Steering aktivieren, muss dieses innerhalb der zu managenden Infrastruktur für jeden AP aktiviert sein. Weitere Informationen dazu finden Sie im Abschnitt *Client Steering über den WLC* auf Seite 109.

7. Geben Sie den Anfang und das Ende des **Quell-IP-Bereich**s an, für den die Zuweisungs-Gruppe gilt.
   Ein neuer AP muss sich mit einer IP-Adresse aus diesem Bereich beim WLC anmelden, um die für die Gruppe hinterlegte Konfiguration zu erhalten.
8. Schließen Sie alle Dialogfenster mit **OK** und schreiben Sie die Konfiguration zurück auf Ihr Gerät.

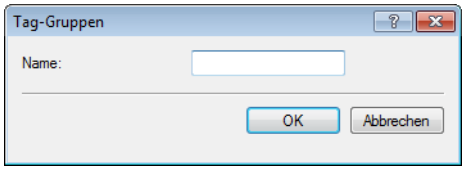
Der WLC weist fortan allen neuen APs die in den Zuweisungs-Gruppen referenzierten Profile zu. Über die LCOS-Konsole haben Sie dann die Möglichkeit, Informationen zur Kategorisierung abzurufen, siehe *Übersicht der capwap-Parameter im show-Befehl* auf Seite 130.

Achten Sie darauf, dass in der Access-Point-Tabelle kein AP-Profil (z. B. das Default-Profil) vorliegt, welches der WLC den neuen APs zuweisen könnte. Sofern ein geeignetes AP-Profil vorliegt, erhält dies gegenüber Zuweisungs-Gruppen stets die höhere Priorität.

Einrichten von Tag-Gruppen für die selektive Auswahl von APs

Das nachfolgende Tutorial zeigt Ihnen, wie Sie eine AP-Konfiguration auf einem WLC um eine Tag-Gruppe erweitern. Dazu legen Sie zunächst eine Tag-Gruppe an und weisen diese Gruppe anschließend einem WLAN-Profil zu.

1. Öffnen Sie den Konfigurationsdialog für Ihr Gerät und wählen Sie **WLAN-Controller** > **AP-Konfiguration** > **Tag-Gruppen**.
2. Klicken Sie **Hinzufügen**, um eine neue Gruppe anzulegen.



3. Geben Sie unter **Name** den zu definierenden Tag ein und speichern Sie den Eintrag mit **OK**.
4. Wechseln Sie in den Dialog **WLAN-Controller** > **AP-Konfiguration** > **Access-Point-Tabelle**.
5. Wählen Sie ein bestehendes AP-Profil über **Bearbeiten** aus oder fügen Sie ggf. ein neues hinzu.
6. Wählen Sie unter **Gruppen** die zuvor anlegte(n) Tag-Gruppe(n) aus.
   Mehrere Tag-Gruppen trennen Sie durch eine kommaseparierte Liste.

   Die Taggruppen sind unabhängig von den Zuweisungs-Gruppen, deren Zuweisung im selben Eingabefeld erfolgt. Zuweisungs-Gruppen werden generell vom Gerät zugewiesen und bedürfen keiner nutzerseitigen Zuordnung. Das manuelle Zuordnen einer Zuweisungs-Gruppe hat gemäß der unter *IP-abhängige Autokonfiguration und Tagging von APs* auf Seite 69 beschriebenen Zustandsprüfung keinen Effekt auf die AP-Konfiguration. Auswirkungen bestehen lediglich auf die Filterung im Befehl `show capwap group` an der Konsole.

   Das manuelle Hinzufügen von Zuweisungs-Gruppen zu Filterungszwecken ist nicht empfehlenswert. Legen Sie stattdessen separate Tag-Gruppen an.
7. Schließen Sie alle Dialogfenster mit **OK** und schreiben Sie die Konfiguration zurück auf Ihr Gerät.

Der WLC versieht fortan alle APs, die das bearbeitete WLAN-Profil erhalten, mit den darin referenzierten Tags.

1.5 Access Point Verwaltung

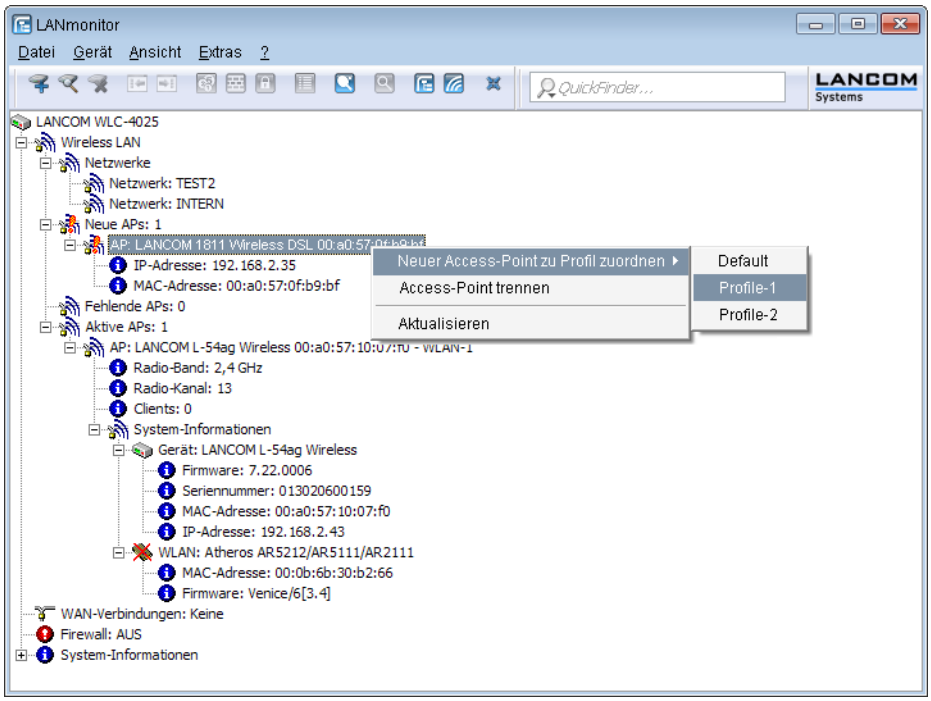
1.5.1 Neue Access Points manuell in die WLAN-Struktur aufnehmen

Wenn Sie die APs nicht automatisch in die WLAN-Struktur aufnehmen wollen, können Sie die APs auch manuell akzeptieren.

Access Points akzeptieren über den LANmonitor

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

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

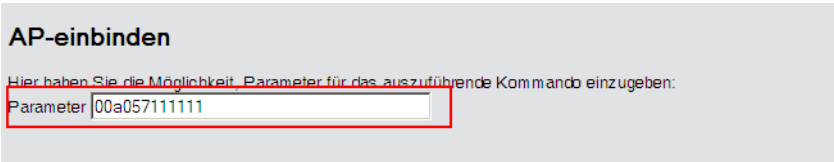


Mit dem Zuweisen der Konfiguration wird der AP in der AP-Tabelle des WLCs eingetragen. Es dauert jedoch einige Sekunden, bis der WLC dem AP auch ein Zertifikat zugewiesen hat und dieser ein aktives Element der zentralen WLAN-Struktur wird. Der neu aufgenommene AP wird also für eine kurze Zeit als "Lost AP" im LANmonitor und soweit vorhanden durch die rote Lost-AP-LED und im Gerätedisplay angezeigt, bis die Zertifikatszuweisung abgeschlossen ist.

Access Points akzeptieren über WEBconfig mit Zuweisung eines Zertifikats

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

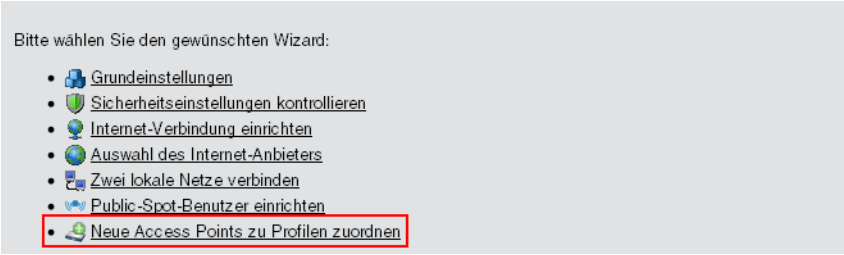
1. Öffnen Sie die Konfiguration des WLCs mit WEBconfig.
2. Wählen Sie unter **Extras** > **LCOS-Menübaum** > **Setup** > **WLAN-Management** die Aktion **AP-einbinden**.
3. Geben Sie als Parameter für die Aktion die MAC-Adresse des APs ein, den Sie akzeptieren möchten, und bestätigen Sie mit **Ausführen**.



Access Points akzeptieren über WEBconfig mit Zuweisung von Zertifikat und Konfiguration

Neue APs, 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 AP nach der Übertragung eines neuen Zertifikats zugewiesen wird.

1. Öffnen Sie die Konfiguration des WLCs mit WEBconfig. Wählen Sie unter **Setup-Wizards** den Wizard **Neue Access Points zu Profilen zuordnen**.



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

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

Neue APs über den WEBconfig Setup-Wizard hinzufügen

Ab LCOS 9.00 verfügen WLCs über einen überarbeiteten Setup-Wizard **Neue Access Points zu Profilen zuordnen**, der Ihnen das Hinzufügen neuer APs über WEBconfig erleichtert. Der neue Setup-Wizard erlaubt Ihnen, mit wenigen Mausklicks

- gezielt nach einem neuen AP zu suchen;
- ein oder mehrere neue APs gleichzeitig zu akzeptieren;
- einem neuen AP ein WLAN-Profil oder eine Kanalliste zuzuweisen;
- die Konfiguration eines bereits akzeptierten AP an einen neuen AP zu vererben;
- die Konfiguration eines akzeptierten fehlenden AP mit der eines neuen AP zu wechseln. Beim Wechseln einer Konfiguration erhält der neue AP die vollständige Konfiguration des akzeptierten fehlenden AP (mit Ausnahme der

MAC-Adresse). Beim Einbinden des neuen AP löscht der WLC anschließend die Konfiguration des akzeptierten fehlenden AP.

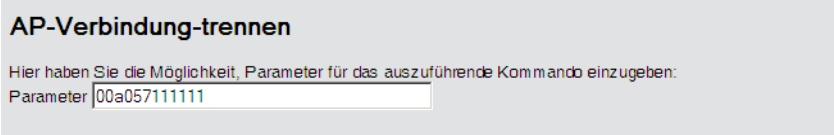
Um einen neuen AP mit den getätigten Einstellungen zu akzeptieren, klicken Sie abschließend auf **AP-einbinden**.

Sofern ein Sie einen AP über Zuweisungs-Gruppen konfigurieren lassen, brauchen Sie für den betreffenden AP keine Einstellungen in diesem Setup-Wizard vornehmen. Der WLC weist dem AP automatisch beim Einbinden die Einstellungen aus den entsprechenden Gruppen zu.

1.5.2 Access Points manuell aus der WLAN-Struktur entfernen

Um einen AP, der vom WLC verwaltet wird, aus der WLAN-Struktur zu entfernen, müssen Sie folgende Aktionen ausführen:

1. Stellen Sie im AP die WLAN-Betriebsart für die WLAN-Module von 'Managed' auf 'Client' oder 'Access-Point' um.
2. Löschen Sie im WLC die Konfiguration für den AP bzw. deaktivieren Sie die **Automatische Zuweisung der Default-Konfiguration** über **Extras** > **LCOS-Menübaum** > **Setup** > **WLAN-Management** > **AP-automatisch-einbinden**.
3. Trennen Sie die Verbindung zum AP unter WEBconfig im Bereich **Extras** > **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 APs ein, zu dem Sie die Verbindung trennen möchten, und bestätigen Sie mit **Ausführen**.



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

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

Access Point deaktivieren

Um einen AP 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 AP gelöscht.

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

Ein so deaktivierter AP bleibt mit dem WLC verbunden, die Zertifikate bleiben erhalten. Der WLC 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 AP und seine WLAN-Module im Managed-Modus wieder einschalten.

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

Access Point dauerhaft aus der WLAN-Struktur entfernen

Damit ein AP 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 AP 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 WLCs widerrufen werden. Wechseln Sie dazu unter WEBconfig in den Bereich **Extras** > **LCOS-Menübaum** > **Status** > **Zertifikate** > **SCEP-CA** > **Zertifikate** in die **Zertifikatsstatus-Tabelle**. Löschen Sie dort das Zertifikat für die MAC-Adresse des APs, den Sie aus der WLAN-Struktur entfernen möchten. Die Zertifikate werden dabei nicht gelöscht, aber als abgelaufen markiert.

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

1.6 AutoWDS – Kabellose Integration von APs über P2P-Verbindungen

In einem zentral gemanagten WLAN sind die angeschlossenen Access Points (APs) klassischerweise über das LAN mit dem WLAN-Controller (WLC) verbunden. Diese LAN-Verbindungen geben gleichzeitig die Topologie des verwalteten Netzes vor. Eine Erweiterung des Netzes um zusätzliche APs ist jedoch auf die Reichweite der kabelgebundenen Netzarchitektur beschränkt und erfordert ggf. einen Ausbau der betreffenden Infrastruktur.

Mittels **AutoWDS** haben Sie die Möglichkeit, die Erweiterung eines WLANs auf Basis von Funkstrecken (P2P) vorzunehmen und dadurch kostengünstig und schnell sehr skalierbare Netze zu errichten. "AutoWDS" steht dabei für "Automatic Wireless Distribution System". Die Funktion erlaubt Ihnen, ein FunkNetz aus mehreren APs herzustellen, welche ausschließlich drahtlos untereinander verbunden sind: die logische Verbindung allein genügt. Die möglichen Einsatzgebiete erstrecken sich z. B. auf die flächendeckende Anbindung kleiner Areale oder ganzer Gebiete an das Internet oder ein FirmenNetz, in denen eine Verbindung über LAN nicht sinnvoll oder unpraktikabel ist.

Im einfachsten Fall benötigen Sie lediglich einen WLC, der mit einem AutoWDS-fähigen AP via LAN verbunden ist. Der AP spannt das gemanagte WLAN auf und agiert gleichzeitig als "Zugangs-AP". Über den Zugangs-AP stellen hinzukommende AutoWDS-fähige APs die Verbindung zum WLC her, welcher ihnen mittels CAPWAP eine Konfiguration übermittelt. Nach Erhalt der Konfiguration und Eingliederung in das gemanagte WLAN nutzen die einzelnen APs P2P-Strecken, um Nutzerdaten weiterzuleiten, miteinander zu kommunizieren und die Topologie aufrecht zu erhalten. Weitere hinzukommende APs sind in der Lage, die eingebundenen APs ihrerseits als Zugangs-APs zu nutzen. Auf diese Weise lassen sich mehrere APs miteinander verketten und vermaschte Netze aufbauen, die optional via RSTP redundante

Verbindungen aufweisen. Aus Sicht eines hinzukommenden AP sind eingebundene APs "Master-APs". Aus Sicht des Master-AP sind hinzukommende APs "Slave-APs".

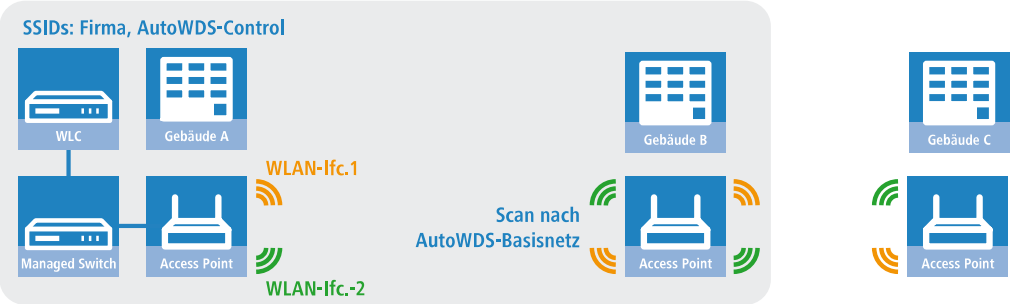


Abbildung 5: Phase 1 – Hinzukommender AP in Gebäude B sucht nach AutoWDS-Basisnetz und findet Zugangs-AP in Gebäude A

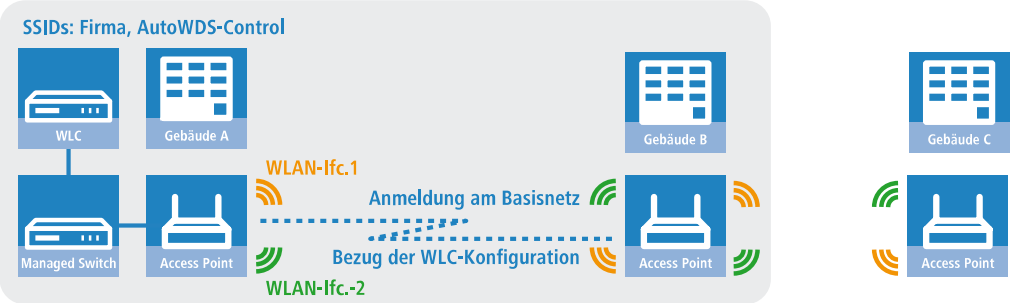


Abbildung 6: Phase 2 – Hinzukommender AP in Gebäude B findet WLC und bezieht AP-Konfiguration über CAPWAP

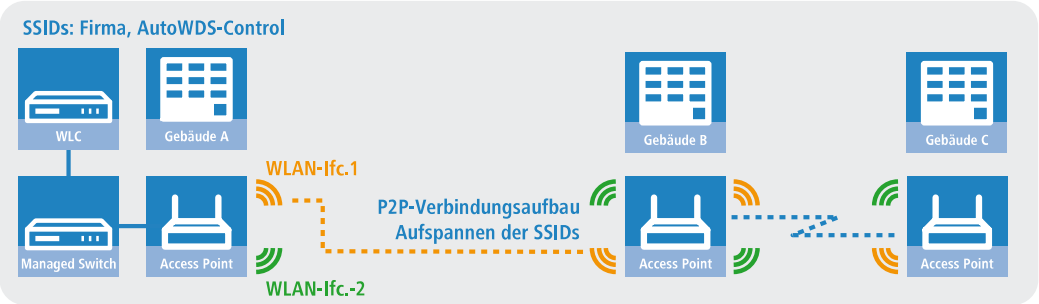


Abbildung 7: Phase 3 – Hinzukommender AP in Gebäude B integriert sich in das gemanagte WLAN. Hinzukommender AP in Gebäude C sucht nach AutoWDS-Basisnetz und findet Zugangs-AP in Gebäude B.

Genauere Informationen zum Integrationsablauf und zu den Betriebsmodi beim Topologie-Management erhalten Sie in den nachfolgenden Abschnitten zur Funktionsweise von AutoWDS.

AutoWDS eignet sich ausschließlich für statische Infrastrukturen, nicht für sich bewegende APs. Sollte ein AP aus der Reichweite seines P2P-Partners wandern und die Verbindung zum Netz verlieren, erfolgt eine temporäre Downtime mit anschließender *Rekonfiguration*. Das Roaming von WLAN-Clients zwischen einzelnen AutoWDS-APs hingegen unterscheidet sich nicht von dem zwischen normalen APs.

AutoWDS unterstützt keine Netztrennung von SSIDs auf VLANs über eine statische Konfiguration oder eine dynamische VLAN-Zuweisung über RADIUS. Soll eine Netztrennung von SSIDs erfolgen, müssen Sie diese durch Layer-3-Tunnel separieren.

Das DFS-Verhalten eines AP im 5-GHz-Betrieb ist von AutoWDS unberührt und besitzt höhere Priorität. Die DFS-Radarerkennung kann bewirken, dass der AP während des Betriebs einen plötzlichen Kanalwechsel durchführt oder das WLAN bei Ausfall der möglichen Frequenzen – aufgrund mehrerer Radarerkennungen auf verschiedenen Kanälen – für einige Zeit komplett deaktiviert. Der betroffene AP kann somit für Störungen des gesamten AutoWDS-Verbundes verantwortlich sein oder eine Zeit lang gar keine SSIDs aufspannen. Innerhalb von Gebäuden haben Sie die Möglichkeit, evtl. auftretenden Störungen durch Aktivieren des Indoor-Modus entgegenzuwirken.

Wenn Sie AutoWDS auf einem Gerät mit einer einzigen physikalischen WLAN-Schnittstelle einsetzen, drittelt sich im Betrieb deren Datenrate, da das Gerät eingehende/ausgehende Daten mehrfach senden muss: An die WLAN-Clients, an einen Master-AP und ggf. an einen Slave-AP. Um diesen Effekt zu mildern, sollten Sie ausschließlich Geräte mit mehreren physikalischen WLAN-Schnittstellen einsetzen und auf diesen eine Trennung des Datenverkehrs vornehmen. Dazu reservieren Sie eine physikalische WLAN-Schnittstelle für die Anbindung der APs und eine physikalische WLAN-Schnittstelle für die Anbindung der Clients.

MultiHop auf ein und derselben WLAN-Schnittstelle aktivieren Sie bei Bedarf in der AutoWDS-Profil-Konfiguration, da dieses aufgrund der Performance-Verluste standardmäßig deaktiviert ist.

1.6.1 Hinweise zur Nutzung von AutoWDS

Die Einsatzmöglichkeiten von AutoWDS unterliegen technischen Beschränkungen, wodurch sich die Funktion ausschließlich für bestimmte Anwendungsszenarien eignet. Bitte beachten Sie daher aufmerksam die in diesem Kapitel beschriebenen allgemeinen Hinweise, um möglichen Komplikationen vorzubeugen. Die hier gelisteten Punkte sind als Ergänzung zu den Hinweisen des übrigen AutoWDS-Kapitels zu verstehen, wobei Überschneidungen möglich sind.

- APs müssen bei Radarerkennung (5-GHz-Band, Outdoor bzw. DFS) den Kanal wechseln. Dadurch sind kurzzeitige Unterbrechungen des WLANs durch notwendigen Kanalwechsel möglich.
- Generell ist ein AutoWDS-Betrieb von bis zu maximal 3 Hops empfehlenswert.
- Bei Verwendung von AutoWDS auf ausschließlich einem Funkkanal treten Mehrfachübertragungen und Hidden-Station-Probleme auf. Empfehlenswert ist daher der Einsatz von APs mit zwei physikalischen WLAN-Schnittstellen (Dual Radio) auf separaten Funkkanälen.
- AutoWDS unterstützt keine Netztrennung von SSIDs auf VLANs über eine statische Konfiguration oder eine dynamische VLAN-Zuweisung über RADIUS. Soll eine Netztrennung von SSIDs erfolgen, müssen Sie diese durch Layer-3-Tunnel separieren.

Betreiben Sie DFS in Kombination mit AutoWDS, konfigurieren Sie für den autarken Weiterbetrieb (Continuation-Time) des AutoWDS-Profils mindestens 2 Minuten. So bleibt dem CAPWAP-Layer nach der Downtime einer P2P-Verbindung aufgrund eines DFS-Scans von einer Minute eine zusätzliche Minute Zeit, die CAPWAP-Verbindung zum WLC über die P2P-Verbindung nach dem DFS-Scan wieder herzustellen.

Achten Sie nach Möglichkeit darauf, dass alle beteiligten APs je physikalischer WLAN-Schnittstelle (WLAN-1, WLAN-2) durchgehend das gleiche Frequenzband (2,4GHz oder 5GHz) verwenden, um so eventuelle Probleme bei der automatischen Topologie-Konfiguration auszuschließen.

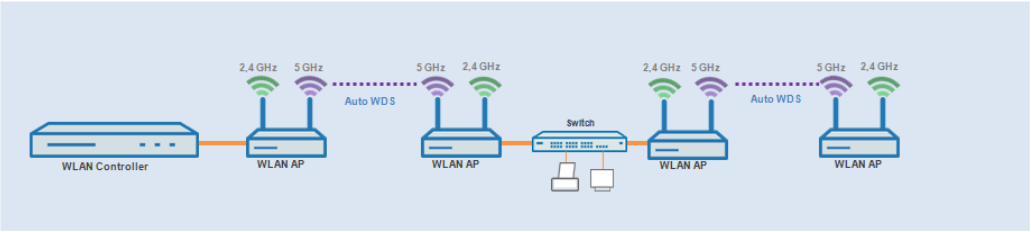
Nachfolgend finden Sie eine Bewertung der **Eignung von AutoWDS** für bestimmte von Anwendungsszenarien.

Gut geeignet:

Nutzung einer **dedizierten** physikalischen WLAN-Schnittstelle für die P2P-Strecken.

- Verwendung von unterschiedlichen Kanälen für die P2P-Strecken (Indoor)

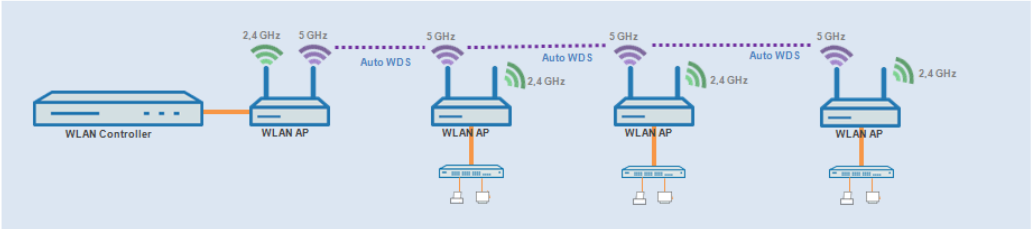
- Verwendung von AutoWDS auf bis zu 3 Hops



Bedingt geeignet:

Nutzung einer physikalischen WLAN-Schnittstelle **gleichzeitig** für AutoWDS-Uplink und -Downlink (Repeater-Modus), wobei alle P2P-Strecken den gleichen Funkkanal verwenden.

- Verwendung für Betrieb ohne DFS (Indoor)
- Verwendung von AutoWDS auf bis zu 3 Hops



Mögliche auftretende Probleme sind z. B. das sogenannte Hidden-Station-Phänomen oder die Durchsatz-Reduzierung durch Mehrfachübertragung.

- **Hidden-Station-Phänomen**: Bei größeren Entfernungen können sich weit entfernte APs des selben Netzwerkes u. U. nicht mehr gegenseitig sehen, da die Empfangsradien nicht ausreichen. In diesem Fall steigt die Wahrscheinlichkeit, dass mehrere APs gleichzeitig senden und sich in der Übertragung gegenseitig stören. Diese Kollisionen führen zu Mehrfachübertragungen und Performanz-Einbußen.

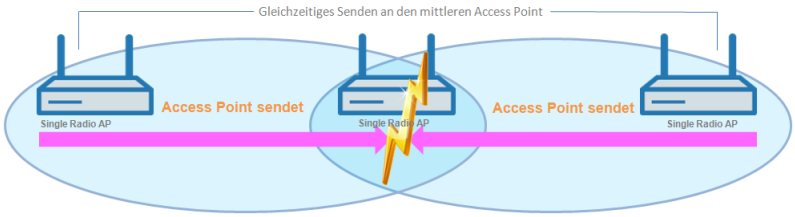


Abbildung 8: Gleichzeitiges senden an den mittleren AP: Die beiden äußeren APs erkennen die Kollision nicht.

- **Durchsatz-Reduzierung durch Mehrfachübertragung**: Überträgt ein AP Datenpakete auf dem gleichen Kanal mehrfach, reduziert sich in der Praxis der maximal erreichbare Durchsatz (Halbierung pro Hop).

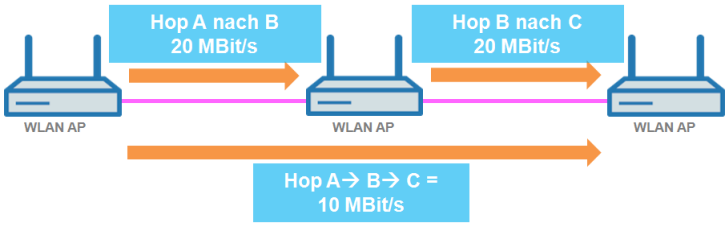
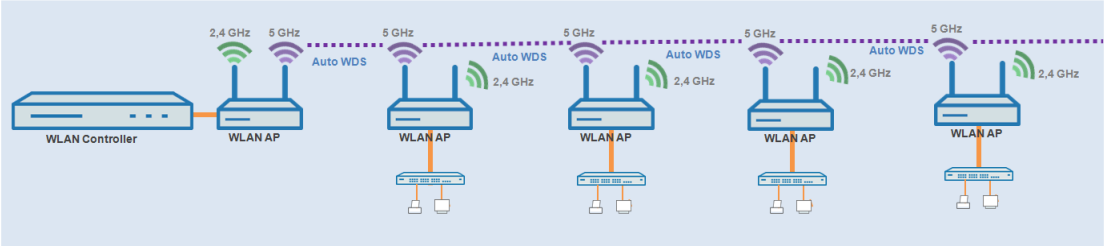


Abbildung 9: Übertragung der Datenpakete auf jedem Hop

Nicht geeignet:

Nutzung einer physikalischen WLAN-Schnittstelle **gleichzeitig** für AutoWDS-Uplink und -Downlink (Repeater-Modus) bei Outdoor-Betrieb mit mehr als 1 Hop im 5-GHz-Band.



Im Repeater-Modus nimmt die physikalische WLAN-Schnittstelle eine Doppelrolle ein: In Richtung des WLCs agiert die Schnittstelle als Master, in Richtung eines Nachbar-APs hingegen als Slave. Hierzu arbeiten alle APs notwendigerweise auf dem selben Funkkanal. Bei der Erkennung von DFS-Signalen dürfen die APs jedoch nicht mehr auf den entsprechenden Frequenzen senden. Somit kann Seitens der APs keine Meldung an den WLC über die DFS-Erkennung erfolgen und der WLC kann seinerseits keinen Frequenzwechsel für das Netz einleiten. Im Ergebnis sind die betroffenen APs ggf. permanent vom Netz getrennt.

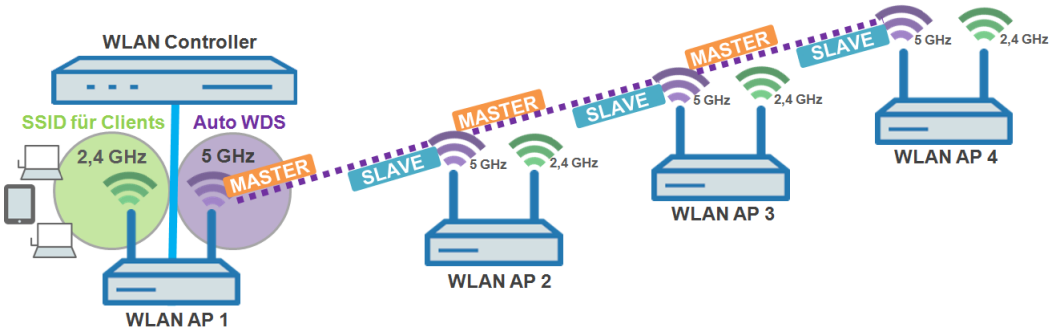


Abbildung 10: Verbindungssperre bei DFS-Erkennung

1.6.2 Funktionsweise

Aufspannen des AutoWDS-Basisnetzes

AutoWDS stellt verschiedene Integrationsmodi bereit, über die das Management von P2P-Strecken zum Errichten vermaschter Netze erfolgen kann. Den Großteil der Konfiguration nehmen Sie auf dem WLC vor, der die einzelnen logischen WLAN-Netze verwaltet. Dazu verknüpfen Sie ein aktives AutoWDS-Profil mit einem eingerichteten WLAN-Profil

Ihres gemanagten WLANs. Das AutoWDS-Profil gruppiert die Einstellungen und Grenzwerte für die Gestaltung der P2P-Topologie und des AutoWDS-Basisnetzes.

Das AutoWDS-Basisnetz bzw. die dazugehörige SSID (Vorgabename: **AutoWDS-Rollout**) ist ein reines Managementnetz: Es dient ausschließlich der Authentifizierung eines AP bei der vorkonfigurierten Integration sowie dem Aufbau des WLC-Tunnels für den Konfigurationsaustausch. Auf diese Weise lassen sich hinzukommende APs bei der Integration in das gemanagte WLAN vom operativen Betrieb isolieren. Sobald eine P2P-Verbindung zu einem Master-AP besteht, gilt ein hinzukommender AP als integriert und wickelt die weitere Kommunikation über die Bridge auf Layer 2 ab. Ähnlich wie bei klassischen P2P-Verbindungen spannen die P2P-Partner dazu eine Management-SSID auf, über die sie den Datenverkehr und den CAPWAP-Tunnel zum WLC abwickeln (siehe *Update der AP-Konfiguration und Aufbau der P2P-Strecke* auf Seite 82).

Für WLAN-Clients wie Smartphones, Laptops, etc. ist das AutoWDS-Basisnetz nicht benutzbar. Für sie muss innerhalb der WLAN-Infrastruktur eine eigene SSID aufgespannt sein.

Nachdem Sie Ihrem gemanagten WLAN ein aktives AutoWDS-Profil zugewiesen haben, spannen die betreffenden (Zugangs-)APs das AutoWDS-Basisnetz auf und senden in ihren Beacons (sofern Sie im AutoWDS-Profil 'SSID-Broadcast' aktiviert haben) und Probe-Responses eine zusätzliche, herstellerspezifische Kennung aus. Diese auch als "AutoWDSInfoFlags" bezeichnete Kennung signalisiert hinzukommenden AutoWDS-fähigen APs die generelle Unterstützung der Funktion und teilt ihnen mit, …

- ob AutoWDS für die erkannte SSID aktiv/inaktiv ist;
- ob der AP der betreffenden SSID eine aktive/inaktive WLC-Verbindung besitzt;
- ob der WLC hinzukommende APs im Express-Modus akzeptiert oder verbietet; und
- ob sich APs für die Integration mit der äquivalenten physikalischen WLAN-Schnittstelle des Zugangs-AP verbinden müssen (strikte Schnittstellen-Paarung, d. h. mit WLAN-1 auf WLAN-1 sowie mit WLAN-2 auf WLAN-2) oder gemischte Schnittstellen-Paarungen erlaubt sind.

Ein gemanagter AP funktioniert automatisch als AutoWDS-AP, sobald er sich einmal initial mit einem WLC per LAN-Kabel gepaart und ein gültiges Zertifikat sowie ein AutoWDS-Profil mit der weiteren AP-Konfiguration korrekt übertragen hat. Ein konfigurierter AutoWDS-AP funktioniert automatisch als hinzukommender AP, sobald eine CAPWAP-Verbindung zu einem WLC nach einer vordefinierten Zeit nicht gelingt, weil z. B. keine kabelgebundene LAN Verbindung existiert. Der betreffende AP wechselt die Betriebsart daraufhin temporär in den **Client**-Modus und scannt solange die einzelnen WLANs, bis er einen geeigneten Zugangs-AP erkennt. Der Scan erfolgt sowohl im 2,4-GHz- als auch im 5-GHz-Frequenzband.

Sofern Ihr Gerät über zwei physikalische WLAN-Schnittstellen verfügt und beide aktiv sind, scannen beide WLAN-Schnittstellen gleichzeitig nach einem geeigneten AutoWDS-Basisnetz. Erkennt eine physikalische WLAN-Schnittstelle eine geeignete SSID, assoziiert sie sich mit dem Zugangs-AP, sofern es die oben erwähnte Schnittstellen-Paarung erlaubt. Die andere physikalische WLAN-Schnittstelle scannt für den Fall weiter, dass die bereits assoziierte physikalische WLAN-Schnittstelle die Verbindung wieder verliert. Die andere physikalische WLAN-Schnittstelle verbindet sich aber bis dahin mit keinem weiteren AutoWDS-Basisnetz. Sobald Ihr Gerät die WLC-Konfiguration erhalten hat, verhalten sich beide physikalischen WLAN-Schnittstellen wie im Profil festgelegt und spannen die Ihnen zugewiesenen SSIDs und das AutoWDS-Basisnetz auf.

Der Ablauf des Suchvorgangs nach einem AutoWDS-Basisnetz ist identisch mit dem der Rekonfiguration bei Verlust der WLAN-Verbindung (siehe *Verlust der Konnektivität und Rekonfiguration* auf Seite 83).

Unterschiede der Integrationsmodi

Bei der Integration von hinzukommenden APs in Ihr gemanagtes WLAN haben Sie die Wahl zwischen zwei verschiedenen Integrationsmodi. Der Integrationsmodus legt die Bedingungen fest, unter denen Ihr WLC einen hinzukommenden AP akzeptiert:

- Die **vorkonfigurierte Integration** stellt den kontrollierten und bevorzugten Weg dar, einen hinzukommenden AP über eine Funkstrecke in ein gemanagtes WLAN zu integrieren. In diesem Modus gestattet der WLC ausschließlich die Integration von APs, die über eine lokal vorkonfigurierte SSID und gültige WPA2-Passphrase für das AutoWDS-Basisnetz verfügen.

Der Modus eignet sich für sämtliche Produktivumgebungen und dient dazu, einen vorgegebenen Bezug zwischen einem hinzukommenden AP und einem AutoWDS-Basisnetz herzustellen. Sobald der betreffende AP eine Konfiguration vom WLC erhält, priorisiert der AP diese Konfiguration höher als die lokale AutoWDS-Konfiguration, bis der WLC via CAPWAP die Konfiguration widerruft oder Sie den AP resetten.

- Die **Express-Integration** stellt den schnellen Weg dar, einen hinzukommenden AP über eine Funkstrecke in ein gemanagtes WLAN zu integrieren. In diesem Modus erlaubt der WLC sowohl die Integration vorkonfigurierter Geräte als auch die Integration vollkommen unkonfigurierter Geräte. Unkonfigurierte APs verfügen weder über eine eingetragene SSID noch über eine individuelle WPA2-Passphrase für ein AutoWDS-Basisnetz. Für die Authentifizierung an einem beliebigen AutoWDS-Basisnetz nutzen die Geräte stattdessen einen fest in die Firmware implementierten Pre-Shared-Key.

  Der Modus eignet sich zur einfachen Integration neuer APs in ein gemanagtes WLAN. Die Wahl eines AutoWDS-Basisnetzes geschieht hierbei automatisch und entzieht sich Ihrer Kontrolle. Sobald die betreffenden APs vom WLC eine Konfiguration erhalten, speichern die Geräte die Einstellungen als voreingestellte Werte, bis der WLC via CAPWAP die Konfiguration widerruft, das Gerät nach einem Verbindungsabbruch die Express-*Rekonfiguration* ausführt oder Sie das Gerät resetten.

  Achten Sie bei der Express-Integration darauf, dass sich keine anderen AutoWDS-Basisnetze in Reichweite befinden. Andernfalls ist es möglich, dass ein fremder WLC Ihren AP übernimmt und so Ihrem weiteren Fernzugriff entzieht. Ein aktivierter Express-Modus erweitert die Angriffsmöglichkeiten. Deshalb ist es ratsam, den Express-Modus zu deaktivieren, wenn er nicht unbedingt notwendig ist.

  LANCOM empfiehlt aus o. g. Sicherheitsgründen vornehmlich die vorkonfigurierte Integration. Über das Pairing von WLC und APs haben Sie die Möglichkeit, den Aufwand für die vorkonfigurierte Integration weiter zu reduzieren. Mehr dazu erfahren Sie im Abschnitt *Vorkonfigurierte Integration durch Pairing beschleunigen* auf Seite 88.

Nach erfolgreicher Authentifizierung am AutoWDS-Basisnetz und dem Beziehen einer IP-Adresse scannen die hinzukommenden APs das Netz nach einem WLC. Sobald sie einen WLC erkannt haben, versuchen sie, sich mit ihm zu verbinden und eine Konfiguration zu beziehen. Im LANmonitor erscheinen diese APs als neue Geräte, deren Aufnahme in das gemanagte WLAN der Administrator noch bestätigen und ihnen noch ein WLAN-Profil zuweisen muss. Die Zuweisung unterscheidet sich dabei nicht von der Aufnahme normaler APs. Alternativ kann die Zuweisung durch den WLC erfolgen, wenn Sie

- ein Default-WLAN-Profil eingerichtet und die automatische Zuweisung dessen aktiviert haben; oder
- den betreffenden AP in die Access-Point-Tabelle eingetragen und mit einem WLAN-Profil verknüpft haben.

Durch gleichzeitiges Setzen der automatischen Annahme hinzukommender APs durch den WLC ("Auto Accept") lässt sich die Integration hinzukommender APs automatisieren. Für die Express-Integration sollten Sie diese Einstellung jedoch unbedingt deaktivieren, um ein Mindestmaß an Sicherheit zu erhalten und Rogue-AP-Intrusion zu erschweren.

Der Ablauf der Zertifikatserstellung und die Zertifikatsprüfung sowie die automatische Annahme oder Verweigerung von Verbindungsanfragen durch den WLC gleichen dem eines WLAN-Szenarios mit kabelgebundenen APs. Weitere Informationen dazu finden Sie im Abschnitt *Kommunikation zwischen Access Point und WLAN-Controller* auf Seite 8.

Gestaltung der Topologie

Mit der Zuweisung des WLAN-Profils durch den WLC erhalten die Slave-APs gleichzeitig Informationen darüber, wie Ihre P2P-Strecken der Topologie des vermaschten Netzes aufzubauen sind. Die Topologie ergibt sich unmittelbar aus der Hierarchie der unter den APs aufgebauten P2P-Verbindungen. Für deren Gestaltung bietet Ihnen der WLC folgende Management-Modi an:

- **Automatisch**: Der WLC generiert automatisch eine P2P-Konfiguration. Manuell festgelegte P2P-Strecken ignoriert das Gerät.

- **Halb-automatisch**: Der WLC generiert ausschließlich dann eine P2P-Konfiguration, wenn keine manuelle P2P-Konfiguration für den hinzukommenden AP existiert. Andernfalls verwendet der WLC die manuelle Konfiguration.
- **Manuell**: Der WLC generiert selbständig keine P2P-Konfiguration. Wenn eine manuelle P2P-Konfiguration existiert, wird diese verwendet. Andernfalls überträgt der WLC keine P2P-Konfiguration zum AP.

Standardmäßig übernimmt der WLC automatisch die Berechnung der Topologie, bei der sich ein Slave-AP i. d. R. mit dem nächstgelegenen Master-AP verbindet. Die in Echtzeit berechnete Topologie protokolliert der WLC in der Status-Tabelle **AutoWDS-Auto-Topology**. Sofern Sie das halb-automatische oder manuelle Management verwenden, definieren Sie die statischen P2P-Strecken innerhalb der Setup-Tabelle **AutoWDS-Topology**. Dazu legen Sie die Beziehungen zwischen den einzelnen Master-APs und Slave-APs ähnlich einer normalen P2P-Verbindung fest. Mehr dazu finden Sie im Abschnitt *Manuelles Topologie-Mangement* auf Seite 90.

Die automatische Berechnung einer P2P-Konfiguration (z. B. bei Initial- oder Wiederverbindung eines AP) ersetzt einen in der AutoWDS-Auto-Topology-Tabelle ggf. bereits vorhandenen Eintrag.

Die automatisch generierten Topologie-Einträge sind nicht boot-persistent. Die Tabelle leert sich bei einem Neustart des WLC.

Bei der manuellen Topologie-Konfiguration ist es wichtig, dass sich ein konfigurierter P2P-Master-AP innerhalb der Topologie näher am WLC befindet als ein entsprechender P2P-Slave-AP, da bei einer kurzzeitigen Unterbrechung der P2P-Verbindung der Slave-AP nach dem Master-AP scannt.

Update der AP-Konfiguration und Aufbau der P2P-Strecke

Hat ein hinzukommender AP vom WLC via CAPWAP das WLAN-Profil mit sämtlichen darin enthaltenen Einstellungen empfangen, versucht er, als Slave eine P2P-Strecke zu dem ihm zugewiesenen Master-AP aufzubauen. Bei diesem Prozess wechselt der AP gleichzeitig seine WLAN-Betriebsart von **Client** zurück zu **Managed**.

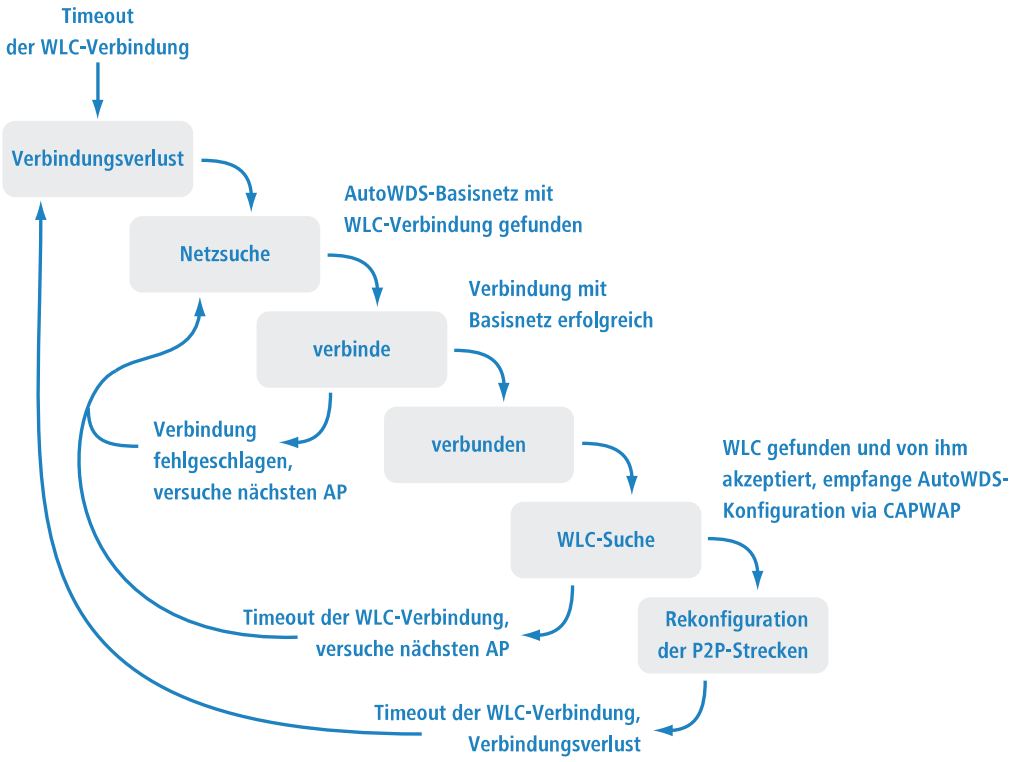
Da der Master-AP bereits im Managed-Modus agiert, erhält er vom WLC via CAPWAP lediglich ein Update seiner P2P-Konfiguration. Diese teilt dem AP neben der WPA2-Passphrase die Peer-Identifikation des AP mit. Bei einer automatisch generierten P2P-Konfiguration entspricht die Peer-Identifikation der MAC-Adresse; bei einer manuellen P2P-Konfiguration dem Namen des Slave-AP. Der Master-AP kennzeichnet derartige SSIDs mit der Kennung ***** P2P Info *****.

Sobald beide APs eine P2P-Verbindung aufgebaut haben, ist der AutoWDS-Integrationsprozess abgeschlossen. Der hinzukommende AP ist dann für Clients (Smartphones, Laptops, andere APs im Client-Modus auf der Suche nach einem Master, etc.) benutzbar.

Solange sich der hinzukommende AP im Client-Modus befindet, ist das Bridging zwischen einer physikalischen WLAN-Schnittstelle und einer LAN-Schnittstelle oder einer anderen physikalischen Funkschnittstelle während des gesamten Integrationsprozesses deaktiviert. Dazu legt das Gerät die physikalischen WLAN-Schnittstellen automatisch auf verschiedene Bridges. Erst nach dem erfolgreichen Aufbau der P2P-Verbindung schaltet der AP das Bridging wieder in den Ursprungszustand zurück.

Verlust der Konnektivität und Rekonfiguration

Sobald Sie AutoWDS auf einem hinzukommenden AP aktivieren, die Anmeldung an einem Zugangs-AP fehlschlägt oder ein eingebundener AP die Verbindung zum WLC verliert, setzt dies einen automatischen (Re-)Konfigurationsprozess in Gang, der gemäß dem abgebildeten Schema verläuft:



Ein AP durchläuft den (Re-)Konfigurationsprozess nicht, wenn er im Client-Modus zwar eine Verbindung zu einem Zugangs-AP, jedoch nicht zum WLC aufbauen kann. Der AP wartet 5 Minuten ab Verbindung zum AutoWDS-Basisnetz, ob der WLC eine Konfiguration des Gerätes durchführt. Erfolgt in dieser Zeit keine Konfiguration (z. B. weil kein Administrator den AP akzeptiert), trennt sich der AP vom AutoWDS-Basisnetz und scannt nach weiteren passenden SSIDs. Ist nur eine SSID in Reichweite, wählt der AP diese erneut für den Integrationsvorgang.

Sofern Verbindung zu einem LAN besteht, versucht der AP während der kompletten Downtime zusätzlich, per Broadcast den WLC über LAN zu erreichen. Findet der AP den WLC via LAN, erfolgt kein Aufsetzen einer neuen P2P-Strecke und der WLC löscht sämtliche automatisch generierten P2P-Strecken, die den AP als Slave festlegten.

Konfigurations-Timeouts

Sowohl die initiale Konfiguration als auch die Rekonfiguration eines hinzukommenden APs werden durch den Ablauf einzelner Zähler ausgelöst, deren Zusammenspiel das Verhalten des Gerätes steuert. Hierzu gehören, sofern festgelegt:

1. die Zeit für den autarken Weiterbetrieb der P2P-Strecke bei Verlust der CAPWAP-Verbindung (ausschließlich Rekonfiguration);
2. die Wartezeit bis zum Beginn der automatischen (Re-)Konfiguration für die vorkonfigurierte Integration; sowie
3. die Wartezeit bis zum Beginn der automatischen (Re-)Konfiguration für die Express-Integration.

Die Weiterbetriebszeit bezeichnet die Lebensdauer einer jeden P2P-Strecke für den Fall, dass der AP die CAPWAP-Verbindung zum WLC verliert. Erkennt der AP einen Verlust der CAPWAP-Verbindung, versucht er, die Verbindung innerhalb der festgelegten Weiterbetriebszeit wiederherzustellen. Während dieser Zeiten bleiben Verbindungen zu den P2P-Partnern und eingebuchten WLAN-Clients bestehen. Gelingt dem AP die Wiederherstellung nicht und ist die Weiterbetriebszeit abgelaufen, verwirft das Gerät den P2P-Teil der WLC-Konfiguration. Wenn die autarke Weiterbetriebszeit mit 0 festgelegt ist, verwirft der AP den betreffenden Konfigurationsteil sofort.

Anschließend beginnt das Gerät damit, anhand des verbliebenen Konfigurationsteils – der SSID des AutoWDS-Basisnetzes, der dazugehörigen WPA2-Passphrase sowie der Wartezeiten für die vorkonfigurierte und Express-Integration – die eingestellte Zeit bis zum Beginn der automatischen (Re-)Konfiguration für die vorkonfigurierte Integration herabzuzählen. Nach Ablauf dieser Wartezeit schaltet das Gerät seine physikalische(n) WLAN-Schnittstelle(n) in den Client-Modus um und scannt die verfügbaren SSIDs nach dem zuletzt erkannten AutoWDS-Basisnetz. Parallel dazu beginnt der Zähler bis zum Beginn der automatischen (Re-)Konfiguration für die Express-Integration herabzuzählen.

Hat das Gerät bei Ablauf des Express-Zählers das ihm bekannte AutoWDS-Basisnetz nicht gefunden, stellt das Gerät automatisch auf Express-Integration um. Anschließend sucht der AP solange nach einem beliebigen AutoWDS-fähigen Netz, bis schließlich ein geeigneter Zugangs-AP erkannt ist.

Durch intelligentes Zusammenspiel der einzelnen Wartezeiten haben Sie die Möglichkeit, das Gerät auf unvorhergesehene Ereignisse flexibel reagieren zu lassen. So lässt sich z. B. eine Fallback-Lösung für den Fall realisieren, dass Sie den Pre-Shared-Key für das AutoWDS-Basisnetz ändern, die Änderung am hinzukommenden AP jedoch fehlschlägt und sich das Gerät aufgrund einer ungültigen Konfiguration nicht mehr erreichen lässt. Bitte beachten Sie dabei die unter *Unterschiede der Integrationsmodi* auf Seite 80 aufgeführten Hinweise.

Die betreffenden Zähler konfigurieren Sie sowohl auf dem AP (z. B. via LANconfig) als auch auf dem WLC (ausschließlich im Setup-Menü). Auf dem AP werden die Zähler ausschließlich dann beachtet, wenn noch keine WLC-Konfiguration vorliegt (initiale Konfiguration). Sobald eine Konfiguration vorliegt, sind die im AutoWDS-Profil festgelegten Zählerwerte maßgebend (Rekonfiguration). Näheres zur Prioritätensetzung der Konfigurationen finden Sie unter *Unterschiede der Integrationsmodi* auf Seite 80.

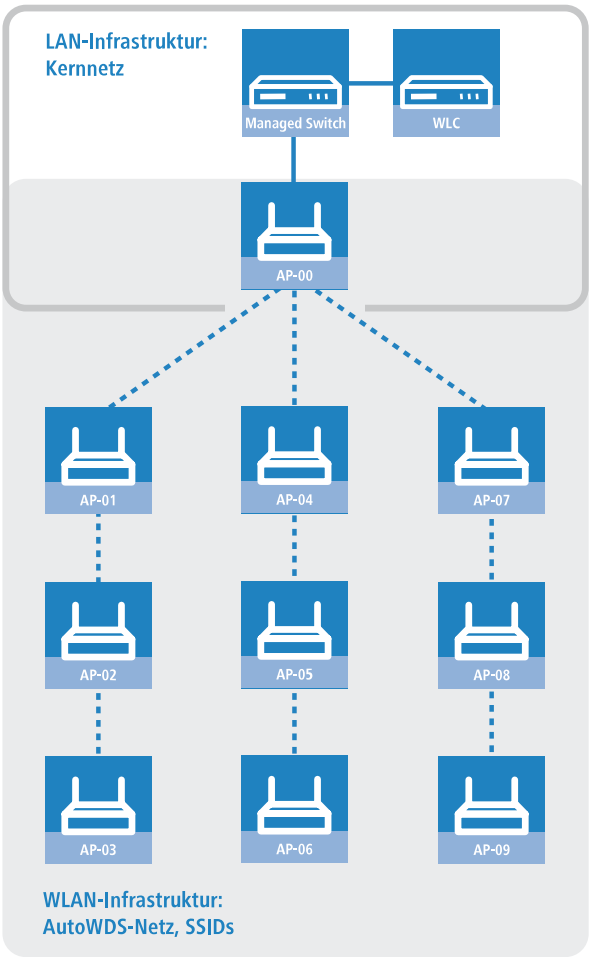
Wenn Sie den Express- oder den Vorkonfigurations-Zähler deaktivieren, überspringt das Gerät den entsprechenden Integrationsschritt. Durch Deaktivieren beider Zähler lässt sich die automatische Rekonfiguration ausschalten. Das Gerät ist dann nach einem entsprechend langen Verbindungsabbruch nicht mehr mittels AutoWDS zu erreichen. Das Gerät bleibt aber über die LAN-Schnittstelle erreichbar und sucht im LAN nach einem WLC, sofern eine entsprechende Verbindung besteht.

Der Prozess zur vorkonfigurierten Integration startet nicht, wenn die Angaben für das AutoWDS-Basisnetz (SSID, Passphrase) unvollständig sind oder der Vorkonfigurations-Zähler bei `0` liegt.

Beispiel: Ausfall eines AP

Die CAPWAP-Verbindung eines jeden AP sichert sich in einem festgelegten Intervall durch Echo-Requests zum WLC ab. Fällt ein AP aus oder ist seine Anbindung gestört, läuft ein solcher Request ins Leere. Erhalten die betreffenden APs nach mehrmaliger Wiederholung des Echo-Requests keine Antwort des WLC, gilt die CAPWAP-Verbindung als verloren und

die betreffenden APs beginnen mit dem unter *Verlust der Konnektivität und Rekonfiguration* auf Seite 83 beschriebenen Rekonfigurationsprozess.



Für die oben abgebildete Infrastruktur hätte ein Ausfall von AP-01 die nachfolgenden Auswirkungen, sofern das automatische Topologie-Management aktiviert ist:

1. AP-01 ist defekt.
2. AP-02 und AP-03 wiederholen ihre Echo-Requests; alle Wiederholungen schlagen fehl.
3. AP-02 und AP-03 gehen in den autarken Weiterbetrieb (sofern konfiguriert) und versuchen weiterhin, den WLC zu erreichen (sowohl über WLAN als auch LAN, sofern Konnektivität besteht).
4. AP-02 und AP-03 beenden den autarken Weiterbetrieb für die P2P-Verbindungen.
5. AP-02 und AP-03 zählen die Wartezeit für den Beginn der vorkonfigurierten Integration herunter.
6. AP-02 und AP-03 schalten nach Ablauf der Wartezeit in den Client-Modus und scannen das WLAN nach dem letzten bekannten AutoWDS-Basisnetz.
7. AP-02 und AP-03 finden einen neuen Zugangs-AP (z. B. AP-05 oder AP-06) und buchen sich als Client ein.
8. AP-02 und AP-03 stellen über den **WLC-TUNNEL-AUTOWDS** die CAPWAP-Verbindung wieder her und melden dem WLC den neuen Zugangs-AP sowie die verwendeten physikalischen WLAN-Schnittstellen.
9. Der WLC generiert für die betroffenen physikalischen WLAN-Schnittstellen eine P2P-Strecke und übermittelt den APs die Konfiguration via CAPWAP.
10. Die APs setzen die neue P2P-Strecke zu den Ihnen zugewiesenen Master-APs auf und kommunizieren mit dem WLC nicht mehr über den **WLC-TUNNEL-AUTOWDS**, sondern ins LAN gebridged.

1.6.3 Einrichtung mittels vorkonfigurierter Integration

Die nachfolgenden Abschnitte zeigen Ihnen, wie Sie ein AutoWDS-Netz über die vorkonfigurierte Integration einrichten. Die Konfiguration verwendet dabei das automatische Topologie-Management des WLC.

In diesem Szenario erweitert ein Unternehmen seine Geschäftsräume um einen weiteren Gebäudekomplex. Das Unternehmen will die neuen Geschäftsräume in sein bestehendes gemanagtes WLAN integrieren. Dazu sollen die betreffenden APs ausschließlich per Funkstrecke verbunden sein. Zwischen Gebäude A (alt) und Gebäude B (neu) ist keine kabelgebundene Netzverbindung erwünscht.

Um die Konfiguration einfach zu halten, konfiguriert das Unternehmen alle APs mit einem einzelnen WLC. Die genaue Anzahl der APs in Gebäude A und Gebäude B ist nebensächlich. Besonderheiten wie mehrere physikalische WLAN-Schnittstellen berücksichtigt der WLC beim Topologie-Management automatisch.

Die Konfiguration selbst gliedert sich in zwei Teile:

1. Konfiguration des WLC in Gebäude A
2. Konfiguration aller APs in Gebäude B

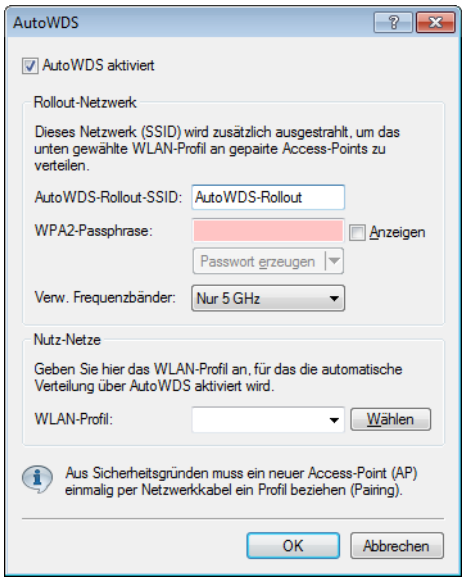
Das Anwendungsbeispiel setzt eine gültige WLAN-Konfiguration mit gültigen Zertifikaten im WLC voraus. Wie Sie ein gemanagtes WLAN einrichten, entnehmen Sie bitte dem Kapitel zum WLAN-Management.

Konfiguration des WLC

Die nachfolgenden Handlungsanweisungen beschreiben die AutoWDS-Konfiguration eines zentralen WLC für die vorkonfigurierte Integration.

Achten Sie darauf, dass die AutoWDS-APs, die sich als WLAN-Client in das Netzwerk integrieren, über das WLC-TUNNEL-AUTOWDS-Interface einen DHCP-Server erreichen. Ohne IP-Adresse werden die APs nicht nach dem WLC suchen und keine Konfiguration vom WLC erhalten.

1. Öffnen Sie den Konfigurationsdialog in LANconfig und klicken Sie **WLAN-Controller** > **Profile** > **AutoWDS**, um zum AutoWDS-Einstellungsfenster zu gelangen.



2. Klicken Sie **AutoWDS aktiviert**, um die Funktion auf dem Gerät generell zu aktivieren.
3. Geben Sie unter **AutoWDS-Rollout-SSID** den Namen des AutoWDS-Basisnetzes ein. Standardmäßig verwendet LANconfig die Bezeichnung `AutoWDS-Rollout`.

   Die hier festgelegte SSID agiert als Managementnetz für sämtliche ein AutoWDS-Netz suchenden APs und ist – bis auf die Passphrase – nicht weiter konfigurierbar. Der WLC verbindet die angegebene SSID intern automatisch mit

einem WLC-Tunnel (**WLC-TUNNEL-AUTOWDS**). Normale WLAN-Clients sind nicht in der Lage, dieses Managementnetz zu benutzen.

Vergeben Sie hier zweckmäßigerweise eine vom LANconfig-Standard abweichende individuelle AutoWDS-Rollout-SSID.

Die Einrichtung des AutoWDS-Basisnetzes reduziert die Anzahl der SSIDs, die Ihr Gerät über eine physikalische WLAN-Schnittstelle maximal aufspannen kann, um den Wert 1.

4. Geben Sie unter **WPA2-Passphrase** einen Schlüssel ein, mit dem Sie das AutoWDS-Basisnetz absichern.

   Wählen Sie dazu einen möglichst komplexen Schlüssel mit mindestens 8 und maximal 63 Zeichen. Für eine angemessene Verschlüsselung sollte der Schlüssel mindestens 32 Zeichen umfassen.

5. Geben Sie unter **Verw. Frequenzbänder** das Frequenzband an, in dem die APs das AutoWDS-Basisnetz ausstrahlen.
6. Wählen Sie das **WLAN-Profil** aus, dessen SSIDs Sie mittels AutoWDS erweitern wollen.

   Die APs des betreffenden WLAN-Profils fungieren als Zugangs-APs und spannen das AutoWDS-Basisnetz auf. Gleichzeitig erhalten via AutoWDS eingebundene APs dieses WLAN-Profil als Standardkonfiguration, unter der sie nach erfolgreicher Integration die dazugehörige SSID aussenden.

7. Schließen Sie die geöffneten Dialogfenster mit **OK** und schreiben Sie die Konfiguration zurück auf das Gerät.

Der WLC weist nun allen gemanagten AutoWDS-fähigen APs in Ihrem WLAN die AutoWDS-Einstellungen zu, woraufhin diese das AutoWDS-Basisnetz aufspannen. Für künftige Rekonfigurationsprozesse verwenden die APs ausschließlich die hier hinterlegte SSID und Passphrase, sofern nicht anders konfiguriert (siehe *Unterschiede der Integrationsmodi* auf Seite 80).

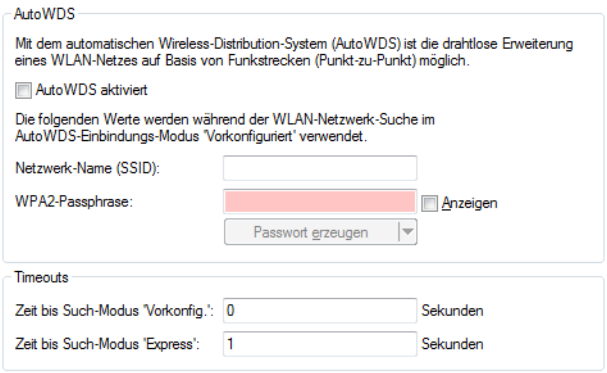
Die Konfiguration des WLC ist damit abgeschlossen. Fahren Sie nun mit der Konfiguration der APs fort.

Konfiguration der APs

Die nachfolgenden Handlungsanweisungen beschreiben die AutoWDS-Konfiguration eines AP für die vorkonfigurierte Integration. Die Konfigurationsschritte sind für sämtliche hinzukommenden APs identisch.

Die Konfiguration eines APs ist nicht notwendig, wenn der AP sich initial bereits mit einem WLC gepaired hat. Die manuelle Eingabe der SSID und der Passphrase ist optional für Geräte, die sich außerhalb der Reichweite des WLC befindet und damit ein Pairing unmöglich ist.

1. Öffnen Sie den Konfigurationsdialog in LANconfig und klicken Sie **Wireless-LAN** > **AutoWDS**, um zum AutoWDS-Einstellungsfenster zu gelangen.



2. Klicken Sie **AutoWDS aktiviert**, um die Funktion auf dem Gerät generell zu aktivieren.
3. Geben Sie unter **Netzwerk-Name (SSID)** den Namen des AutoWDS-Basisnetzes ein, das Sie auf dem WLC konfiguriert haben (z. B. `AutoWDS-Rollout`).
4. Geben Sie unter **WPA2-Passphrase** den Schlüssel des AutoWDS-Basisnetzes ein, den Sie auf dem WLC konfiguriert haben.

5. Ändern Sie die Timeout-Werte für die **Zeit bis Such-Modus 'Vorkonfig'** auf `1` und die **Zeit bis Such-Modus 'Express'** auf `0`.
6. Stellen Sie unter **Wireless LAN** > **Allgemein** > **Physikalische WLAN-Einst.** sicher, dass sich mindestens eine physikalische WLAN-Schnittstelle in der Betriebsart **Managed** befindet.
   Andernfalls sucht das Gerät zu keiner Zeit nach einem AutoWDS-Basisnetz.
7. Schließen Sie das Dialogfenster mit **OK** und schreiben Sie die Konfiguration zurück auf das Gerät.

Nach erfolgreichem Konfigurations-Update schaltet der AP seine physikalische(n) WLAN-Schnittstelle(n) in den Client-Modus und sucht nach dem eingetragenen AutoWDS-Basisnetz. Weitere Informationen zum Ablauf erhalten Sie im *Kapitel zur Funktionsweise*.

1.6.4 Vorkonfigurierte Integration durch Pairing beschleunigen

Über das einmalige Pairing von WLC und APs haben Sie die Möglichkeit, den Aufwand für die vorkonfigurierte Integration weiter zu reduzieren. Beim Pairing verbinden Sie im Vorfeld einen zurückgesetzten AP via LAN mit dem WLC, auf dem Sie Ihr gemanagtes WLAN inklusive AutoWDS eingerichtet haben. Im zurückgesetzten Zustand befindet sich der AP nach dem Einschalten automatisch im Managed-Modus. Findet der AP den WLC und akzeptiert der WLC den AP, erhält der AP automatisch sämtliche relevanten Zertifikate und Konfigurationsteile, welche die notwendigen Parameter im Gerät konfigurieren. Das Pairing ist dann abgeschlossen. Am Einsatzort installiert ein Mitarbeiter den AP und schaltet ihn ein. Das Gerät sucht dann automatisch nach dem vorkonfigurierten AutoWDS-Basisnetz.

Die nachfolgenden Schritte fassen die Vorgehensweise beim Pairing zusammen. Zusätzlich beinhalten Sie die Schritte zur automatischen Konfigurationszuweisung, um das Pairing bei einer hohen Anzahl von APs weiter zu vereinfachen.

1. Starten Sie LANconfig und richten Sie auf Ihrem WLC ein gemanagtes WLAN mit einem gültigen WLAN-Profil ein, sofern noch nicht geschehen. In LANconfig konfigurieren Sie ein solches Profil unter **WLAN-Controller** > **Profile** > **WLAN-Profile**.
2. Aktivieren Sie für dieses WLAN-Profil die AutoWDS-Funktion, wie im Abschnitt *Konfiguration des WLC* auf Seite 86 beschrieben.
3. Legen Sie unter **WLAN-Controller** > **AP-Konfiguration** > **Access-Point-Tabelle** über die Schaltfläche **Default** ein für sämtliche APs allgemein gültiges Profil an. Weisen Sie diesem Profil dabei das zuvor eingerichtete **WLAN-Profil** zu
4. Aktivieren Sie unter **WLAN-Controller** > **Allgemein** die Option **APs automatisch eine Default-Konfiguration zuweisen**.
5. **Optional:** Um die Annahme hinzukommender APs in LANmonitor nicht manuell zu bestätigen, sondern dies durch den WLC zu automatisieren, aktivieren Sie in dem Dialog zusätzlich die Option **Automatische Annahme neuer APs aktiviert (Auto-Accept)**.

   Aus Sicherheitsgründen sollten Sie diese Option lediglich dann aktivieren, wenn Sie die hinzukommenden APs über eine LAN-Schnittstelle mit dem WLC verbunden haben. Achten Sie darauf, dass keine weiteren Geräte mit dem WLC verbunden sind, um ein mögliches Rogue-AP-Intrusion auszuschließen.
6. Übertragen Sie die Konfiguration zum WLC.
7. Resetten Sie den hinzukommenden AP und schließen Sie das Gerät via LAN an den WLC an.
   Das Gerät beginnt automatisch damit, nach einem WLC zu suchen.
8. Akzeptieren Sie im LANmonitor unter **Wireless LAN** > **Neue APs** den AP, sofern Sie keine automatische Annahme eingerichtet haben.
   Das Gerät erhält daraufhin vom WLC die benötigten Konfigurationsteile für den zukünftigen gemanagten Betrieb. Nach erfolgreicher Konfiguration listet LANmonitor das Gerät im Zweig **Aktive APs**.

Das Pairing ist damit abgeschlossen und der AP für den zukünftigen AutoWDS-Betrieb einsatzbereit.

1.6.5 Einrichtung mittels Express-Integration

Die nachfolgenden Abschnitte zeigen Ihnen, wie Sie ein AutoWDS-Netz über die Express-Integration einrichten. Die Konfiguration verwendet dabei das automatische Topologie-Management des WLC.

Das Ausgangsszenario gleicht dem der *vorkonfigurierten Integration*.

Auf einem zurückgesetzten AP ist AutoWDS standardmäßig deaktiviert, sodass Sie zunächst einen kabelgebundenen Zugriff wählen müssen, um die Funktion zu aktivieren. Eine Ausnahme besteht jedoch bei Geräten, die auf Kundenwunsch explizit auf das Feature hin getauft sind: In diesem Fall ist AutoWDS standardmäßig aktiviert. Der *2. Konfigurationteil* entfällt und die Geräte lassen sich im Express-Integrationsmodus unmittelbar in Betrieb nehmen.

Die Express-Konfiguration unterliegt sicherheitsrelevanten Besonderheiten. Lesen Sie sich daher das Kapitel *Unterschiede der Integrationsmodi* auf Seite 80 aufmerksam durch.

Konfiguration des WLC

Die nachfolgenden Handlungsanweisungen beschreiben die AutoWDS-Konfiguration eines zentralen WLC für die Express-Integration.

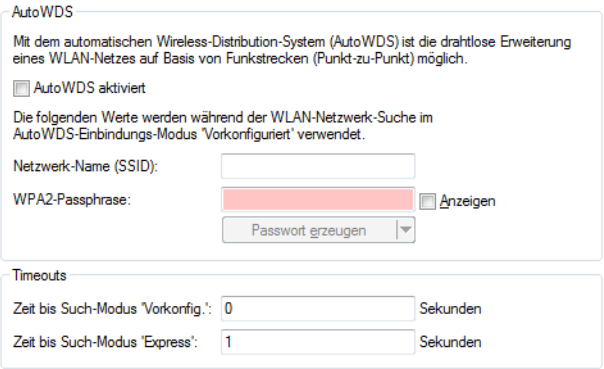
1. Führen Sie die einzelnen Handlungsschritte unter *Konfiguration des WLC* auf Seite 86 für die vorkonfigurierte Integration aus.
2. Melden Sie sich über WEBconfig oder die Konsole an Ihrem Gerät an.
3. Wechseln Sie innerhalb des Setup-Menüs in die Tabelle **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**.
4. Klicken Sie auf den Eintrag **DEFAULT**, um das AutoWDS-Standardprofil zu bearbeiten.
5. Ändern Sie den Parameter **Erlaube-Express-Integration** auf **ja** und speichern Sie die Einstellung mit einem Klick auf **Setzen**.

Die Konfiguration des WLC ist damit abgeschlossen. Fahren Sie nun mit der Konfiguration der APs fort.

Konfiguration der APs

Die nachfolgenden Handlungsanweisungen beschreiben die AutoWDS-Konfiguration eines AP für die Express-Integration. Die Konfigurationsschritte sind für sämtliche hinzukommenden APs identisch.

1. Öffnen Sie den Konfigurationsdialog in LANconfig und klicken Sie **Wireless-LAN** > **AutoWDS**, um zum AutoWDS-Einstellungsfenster zu gelangen.



2. Klicken Sie **AutoWDS aktiviert**, um die Funktion auf dem Gerät generell zu aktivieren.
3. Stellen Sie unter **Wireless LAN** > **Allgemein** > **Physikalische WLAN-Einst.** sicher, dass sich mindestens eine physikalische WLAN-Schnittstelle in der Betriebsart **Managed** befindet.
   Andernfalls sucht das Gerät zu keiner Zeit nach einem AutoWDS-Basisnetz.
4. Schließen Sie das Dialogfenster mit **OK** und schreiben Sie die Konfiguration zurück auf das Gerät.

Nach erfolgreichem Konfigurations-Update schaltet der AP seine physikalische(n) WLAN-Schnittstelle(n) in den Client-Modus und sucht nach einem beliebigen AutoWDS-Basisnetz. Weitere Informationen zum Ablauf erhalten Sie unter *Aufspannen des AutoWDS-Basisnetzes* auf Seite 79.

1.6.6 Umschalten von Express- zu vorkonfigurierter Integration

Um nach einem Netz-Rollout mittels Express-Integration auf eine vorkonfigurierte Integration umzuschalten, deaktivieren Sie die Express-Integration auf dem WLC. Ein gezieltes Umschalten der APs entfällt, da die APs im Rahmen der Express-Integration bereits eine AutoWDS-Konfiguration erhalten haben, die ein AutoWDS-Netz für spätere Rekonfigurationsprozesse vorkonfiguriert.

1. Melden Sie sich über WEBconfig oder die Konsole an Ihrem Gerät an.
2. Wechseln Sie innerhalb des Setup-Menüs in die Tabelle **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**.
3. Klicken Sie auf den Eintrag **DEFAULT**, um das AutoWDS-Standardprofil zu bearbeiten.
4. Ändern Sie den Parameter **Erlaube-Express-Integration** auf **nein** und speichern Sie die Einstellung mit einem Klick auf **Setzen**.

Damit haben Sie die Express-Integration für weitere hinzukommende APs deaktiviert.

1.6.7 Manuelles Topologie-Mangement

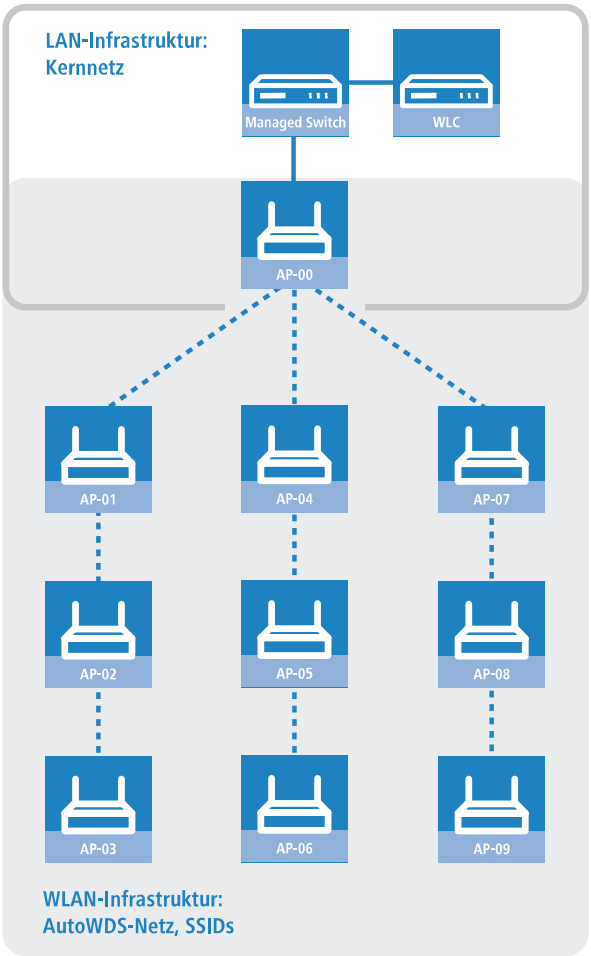
Die Einrichtungsbeispiele für AutoWDS verfolgen das automatische Topologie-Management durch den WLC, um die Konfiguration zu vereinfachen. Je nach Einsatzszenario kann es jedoch erforderlich sein, einzelne oder sämtliche P2P-Strecken manuell zu definieren.

Der nachfolgende Abschnitt zeigt Ihnen, wie Sie das automatische Topologie-Management auf dem WLC deaktivieren und eine manuelle P2P-Konfiguration anlegen. Für die Konfiguration der P2P-Strecken ordnen Sie den APs zunächst eindeutige Namen zu, die Sie anschließend mit der Topologiekonfiguration und den verwendeten physikalischen WLAN-Schnittstellen verknüpfen. Das Kapitel geht davon aus, dass Sie die unter *Einrichtung mittels vorkonfigurierter Integration* auf Seite 86 beschriebenen Schritte für den WLC bereits ausgeführt haben, um die Basis-Konfiguration abzuschließen und AutoWDS auf dem WLC generell zu aktivieren.

Generell ist ein AutoWDS-Betrieb von bis zu maximal 3 Hops empfehlenswert.

Änderungen am Ausgangsszenario

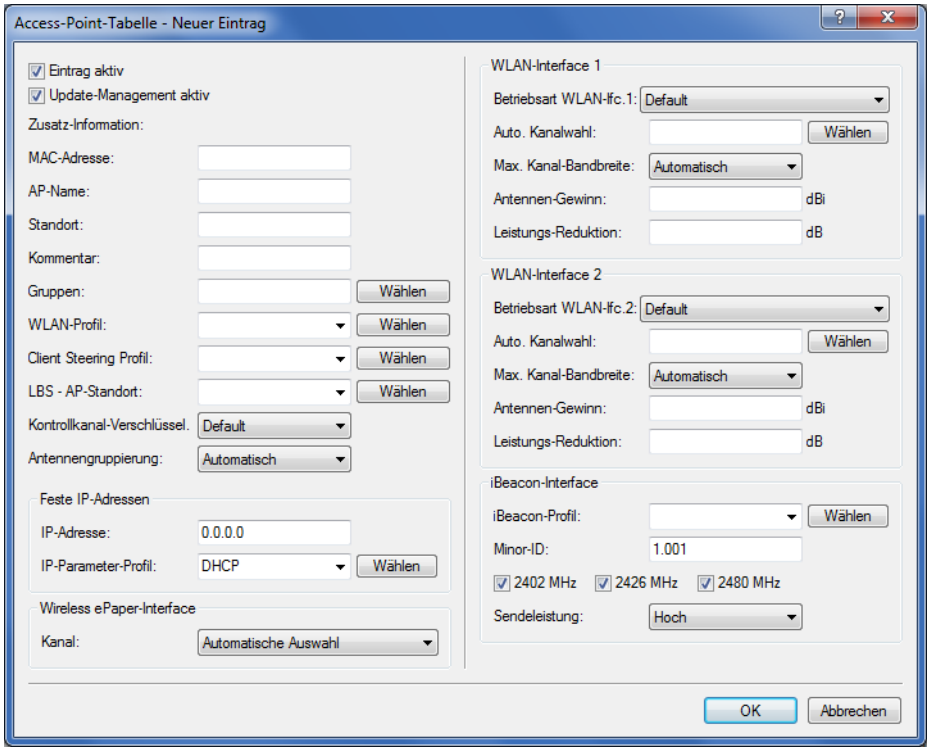
Das Ausgangsszenario gleicht dem der vorkonfigurierten Integration. Für die gesamte WLAN-Infrastruktur kommen ausschließlich Dual-Radio-APs zum Einsatz, die entsprechend der untenstehenden Grafik angeordnet sind. Das gemanagte WLAN besteht zu Beginn aus einem einzigen AP, der den hinzukommenden APs als initialer Zugangs-AP dient.



Konfiguration des WLC

Die nachfolgenden Handlungsanweisungen beschreiben die Deaktivierung des automatischen Topologie-Managements und die Konfiguration manueller P2P-Strecken gemäß des unter *Manuelles Topologie-Mangement* auf Seite 90 beschriebenen Szenarios.

1. Öffnen Sie den Konfigurationsdialog in LANconfig und klicken Sie **WLAN-Controller** > **AP-Konfiguration** > **Access-Point-Tabelle**, um zur Liste der verwalteten APs zu gelangen.



2. Geben Sie für jeden hinzukommenden AP die **MAC-Adresse** und unter **AP-Name** einen eindeutigen Namen an. Auf diesen Namen referenzieren Sie später in der Topologie-Konfiguration.

   Für das Beispielszenario lauten die einzelnen Konfigurationseinträge wie folgt:

   Tabelle 1: Konfiguration der hinzukommenden APs in der Access-Point-Tabelle

Eintrag	MAC-Adresse	AP-Name
01	00-80-63-a6-3d-f0	AP-00
02	00-a0-57-99-c6-4f	AP-01
03	00-80-63-b1-df-87	AP-02
04	00-a0-57-12-a8-01	AP-03
05	00-80-63-d9-ae-22	AP-04
06	00-a0-57-60-c4-3d	AP-05
07	00-a0-57-24-d4-1b	AP-06
08	00-80-63-a8-b1-37	AP-07
09	00-80-63-b1-df-99	AP-08
10	00-a0-57-33-e1-05	AP-09

   Der Tabelleneintrag AP-00 bezieht sich auf Ihren bereits vorhandenen AP, welchen die hinzukommenden APs als Zugangs-AP nutzen.

3. Wählen Sie das **WLAN-Profil** aus, für das Sie AutoWDS aktiviert haben.
   Über das betreffende WLAN-Profil erhalten die APs automatisch die Einstellungen für AutoWDS und damit auch die P2P-Konfiguration zugewiesen.

4. Schließen Sie die geöffneten Dialogfenster mit **OK** und schreiben Sie die Konfiguration zurück auf das Gerät.
5. Melden Sie sich über WEBconfig oder die Konsole an Ihrem Gerät an.
6. Wechseln Sie innerhalb des Setup-Menüs in die Tabelle **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**.
7. Klicken Sie auf den Eintrag **DEFAULT**, um das AutoWDS-Standardprofil zu bearbeiten.
8. Ändern Sie den Parameter **Topology-Management** auf **Manuell** und speichern Sie die Einstellung mit einem Klick auf **Setzen**.
9. Wechseln Sie in die Tabelle **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology** und klicken Sie **Hinzufügen**.
10. Legen Sie für jedes P2P-Paar eine manuelle P2P-Konfiguration an. Die festgelegte P2P-Strecke gilt stets aus Sicht des Slave-AP.
    a) Geben Sie im Feld **AutoWDS-Profil** das AutoWDS-Profil an, für das die manuelle P2P-Konfiguration gilt, z. B. `DEFAULT`.
    b) Setzen Sie die **Priorität** der P2P-Konfiguration auf `0` (höchste Priorität).
    c) Geben Sie für **Slave-AP-Name** und **Master-AP-Name** den Namen der APs entsprechend der von Ihnen gewählten Hierarchie ein.

       Für das Beispielszenario lauten die einzelnen Konfigurationseinträge bei strikter Schnittstellen-Paarung wie folgt:

       Tabelle 2: Konfiguration der P2P-Paare in der AutoWDS-Topology-Tabelle

Eintrag	Slave-AP-Name	Slave-AP-WLAN-Ifc.	Master-AP-Name	Master-AP-WLAN-Ifc.
01	AP-01	WLAN-1	AP-00	WLAN-1
02	AP-02	WLAN-2	AP-01	WLAN-2
03	AP-03	WLAN-1	AP-02	WLAN-1
04	AP-04	WLAN-2	AP-00	WLAN-2
05	AP-05	WLAN-1	AP-04	WLAN-1
06	AP-06	WLAN-2	AP-05	WLAN-2
07	AP-07	WLAN-1	AP-00	WLAN-1
08	AP-08	WLAN-2	AP-07	WLAN-2
09	AP-09	WLAN-1	AP-08	WLAN-1

    d) Geben Sie unter **Schluessel** die WPA2-Passphrase an, mit der die P2P-Partner die P2P-Strecke verschlüsseln.

       Wählen Sie dazu einen möglichst komplexen Schlüssel mit mindestens 8 und maximal 63 Zeichen. Für eine angemessene Verschlüsselung sollte der Schlüssel mindestens 32 Zeichen umfassen. Wenn Sie das Eingabefeld leer lassen, erzeugt das Gerät automatisch eine Passphrase mit einer Länge von 32 Zeichen.
    e) Schalten Sie den Eintrag **Aktiv** auf **Ja**.
    f) Speichern Sie den jeweiligen Eintrag mit einem Klick auf **Setzen**.

Waren bereits APs angeschlossen, übermittelt der WLC die neue Konfiguration an die APs und löst damit einen Rekonfigurationsprozess auf diesen aus. Waren noch keine APs angeschlossen, überträgt der WLC die P2P-Konfiguration beim ersten Verbindungsaufbau der hinzukommenden APs.

1.6.8 Redundante Strecken mittels RSTP

Das manuelle Topologie-Management eröffnet Ihnen in Kombination mit dem Rapid Spanning Tree Protocol (RSTP) die Möglichkeit, redundante P2P-Strecken einzurichten, um die Ausfallsicherheit Ihres gesamten AutoWDS-Basisnetzes zu verbessern. Hierzu müssen Sie RSTP zunächst im Setup-Menü eines jeden APs aktivieren, da sich die Management-Einstellungen des WLC nicht auf diesen Konfigurationsteil erstrecken. Um den Konfigurationsaufwand zu

reduzieren, ist der Einsatz eines Skripts empfehlenswert, welches Sie über das Skript-Management des WLC an sämtliche APs übertragen.

Die nachfolgenden Schritte zeigen Ihnen, wie Sie dabei vorgehen. Die Schritte implizieren, dass Sie ein AutoWDS-Basisnetz bereits erfolgreich eingerichtet haben. Nach seiner Aktivierung führt RSTP die Pfadsuche vollautomatisch durch.

1. Erstellen Sie eine Textdatei mit dem Namen `WLC_Script_1.lcs`.
2. Kopieren die folgenden Codezeilen in die Textdatei und speichern Sie.

```
# Script (9.000.0000 / 15.07.2014)

lang English
flash No

set /Setup/LAN-Bridge/Spanning-Tree/Protocol-Version        Rapid
set /Setup/LAN-Bridge/Spanning-Tree/Path-Cost-Computation   Rapid
set /Setup/LAN-Bridge/Spanning-Tree/Operating               yes

flash Yes

# done
exit
```

3. Melden Sie sich an der WEBconfig-Oberfläche Ihres WLCs an und wählen Sie **Extras** > **Dateimanagement** > **Zertifikat oder Datei hochladen**.
4. Wählen Sie in der Auswahlliste **Dateityp** den Eintrag **CAPWAP – WLC_Script_1.lcs** und über die Schaltfläche **Durchsuchen** die zuvor angelegte Skriptdatei aus. Klicken Sie anschließend auf **Upload starten**.
   Den erfolgreichen Upload des Skripts in den WLC prüfen Sie z. B. über das Status-Menü unter **Dateisystem** > **Inhalt**.
5. Wechsel Sie im Setup-Menü zum Menüpunkt **WLAN-Management** > **Zentrales-Firmware-Management** > **Skriptverwaltung** und klicken Sie **Hinzufügen**.
6. Geben Sie als **Profil** Ihr entsprechendes WLAN-Profil an und als **Name** `WLC_Script_1.lcs` ein, um das AutoWDS-Profil mit dem Skriptnamen zu verbinden und an die APs auszurollen.
7. Weisen Sie – wie in Kapitel *Konfiguration des WLC* auf Seite 91 beschrieben – den APs im WLC eindeutige Namen zu und richten Sie die manuellen P2P-Strecken ein.

Damit haben Sie die Konfiguration erfolgreich abgeschlossen.

1.7 Zentrales Firmware- und Skript-Management

Mit einem WLC kann die Konfiguration von mehreren LANCOM Wireless Routern und APs 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.

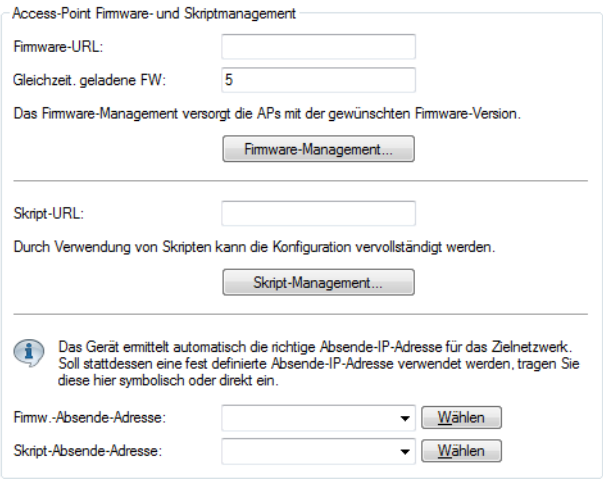
Dazu werden die Firmware- und Skript-Dateien auf einem Web-Server abgelegt (Firmware als *.UPX, Skripte als *.LCS). Der WLC prüft einmal täglich oder aufgrund einer entsprechenden Benutzeraktion den Bestand und vergleicht die verfügbaren Dateien mit den Versionen in den Geräten – alternativ kann dieser Vorgang auch über einen Cron-Job z. B. nachts erledigt werden. Wenn ein Update durchgeführt werden kann oder nicht die gewünschte Version auf dem AP läuft, lädt der WLC diese vom Webserver herunter und spielt sie in die entsprechenden Wireless Router und APs 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 AP automatisch neu.
- Wenn der AP schon verbunden ist, startet das Gerät danach **nicht** automatisch neu. In diesem Fall wird der AP manuell über die Menüaktion **Setup** > **WLAN-Management** > **Zentrales-Firmware-Management** > **Aktualisierte-APs-neustarten** oder zeitgesteuert per Cron-Job neu gestartet.

- Mit der Aktion **Setup** > **WLAN-Management** > **Zentrales-Firmware-Management** > **Aktualisiere-Firmware-und-Skript-Information** können Skript- und Firmwareverzeichnisse aktualisiert werden.



Sie finden die Parameter zur Konfiguration auf folgenden Pfaden:

LANconfig: **WLAN-Controller** > **AP-Update**

WEBconfig: **Setup** > **WLAN-Management** > **Zentrales-Firmware-Management**

1.7.1 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

  Beachten Sie, dass der angegebene Web-Server das Directory Listing erlauben muss. Das Firmware-Management bezieht auf diese Weise die Information über die angebotenen Firmwares.

- **Gleichzeitig geladene FW**

  Anzahl der gleichzeitig im Arbeitsspeicher des WLCs vorgehaltenen Firmware-Versionen.

  Die hier vorgehaltenen Fimrware-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' fur 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.

  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

In dieser Tabelle wird hinterlegt, welche Geräte (MAC-Adresse) und Gerätetypen mit welcher Firmware betrieben werden sollen.

Gerätetypen

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

- Mögliche Werte: Alle oder 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. Auf diese Version der Firmware wird ggf. ein Update für die spezifizierten Geräte bzw. Gerätetypen erfolgen. Die Angabe erfolgt in der Form: „xx.yy“, z. B. 10.40. Default: Leer

Datum

Das Datum ermöglicht ein Downgrade auf eine spezifische Firmware-Version innerhalb einer Release, z. B. von einem Release-Upgrade (RU) auf ein früheres Upgrade.

- Mögliche Werte: 8 Zeichen aus 0123456789. Der Eintrag muss dem Format des UPX-Headers entsprechen, also z. B. „01092014“ für den 01.09.2014.
- 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

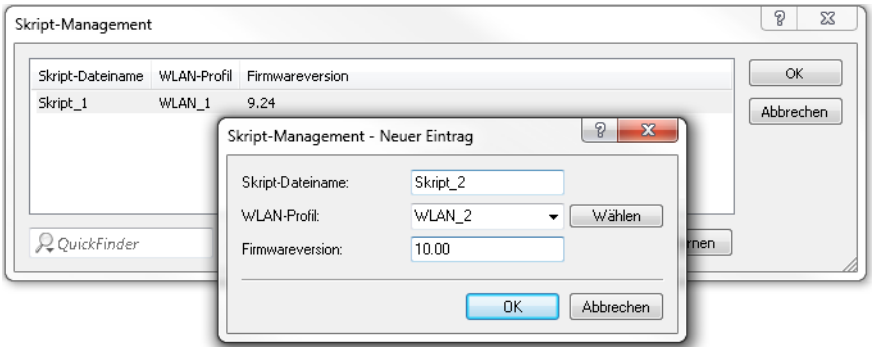
Skript-Management-Tabelle

In dieser Tabelle werden Skripte anhand ihres Dateinamens einem WLAN-Profil zugeordnet.

Die Konfiguration eines Wireless Routers und 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-Profils verwaltet werden. Dabei erfolgt die Zuordnung ebenfalls über

die WLAN-Profile, um für die Wireless Router und APs 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 Wireless Router oder Access Point wird allerdings eine MD5-Prüfsumme der Skript-Datei gespeichert. Über diese Prüfsumme kann der WLC bei einer neuen oder geänderten Skript-Datei mit gleichem Dateinamen feststellen, ob die Skript-Datei erneut übertragen werden muss.



Skript-Dateiname

Tragen Sie den CAPWAP-Slot ein, den Sie beim Upload des Skriptes in den WLAN-Controller ausgewählt haben (WLC_Script_1.lcs, WLC_Script_2.lcs oder WLC_Script_3.lcs). Bezieht der WLAN-Controller das Skript von einem Web-Server, muss der Skript-Name des Skriptes auf dem Web-Server hinterlegt werden. 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

Firmwareversion

Mit der Angabe einer Firmwareversion legen Sie fest, für welche LCOS-Version das entsprechende Skript ausgerollt werden soll.

Bitte beachten Sie, die Firmware in der Form „xx.yy“ anzugeben, z. B. 10.00 oder 9.24.

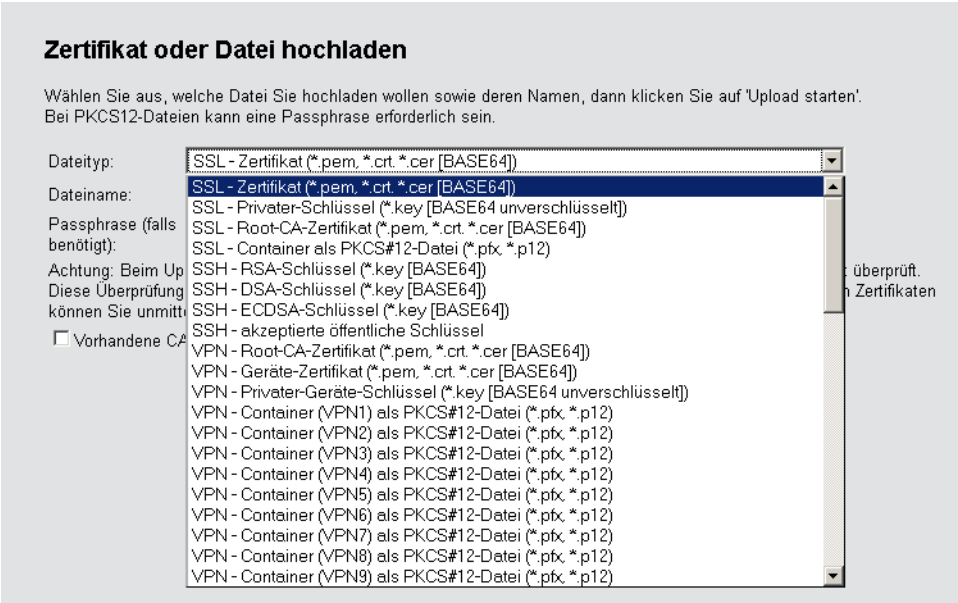
Interner Skript-Speicher (Skript-Management ohne HTTP-Server)

Skripte haben im Gegensatz zu Firmware-Dateien oft nur ein geringes Datenvolumen. Im internen Skript-Speicher der WLCs 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!



1.8 RADIUS

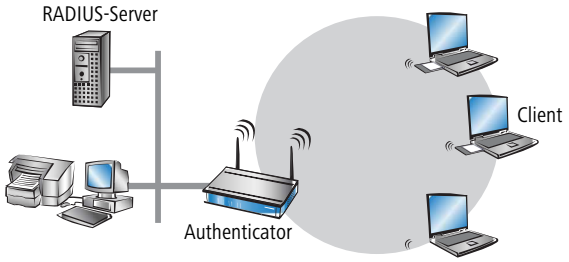
RADIUS steht für „Remote Authentication Dial-In User Service“ und wird als „Triple-A-Protokoll“ bezeichnet. Dabei stehen die drei „A“ für

- Authentication (Authentifizierung)
- Authorization (Autorisierung)
- Accounting (Abrechnung)

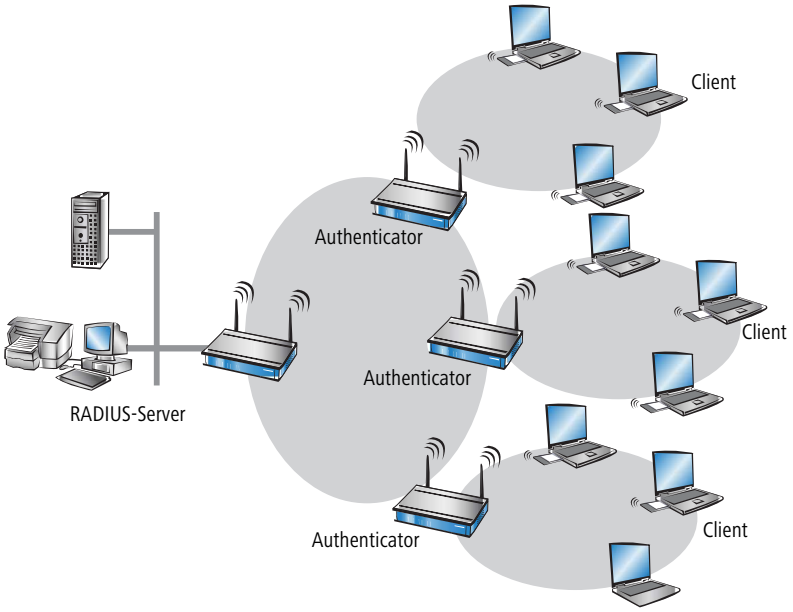
Sie können mit diesem Protokoll Benutzern Zugang zu einem Netz gewähren, ihnen bestimmte Rechte zuweisen und ihre Aktionen verfolgen. Gegebenenfalls können Sie auch die in Anspruch genommenen Leistungen gegenüber dem Benutzer mit Hilfe des RADIUS-Servers abrechnen (z. B. bei WLAN Hotspots). Für jede Aktion, die vom Benutzer durchgeführt wird, kann der RADIUS-Server eine Autorisierung durchführen, und so den Zugriff auf Netzwerkressourcen je nach Benutzer freigeben oder sperren.

Damit RADIUS funktioniert, sind 3 verschiedene Geräte nötig.

- Client: Das ist ein Gerät (PC, Notebook etc.) über das der Benutzer sich in das Netz einwählen möchte.
- Authenticator: Eine Netzwerkkomponente, welche die Authentifizierung weiterleitet und zwischen dem Netz und dem Client liegt. Diese Aufgabe kann z. B. ein Access Point übernehmen. Der Authenticator wird auch als Network Access Server (NAS) bezeichnet.



- Authentication-Server: RADIUS-Server, auf dem die Daten für die Benutzer konfiguriert sind. Dieser steht gewöhnlich in dem Netz, für das er Zugangsberechtigungen erteilen soll. Er ist für den Client über den Authenticator erreichbar. Auch für diese Aufgabe kann in entsprechenden Szenarien ein Access Point eingesetzt werden.



Der Authenticator hat zunächst keine Informationen über die Clients, die sich anmelden wollen. Diese sind alle in einer Datenbank des RADIUS-Servers gespeichert. Welche Anmeldeinformationen der RADIUS-Server für die Authentifizierung benötigt, ist dort in der Datenbank hinterlegt und kann von Netzwerk zu Netzwerk variieren. Der Authenticator hat nur die Aufgabe, die Informationen zwischen dem Client und dem RADIUS-Server zu übertragen.

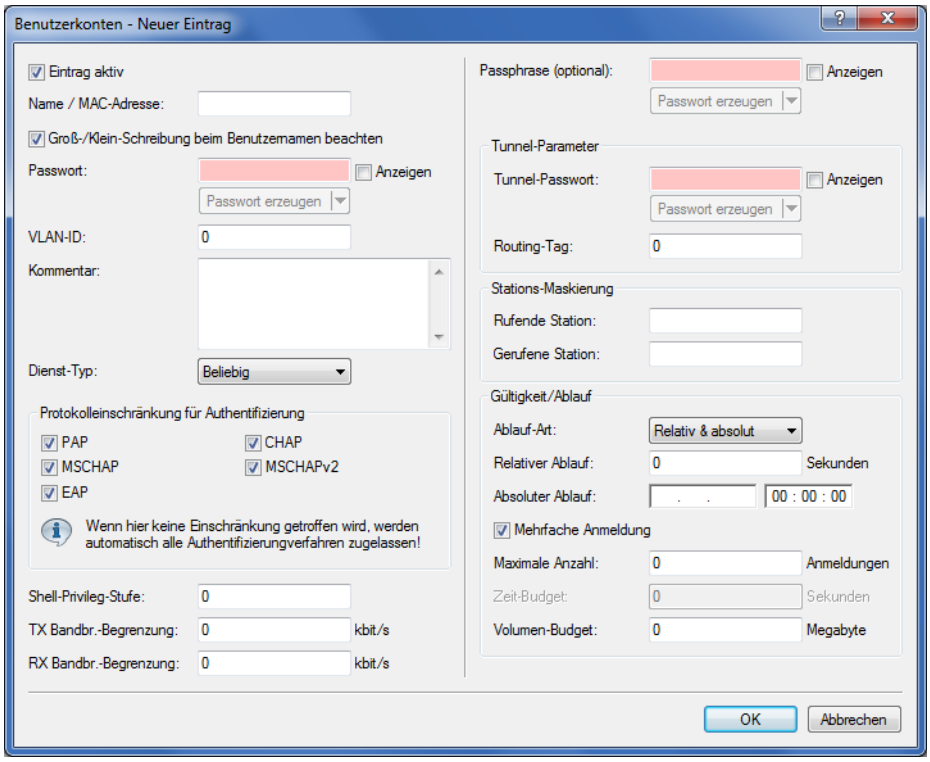
Der Zugang zu einem RADIUS-Server kann über verschiedene Wege aufgebaut werden:

- Über PPP bei der Einwahl in ein Netzwerk
- Über WLAN
- Über einen Public Spot für Benutzer, die sich per Browser anmelden
- über das 802.1X-Protokoll

1.8.1 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 WLC genutzt werden, um nur bestimmten WLAN-Clients anhand ihrer MAC-Adresse den Zugang zum WLAN zu erlauben.

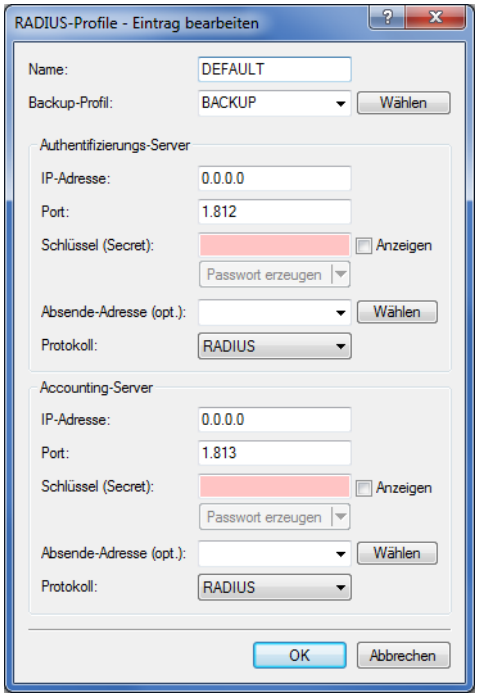
Tragen Sie die zugelassenen MAC-Adressen über LANconfig in die RADIUS-Datenbank im Konfigurationsbereich **RADIUS** > **Server** auf der Registerkarte **Allgemein** ein. Verwenden Sie dabei die MAC-Adresse als **Name** und ebenso als **Passwort** und wählen Sie als Authentifizierungsmethode **Alle**.



1.8.2 Externer RADIUS-Server

Standardmäßig übernimmt der WLC die Weiterleitung von Anfragen für die Konto- bzw. Zugangsverwaltung an einen RADIUS-Server. Damit die APs den RADIUS-Server direkt ansprechen können, müssen entsprechenden Server-Informationen hier definiert werden. Somit funktioniert die RADIUS-Anwendung auch dann noch, wenn der WLC nicht erreichbar ist. Allerdings müssen dafür Einstellungen für jeden einzelnen AP im adressierten RADIUS-Server vorgenommen werden und

die managed APs 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** > **Profile** > **RADIUS-Profile**

Name

Geben Sie eine Bezeichnung für diesen Eintrag ein.

Backup-Profil

Wählen Sie aus der Liste der RADIUS-Server-Profile ein Profil als Backup-Server.

Authentifizierungs-Server

IP-Adresse

Tragen Sie die IP-Adresse des Authentifizierungs-Servers ein.

Port

Tragen Sie den Port des Authentifizierungs-Servers ein.

Schlüssel (Secret)

Dieser Eintrag enthält den Schlüssel (Shared Secret) zur Autorisierung.

Anzeigen

Ativiert / deaktiviert die Anzeige des Schlüssels.

Absende-Adresse (optional)

Geben Sie hier ggf. die Loopback-Adresse des Gerätes an.

Protokoll

Wählen Sie aus dem Drop-Down-Menü zwischen dem normalen RADIUS-Protokoll und dem sicheren RADSEC-Protokoll für die RADIUS-Anfrage.

Accounting-Server

IP-Adresse

Tragen Sie die IP-Adresse des Accounting-Servers ein.

Port

Tragen Sie den Port des Accounting-Servers ein.

Schlüssel (Secret)

Dieser Eintrag enthält den Schlüssel (Shared Secret) zur Autorisierung.

Anzeigen

Ativiert / deaktiviert die Anzeige des Schlüssels.

Absende-Adresse (optional)

Geben Sie hier ggf. die Loopback-Adresse des Gerätes an.

Protokoll

Wählen Sie aus dem Drop-Down-Menü zwischen dem normalen RADIUS-Protokoll und dem sicheren RADSEC-Protokoll für die RADIUS-Anfrage.

1.8.3 Dynamische VLAN-Zuweisung

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

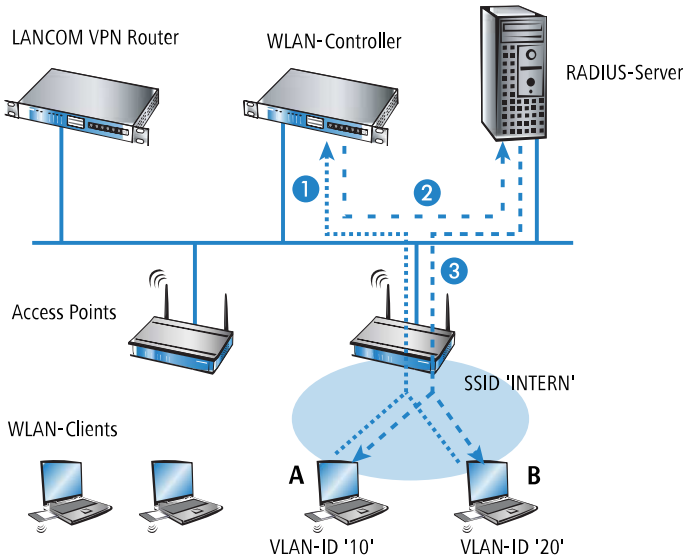
Um die WLAN-Clients **unabhängig** von dem WLAN-Netzwerk, in dem sie sich gerade eingebucht haben, in ein bestimmtes Netzwerk zu leiten, können dynamisch zugewiesene VLANs genutzt werden. Anders als bei den statisch konfigurierten VLAN-IDs für eine bestimmte SSID wird die VLAN-ID dabei dem WLAN-Client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

Beispiel:

- Die WLAN-Clients der Mitarbeiter buchen sich über einen AP in das WPA2-gesicherte WLAN mit der SSID 'INTERN' ein. Bei der Anmeldung werden die RADIUS-Anfragen der WLAN-Clients an den AP gestellt. Wenn sich das entsprechende WLAN-Interface in der Betriebsart 'Managed' befindet, werden die RADIUS-Anfragen automatisch an den WLC weitergereicht. Dieser leitet die Anfragen seinerseits an den konfigurierten RADIUS-Server weiter. Der RADIUS-Server kann die Zugangsberechtigung der WLAN-Clients prüfen. Darüber hinaus kann er allerdings auch z. B. anhand der MAC-Adresse eine bestimmte VLAN-ID 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 AP 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 einen 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. Auf diese Weise kann z. B. den unbekannten MAC-Adressen der Besucher in einer Firma eine VLAN-ID zugewiesen werden, die für den Gastzugang z. B. nur die Internetnutzung erlaubt, jedoch keinen Zugang zu anderen Netzwerkressourcen.

Alternativ zu einem externen RADIUS-Server kann den WLAN-Clients auch über den internen RADIUS-Server oder die Stationstabelle im WLC eine VLAN-ID zugewiesen werden.



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

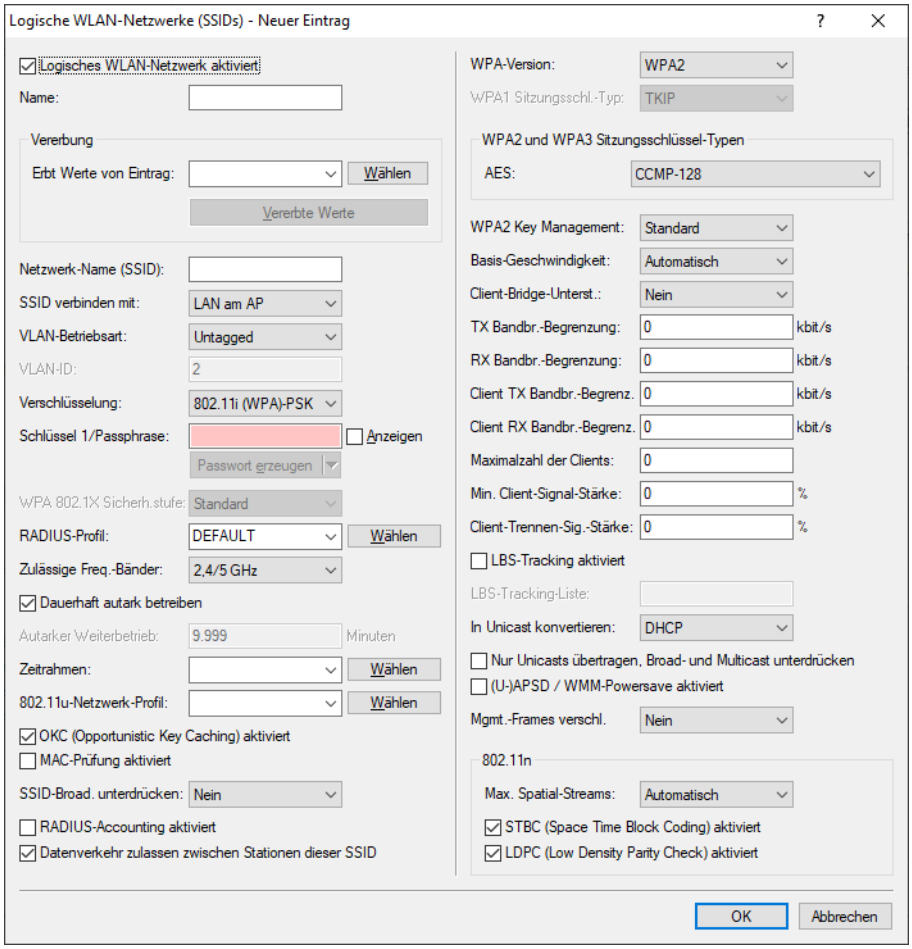
   Sowohl für die Authentifizierung über 802.1X als auch für die Prüfung der MAC-Adressen ist bei der Verwaltung von WLAN-Modulen über einen WLC ein RADIUS-Server erforderlich. Der WLC trägt sich dabei automatisch in den von ihm verwalteten APs als RADIUS-Server ein – alle RADIUS-Anfragen an die APs werden daher direkt an den WLC weitergeleitet, der die Anfragen entweder selbst bearbeiten oder sie alternativ an einen externen RADIUS-Server weiterleiten kann.
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 **Menübaum** > **LCOS-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.
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.

1.8.4 RADIUS-Accounting im WLAN-Controller für logische WLANs aktivieren

Die Konfiguration der logischen WLAN-Netzwerke finden Sie in folgendem Menü:

LANconfig: **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke (SSIDs)**



RADIUS-Accounting aktiviert

Stellen Sie hier ein, ob das RADIUS-Accounting in diesem logischen WLAN-Netzwerk aktiviert werden soll.

Mögliche Werte:

- ja, nein

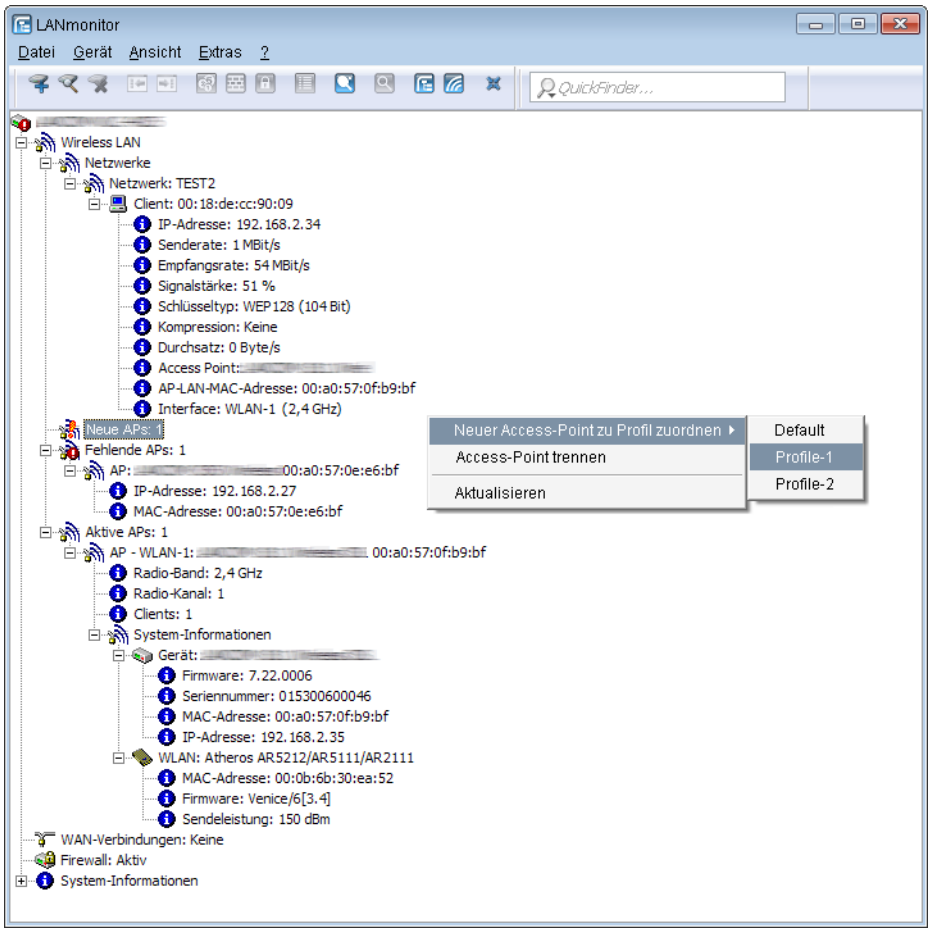
Default:

- nein

Die APs, die der WLC mit diesem logischen WLAN-Netzwerk konfiguriert, müssen eine LCOS-Version 8.00 oder höher verwenden.

1.9 Anzeigen und Aktionen im LANmonitor

Über den LANmonitor haben Sie einen schnellen Überblick über die WLC im Netzwerk und die APs in der WLAN-Struktur. LANmonitor zeigt dabei u. a. die folgenden Informationen:



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

> Falls der AP wegen einer älteren Firmware diese Daten nicht überträgt, entnimmt der WLC den Kanal und die Frequenz aus der Status-Tabelle **Aktive-Radios** unter **Status** > **Aktive-Radios** > **WLAN-Management** > **AP-Status**.

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

- **Neuen Access Point zu Profil zuordnen**

  Bietet die Möglichkeit, einem neuen AP eine Konfiguration zuzuordnen und ihn so in die WLAN-Struktur aufzunehmen.

- **Access Point trennen**

Trennt die Verbindung zwischen AP und WLC. Der AP sucht dann erneut nach einem zuständigen WLC. Diese Aktion wird z. B. verwendet, um APs nach einem Backup-Fall vom Backup-WLC zu trennen und wieder auf den eigentlichen WLC zu leiten.

> **Aktualisieren**

Aktualisiert die Anzeige des LANmonitors.

1.10 Funkfeldoptimierung

Mit der Auswahl des Kanals in der Kanal-Liste wird der Teil des Frequenzbandes festgelegt, den ein AP für seine logischen WLANs verwendet. Alle WLAN-Clients, die sich mit einem AP 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 AP Daten übertragen. Um in der Funkreichweite eines anderen APs ein WLAN mit maximaler Bandbreite betreiben zu können, muss jeder AP einen separaten Kanal nutzen – anderenfalls müssen sich die WLANs die Bandbreite des Kanals teilen.

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

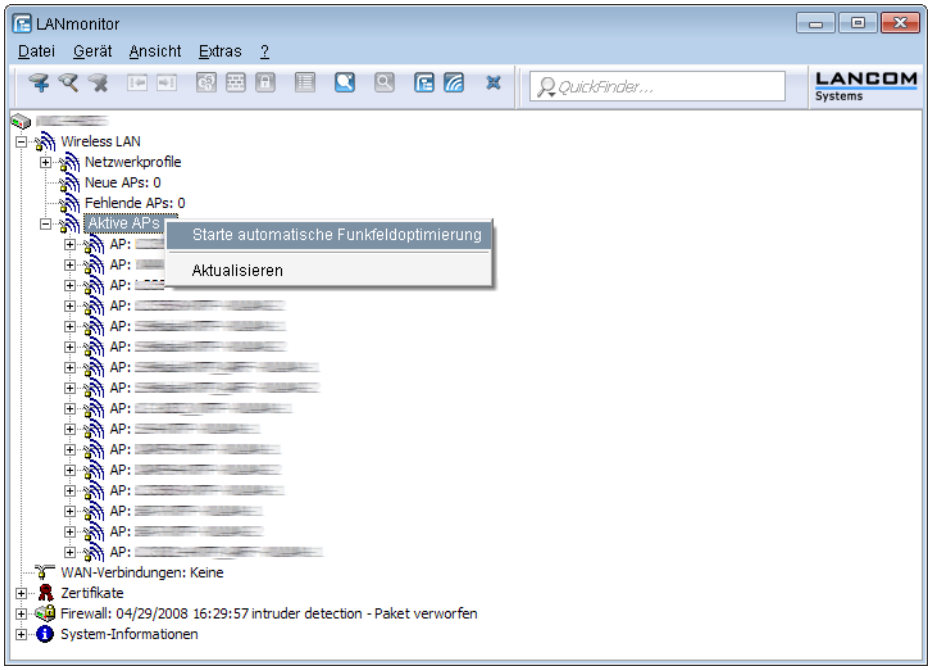
In größeren Installationen mit mehreren APs ist es manchmal schwierig, für jeden AP einen geeigneten Kanal einzustellen. Mit der automatischen Funkfeldoptimierung bieten die WLCs ein Verfahren, um die optimalen Kanäle der APs für das 2,4-GHz- und 5-GHz-Band automatisch einzustellen.

Für APs, die im 5-GHz-Band funken, muss sichergestellt sein, dass der "Indoor-Only"-Modus aktiviert ist.

Konsole: **Setup** > **WLAN-Management** > **Starte-automatische-Funkfeldoptimierung**

Sie können die Optimierung auch gezielt für einen einzelnen AP starten, indem Sie die MAC-Adresse als Parameter für die Aktion eintragen.

LANmonitor: Klicken Sie mit der rechten Maustaste auf die Liste der aktiven APs oder auf ein bestimmtes Gerät und wählen Sie danach im Kontextmenü **Starte automatische Funkfeldoptimierung**.



Die Optimierung läuft dann in den folgenden Schritten ab:

1. Der WLC weist allen APs den gleichen Kanal zu. Hierbei verwendet er den Kanal, der von den meisten APs genutzt wird.
2. Die APs führen einen "Background-Scan" durch und melden das Ergebnis an den WLC.
3. Der WLC bestimmt für jeden AP auf Basis der im "Background-Scan" erkannten Geräte einen Interferenzwert.
4. Anschließend löscht er die AP-Kanalliste aller APs. Da die Kanalliste nun leer ist, erhalten die APs über ein Konfigurations-Update die neue Kanalliste ihres jeweiligen Profils.
5. Der WLC deaktiviert die Funkmodule aller APs.
6. Die einzelnen APs durchlaufen nun nacheinander die folgenden Schritte. Es beginnt der AP mit dem höchsten Interferenzwert, um sicherzustellen, dass dieser AP zuerst einen Kanal wählen kann.
7. In der Reihenfolge der Interferenzwerte aktiviert der WLC die Funkmodule der APs, die daraufhin die automatische Einmessung starten. Der jeweilige AP sucht selbstständig den für ihn besten Kanal aus der ihm zugewiesenen Kanalliste. Zur Bestimmung des am besten geeigneten Kanals führt der AP jeweils eine Interferenz-Messung durch, so dass er Signalstärken und Kanäle anderer APs entsprechend berücksichtigen kann. Da die bisherige Liste in der Konfiguration des WLCs gelöscht wurde, ist dies nun die Profilkanalliste. Wenn die Profilkanalliste leer ist, hat der AP die freie Auswahl aus den nicht durch andere Funk-Module belegten Kanälen. Der gefundene Kanal wird zurück an den WLC gesendet und dort in der AP-Kanalliste gespeichert. Somit erhält der AP beim nächsten Verbindungsaufbau wieder diesen Kanal. Die AP-Kanalliste hat so gesehen ein höheres Gewicht als die Profilkanalliste.

Verfügt ein AP über mehrere WLAN-Module, so durchläuft jedes WLAN-Modul nacheinander diesen Vorgang.

Die Funkfeldoptimierung ist Bestandteil von LANCOM Active Radio Control (ARC).

1.10.1 Gruppenbezogene Funkfeldoptimierung

Ein WLC erlaubt eine Gruppierung von APs anhand von Standortinformationen, Geräteeigenschaften oder Netzgliederungen. Auf Basis dieser Gruppenzugehörigkeit lässt sich auch eine Funkfeldoptimierung durchführen. Statt also entweder für alle oder nur für einen AP eine Funkfeldoptimierung durchzuführen, können Sie z. B. alle AP innerhalb eines Gebäudetrakts mit einer speziellen Bezeichnung oder mit einer bestimmten Firmware-Version adressieren.

Die entsprechende Gruppe lässt sich sowohl über WEBconfig als auch die Konsole mit dem Gruppen-Parameter ansprechen:

```
do /Setup/WLAN-Management/start optimization <Gruppe>
```

Die APs sind über folgende Optionen des Gruppen-Parameters filterbar:

-g <Gruppenname>

APs, die der Gruppe angehören. Mehrere Gruppennamen sind durch Komma getrennt möglich.

-l <Standort>

APs, deren Standort entsprechend festgelegt ist.

Die Kombination von `-l` und einer der Standort-Optionen `-c` bis `-r` ist nicht sinnvoll.

-c <Land>

APs mit der entsprechenden Landesangabe.

-i <Stadt>

APs mit der entsprechenden Stadtangabe.

-s <Straße>

APs mit der entsprechenden Straßenangabe.

-b <Gebäude>

APs mit der entsprechenden Gebäudeangabe.

-f <Etage>

APs mit der entsprechenden Etagenangabe.

-r <Raum>

APs mit der entsprechenden Raumangabe.

-d <Gerätename>

APs mit den entsprechenden Gerätenamen.

-a <Antennen>

APs mit der entsprechenden Anzahl an Antennen.

Eine Kombination aus den Optionen `-d` und `-a` ist nicht sinnvoll.

-v <Firmware>

APs, die genau diese Firmwareversion besitzen.

-x <Firmware>

APs, deren Firmwareversion niedriger als die angegebene Version ist.

-y <Firmware>

APs, deren Firmwareversion niedriger oder gleich der angegebenen Version ist.

-z <Firmware>

APs, der Firmwareversion höher als die angegebene Version ist.

-t <Firmware>

APs, deren Firmwareversion höher oder gleich der angegebenen Version ist.

Kombinationen sind möglich, um z. B. APs mit einer Firmwareversion zwischen zwei Versionsständen zu adressieren.

-n <Intranet-Adresse>

APs, die sich im Intranet mit der angegebenen Adresse befinden.

-p <Profilname>

APs, die sich im angegebenen WLAN-Profil befinden.

1.11 Client Steering über den WLC

Das Client Steering ermöglicht den APs, die im Sendebereich befindlichen WLAN-Clients anhand bestimmter Kriterien zu veranlassen, sich immer mit dem für sie idealen AP zu verbinden. Die Kriterien sind zentral im WLC definiert. Die verwalteten APs melden ständig die aktuellen Werte an den WLC, der aufgrund der Kriterien entscheidet, welche APs die Anfragen von WLAN-Clients beantworten dürfen. Deshalb ist das Client Steering auch nur mit APs möglich, die ein WLC zentral verwaltet.

In gemanagten Netzen zentralisiert ein WLC das Client Steering aller angeschlossenen APs. Das Client Steering läuft in diesem Fall wie folgt ab:

1. Der WLC sammelt die Daten über die angemeldeten WLAN-Clients von den angeschlossenen APs. Aus diesen Daten erstellt der WLC die Bewertung für das Client Steering.
2. Alle APs sind so konfiguriert, dass das Client Steering über den WLC erfolgt.
3. Ein hinzukommender WLAN-Client sendet einen Probe-Request an die APs in seiner Reichweite.
4. Die APs übermitteln diese Anfrage zusammen mit der Signalstärke des WLAN-Clients via CAPWAP an den WLC.
5. Der WLC berechnet für jeden AP im Bereich des WLAN-Clients einen Wert, der sich aus drei Bestandteilen zusammensetzt:
   - Signalstärke-Wert
   - Wert aus der Anzahl der am AP angemeldeten Clients
   - Frequenzband-Wert

   Zusammen mit der jeweiligen Gewichtung, mit der der WLC jeden einzelnen Wert multipliziert, ergibt sich der endgültige Wert.
6. Der WLC sendet den APs mit dem höchsten oder einem maximal um ein Toleranz-Level davon abweichenden Wert die Nachricht, dass dieser den WLAN-Client beim nächsten Anmeldeversuch annehmen darf.
7. Versucht der WLAN-Client, sich noch vor der Antwort des WLC mit einem AP zu verbinden, weist ihn dieser zurück, solange die Antwort vom WLC aussteht.
8. Versucht ein WLAN-Client nicht, sich trotz einer bestehenden Verbindung mit niedriger Qualität an einem anderen AP mit höherer Verbindungsqualität zu verbinden ("Sticky Client"), kann der WLC den aktuellen AP dazu veranlassen, den WLAN-Client abzumelden. Der WLAN-Client ist daraufhin gezwungen, sich mit dem AP zu verbinden, der die bessere Verbindung anbietet.

Wenn ein AP die Verbindung zu dem WLC verliert, der für das Client Steering verantwortlich ist, lässt der AP alle Verbindungen von berechtigten WLAN-Clients zu.

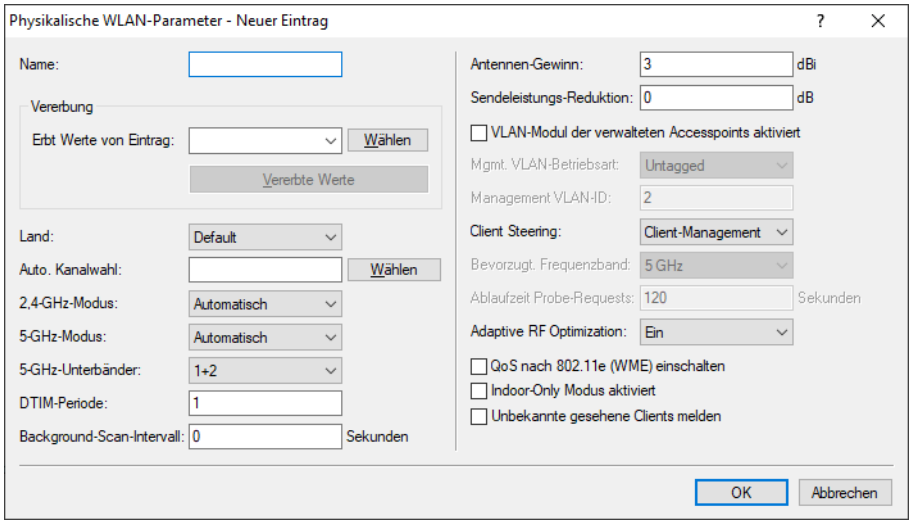
Für die optimale Funktionsweise des gemanagten Client-Steerings muss auf sämtlichen APs LCOS 9.00 oder höher installiert sein. Wenn Sie im Mischbetrieb APs mit einer älteren LCOS-Version einsetzen, kann in Ihrem WLAN keine sinnvolle Verteilung der Clients erfolgen.

In Szenarien mit zeitkritischem Roaming, z. B. bei VoIP-Telefonen, sollten Sie Client Steering nicht einsetzen, da Client Steering den Einbuchvorgang eines Clients verzögern kann.

1.11.1 Konfiguration

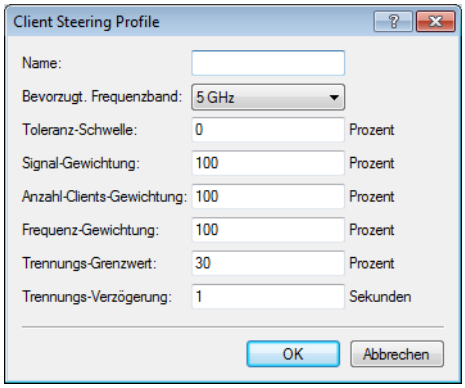
Mit LANconfig konfigurieren Sie das Client Steering wie folgt:

1. Aktivieren Sie zunächst im WLC das Client Steering für einen AP unter **WLAN-Controller** > **Profile** > **Physikalische WLAN-Parameter** über die Auswahlliste **Client Steering**.
   - **Aus**: Das Client Steering ist deaktiviert.
   - **AP-basiertes Band Steering**: Der AP leitet den WLAN-Client eigenständig auf ein bevorzugtes Frequenzband.
   - **Ein**: Der AP lässt das Client Steering vom WLC durchführen.



2. Im Menü **WLAN-Controller** > **AP-Konfiguration** > **Client Steering Profile** sind bereits zwei Standard-Profile vorkonfiguriert (High-Density, Default), die für die meisten Anwendungsfälle genügen. Optional erstellen Sie dort mit einem Klick auf **Hinzufügen** ein neues Client Steering-Profil.

   Client Steering-Profile legen die Bedingungen fest, nach denen der WLC entscheidet, welche APs beim nächsten Anmeldeversuch einen Client annehmen.



   Die Einträge haben folgende Bedeutung:

Name

Bezeichnung des Client Steering-Profils.

Bevorzugt. Frequenzband

Gibt das Frequenzband vor, auf welches der WLC den WLAN-Client leitet.

- **2,4GHz**: Der WLC leitet den WLAN-Client auf das 2,4 GHz Frequenzband.
- **5GHz**: Der WLC leitet den WLAN-Client auf das 5 GHz Frequenzband.

Toleranz-Schwelle

Um diesen Prozentwert darf der errechnete Wert für einen AP vom maximal errechneten Wert abweichen, so dass der AP die Erlaubnis erhält, den Client beim nächsten Anmeldeversuch anzunehmen.

Signal-Gewichtung

Gibt an, mit wie viel Prozent der Signalstärke-Wert in den endgültigen Wert eingeht.

Anzahl-Clients-Gewichtung

Gibt an, mit wie viel Prozent der Wert für die Anzahl angemeldeter Clients bei einem AP in den endgültigen Wert eingeht.

Frequenzband-Gewichtung

Gibt an, mit wie viel Prozent der Wert für das Frequenzband in den endgültigen Wert eingeht.

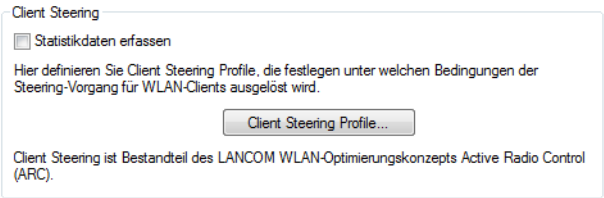
Trennungs-Grenzwert

Gibt den Prozentwert vom maximal gesehenen Signalstärkewert an, unter den der aktuelle Wert sinken muss, bevor der AP die Verbindung zum Client trennt.

Trennungs-Verzögerung

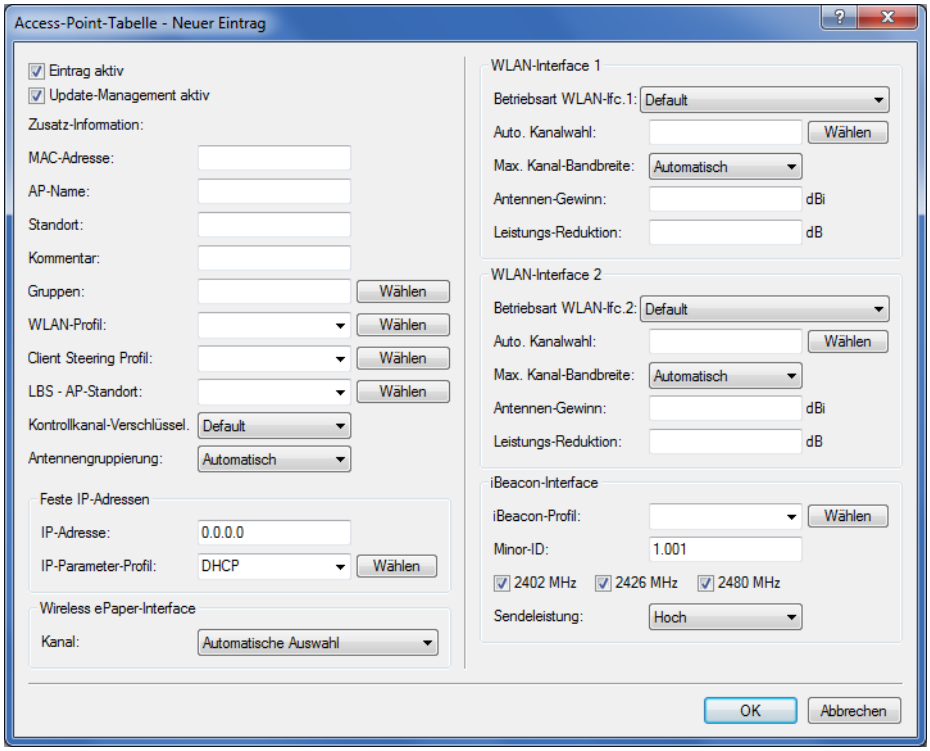
Gibt die Anzahl der Sekunden an, in denen keine Datenübertragung zwischen AP und Client stattfinden darf, bevor der AP den Client trennt.

3. Optional: Aktivieren Sie über den Parameter **Statistikdaten erfassen** die Aufzeichnung von Client Steering-Statistiken. Die Statistikdaten lassen sich anschließend z. B. mittels LANmonitor auswerten.

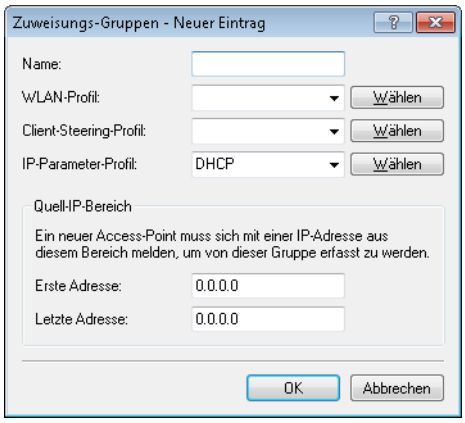


Die Statistikaufzeichnung erhöht die Last auf dem WLC. LANCOM empfiehlt daher, die Statistikaufzeichnung nicht dauerhaft zu aktivieren.

4. Weisen Sie jetzt unter **WLAN-Controller** > **AP-Konfiguration** > **Access-Point-Tabelle** dem entsprechenden AP eines der Client Steering-Profile zu.



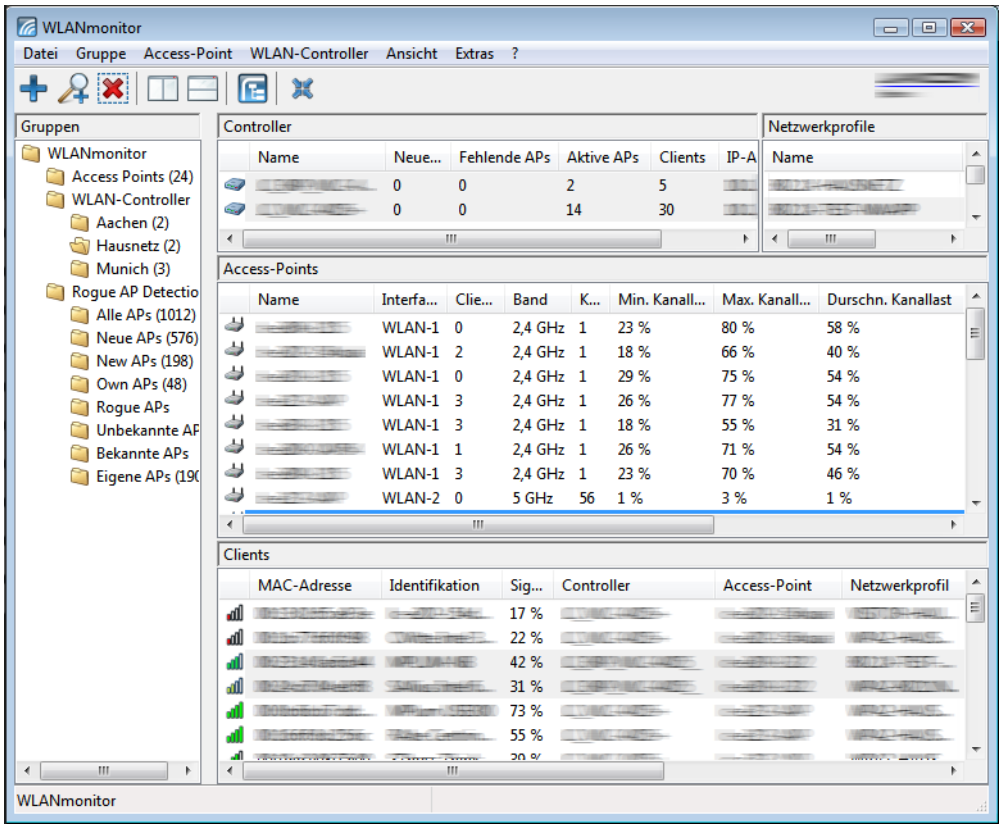
5. Optional: Ordnen Sie ggf. definierten Zuweisungs-Gruppen ein entsprechendes Client Steering-Profil zu.



Damit haben Sie die Konfiguration des Client-Steerings abgeschlossen.

1.12 Kanallastanzeige im WLC-Betrieb

Für die von einem WLC verwalteten APs wird die Last auf den verwendeten Kanälen in drei Werten als minimale, maximale und durchschnittliche Kanallast angezeigt. Die angezeigten Werte werden in einem Messintervall von drei Minuten ermittelt. Die ersten Werte werden demnach auch erst nach drei Minuten angezeigt.



1.13 Sicherung der Zertifikate

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

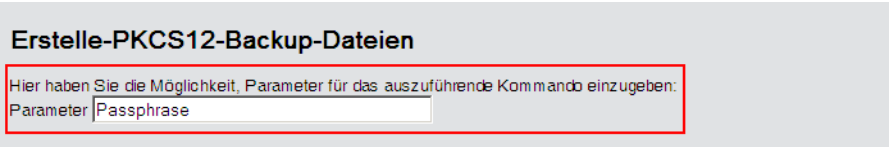
Wenn mehrere WLCs in der gleichen WLAN-Infrastruktur parallel eingesetzt werden (Load-Balancing) oder wenn ein Gerät ersetzt bzw. neu konfiguriert werden muss, sollten immer die gleichen Root-Zertifikate verwendet werden, um einen reibungslosen Betrieb der verwalteten APs zu gewährleisten.

1.13.1 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 WLC erzeugt werden. Außerdem sollten folgende noch weitere Dateien mit Informationen über die ausgestellten Geräte-Zertifikate gesichert werden. Damit diese vertraulichen Daten auch beim Export aus dem Gerät heraus geschützt bleiben, werden sie zunächst in einen PCKS12-Container gespeichert, der mit einer Passphrase geschützt ist.

WEBconfig

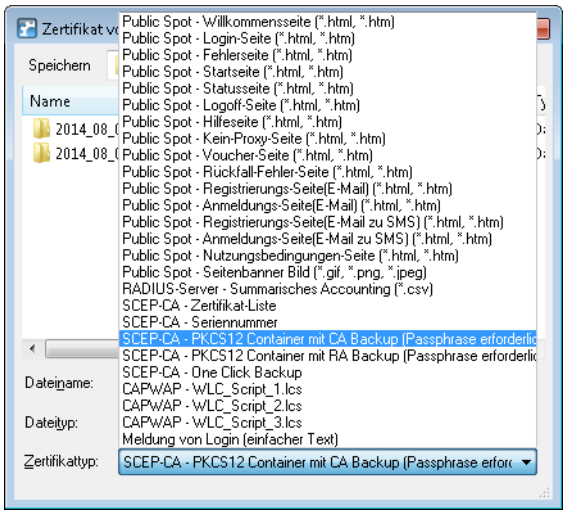
1. Öffnen Sie die Konfiguration des WLCs mit WEBconfig im Bereich **Extras** > **LCOS-Menübaum** > **Setup** > **Zertifikate** > **SCEP-CA** > **CA-Zertifikate**.
2. Wählen Sie den Befehl **Erstelle-PKCS12-Backup-Dateien** und geben Sie als Parameter die Passphrase für die PKCS12-Container an.



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

LANconfig

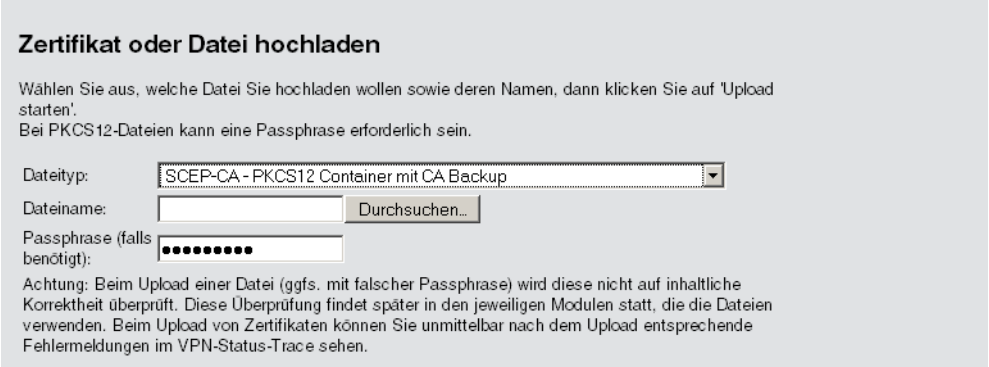
1. Markieren Sie den entsprechenden WLC in der Geräteübersicht und wählen Sie im Menü **Gerät** > **Konfigurations-Verwaltung** den Punkt **Zertifikat als Datei sichern.**.
2. Wählen Sie in der Liste **Zertifikattyp** den gewünschten PKCS12-Container aus und klicken Sie auf **Speichern**.



1.13.2 Zertifikats-Backup in das Gerät einspielen

1. Wählen Sie **Extras** > **Dateimanagement** > **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**:



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. Löschen Sie nach dem Zurückspielen des Backups alle Dateien, die mit `controller_` oder `eaptls_` beginnen.
6. Danach muss im Verzeichnis **Setup** > **Certificates** > **SCEP-Client** der Befehl `Reinit` aufgerufen werden:

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

1.13.3 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 APs wichtig.

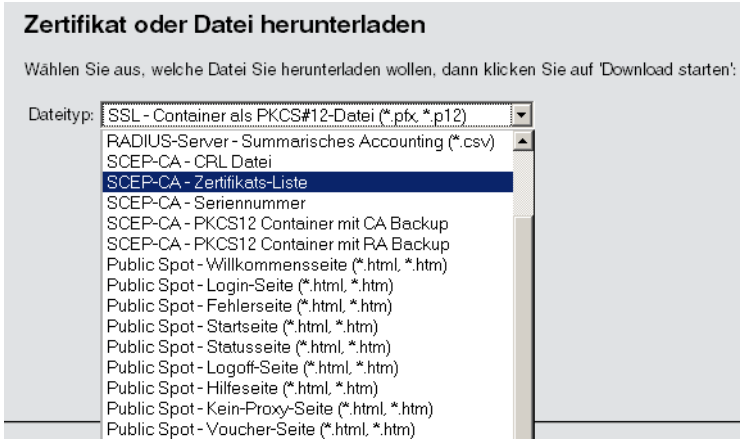
Wenn nur die Root-Zertifikate gesichert werden, können die ausgestellten Geräte-Zertifikate nicht mehr zurückgerufen werden!

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

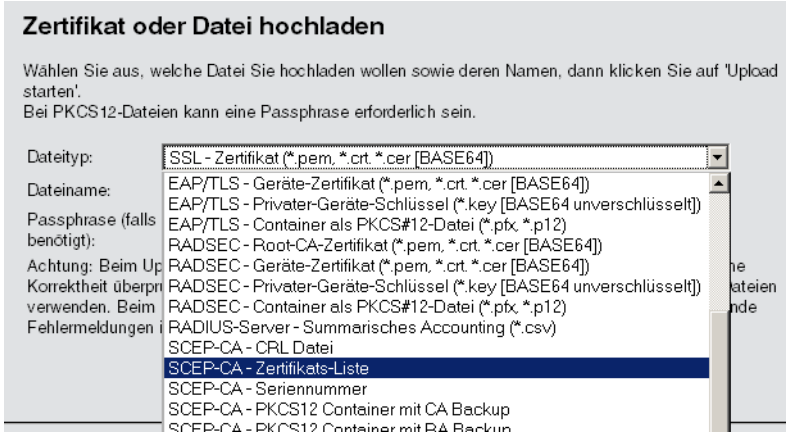
- SCEP-Zertifikatsliste: Liste aller von der SCEP-CA jemals ausgestellten Zertifikate.
- SCEP-Seriennummern: Enthält die Seriennummer für das nächste Zertifikat.

1. Wählen Sie **Extras** > **Dateimanagement** > **Zertifikat oder Datei herunterladen**.

2. Wählen Sie dann als Dateityp nacheinander die oben aufgeführten Einträge und bestätigen Sie mit **Download starten**.



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**.



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.

1.13.4 One Click Backup der SCEP-CA

Um das Backup der im WLC vorliegenden CA zu vereinfachen, bietet Ihnen das Gerät die Möglichkeit, mit einer einzigen Aktion einen kompletten Zertifikats-Datensatz zu erzeugen (One Click Backup). Dieser Datensatz erlaubt Ihnen die vollständige Sicherung und Wiederherstellung der CA und vermeidet das Auftreten von Zertifikats-Konflikten.

Derartige Konflikte können dann auftreten, wenn Sie die einzelnen PKCS12-Container separat vom Gerät heruntergeladen haben und anschließend wieder einspielen: Hat der WLC in der Zwischenzeit eine neue CA aufgesetzt und neue Zertifikate ausgestellt, führen die abweichenden CAs temporär zu Authentisierungsproblemen bei den verschiedenen Diensten im LCOS. Sofern nicht gewartet werden kann, bis die einzelnen Dienste neue Zertifikate anfordern, erfordert die manuelle Konfliktlösung ein Löschen der SCEP-Dateien aus dem LCOS-Dateisystem und eine Reinitialisierung des SCEP-Clienten. Mit dem Zurückspielen eines One Click Backups dagegen führt das LCOS die notwendigen Schritte automatisch aus.

Erstellen einer Backup-Datei

Um einen Zertifikats-Datensatz zu erzeugen, führen Sie die Aktion **Erstelle-PKCS12-Backup-Dateien** unter **Setup** > **Zertifikate** > **SCEP-CA** > **CA-Zertifikate** aus. Diese Aktion erzeugt eine Zip-Datei innerhalb des LCOS-Dateisystems, die alle notwendigen Dateien enthält. Zum Schutz der enthaltenen Zertifikate und Schlüssel ist die Zip-Datei automatisch mit dem Gerätepasswort geschützt, sofern Sie kein gesondertes Passwort angeben. Die erzeugte Zip-Datei lässt sich anschließend z. B. im WEBconfig über **Extras** > **Dateimanagement** > **Zertifikat oder Datei herunterladen** > **SCEP-CA – One Click Backup** herunterladen.

Zurückspielen der Backup-Datei

Um einen Zertifikats-Datensatz zurückzuspielen, laden Sie die gesicherte Zip-Datei unter Angabe der Passphrase direkt in das Gerät. Im WEBconfig z. B. erfolgt dies über die Auswahl **Extras** > **Dateimanagement** > **Zertifikat oder Datei hochladen** > **SCEP-CA – One Click Backup**. Setzen Sie dabei die Option **Vorhandene CA Zertifikate ersetzen**, damit das Gerät den Zertifikats-Datensatz nach dem Hochladen automatisch zurückspielt.

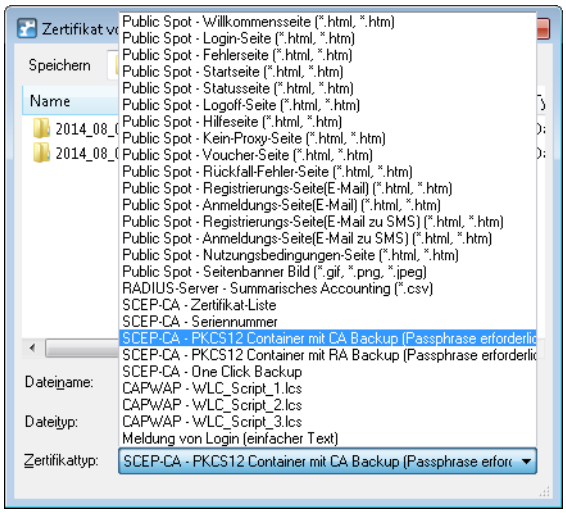
Sofern Sie die Option nicht setzen oder die Backup-Datei auf andere Weise ins Gerät laden, müssen Sie nach dem Hochladen die Aktion *2.39.2.2.11 Zertifikate-aus-Backup-wiederherstellen* ausführen, damit das Gerät den Zertifikats-Datensatz zurückspielt.

1.13.5 Backup und Einspielen der Zertifikate über LANconfig

Um die Zertifikate über LANconfig zu speichern und hochzuladen, gehen Sie wie folgt vor:

Speichern

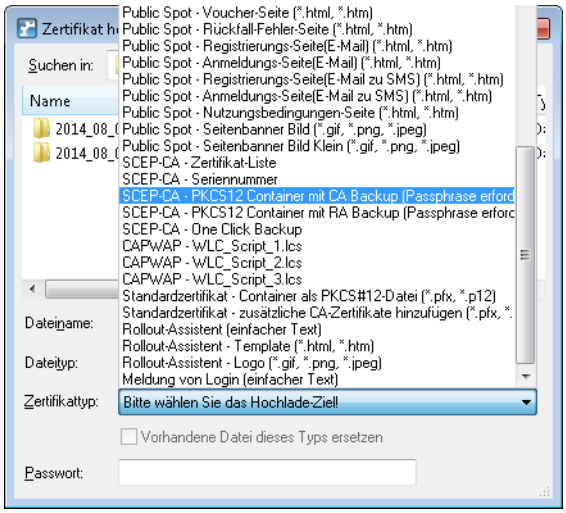
1. Markieren Sie den entsprechenden WLC in der Geräteübersicht und wählen Sie im Menü **Gerät** > **Konfigurations-Verwaltung** den Punkt **Zertifikat als Datei sichern**.
2. Wählen Sie in der Liste **Zertifikattyp** den gewünschten PKCS12-Container-Typ aus und klicken Sie auf **Speichern**.



Hochladen

1. Markieren Sie den entsprechenden WLC in der Geräteübersicht und wählen Sie im Menü **Gerät** > **Konfigurations-Verwaltung** den Punkt **Zertifikat oder Datei hochladen**.
2. Wählen Sie in der Liste **Zertifikattyp** den gewünschten PKCS12-Container-Typ aus.

3. Navigieren Sie anschließend zur gewünschten Datei, geben Sie ggf. ein Passwort an und klicken Sie auf **Öffnen**.



One Click Backup

Für das One Click Backup wählen Sie aus der Dialogliste jeweils den Eintrag "SCEP-CA – One Click Backup" aus.

1.14 Backuplösungen

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

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

1.14.1 WLC-Cluster

Sofern Sie in Ihrem Netz mehrere WLCs einsetzen, haben Sie die Möglichkeit, diese Geräte zu einem geschlossenen Verbund (Cluster) zusammenfassen. Die APs eines gemanagten WLANs werden dann nicht mehr von einem einzigen, zentralen WLC verwaltetet, sondern von mehreren miteinander synchronisierten WLCs. Ein solcher WLC-Cluster bietet Ihnen vor allem in größeren Netzen diverse Vorteile:

- Automatische Verteilung der Netzlast zwischen den einzelnen APs und WLCs („Load-Balancing“).
- Erhöhte Ausfallsicherheit durch die Bereitstellung von Backup-WLCs („Hot Standby“) und automatische Neuverteilung der APs im Falle eines WLC-Ausfalls.
- Aufbau einer Zertifikatshierarchie: Verwaltung der Zertifikate durch eine zentrale Zertifizierungsstelle (CA), dargestellt wahlweise durch einen Master-WLC oder eine externe Stelle (z. B. einen Server).

Ab LCOS 9.00 hat die Cluster-Funktion die im Folgenden näher beschriebenen Verbesserungen erhalten.

CAPWAP im WLC gezielt (de)aktivieren

Um mehrere WLCs in einem Verbund (Cluster) zu betreiben, müssen alle beteiligten Geräte eine identische Konfiguration aufweisen. Dies ist auf einem WLC standardmäßig jedoch nicht der Fall, da dieser bestimmte Konfigurationsbestandteile

(wie Zertifikate) automatisch generiert. Durch Deaktivieren von CAPWAP auf allen Geräten bis auf einem haben Sie die Möglichkeit, in Ihrem WLC-Cluster einen Master-Controller zu definieren, dessen Konfiguration sich anschließend auf die übrigen WLCs spiegeln lässt.

Mehr zum Spiegeln einer Konfiguration erfahren Sie im Abschnitt *Config-Sync*.

WLC-Tunnel für die interne Kommunikation

Der Einsatz von WLC-Tunneln ist ein essentieller Bestandteil eines WLC-Clusters. Die am WLC-Cluster beteiligten WLCs nutzen diese Tunnel zur Kommunikation untereinander, um die verteilten Statusinformationen im Verbund abzugleichen. Im Rahmen der Funktionserweiterungen ab LCOS 9.00 verbessert sich daher auch der LCOS-interne Umgang mit WLC-Tunneln:

- WLCs sind dazu in der Lage, sich untereinander automatisch zu finden.
- Sie haben die Möglichkeit, WLC-Tunnel statisch zu konfigurieren.
- WLCs trennen einen WLC-Tunnel erst nach Ablauf eines Timeouts.
- WLC-Tunnel lassen sich global ein- oder ausschalten.

Die Einstellungen für die WLC-Tunnel und die weiteren WLCs (Remote-WLCs) nehmen Sie in LANconfig im Abschnitt **WLAN-Controller** > **Allgemein** > **WLC-Cluster** vor. Über die Einstellung **WLC-Tunnel aktiv** deaktivieren Sie den Einsatz von WLC-Tunneln, was de facto ein Abschalten der Clustering-Funktion bewirkt.

Ermittlung des idealen WLC

Die im LCOS implementierten Algorithmen ermöglichen die intelligente Verteilung von APs auf einzelne WLCs. Dies erlaubt den APs, innerhalb von WLC-Clustern die Netzlast gleichmäßig auf alle WLCs aufzuteilen oder nach Ausfall eines WLCs ein alternatives Gerät zu wählen. Hierzu sendet ein AP zunächst einen Discovery Request ins Netz, um sämtliche verfügbaren WLCs zu ermitteln. Die WLCs antworten ihrerseits mit einem Discovery Response, anhand dessen ein AP eine Liste von WLCs erstellt. Diese Liste priorisiert ein der AP anhand verschiedener Kritieren.

Ein AP arbeitet dabei die einzelnen Kriterien sequentiell ab: Sofern nach der Anwendung eines Kriteriums mehrere WLCs für den idealen WLC in Frage kommen, zieht der AP das nächste Kriterium zur Priorisierung heran. Dieser Prozess endet, wenn im Rahmen der nachfolgend beschriebenen Priorisierung schließlich ein WLC als idealer WLC verbleibt.

Kriterien zur Priorisierung

- **Spezifität der AP-Konfiguration**: Ein AP wertet aus, ob ein WLC für den AP eine Konfiguration bereithält und ob diese ein spezifisches AP-Profil oder ein Default-Profil umfasst. Ein spezifisches AP-Profil priorisiert der AP am höchsten, gefolgt von einem Default-Profil. Ein fehlendes Profil erhält die niedrigste Priorität.
- **Höhe des Präferenzwerts**: Der AP wertet aus, welchen Präferenzwert Sie einem WLC zugewiesen haben. Je höher die betreffende Zahl zwischen 0 und 255 liegt, desto höher priorisiert der AP den WLC.

Sofern immer noch mehrere WLCs für die Rolle des idealen WLCs in Frage kommen, hängt der weitere Priorisierungsprozess vom Verbindungsstatus und der Art des Auswahlprozesses (automatisch vs. manuell initiiert) ab:

- Bei der **erstmaligen Ermittlung** bildet ein AP für jeden verbliebenen WLC einen gewichteten Wert aus der Zahl der verbundenen sowie der maximal möglichen APs (**Lizenzauslastung**). Als idealen WLC wählt ein AP schließlich den WLC mit der geringsten Lizenzauslastung.

  ⓘ Hat ein WLC die maximal mögliche Anzahl von AP-Verbindungen erreicht (Lizenzkontingent erschöpft), berücksichtigt ein AP den betreffenden WLC nicht mehr für den aktuellen Auswahlprozess.
- Bei der **automatischen Überprüfung** der idealen AP-Verteilung verbleibt ein AP bei dem mit ihm verbundenen WLC, sofern sich dieser WLC in der Liste der verbliebenen WLCs befindet. Andernfalls sorgt ein **zufallsgesteuerter Algorithmus** dafür, dass der AP einen beliebigen AP auswählt.
- Bei der **manuell ausgelösten Überprüfung** der idealen AP-Verteilung sorgt ein **zufallsgesteuerter Algorithmus** dafür, dass die einzelnen APs die im Netz verfügbaren Lizenzkontingente möglichst gleichmäßig ausnutzen.

Ermittlung der idealen AP-Verteilung

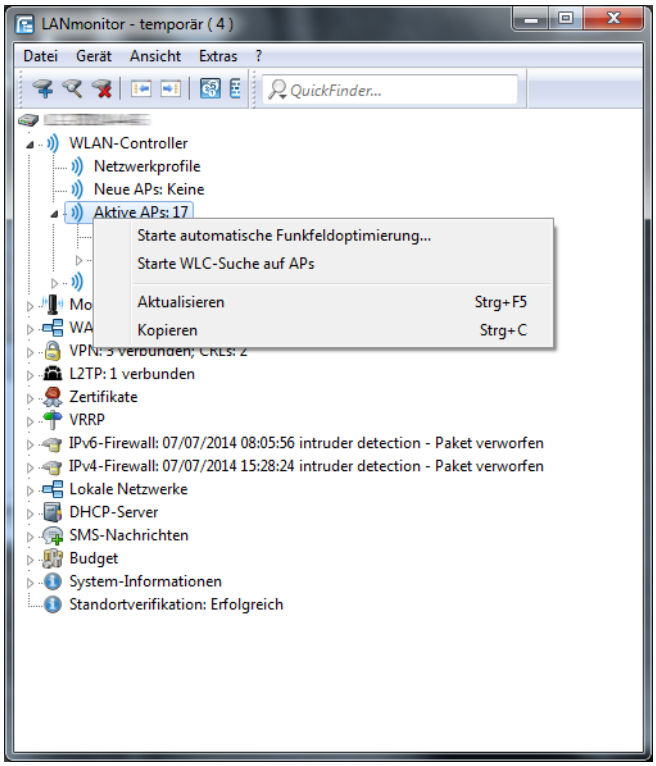
Die Ermittlung der idealen AP-Verteilung in einem WLC-Cluster und eine dadurch ggf. ausgelöste Umverteilung erfolgt grundsätzlich automatisch. Dazu durchläuft ein jeder AP in unregelmäßigen Abständen von 30 bis 60 Minuten den Prozess zur *Ermittlung des idealen WLC*. Gewinnt bei diesem Vorgang der WLC, zu dem bereits eine Verbindung besteht, erfolgt keine Umverteilung. Weist jedoch ein anderer WLC eine höhere Priorisierung auf, so versucht der AP, sich mit diesem WLC zu verbinden.

Sie haben aber auch als Administrator die Möglichkeit, via LANmonitor die Ermittlung der idealen AP-Verteilung und eine ggf. daraus resultierende Umverteilung der APs manuell auszulösen (siehe *Ideale AP-Verteilung manuell initiieren* auf Seite 120).

Ideale AP-Verteilung manuell initiieren

Die nachfolgenden Schritte zeigen Ihnen, wie Sie die Berechnung der idealen Verteilung manuell starten und dadurch ggf. eine Neuverteilung auslösen.

1. Starten Sie LANmonitor und wählen Sie einen WLC aus.
2. Wechseln Sie in den Menüzweig **Wireless LAN** > **Aktive APs**.
3. Öffnen Sie das Kontextmenü auf einem beliebigen AP und wählen Sie **Starte WLC-Suche auf APs**.



Die betreffenden Access Points bestimmen den für sie optimalen WLC und verteilen sich entsprechend der Vorgaben über den WLC-Verbund.

Einrichten einer CA-Hierarchie

Um mehrere WLC im Verbund zu betreiben (WLC-Cluster), müssen alle beteiligten Geräte eine identische Konfiguration aufweisen. Dies umfasst auch die innerhalb des WLC-Clusters eingesetzten Zertifikate. Die Lösung liegt in dem Aufbau einer Zertifikats- bzw. CA-Hierarchie: Hierbei definieren Sie die CA eines WLC als Root-CA, von welcher die übrigen WLCs das Zertifikat für ihre (Sub-)CA beziehen.

Das nachfolgende Szenario zeigt Ihnen, welche Konfigurationsschritte für den Aufbau einer CA-Hierarchie notwendig sind. Die Konfiguration erfolgt exemplarisch anhand zweier WLCs:

- WLC-MAIN stellt das Gerät mit der Root-CA dar;
- WLC-SUB stellt das Gerät dar, welches bei der Root-CA ein Zertifikat bezieht, um als Sub-CA weitere Zertifikate ausstellen zu können.

Konfiguration der Root-CA

Der nachfolgende Abschnitt beschreibt die Einrichtung einer Root-CA auf einem WLC. Die einzelnen Handlungsschritte gehen von einem zurückgesetzten Gerät aus, bei dem Sie die Standard-Inbetriebnahme durchgeführt und die korrekte Uhrzeit gesetzt haben.

1. Melden Sie sich via WEBconfig oder über die Konsole am Gerät an.
2. Wechseln Sie in das Menü **Setup** > **Zertifikate** > **SCEP-CA** > **CA-Zertifikate**. Passen Sie hier die Namen für die Certificate Authority (CA) und die Registration Authority (RA) über die Parameter **CA-Distinguished-Name** und **RA-Distinguished-Name** an.

   Beispiel: `/CN=WLC-MAIN CA/O=LANCOM SYSTEMS/C=DE`

3. Wechsel Sie in das Menü **Setup** > **Zertifikate** > **SCEP-CA** und setzten Sie den Parameter **Aktiv** auf **Ja**.

Damit haben Sie die Konfiguration der Root-CA abgeschlossen. Mit dem Befehl `show ca cert` an der Kommendozeile lässt sich überprüfen, ob der WLC das Zertifikat korrekt erstellt hat.

Konfiguration der Sub-CA

Der nachfolgende Abschnitt beschreibt die Einrichtung einer Sub-CA auf einem WLC. Die einzelnen Handlungsschritte gehen von einem zurückgesetzten Gerät aus, bei dem Sie die Standard-Inbetriebnahme durchgeführt und die korrekte Uhrzeit gesetzt haben.

1. Melden Sie sich via WEBconfig oder über die Konsole am Gerät an.
2. Wechseln Sie in das Menü **Setup** > **Zertifikate** > **SCEP-CA** und setzten Sie den Parameter **Root-CA** auf **Nein**.
3. Wechseln Sie in das Menü **Setup** > **Zertifikate** > **SCEP-CA** > **CA-Zertifikate**. Passen Sie hier die Namen für die Certificate Authority (CA) und die Registration Authority (RA) über die Parameter **CA-Distinguished-Name** und **RA-Distinguished-Name** an.

   Beispiel: `/CN=WLC-SUB CA/O=LANCOM SYSTEMS/C=DE`

4. Wechseln Sie in das Menü **Setup** > **Zertifikate** > **SCEP-CA** > **Sub-CA** und tragen Sie für den Parameter **CADN** den Distinguished Name der Root-CA ein.

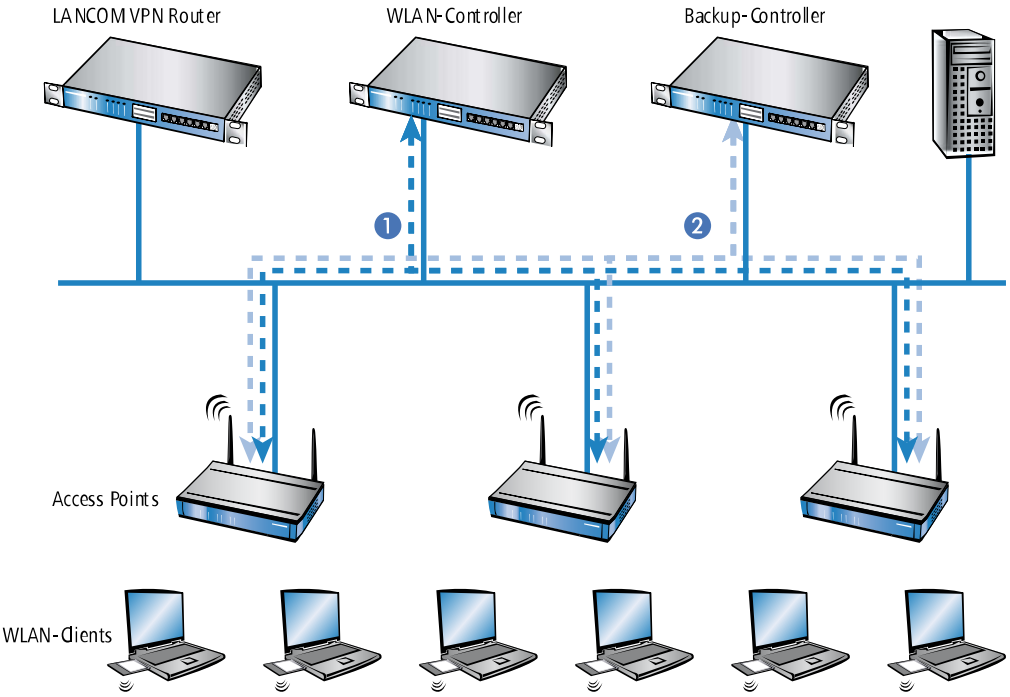
   Beispiel: `/CN=WLC-MAIN CA/O=LANCOM SYSTEMS/C=DE`

5. Tragen Sie für den Parameter **Challenge-Pwd** das Challenge-Passwort ein, das auf WLC-MAIN unter **Setup** > **Zertifikate** > **SCEP-CA** hinterlegt ist.
6. Hinterlegen im Parameter **CA-Url-Adresse** die URL (Adresse) zur Root-CA.
   Stellt ein anderer WLC mit LCOS-Betriebssystem die Root-CA zur Verfügung, müssen Sie lediglich die IP-Adresse im Default-Wert durch jene Adresse austauschen, unter der das entsprechende Gerät zu erreichen ist. Beispiel: `http://192.168.1.1/cgi-bin/pkiclient.exe`.
7. Optional: Spezifizieren Sie die **Ext-Key-Usage** und **Cert-Key-Usage**, um die Funktionen der Sub-CA einzuschränken. Weitere Informationen hierzu finden Sie in der Menüreferenz.
8. Setzten Sie den Parameter **Auto-generiert-Request** auf **ja**, um die Sub-CA zu aktivieren..
9. Wechseln Sie in das Menü **Setup** > **Zertifikate** > **SCEP-CA** und setzten Sie den Parameter **Aktiv** auf **ja**, um den CA-Server mit SCEP zu aktivieren.

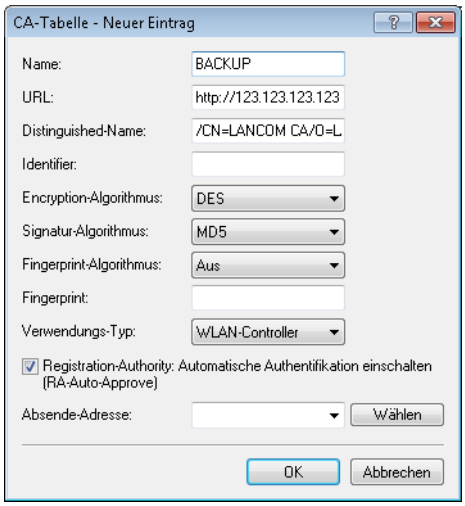
Damit haben Sie die Konfiguration der Sub-CA abgeschlossen. Mit dem Befehl `show ca cert` an der Kommendozeile lässt sich überprüfen, ob der WLC das Zertifikat korrekt erstellt hat. Die Hierarchie der Zertifikate muss hierbei sichtbar sein: Als erstes zeigt der WLC das Zertifikat der Root-CA an, dann das Zertifikat der Sub-CA.

1.14.2 Backup mit redundanten WLAN-Controllern

Diese Form des Backups bietet sich an, wenn Sie einen WLC durch einen zweiten WLC absichern und dabei jederzeit die volle Kontrolle über alle gemanagten APs behalten möchten. Der Backup-WLC wird dabei so konfiguriert, dass er die benötigten Zertifikate über SCEP vom abgesicherten Haupt-WLC bezieht.



1. Stellen Sie auf beiden WLCs **1** und **2** die gleiche Uhrzeit ein.
2. Schalten Sie die CA auf dem Backup-WLC aus (WEBconfig: LCOS-Menübaum > Setup > Zertifikate > SCEP-CA > Aktiv).
3. Erstellen Sie in der Konfiguration des SCEP-Clients im Backup-WLC einen neuen Eintrag in der CA-Tabelle (in LANconfig unter **Zertifikate** > **SCEP-Client** > **CA-Tabelle**). Darin wird die CA des Haupt-WLC eingetragen.

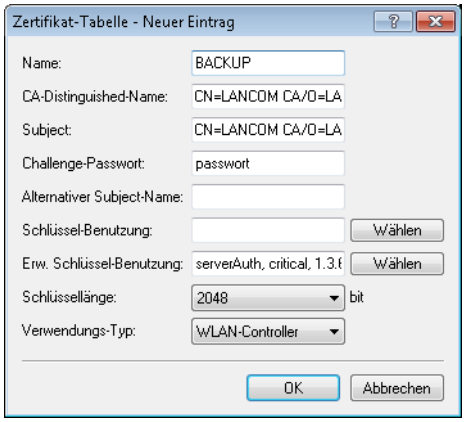


4. Geben Sie als URL die IP-Adresse oder den DNS-Namen des Haupt-WLCs ein gefolgt vom Pfad zur CA `/cgi-bin/pkiclient.exe`, also z. B. `10.1.1.99/cgi-bin/pkiclient.exe`.

   › **Distinguished-Name**: Standardname der CA (/CN=LANCOM CA/O=LANCOM SYSTEMS/C=DE) bzw. der Name der auf dem primären Controller vergeben wurde

- **RA-Auto-Approve** einschalten
- **Verwendungs-Typ**: WLAN-Controller

5. Erstellen Sie dann einen neuen Eintrag in der Zertifikats-Tabelle mit folgenden Angaben:



- **CA-Distinguished-Name**: Der Standardname, der bei der CA eingetragen wurde, also z. B. /CN=LANCOM CA/O=LANCOM SYSTEMS/C=DE
- **Subject**: Angabe der MAC-Adresse des Haupt-WLAN-Controllers in der Form: /CN=00:a0:57:01:23:45/O=LANCOM SYSTEMS/C=DE
- **Challenge**: Das allgemeine Challenge-Passwort der CA auf dem primären WLAN-Controller oder ein extra für den Controller manuell vergebenes Passwort.
- **Erweiterte Schlüsselbenutzung**: critical,serverAuth,1.3.6.1.5.5.7.3.18
- **Schlüssellänge**: 2048 Bit
- **Verwendungs-Typ**: WLAN-Controller

6. Wenn im Backup-Controller zuvor schon eine SCEP-Konfiguration aktiv war, müssen folgende Aktionen unter WEBconfig ausgeführt werden (**Experten-Konfguration** > **Setup** > **Zertifikate** > **SCEP-Client**):
   - Bereinige-SCEP-Dateisystem
   - Aktualisieren (2x: beim ersten Mal holt sich der SCEP-Client nur die neuen CA/RA Zertifikate, beim zweiten Mal wird das Gerätezertifikat aktualisiert)

7. Konfigurieren Sie den ersten WLC **1** wie gewünscht mit allen Profilen und der zugehörigen AP-Tabelle. Die APs bauen dann die Verbindung zum ersten WLC auf. Die APs erhalten von diesem WLC ein gültiges Zertifikat und eine Konfiguration für die WLAN-Module.
8. Übertragen Sie die Konfiguration des ersten WLCs **1** z. B. mit LANconfig auf den Backup-Controller **2**. Dabei werden auch die Profile und die AP-Tabellen mit den MAC-Adressen der APs auf den Backup-WLC übertragen. Alle APs bleiben in diesem Zustand weiterhin beim ersten WLC angemeldet. Ist die Übertragung der Konfiguration erfolgt, ist es erforderlich, dass Sie dem Backup-Controller eine neue IP-Adresse zuweisen.

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

Die APs bleiben in diesem Szenario so lange in der Verwaltung des Backup-WLCs, bis dieser entweder selbst einmal nicht erreichbar ist oder bis sie manuell getrennt werden.

Mit der Einstellung des autarken Weiterbetriebs können die APs auch während der Suche nach einem Backup-WLC mit der aktuellen WLAN-Konfiguration in Betrieb bleiben, und die WLAN-Clients bleiben eingebucht.

1.14.3 Backup mit primären und sekundären WLAN-Controllern

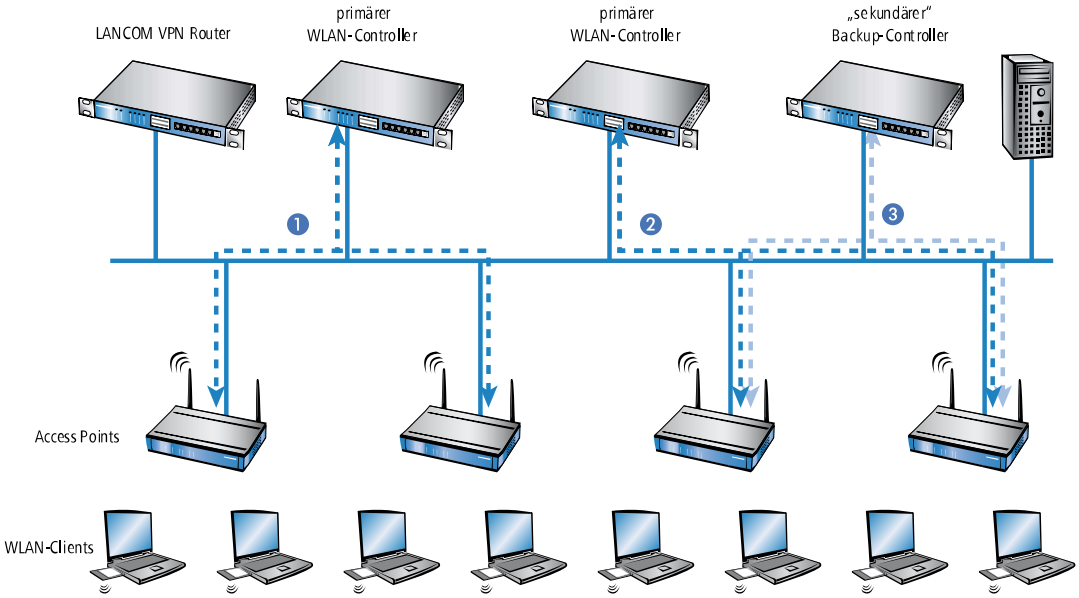
Mit einer zweiten Form des Backups können Sie für eine größere Anzahl von "primären" WLCs einen gemeinsamen, "sekundären" Backup-WLC bereitstellen. Beim Ausfall eines WLCs bleiben die APs zwar in Betrieb, arbeiten allerdings mit der aktuellen Konfiguration der WLAN-Module weiter. Der Backup-WLC kann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

1.14.4 Primäre und sekundäre Controller

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

- Der WLC kann das **Zertifikat** des APs authentifizieren und hat für die MAC-Adresse des suchenden APs eine **Konfiguration** gespeichert. Einen solchen WLC bezeichnet man als "primären" WLC.
- Ein WLC kann das **Zertifikat** des APs authentifizieren, hat aber für die MAC-Adresse des suchenden APs **keine Konfiguration** gespeichert und auch **keine Default-Konfiguration**. Einen solchen WLC bezeichnet man als "sekundären" WLC.

Beispiel einer Backup-Lösung mit drei WLCs für 50 gemanagte APs: Zwei der WLCs verwalten jeweils 25 APs, der dritte steht als Backup-WLC bereit:



Ein WLC kann nun in seiner AP-Tabelle die fünffache Anzahl der von ihm selbst maximal verwalteten APs aufnehmen. Für jeweils fünf WLCs (mit gleicher Ausstattung) reicht also ein zusätzlicher WLC aus, um eine vollständige Absicherung bei Ausfall eines Gerätes zu realisieren.

1. Stellen Sie auf allen WLCs **1** und **2** und **3** die gleiche Uhrzeit ein.
2. Übertragen Sie die CA- und RA-Zertifikate aus dem ersten primären WLC **1** in den zweiten, primären **2** und den sekundären "Backup-WLC" **3**.
3. Konfigurieren Sie den ersten WLC **1** wie gewünscht mit den Profilen und der zugehörigen AP-Tabelle für eine Hälfte der APs. Dieser WLC wird somit zum primären WLC für die bei ihm eingetragenen APs.

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

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

1. Konfigurieren Sie den zweiten WLC **2** für die andere Hälfte der APs, welche dann diesen WLC als primären WLC betrachten.
2. Der Backup-WLC **3** bleibt bis auf die Uhrzeit und die Root-Zertifikate ohne weitere Konfiguration.
3. Die APs suchen nach dem Start über eine Discovery-Message nach einem WLC. In diesem Fall antworten alle drei WLCs auf diese Nachricht – die APs wählen jeweils "ihren" primären WLC für die folgende DTLS-Verbindung. Die eine Hälfte der APs entscheidet sich für WLC **1**, die andere Hälfte für WLC **2**. Da WLC **3** für keinen der APs als primärer WLC fungiert, meldet sich kein AP bei ihm an.
4. Fällt z. B. der erste WLC **2** aus, suchen die APs automatisch nach einem anderen WLC. Sie finden die WLC **A** und **C**, wobei **A** schon mit seinen 25 APs vollständig ausgelastet ist. Backup-Controller **C** kann die Gültigkeit der Zertifikate prüfen, die APs also authentifizieren und als gemanagte APs annehmen. Da die APs jedoch **nicht** mit ihrer MAC-Adresse in der AP-Tabelle des Backup-WLCs eingetragen sind, kann der Backup-WLC die APs nicht weiter verwalten, sie werden nur mit der jeweiligen aktuellen WLAN-Konfiguration weiterbetrieben.

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

Mit der Einstellung des autarken Weiterbetriebs bleiben die APs auch während der Suche nach einem Backup-WLC mit der aktuellen WLAN-Konfiguration in Betrieb, die WLAN-Clients können weiterhin alle Funktionen nutzen.

1.14.5 Automatische Suche nach alternativen WLCs

Ab LCOS 9.00 versucht ein AP nicht mehr, sich bei einem Verbindungsabbruch mit dem zuletzt bekannten WLC neu zu verbinden. Stattdessen sucht der AP im Netz nach einem erreichbaren WLC, der den Kriterien für die *Ermittlung des idealen WLC* entspricht.

1.14.6 One Click Backup der SCEP-CA

Um das Backup der im WLC vorliegenden CA zu vereinfachen, bietet Ihnen das Gerät die Möglichkeit, mit einer einzigen Aktion einen kompletten Zertifikats-Datensatz zu erzeugen (One Click Backup). Dieser Datensatz erlaubt Ihnen die vollständige Sicherung und Wiederherstellung der CA und vermeidet das Auftreten von Zertifikats-Konflikten.

Derartige Konflikte können dann auftreten, wenn Sie die einzelnen PKCS12-Container separat vom Gerät heruntergeladen haben und anschließend wieder einspielen: Hat der WLC in der Zwischenzeit eine neue CA aufgesetzt und neue Zertifikate ausgestellt, führen die abweichenden CAs temporär zu Authentisierungsproblemen bei den verschiedenen Diensten im LCOS. Sofern nicht gewartet werden kann, bis die einzelnen Dienste neue Zertifikate anfordern, erfordert die manuelle Konfliktlösung ein Löschen der SCEP-Dateien aus dem LCOS-Dateisystem und eine Reinitialisierung des SCEP-Clienten. Mit dem Zurückspielen eines One Click Backups dagegen führt das LCOS die notwendigen Schritte automatisch aus.

Erstellen einer Backup-Datei

Um einen Zertifikats-Datensatz zu erzeugen, führen Sie die Aktion **Erstelle-PKCS12-Backup-Dateien** unter **Setup** > **Zertifikate** > **SCEP-CA** > **CA-Zertifikate** aus. Diese Aktion erzeugt eine Zip-Datei innerhalb des LCOS-Dateisystems, die alle notwendigen Dateien enthält. Zum Schutz der enthaltenen Zertifikate und Schlüssel ist die Zip-Datei automatisch mit dem Gerätepasswort geschützt, sofern Sie kein gesondertes Passwort angeben. Die erzeugte Zip-Datei lässt sich anschließend z. B. im WEBconfig über **Extras** > **Dateimanagement** > **Zertifikat oder Datei herunterladen** > **SCEP-CA – One Click Backup** herunterladen.

Zurückspielen der Backup-Datei

Um einen Zertifikats-Datensatz zurückzuspielen, laden Sie die gesicherte Zip-Datei unter Angabe der Passphrase direkt in das Gerät. Im WEBconfig z. B. erfolgt dies über die Auswahl **Extras** > **Dateimanagement** > **Zertifikat oder Datei hochladen** > **SCEP-CA – One Click Backup**. Setzen Sie dabei die Option **Vorhandene CA Zertifikate ersetzen**, damit das Gerät den Zertifikats-Datensatz nach dem Hochladen automatisch zurückspielt.

Sofern Sie die Option nicht setzen oder die Backup-Datei auf andere Weise ins Gerät laden, müssen Sie nach dem Hochladen die Aktion *2.39.2.2.11 Zertifikate-aus-Backup-wiederherstellen* ausführen, damit das Gerät den Zertifikats-Datensatz zurückspielt.

1.15 Automatischer Konfigurationsabgleich (Config-Sync) mit der LANCOM WLC High Availability Clustering XL Option

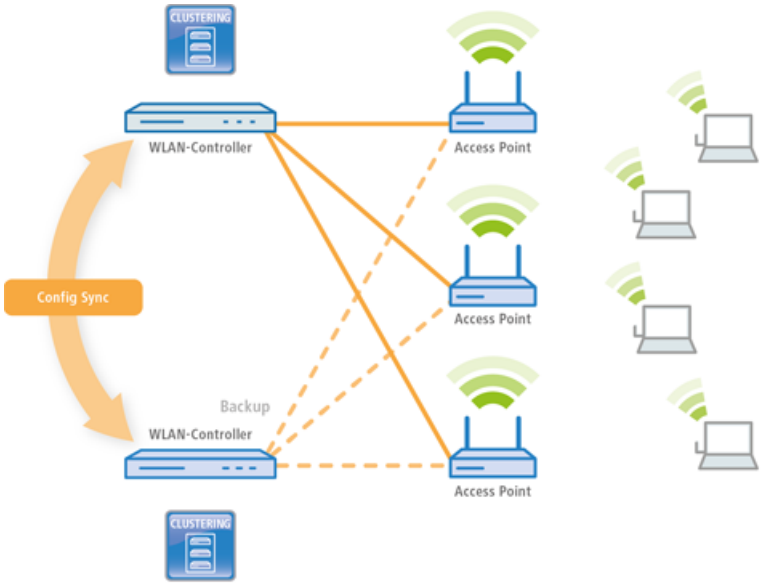
Anwendungsbeispiel WLAN-Controller:

WLAN-Infrastrukturen sind inzwischen integraler Bestandteil moderner Unternehmensnetzwerke. Mit zunehmendem Anspruch an die Verfügbarkeit einer WLAN-Lösung im Kontext des "All Wireless Office" steigt auch der Bedarf an zuverlässigen Backup- und Hochverfügbarkeitslösungen ("High Availability"). In WLAN-Infrastrukturen mit genau einem WLAN-Controller und verbundenen APs kommt es bisher bei Ausfall oder Wartung (z. B. Firmware-Update) des WLCs zu einem automatischen und autarken Weiterbetrieb der am WLC angebundenen APs. Das bedeutet, dass die APs im autarken Betriebsmodus nicht mehr auf die Funktionen zugreifen können, die auf dem WLC zentral verfügbar sind, wie z. B. Public Spot, IEEE 802.1X-Authentifizierung oder Layer-3-Tunnel.

Um dies zu vermeiden und den vollständigen Weiterbetrieb aller WLAN-Funktionen auch bei einer temporären Nichtverfügbarkeit eines WLCs aufrecht zu erhalten, können ein oder mehrere Redundanz- oder Backup-WLCs eingesetzt werden. Im Backup-Fall wechseln die APs automatisch vom temporär nicht verfügbaren WLC zu einem Backup-WLC. Hierfür ist auf dem Backup-WLC die gleiche Konfiguration (z. B. AP-Tabelle oder WLAN-Profile) wie auf dem primären WLC der APs erforderlich. Ersteinrichtung der WLCs sowie jede weitere Konfigurationsänderung muss auf den Geräten dabei jeweils separat und identisch erfolgen – für den Administrator ein enormer Aufwand. Die manuelle Pflege von Konfigurationen über mehrere identische Geräte kann im Backup-Fall mit veralteter oder nicht synchroner Konfiguration des Backup-WLCs zu einem fatalen Zustand der gesamten WLAN-Infrastruktur führen. Die dann startende Fehlersuche gestaltet sich in der Regel als Herausforderung. Auf der Anwenderseite von WLAN-Clients führt dies zu einem Ausfall der Produktivität, die unter Umständen unternehmensweit großen Schaden verursachen kann.

Neu mit der LANCOM WLC High Availability Clustering XL Option: Diese Software-Option ermöglicht die Gruppierung von mehreren WLCs zu einer hochverfügbaren Gerätegruppe (High Availability Cluster). Damit können Konfigurationsänderungen, Funktionen und Erweiterungen, die an einem WLC vorgenommen werden, automatisch auf die anderen WLCs des Clusters übertragen werden, ohne dass jedes einzelne Gerät manuell gemanagt werden muss.

Gemeinsame Parameter in einem Cluster (z. B. WLAN-Profile, AP-Tabellen oder Public Spot-Einstellungen) werden hierbei synchronisiert, individuelle Parameter (wie z. B. die IP-Adresse des WLCs) werden nicht untereinander ausgetauscht.



Mit der LANCOM WLC High Availability Clustering XL Option profitieren Sie von einer deutlich vereinfachten Administration sowie einer enormen Zeitersparnis, da Sie nur einen WLC des Clusters konfigurieren müssen. Die vorgenommenen Änderungen überträgt dieser WLC dann automatisch auf die anderen Cluster-Geräte. In Hinblick auf das oben beschriebene Szenario verbinden sich nun bei Ausfall oder Wartung (z. B. Firmware-Update) eines WLCs die APs automatisch mit einem anderen WLC, der dank Config Sync ganz ohne Zutun des Administrators bereits die identische Konfiguration besitzt. Dadurch wird eine komfortable Hochverfügbarkeit realisiert.

Die Voraussetzungen für eine gültige Gruppenmitgliedschaft eines Gerätes sind:

- Es muss eine LANCOM WLC High Availability Clustering XL Option vorhanden sein (ab LCOS-Version 9.10).
- Es muss eine IP-Kommunikation zu allen anderen Geräten möglich sein, z. B. über LAN, WAN oder VPN.
- Es muss in der Gruppenliste aufgeführt sein, die in jedem Gerät gespeichert ist.
- Es muss ein gültiges Zertifikat vorhanden sein.
- Es muss sich als Gruppenmitglied per Zertifikat authentifizieren können.

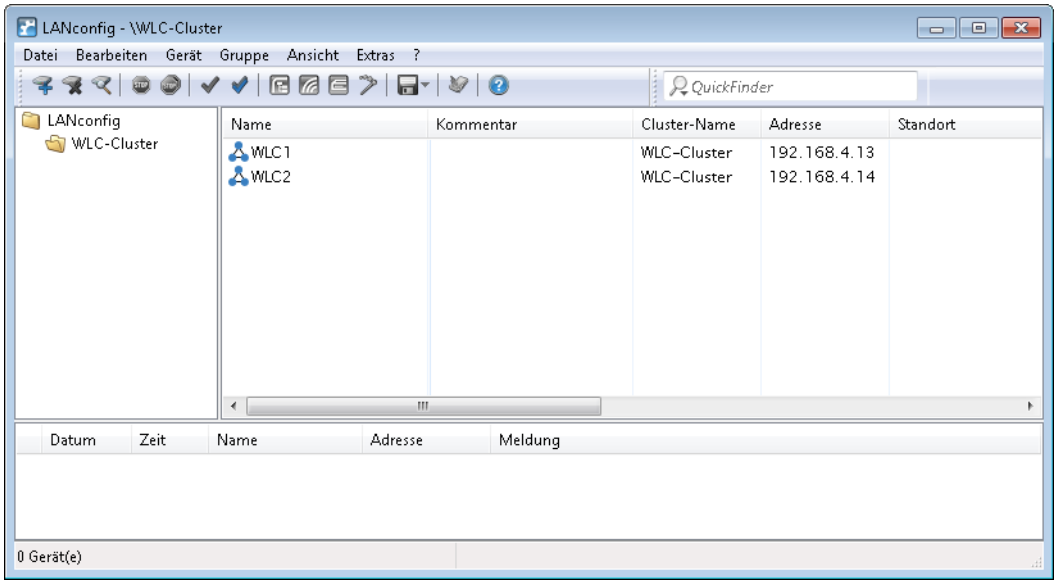
1.15.1 Spezielles LANconfig-Icon für Cluster-Geräte oder mit Config-Sync

LANconfig markiert Geräte, die ihre Konfiguration per Config-Sync teilen, mit einem eigenen Symbol. Zudem ist in der Spalte **Config Cluster** die Konfigurationsgruppe jedes Gerätes ersichtlich. Somit bietet Ihnen LANconfig die Möglichkeit, die Geräteauflistung nach Clusternamen zu sortieren und zu bearbeiten.

Möchten Sie an der Konfiguriation eines Clustermitgliedes Änderungen vornehmen, so erhalten Sie folgende Warnung:

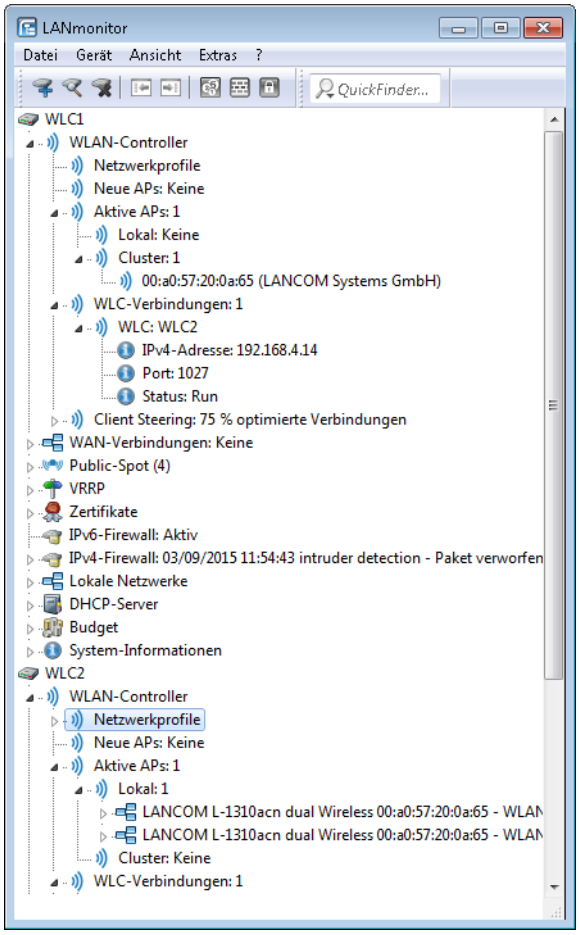
"Dieses Gerät gehört zu dem Config-Cluster: [clustername]. Das Bearbeiten dieser Konfiguration wirkt sich auch auf folgende Geräte aus: [Auflistung aller Geräte des gleichen Clusters]"

Diese Meldung können Sie bei Bedarf umgehen. Aktivieren Sie hierfür die Option **Nicht wieder anzeigen** innerhalb des angezeigten Fensters.



1.15.2 Spezielles LANmonitor-Icon für Cluster-Geräte oder mit Config-Sync

LANmonitor markiert Geräte, die ihre Konfiguration per Config-Sync teilen, mit einem eigenen Symbol. Zudem wird hinter den Gerätenamen der Name der Konfigurationsgruppe (Cluster name) angegeben. Somit können Sie mit LANmonitor die Geräte mit gleicher Konfiguration leichter zuordnen.



2 Anhang

2.1 Übersicht der capwap-Parameter im show-Befehl

Über die Konsole lassen sich folgende Informationen zum CAPWAP-Dienst aufrufen:

Tabelle 3: Übersicht aller capwap-Parameter im show-Befehl

Parameter	Bedeutung
`-addresses [<IfcNum>]`	Zeigt die Adresstabellen eines einzelnen oder aller WLC-Tunnel. Im Falle eines einzelnen WLC-Tunnels geben Sie für `<IfcNum>` die Nummer der logischen WLC-Tunnel-Schnittstelle an, z. B. `10`.
`-groups`	Zeigt Informationen zu einzelnen oder allen vorhandenen Zuweisungs- / Tag-Gruppen.

Den Befehl `show capwap groups` erweitern Sie um die nachfolgend gelisteten Parameter, wodurch sich der Umfang der angezeigten Informationen regulieren lässt:

Tabelle 4: Übersicht aller 'capwap group'-Parameter im show-Befehl

Parameter	Bedeutung
`all`	Zeigt die im Setup-Menü konfigurierten Namen und die geräteinternen Namen sämtlicher eingerichteten Zuweisungs- / Tag-Gruppen sowie der Default-Gruppe. Die Default-Gruppe stellt eine interne Gruppe dar, die sämtliche APs enthält.
`<group1> <group2> <…>`	Zeigt alle APs der betreffenden Zuweisungs-/Tag-Gruppen.
`-l <location>`	Zeigt alle APs des betreffenden Standorts.
`-c <country>`	Zeigt alle APs des betreffenden Landes.
`-i <city>`	Zeigt alle APs der betreffenden Stadt.
`-s <street>`	Zeigt alle APs der betreffenden Straßen.
`-b <building>`	Zeigt alle APs des betreffenden Gebäudes.
`-f <floor>`	Zeigt alle APs der betreffenden Etage.
`-r <room>`	Zeigt alle APs der betreffenden Raumbezeichnung.
`-d <device>`	Zeigt alle APs, die den angegebenen Gerätenamen tragen.
`-v <firmware>`	Zeigt alle APs, welche die angegebene Firmware besitzen. Geben Sie dazu für `<firmware>` die Versionsnummer gefolgt von der Build-Nummer an, z. B. `9.00.0001`.
`-x <firmware>`	Zeigt alle APs, deren Firmware-Version kleiner ist als die auf dem aktuellen Gerät installierte.
`-y <firmware>`	Zeigt alle APs, deren Firmware-Version gleich groß oder kleiner ist als die auf dem aktuellen Gerät installierte.

Parameter	Bedeutung
`-z <firmware>`	Zeigt alle APs, deren Firmware-Version größer ist als die auf dem aktuellen Gerät installierte.
`-t <firmware>`	Zeigt alle APs, deren Firmware-Version gleich groß oder größer ist als die auf dem aktuellen Gerät installierte.
`-n <intranet>`	Zeigt alle APs, deren IP zur angegebenen Intranet-Adresse gehört.
`-p <profile>`	Zeigt alle APs, denen das angegebene WLAN-Profil zugeordnet ist.
`rmgrp <group1 intern_name> <group2 intern_name> …`	Löscht die Gruppe(n) mit dem angegebenen internen Namen aus dem Arbeitsspeicher des Gerätes. Nutzen Sie diesen Befehl, um die Arbeitsspeicher freizugeben, falls eine zu hohe Zahl von Gruppen die Perfomanz des Gerätes verschlechtert. Der Eintrag im Setup-Menü bleibt von dieser Aktion unberührt.
`resetgrps`	Löscht alle Gruppen bis auf die Default-Gruppe.

Für die Standort-Informationen wertet das Gerät die in der Access-Point-Tabelle unter **Standort** eingetragenen Informationen aus. Folgende Feld-Bezeichnungen stehen Ihnen zur Verfügung:

- co=Country
- ci=City
- st=Street
- bu=Building
- fl=Floor
- ro=Room

Der Standort-Eintrag `co=Deutschland,ci=Aachen` z. B. ermöglicht Ihnen, über den Befehl `+show capwap group -i Aachen` an der Konsole alle vom WLC verwalteten APs in Aachen aufzulisten.

Befehlsbeispiele

```
show capwap group all
show capwap group group1
show capwap group -l yourlocation
show capwap group -s yourstreetname
show capwap group -d yourdevicename
show capwap group -p yourprofilename
show capwap group -d yourdevicename -p yourprofile -v yourfirmversion …
```