



... connecting your business

Zentrales WLAN Management

- LANCOM WLAN Controller
- LANCOM WLC-Option für Router

LANCOM
Systems

Inhalt

1 Zentrales WLAN-Management.....	4
1.1 Ausgangslage.....	4
1.2 Technische Konzepte.....	4
1.2.1 Der CAPWAP-Standard.....	4
1.2.2 Die Smart-Controller-Technologie.....	5
1.2.3 Kommunikation zwischen Access Point und WLAN-Controller.....	7
1.2.4 Zero-Touch-Management.....	8
1.2.5 Split-Management.....	8
1.3 Grundkonfiguration der WLAN Controller Funktion.....	9
1.3.1 Zeitinformation für den LANCOM WLAN Controller einstellen.....	9
1.3.2 Erstellen einer Default-Konfiguration.....	9
1.3.3 Konfiguration der Access Points.....	13
1.4 Konfiguration.....	14
1.4.1 Allgemeine Einstellungen.....	14
1.4.2 Profile.....	15
1.4.3 Access Point Konfiguration.....	20
1.5 Access Point Verwaltung.....	40
1.5.1 Neue Access Points manuell in die WLAN-Struktur aufnehmen.....	40
1.5.2 Access Points manuell aus der WLAN-Struktur entfernen.....	42
1.5.3 Access Point deaktivieren oder dauerhaft aus der WLAN-Struktur entfernen.....	43
1.6 Zentrales Firmware- und Skript-Management.....	43
1.6.1 Allgemeine Einstellungen für das Firmware-Management.....	44
1.7 WLAN Layer-3 Tunneling.....	47
1.7.1 Einleitung.....	47
1.7.2 Tutorials.....	48
1.8 RADIUS.....	61
1.8.1 Prüfung der WLAN-Clients über RADIUS (MAC-Filter).....	61
1.8.2 Externer RADIUS-Server.....	62
1.8.3 Dynamische VLAN-Zuweisung.....	63
1.9 RADIUS-Accounting im WLAN-Controller für logische WLANs aktivieren.....	65
1.10 Anzeigen und Aktionen im LANmonitor.....	66
1.11 Funkfeldoptimierung.....	67
1.12 Kanallastanzeige im WLC-Betrieb.....	69
1.13 Sicherung der Zertifikate.....	69
1.13.1 Backup der Zertifikate anlegen.....	69
1 Sichern und Wiederherstellen weiterer Dateien der SCEP-CA.....	70
2 Zertifikats-Backup in das Gerät einspielen.....	71
1.14 Backuplösungen.....	72
1 Backup mit redundanten WLAN-Controllern.....	72
1.14.1 Backup mit primären und sekundären WLAN-Controllern.....	74

1.14.2 Primäre und sekundäre Controller.....74

1 Zentrales WLAN-Management

LANCOM WLAN Controller und LANCOM Router mit WLC-Option dienen dem zentralen WLAN-Management in einer größeren WLAN-Infrastruktur. Der WLAN-Controller speichert zentral die Konfigurationen der einzelnen Access-Points in Profilen und verteilt diese an die entsprechenden Geräte.



Diese Dokumentation verwendet im weiteren Verlauf den Begriff WLAN-Controller als Oberbegriff für LANCOM WLAN Controller und LANCOM Router mit WLC-Option.

1.1 Ausgangslage

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

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

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

1.2 Technische Konzepte

Mit einem zentralen WLAN-Management lassen sich diese Probleme lösen. Die Konfiguration der Access Points wird dabei nicht mehr in den Geräten selbst vorgenommen, sondern in einer zentralen Instanz, dem WLAN-Controller. Der WLAN-Controller authentifiziert die Access Points und überträgt den zugelassenen Geräten eine passende Konfiguration. Dadurch kann die Konfiguration des WLANs komfortabel von einer zentralen Stelle übernommen werden und die Konfigurationsänderungen wirken sich zeitgleich auf alle Access Points aus. Da die vom WLAN-Controller zugewiesene Konfiguration in den Access Points optional **nicht** im Flash, sondern im RAM abgelegt wird, können in besonders sicherheitskritischen Netzen bei einem Diebstahl der Geräte auch keine sicherheitsrelevanten Daten in unbefugte Hände geraten. Nur im "autarken Weiterbetrieb" wird die Konfiguration für eine definierte Zeit optional im Flash gespeichert (in einem Bereich, der nicht mit LANconfig oder anderen Tools auszulesen ist).

1.2.1 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 WLAN-Controller und dem Access Point 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.

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

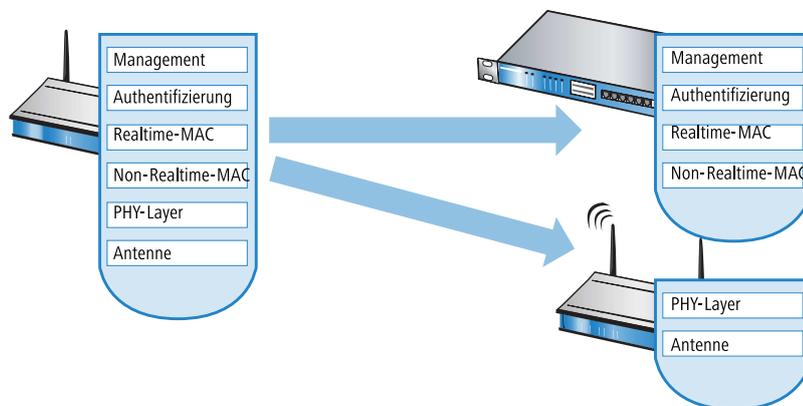
1.2.2 Die Smart-Controller-Technologie

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

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

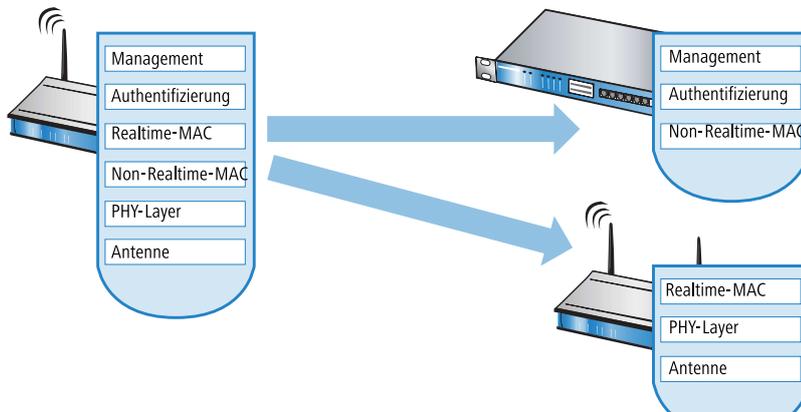
CAPWAP beschreibt drei unterschiedliche Szenarien für die Verlagerung von WLAN-Funktionen in den zentralen WLAN-Controller.

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

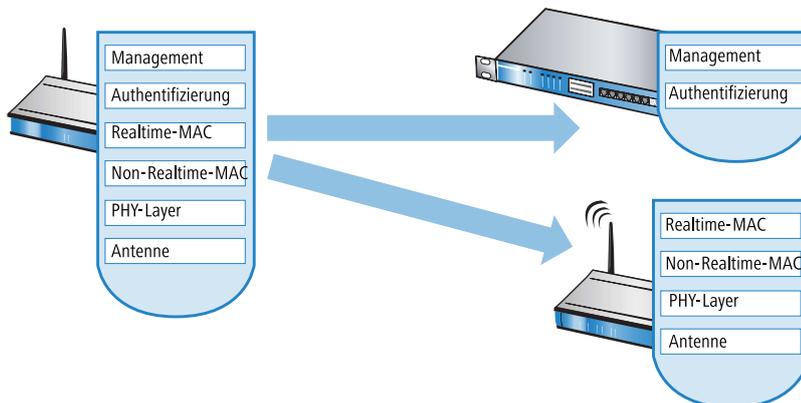


- Split-MAC: Bei dieser Variante wird nur ein Teil der WLAN-Funktionen an den WLAN-Controller übertragen. Üblicherweise werden die zeitkritischen Anwendungen (Realtime-Applikationen) weiterhin auf dem Access Point

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



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



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

! Layer-3-Tunneling und Layer-3-Roaming

Die LANCOM WLAN Controller unterstützen auch die Übertragung der Nutzdaten durch einen CAPWAP-Tunnel.

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

1.2.3 Kommunikation zwischen Access Point und WLAN-Controller

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

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

- Bei LANCOM Access Points sind im Auslieferungszustand die WLAN-Module auf die Betriebsart 'Managed' eingestellt. In diesem Modus suchen die LANCOM Access Points nach einem zentralen WLAN-Controller, der ihnen eine Konfiguration zuweisen kann, und bleiben so lange im "Such-Modus", bis sie einen passenden WLAN-Controller gefunden haben oder die Betriebsart für die WLAN-Module manuell geändert wird.
- Während der Access Point nach einem WLAN Controller 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 LANCOM 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 LANCOM Wireless Routern auf 'Managed' umgestellt werden.

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

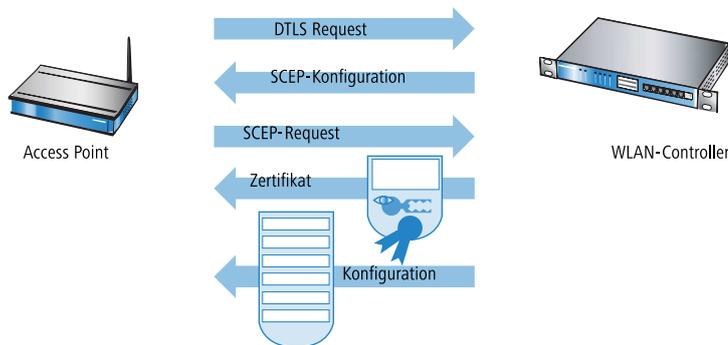
! Außerdem können auch DNS-Namen von WLAN-Controllern aufgelöst werden. Alle Access Points mit LCOS 7.22 oder höher haben den Standardnamen 'WLC-Address' bereits konfiguriert, sodass ein DNS-Server diesen Namen zu einem LANCOM WLAN Controller auflösen kann. Gleiches gilt auch für die über DHCP gelernten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

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

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

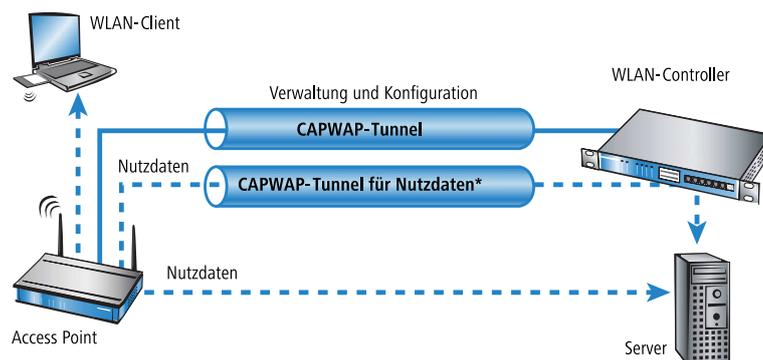
Über die gesicherte DTLS-Verbindung wird dem Access Point die Konfiguration für den integrierten SCEP-Client mitgeteilt – der Access Point kann dann über SCEP sein Zertifikat bei der SCEP-CA abholen. Anschließend wird die dem Access Point zugewiesene Konfiguration übertragen.

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



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

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



1.2.4 Zero-Touch-Management

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

1.2.5 Split-Management

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

1.3 Grundkonfiguration der WLAN Controller Funktion

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

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

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

1.3.1 Zeitinformation für den LANCOM WLAN Controller einstellen

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

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

 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 WLAN Controller und wählen im Kontext-Menü den Eintrag **Datum/Zeit setzen**. Alternativ klicken Sie in WEBconfig im Bereich **Extras** den Link **Datum und Uhrzeit einstellen**.

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

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

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

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

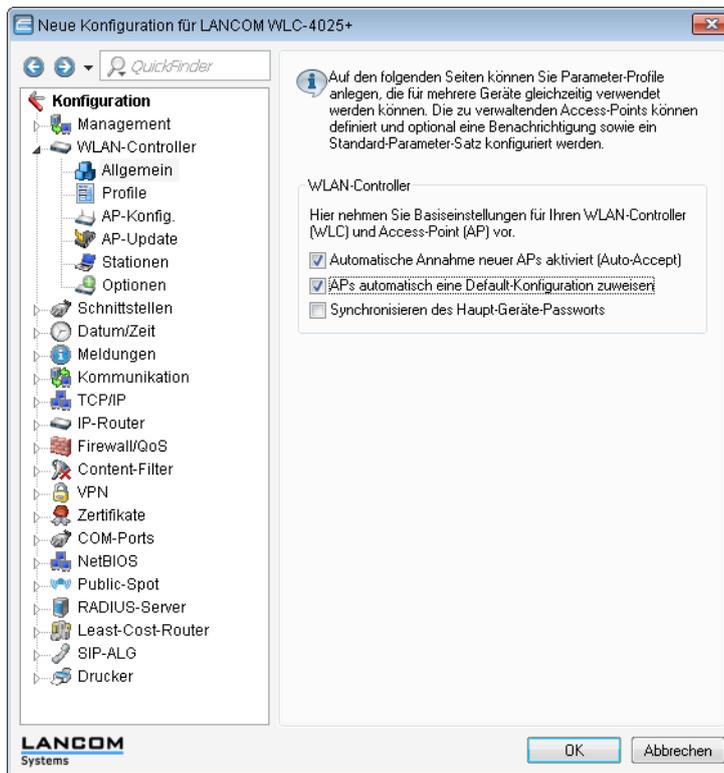
1.3.2 Erstellen einer Default-Konfiguration

Mit der Zeitinformation und den Zertifikaten ist der LANCOM WLAN Controller grundsätzlich betriebsbereit. Sofern sich im LAN Access Points im Managed-Modus befinden (Standardmodus für werksseitig ausgelieferte Access Points bzw. nach Reset mit LCOS 7.20 oder höher, manuelle Einstellung siehe *Konfiguration der Access Points*), zeigt der WLAN Controller diese nach einer kurzen Zeit als "Neue Access Points" im LANmonitor an. Bei Geräten mit New-APs-LED blinkt diese orange und bei Geräten mit einem Display wird die Anzahl der neuen Access Points (New APs) angezeigt.

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

Beispiel einer Default-Konfiguration

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



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

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

3. Wechseln Sie 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 LANCOM WLAN Controller verwendet.
 - **SSID:** Mit dieser SSID verbinden sich die WLAN-Clients.
 - **Verschlüsselung:** Wählen Sie die Verschlüsselung passend zu den Möglichkeiten der verwendeten WLAN-Clients und geben Sie ggf. einen Schlüssel bzw. eine Passphrase ein.
 - Deaktivieren Sie die MAC-Prüfung. Hinweise zur Nutzung der MAC-Filterlisten in gemanagten WLAN-Strukturen finden Sie unter [Prüfung der WLAN-Clients über RADIUS \(MAC-Filter\)](#).
4. Erstellen Sie auch bei den physikalischen WLAN-Parametern einen neuen Eintrag. Für die Default-Konfiguration reicht hier in vielen Fällen nur die Angabe eines Namens. Die restlichen Einstellungen können bei Bedarf angepasst werden.

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

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

6. Wechseln Sie auf in Ansicht **AP-Konfig.**, 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 'ffffffff' gesetzt und ist nicht editierbar. Damit gilt dieser Eintrag als Standard für alle Access Points, die nicht mit ihrer MAC-Adresse explizit in dieser Tabelle eingetragen sind.

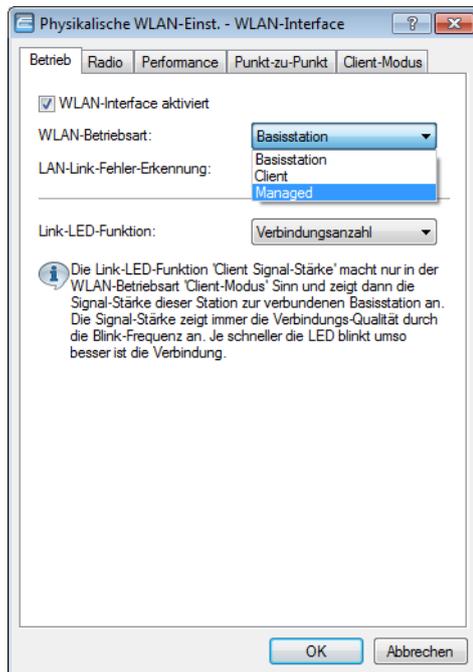
1.3.3 Konfiguration der Access Points

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

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

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

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



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

```
# Script
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 LANCOM 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 WLAN-Controller vor.

- Automatische Annahme neuer APs (Auto-Accept)

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

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

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

- Automatische Zuweisung der Default-Konfiguration

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



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

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

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

1.4.2 Profile

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

WLAN-Profilen

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

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

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

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

- **Profil-Name**

Name des Profils, unter dem die Einstellungen gespeichert werden.

WLAN-Netzwerk-Liste

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



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

Physikalische WLAN-Parameter

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

IP-Adresse alternativer WLAN-Controller

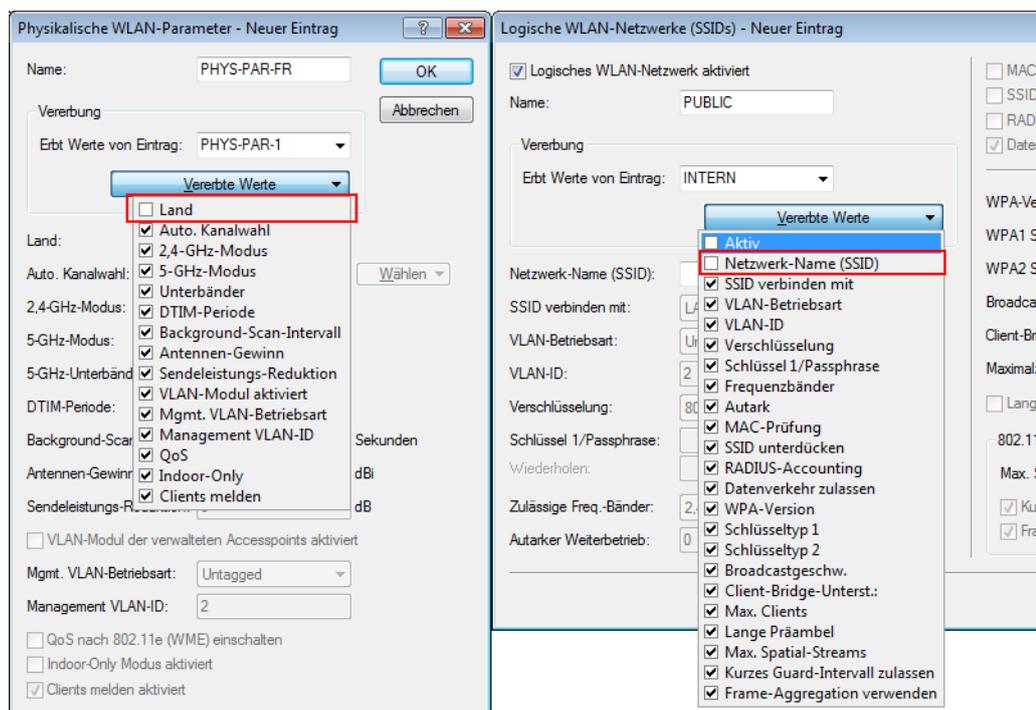
Liste der WLAN-Controller, bei denen der Access Point eine Verbindung versuchen soll. Der Access Point leitet die Suche nach einem WLAN-Controller über einen Broadcast ein. Wenn nicht alle WLAN-Controller über einen solchen Broadcast erreicht werden können (WLAN-Controller steht z. B. in einem anderen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

Vererbung von Parametern

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

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

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



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

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

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

Logische WLAN-Netzwerke

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

LANconfig: **WLAN-Controller > Profile > Logische WLAN-Netzwerke**

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

- **Netzwerkname**

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

- **Vererbung**

Auswahl eines schon definierten logischen WLAN-Netzwerks, von dem die Einstellungen übernommen werden sollen.

- **SSID**

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

- **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)!

■ Autarker Weiterbetrieb

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

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

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

Durch diese Option kann der Access Point auch dann weiter arbeiten, wenn die Verbindung zum WLAN-Controller kurzfristig unterbrochen wird. Außerdem stellt diese Maßnahme einen wirksamen Schutz gegen Diebstahl dar, da die sicherheitsrelevanten Parameter der Konfiguration nach Ablauf der eingestellten Zeit automatisch gelöscht werden.



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



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



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

Physikalische WLAN-Parameter

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

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

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

- **Name**

Eindeutiger Name für diese Zusammenstellung von physikalischen WLAN-Parametern.

- **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**

Standardmäßig können die Access Points alle Kanäle nutzen, die aufgrund der Ländereinstellung erlaubt sind. Um die Auswahl auf bestimmte Kanäle zu beschränken, können hier die gewünschten Kanäle als kommaseparierte Liste eingetragen werden. Dabei ist auch die Angabe von Bereichen (z. B. '1,6,11') möglich.

- **Management-VLAN-ID**

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



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

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

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

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

1.4.3 Access Point Konfiguration

IP-Parameter-Profil

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

LANconfig: **WLAN Controller > AP-Konfig. > IP-Parameter-Profil**

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

- **Name:** Name des IP-Parameter-Profiles

Mögliche Werte

Maximal 31 Zeichen

Default

leer

- **Vererbung:** Auswahl eines schon definierten IP-Parameter-Profiles, von dem die Einstellungen übernommen werden sollen (*Vererbung von Parametern*).

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

Mögliche Werte

Max. 63 Zeichen

Default

leer

- **Netzmaske:** Netzmaske des Profils

Mögliche Werte

gültige Netzmaske

Default

leer

- **Standard-Gateway:** Das Standard-Gateway, dass das Profil verwendet.

Mögliche Werte

gültige IP-Adresse

Default

leer

- **Erster DNS:** Der DNS (Domain Name System), den das Profil verwenden soll.

Mögliche Werte

gültige IP-Adresse

Default

leer

- **Zweiter DNS:** Zweiter, alternativer DNS, sollte der erste nicht erreichbar sein.

Mögliche Werte

gültige IP-Adresse

Default

leer

Liste der Access Points

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

die Möglichkeit, eine Verbindung zu einem WLAN-Controller aufbauen zu können. Für jeden Access Point können Sie die folgenden Parameter definieren:

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

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

- **Eintrag aktiv**

Aktiviert bzw. deaktiviert diesen Eintrag.

- **Update-Management aktiv**

Wenn Sie für den Access-Point das Update-Management aktivieren, können neue Firmware- oder Script-Versionen automatisch geladen werden. Nehmen Sie alle weiteren Einstellungen unter AP-Update vor ([Zentrales Firmware- und Skript-Management](#)).

- **MAC-Adresse**

MAC-Adresse des Access Points.

- **AP-Name**

Name des Access Point im Managed-Modus.

- **Standort**

Standort des Access Point im Managed-Modus.

- **WLAN-Profil**

WLAN-Profil aus der Liste der definierten Profile.

- **WLAN-Interface 1**

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

■ **Auto. Kanalwahl Ifc 1**

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

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

■ **WLAN-Interface 2**

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

■ **Auto. Kanalwahl Ifc 2**

Automatische Kanalwahl für das zweite WLAN-Modul.



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

■ **Verschlüsselung**

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

■ **Doppelte Bandbreite**

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

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

Stationen

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

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

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

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

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

Buttons: OK, Abbrechen

LANconfig: **WLAN Controller > Stationen > Stationen**

WEBconfig: **LCOS-Menübaum > Setup > WLAN-Management > Zugangsliste**

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

Mögliche Werte

Gültige MAC-Adresse

Default

leer

- **Name:** Sie können zu jedem WLAN-Client einen beliebigen Namen und einen Kommentar eingeben. Dies ermöglicht Ihnen eine einfachere Zuordnung der MAC-Adressen zu bestimmten Stationen oder Benutzern.

Mögliche Werte

Max. 32 Zeichen

Default

leer

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

Mögliche Werte

ASCII-Zeichenkette mit einer Länge von 8 bis 63 Zeichen

Default

leer

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

Mögliche Werte

0 bis 65535 kbit/s

Default

0

Besondere Werte

0: keine Begrenzung

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

Mögliche Werte

0 bis 65535 kbit/s

Default

0

Besondere Werte

0: keine Begrenzung



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

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

Mögliche Werte

0 bis 4096

Default

0

Besondere Werte

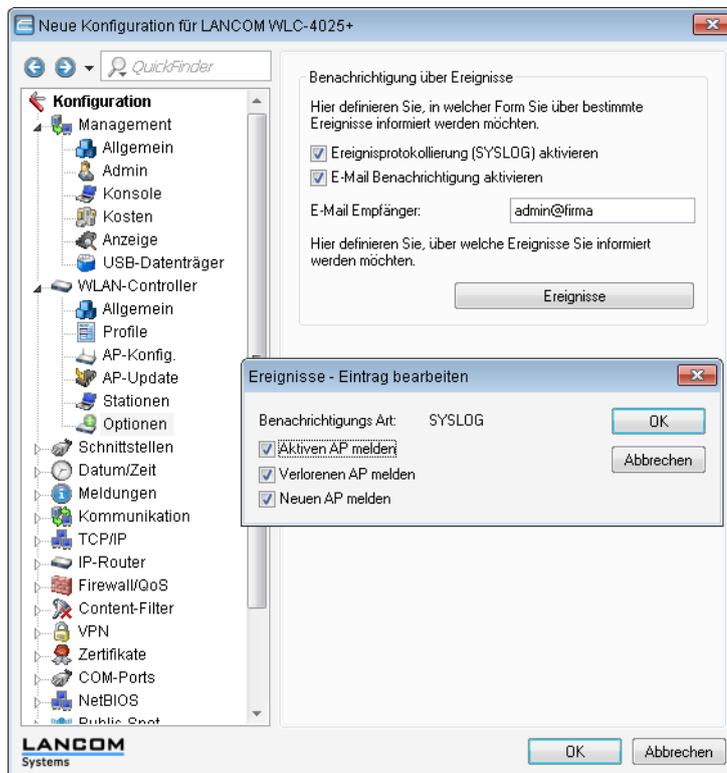
Bei der VLAN-ID 0 wird der Station keine spezielle VLAN-ID zugewiesen, es gilt die VLAN-ID der Funkzelle (SSID).

Optionen für den WLAN-Controller

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

Benachrichtigungen über Ereignisse

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



LANconfig: **WLAN-Controller > Optionen > Benachrichtigungen**

WEBconfig: **LCOS-Menübaum > Setup > WLAN-Management > Benachrichtigung**

■ SYSLOG

Aktiviert die Benachrichtigung über SYSLOG.

- Mögliche Werte: Ein/Aus.

■ E-Mail

Aktiviert die Benachrichtigung über E-Mail.

- Mögliche Werte: Ein/Aus.

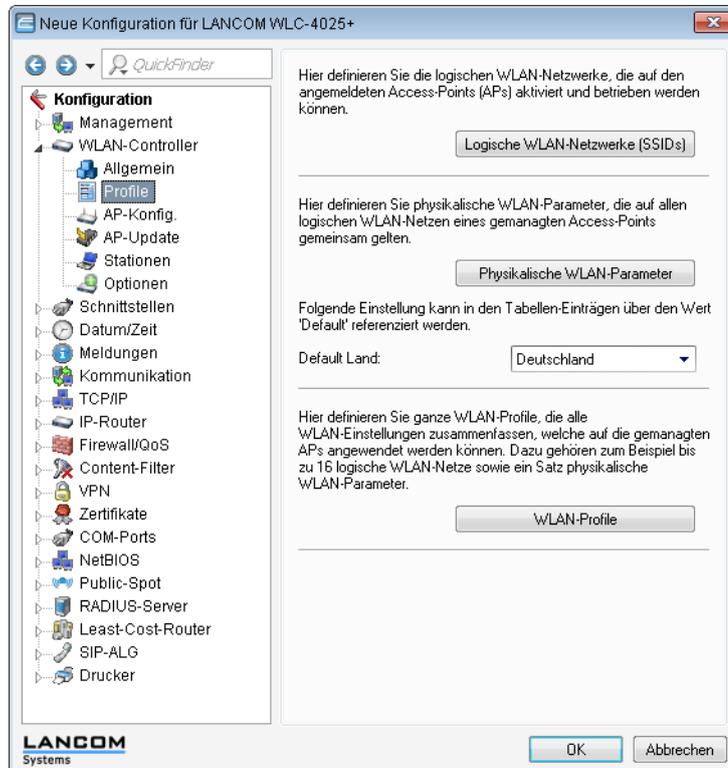
■ Ereignisse

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

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

Default-Parameter

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



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

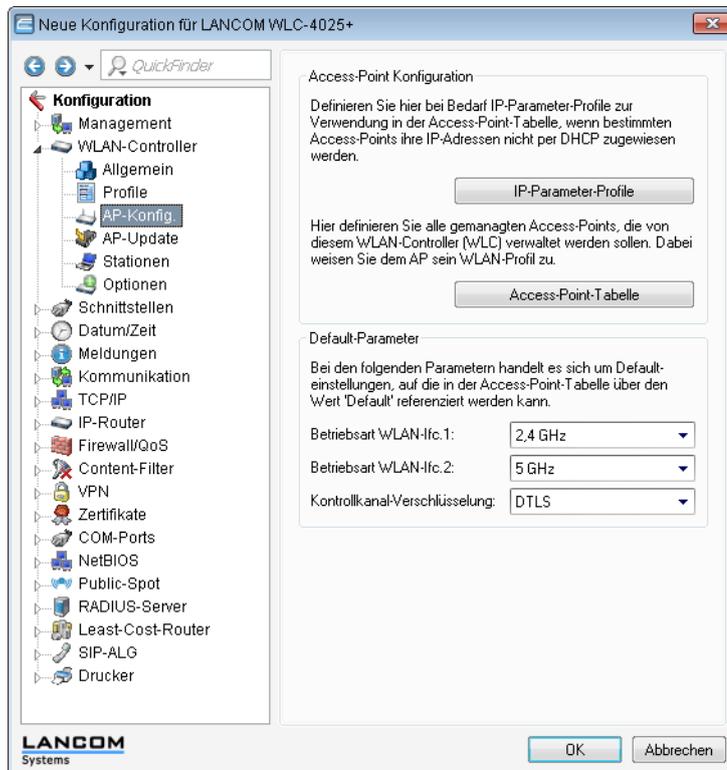
Webconfig: **LCOS-Menübaum > Setup > WLAN Management > AP-Konfiguration > Laendereinstellung**

■ Default Land

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

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

▶ Deutschland



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.

Tutorial: Virtualisierung und Gastzugang über LANCOM WLAN Controller

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

! Public Spot Option ist erforderlich.

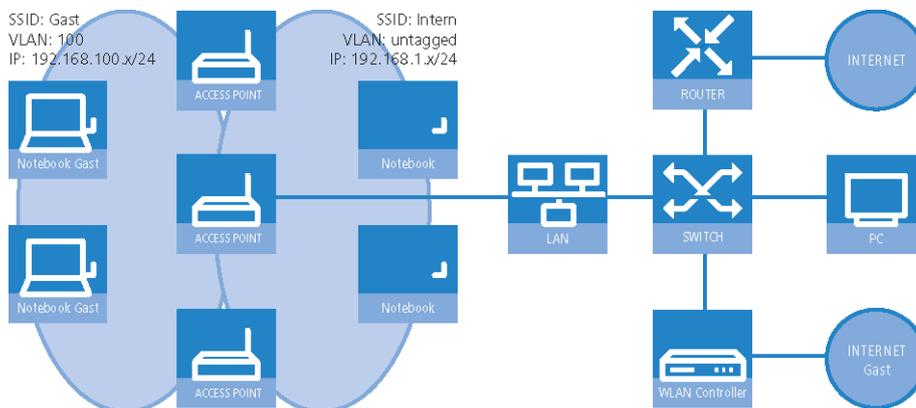
Ziele

- Nutzung der WLAN-Infrastruktur für interne Mitarbeiter und Gäste
- Nutzung der gleichen physikalischen Komponenten (Kabel, Switches, Access Points)
- Trennung der Netzwerke über VLAN und ARF

- Auskopplung der Datenströme zu bestimmten Zielnetzwerken:
 - Gäste: nur Internet
 - Interne Mitarbeiter: Internet sowie alle lokalen Geräte und Dienste
- Gäste melden sich über ein Webformular am WLAN an.
- Interne Mitarbeiter nutzen die WLAN-Verschlüsselung zur Authentifizierung.

Aufbau

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

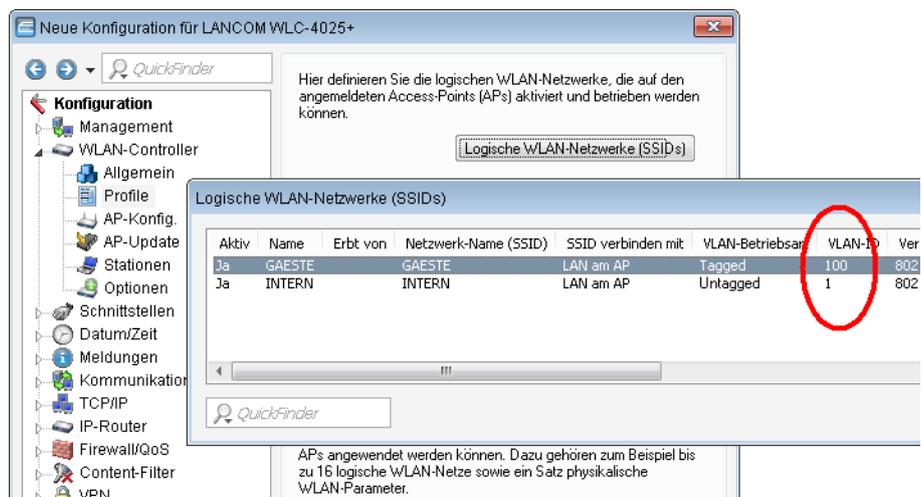


WLAN-Konfiguration des WLAN Controllers

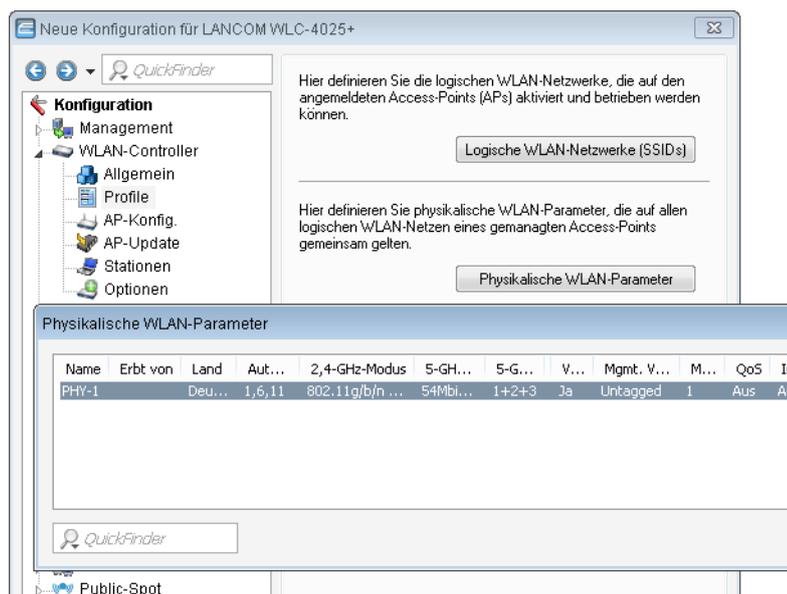
Bei der WLAN-Konfiguration werden die benötigten WLAN-Netzwerke definiert und zusammen mit den physikalischen WLAN-Einstellungen den vom Controller verwalteten Access Points zugewiesen.

1. Erstellen Sie ein logisches WLAN für die Gäste und eins für die internen Mitarbeiter:
 - Das WLAN mit der SSID 'GAESTE' nutzt die VLAN-ID '100', hier wird keine Verschlüsselung verwendet.

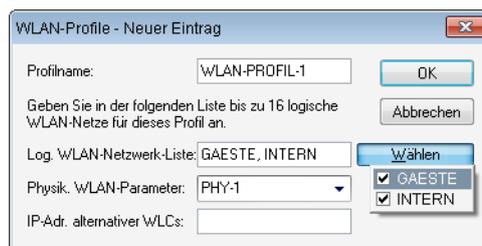
- Das WLAN mit der SSID 'INTERN' nutzt die VLAN-ID '1' (wird ohne VLAN-Tag in das Ethernet übertragen), hier wird eine Verschlüsselung nach WPA2 verwendet.



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



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



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

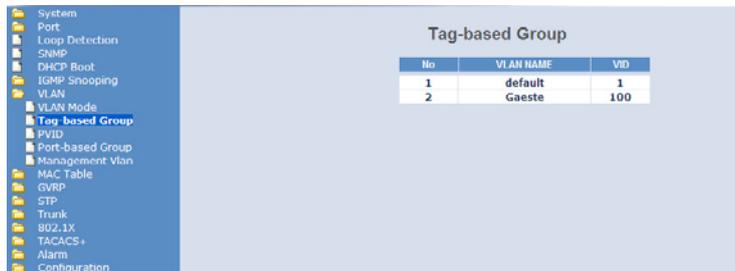
Konfiguration des Switches

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

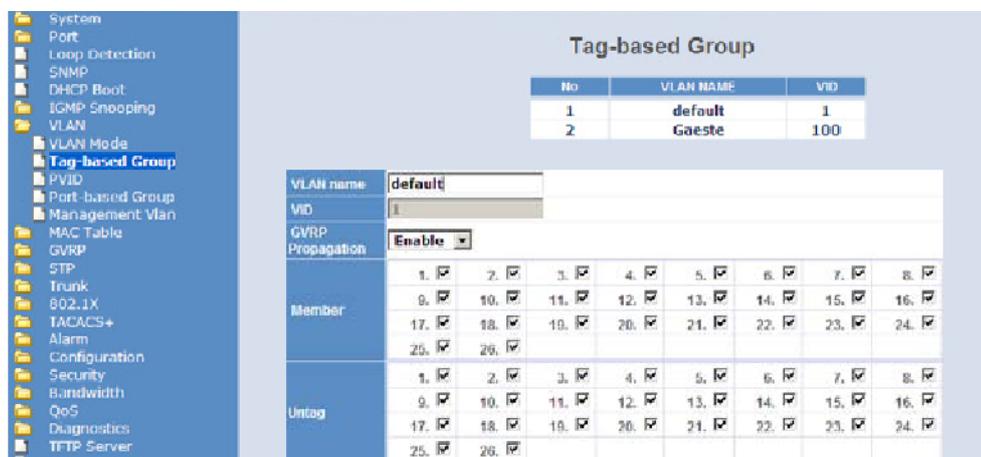
- Stellen Sie den VLAN-Modus auf 'Tag-based' ein, da die Zuweisung der VLAN-Tags durch die Access Points erfolgt.

1 Zentrales WLAN-Management

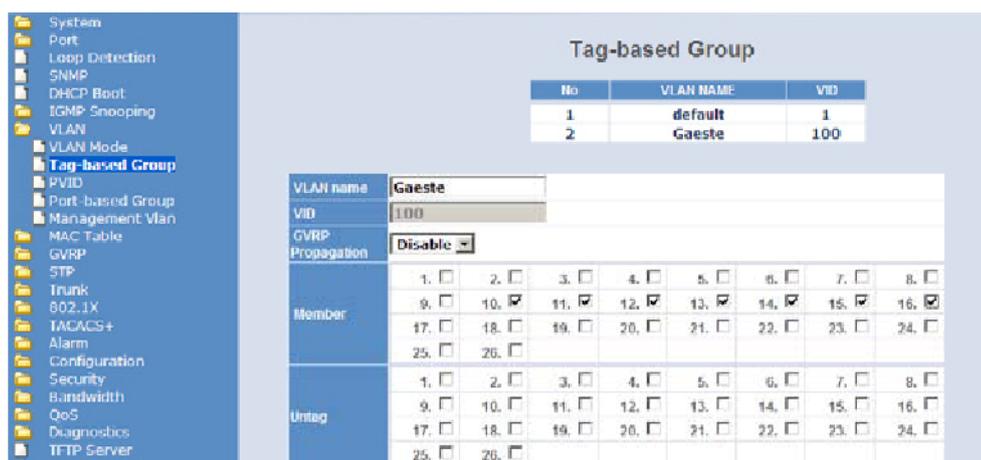
- Zur Unterscheidung der VLANs im Switch werden zwei Gruppen verwendet. Das interne Netz für die Mitarbeiter wird in der Default-Gruppe abgebildet, für die Gäste wird eine eigene Gruppe eingerichtet. Dabei werden jeweils die VLAN-IDs verwendet, die auch schon bei der Konfiguration der WLANs im Controller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



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



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



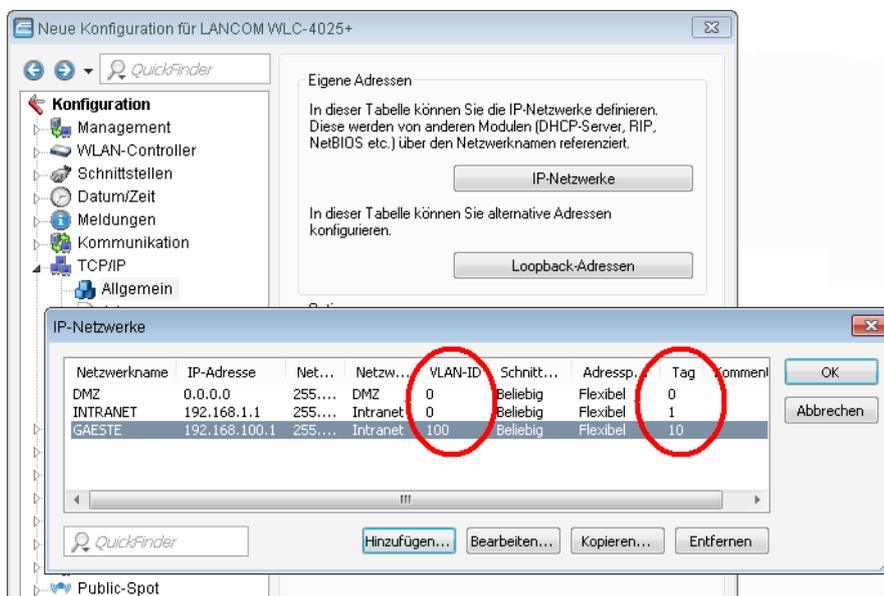
- Die Port VLAN ID (PVID) wird für alle Ports auf '1' gestellt, um die Ports dem internen Netz zuzuordnen. Ungetaggt eingehende Pakete werden auf diesen Ports also mit der VLAN-ID '1' weitergeleitet.

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

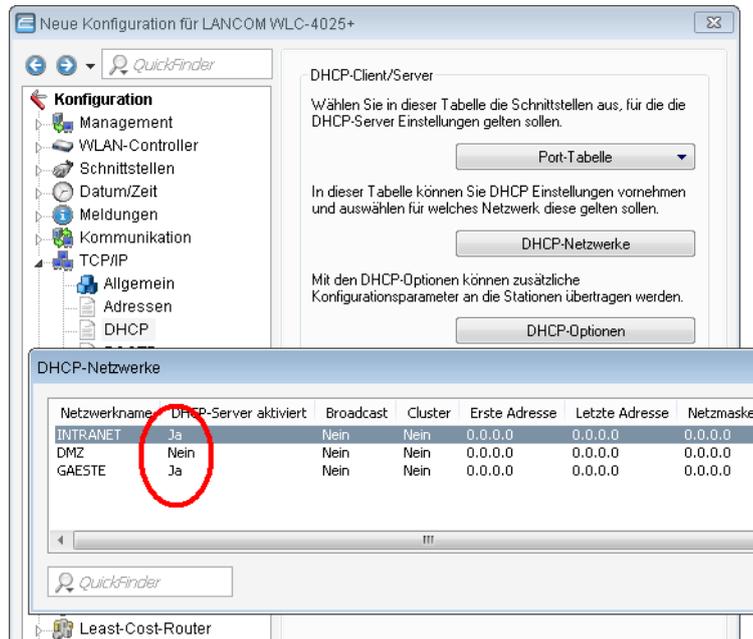
Konfiguration der IP-Netzwerke im WLAN Controller

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

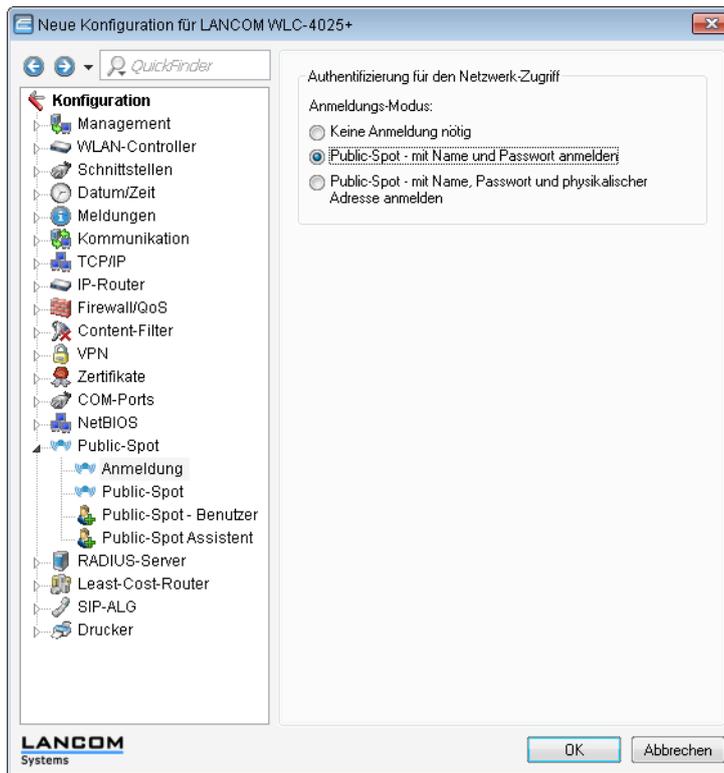
- Stellen Sie den VLAN-Modus auf 'Tag-based' ein, da die Zuweisung der VLAN-Tags durch die Access Points erfolgt.
 - Stellen Sie für das interne Netzwerk das 'Intranet' auf die Adresse '192.168.1.1' ein. Dieses IP-Netzwerk verwendet die VLAN-ID '0', damit werden alle ungetaggten Datenpakete diesem Netzwerk zugeordnet (das VLAN-Modul des Controllers selbst muss dazu deaktiviert sein). Das Schnittstellen-Tag '1' wird verwendet.
 - Legen Sie für die Gäste ein neues IP-Netzwerk mit der Adresse '192.168.100.1' an. Dieses Netzwerk verwendet die VLAN-ID '100', damit werden alle Datenpakete mit dieser ID dem Gäste-Netzwerk zugeordnet. Auch hier dient das Schnittstellen-Tag '10' der späteren Verwendung im virtuellen Router.



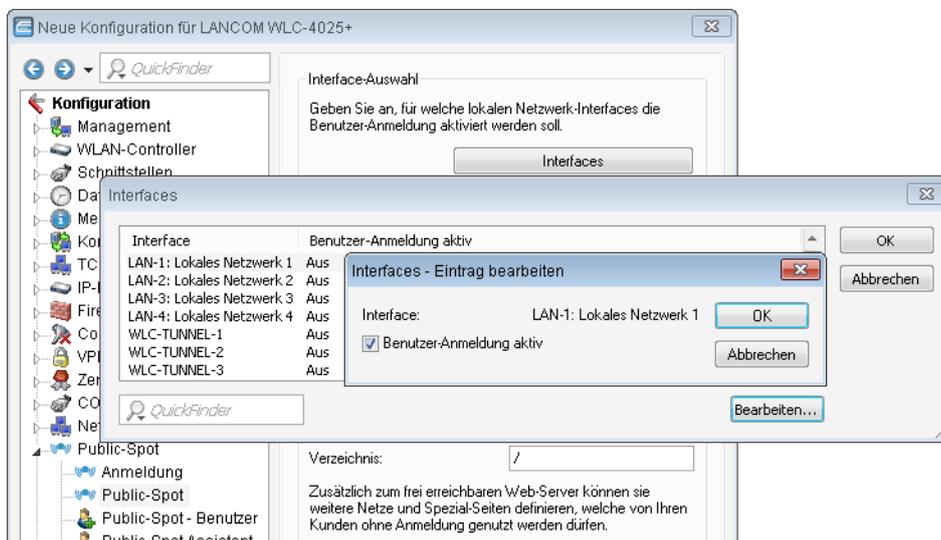
2. Für beide IP-Netzwerke wird ein Eintrag bei den DHCP-Netzwerken angelegt, mit dem der DHCP-Server fest eingeschaltet wird.



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

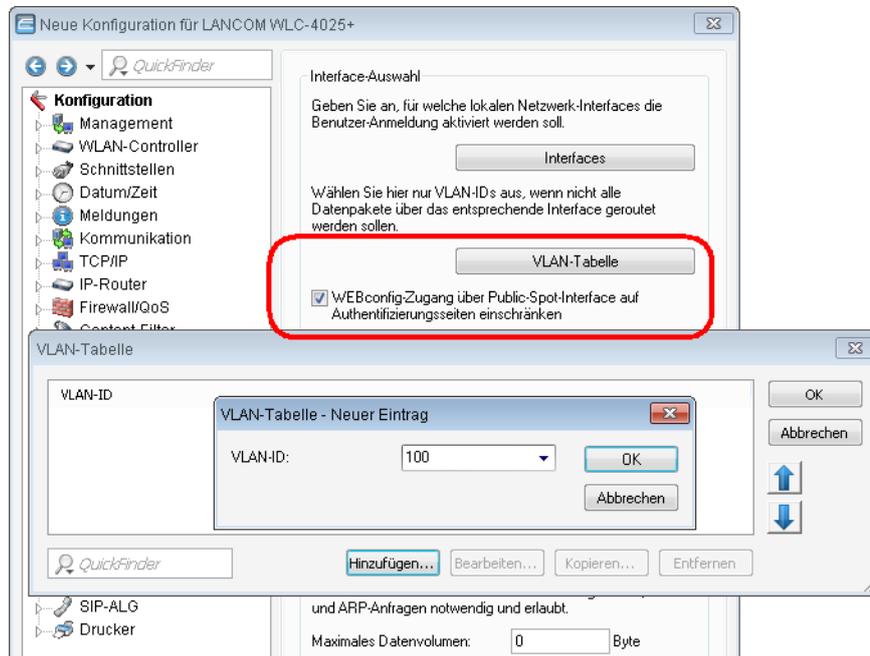


2. Schalten Sie die Benutzeranmeldung für das Interface des Controllers ein, über das er mit dem Switch verbunden ist.



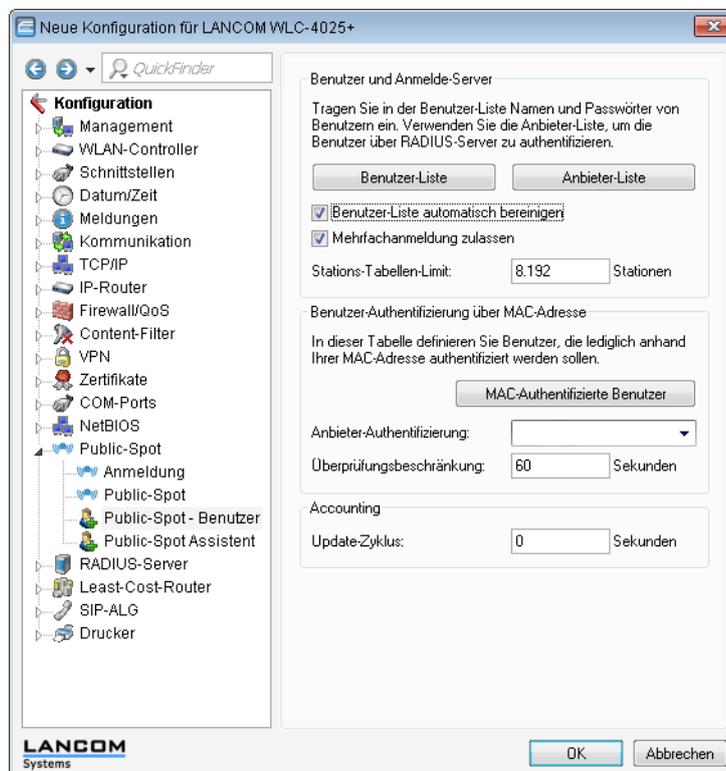
3. Mit dem Eintrag der VLAN-ID '100' für das Gästenetzwerk in der VLAN-Tabelle wird die Public-Spot-Verwendung auf Datenpakete aus diesem virtuellen LAN eingeschränkt. Alle Datenpakete aus anderen VLANs werden ohne Anmeldung am Public Spot weitergeleitet. Achten Sie dabei auch darauf, dass der WEBconfig-Zugang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

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



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

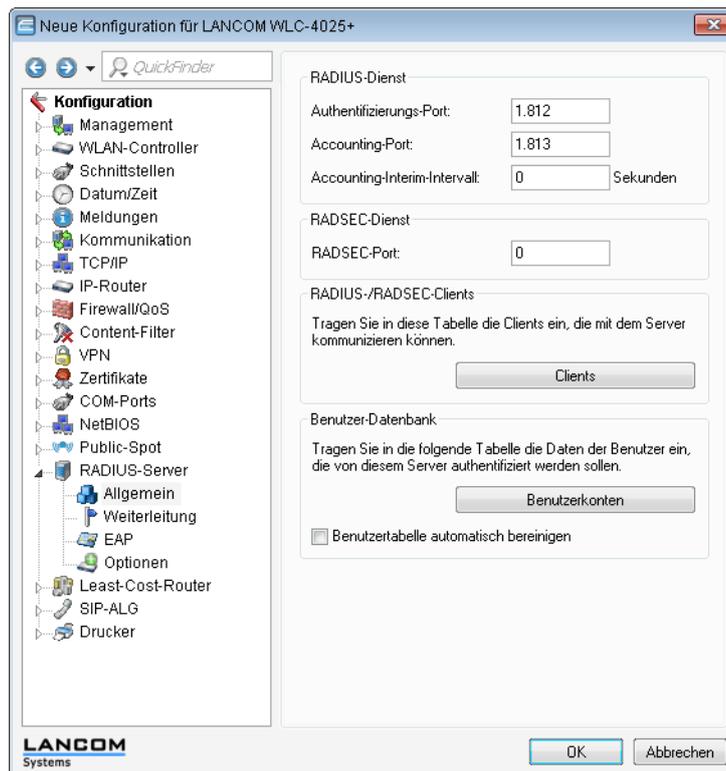
- ! Verwendung nur bis LCOS Version 7.7 notwendig oder wenn die Benutzerliste verwendet wird.



RADIUS-Server für Public-Spot-Nutzung konfigurieren

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

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



! Aktivieren Sie bei Bedarf die Option "Benutzertabelle automatisch bereinigen", damit die nicht mehr benötigten Einträge in der Benutzerdatenbank automatisch gelöscht werden können.

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

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

Anbieter-Liste - Neuer Eintrag

Anbieter: RADIUS-INTERN OK

Backup-Anbieter: Abbrechen

Authentifizierungs-Server

Auth.-Server IP-Adresse: 127.0.0.1

Auth.-Server Port: 1.812

Auth.-Server Schlüssel: Anzeigen
Passwort erzeugen

Absende-Adresse:

Accounting-Server

Acc.-Server IP-Adresse: 127.0.0.1

Acc.-Server Port: 1.813

Acc.-Server Schlüssel: Anzeigen
Passwort erzeugen

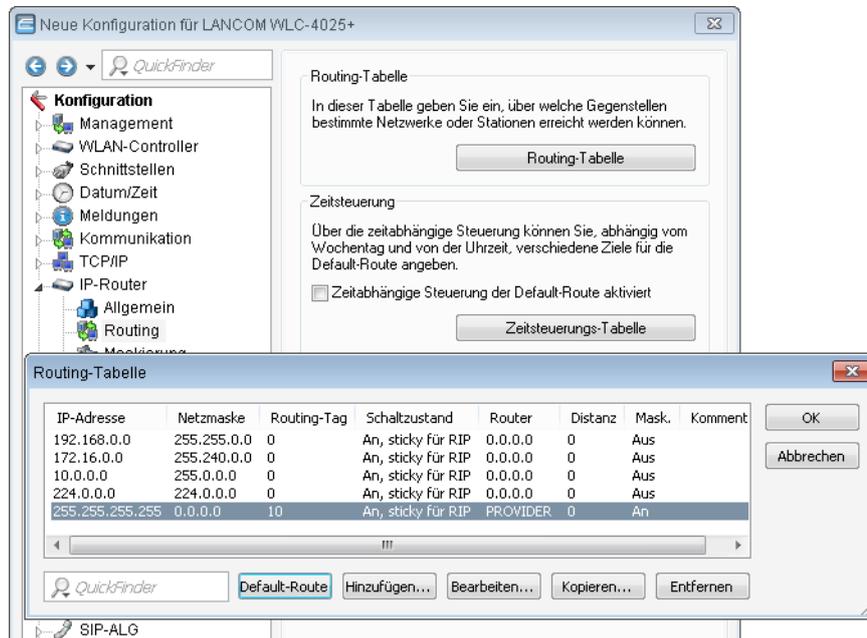
Absende-Adresse:

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

Konfiguration des Internetzugangs für das Gästernetzwerk

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

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



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

1.5 Access Point Verwaltung

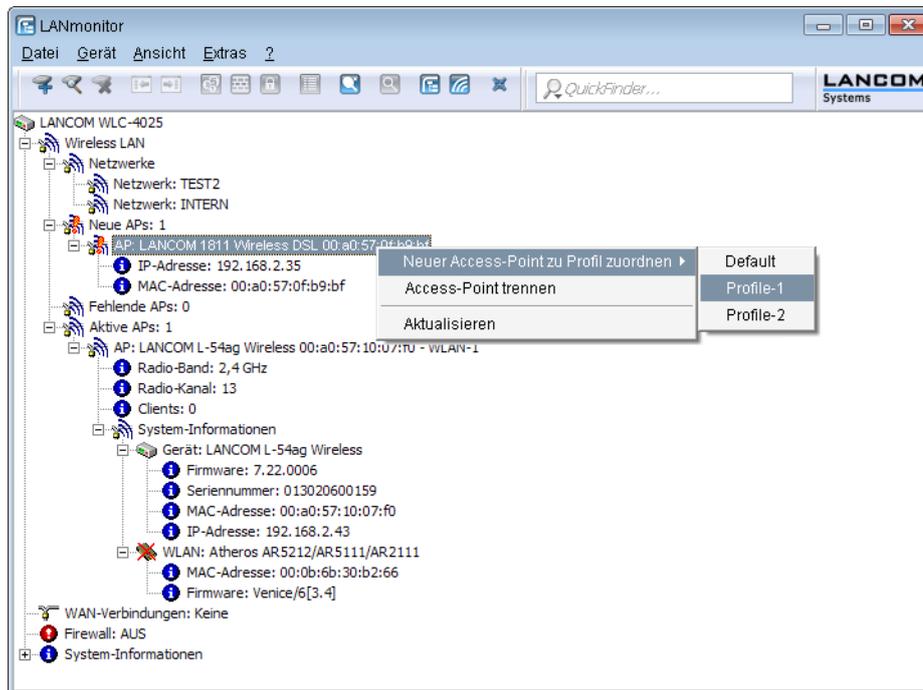
1.5.1 Neue Access Points manuell in die WLAN-Struktur aufnehmen

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

Access Points akzeptieren über den LANmonitor

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

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

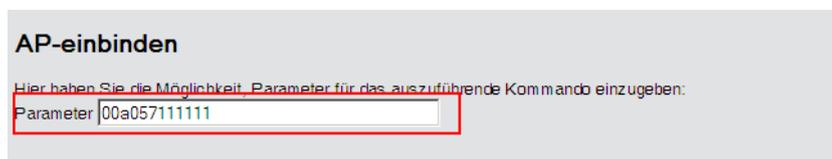


! Mit dem Zuweisen der Konfiguration wird der Access Point in der Access-Point-Tabelle des WLAN-Controllers eingetragen. Es dauert jedoch einige Sekunden, bis der WLAN-Controller dem Access Point auch ein Zertifikat zugewiesen hat und dieser ein aktives Element der zentralen WLAN-Struktur wird. Der neu aufgenommene Access Point wird also für eine kurze Zeit als "Lost AP" 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 Access Points, die kein gültiges Zertifikat haben, für die jedoch ein Eintrag in der Access-Point-Tabelle vorliegt, können über eine Aktion in WEBconfig manuell akzeptiert werden.

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



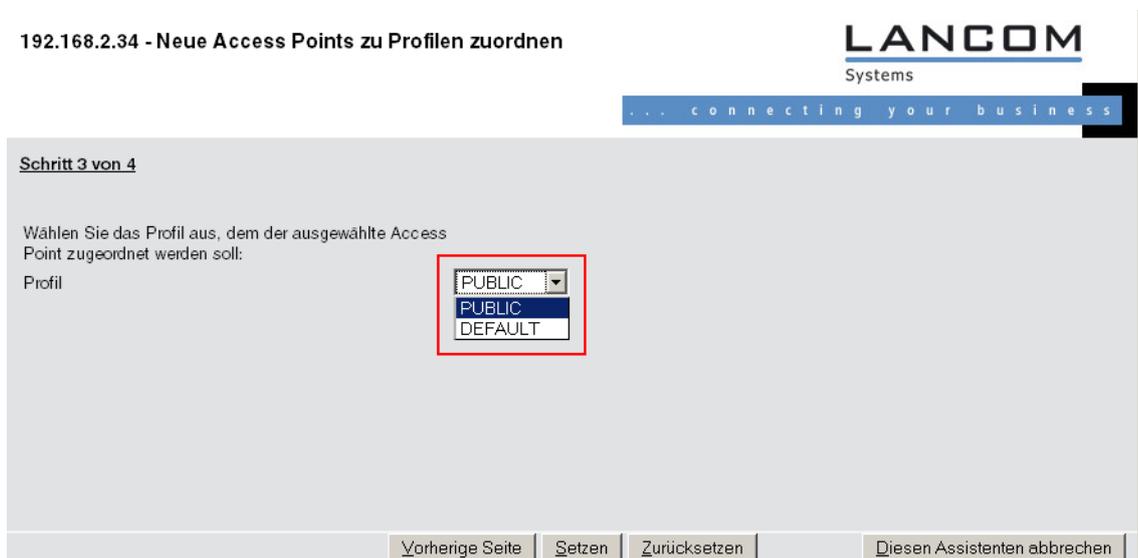
Access Points akzeptieren über WEBconfig mit Zuweisung von Zertifikat und Konfiguration

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

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



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



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

1.5.2 Access Points manuell aus der WLAN-Struktur entfernen

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

- Stellen Sie im Access Point die WLAN-Betriebsart für die WLAN-Module von 'Managed' auf 'Client' oder 'Access-Point' um.
- Löschen Sie im WLAN-Controller die Konfiguration für den Access Point bzw. deaktivieren Sie die **Automatische Zuweisung der Default-Konfiguration** über **LCOS Menübaum > Setup > WLAN-Management > AP-automatisch-einbinden**.
- Trennen Sie die Verbindung zum Access Point unter WEBconfig im Bereich **LCOS Menübaum > Setup > WLAN-Management** mit der Aktion **AP-Verbindung-trennen** oder alternativ im LANmonitor.

4. Geben Sie als Parameter für die Aktion die MAC-Adresse des Access Points ein, zu dem Sie die Verbindung trennen möchten, und bestätigen Sie mit **Ausführen**.

AP-Verbindung-trennen

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

Parameter

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

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

Access Point deaktivieren

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

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

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

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

Access Point dauerhaft aus der WLAN-Struktur entfernen

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

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

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

1.6 Zentrales Firmware- und Skript-Management

Mit einem LANCOM WLAN Controller kann die Konfiguration von mehreren LANCOM Wireless Routern und LANCOM Access Points von einer Stelle aus komfortabel und konsistent verwaltet werden. Mit dem zentralen Firmware- und

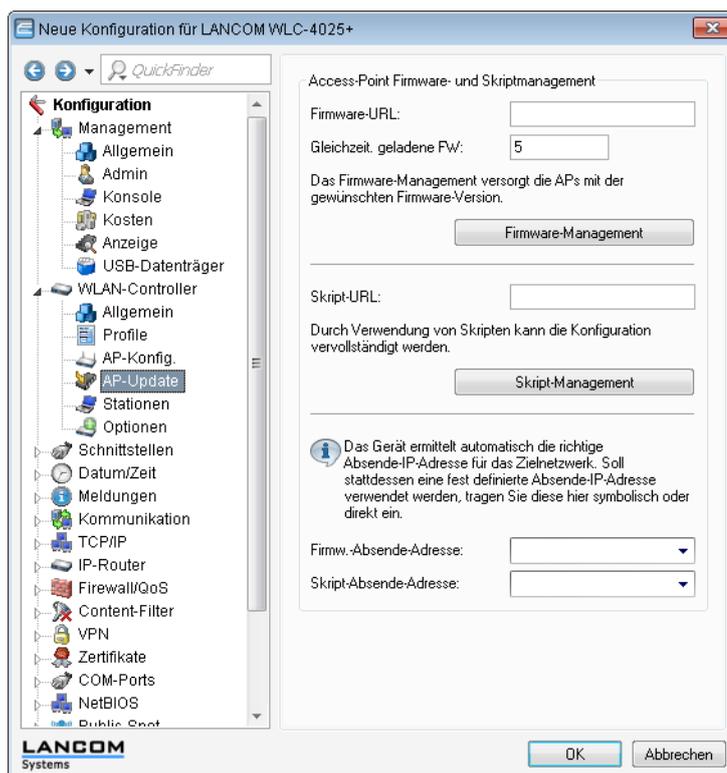
Skript-Management können auch Firmware- und Skript-Uploads auf allen verwalteten WLAN-Geräten automatisch ausgeführt werden.

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

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

Das Update kann in zwei möglichen Zuständen ausgeführt werden:

- Beim Verbindungsaufbau, danach startet der Access Point automatisch neu.
- Wenn der Access Point schon verbunden ist, startet das Gerät danach **nicht** automatisch neu. In diesem Fall wird der Access Point manuell über die Menüaktion **Setup > WLAN-Management > 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**

1.6.1 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

■ Gleichzeitig geladene FW

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

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

- Mögliche Werte: 1 bis 10
- Default: 5

■ Firmware-Absende-IP-Adresse

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

Mögliche Werte:

- Name eines definierten IP-Netzwerks.
- 'INT' für die IP-Adresse im ersten Netzwerk mit der Einstellung 'Intranet'.
- 'DMZ' für die IP-Adresse im ersten Netzwerk mit der Einstellung 'DMZ'.
- Name einer Loopback-Adresse.
- Beliebige andere IP-Adresse.

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

■ MAC-Adresse

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

- Mögliche Werte: Gültige MAC-Adresse.
- Default: Leer

■ Version

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

- Mögliche Werte: Firmware-Version in der Form `x.xx`

- Default: Leer

Allgemeine Einstellungen für das Skript-Management

■ Skript-URL

Pfad zum Verzeichnis mit den Skript-Dateien.

- Mögliche Werte: URL in der Form `Server/Verzeichnis` oder `http://Server/Verzeichnis`
- Default: Leer

■ Skript-Absende-IP-Adresse

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

Mögliche Werte:

- Name eines definierten IP-Netzwerks.
- 'INT' für die IP-Adresse im ersten Netzwerk mit der Einstellung 'Intranet'.
- 'DMZ' für die IP-Adresse im ersten Netzwerk mit der Einstellung 'DMZ'.
- Name einer Loopback-Adresse.
- Beliebige andere IP-Adresse.

Default:

- leer

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

Skript-Management-Tabelle

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-Profiles verwaltet werden. Dabei erfolgt die Zuordnung ebenfalls über die WLAN-Profile, um für die Wireless Router und Access Points mit gleicher WLC-Konfiguration auch das gleiche Skript zu verwenden.

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

■ Skript-Dateiname

Name der zu verwendenden Skript-Datei.

- Mögliche Werte: Dateiname in der Form `*.lcs`
- Default: leer

■ WLAN-Profil

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

- Mögliche Werte: Auswahl aus der Liste der definierten WLAN-Profile.
- Default: Leer

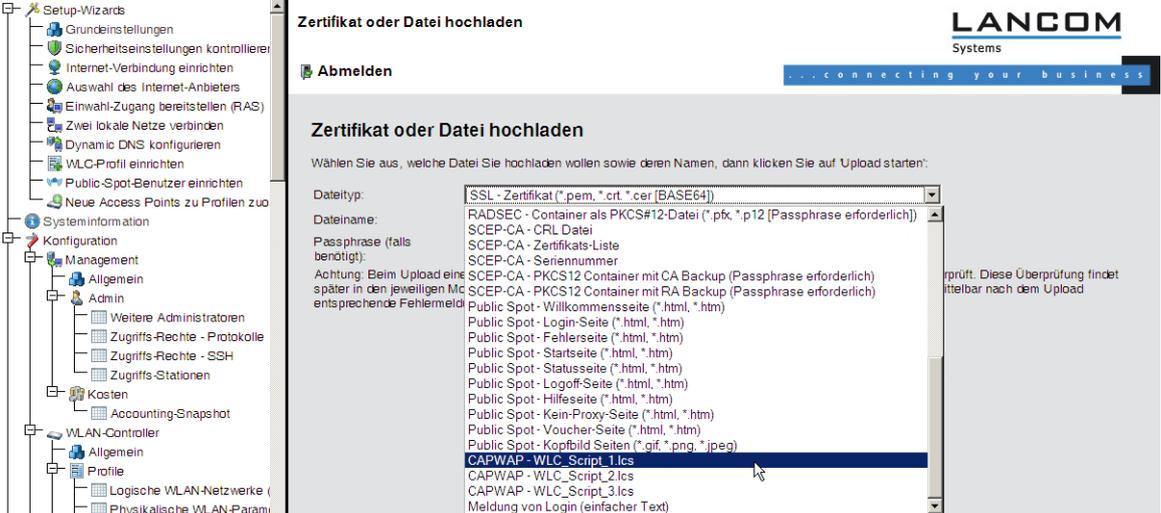
Interner Skript-Speicher (Skript-Management ohne HTTP-Server)

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

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

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

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



1.7 WLAN Layer-3 Tunneling

1.7.1 Einleitung

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

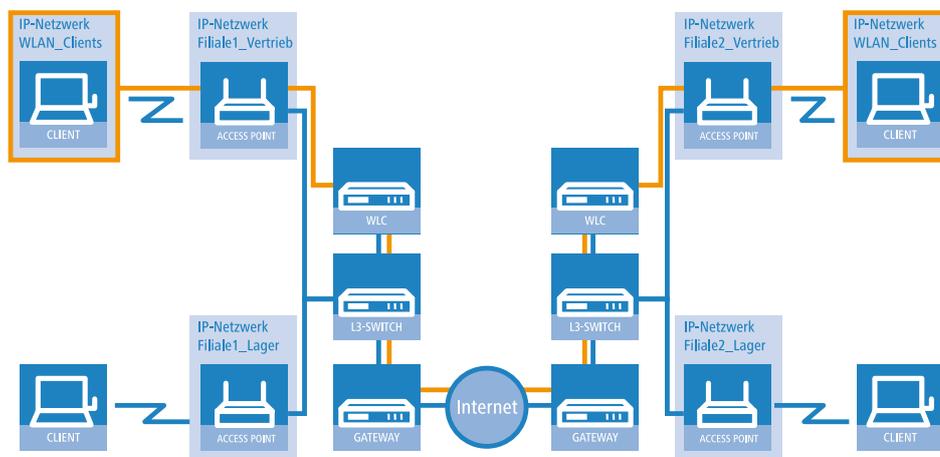
- Der obligatorische Kontrollkanal überträgt Verwaltungsdaten zwischen dem verwalteten Access Point und dem WLAN-Controller.
- Der optionale Datenkanal überträgt die Nutzdaten aus den jeweiligen WLAN-Netzwerken (SSID) zwischen dem verwalteten Access Point und dem WLAN-Controller.

Die optionale Nutzung des Datenkanals zwischen dem verwalteten Access Point und dem WLAN-Controller entscheidet über den Weg der Nutzdaten:

- Wenn Sie den Datenkanal deaktivieren, leitet der Access Point 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 Controllers und des gesamten Netzwerks, weil der Access Point ausschließlich die Verwaltungsdaten über den CAPWAP-Tunnel überträgt, während er die Nutzdaten auf dem kürzesten Weg überträgt.

- Wenn Sie den Datenkanal aktivieren, leitet der Access Point auch die Nutzdaten an den zentralen WLAN-Controller weiter. Dieser Ansatz hat folgende Vorteile:
 - Die Access Points können Netzwerke anbieten, die nur auf dem Controller verfügbar sind, z. B. einen zentralen Internetzugang für einen Public Spot.
 - Die von den Access Points 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 Access Points in verschiedenen IP-Netzwerken angemeldeten WLAN-Clients können ohne Unterbrechung der IP-Verbindung zu einem anderen Access Point roamen, weil die Verbindung fortlaufen vom zentralen Controller verwaltet wird und nicht vom Access Point (Layer-3-Roaming).

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



Overlay-Netzwerk über mehrere IP-Netzwerke hinweg

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

Mehrere WLC innerhalb einer Broadcast-Domäne können das gleiche Overlay-Netzwerk unterstützen. Deaktivieren Sie den WLC-Datenkanal zwischen diesen Controllern (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 Controller in getrennten Netzen die Möglichkeit, den CAPWAP-Datenkanal zu aktivieren.

Die Access Points nutzen virtuelle WLC-Schnittstellen (WLC-Tunnel), um die Datenkanäle der jeweiligen SSIDs zwischen dem Access Point und dem WLAN-Controller zu verwalten. Jeder WLAN-Controller 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.

1.7.2 Tutorials

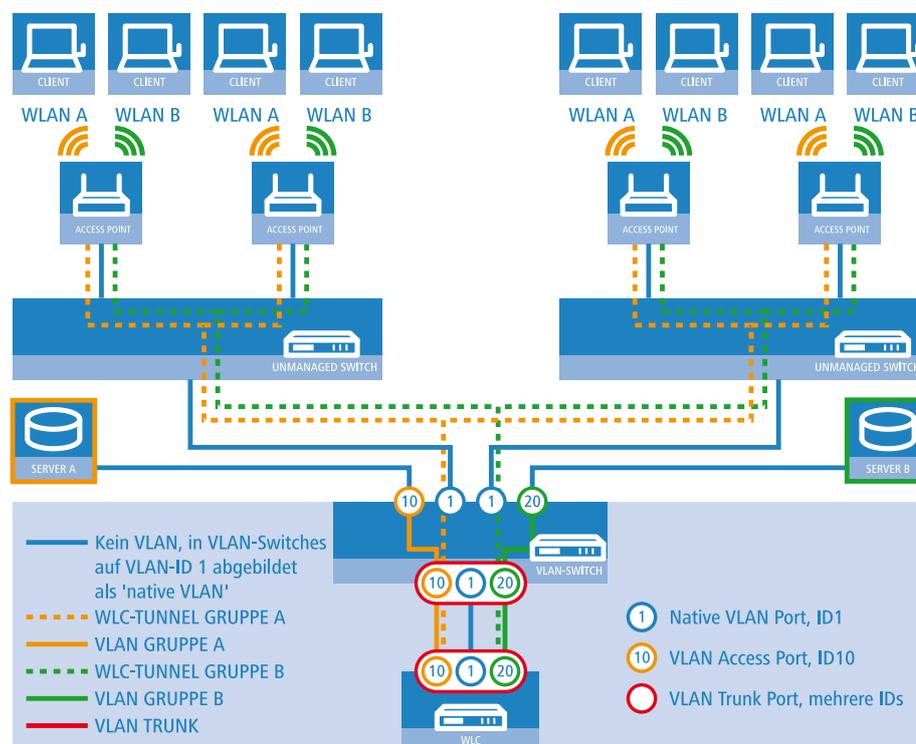
In den folgenden Abschnitten finden Sie konkrete Szenarien mit Schritt-für-Schritt Anleitungen für eine Reihe von Standard-Szenarien beim Einsatz von WLAN Controllern.

"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 WLAN-Controller können Sie die Netze auch mit minimalem Einsatz von VLANs trennen. Über einen CAPWAP-Datentunnel leiten die Access Points die Nutzdaten der angeschlossenen WLAN-Clients direkt zum Controller, der die Daten den entsprechenden VLANs zuordnet. Die VLAN-Konfiguration beschränkt sich dabei auf den Controller 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.



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 Access Points, angeschlossen an den jeweiligen Switch.
- Jeder Access Point 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 WLAN-Controller verwaltet alle Access Points in Netz.
- Ein zentraler, VLAN-fähiger Switch verbindet die Switches der Segmente, die gruppenbezogenen Server und den WLAN-Controller.

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

! Die folgende Beschreibung basiert auf einer funktionsfähigen Grundkonfiguration des WLAN-Controllers. 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)** .

Logische WLAN-Netze für Overlay-Netze

2. Erstellen Sie einen Eintrag in der Liste der physikalischen WLAN-Parameter mit den passenden Einstellungen für Ihre Access Points, 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 Access Points einzuschalten. Stellen Sie die Betriebsart für das Management-VLAN in den Access Points auf

'Ungetagged' ein. In LANconfig finden Sie diese Einstellungen unter **Konfiguration > WLAN-Controller > Profile > Physikalische WLAN-Parameter** .

Physikalische WLAN-Parameter für Overlay-Netze

- 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 > Physikalische WLAN-Profile** .

WLAN-Profile für Overlay-Netze

- Erstellen Sie für jeden verwalteten Access Point einen Eintrag in der Access-Point-Tabelle mit einem passenden Namen und der zugehörigen MAC-Adresse. Ordnen Sie diesem Access Point das zuvor erstellte WLAN-Profil zu. In

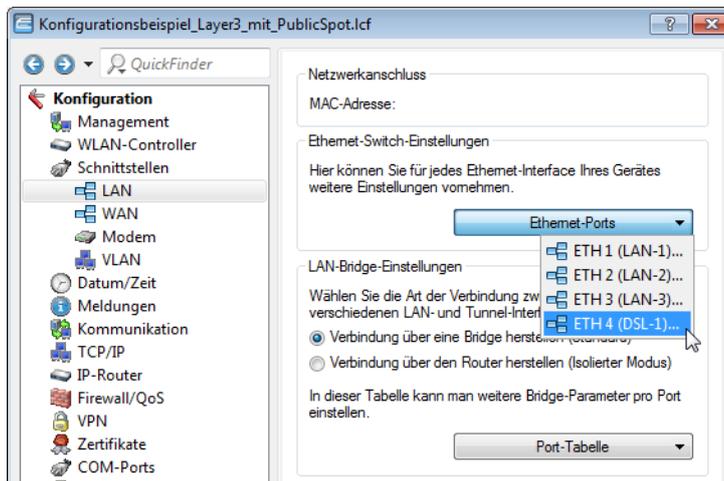
LANconfig finden Sie diese Einstellungen unter **Konfiguration > WLAN-Controller > AP-Konfig > Access-Point-Tabelle** .



Access-Point-Tabelle für Overlay-Netze

Konfiguration der Schnittstellen am WLC

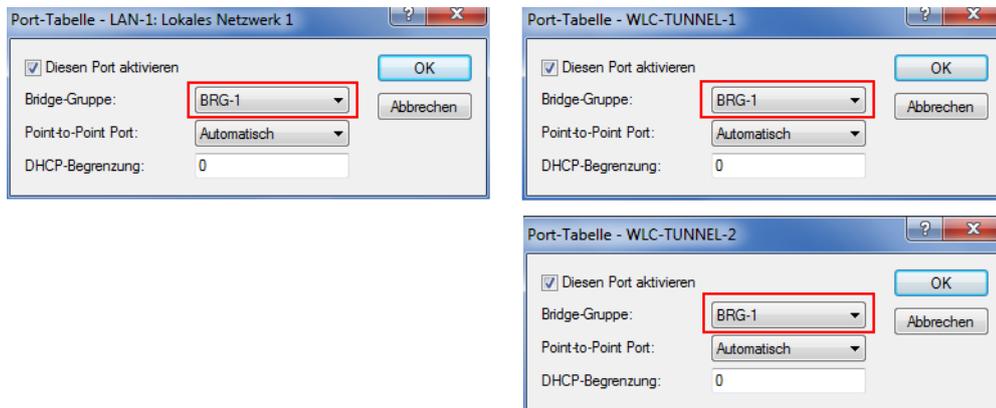
- Ordnen Sie jedem physikalischen Ethernet-Port eine separate logische LAN-Schnittstelle zu, z. B. 'LAN-1'. Stellen Sie sicher, dass die anderen Ethernet-Ports nicht der gleichen LAN-Schnittstelle zugeordnet sind. In LANconfig finden Sie diese Einstellungen unter **Konfiguration > Schnittstellen > LAN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



Ethernet-Einstellungen für Overlay-Netze

- 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

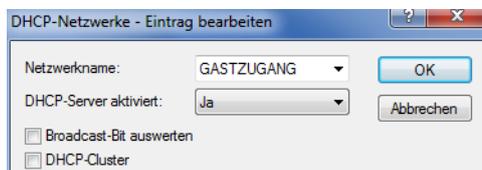
zugeordnet sind. In LANconfig finden Sie diese Einstellungen unter **Konfiguration > Schnittstellen > LAN > Port-Tabelle** .



Port-Einstellungen für Overlay-Netze

! 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.

- Der WLAN-Controller kann optional als DHCP-Server für die Access Points fungieren. Aktivieren Sie dazu den DHCP-Server für das 'INTRANET'. In LANconfig finden Sie diese Einstellungen unter **Konfiguration > TCP/IP > DHCP > DHCP-Netzwerke** .

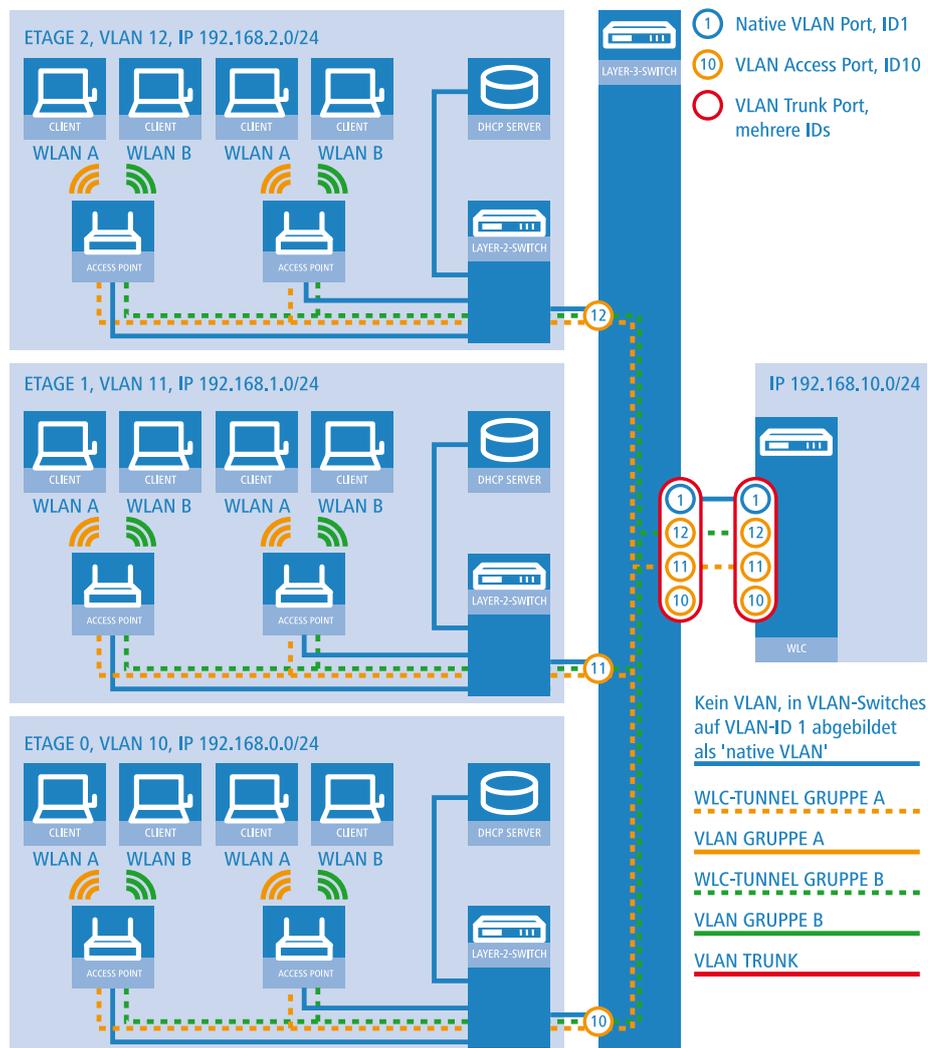


DHCP-Netzwerk für Overlay-Netze

"Layer-3-Roaming"

Die Durchleitung der Nutzdaten aus den WLANs über WLC-Tunnel bis zum Controller 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 Access Points in mehreren Etagen des Gebäudes bieten die beiden SSIDs 'GRUPPE_A' und 'GRUPPE_B' an.



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 Access Points die folgenden Informationen übermittelt:
 - IP-Adresse des Gateways
 - IP-Adresse des DNS-Servers
 - Domänen-Suffix



Die Bereitstellung dieser Informationen ermöglicht es den Access Points, Kontakt mit dem WLC-Controller 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 Access Point 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 Access Points auf Layer 3 direkt über den zentralen WLAN-Controller über die Grenzen der VLANs hinweg.

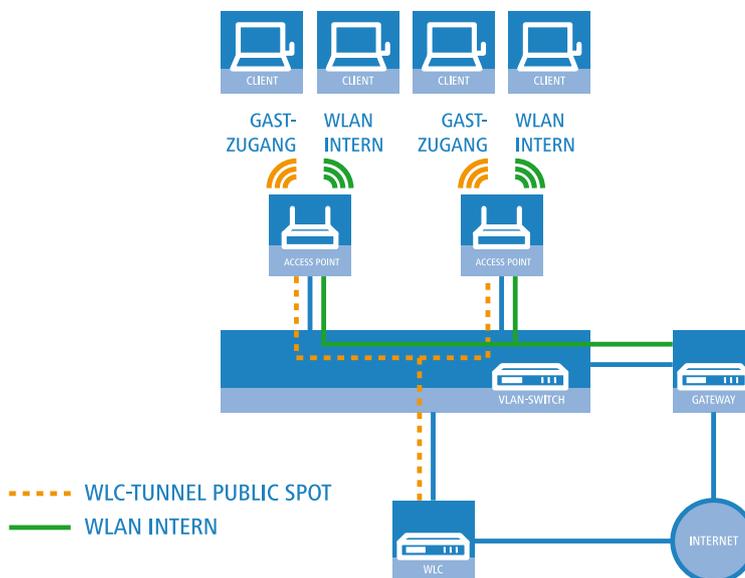
! Die Konfiguration entspricht dem Beispiel *"Overlay Netzwerk": Netzwerke für Access Points trennen ohne VLAN* auf Seite 49.

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 Controller 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 Access Points in allen Bereichen des Gebäudes bieten die beiden SSIDs 'FIRMA' und 'GAESTE' an.



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 Access Points 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 Access Points leiten die Nutzdaten der Gäste-Clients über einen WLC-Tunnel direkt zum WLAN-Controller, 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 mit z. B. mit 'WLC-TUNNEL-1'. Deaktivieren Sie bei der SSID für das Gästernetzwerk 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)**

The screenshot shows the configuration window for a new logical WLAN network. The following settings are highlighted with red boxes:

- Name:** FIRMA
- Netzwerk-Name (SSID):** WLAN-INTERN
- SSID verbinden mit:** LAN am AP

Other visible settings include:

- Logisches WLAN-Netzwerk aktiviert
- Vererbung: Erbt Werte von Eintrag: (dropdown)
- VLAN-Betriebsart: Untagged
- VLAN-ID: 2
- Verschlüsselung: 802.11i (WPA)-PSK
- Schlüssel 1/Passphrase: (redacted) Anzeigen
- Zulässige Freq.-Bänder: 2,4/5 GHz (802.11a)
- Autarker Weiterbetrieb: 0 Minuten
- MAC-Prüfung aktiviert
- SSID-Broad. unterdrücken: Nein
- RADIUS-Accounting aktiviert
- Datenverkehr zulassen zwischen Stationen dieser SSID
- WPA-Version: WPA1/2
- WPA1 Sitzungsschl.-Typ: TKIP
- WPA2 Sitzungsschl.-Typ: AES
- Broadcastgeschwindigk.: 2 Mbit/s
- Client-Bridge-Unterst.: Nein
- Maximalzahl der Clients: 0
- Lange Präambel bei 802.11b verwenden
- 802.11n:
 - Max. Spatial-Streams: Automatisch
 - Kurzes Guard-Intervall zulassen
 - Frame-Aggregation verwenden

Logische WLAN-Netze für interne Nutzung

The screenshot shows the configuration window for a new logical WLAN network. The following settings are highlighted with red boxes:

- Name:** GASTZUGANG
- Netzwerk-Name (SSID):** WLAN-PUBLIC
- SSID verbinden mit:** WLC-TUNNEL-1
- Verschlüsselung:** Keine
- Datenverkehr zulassen zwischen Stationen dieser SSID

Other visible settings include:

- Logisches WLAN-Netzwerk aktiviert
- Vererbung: Erbt Werte von Eintrag: (dropdown)
- VLAN-Betriebsart: Untagged
- VLAN-ID: 2
- Schlüssel 1/Passphrase: (redacted) Anzeigen
- Zulässige Freq.-Bänder: 2,4/5 GHz (802.11a)
- Autarker Weiterbetrieb: 0 Minuten
- MAC-Prüfung aktiviert
- SSID-Broad. unterdrücken: Nein
- RADIUS-Accounting aktiviert
- WPA-Version: WPA1/2
- WPA1 Sitzungsschl.-Typ: TKIP
- WPA2 Sitzungsschl.-Typ: AES
- Broadcastgeschwindigk.: 2 Mbit/s
- Client-Bridge-Unterst.: Nein
- Maximalzahl der Clients: 0
- Lange Präambel bei 802.11b verwenden
- 802.11n:
 - Max. Spatial-Streams: Automatisch
 - Kurzes Guard-Intervall zulassen
 - Frame-Aggregation verwenden

Logische WLAN-Netze für den Gastzugang

- Erstellen Sie einen Eintrag in der Liste der physikalischen WLAN-Parameter mit den passenden Einstellungen für Ihre Access Points, 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** .

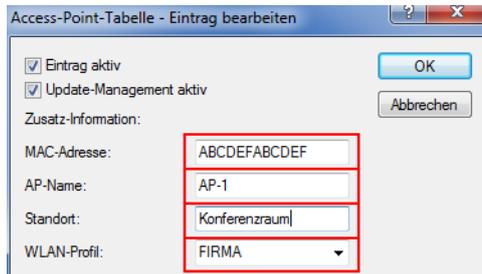
Physikalische WLAN-Parameter für Public-Spot-APs

- 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-Profil** .

WLAN-Profil für Public-Spot-APs

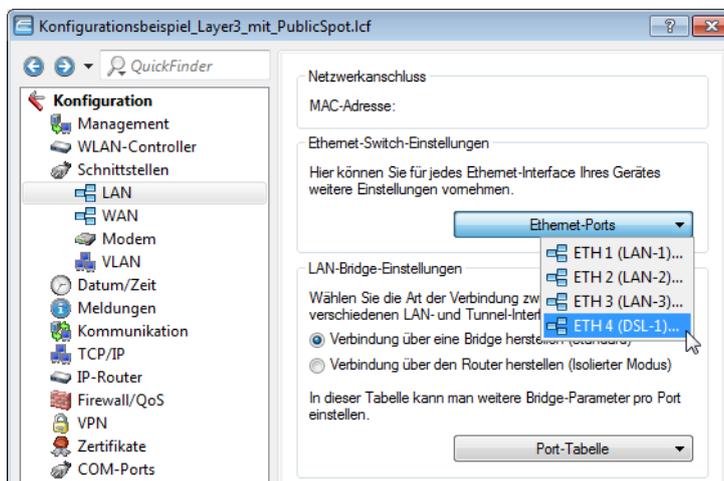
- Erstellen Sie für jeden verwalteten Access Point einen Eintrag in der Access-Point-Tabelle mit einem passenden Namen und der zugehörigen MAC-Adresse. Ordnen Sie diesem Access Point das zuvor erstellte WLAN-Profil zu. In

LANconfig finden Sie diese Einstellung unter **Konfiguration > WLAN-Controller > AP-Konfig > Access-Point-Tabelle** .



Access-Point-Tabelle für Public-Spot-APs

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



Ethernet-Einstellungen für Public-Spot-APs

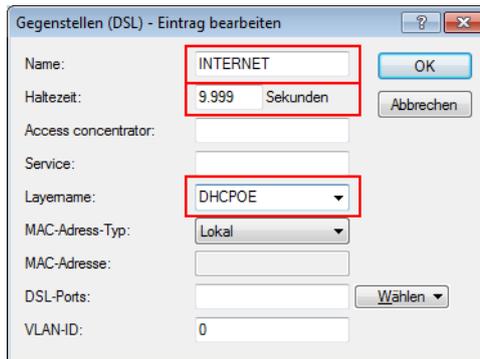
- Überprüfen Sie, dass die logische LAN-Schnittstelle 'WLC-Tunnel 1' keiner Bridge-Gruppe zugeordnet ist. So stellen Sie sicher, dass die anderen LAN-Schnittstellen keine Daten zum Public-Spot-Netzwerk übertragen. In LANconfig finden Sie diese Einstellung unter **Konfiguration > Schnittstellen > LAN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



Port-Einstellungen für Public-Spot-APs

- 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 (DSL)** .



Gegenstellen (DSL) - Eintrag bearbeiten

Name: INTERNET

Haltezeit: 9.999 Sekunden

Access concentrator:

Service:

Layename: DHCPOE

MAC-Adress-Typ: Lokal

MAC-Adresse:

DSL-Ports: Wählen

VLAN-ID: 0

Gegenstelle für Internet-Zugang

- 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 WLAN-Controller 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** .



IP-Netzwerke - Eintrag bearbeiten

Netzwerkname: INTRANET

IP-Adresse: 192.168.1.100

Netzmaske: 255.255.255.0

Netzwerktyp: Intranet

VLAN-ID: 0

Schnittstellen-Zuordnung: Beliebig

Adressprüfung: Flexibel

Schnittstellen-Tag: 1

Kommentar:

IP-Netzwerk für interne Nutzung



IP-Netzwerke - Eintrag bearbeiten

Netzwerkname: GASTZUGANG

IP-Adresse: 192.168.200.1

Netzmaske: 255.255.255.0

Netzwerktyp: Intranet

VLAN-ID: 0

Schnittstellen-Zuordnung: Beliebig

Adressprüfung: Flexibel

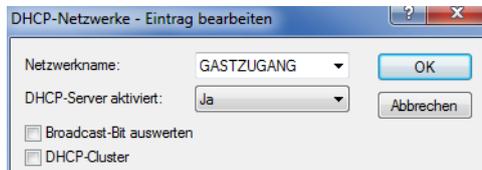
Schnittstellen-Tag: 2

Kommentar:

IP-Netzwerk für Gastzugang

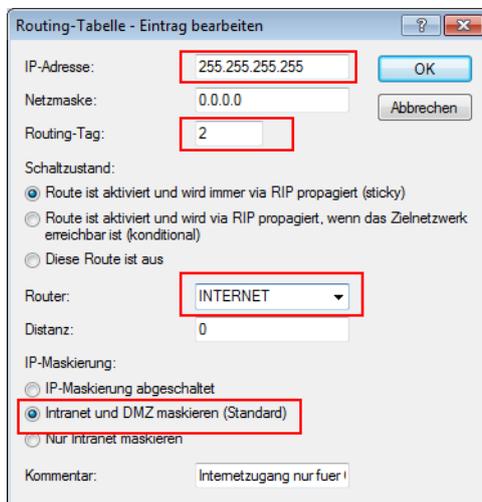
- Der WLAN-Controller kann als DHCP-Server für die Access Points und die angemeldeten WLAN-Clients fungieren. Aktivieren Sie dazu den DHCP-Server für das 'INTRANET' und den 'GASTZUGANG'. In LANconfig finden Sie diese Einstellung unter **Konfiguration > TCP/IP > DHCP > DHCP-Netzwerke** .

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



DHCP-Netzwerk für Gastzugang

10. Erstellen Sie eine neue Standard-Route in der Routing-Tabelle, welche die Daten aus dem Gästernetz auf den Internet-Zugang des WLAN-Controllers 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**.



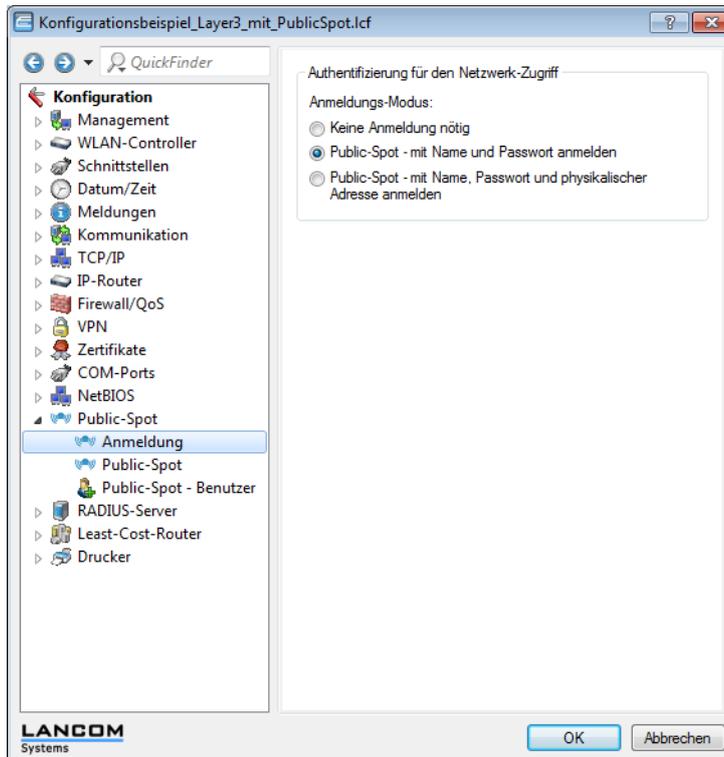
Routing-Eintrag für Internet-Zugang

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 > Public-Spot-Interfaces**.



Aktivierung der Benutzer-Anmeldung für den WLC-Tunnel

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



Aktivierung der Anmeldung über den Public-Spot

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

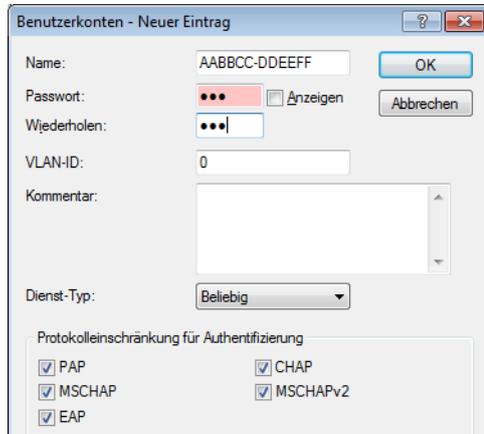
- ! Eine Beispielkonfiguration des Public Spots finden Sie im Tutorial [Virtualisierung und Gastzugang über LANCOM WLAN Controller](#).

1.8 RADIUS

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

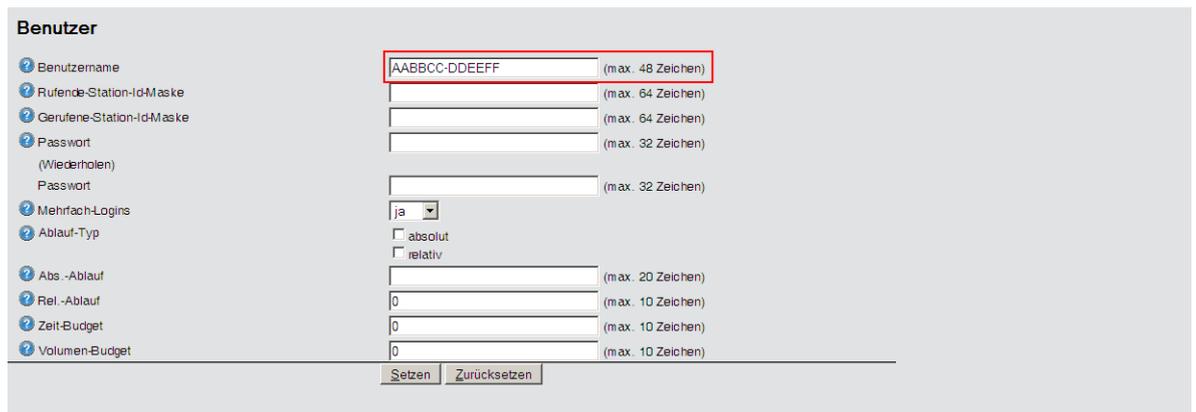
Bei der Nutzung von RADIUS zur Authentifizierung der WLAN-Clients kann neben einem externen RADIUS-Server auch die interne Benutzertabelle der LANCOM WLAN Controller genutzt werden, um nur bestimmten WLAN-Clients anhand ihrer MAC-Adresse den Zugang zum WLAN zu erlauben.

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



Alternativ tragen Sie die zugelassenen MAC-Adressen über WEBconfig ein unter **LCOS Menübaum > Setup > RADIUS > Server > Benutzer**.

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



1.8.2 Externer RADIUS-Server

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

Management-Netz heraus erreichen können. Ist der RADIUS-Server in einem anderen IP-Netz, muss über das IP-Parameter-Profil insbesondere das Gateway definiert werden.

LANconfig: **WLAN Controller > Stationen > RADIUS-Server**

WEBconfig: **LCOS-Menübaum > Setup > WLAN Management > RADIUS-Server**

- **Typ:** Type der RADIUS Anwendung.

Mögliche Werte:

Konto oder Zugang

Default:

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

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

Mögliche Werte:

Gültige IP-Adresse.

Default:

leer

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

Mögliche Werte:

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

Default:

0

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

Mögliche Werte:

max. 31 ASCII-Zeichen.

Default:

leer

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 Access Points befinden, kann diese Zuweisung über die SSID in Verbindung mit einem bestimmten IP-Netzwerk realisiert werden. Wechseln die WLAN-Clients hingegen

häufig die Position und buchen sich dann bei unterschiedlichen Access Points ein, befinden sie sich je nach Konfiguration in einem anderen IP-Netzwerk.

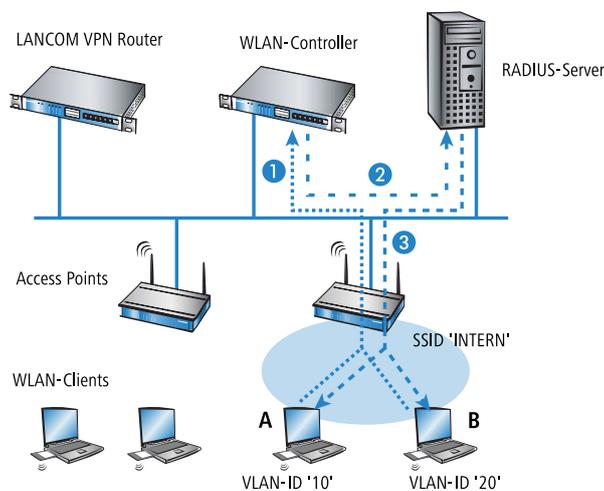
Um die WLAN-Clients **unabhängig** von dem WLAN-Netzwerk, in dem sie sich gerade eingebucht haben, in ein bestimmtes Netzwerk zu leiten, können dynamisch zugewiesene VLANs genutzt werden. Anders als bei den statisch konfigurierten VLAN-IDs für eine bestimmte SSID wird die VLAN-ID dabei dem WLAN-Client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

Beispiel:

- Die WLAN-Clients der Mitarbeiter buchen sich über einen Access Point in das WPA2-gesicherte WLAN mit der SSID 'INTERN' ein. Bei der Anmeldung werden die RADIUS-Anfragen der WLAN-Clients an den Access Point gestellt. Wenn sich das entsprechende WLAN-Interface in der Betriebsart 'Managed' befindet, werden die RADIUS-Anfragen automatisch an den WLAN-Controller weitergereicht. Dieser leitet die Anfragen seinerseits an den konfigurierten RADIUS-Server weiter. Der RADIUS-Server kann die Zugangsberechtigung der WLAN-Clients prüfen. Darüber hinaus kann er allerdings auch z. B. anhand der MAC-Adresse eine bestimmte VLAN-ID für die jeweilige Abteilung zuweisen. Dabei erhält z. B. der WLAN-Client aus dem Marketing die VLAN-ID '10' und WLAN-Client aus der Entwicklung die '20'. Wenn für den Benutzer keine VLAN-ID definiert ist, wird die Haupt-VLAN-ID der SSID verwendet.
- Die WLAN-Clients der Gäste buchen sich über den gleichen Access Point in das nicht gesicherte WLAN mit der SSID 'PUBLIC' ein. Diese SSID ist statisch auf die VLAN-ID '99' gebunden und leitet die Gäste so in ein bestimmtes Netzwerk. Statische und dynamische VLAN-Zuweisung können also sehr elegant parallel genutzt werden.

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

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



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

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

4. Für eine Weiterleitung der RADIUS-Anfragen an einen anderen RADIUS-Server tragen Sie dessen Adresse über LANconfig in die Liste der Forwarding-Server im Konfigurationsbereich 'RADIUS-Server' auf der Registerkarte **Forwarding** ein. Alternativ tragen Sie die externen RADIUS-Server über WEBconfig ein unter **LCOS Menübaum > Setup > RADIUS > Server > Weiterleit-Server**. Stellen Sie außerdem den Standard-Realm sowie den leeren Realm ein, um auf unterschiedliche Benutzerinformationen (mit unbekanntem oder ganz ohne Realm) gezielt reagieren zu können.
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.

1.9 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)**

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

■ RADIUS-Accounting aktiviert

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

Mögliche Werte:

- ja, nein

Default:

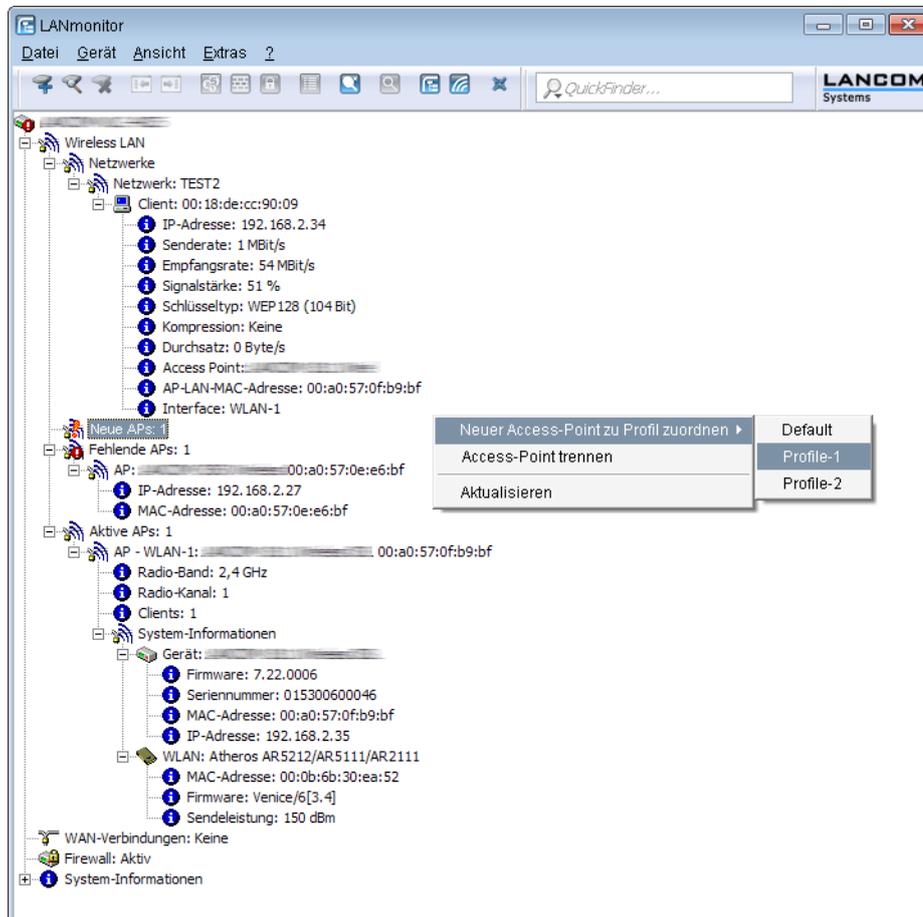
- nein



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

1.10 Anzeigen und Aktionen im LANmonitor

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



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

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

- **Neuen Access Point zu Profil zuordnen**

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

- **Access Point trennen**

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

- **Aktualisieren**

Aktualisiert die Anzeige des LANmonitors.

1.11 Funkfeldoptimierung

Mit der Auswahl des Kanals in der Kanal-Liste wird der Teil des Frequenzbandes festgelegt, den ein Access Point für seine logischen WLANs verwendet. Alle WLAN-Clients, die sich mit einem Access Point verbinden wollen, müssen den gleichen Kanal im gleichen Frequenzband verwenden. Im 2,4-GHz-Band stehen je nach Land die Kanäle 1 bis 13, im 5-GHz-Band die Kanäle 36 bis 64 zur Verfügung. Auf einem Kanal kann dabei zeitgleich jeweils nur ein Access Point Daten übertragen. Um in der Funkreichweite eines anderen Access Points ein WLAN mit maximaler Bandbreite betreiben zu können, muss jeder Access Point einen separaten Kanal nutzen – anderenfalls müssen sich die WLANs die Bandbreite des Kanals teilen.

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

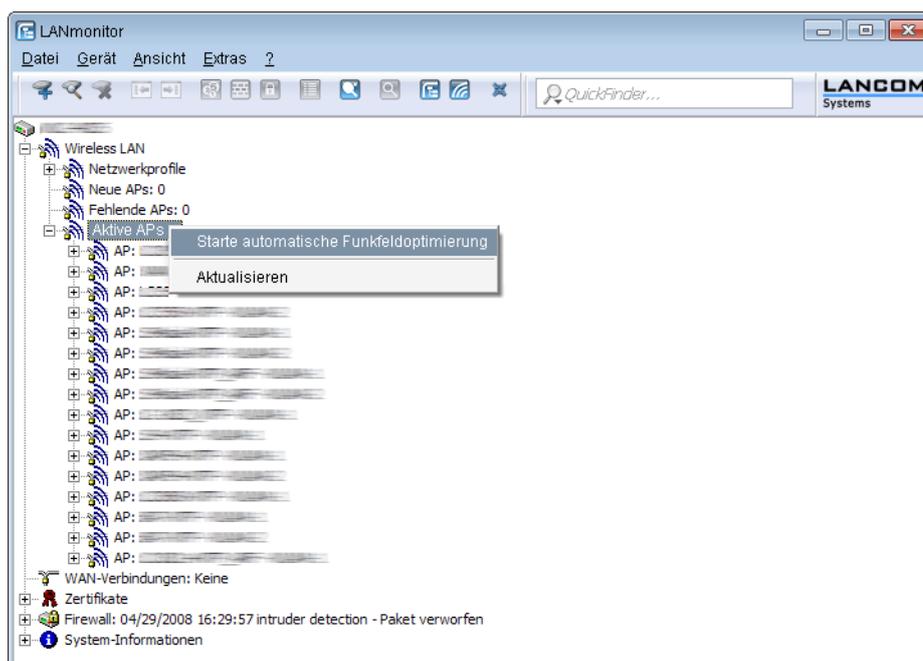
In größeren Installationen mit mehreren Access Points ist es manchmal schwierig, für jeden Access Point einen geeigneten Kanal einzustellen. Mit der automatischen Funkfeldoptimierung bieten die LANCOM WLAN Controller ein Verfahren, um die optimalen Kanäle der Access Points für das 2,4-GHz- und 5-GHz-Band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

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

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

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

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



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

1.12 Kanallastanzeige im WLC-Betrieb

Für die von einem WLAN Controller verwalteten Access Points 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.

The screenshot shows the WLANmonitor application window. The left sidebar displays a tree view of groups including 'WLANmonitor', 'Access Points (24)', 'WLAN-Controller', 'Aachen (2)', 'Hausnetz (2)', 'Munich (3)', 'Rogue AP Detection', 'Alle APs (1012)', 'Neue APs (576)', 'New APs (198)', 'Own APs (48)', 'Rogue APs', 'Unbekannte APs', 'Bekannte APs', and 'Eigene APs (19)'. The main area is divided into three sections: 'Controller', 'Access-Points', and 'Clients'.

Controller Table:

Name	Neue...	Fehlende APs	Aktive APs	Clients	IP-A
[Icon]	0	0	2	5	[Icon]
[Icon]	0	0	14	30	[Icon]

Access-Points Table:

Name	Interfa...	Clie...	Band	K...	Min. Kanall...	Max. Kanall...	Durschn. Kanallast
[Icon]	WLAN-1	0	2,4 GHz	1	23 %	80 %	58 %
[Icon]	WLAN-1	2	2,4 GHz	1	18 %	66 %	40 %
[Icon]	WLAN-1	0	2,4 GHz	1	29 %	75 %	54 %
[Icon]	WLAN-1	3	2,4 GHz	1	26 %	77 %	54 %
[Icon]	WLAN-1	3	2,4 GHz	1	18 %	55 %	31 %
[Icon]	WLAN-1	1	2,4 GHz	1	26 %	71 %	54 %
[Icon]	WLAN-1	3	2,4 GHz	1	23 %	70 %	46 %
[Icon]	WLAN-2	0	5 GHz	56	1 %	3 %	1 %

Clients Table:

MAC-Adresse	Identifikation	Sig...	Controller	Access-Point	Netzwerkprofil
[Icon]	[Icon]	17 %	[Icon]	[Icon]	[Icon]
[Icon]	[Icon]	22 %	[Icon]	[Icon]	[Icon]
[Icon]	[Icon]	42 %	[Icon]	[Icon]	[Icon]
[Icon]	[Icon]	31 %	[Icon]	[Icon]	[Icon]
[Icon]	[Icon]	73 %	[Icon]	[Icon]	[Icon]
[Icon]	[Icon]	55 %	[Icon]	[Icon]	[Icon]
[Icon]	[Icon]	26 %	[Icon]	[Icon]	[Icon]

1.13 Sicherung der Zertifikate

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

Wenn mehrere WLAN-Controller in der gleichen WLAN-Infrastruktur parallel eingesetzt werden (Load-Balancing) oder wenn ein Gerät ersetzt bzw. neu konfiguriert werden muss, sollten immer die gleichen Root-Zertifikate verwendet werden, um einen reibungslosen Betrieb der verwalteten Access Points 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 LANCOM WLAN Controller 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 PKCS12-Container gespeichert, der mit einer Passphrase geschützt ist.

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

Erstelle-PKCS12-Backup-Dateien

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

Parameter

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

1 Sichern und Wiederherstellen weiterer Dateien der SCEP-CA

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

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

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

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

1. Wählen Sie **Dateimanagement > Zertifikat oder Datei herunterladen** .
2. Wählen Sie dann als Dateityp nacheinander die oben aufgeführten Einträge und bestätigen Sie mit **Download starten**.

Zertifikat oder Datei herunterladen

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

Dateityp:

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

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

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

- ! 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.

2 Zertifikats-Backup in das Gerät einspielen

1. Wählen Sie **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.

```
del controller_*
del eaptls_*
```

6. Danach muss im Verzeichnis **Setup > Certificates > SCEP-Client** der Befehl `Reinit` aufgerufen werden:

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

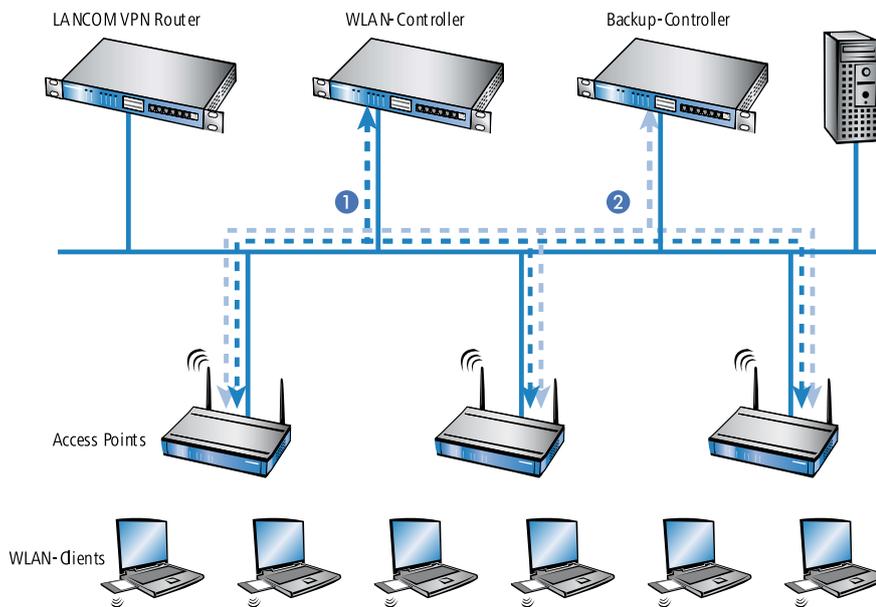
1.14 Backuplösungen

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

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

1 Backup mit redundanten WLAN-Controllern

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



1. Stellen Sie auf beiden LANCOM WLAN Controllern **1** und **2** die gleiche Uhrzeit ein.
2. Schalten Sie die CA auf dem Backup-Controller aus (WEBconfig: LCOS-Menübaum > Setup > Zertifikate > SCEP-CA > Aktiv).

- Erstellen Sie in der Konfiguration des SCEP-Clients im Backup-Controller einen neuen Eintrag in der CA-Tabelle (in LANconfig unter **Zertifikate > SCEP-Client > CA-Tabelle**). Darin wird die CA des Haupt-WLAN-Controllers eingetragen.

- Geben Sie als URL die IP-Adresse oder den DNS-Namen des Haupt-WLAN-Controllers 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
- 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
- Wenn im Backup-Controller zuvor schon eine SCEP-Konfiguration aktiv war, müssen folgende Aktionen unter WEBconfig ausgeführt werden (**Experten-Konfiguration > 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 WLAN-Controller **1** wie gewünscht mit allen Profilen und der zugehörigen Access-Point-Tabelle. Die Access Points bauen dann die Verbindung zum ersten WLAN-Controller auf. Die Access Points erhalten von diesem WLAN-Controller ein gültiges Zertifikat und eine Konfiguration für die WLAN-Module.
8. Übertragen Sie die Konfiguration des ersten WLAN-Controllers **1** z. B. mit LANconfig auf den Backup-Controller **2**. Dabei werden auch die Profile und die Access-Point-Tabellen mit den MAC-Adressen der Access Points auf den Backup-Controller übertragen. Alle Access Points bleiben in diesem Zustand weiterhin beim ersten WLAN-Controller angemeldet.

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

-
-  Die Access Points bleiben in diesem Szenario so lange in der Verwaltung des Backup-Controllers, bis dieser entweder selbst einmal nicht erreichbar ist oder bis sie manuell getrennt werden.
 -  Mit der Einstellung des autarken Weiterbetriebs können die Access Points auch während der Suche nach einem Backup-Controller mit der aktuellen WLAN-Konfiguration in Betrieb bleiben, und die WLAN-Clients bleiben eingebucht.

1.14.1 Backup mit primären und sekundären WLAN-Controllern

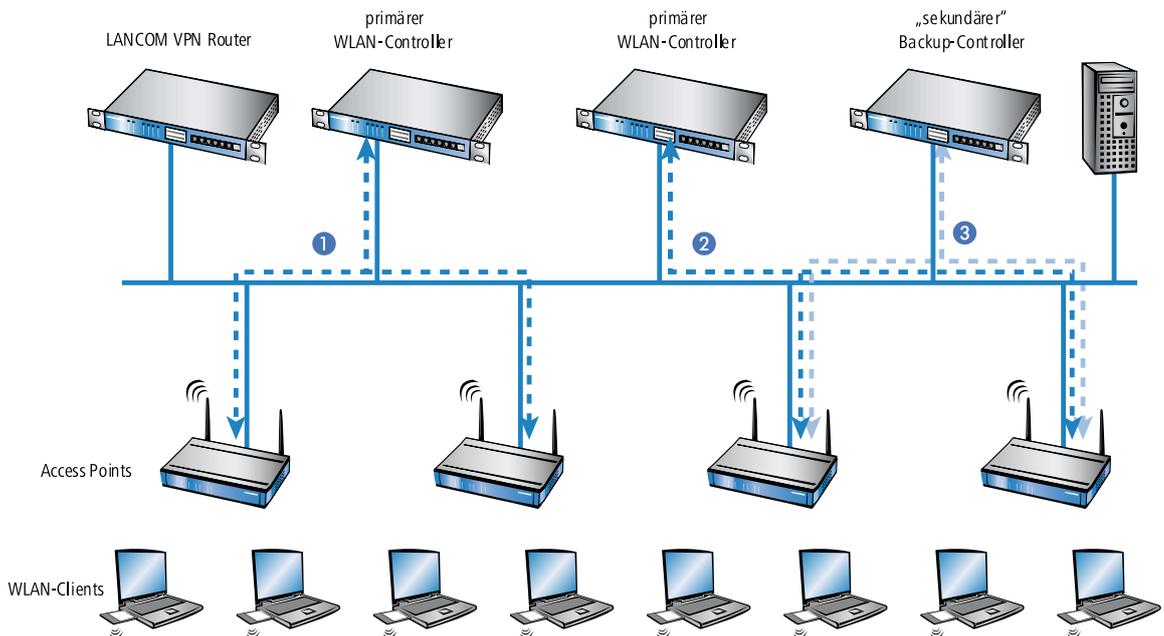
Mit einer zweiten Form des Backups können Sie für eine größere Anzahl von "primären" WLAN-Controllern einen gemeinsamen, "sekundären" Backup-Controller bereitstellen. Beim Ausfall eines WLAN-Controllers bleiben die Access Points zwar in Betrieb, arbeiten allerdings mit der aktuellen Konfiguration der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

1.14.2 Primäre und sekundäre Controller

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

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

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



! Ein LANCOM WLAN Controller kann nun in seiner Access-Point-Tabelle die fünffache Anzahl der von ihm selbst maximal verwalteten Access Points aufnehmen. Für jeweils fünf WLAN-Controller (mit gleicher Ausstattung) reicht also ein zusätzlicher WLAN-Controller aus, um eine vollständige Absicherung bei Ausfall eines Gerätes zu realisieren.

1. Stellen Sie auf allen LANCOM WLAN Controllern **1** und **2** und **3** die gleiche Uhrzeit ein.
2. Übertragen Sie die CA- und RA-Zertifikate aus dem ersten primären WLAN-Controller **1** in den zweiten, primären **2** und den sekundären "Backup-Controller" **3**.
3. Konfigurieren Sie den ersten WLAN-Controller **1** wie gewünscht mit den Profilen und der zugehörigen Access-Point-Tabelle für eine Hälfte der Access Points. Dieses WLAN-Controller wird somit zum primären Controller für die bei ihm eingetragenen Access Points.

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

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

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

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

-
-  Sollte WLAN-Controller **A** nicht ausgelastet sein, weil z. B. einige "seiner" Access Points ausgeschaltet sind, so könnten sich auch einige der suchenden Access Points bei diesem anmelden. WLAN-Controller **A** bleibt für diese Access Points aber ein "sekundärer" Controller, da er nicht über Konfigurationsprofile für diese Geräte verfügt. Wird in diesem Fall einer der Access Point wieder eingeschaltet, der über einen Eintrag in der Access-Point-Tabelle von WLAN-Controller **A** verfügt, nimmt **A** diesen reaktivierten Access Point wieder auf und trennt sich dafür von einem der Access Points im Backup-Fall.
-
-  Mit der Einstellung des autarken Weiterbetriebs bleiben die Access Points auch während der Suche nach einem Backup-Controller mit der aktuellen WLAN-Konfiguration in Betrieb, die WLAN-Clients können weiterhin alle Funktionen nutzen.

Index

A

Access Points manuell akzeptieren [40](#)

B

Bridge-Gruppe [53](#)

C

CA

[8](#)

Certification Authority [8](#)

CAPWAP

[4, 8, 23, 47](#)

Control And Provisioning of Wireless Access Points [4](#)

Datenkanal [47](#)

Kontrollkanal [23, 47](#)

Übertragungskanäle [47](#)

CAPWAP-Datentunnel [49](#)

CAPWAP-Standard

[47–48](#)

Datenkanal-Vorteile [48](#)

Nutzdaten [47](#)

D

Datenkanal

[5](#)

CAPWAP [5](#)

Discovery Request Message

[7](#)

Zentrales WLAN-Management [7](#)

DNS-Auflösung

[7](#)

Zentrales WLAN-Management [7](#)

E

EAP

[5](#)

Zentrales WLAN-Management [5](#)

K

Konfiguration WLAN-Controller

[14–15](#)

Auto-Accept [14](#)

Automatische Zuweisung der Default-Konfiguration [15](#)

WLAN-Profil [15](#)

Kontrollkanal

[5, 23](#)

CAPWAP [5](#)

Verschlüsselung [23](#)

L

Layer-3-Roaming

[53–54](#)

Anwendungsbeispiel [54](#)

Local-MAC

[6](#)

Zentrales WLAN-Management [6](#)

M

MAC-Funktionen

[5](#)

Zentrales WLAN-Management [5](#)

N

Netzwerke

[49](#)

trennen [49](#)

Netzwerktrennung

[49](#)

Anwendungsbeispiel [49](#)

Nutzdaten

[53](#)

Durchleitung aus WLANs [53](#)

O

Overlay Netzwerk

[49, 55](#)

Konfiguration Public Spot [55](#)

Overlay-Netzwerk [48](#)

P

PHY-Layer

[5](#)

Zentrales WLAN-Management [5](#)

Public Spot

[55](#)

WLAN-Controller [55](#)

R

RADIUS

[5](#)

Zentrales WLAN-Management [5](#)

Remote-MAC

[5](#)

Zentrales WLAN-Management [5](#)

Roaming

[53](#)

Layer-3 [53](#)

S

SCEP

[8](#)

Simple Certificate Encryption Protocol [8](#)

Smart-Controller

[6](#)

Zentrales WLAN-Management [6](#)

Split-MAC

[5](#)

Zentrales WLAN-Management [5](#)

T

Trennen von Netzwerken [49](#)

V

Verschlüsselung

[5, 7](#)

DTLS [5, 7](#)

TLS [5](#)

Zufallszahl [7](#)

W

WLAN-Controller

[4, 49, 55](#)

Aufgaben [4](#)

Public Spot [55](#)

WLAN-Einstellungen [50](#)

WLAN-Parameter [50](#)

WLAN-Profil [51](#)

WLC-Schnittstellen (virtuelle) [48](#)

WLC-Tunnel [48, 50](#)

Z

Zertifikat

[7, 14](#)

SCEP [7](#)

Zertifikate

[70](#)

PKCS12-Container [70](#)