Einführung in den bintec elmeg WLAN-Controller

1 Überblick über die Funktionen

Der bintec elmeg WLAN-Controller bietet Ihnen folgende Vorteile beim Management Ihrer WLAN-Infrastruktur:

- Assistenten-geführte Schnellinstallation des WLAN-Netzes in maximal drei Schritten.
- Vollautomatische Erkennung und Inbetriebnahme weiterer bintec elmeg Access-Points mit allen Einstellungen ihres (Multi-SSID-)WLAN-Netzwerks, sobald diese mit dem WLAN-Controller per LAN verbunden sind.
- Zentrale einfache Verwaltung und Konfiguration aller Access-Points:
  - Zentral steuerbare Firmware-Updates für alle gemanagten Access-Points.
  - Die Konfiguration wird zentral im WLAN-Controller gespeichert und wird u.a. nach einem Stromausfall automatisch neu auf die Access-Points verteilt.
  - Das Hinzufügen neuer SSIDs erfordert nur wenige Klicks und ist innerhalb weniger Sekunden erledigt. Ebenso schnell werden Änderungen an SSIDs und anderer Einstellungen auf alle verknüpften APs ausgerollt.
- Parallele Unterstützung aller WLAN-Generationen einschließlich WiFi 6 (802.11ax) mit optimierten Voreinstellungen, sowie Anzeige des unterstützten Funktionsumfanges eines gemanagten Access-Points, wie mögliche Funkfrequenzen oder ob er WPA3 kann.
- Multi-SSID-WLAN-Netzwerke mit sicherer Trennung per VLAN und Firewall für Gastnetzwerke und andere Szenarien, Unterstützung aller gängigen WLAN-Verschlüsselungsstandards inklusive WPA3 sowie (mit einem externen Radius-Server) WPA-Enterprise-Authentifizierung (802.1X) von WLAN-Clients für Hochsicherheitslösungen.
- Access-Points an öffentlich zugänglichen Stellen sind nicht länger ein Sicherheitsrisiko:
  - Alle WLAN-Netzwerkeinstellungen inklusive Passwörter werden nur flüchtig im Arbeitsspeicher des AP gehalten und nicht im AP abgespeichert. Sobald die Online-Verbindung zum WLAN-Controller unterbrochen wird, startet der AP automatisch neu und ist wieder im Auslieferungszustand. WLAN-Passwörter etc. können deshalb nicht durch Diebstahl der APs in unbefugte Hände gelangen.
  - Sobald ein Access-Point vom WLAN-Controller gemanagt ist, ist der direkte Konfigurations- und Monitoring-Zugriff auf den AP gesperrt, sodass er auch im Betrieb nicht unbefugt ausgelesen werden kann.
- Automatisiertes Frequenzmanagement:
  - Integrierte Kanalplanung mit vordefinierten Kanalplänen für jedes Frequenzband, um eine überlappungsfreie Frequenzvergabe zu erreichen.
  - Minimierung der Interferenzen durch intelligente Frequenzvergabe unter Berücksichtigung der Nachbar-Access-Points.
- Überwachung:
  - der Access-Points inklusive ihrer Radio-Module mit aussagekräftigen Indikatoren.
  - der Client-Aktivität inklusive Funkzellen-basierte Lokalisierung der Clients.
  - Erkennung und Anzeige von (unerwünschten) Access-Points in der Umgebung (Nachbar-APs, Rogue-APs usw.)
  - E-Mail-Benachrichtigung bei Ausfall eines verwalteten Access Points
  - Programmgesteuerte Aktionen (z. B. Ausschalten des WLANs während der Nacht)

2 Projektplanung

2.1 Anforderungen des Kunden ermitteln

Am Anfang stehen der Kunde und die Frage, was er wirklich benötigt. In den meisten Fällen wünscht sich der Kunde eine WLAN-Infrastruktur mit zwei getrennten WLAN-Netzen für Mitarbeiter und Gäste in den Büros und in den Besprechungsräumen, damit sich die Mitarbeiter mit dem Firmennetz und mit dem Internet drahtlos verbinden können und die Gäste per WLAN nur auf das Internet zugreifen können.

Zu diesem Zeitpunkt muss auch die Frage beantwortet werden, ob eine professionelle Funkausleuchtung notwendig ist. Aufgrund der hohen Kosten für eine solche Analyse wird man in den meisten Fällen darauf verzichten und stattdessen die Access-Points entsprechend der Wünsche des Kunden und unter Berücksichtigung der räumlichen Gegebenheiten positionieren.

Bei komplexen Gebäuden oder dann, wenn der Kunde ein Hochleistungsnetz mit lückenloser Abdeckung wünscht, das darüber hinaus auch für „Voice over WLAN“ (VoWLAN) geeignet sein soll, sollte man auf eine Standortmessung aber keinesfalls verzichten.

2.2 Empfohlene Hardware-Installation vor Ort

Im Anschluss ist der Elektriker gefragt die Access-Points in den Gängen und Büros zu montieren. Falls keine Funkausleuchtung durchgeführt wurde, sollten die APs (je nach Art und Anzahl der Zwischenwände) im Abstand von 15 bis 25 Metern montiert werden. Bei Einhaltung dieser Faustregel befindet man sich zumeist auf der sicheren Seite.

Alle APs sollten über ein Ethernet-Kabel mit einem PoE-fähigen Switch verbunden werden. Die Stromversorgung über das Ethernet-Kabel (PoE) erspart die Installation einer 230V-Steckdose und vereinfacht die Montage erheblich.

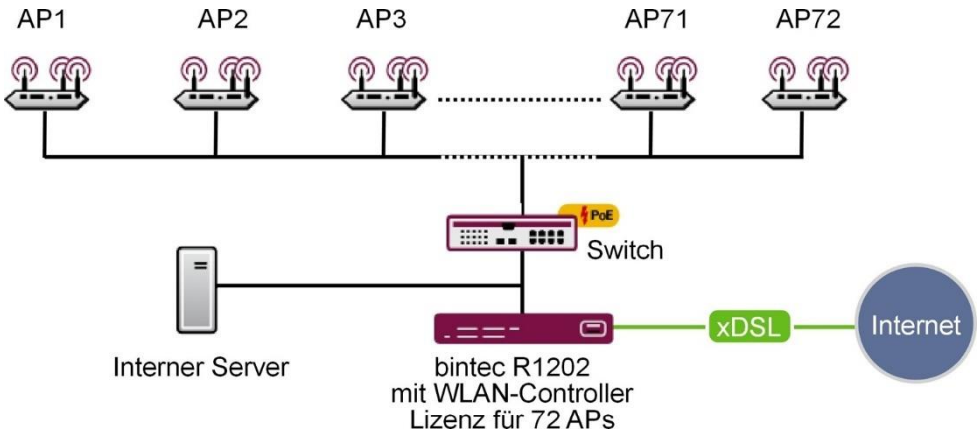


Abbildung 1: WLAN-Infrastruktur

Abschließend sollte der Monteur die Standorte und die MAC-Adressen der Geräte notieren, damit den Geräten später bei der Konfiguration Namen bzw. Standorte zugewiesen werden können.

3 Systemanforderungen

3.1 WLAN-Controller-Hardware

Fast alle BOSS-basierten bintec elmeg Geräte, deren BOSS-Firmware-Version 7.9.6 (veröffentlicht im Oktober 2010) oder höher ist, können als WLAN-Controller verwendet werden (unterstützte Geräte, deren BOSS-Firmwareversion älter als 7.9.6 ist, müssen vor der Installation aktualisiert werden).

Empfohlen ist es für den WLAN-Controller einen Gerätetyp zu verwenden für den eine aktuelle BOSS-Firmware-Version ab 10.2.12 (veröffentlicht im September 2022) verfügbar ist:

- Für die be.IP swift ist der WLAN-Controller künftig vorgesehen
- Alle BOSS-Firmware basierten Router der be.IP-Serie (be.IP Plus V2, be.IP Plus, be.IP Plus World Edition, be.IP 4isdn, be.IP)
- Alle BOSS-Firmware basierten Router der RSxx3-Serie (RS123, RS123w, RS123w-4G, RS353a, RS353aw, RS353awv-4G, RS353j, RS353j-4G, RS353jv, RS353jv-4G, RS353jw, RS353w-4G, RS353jwv, RS353jwv-4G)
- Alle BOSS-Firmware basierten Router der RXL-Serie (RXL12500 und RXL12100)
- Alle Router der Rxxx2-Serie (R1202, RT1202, R3002, RT3002, R3502, R3802, R4402, RT4202, RT4402)
- Alle Access-Points der WIQ-Serie (W2003ac, W2003ac-ext, WO2003ac, WO1003ac, APR222ac, W2004n, W2003n, W2003n-ext, W1001n, W1003n, WI1003n, WO2003n, WO1003n, W2002T-n)

Für kleine Installationen mit bis zu sechs Access-Points wird keine dedizierte WLAN-Controller-Hardware benötigt und einer der Access-Points, der als Master-Access-Point betrieben wird, kann die Funktion des WLAN-Controllers übernehmen. Falls ein WLAN-Netzwerk mit mehr als sechs Access-Points gewünscht wird, ist ein Router als WLAN-Controller-Hardware notwendig.

3.2 Access-Point-Hardware

Der WLAN-Controller kann alle OSDx-Firmware basierten bintec elmeg Access-Points sowie alle BOSS-basierten bintec elmeg Access-Points, die mindestens WiFi 4 (802.11n) unterstützen (ab Firmwareversion 7.9.6), sowie alle bintec elmeg Router mit integriertem WLAN, die mindestens WiFi 4 (802.11n) unterstützen, verwalten.

Empfohlen ist es als Access-Point die OSDx-Firmware basierten aktuellen bintec elmeg Access-Points zu verwenden, sowie bei den BOSS-basierten Access-Points und Routern mit integriertem WLAN die Gerätetypen, für die eine aktuelle BOSS-Firmware-Version ab 10.2.12 (veröffentlicht im September 2022) verfügbar ist:

- Router mit integriertem WLAN der be.IP-Serie und der RSxx3-Serie (Diese Router können sich selbst und weitere APs managen, aber nicht von anderen Routern gemanagt werden)
- Die OSDx-Firmware basierten Access-Points W2044ax, W2022ax, APR2044ax, W2022ac und W2022ac-ext
- Alle Access-Points der WIQ-Serie (W2003ac, W2003ac-ext, WO2003ac, WO1003ac, APR222ac, W2004n, W2003n, W2003n-ext, W1001n, W1003n, WI1003n, WO2003n, WO1003n, W2002T-n)

3.3 WLAN-Controller-Lizenzen

Ab BOSS-Firmware-Version 10.2.12 ist in jedem unterstützten Gerät der WLAN-Controller mit bis zu 6 frei verwaltbaren APs (d. h. ohne die Notwendigkeit bis zu dieser Netzwerkgröße zusätzliche Lizenzen zu erwerben) freigeschaltet. In vorhergehenden BOSS-Firmware-Versionen konnte ohne zusätzliche Lizenzen nur maximal ein AP per WLAN-Controller verwaltet werden.

Mit jeder zusätzlich im WLAN-Controller-Router installierten WLAN-Controller-Lizenz lassen sich sechs weitere Access-Points verwalten. Auf einem RSxx3-Router (z.B. RS123) lassen sich bis zu 11 WLAN-Controller-Lizenzen installieren und damit bis zu 72 Access-Points verwalten. Auf Central Routern (z.B. RXL12100) können bis zu 24 Lizenzen installiert werden, damit können bis zu maximal 150 Access-Points administriert werden.

In der folgenden Tabelle finden Sie die minimal benötigte WLAN-Controller-Hardware sowie die entsprechenden, notwendigen Lizenzen in Abhängigkeit der AP-Anzahl:

	Bis zu 6 AP	**Bis zu 48 AP**	**Bis zu 72 AP**	**Bis zu 150 AP**
Benötigte WLC-Hardware	Keine, läuft auf dem Master-AP	Router der be.IP-Serie	Router der RSxx3-Serie oder der Rxxx2-Serie	Router der RXL-Serie
WLC-Lizenzen	Keine	7x	11x	24x

4 Netzwerk-Konfiguration

4.1 Interner DHCP-Server

Falls sich noch kein anderer DHCP-Server in ihrem Netzwerk befindet und der WLAN-Controller auch DHCP-Server sein soll, können Sie zur WLAN-Installation mithilfe des WLAN-Controller-Assistenten auf Seite 6 wechseln, da der Assistent auch alle Einstellungen für den DHCP-Server mit vornimmt.

4.2 Externer DHCP-Server

Damit die Access-Points mithilfe des WLAN-Controllers verwaltet werden können, muss ihnen die IP-Adresse des WLAN-Controllers bekannt sein. Neben den benötigten Grundeinstellungen für das Netzwerk, wie die IP-Adressen der Geräte, dem Standard-Gateway oder dem DNS-Name-Server, teilt der DHCP-Server über die Option 138 des DHCP-Protokolls dem Access-Point die IP-Adresse des WLAN-Controllers mit. Dazu muss diese Option, auch als CAPWAP-Access-Controller bekannt, beim DHCP-Server aktiviert und dort die IP-Adresse des WLAN-Controllers eingetragen werden:

- **Ein anderer bintec-Router arbeitet als DHCP-Server**: Die notwendigen Konfigurationsschritte sind im Anhang auf Seite 21 erläutert.
- **Ein Microsoft Server 2003 oder Server 2008 arbeitet als DHCP-Server**: Die notwendigen Konfigurationsschritte sind im Anhang auf Seite 21 erläutert.
- **Ein Linux-Server arbeitet als DHCP-Server**: Die notwendigen Konfigurationsschritte sind im Anhang auf Seite 25 erläutert.
- **Ein Router eines Drittanbieters arbeitet als DHCP-Server**: Bitte nehmen Sie die Konfiguration der DHCP-Option 138 anhand der Kundendokumentation des Routers vor.

4.3 Kein DHCP-Server – APs mit statischen IP-Adressen

Bisweilen ist es notwendig – aber aufgrund des erheblichen konfigurativen Mehraufwands nicht empfohlen – die Access-Points am WLAN-Controller mit statischen IP-Adressen und Netzwerkeinstellungen zu betreiben. Dazu muss vorher auch jedem AP manuell eine IP-Adresse zugeordnet werden. Die benötigten Konfigurationsschritte für alle Access-Points werden im Anhang auf Seite 25 beschrieben.

5 WLAN-Installation mithilfe des WLAN-Controller-Assistenten

Der WLAN-Controller-Assistent führt Sie in maximal drei Schritten durch die Konfiguration Ihres WLAN-Netzwerkes. Im folgenden Beispiel gehen wir davon aus, dass das WLAN-Controller-Gerät auch ihr Internet-Zugangs-Router ist.

5.1 Schritt 1: Aktivierung des WLAN-Controllers

Gehen sie in der GUI ihres WLAN-Controller-Geräts in das Menü „Assistenten > WLAN (WLC)“. Nur wenn der WLAN-Controller in ihrem Gerät noch deaktiviert ist, sehen sie die nachfolgende Hinweisseite mit der „Warnung: Wireless LAN Controller ist nicht aktiviert.“ Wenn sie diesen Hinweis nicht sehen (wie bspw. bei der „be.IP Plus“ in Werkseinstellungen) ist der WLAN-Controller bereits aktiv und sie können direkt zum Schritt 2 vorspringen.

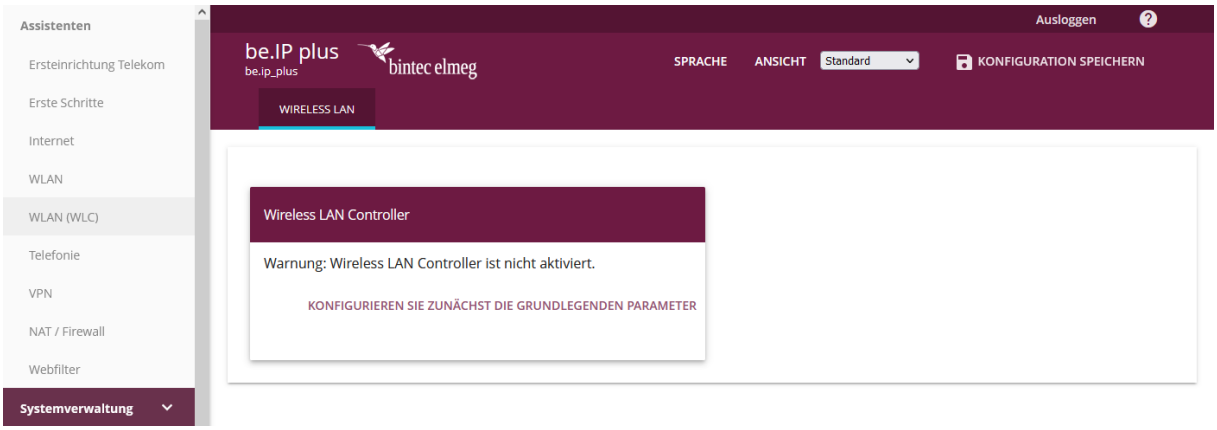


Abbildung 2: „Assistenten > WLAN (WLC) > Wireless LAN Controller“ WLAN-Controller deaktiviert

Klicken sie auf den Link „Konfigurieren sie zunächst die grundlegenden Parameter“. Sie werden nun auf die GUI-Seite „Wireless LAN Controller > Controller-Konfiguration > Allgemein“ weitergeleitet:

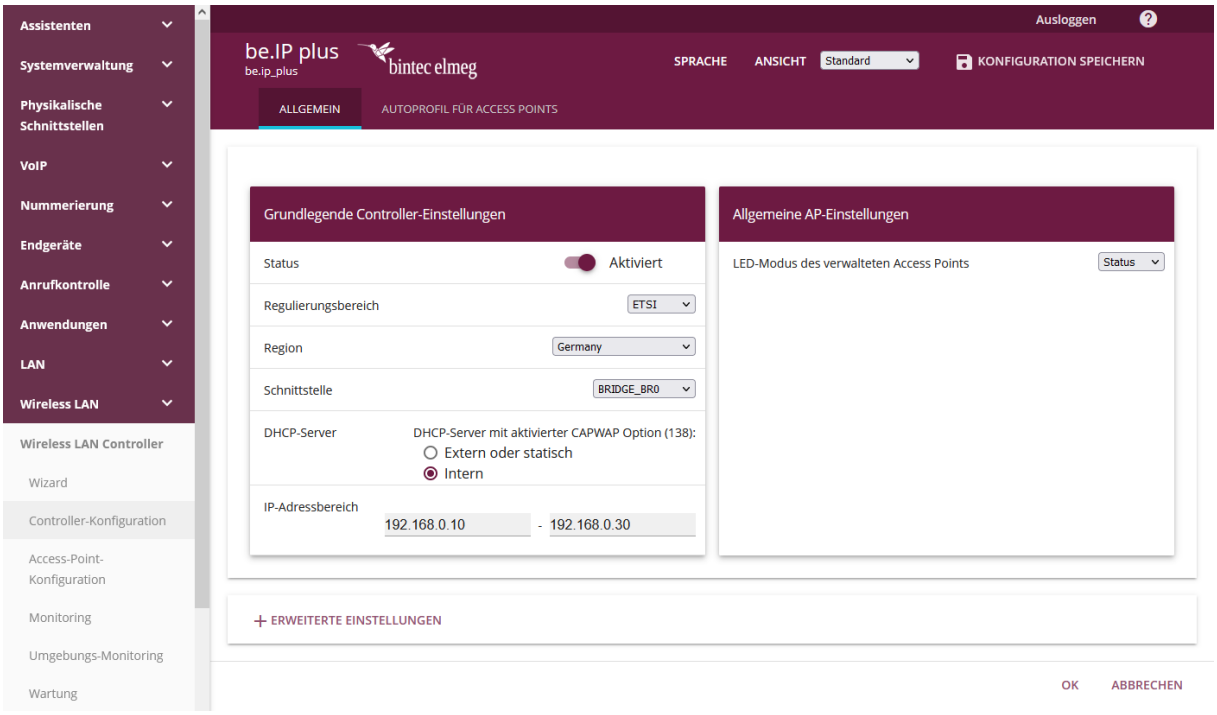


Abbildung 3: „Wireless LAN Controller > Controller-Konfiguration > Allgemein“ WLAN-Controller aktiviert

Hier legen Sie die grundlegenden Eigenschaften des WLAN-Controllers fest:

1. **Status**: Setzen sie den Status auf „Aktiviert“, um die Grundeinstellungen für den Wireless LAN Controller zu konfigurieren.
2. **Regulierungsbereich**: Wählen Sie hier den Regulierungsbereich. Er definiert welche Frequenzen für WLAN erlaubt sind und muss identisch zum werkseitig festgelegten Regulierungsbereich ihrer Access-Points sein, andernfalls bleibt das WLAN ihrer Access-Points aus. Der Standardwert ist hier „ETSI“ (European Telecommunications Standards Institute). Ändern sie diesen Wert nur, wenn sie speziell dafür werkseitig angepasste Access-Points haben.
3. **Region**: Diese Einstellung passt Ihr WLAN-Netzwerk an die spezifischen WLAN-Funkbestimmungen in Ihrer Region an. Sie müssen hier das Land einstellen, in dem sich ihre Access-Point befinden.
4. **Schnittstelle**: Legt fest, über welche Schnittstelle der Controller mit den APs kommuniziert (die IP-Adresse dieser Schnittstelle muss in der CAPWAP-Option 138 des DHCP-Servers eingetragen sein).
5. **DHCP-Server**: Legt fest, ob der „interne“ oder ein „externer“ DHCP-Server für die Access-Points verwendet wird. Bei Verwendung des internen DHCP-Servers werden alle Einstellungen des DHCP-Servers, z.B. die Konfiguration der Option 138, automatisch durchgeführt. Hinweise zur Konfiguration eines externen DHCP-Servers finden Sie im Anhang ab Seite 21.
6. **IP-Adressbereich**: Legt den IP-Adressbereich für den internen DHCP-Server fest.

Achtung: Falls ein DHCP-Server schon zum Zeitpunkt der Installation der APs aktiv war, aber die DHCP-Option 138 erst später aktiviert wurde, kann es sein, dass der WLAN-Controller die APs im Netz

nicht findet. Der Grund dafür ist, dass die APs bereits eine IP-Adresse bezogen, aber noch keine IP-Adresse des WLAN-Controllers erhalten haben. Deshalb muss entweder der Ablauf der Lease-Time des DHCP-Servers abgewartet werden oder ein Neustart der APs durchgeführt werden.

5.2 Schritt 2: Einrichtung des internen WLAN

Sie befinden sich nun auf der Übersichtsseite des WLAN-Controller-Assistenten, der ihnen mitteilt, wie viele Access-Points aktuell vom WLAN-Controller verwaltet werden, wie viele WLAN-Clients gerade in Summe über alle eingerichtete WLAN-Netzwerke verbunden sind und welche WLAN-Netzwerke konfiguriert sind und auf wie vielen Funkzellen (ein bis zwei pro AP, je nach Hardware-Ausstattung des AP) die WLAN-Netze jeweils aktiv sind. Standardmäßig ist in der hier abgebildeten „be.IP Plus“ ein internes WLAN-Netzwerk vorhanden, welches mit ihrem LAN-Netzwerk gekoppelt ist:

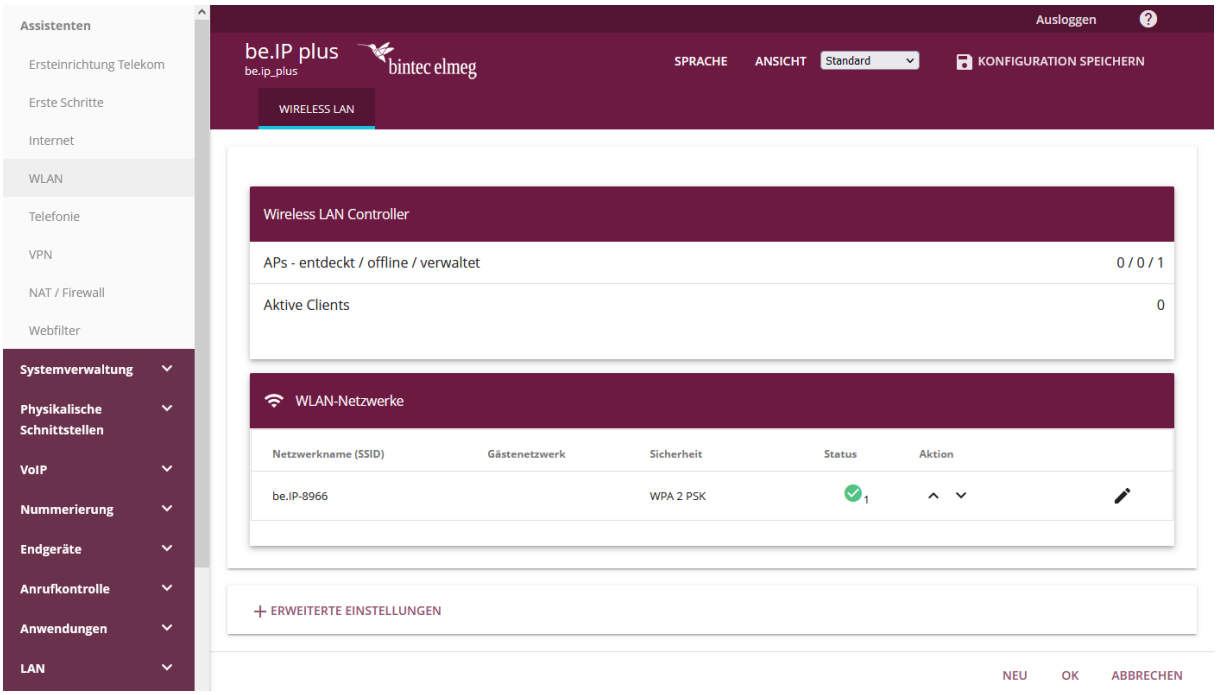


Abbildung 4: „Assistenten > WLAN (WLC) > Wireless LAN Controller“ Übersicht

Mit einem Klick auf den Stift können sie dieses WLAN-Netzwerk bearbeiten:

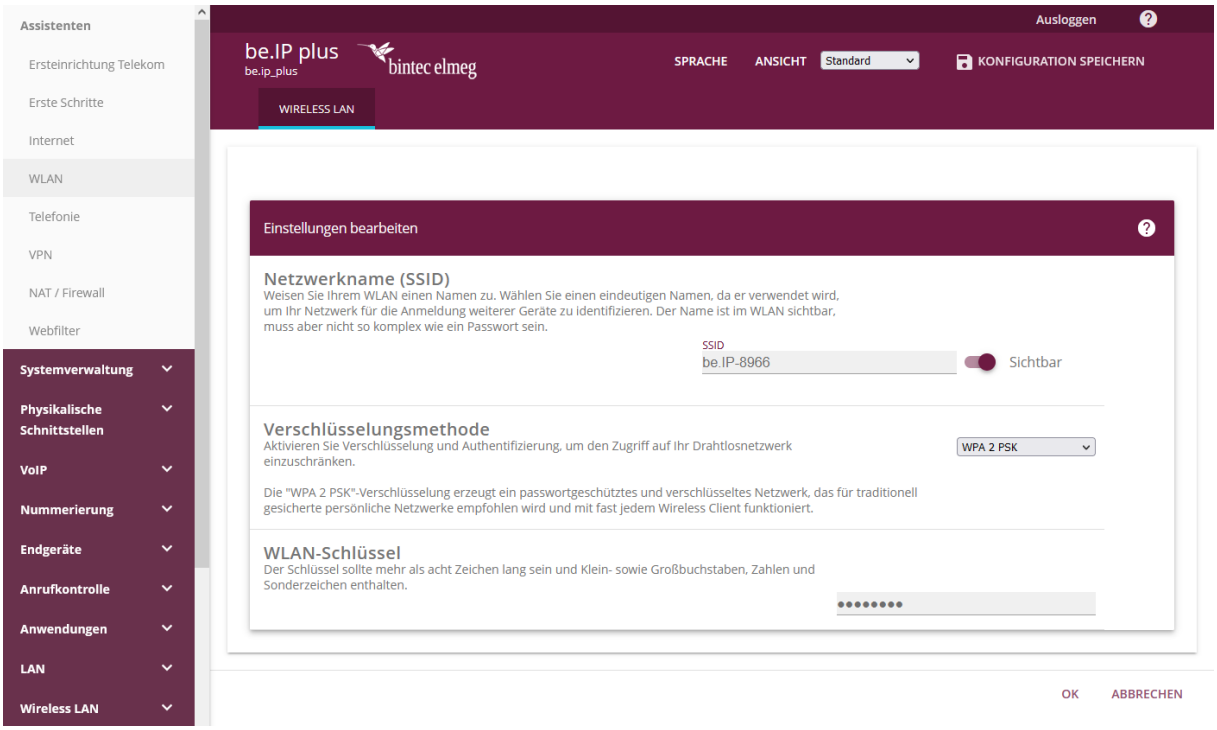


Abbildung 5: „Assistenten > WLAN (WLC) > Wireless LAN Controller“ WLAN-Netzwerk bearbeiten

Hier richten sie ihr WLAN-Netzwerk ein:

1. **Netzwerkname (SSID)**: Hier können sie ihrem WLAN einen Namen zuweisen, unter dem es von WLAN-Clients gefunden wird. Optional können sie einstellen, dass der WLAN-Name für WLAN-Clients nicht sichtbar sein soll. Bei unsichtbaren WLAN-Netzen müssen WLAN-Benutzer den Namen kennen und manuell in ihren WLAN-Client eingeben, um sich mit dem WLAN-Netzwerk verbinden zu können.
2. **Verschlüsselungsmethode**: Die Verschlüsselungsmethode bestimmt ob und wie Benutzer das WLAN-Netzwerk nutzen können. Voreingestellt ist „WPA 2 PSK“, welches zugleich sicher ist und größtmögliche Kompatibilität bietet. Sie können hier von offenen unverschlüsselten WLAN-Netzen bis hin zum hochsicheren WPA 3 aus verschiedenen Methoden wählen. Bitte beachten sie die diesbezüglichen Hinweistexten im Assistenten, insbesondere dass das interne WLAN-Modul der bintec-elmeg-Router WPA 3 nicht unterstützt. Für WPA 3 benötigen sie W2022ac, W2022ac-ext, W2022ax oder W2044ax Access-Points ab OSDx-Firmware-Version 2.4.1.1.
3. **WLAN-Schlüssel**: Der WLAN-Schlüssel muss mindestens 8 Zeichen lang sein und sollte hinreichend komplex sein, damit er nicht von unbefugten Dritten durch Ausprobieren herausgefunden werden kann.

Mit dem Klick auf „OK“ werden diese Einstellungen sofort übernommen und auf alle gemanagten Access-Points sowohl im 2,4GHz Band und (sofern im Access-Point vorhanden) im 5GHz-Band ausgerollt. Darüber hinaus werden auch erst zu einem späteren Zeitpunkt hinzugefügte Access-Points automatisch mit diesen Einstellungen unmittelbar bei Verkabelung mit dem LAN-Netzwerk mit diesen WLAN-Netzwerk-Einstellungen in Betrieb genommen. Eine Erweiterung des WLAN-Netzwerks um zusätzliche Access-Points funktioniert also – bis auf die Montage der Access-Points –

vollautomatisch. In der Übersichtsseite des Assistenten können sie summarisch überprüfen (und eingehender in den weiter unten erläuterten Detail-Menüs), ob die Inbetriebnahme der Access-Points korrekt erfolgte.

Verwaltete Access-Points werden vom WLAN-Controller gegen jede Art eines externen Zugriffs gesperrt. Ein Access-Point kann erst dann wieder lokal konfiguriert werden, nachdem er vom WLAN-Controller freigegeben wurde.

5.3 Schritt 3: Hinzufügen eines Gast-WLAN

In der Übersichtsseite des WLAN-Controller-Assistenten können sie über einen Klick auf „Neu“ (in der rechten unteren Ecke) weitere WLAN-Netzwerke hinzufügen. Sie können bis zu 8 WLAN-Netzwerke einrichten.

In diesem Beispiel legen wir ein weiteres WLAN-Netzwerk für den Gastzugang an. Nach dem Klick auf „Neu“ erscheint eine WLAN-Netzwerk-Einstellungsseite mit einem zusätzlichen Einstellungspunkt „Gästenetzwerk“, der nur für neu angelegte Netze verfügbar ist. Wir richten unser Gästenetzwerk analog zum vorhergehenden Schritt mit einem eigenen Netzwerknamen und WLAN-Schlüssel ein und setzen zusätzlich den Haken bei „Gästenetzwerk“:

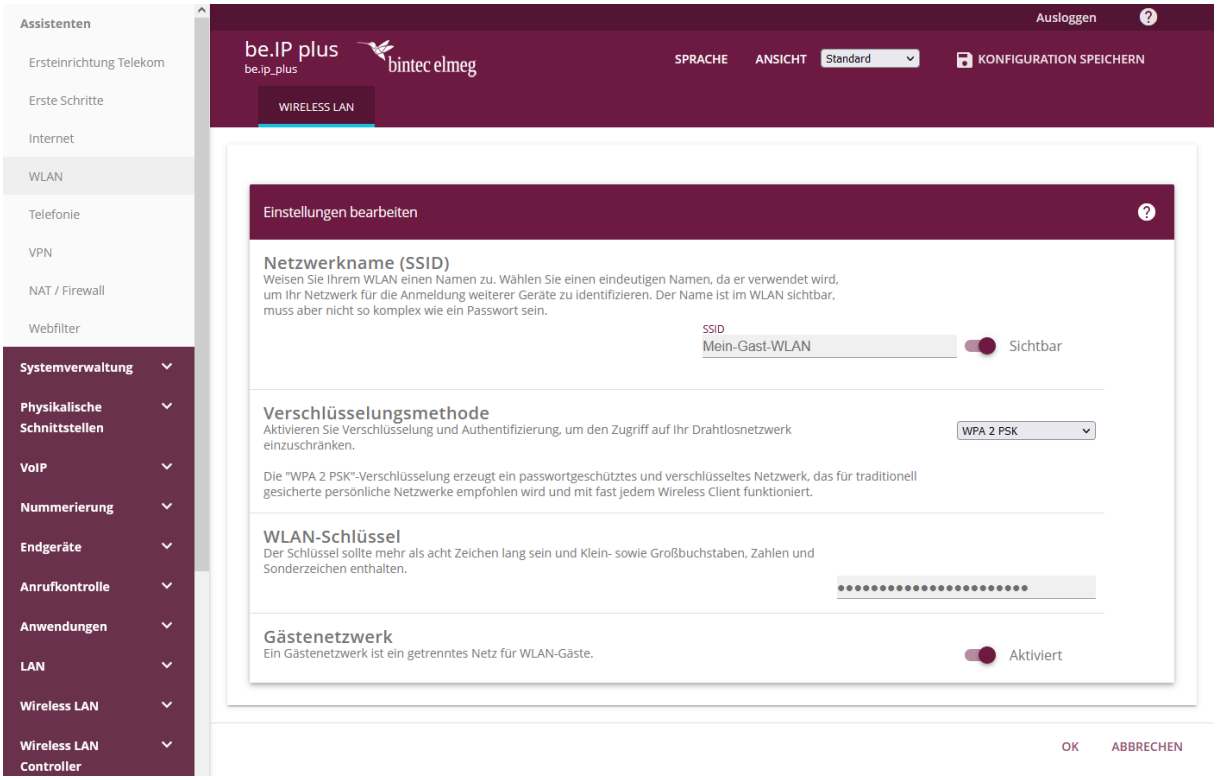


Abbildung 6: „Assistenten > WLAN (WLC) > Wireless LAN Controller“ Gast-WLAN-Netzwerk hinzufügen

Wenn im WLAN-Controller-Router kein Internetzugang über PPPoE (bspw. via xDSL) eingerichtet ist erscheint bei Aktivierung des Hakens „Gästenetzwerk“ im Kopf der Einstellungsseite der Warnhinweis: „Achtung! Es ist keine Internetverbindung über die PPPoE-Schnittstelle eingerichtet. Die Einstellungen der Firewall müssen für WLAN-Gästenetzwerke manuell vorgenommen werden.“ Im obigen Beispiel ist der Internetzugang bereits eingerichtet. Es empfiehlt sich insbesondere für

Gast-WLAN-Netzwerke den WLAN-Controller-Router auch als Internetzugangsrouter zu verwenden, da die vom Assistenten in dem Fall dafür automatisch ausgerollten Firewall-Regeln und ggf. weitere Einstellungen (auch auf dem anderen Router, der den Internetzugang bereitstellt) andernfalls nachträglich händisch selbst erstellt und an die jeweilige Situation angepasst werden müssten.

Wir verlassen die Seite nun mit „OK“ und sehen anschließend die Übersichtsseite des WLAN-Controller-Assistenten mit beiden Netzwerken:

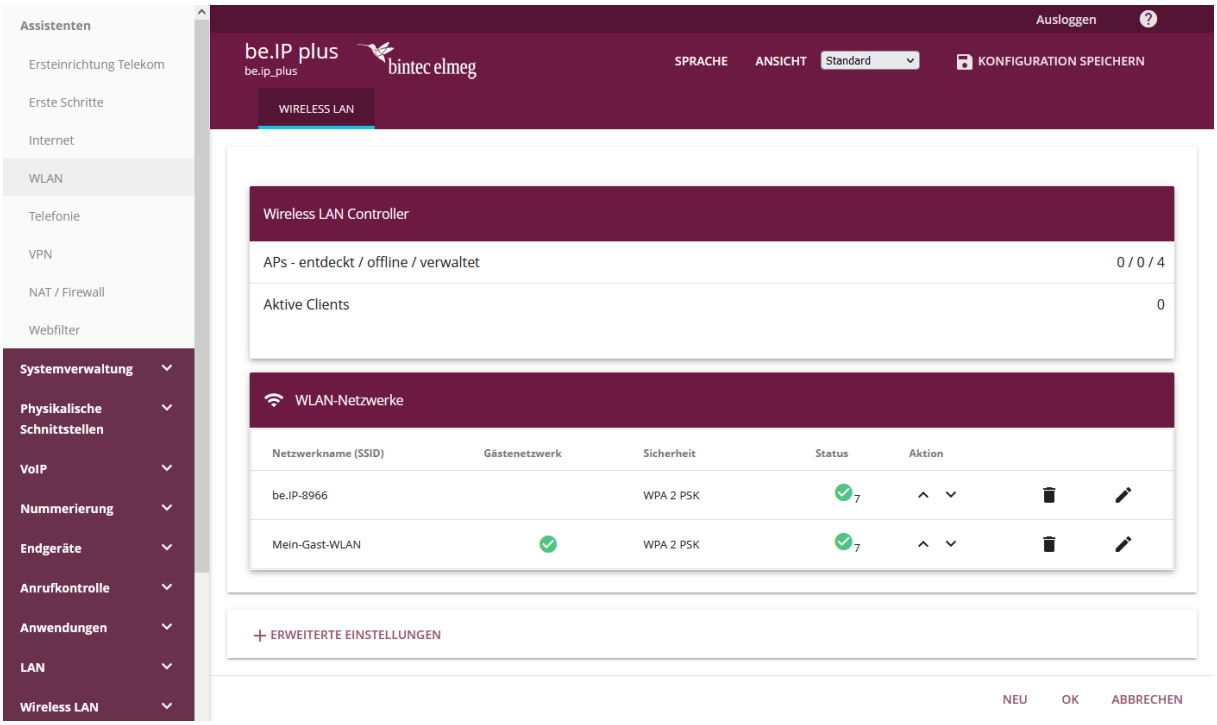


Abbildung 7: „Assistenten > WLAN (WLC) > Wireless LAN Controller“ Übersicht über die fertige Konfiguration

Auch das Gäste-WLAN wird wie das interne WLAN automatisch auf alle aktuellen und künftig hinzuzufügenden Access-Points ausgerollt (im obigen Beispiel wurden 3 weitere APs hinzugefügt).

Die eigentliche Inbetriebnahme der WLAN-Infrastruktur mit zwei getrennten WLAN-Netzen für Mitarbeiter und Gäste ist hiermit nun erfolgreich abgeschlossen und sie können ihr WLAN nutzen. Bitte vergessen sie nicht ihre erfolgreiche Konfiguration über „Konfiguration speichern“ in der rechten oberen Ecke auch boot-fest zu speichern.

Die Access-Points selbst halten ihre eigenen Einstellungen nur im flüchtigen Speicher. Im Fall eines Stromausfalls erhalten die Access-Points automatisch nach dem Wiederherstellen der Stromversorgung vom WLAN-Controller ihre Einstellungen. Das Halten der Konfiguration ausschließlich im flüchtigen Speicher der Access-Points hat entscheidende Sicherheitsvorteile, da keine sensiblen Daten, wie die WLAN-Schlüssel, durch Diebstahl eines öffentlich zugänglichen Access-Points kompromittiert werden können.

Alles Weitere dient dem vertieften Verständnis für die von diesem Assistenten ausgerollte Konfiguration, für Troubleshooting einzelner Netzwerkkomponenten und falls sie Anpassungen vornehmen möchten, die über diesen Assistenten hinausgehen.

6 Details und optionale Anpassung der Konfiguration des WLAN-Controller-Assistenten

Um sich die Details der vom WLAN-Controller-Assistenten vorgenommenen Konfiguration anzusehen, müssen sie auf Routern der be.IP-Serie zunächst die „Ansicht“ in der rechten oberen Ecke auf „Vollzugriff“ umschalten. Auf allen anderen Geräten ist dieser Zwischenschritt nicht notwendig, da diese immer im „Vollzugriff“ laufen.

6.1 Übersicht über die ausgerollte WLAN-Controller-Konfiguration

Über das linke Menü gehen wir nun zum Menüpunkt „Wireless LAN Controller > Controller-Konfiguration > Allgemein“. Diese Seite kennen sie entweder schon von der Erstinbetriebnahme oder falls der WLAN-Controller schon aktiv, war können sie hier nun die grundlegenden Einstellungen ihres WLAN-Controllers ansehen.

Sollte sie das Blinken ihrer Access-Points stören, können sie hier global für alle verwalteten Access-Points den LED-Modus auf „aus“ stellen. Bitte beachten sie dabei: Die Access-Points sehen nun so aus als seien sie ausgeschaltet. Sie können nicht mehr anhand der LED sehen, ob ein AP tatsächlich funktioniert oder nicht. Für BOSS-basierte Access-Points gilt dies boot-fest selbst dann, wenn der AP gar nicht mehr mit dem WLAN-Controller verbunden ist. Sie müssen diese Einstellung (entweder im WLAN-Controller oder falls er nicht mehr gemanagt ist über die interne GUI des AP) wieder zurücknehmen, damit die LED wieder leuchten.

Wir gehen einen Reiter weiter zu „Wireless LAN Controller > Controller-Konfiguration > Autoprofil für Access Points“. Dort sehen sie das vom Assistenten angelegte (und erweiterte) Autoprofil das neue Access-Points automatisch mit Ihren WLAN-Einstellungen konfiguriert:

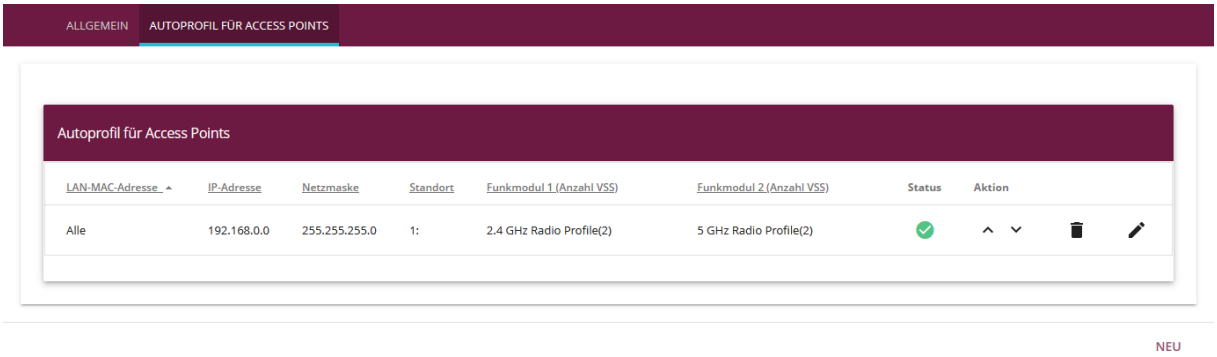


Abbildung 8: „Wireless LAN Controller > Controller-Konfiguration > Autoprofil für Access Points“ Übersicht

Im Menüpunkt „Wireless LAN Controller > Access-Point-Konfiguration > Access-Points“ sehen sie alle gefundenen und verwalteten Access-Points mit ihrem Status und Konfiguration. Bei der Vergabe der Funkkanäle sorgt der WLAN-Controller dafür, dass von den APs ausschließlich überlappungsfreie Kanäle genutzt werden und die verwalteten Access-Points sorgen dafür, dass die Interferenzen untereinander so gering wie möglich sind.

Um nach längerem Betrieb (z.B., wenn andere Nachbar-APs hinzugekommen sind) eine erneute Abstimmung der genutzten Kanäle anzustoßen und um somit etwaige WLAN-Interferenzen zu minimieren, können sie über die Funktion „Neue Kanalfestlegung“ durch den Klick auf „START“ diese

erneut vornehmen. Hierbei kommt es prinzipbedingt an den APs (hintereinander) zu kurzen Betriebsunterbrechungen des WLANs:

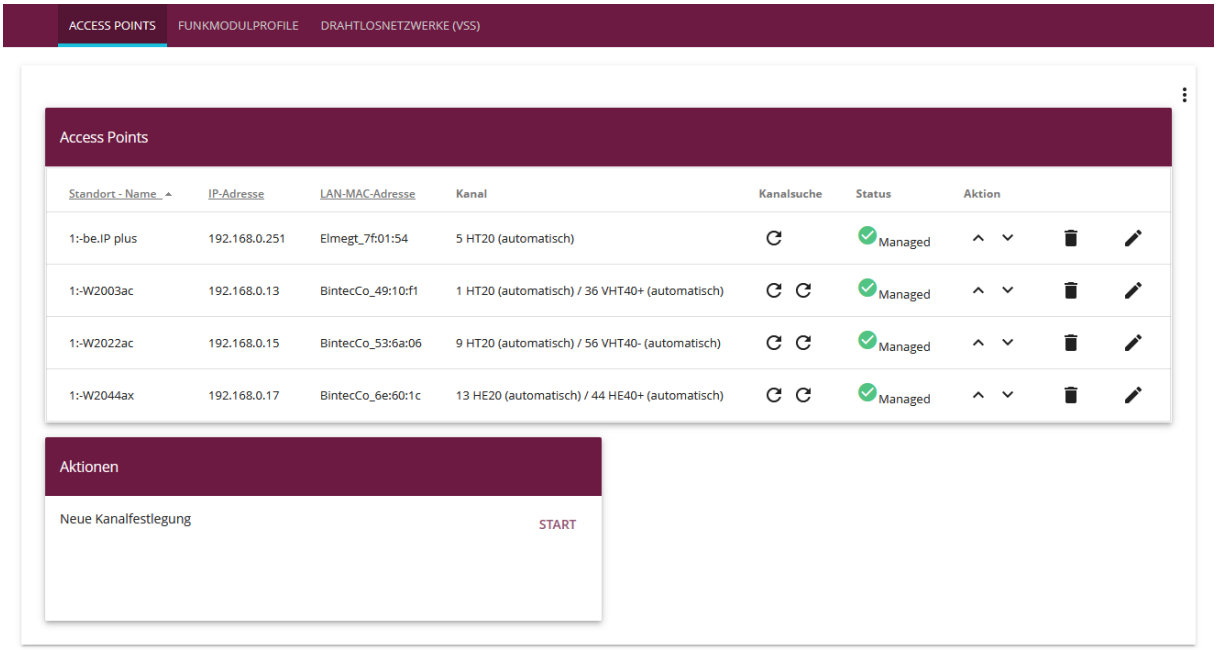


Abbildung 9: „Wireless LAN Controller > Access-Point-Konfiguration > Access-Points“ Übersicht

Über den Stift können sie für jeden Access-Point seine Hardware-Eigenschaften (Anzahl und Eigenschaften der Radiomodule und ob der Access-Point bspw. WPA 3 unterstützt oder nicht usw.), die auf ihn gebundenen Funkmodulprofile und Drahtlosnetzwerke sowie weitere individuelle Einstellungen sehen. Außerdem können sie hier jedem Gerät eine individuelle Standortbeschreibung geben, was sich für den besseren Überblick in Netzen mit vielen Access-Points empfiehlt:

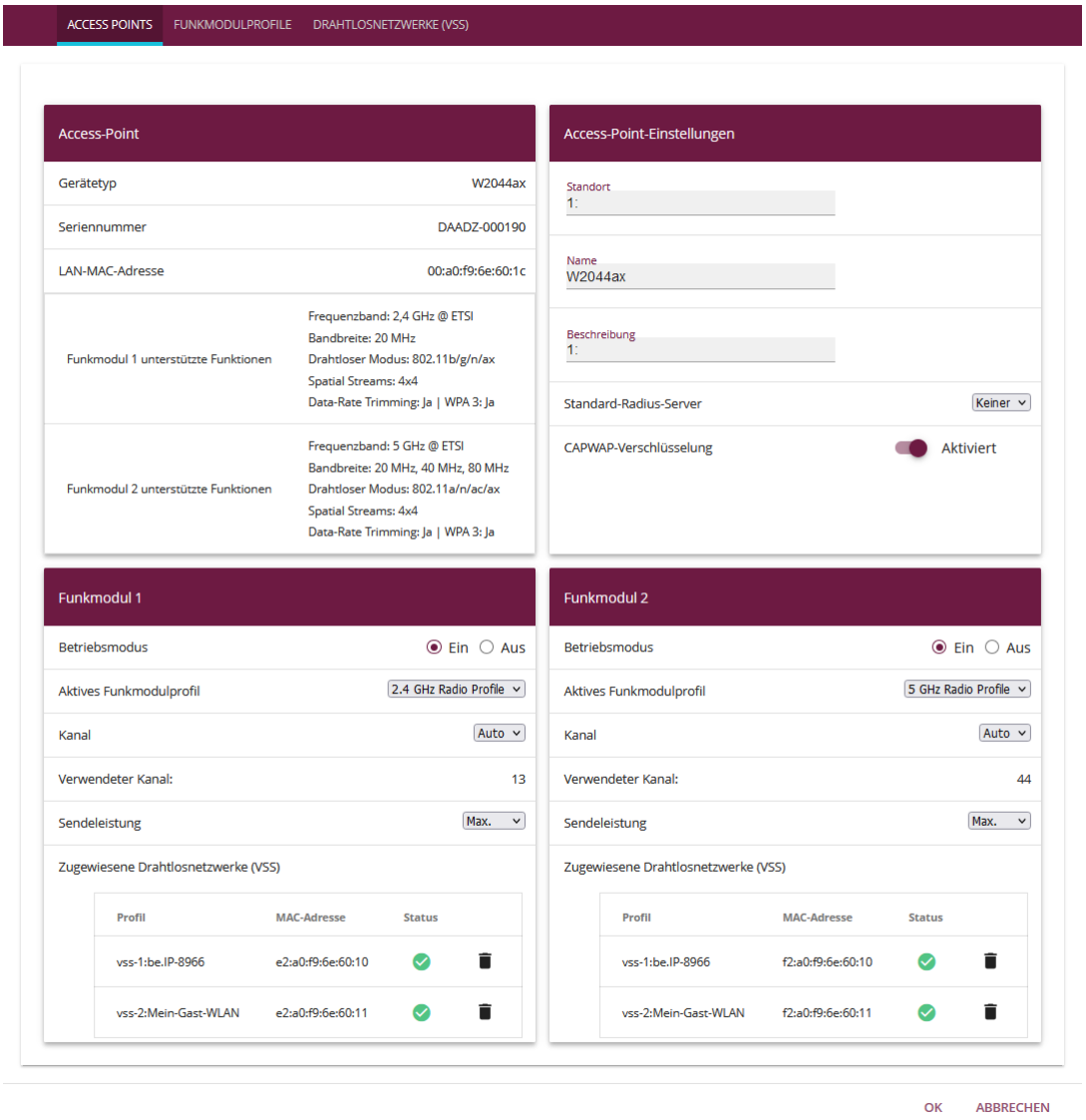


Abbildung 10: „Wireless LAN Controller > Access-Point-Konfiguration > Access-Points“ Bearbeitungsseite

Im Menüpunkt „Wireless LAN Controller > Access-Point-Konfiguration > Funkmodulprofile“ finden sie zwei Funkmodulprofile, je eins für das 2,4GHz-Band und das 5GHz-Band, die auf die gemanagten Access-Points für deren Radiomodule angewandt werden.

Das 2,4GHz-Radio-Profil ist in Standardeinstellungen mit 802.11g/n/ax für den drahtlosen Modus, 4 Spatial Streams, dem ETSI-Modus-Kanalplan (1 – 5 – 9 – 13), aktiviertem Short-Guard-Interval und einer Beacon-Periode von 100ms auf bestmöglichen Datendurchsatz und Frequenznutzung in Europa für WLAN-Netze mit mehr als einem Access-Point optimiert. Das 5GHz-Radio-Profil hat analoge Einstellungen mit höherer Kanalbandbreite und einem für den Einsatzbereich im 5GHz-Band optimierten Kanalplan, da dort mehr Kanäle zur Verfügung stehen.

Sie können hier Funkfrequenzen, Drahtlosmodus, Kanalpläne und mehr anpassen. Bitte beachten sie zu den einzelnen Parametern die kontextsensitive Online-Hilfe und das in der Seite verlinkte Online-Dokument welche Einstellungen von welchem Access-Point-Typ unterstützt werden. Wird ein Access-Point vom WLAN-Controller mit einer Einstellung konfiguriert, die er nicht unterstützt, wählt er eine

Einstellung, die der übermittelten Konfiguration am nächsten kommt. Dank dieses „Best-Effort-Ansatzes“ können sie auch für unterschiedliche AP-Generationen innerhalb eines Frequenzbandes meistens dasselbe Radioprofil verwenden und so die WLAN-Controller-Konfiguration auch in historisch gewachsenen WLAN-Netzen übersichtlich halten:

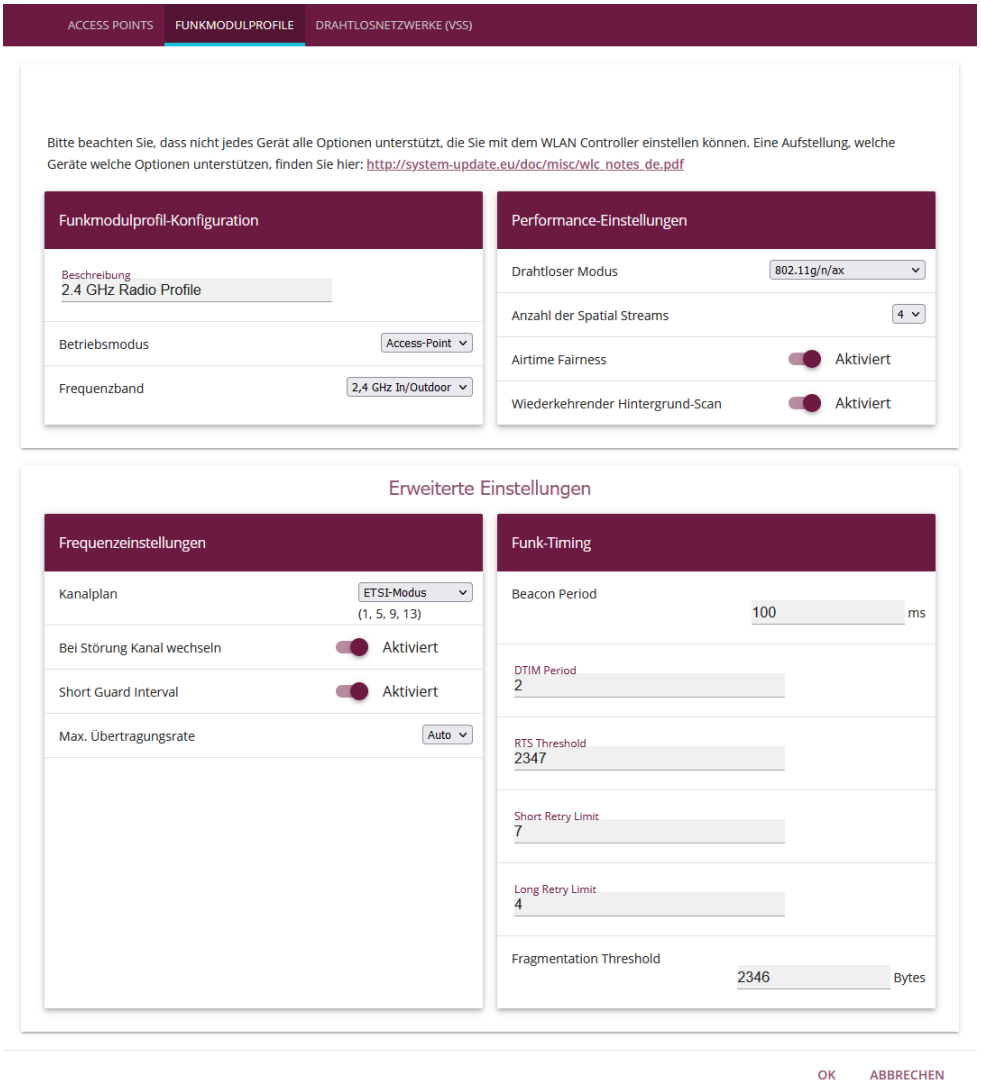


Abbildung 11: „Wireless LAN Controller > Access-Point-Konfiguration > Funkmodulprofile“ Bearbeitungsseite für das „2.4GHz Radio Profile“

Im Menüpunkt „Wireless LAN Controller > Access-Point-Konfiguration > Drahtlosnetzwerke (VSS)“ finden sie die Drahtlosnetzwerkprofile ihrer zuvor im WLAN-Controller-Assistenten angelegten WLAN-Netzwerke. Dort können sie zahlreiche weitere Detaileinstellungen vornehmen und für ihren jeweiligen Einsatzzweck optimieren, die der Assistent mit möglichst allgemein gültigen Werten vorbelegt hat. So kann man dort auch die über den Assistenten nicht auswählbaren Sicherheitseinstellungen zu WPA-Enterprise (u.a. das für Hochsicherheitsnetze vorgesehene WPA-3-Enterprise-CNSA) vornehmen, die insbesondere in WLAN-Netzen von Unternehmen und Behörden Standard sind. Wir sehen uns nun das Drahtlosnetzwerkprofil für das Gästenetzwerk an. Gästenetzwerke werden vom WLAN-Controller mittels VLAN realisiert. In der Einstellungsseite des Drahtlosnetzwerkprofils des Gästenetzwerks finden sie weiter unten die Box „VLAN“. Dort sehen sie,

dass VLAN aktiviert und die VLAN-ID 3 vergeben wurde (jedes über den Assistenten angelegte Gästenetzwerk erhält eine eigene VLAN-ID in aufsteigender Reihenfolge). Dadurch werden alle Daten von WLAN-Clients, die sich an einem verwalteten Access-Point mit diesem Gästenetzwerk verbinden im Ethernet-LAN stets mit der VLAN-ID 3 versehen, sodass dieses Netz sicher vom Datenverkehr des ungetaggten LAN-Netzwerks getrennt ist, aber dieselbe LAN-Kabelinfrastruktur nutzt:

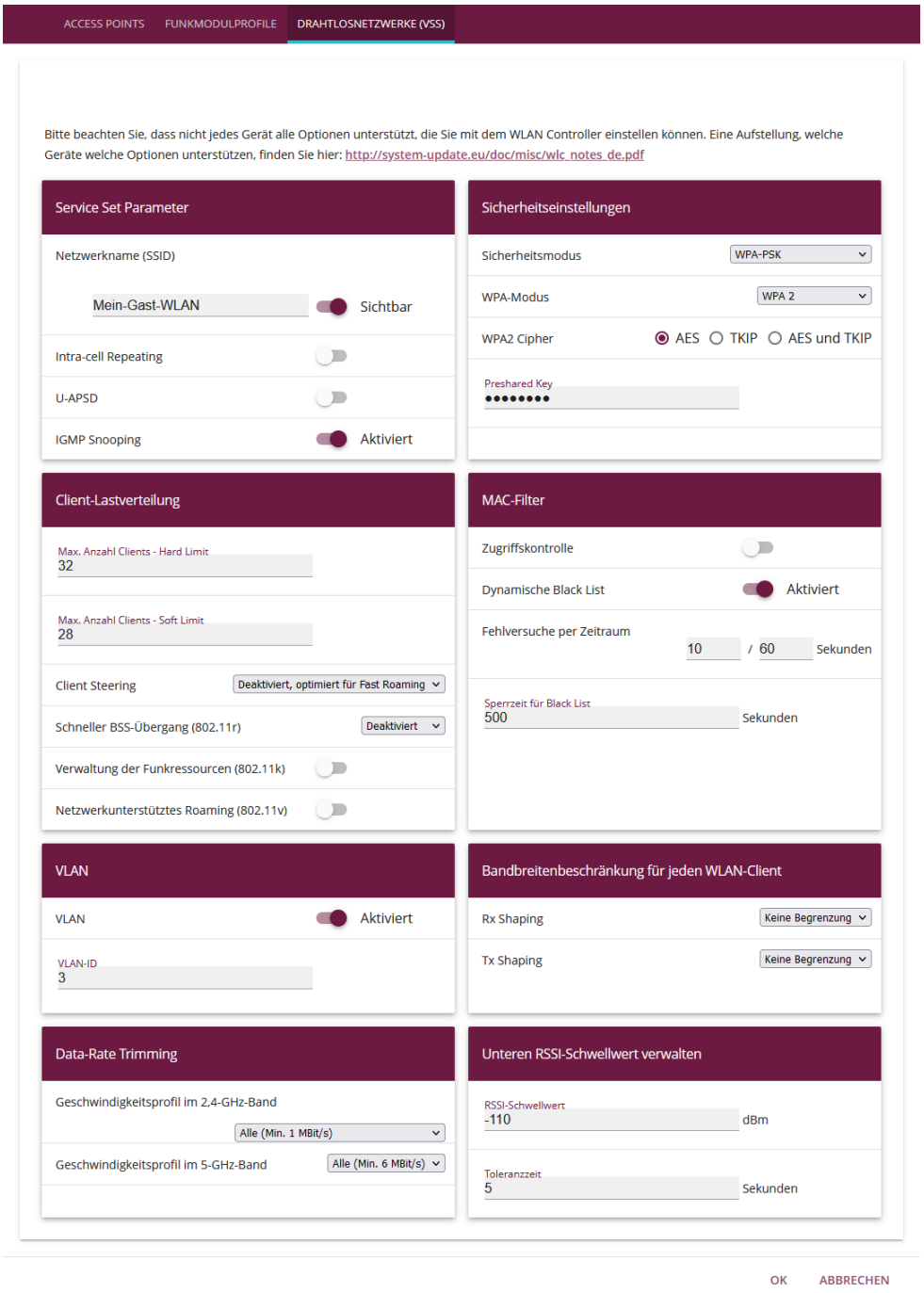


Abbildung 12: „Wireless LAN Controller > Access-Point-Konfiguration > Drahtlosnetzwerke (VSS)“ Bearbeitungsseite für das Gast-WLAN-Netzwerk

6.2 Einzelheiten der LAN-Konfiguration für das Gast-WLAN

Ein VLAN benötigt jedoch auch einen eigenen Zugangspunkt, der ein separates IP-Netzwerk per DHCP verteilt, sowie Dienste wie DNS bereitstellt und den Zugang ins Internet regelt. Dafür hat der WLAN-Controller-Assistent im WLAN-Controller-Router eine eigene virtuelle Schnittstelle mit der VLAN-ID 3 basierend auf der Schnittstelle des WLAN-Controllers angelegt, die sie im Menü „LAN > IP-Konfiguration“ finden. In der be.IP-Serie heißt diese virtuelle Schnittstelle in der Standardkonfiguration „br0-1“ (da die Schnittstelle des WLAN-Controllers in der Standardkonfiguration dort „br0“ ist). In den Einstellungen dieser virtuellen Schnittstelle sehen sie wieder die VLAN-ID 3, sowie die IP-Adresse 192.168.3.1 (der vorletzte Block der IP-Adresse wird vom Assistenten der besseren Übersicht wegen immer mit derselben Zahl wie die VLAN-ID belegt) und dass die Sicherheitsrichtlinie dieser Schnittstelle auf „Nicht Vertrauenswürdig“ steht:

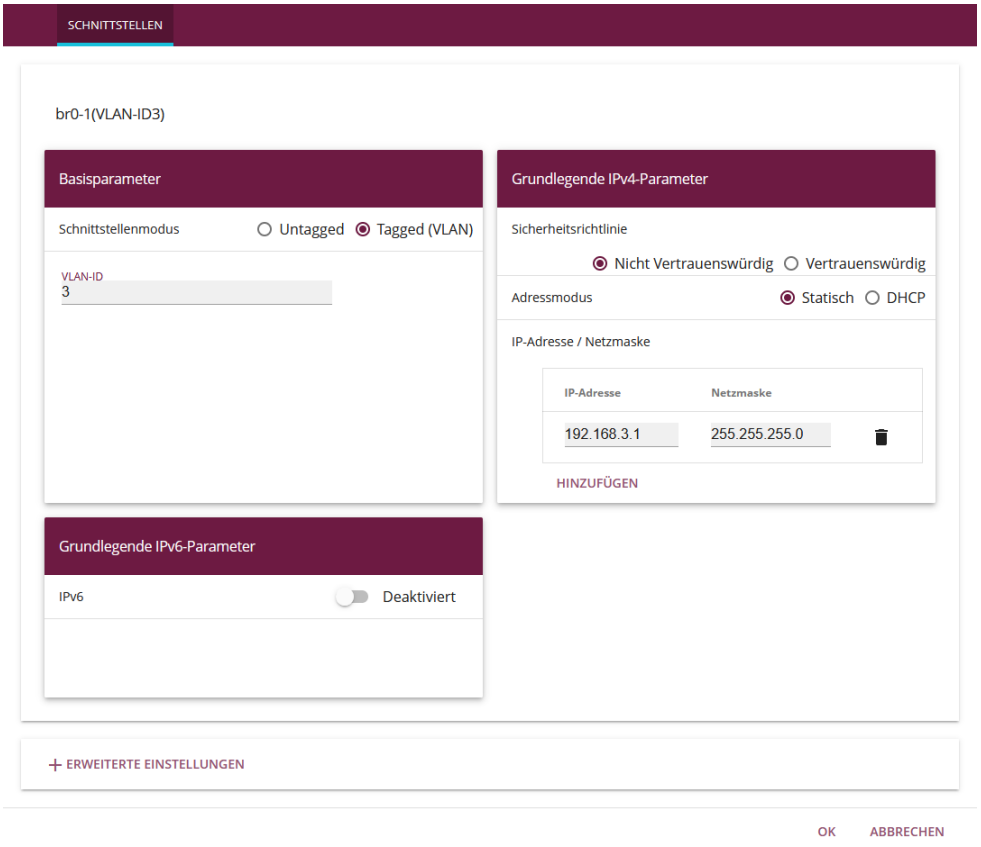


Abbildung 13: „LAN > IP-Konfiguration“ Bearbeitungsseite für virtuelle Schnittstelle „br0-1“

Die vom WLAN-Controller-Assistent angelegte DHCP-Server-Instanz für das VLAN des Gästenetzwerks finden sie im Menü „Lokale Dienste > DHCP-Server“. In der Seite „Lokale Dienste > DHCP-Server > IP-Pool-Konfiguration“ finden sie einen IP-Pool aus dem Netz 192.168.3.x dessen Name identisch zum im Assistenten vergebenen Netzwerknamen für dieses Gäste-WLAN ist:

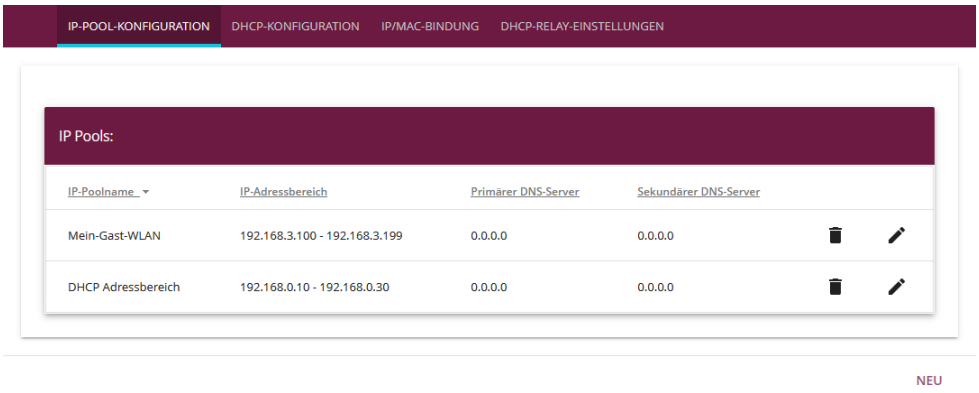


Abbildung 14: „Lokale Dienste > DHCP-Server > IP-Pool-Konfiguration“ Übersicht

In der Seite „Lokale Dienste > DHCP-Server > DHCP-Konfiguration“ finden sie schließlich die DHCP-Server-Instanz für diesen Pool, gebunden auf die virtuelle Schnittstelle für das VLAN 3:

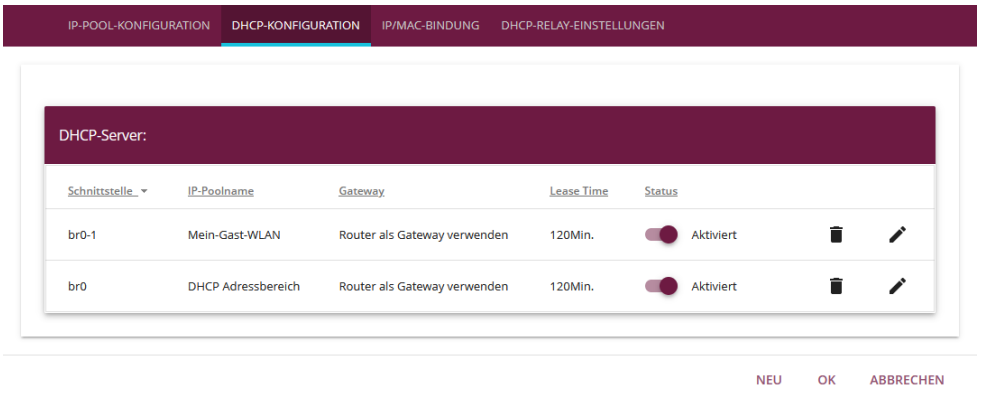


Abbildung 15: „Lokale Dienste > DHCP-Server > DHCP-Konfiguration“ Übersicht

Im Menü „Firewall“ hat der WLAN-Controller-Assistent Firewall-Regeln angelegt, die bewirken, dass die Geräte im Gästenetzwerk ins Internet kommen und der Zugriff auf alle anderen lokalen Netzwerke (inklusive eventuell eingerichteter weiterer Gästenetzwerke) sowie auf den Router selbst blockiert ist. In der Seite „Firewall > Richtlinien > IPv4-Filterregeln“ sehen sie zu diesem Zweck drei vom WLAN-Controller-Assistent angelegte Firewall-Regeln für die virtuelle Schnittstelle im VLAN 3 und eine Standardfilterregel:

1. Die erste Regel erlaubt den Zugriff auf unverzichtbare Dienste (DHCP und DNS) im Router, die in der Dienstgruppe „wlan-guest-local-access“ zusammengefasst sind.
2. Die zweite Regel ist eine optionale Regel (die sie auch über den Haken nachträglich deaktivieren können) die verhindert, dass über das Gästenetzwerk per IP-Telefonie telefoniert werden kann.
3. Die dritte Regel erlaubt den Zugriff auf die Internetschnittstelle und somit auf das Internet für die Dienste, die in der Dienstgruppe „Internet“ aufgeführt sind.
4. Da die virtuelle Schnittstelle für das VLAN 3 – wie erwähnt – auf „Nicht Vertrauenswürdig“ steht, greift somit als vierte Regel die Standardfilterregel „n+2“, die alle anderen durch die obigen Regeln nicht erfassten Datenverbindungen verwirft.

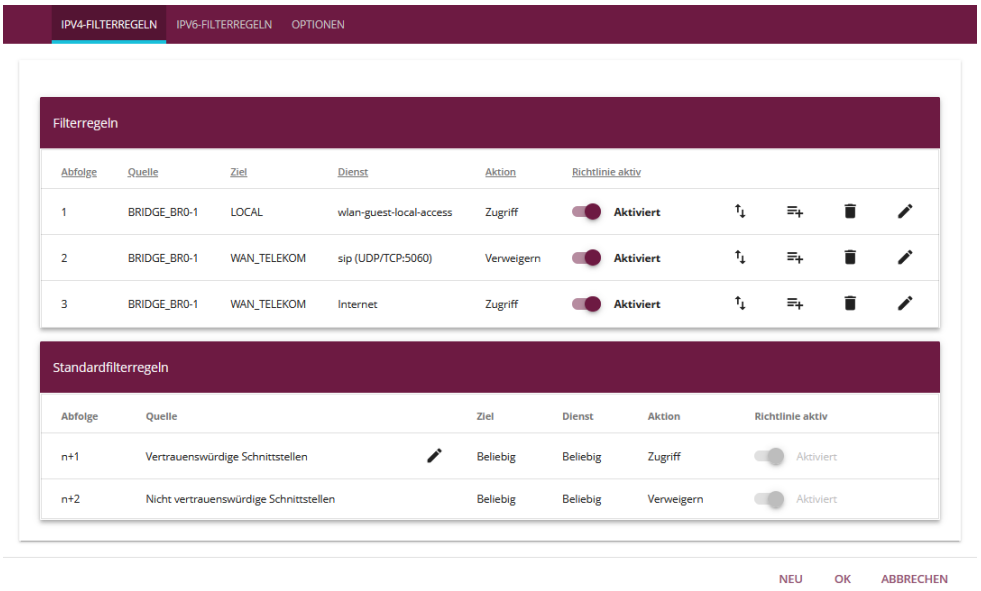


Abbildung 16: „Firewall > Richtlinien > IPv4-Filterregeln“ Übersicht

Die vom Assistenten angelegten Dienstgruppen „wlan-guest-local-access“ und „Internet“ finden sie in der GUI-Seite „Firewall > Dienste > Gruppen“. Dort können sie die in den jeweiligen Gruppen erlaubten Netzwerkdienste einsehen und auch nachträglich an ihre Bedürfnisse anpassen:

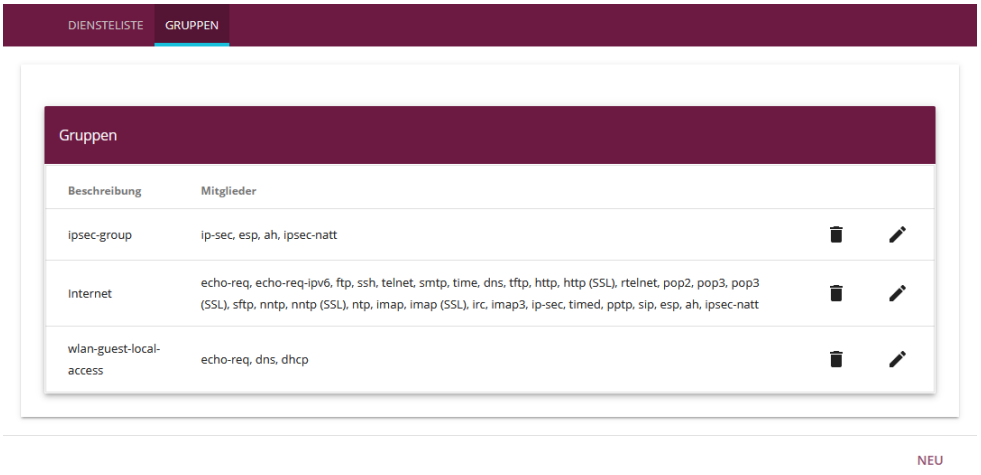


Abbildung 17: „Firewall > Dienste > Gruppen“ Übersicht

6.3 Wichtige Hinweise zum Thema VLAN

Damit das WLAN-Gästenetzwerk und andere VLAN-getaggte WLAN-Netzwerke auch an Access-Points funktionieren, die über einen Netzwerk-Switch an den WLAN-Controller-Router angeschlossen sind, muss ihr Netzwerk-Switch diese VLAN-IDs an allen Ports, an denen die Access-Points und der WLAN-Controller-Router angeschlossen sind, „getaggt“ zulassen. Die meisten modernen Netzwerk-Switche verwerfen alle VLANs, die im Netzwerk-Switch nicht explizit erlaubt sind.

Im Problemfall sehen ihre WLAN-Clients zwar das WLAN-Gästenetzwerk an den Access-Points und können sich auch im WLAN anmelden, erhalten jedoch keinerlei Netzwerkverbindung (und die

meisten Smartphones loggen sich infolgedessen sofort wieder vom WLAN aus, sodass es dort aussieht als könnte sich das Endgerät nicht mit dem WLAN verbinden).

Bitte richten sie daher in diesem Fall an ihrem Netzwerk-Switch die Durchleitung der jeweils benötigten VLANs entsprechend dem Handbuch ihres Netzwerk-Switch-Herstellers ein.

6.4 Einrichtung der E-Mail-Benachrichtigung bei Ausfall eines Access-Points

Seit BOSS-Release 7.10.1 gibt es die Möglichkeit, sich eine E-Mail vom WLAN-Controller schicken zu lassen, sobald ein verwalteter Access-Point ausfällt oder nicht mehr erreichbar ist. Besonders in größeren, komplexen WLAN-Infrastrukturen ist dies sehr hilfreich, da der Ausfall eines einzelnen Access-Points nicht sofort auffällt. Die dazu notwendige Konfiguration finden Sie im Menü „Externe Berichterstellung > Benachrichtigungsdienst > Benachrichtigungsempfänger“ (Die Server-Einstellungen zur E-Mail-Benachrichtigung werden hier nicht beschrieben). Dort fügen sie einen neuen Eintrag hinzu:

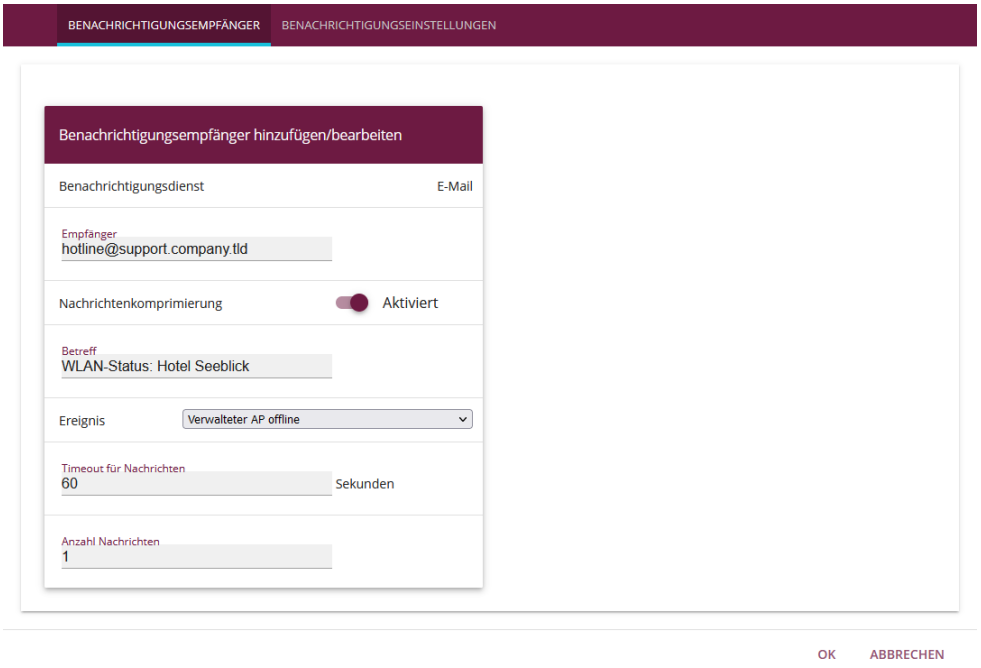


Abbildung 18: „Externe Berichterstellung > Benachrichtigungsdienst > Benachrichtigungsempfänger“ Benachrichtigung für ausgefallenen AP hinzufügen

Hier definieren sie ihre gewünschte E-Mail-Benachrichtigung:

1. **Empfänger**: Die E-Mailadresse des Postfachs, welches diese Benachrichtigung erhalten soll.
2. **Betreff**: Wählen sie einen passenden Betreff aus, damit sie die E-Mail in ihrem E-Mail-Postfach leichter zuordnen können.
3. **Ereignis**: Hier wählen sie in der Auswahlliste das vordefinierte Ereignis „Verwalteter AP offline“ aus.

7 Anhang

7.1 Konfiguration eines DHCP-Servers auf einem anderen bintec elmeg Router

Benötigt wird ein bintec elmeg Router mit BOSS-Software-Release 7.9.5 Patch 4 oder höher. Dort muss im Menü „Lokale Dienste > DHCP-Server > DHCP-Konfiguration“ in der Bearbeitungsseite die Option „CAPWAP Controller“ ausgewählt und die IP-Adresse des WLAN-Controllers ins Feld „Wert“ eingetragen werden:

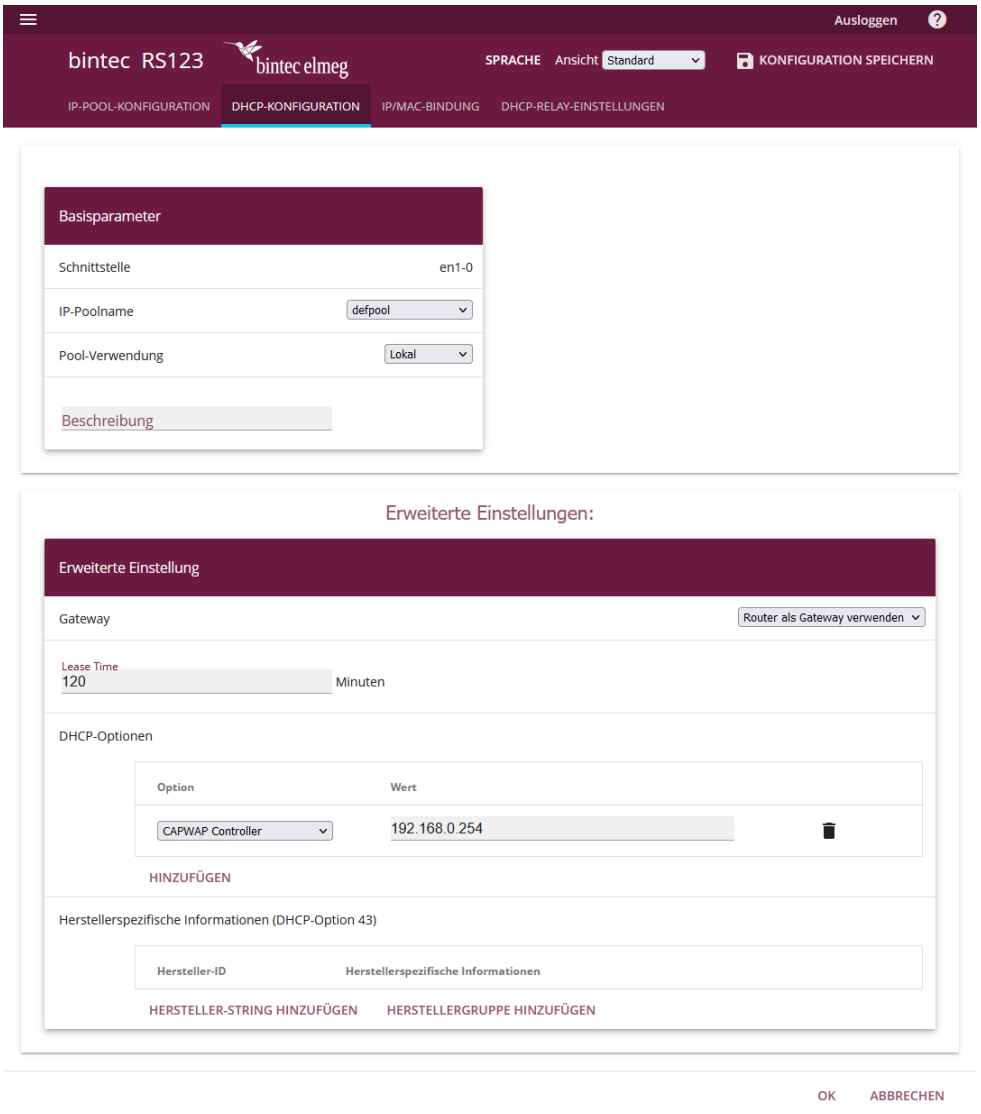


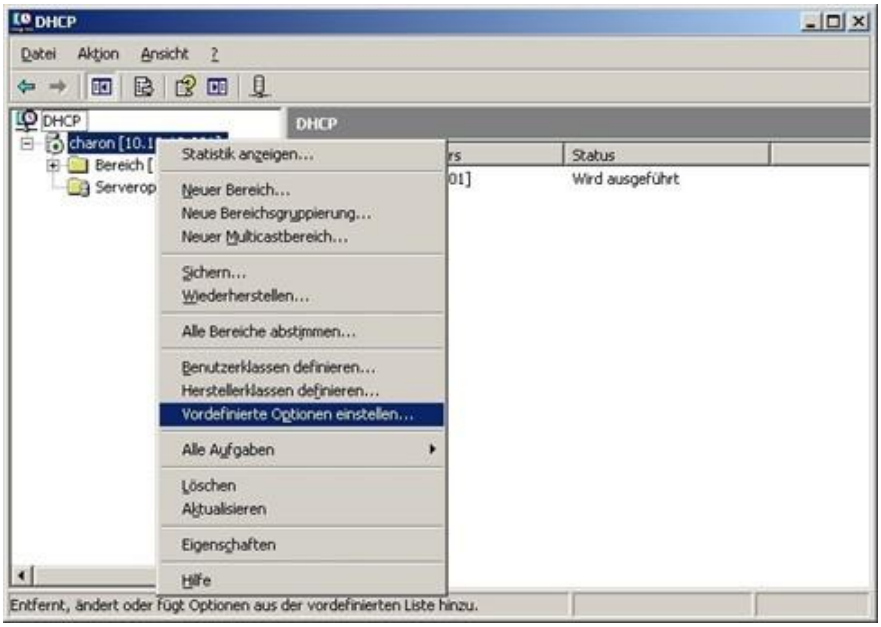
Abbildung 19: „Lokale Dienste > DHCP-Server > DHCP-Konfiguration“ Bearbeitungsseite CAPWAP Controller hinzufügen

7.2 Konfiguration eines DHCP-Servers auf Windows Server 2003/2008

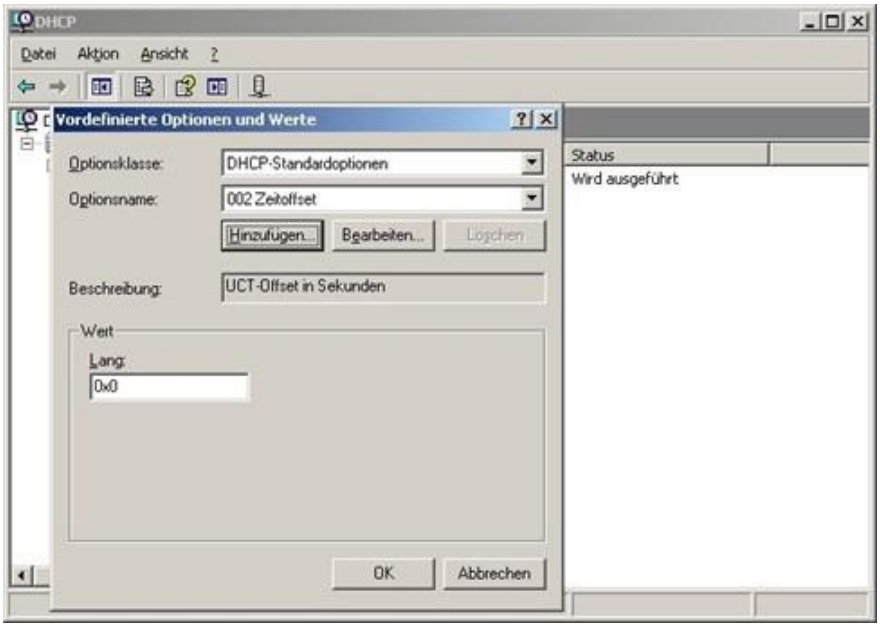
Zunächst sollten Sie Ihren Windows-DHCP-Serverdienst grundlegend einrichten, also den DHCP-IP-Adressbereich definieren, Standardoptionen wie DNS-Server und Standard-Gateway entsprechend der eigenen Netzwerkinfrastruktur konfigurieren.

Im Verwaltungsfenster des DHCP-Dienstes (zu erreichen über die Systemsteuerung und dort unter Verwaltung) führen Sie einen Rechtsklick auf die bestehende DHCP-Dienstinstanz aus und klicken im aufklappenden Kontextmenü auf „Vordefinierte Optionen einstellen“ (Der Name der Dienstinstanz

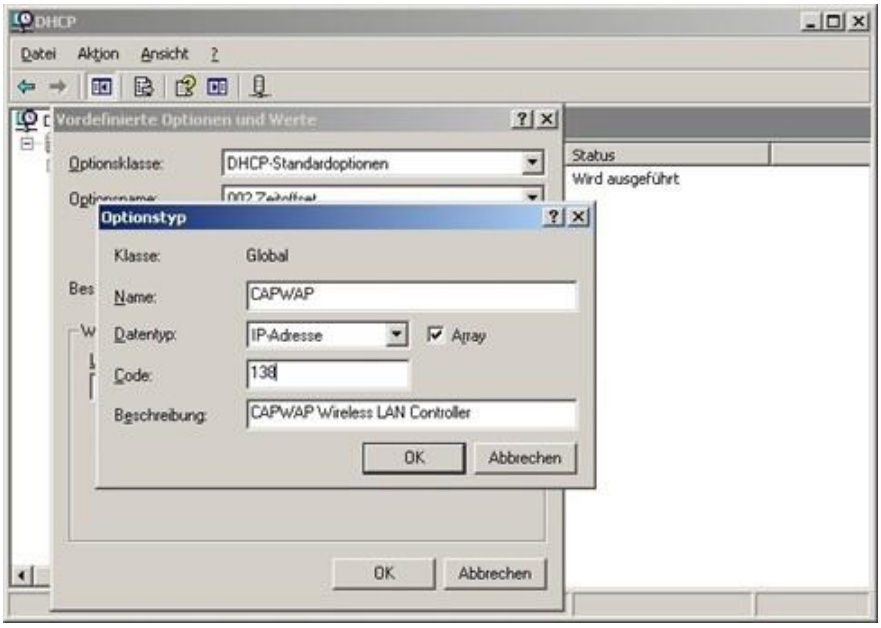
setzt sich zusammen aus dem Computernamen sowie in eckigen Klammern der IP-Adresse, unter der der DHCP-Dienst erreichbar ist):



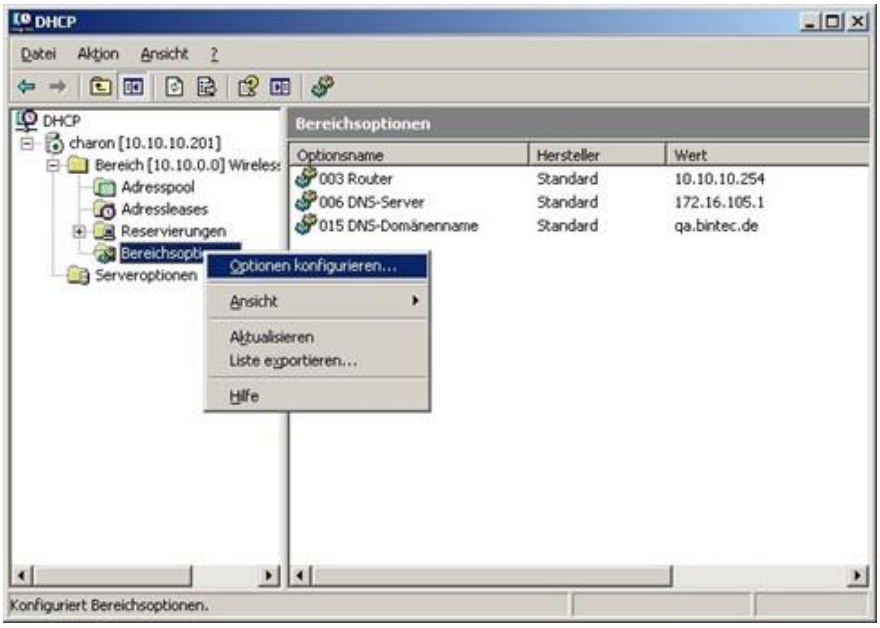
In dem sich nun öffnenden Fenster auf „Hinzufügen“ klicken, um die standardmäßig nicht vordefinierte CAPWAP-Option hinzuzufügen:



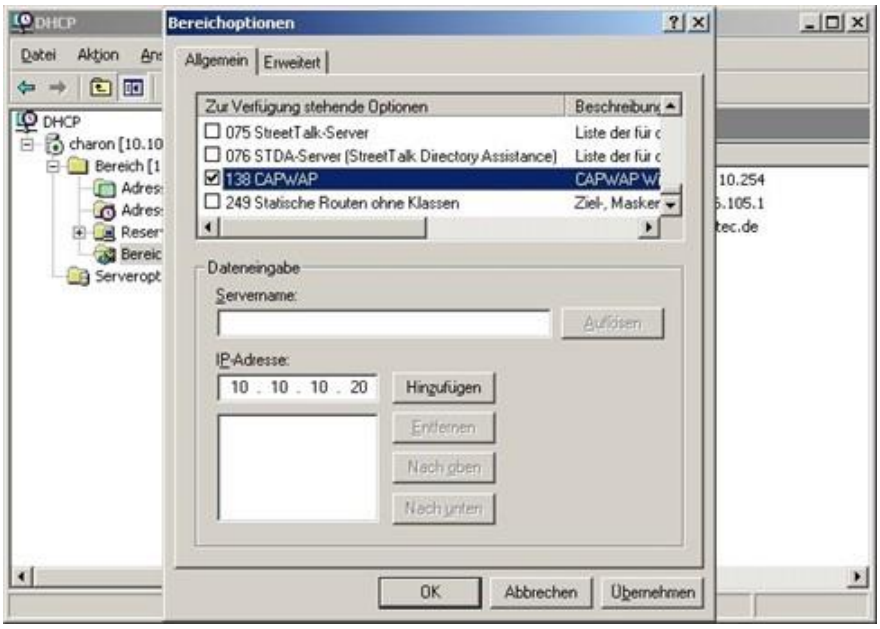
Im neuen Dialogfenster „Optionstyp“ wird jetzt die CAPWAP-Option definiert (nicht aktiviert). „Name“ und „Beschreibung“ sind dabei frei wählbar, sollten aber eingängig benannt werden. Der Datentyp muss auf „IP-Adresse“ eingestellt und der Haken vor „Array“ muss gesetzt sein. Ebenso muss der „Code“ auf „138“ gesetzt sein. Sollte der Code bereits für eine andere, selbst definierte DHCP-Option belegt sein, die nicht der CAPWAP-DHCP-Option entspricht, so muss diese zuvor gelöscht werden. Verlassen Sie den Dialog und das vorherige Fenster anschließend mit „OK“:



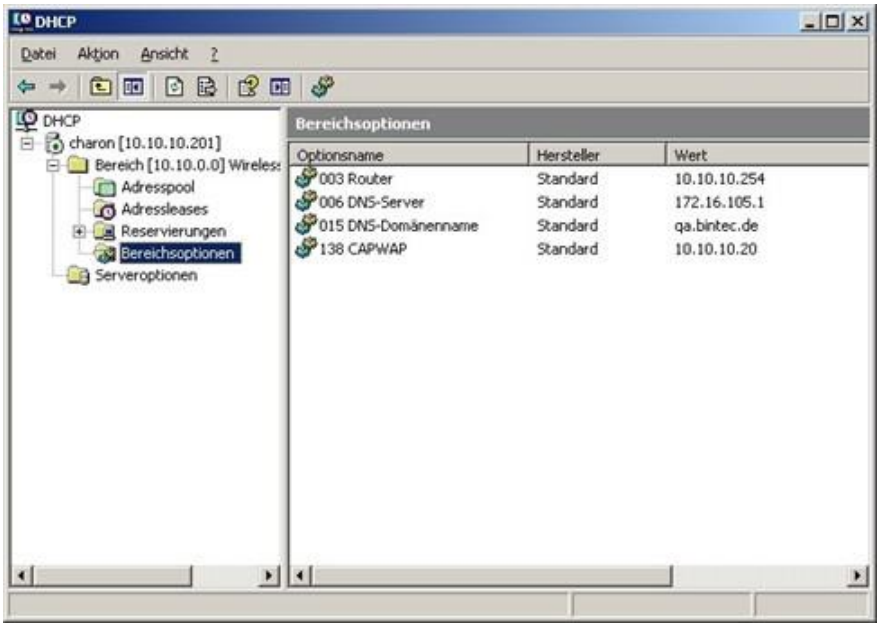
Führen Sie einen Rechtsklick im bereits vorkonfigurierten IP-Adressbereich des DHCP-Dienstes für die künftigen Access-Points auf „Bereichsoptionen“ aus und wählen Sie im Kontextmenü „Optionen konfigurieren“ aus:



Im nun aufklappenden Dialogfenster in der Liste der „Zu Verfügung stehenden Optionen“ die Option „138“ auswählen, im Eingabefeld „IP-Adresse“ die IP-Adresse des WLAN-Controllers eintragen und dann rechts daneben auf „Hinzufügen“ klicken. Theoretisch könnte man hier mehrere WLAN-Controller-IP-Adressen eintragen. Derzeit wird aber nur die erste IP-Adresse von den Access-Points berücksichtigt. Diese Dialogbox wird nun ebenfalls wieder mit „OK“ verlassen:



Im Übersichtsfenster des DHCP-Dienstes sollte nun auch die CAPWAP-Option aufgelistet sein. Im Anschluss können nun die Access-Points und der WLAN-Controller im Netz, in dem der soeben eingerichtete DHCP-Dienst erreichbar ist, in Betrieb genommen werden:



7.3 Konfiguration eines DHCP-Servers unter Linux

Fügen Sie der Konfigurationsdatei „/etc/dhcp/dhcpd.conf“ folgendes (angepasst an ihr Netzwerk) hinzu:

```
# Format definition of DHCP CAPWAP option for WLAN Controller
option wlan-controller code 138 = array of ip-address;
# IP address range for managed Access Points
subnet 192.168.0.0 netmask 255.255.255.255 {
      range 192.168.0.10 192.168.0.200;
      option domain-name-servers mydnsserver.mydomain.tld;
      # IP address of your gateway for this network
      option router 192.168.0.1;
      option broadcast-address 192.168.0.255;
      default-lease-time 7200;
      max-lease-time 7200;
      # IP address of your WLAN Controller
      option wlan-controller 192.168.0.251
}
```

Dabei sind vor allem die beiden Zeilen entscheidend, die mit „option wlan-controller“ beginnen. Die obere der beiden Zeilen definiert das Datenformat der Option 138, da dieses nicht in den Standardformatdefinitionen des dhcpd enthalten ist. Die untere Zeile spezifiziert die IP-Adresse des WLAN-Controllers, bei der sich dann die einzelnen Access-Points melden, nachdem sie alle benötigten Daten (eigene IP-Adresse, IP-Adresse des WLAN-Controllers etc.) vom DHCP-Server erhalten haben.

Die restlichen Angaben entsprechen dem Standard zur Definition eines DHCP-Pools: Sie müssen die Parameter für „subnet“, „range“, „domain-name-servers“, „routers“ usw. entsprechend Ihren eigenen Bedürfnissen konfigurieren.

Nachdem Sie die Konfiguration gesichert haben, müssen Sie den DHCP-Server-Dienst neu starten.

7.4 Betrieb der APs mit statischen IP-Adressen

Auf dem WLAN-Controller-Gerät ist beim Start des WLAN-Controller-Assistenten darauf zu achten, dass im ersten Schritt der Konfiguration für den DHCP-Server „Extern oder statisch“ ausgewählt wird.

Wie auf Seite 5 beschrieben, sorgt der DHCP-Server neben der Vergabe der IP-Adressen auch dafür, dass die zu verwaltenden Access-Points die IP-Adresse des WLAN-Controllers erhalten. Für den Fall, dass die Access-Points mit statischen IP-Adressen betrieben werden, ist es erforderlich, dass auf den zu verwaltenden Access-Points neben der IP-Adresse und der Netzwerkmaske auch die IP-Adresse des WLAN-Controllers konfiguriert wird.

Auf OSDx-basierten APs und auf BOSS-basierten APs ab BOSS-Release 7.10.1 finden sie Sie im Menü „Systemverwaltung > Globale Einstellungen > System“ das dazu benötigte Feld „Manuelle IP-Adresse des WLAN-Controllers“:

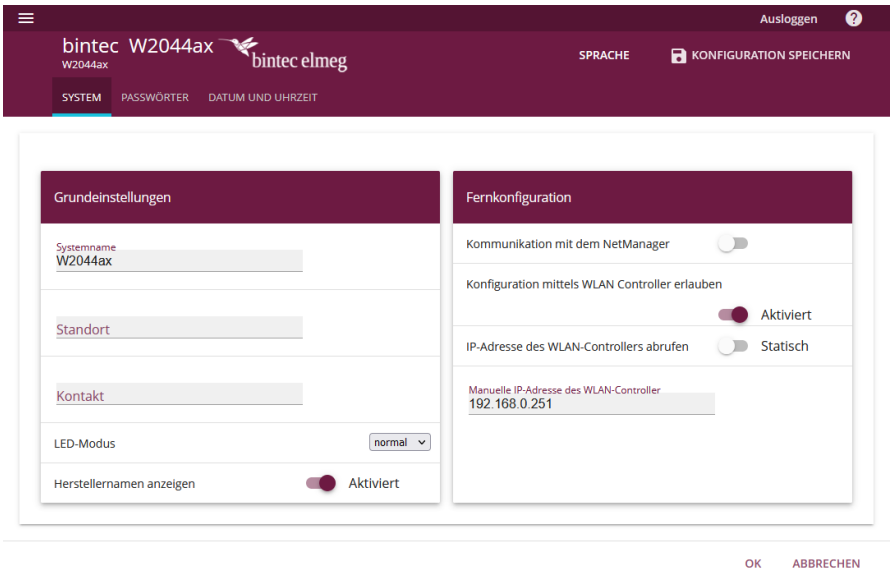


Abbildung 20: Einstellungen auf einem OSDx-basierten AP wie dem W2044ax

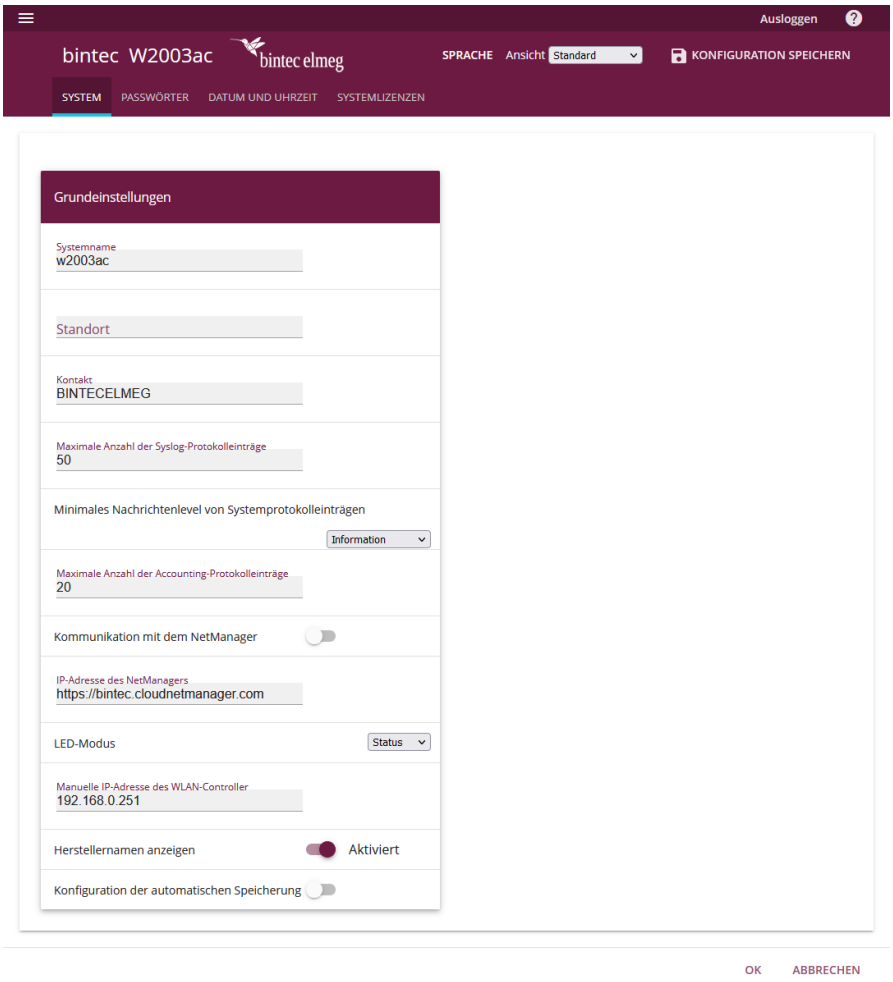


Abbildung 21: Einstellungen auf einem BOSS-basierten AP wie dem W2003ac