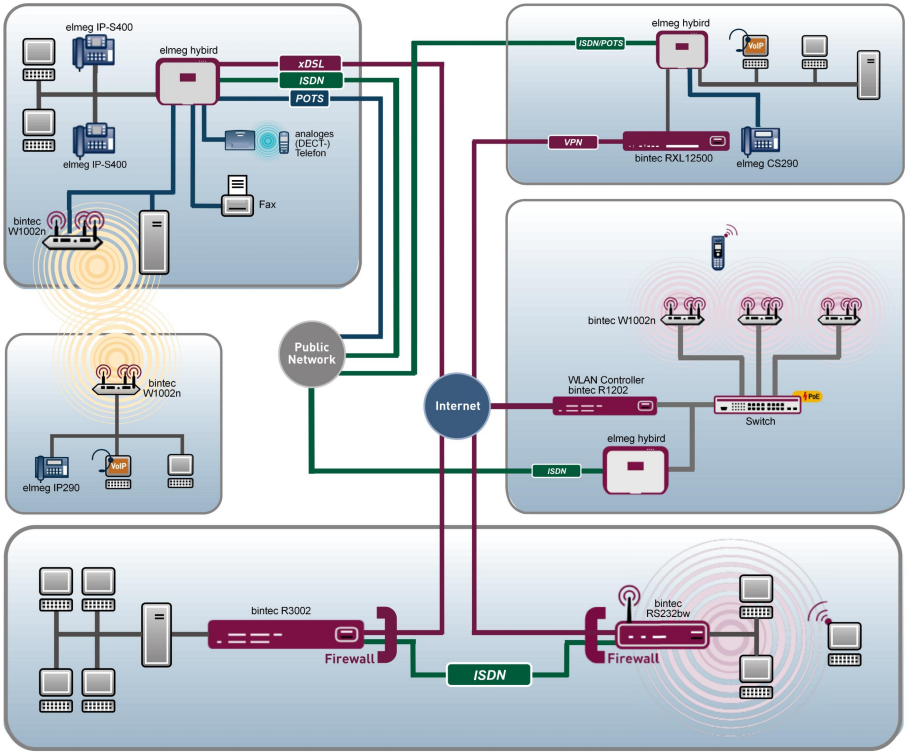


Benutzerhandbuch Workshops (Auszug)

WLAN-Workshops

Rechtlicher Hinweis

Ziel und Zweck
Dieses Dokument ist Teil des Benutzerhandbuchs zur Installation und Konfiguration von Teldat-Geräten. Für neueste Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere Release Notes lesen – insbesondere, wenn Sie ein Software-Update zu einem höheren Release-Stand durchführen. Die aktuellsten Release Notes sind zu finden unter *www.teldat.de* .

Haftung
Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in diesem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Teldat GmbH haftet nur im Umfang ihrer Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen sowie Release Notes für Teldat-Gateways finden Sie unter *www.teldat.de* .

Teldat-Produkte bauen in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen. Teldat GmbH übernimmt keine Verantwortung für Datenverlust, ungewollte Verbindungskosten und Schäden, die durch den unbeaufsichtigten Betrieb des Produkts entstanden sind.

Marken
Teldat und das Teldat-Logo, bintec und das bintec-Logo, artem und das artem-Logo, elmeg und das elmeg-Logo sind eingetragene Warenzeichen der Teldat GmbH.

Erwähnte Firmen- und Produktnamen sind in der Regel Warenzeichen der entsprechenden Firmen bzw. Hersteller.

Copyright

Richtlinien und Normen

Informationen zu Richtlinien und Normen finden Sie in den Konformitätserklärungen unter *www.teldat.de* .

Wie Sie Teldat GmbH erreichen
Teldat GmbH, Südwestpark 94, D-90449 Nürnberg, Deutschland, Telefon: +49 911 9673 0, Fax: +49 911 688 07 25
Teldat France S.A.S., 6/8 Avenue de la Grande Lande, F-33174 Gradignan, Frankreich, Telefon: +33 5 57 35 63 00, Fax: +33 5 56 89 14 05
Internet: *www.teldat.de*

Inhaltsverzeichnis

Kapitel 1 WLAN - Einführung in den bintec-WLAN-Controller

1.1 Überblick über die Funktionen

Der **bintec WLAN Controller** bietet Ihnen folgende Vorteile für das Management Ihrer WLAN-Infrastruktur:

- Assistenten-geführte Schnellinstallation in fünf Schritten
- Automatische Erkennung und Installation fabrikneuer Geräte
- VLAN- und Multi-SSID-Unterstützung
- Integrierter 802.11abgn-Support
- Optimiertes Roaming-Verhalten für VoWLAN
- Zentrale Verwaltung aller Access-Points:
  - Einfache Änderung von Einstellungen auf allen APs
  - Eine Änderung z. B. an den SSIDs wirkt sich immer sofort auf alle APs aus.
- Access-Points, die an öffentlich zugänglichen Stellen installiert sind, stellen nicht länger ein Sicherheitsrisiko dar:
  - Die Sicherung der Netzwerkschlüssel und Passwörter erfolgt nicht auf den APs. Sie können deshalb nicht durch einen Diebstahl der APs in unbefugte Hände gelangen.
  - Jede direkte AP-(Konfigurations)-Verbindung wird durch den WLAN-Controller verworfen.
- Automatisiertes Frequenzmanagement:
  - Integrierte Kanalplanung, um eine überlappungsfreie Frequenzvergabe zu erreichen
  - Minimierung der Interferenzen durch intelligente Frequenzvergabe
  - Berücksichtigung von Access-Points, die nicht zum eigenen Netz gehören (Neighbor AP)
- Überwachung:
  - des Access-Point-Betriebs
  - der Client-Aktivität
  - Erkennung und Anzeige von unerwünschten Access Points (Neighbor Access Points)
- E-Mail-Benachrichtigung bei Ausfall eines verwalteten Access Points
- Programm-gesteuerte Aktionen (z. B. Ausschalten des WLANs während der Nacht)

- Konfigurationsmanagement: Die Konfiguration wird zentral gespeichert und wird automatisch an die APs neu verteilt, z. B. im Fall eines Stromausfalls
- Zentralisierte Software-Updates

1.2 Projektplanung

1.2.1 Anforderungen des Kunden ermitteln

Am Anfang steht der Kunde - und die Frage, was er wirklich benötigt. In den meisten Fällen wünscht sich der Kunde ein WLAN-Netz im 2,4GHz-Frequenzbereich, damit sich Mitarbeiter und Gäste in den Büros und in den Besprechungsräumen mit dem Firmennetz und mit dem Internet drahtlos verbinden können. Zu diesem Zeitpunkt muss auch die Frage beantwortet werden, ob eine professionelle, von einem Fachmann durchgeführte Funkausleuchtung notwendig ist. Aufgrund der hohen Kosten für eine solche Analyse wird man in den meisten Fällen darauf verzichten und statt dessen die Access-Points (AP) 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.

1.2.2 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 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 Ethernetkabel (PoE) erspart die Installation einer 230V-Steckdose und vereinfacht die Montage erheblich.

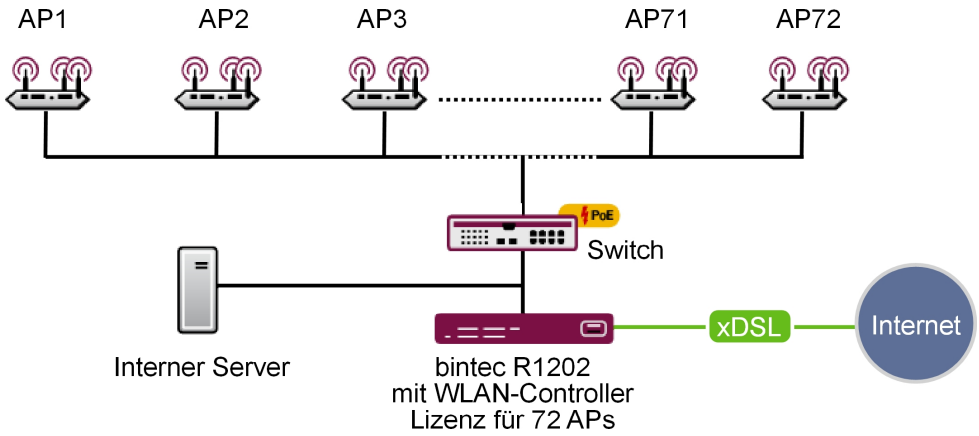


Abb. 2: WLAN-Infrastruktur

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.

1.3 Systemanforderungen

1.3.1 WLAN-Controller-Hardware

Folgende Geräte, deren Firmwareversion 7.9.6 oder höher ist, können als WLAN-Controller verwendet werden (unterstützte Geräte, deren Firmwareversion älter als 7.9.6 ist, müssen vor der Installation aktualisiert werden):

- **bintec W1002n**: Single-Radio-Indoor-Access-Point
- **bintec WI1040n**: Single-Radio-Indoor-Industrial-Access-Point (IP 40)
- **bintec WI2040n**: Dual-Radio-Indoor-Industrial-Access-Point (IP 40)
- **bintec WI1065n**: Single-Radio-Outdoor-Industrial-Access-Point (IP 65)
- **bintec WI2065n**: Dual-Radio-Outdoor-Industrial-Access-Point (IP 65)
- **bintec R1202**: Medium Router, VPN-Gateway
- **bintec R3002**: Medium Router, VPN-Gateway mit ADSL-2+-Modem
- **bintec R3502**: Medium Router, VPN-Gateway mit VDSL-2-Modem (Minimal benötigte Firmwareversion: 7.10.1)
- **bintec R3802**: Medium Router, VPN-Gateway mit SHDSL.bis-Modem
- **bintec R4402**: Medium Router, VPN-Gateway mit PRI-Interface
- **bintec RXL12100**: Central Router, Hochleistungs-Multiplex-VPN-Gateway (Minimal be-

nötigte Firmwareversion: 7.10.1)

- **bintec RXL12500**: Central Router, Hochleistungs-Central-Site-VPN-Gateway (Minimal benötigte Firmwareversion: 7.10.1)

Für kleine Installationen mit bis zu sechs Access-Points wird keine dedizierte WLAN-Controller-Hardware benötigt und einer der Accsess-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 mindestens ein R1202 als WLAN-Controller-Hardware notwendig.

1.3.2 Access-Point-Hardware

Der WLAN-Controller kann die folgenden WLAN-Geräte verwalten. Diese benötigen mindestens die Firmwareversion 7.9.6 (Geräte, deren Firmwareversion älter als 7.9.6 ist, müssen vor der Installation aktualisiert werden):

- **bintec W1002n**: Single-Radio-Indoor-Access-Point
- **bintec WI1040n**: Single-Radio-Indoor-Industrial-Access-Point (IP 40)
- **bintec WI2040n**: Dual-Radio-Indoor-Industrial-Access-Point (IP 40)
- **bintec WI1065n**: Single-Radio-Outdoor-Industrial-Access-Point (IP 65)
- **bintec WI2065n**: Dual-Radio-Outdoor-Industrial-Access-Point (IP 65)

1.3.3 WLAN-Controller-Lizenzen

Bei jedem unterstützten Gerät ist zu Testzwecken der WLAN-Controller in der Software bereits freigeschaltet, allerdings kann lediglich ein Access-Point verwaltet werden. Für den Produktivbetrieb muss auf dem Controller eine WLAN-Controller-Lizenz installiert werden. Mit jeder Lizenz lassen sich sechs Access-Points verwalten. Auf einem Access-Point (z. B. W1002n) lässt sich eine WLAN-Controller-Lizenz installieren, damit können inklusive des Access-Points auf dem der Controller läuft, sechs Access Points verwaltet werden. Auf einem Medium Router (z. B. R1202) lassen sich bis zu zwölf WLAN-Controller-Lizenzen installieren und damit bis zu 72 Access-Points verwalten. Auf Central Routern (z. B. RXL12100) können bis zu 25 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:

Erforderlich	bis zu 6 APs	bis zu 12 APs	bis zu 18 APs	bis zu 72 APs	bis zu 150 APs
Minimal-benötigte Con-	Keine, läuft auf dem Mas-	R1202	R1202	R1202	RXL12100

Erforderlich	bis zu 6 APs	bis zu 12 APs	bis zu 18 APs	bis zu 72 APs	bis zu 150 APs
troller-Hardware	ter-AP				
WLAN-Controller-Lizenzen	1x	2x	3x	6x	25x

1.4 Netzwerk-Konfiguration

1.4.1 Netzwerkeinstellungen des WLAN-Controllers

Bevor Sie den WLAN-Controller mit dem Netzwerk, das aus (noch immer unkonfigurierten) Access-Points besteht, verbinden können, benötigt er gemäß der Netzwerkinstallation in ihrem lokalem Netzwerk eine korrekte IP-Adresse sowie Netzwerkeinstellungen, die sich von den werksseitigen Standardeinstellungen unterscheiden. Andernfalls wird der nächste Schritt scheitern.

1.4.2 DHCP-Server

1.4.2.1 Interner DHCP-Server

Falls sich noch kein anderer aktiver DHCP-Server in ihrem Netzwerk befindet und der WLAN-Controller auch als DHCP-Server dienen soll, können Sie direkt zu *WLAN-Installation mithilfe des Assistenten des WLAN-Controllers* auf Seite 6 wechseln und die WLAN-Installation beginnen, da der Assistent des WLAN-Controllers alle benötigten Einstellungen für den DHCP-Server bereits richtig konfiguriert.

1.4.2.2 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 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 konfiguriert werden.

- Ein anderer bintec-Router arbeitet als DHCP-Server:

  Die notwendigen Konfigurationsschritte sind im Anhang erläutert.

- Ein Microsoft Server 2003 oder Server 2008 arbeitet als DHCP-Server:

  Die notwendigen Konfigurationsschritte sind im Anhang erläutert.
- Ein Linux-Server arbeitet als DHCP-Server:

  Die notwendigen Konfigurationsschritte sind im Anhang erläutert.
- Ein Router eines Drittanbieters arbeitet als DHCP-Server:

  Bitte nehmen Sie die Konfiguration der DHCP-Option 138 anhand der Kundendokumentation des Routers vor.

1.4.2.3 Kein DHCP-Server - APs mit statischen IP-Adressen

Bisweilen ist es notwendig einen WLAN-Controller mit statischen IP-Adressen und Netzwerkeinstellungen zu betreiben. Dazu muss auch vorher jedem AP manuell eine IP-Adresse zugeordnet werden. Die benötigten Konfigurationsschritte für alle Access-Points werden im *Anhang* auf Seite 13 beschrieben.

1.5 WLAN-Installation mithilfe des Assistenten des WLAN-Controllers

Der Assistent des WLAN-Controllers führt Sie in fünf Schritten durch die Konfiguration und Installation Ihres WLAN-Netzwerkes.

1.5.1 Schritt 1 im Assistenten

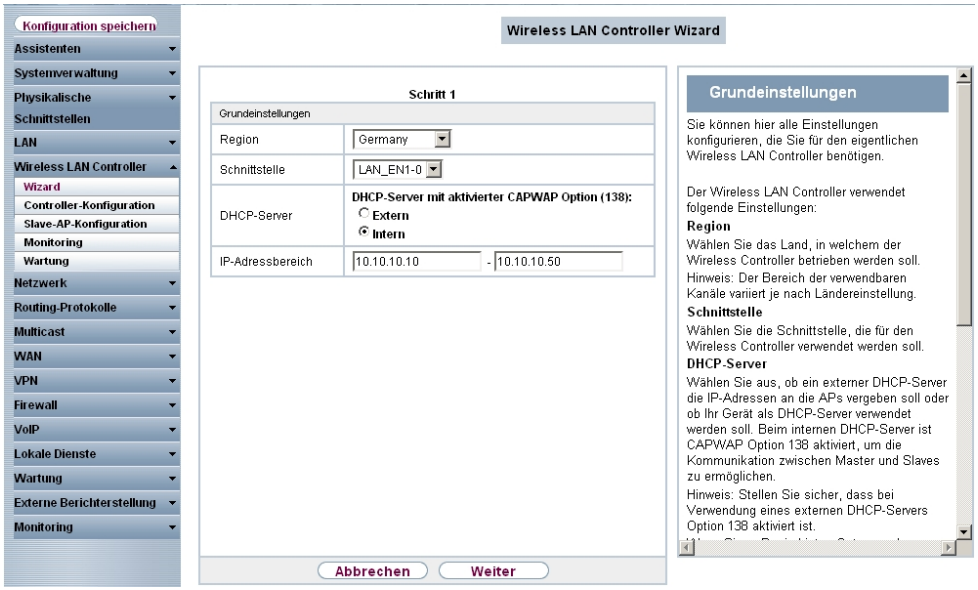


Abb. 3: **Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard**

Hier legen Sie einige grundlegende Eigenschaften des WLAN-Controllers fest:

(1) **Region**: Die Region, in der sich Ihr WLAN-Netzwerk befindet. Diese Einstellung passt Ihr WLAN-Netzwerk an die WLAN-Bestimmungen (z B. welche Frequenzen erlaubt sind) in Ihrem Gebiet an.

(2) **Schnitstelle**: 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).

(3) **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* auf Seite 13.

(4) **IP-Adressbereich**: Legt den IP-Adressbereich für den internen DHCP-Server fest.

Hinweis

Bevor Sie fortfahren, stellen Sie bitte sicher, dass ein eventuell vorhandener externer DHCP-Server betriebsbereit ist und dass die DHCP-Option 138 aktiv ist. Falls ein externer 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 anzeigt. 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 Reset bei den APs durchgeführt werden.

1.5.2 Schritt 2 im Assistenten

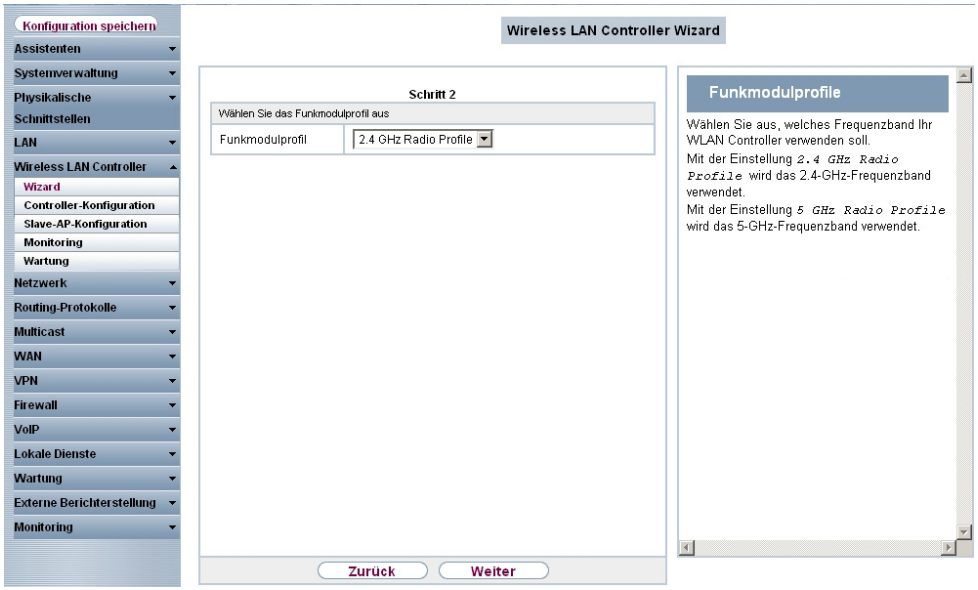


Abb. 4: **Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard**

Hier wird festgelegt, mit welchem Funkprofil das WLAN-Netzwerk arbeiten soll. Standardmäßig sind ein 2,4-GHz- und ein 5-GHz-Funkprofil vorhanden. Weitere Funkprofile lassen sich über das Menü **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Funkmodulprofile** anlegen.

1.5.3 Schritt 3 im Assistenten

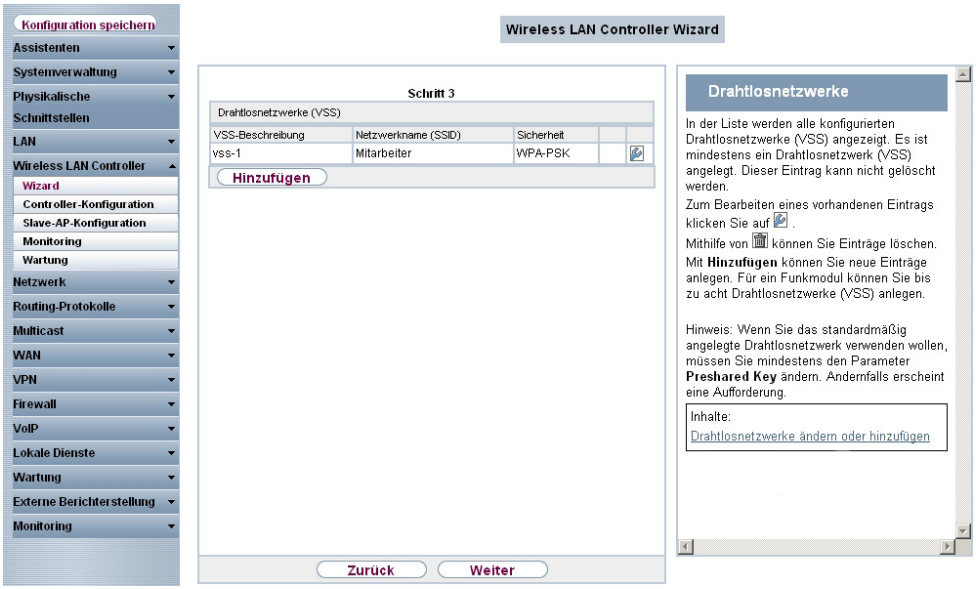


Abb. 5: **Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard**

Hier wird festgelegt, welche SSIDs / VSSs im WLAN-Netz vorhanden sein sollen. Standardmäßig ist bereits ein VSS vorhanden, dieses kann über das Werkzeuglogo angepasst werden. Über **Hinzufügen** können bis zu sieben weitere VSSs angelegt werden.

In diesem Beispiel legen wir ein weiteres VSS für einen Gastzugang an.

Abb. 6: **Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard**

Für das neue Wireless-Network-Profil (VSS) wird ein Netzwerkname vergeben und als **Sicherheitsmodus** wird *WPA-PSK* ausgewählt. Da in diesem Beispiel der Zugang ins Intranet des Unternehmens nicht erlaubt sein soll, wird ein VLAN für dieses VSS (im Beispiel *VLAN-ID 2*) definiert. Daraufhin werden auf Ethernet-Ebene alle Daten aus diesem Netzwerk mit VLAN 2 markiert.

Hinweis

VLAN-ID 0 und 1 sind für die System-Verwaltung reserviert und können deshalb nicht für VSSs verwendet werden.

Durch die Auszeichnung mit Tags haben Sie die Möglichkeit die Gästedaten von den anderen zu trennen und Ihre Netzwerk-Switches oder Internet-Access-Router so einzurichten, dass z. B. alle Daten und Benutzer aus VLAN ID 2 Zugriff auf das Internet haben, aber nicht auf das Intranet des Unternehmens (an dieser Stelle verweisen wir Sie auf das Handbuch Ihres Switches oder Routers, um eine Trennung der Netze mithilfe von VLAN zu konfigurieren).

Nachdem Sie die VSS-Konfiguration mit **OK** verlassen haben, befinden Sie sich wieder in der VSS-Übersichtsseite. Bevor Sie mit Schritt 4 fortfahren, vergewissern Sie sich bitte, dass alle verwalteten Access-Points mit dem LAN verbunden und aktiviert sind.

1.5.4 Schritt 4 im Assistenten

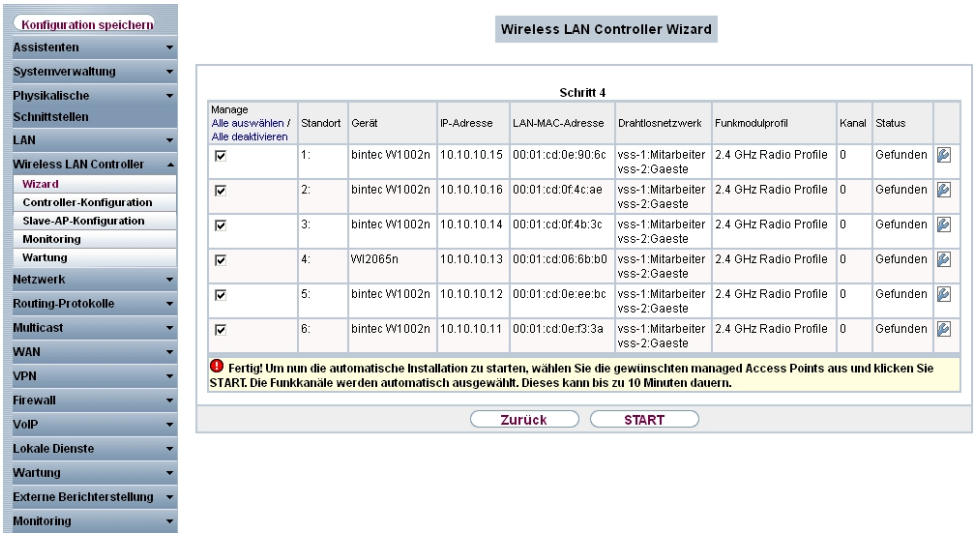


Abb. 7: **Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard**

Hier werden nun alle gefundenen Access-Points angezeigt. Standardmäßig sind allen Access-Points alle definierten Wireless-Network-Profile (VSS) und das zuvor ausgewählte Funkprofil zugeordnet. Mit einem Klick auf das Werkzeugsymbol können Sie nun diese Standardeinstellungen anpassen und außerdem jedem Gerät eine individuelle Standortbeschreibung geben.

Hinweis

In manchen Fällen werden nicht alle erwarteten APs angezeigt. Der WLAN-Controller konnte diese dann nicht finden. Hier können Sie **Zurück** verwenden, um die Display-Anzeige zu aktualisieren.

1.5.5 WLAN-Initiierung der Access-Points starten

Nachdem Sie von jedem Access-Point, den Sie verwenden wollen, die zugehörige Check-Box in der Manage-Spalte ausgewählt haben, können Sie die Initiierung des WLAN-Controllers sowie die automatische Verwaltung der Frequenzen mit einem Klick auf **Start** anstoßen. Die Anzeige wechselt nun zu einer Statusanzeige, die aktuelle Aktivitäten des WLAN-Controllers anzeigt.

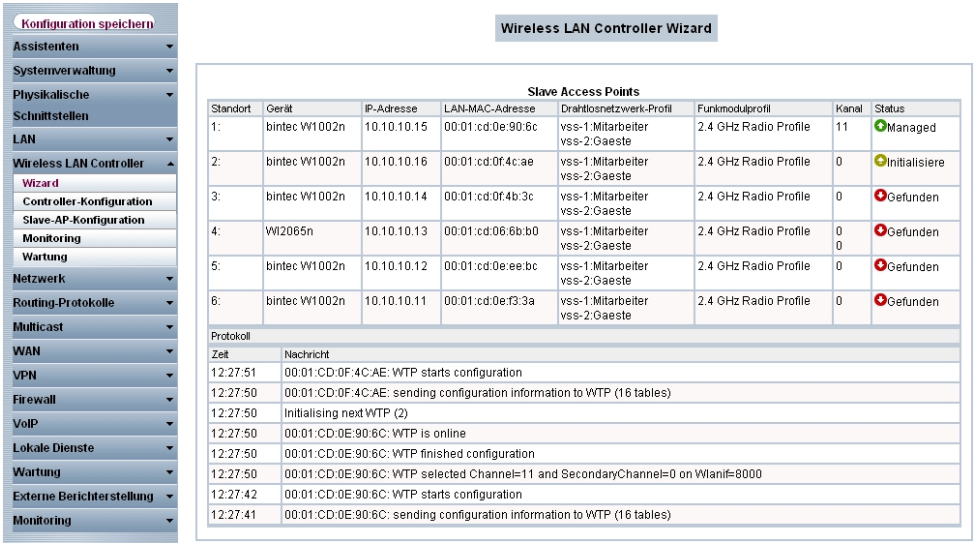


Abb. 8: **Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard**

Die Konfiguration wird jetzt der Reihe nach an alle Access-Points übertragen. Sobald für alle Access-Points der optimale Funkkanal gefunden wurde, ist die Konfiguration der Access-Points abgeschlossen und sie erhalten den Status `Managed`. Bei der Vergabe der Funkkanäle achtet der WLAN-Controller darauf, dass ausschließlich überlappungsfreie Kanäle (in der Voreinstellung 1, 6, 11) vergeben werden und dass die Interferenzen zwischen den einzelnen Access-Points so gering wie möglich sind.

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

Sobald alle Access-Points verwaltet sind, ändert sich die Display-Anzeige noch einmal und zeigt das Ergebnis an.

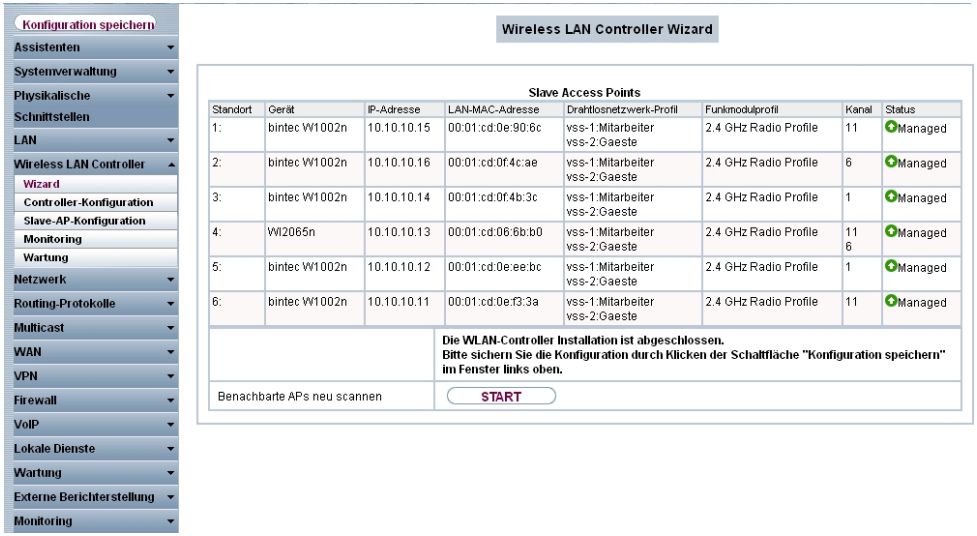


Abb. 9: **Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard**

Die Konfiguration der Access-Points sollte nun auf dem WLAN-Controller durch einen Klick auf die Schaltfläche **Konfiguration speichern** (links oben) bootfest gesichert werden. Die Access-Points halten ihre eigenen Einstellungen nur im flüchtigen Speicher. Im Fall eines Stromausfalls erhalten die Acess-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.

Nach dem Stromausfall werden alle Access-Points gleichzeitig vom WLAN-Controller neu gestartet. Dabei wird das Funkmanagement nicht erneut gestartet, sondern der zuvor benutzte Kanal verwendet. Die Wiederherstellung der WLAN-Infrastruktur erfolgt somit viel schneller als bei einer Erstinstallation.

1.6 Anhang

1.6.1 E-Mail-Benachrichtigung bei Ausfall eines Access-Points

Seit 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-Point nicht sofort auffällt. Die dazu notwendige Konfiguration finden Sie im Menü **Externe Berichterstellung** -> **E-Mail-Benachrichtigung** -> **E-Mail-Benachrichtigungsempfänger** (Die Server-Einstellungen zur E-Mail-Benachrichtigung werden hier nicht beschrieben).

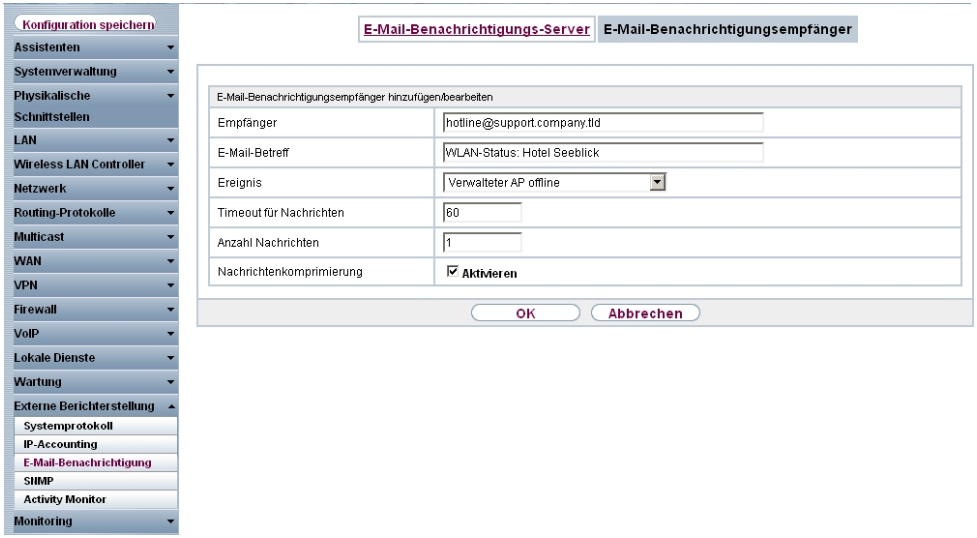


Abb. 10: **Externe Berichterstellung->E-Mail-Benachrichtigung->E-Mail-Benachrichtigungsempfänger**

1.6.2 Konfiguration eines DHCP-Servers auf einem anderen bintec-Router

Benötigt wird ein bintec-Router mit dem Software-Release 7.9.5 Patch 4 oder höher. Dort muss die DHCP-Option `CAPWAP Controller` im Menü **Lokale Dienste** -> **DHCP-Server** -> **DHCP Pool** ausgewählt und die IP-Adresse des WLAN-Controllers ins Feld **Wert** eingetragen werden.

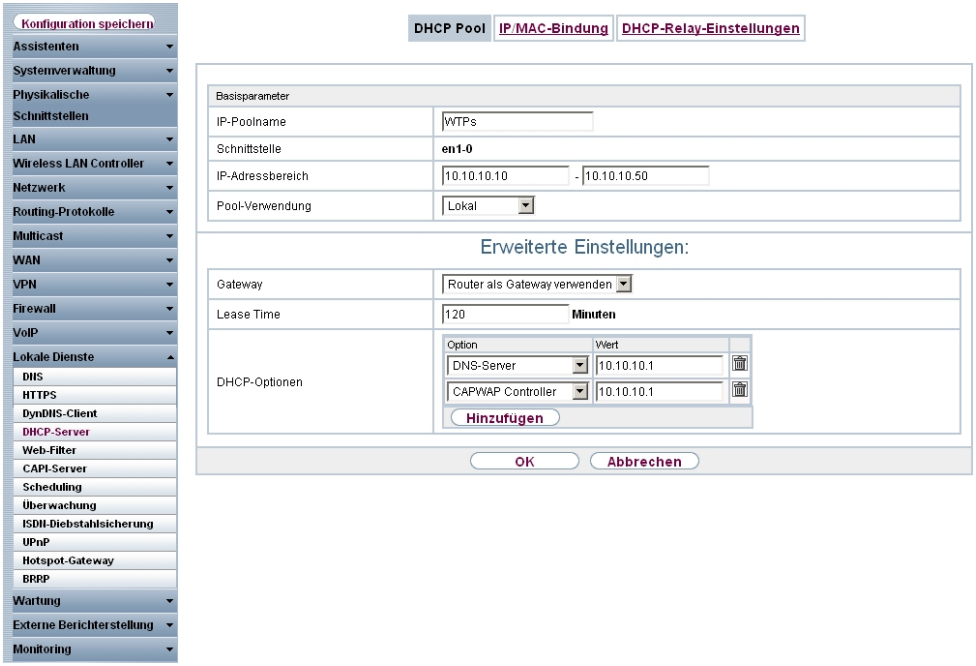
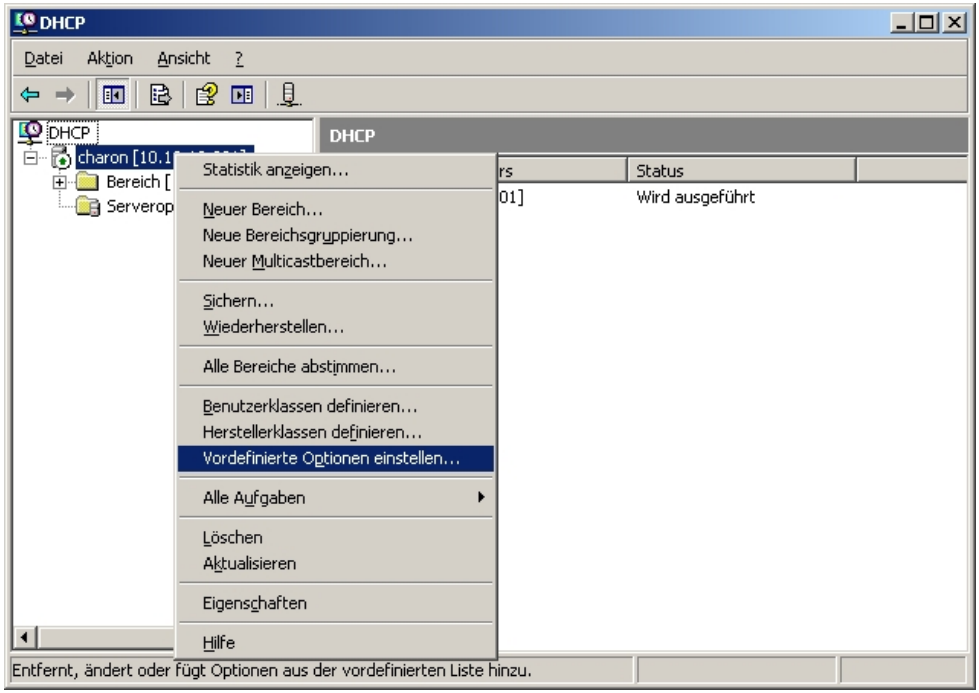


Abb. 11: **Lokale Dienste** -> **DHCP-Server** -> **DHCP Pool**

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

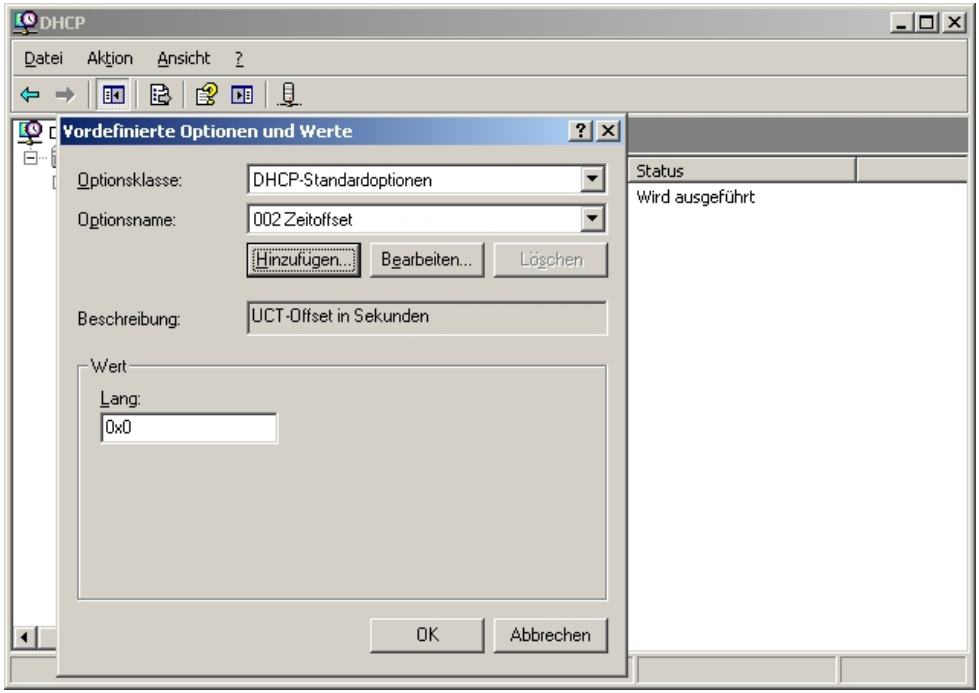
Zunächst sollten Sie Ihren Windows-DHCP-Serverdienst grundlegend einrichten, also den DHCP-IP-Adressbereich definieren, Standardoptionen wie DNS-Server und Standard-Gateway entsprechend der eigenen Netzwerkinfrastruktur konfigurieren.

1.6.3.1 1. Schritt



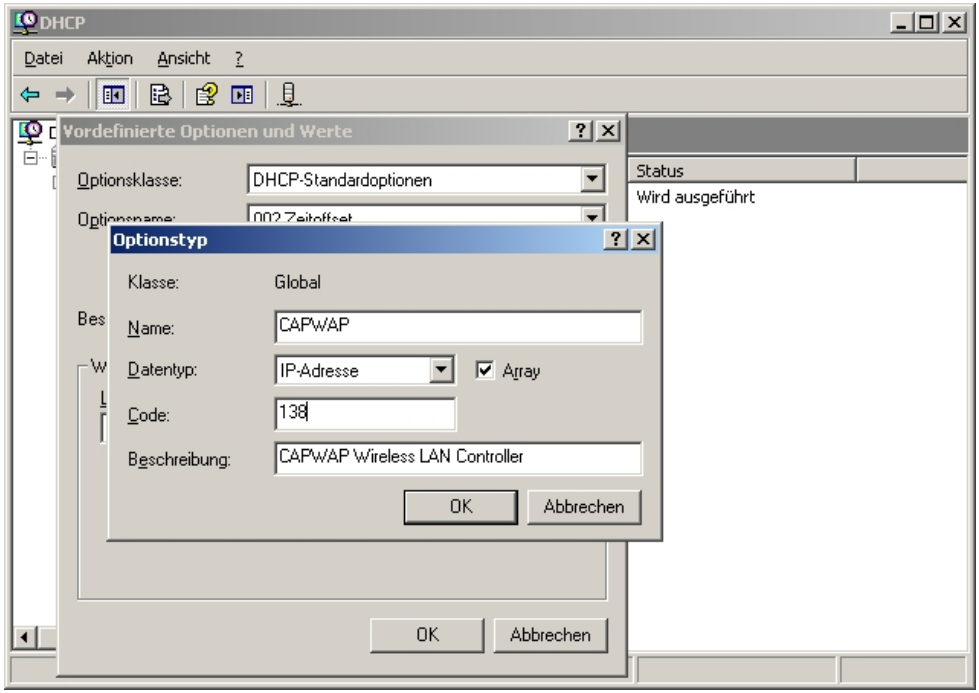
Im Verwaltungsfenster des DHCP-Dienstes (zu erreichen über die Systemsteuerung und dort unter Verwaltung) führen Sie einen Rechtsklick auf die bestehende DHCP-Dienstinstanz aus und klicken im aufklappenden Kontextmenü auf **Vordefinierte Optionen einstellen** (Der Name der Dienstinstanz setzt sich zusammen aus dem Computernamen sowie in eckigen Klammern der IP-Adresse, unter der der DHCP-Dienst erreichbar ist).

1.6.3.2 2. Schritt



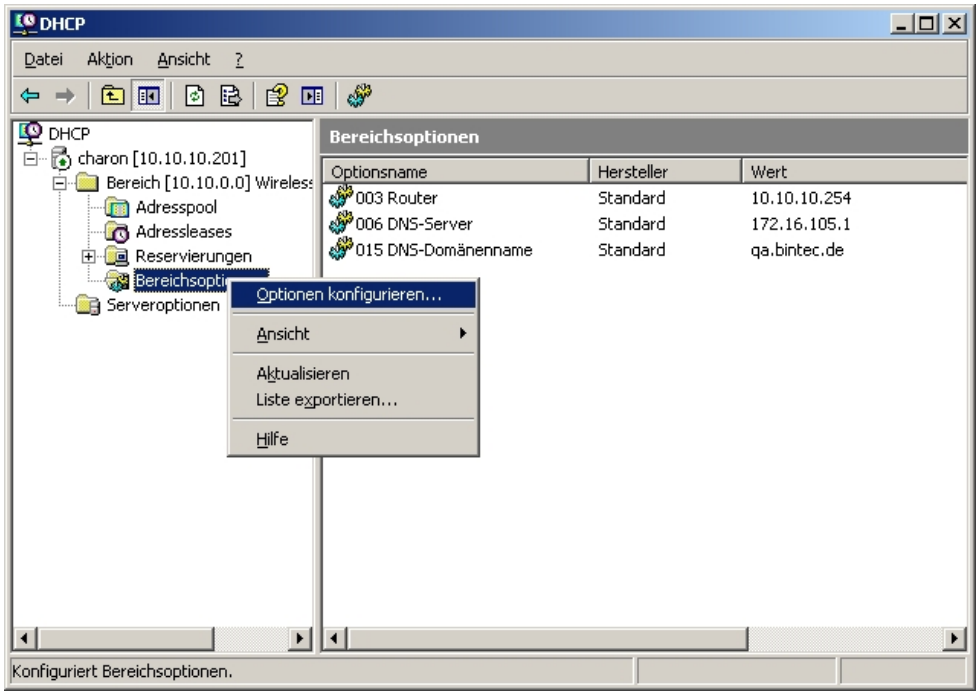
In dem sich nun öffnenden Fenster auf **Hinzufügen** klicken, um die standardmäßig nicht vordefinierte CAPWAP-Option hinzuzufügen.

1.6.3.3 3. Schritt



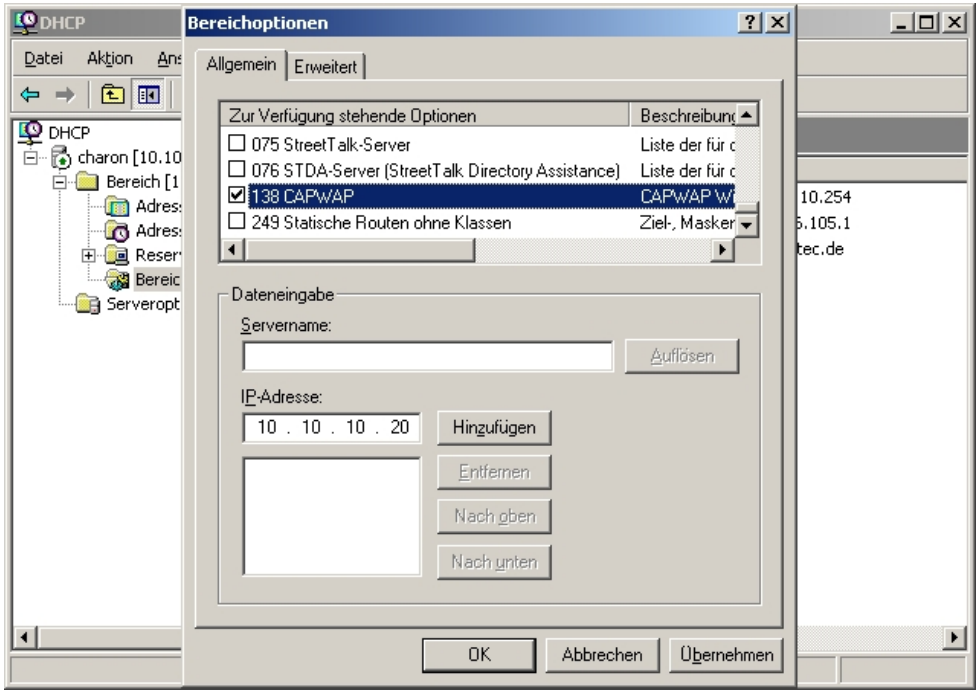
Im neuen Dialogfenster **Optionstyp** wird jetzt die CAPWAP-Option definiert (nicht aktiviert). **Name** und **Beschreibung** sind dabei frei wählbar, sollten aber eingängig benannt werden. Der Datentyp muss auf *IP Adresse* eingestellt und der Haken vor **Array** muss gesetzt sein. Ebenso muss der **Code** 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**.

1.6.3.4 4. Schritt



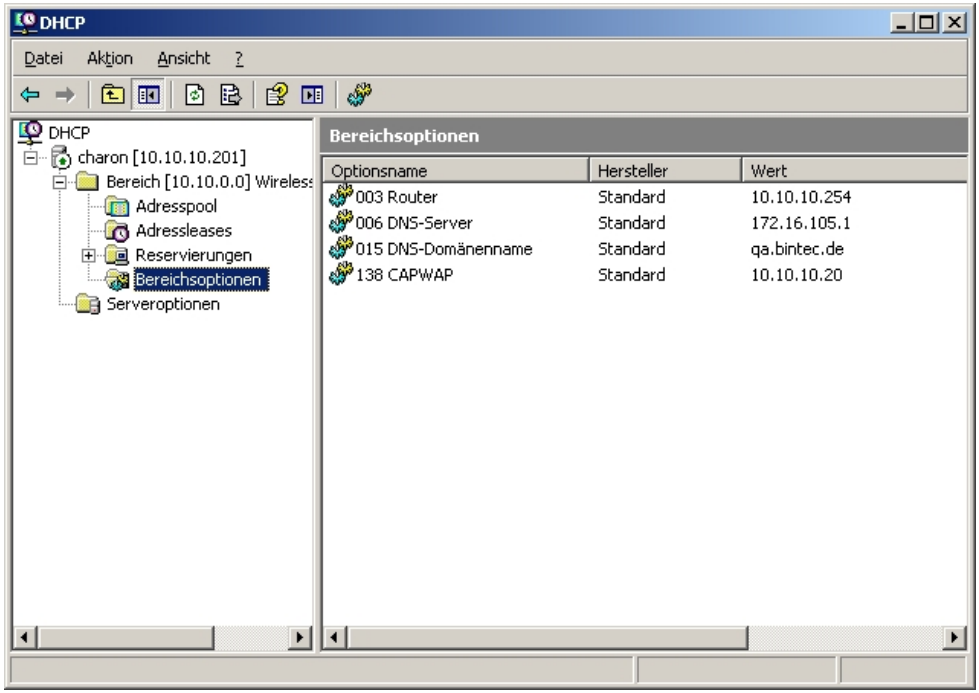
Führen Sie einen Rechtsklick im bereits vorkonfigurierten IP-Adressbereich des DHCP-Dienstes für die künftigen Slave-Access-Points auf **Bereichsoptionen** aus und wählen Sie im Kontextmenü **Optionen konfigurieren** aus.

1.6.3.5 5. Schritt



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.

1.6.3.6 6. Schritt



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.

1.6.4 Konfiguration eines DHCP-Servers unter Linux

Fügen Sie der Konfigurationsdatei "/etc/dhcp/dhcpd.conf" folgendes hinzu:

```
# Format definition of DHCP CAPWAP option for Wireless LAN Controller
option wifi-controller code 138 = array of ip-address;
# IP address range for Slave APs/WTPs<
subnet 10.10.0.0 netmask 255.255.255.0 {
range 10.10.10.10 10.10.10.100;
option domain-name-servers mydnsserver.mydomain.tld;
option routers 10.10.10.1;
option broadcast-address 10.10.10.255;
default-lease-time 600;
max-lease-time 7200;
# IP address of Wireless LAN Controller
option wifi-controller 10.10.10.5;
}
```

Dabei sind vor allem die beiden Zeilen, die mit **option wifi-controller** beginnen, entscheidend. 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 Slave-APs melden, nachdem sie alle benötigten Daten (eigene IP-Adresse, IP-Adresse des WLAN-Controllers, …) 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, können Sie den DHCP-Server mit dem Kommando `/etc/init.d/dhcp-server restart` neu starten.

1.6.5 Betrieb der APs mit statischen IP-Adressen

Wie in *DHCP-Server* 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. Ab Release 7.10.1 finden Sie im Menü **Systemverwaltung** -> **Globale Einstellungen** -> **System** auf den APs das dazu benötigte Feld **Manuelle IP-Adresse des WLAN-Controllers**.

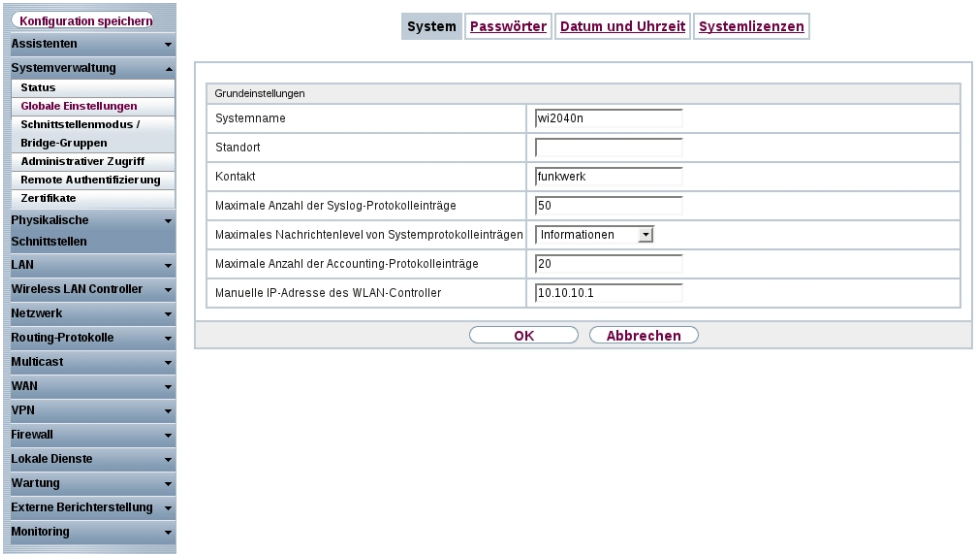


Abb. 12: **Systemverwaltung** -> **Globale Einstellungen** -> **System**

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* ausgewählt wird.