Benutzerhandbuch Workshops (Auszug)

WLAN-Workshops

Copyright© Version 01/2020 bintec elmeg GmbH

Rechtlicher Hinweis

Gewährleistung

Änderungen in dieser Veröffentlichung sind vorbehalten.

bintec elmeg GmbH gibt keinerlei Gewährleistung auf die in dieser Bedienungsanleitung enthaltenen Informationen.bintec elmeg GmbH übernimmt keine Haftung für mittelbare, unmittelbare, Neben-, Folge- oder andere Schäden, die mit der Auslieferung, Bereitstellung oder Benutzung dieser Bedienungsanleitung im Zusammenhang stehen.

Copyright © bintec elmeg GmbH

Alle Rechte an den hier beinhalteten Daten - insbesondere Vervielfältigung und Weitergabe - sind bintec elmeg GmbH vorbehalten.

Inhaltsverzeichnis

Kapitel 1 WLAN - VLAN mit Multi-SSID-WLAN

1.1 Einleitung

Im Folgenden wird die Konfiguration eines Virtual LAN (VLAN) beschrieben. Sie verbinden Ihre WLAN-Clients mittels eines **W2003ac** drahtlos mit dem Firmennetz. **W2003ac** dient als Access Point für die Drahtlosnetzwerke `Management`, `Development` und `Public`. Die Ethernet-Schnittstelle, an die Ihr kabelgebundenes LAN angeschlossen ist, wird im Bridge-Modus betrieben und ist mittels eines VLAN-fähigen Switches an das kabelgebundene Netz angeschlossen. Das Netzwerk ist virtuell in die VLANs `Management`, `Development` und `Public` segmentiert.

Zur Konfiguration wird das **GUI** (Graphical User Interface) verwendet.

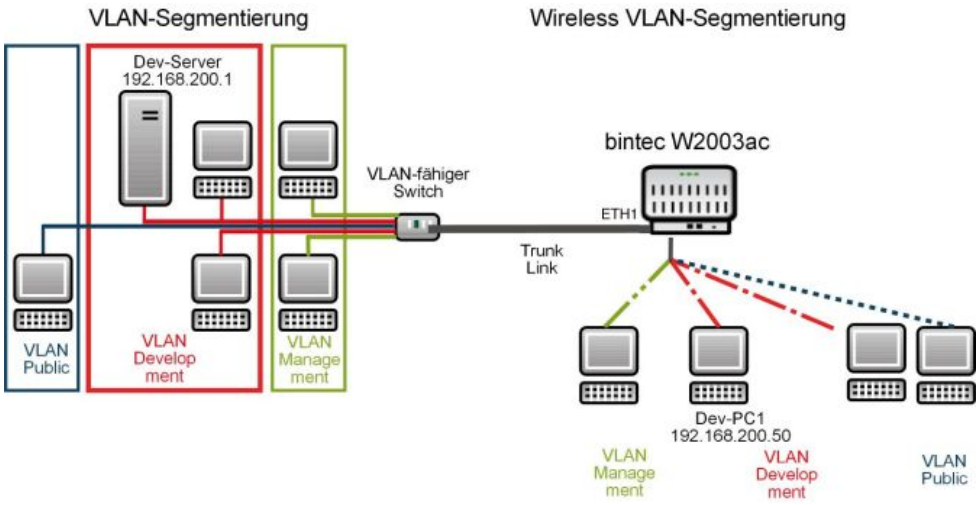


Abb. 1: VLAN-Segmentierung

Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Ein Bootimage der Version 10.1.9 oder höher.
- Ein VLAN-fähiger Switch.

1.2 Konfiguration

1.2.1 Konfiguration der Drahtlosnetzwerke

Damit sich die Clients über Ihren Access Point mit dem Netzwerk verbinden können, müssen Sie auf dem Access Point Drahtlosnetzwerke einrichten.

Gehen Sie zur Erstellung von Drahtlosnetzwerken vor wie folgt:

(1) Gehen Sie zu **Wireless LAN** -> **WLAN**-> **Einstellungen Funkmodul**.

Konfigurieren Sie das Funkmodul, indem Sie den Tabelleneintrag bearbeiten. Klicken Sie dazu bei dem vorhandenen Eintrag auf das -Symbol.

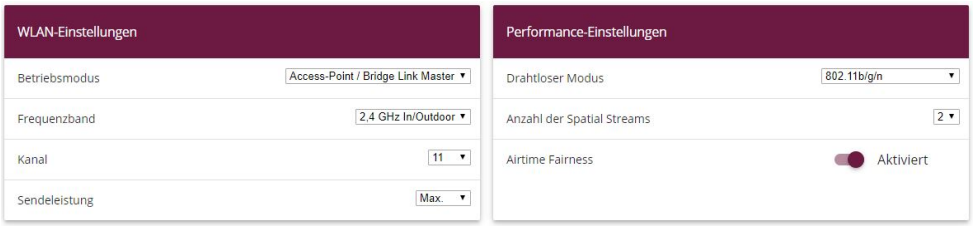


Abb. 2: **Wireless LAN** -> **WLAN** -> **Einstellungen Funkmodul** ->

Gehen Sie folgendermaßen vor:

(1) Den **Betriebsmodus** stellen Sie auf *`Access-Point / Bridge Link Master`*.

(2) Den **Kanal** setzen Sie auf z. B. *`11`*.

(3) Bestätigen Sie mit **OK**.

Legen Sie anschließend die Drahtlosnetzwerk-Einträge an.

(1) Gehen Sie zu **Wireless LAN** -> **WLAN** -> **Drahtlosnetzwerke (VSS)**->.

Konfigurieren Sie die WLAN-Verbindung, indem Sie den Standardeintrag bearbeiten.

Abb. 3: **Wireless LAN** -> **WLAN** -> **Drahtlosnetzwerke (VSS)** ->

Gehen Sie folgendermaßen vor:

(1) Unter **Netzwerkname (SSID)** tragen Sie z. B. `Management` ein.

(2) Bei **Netzwerkname (SSID)** bleibt die Option **Sichtbar** aktiviert.

(3) Den **Sicherheitsmodus** stellen Sie auf `WPA-PSK`.

(4) Im **Preshared Key** geben Sie z. B. `Schluessel-Admin` ein.

(5) Bestätigen Sie mit **OK**.

Hinweis

Um die Sicherheit zu erhöhen, sollten Sie im Schlüssel Sonderzeichen, Zahlen sowie Groß- und Kleinbuchstaben verwenden.

Danach müssen Sie noch das gerade eben konfigurierte Drahtlosnetzwerk aktivieren. Das geschieht in der Übersicht in **Wireless LAN** -> **WLAN**-> **Drahtlosnetzwerke (VSS)**.

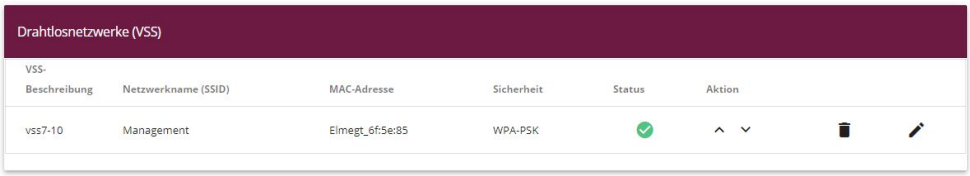


Abb. 4: **Wireless LAN** -> **WLAN**-> **Drahtlosnetzwerke (VSS)**

Gehen Sie zur Aktivierung vor wie folgt:

(1) Klicken Sie bei dem bisher einzigen Listeneintrag unter **Aktion** auf das ^ -Symbol. Beachten Sie die **Status**-Spalte. Hier müsste nach kurzer Zeit das ✓ -Symbol angezeigt werden.

Konfigurieren Sie entsprechend neue Einträge für die Drahtlosnetzwerke `Development` und `Public`.

Hinweis

Achten Sie darauf, dass Sie den verschiedenen Drahtlosnetzwerken verschiedene **Preshared Keys** zuweisen.

Konfigurieren Sie anschließend den Wireless-Adapter der Clients in Ihrem Netzwerk für das entsprechende Drahtlosnetzwerk.

1.2.2 Konfiguration der VLANs

Das VLAN *Management* ist standardmäßig auf Ihrem Gerät vorkonfiguriert. Erstellen Sie nun die VLANs *Development* und *Public*.

Gehen Sie in folgendes Menü, um ein VLAN zu erstellen:

(1) Gehen Sie zu **LAN** -> **VLAN** -> **VLANs** -> **Neu**.

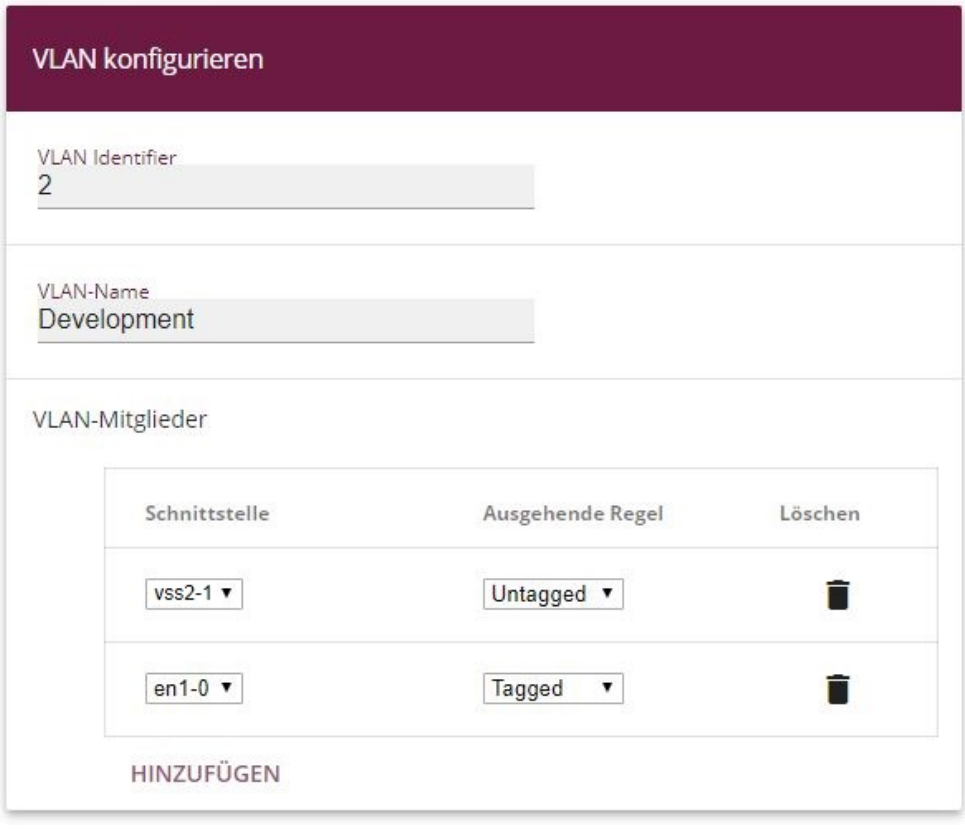


Abb. 5: **LAN** -> **VLAN** -> **VLANs** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Unter **VLAN Identifier** geben Sie einen Wert zwischen 1 und 4094 ein, hier z. B. *2*.

(2) Bei **VLAN-Name** geben Sie z. B. *Development* ein.

(3) Klicken Sie bei **VLAN-Mitglieder** auf **Hinzufügen** und wählen Sie die entsprechende WLAN-Schnittstelle aus, z. B. *vss2-1*. Wählen Sie dafür außerdem unter **Ausgehende Regel** *Untagged* aus.

(4) Klicken Sie bei **VLAN-Mitglieder** ein weiteres Mal auf **Hinzufügen** und wählen Sie die LAN-Schnittstelle aus, z. B. *en1-0*. Wählen Sie dafür außerdem unter **Ausgehende Regel** *Tagged* aus.

(5) Klicken Sie auf **OK**.

Gehen Sie analog für die Erstellung des VLANs *Public* vor.

(1) Unter **VLAN Identifier** geben Sie einen Wert zwischen 1 und 4094 ein, hier z. B. *3*.

(2) Bei **VLAN-Name** geben Sie z. B. *Public* ein.

(3) Klicken Sie bei **VLAN-Mitglieder** auf **Hinzufügen** und wählen Sie die entsprechende WLAN-Schnittstelle aus, z. B. *vss2-2*. Wählen Sie außerdem unter **Ausgehende Regel** *Untagged* aus.

(4) Klicken Sie bei **VLAN-Mitglieder** ein weiteres Mal auf **Hinzufügen** und wählen Sie die LAN-Schnittstelle aus, z. B. *en1-0*. Wählen Sie dafür außerdem unter **Ausgehende Regel** *Tagged* aus.

(5) Klicken Sie auf **OK**.

1.2.3 Regeln für den Empfang an den Ports festlegen

Im Menü **Portkonfiguration** legen Sie Regeln für den Empfang von Frames an den Ports des VLANs fest.

Um den Port VLAN Identifier (PVID) festzulegen, gehen Sie in folgendes Menü:

(1) Gehen Sie zu **LAN** -> **VLAN** -> **Portkonfiguration**.

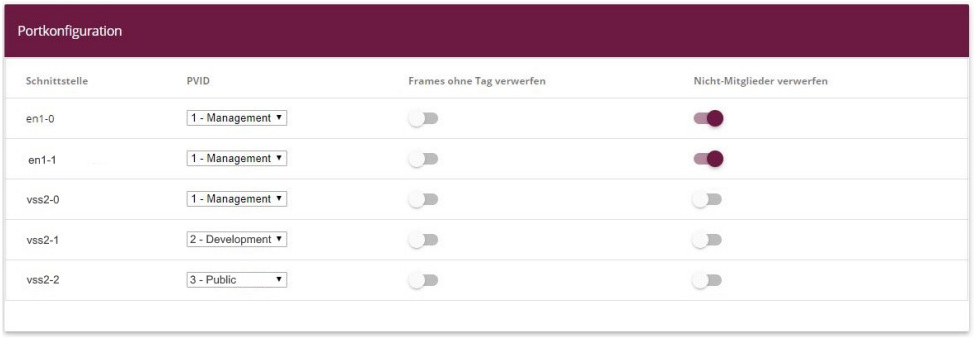


Abb. 6: **LAN** -> **VLAN** -> **Portkonfiguration**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie neben der **Schnittstelle** *vss2-1* den **Port VLAN Identifier (PVID)** aus, hier z. B. *Development*.

(2) Wählen Sie neben der **Schnittstelle** *vss2-2* den **Port VLAN Identifier (PVID)** aus, hier z. B. *Public*.

(3) Lassen Sie bei den Schnittstellen *en1-0* und *en1-1* unter **Frames ohne Tag verwerfen** die Option deaktiviert. Aktivieren Sie bei den Schnittstellen *en1-0* und *en1-1* die Option **Nicht-Mitglieder verwerfen**.

(4) Klicken Sie auf **OK**.

1.2.4 Ports aus VLAN Management entfernen

Die Ports, die Sie den VLANs *Development* und *Public* zugewiesen haben, werden aus dem VLAN *Management* entfernt.

Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **LAN** -> **VLAN** -> **VLANs** -> **<Management>** -> ✎ .

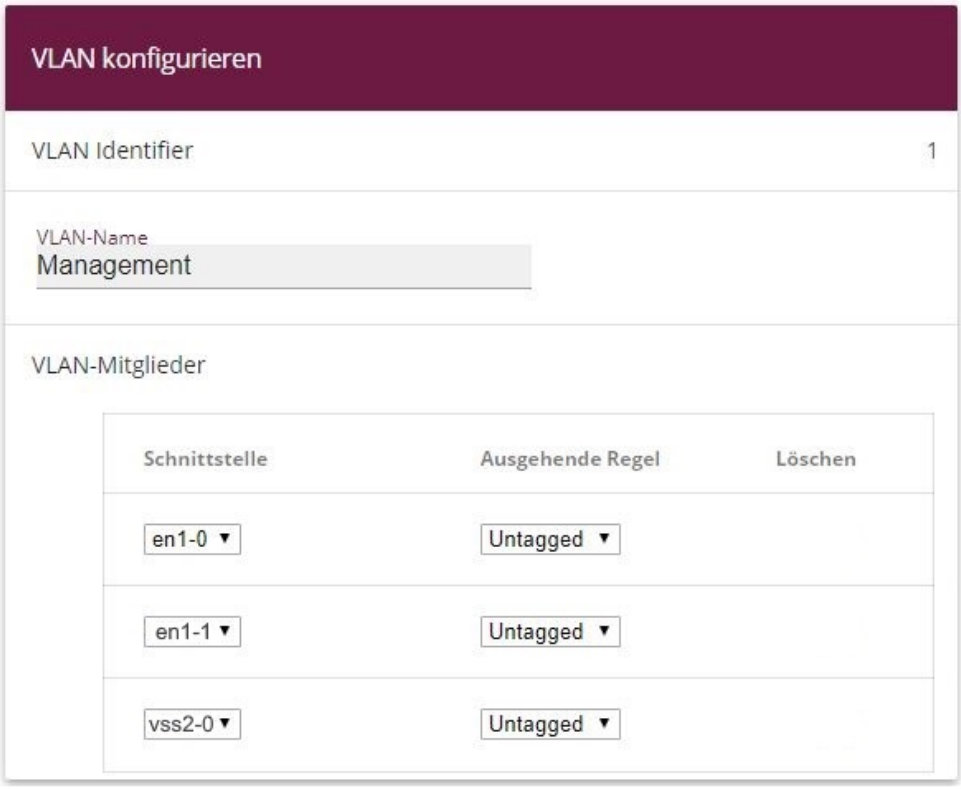


Abb. 7: **LAN** -> **VLAN** -> **VLANs** -> **<Management>** ->

Gehen Sie folgendermaßen vor:

(1) Klicken Sie bei **Schnittstelle** *vss2-1* auf das -Symbol.

(2) Klicken Sie bei **Schnittstelle** *vss2-2* auf das -Symbol.

(3) Belassen Sie bei **Schnittstelle** *en1-0*, *en1-1*, und *vss2-0* unter **Ausgehende Regel** jeweils den Wert *Untagged* .

(4) Klicken Sie auf **OK**.

Sie haben nun alle erforderlichen VLANs eingerichtet. Dieses können Sie in der Liste im Menü **LAN** -> **VLAN** -> **VLANs** überprüfen.

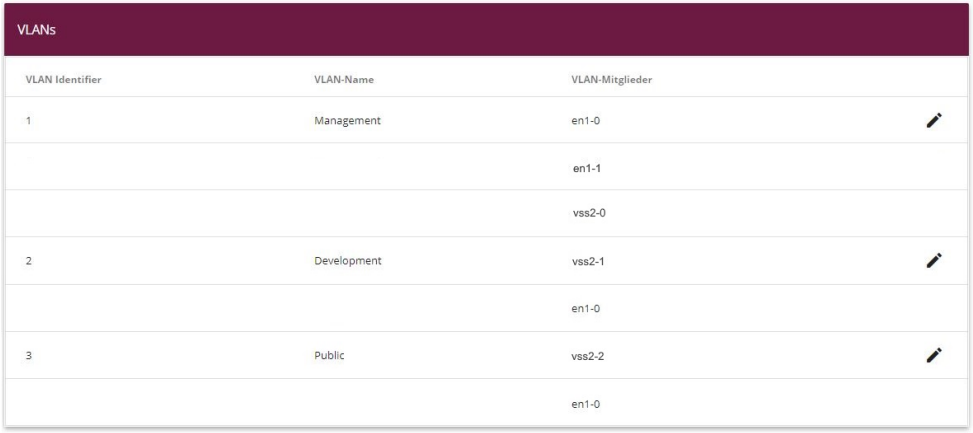


Abb. 8: VLAN Übersicht

1.2.5 VLAN aktivieren

Zum Schluss aktivieren Sie die VLAN-Funktion für die Bridge-Gruppe `br0`.

Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **LAN** -> **VLAN** -> **Verwaltung**.

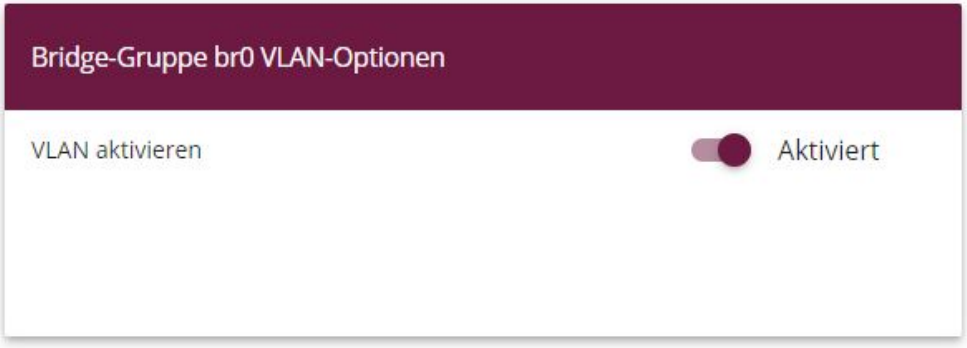


Abb. 9: **LAN** -> **VLAN** -> **Verwaltung**

Gehen Sie folgendermaßen vor:

(1) Aktivieren Sie **VLAN aktivieren**.

(2) Klicken Sie auf **OK**.

1.2.6 Konfiguration am bintec S128p

Der Switch muss analog zum Access Point konfiguriert sein. In Richtung Access Point dürfen nur getaggte (VLAN) Packete verarbeitet werden. In Richtung Server soll das Tagging entfernt werden, da die Server die Packete sonst nicht verarbeiten können.

(1) Starten Sie den Browser und Loggen Sie sich auf dem Switch ein.

(2) Gehen Sie zu **Protocol** -> **VLAN**.

(3) Wählen Sie bei **VLAN Operation Mode** *802.1Q* aus.

(4) Klicken Sie auf **Apply**.

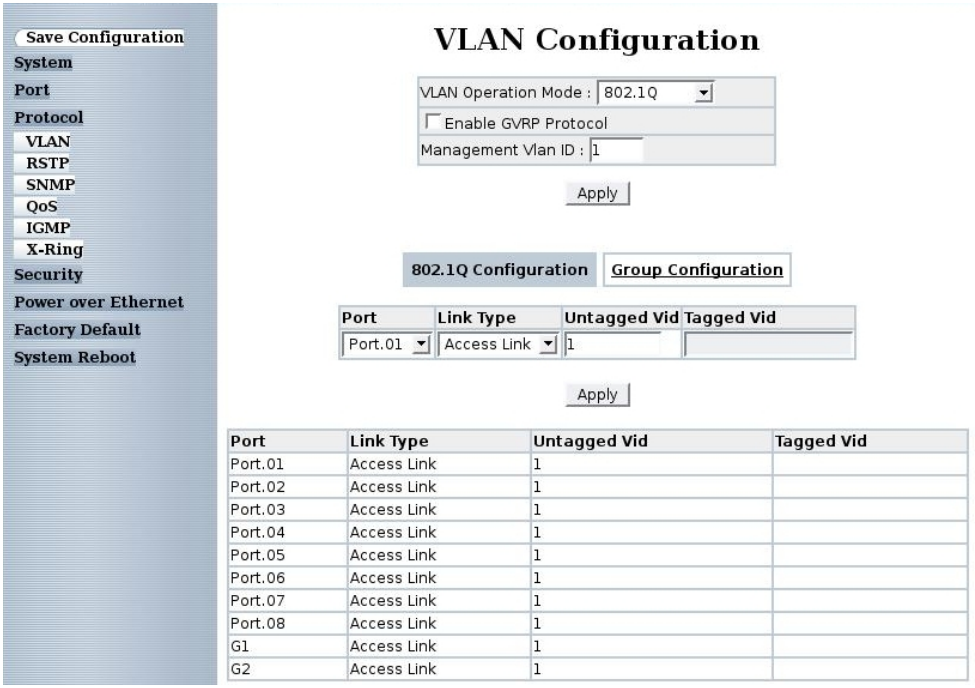


Abb. 10: **Protocol** -> **VLAN** -> **VLAN Configuration**

Es sind insgesamt 3 VLANs erforderlich, wobei jeweils der **Port** (Port.01, Port.02, Port.03) und **Untagged Vid** (1, 102, 103) passend zu setzen sind.

Gehen Sie folgendermaßen vor, um die Ports zu konfigurieren:

(1) Wählen Sie bei **Port** *Port.01* aus.

(2) Wählen Sie bei **Link Type** *Access Link* aus.

(3) Geben Sie bei **Untagged Vid** *1* ein.

(4) Bestätigen Sie Ihre Eingaben mit **Apply**.

(5) Verfahren Sie analog für die Konfiguration von *Port.02* (**Untagged Vid** *102*) und *Port.03* (**Untagged Vid** *103*)

(6) Bestätigen Sie Ihre Eingaben mit **Apply**.

(7) Wählen Sie bei **Port** *Port.08* aus.

(8) Wählen Sie bei **Link Type** *Trunk Link* aus.

(9) Geben Sie bei **Tagged Vid** *1,102,103* ein.

(10) Bestätigen Sie Ihre Eingaben mit **Apply**.

Die fertige Konfiguration sieht nun wie folgt aus:

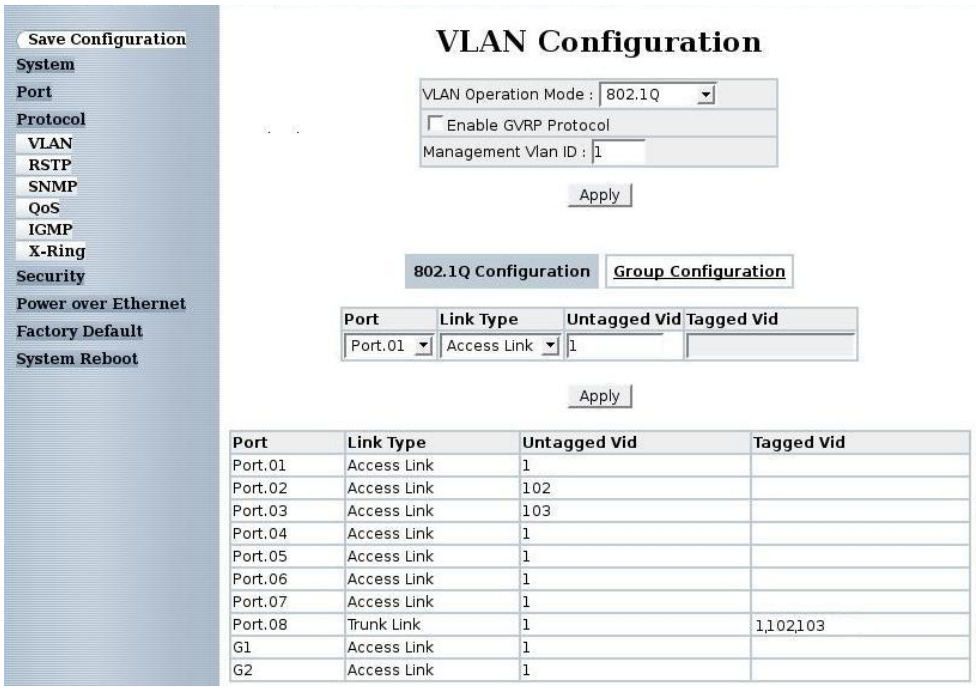


Abb. 11: **Protocol** -> **VLAN** -> **VLAN Configuration**

Kontrolle

Um die Konfiguration zu überprüfen, rufen Sie die Eingabeaufforderung auf einem Rechner auf und geben Sie einen Ping auf das zentrale Netz ab:

z. B. `ping 192.168.100.30`

Sie müssen dann folgende Meldung erhalten:

```
<?xml version='1.0' encoding='UTF-16'?>
C:\>ping 192.168.100.30

Ping wird ausgeführt für 192.168.100.30 mit 32 Bytes Daten:

Antwort von 192.168.100.30: Bytes=32 Zeit&lt;1ms TTL=30
Antwort von 192.168.100.30: Bytes=32 Zeit&lt;1ms TTL=30
Antwort von 192.168.100.30: Bytes=32 Zeit&lt;1ms TTL=30
Antwort von 192.168.100.30: Bytes=32 Zeit&lt;1ms TTL=30

Ping-Statistik für 192.168.100.30:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
C:\>
```

1.3 Ergebnis

Sie haben für die WLAN-Clients in Ihrem Netzwerk verschiedene Drahtlosnetzwerke eingerichtet. Das gesamte Netzwerk wurde in verschiedene VLANs segmentiert.

1.4 Kontrolle

Um die Konfiguration zu überprüfen, rufen Sie die Eingabeaufforderung z. B. auf dem Rechner Dev-PC1 (192.168.200.50) auf und geben Sie einen Ping auf den Dev-Server (192.168.200.1) ab:

z. B. `ping 192.168.200.1`

Sie müssten dann folgende Meldungen erhalten:

```
Ping wird ausgeführt für 192.168.200.1 mit 32 Bytes Daten:

Antwort von 192.168.200.1: Bytes=32 Zeit&lt;1ms TTL=63
Antwort von 192.168.200.1: Bytes=32 Zeit&lt;1ms TTL=63
Antwort von 192.168.200.1: Bytes=32 Zeit&lt;1ms TTL=63
Antwort von 192.168.200.1: Bytes=32 Zeit&lt;1ms TTL=63

Ping-Statistik für 192.168.200.1:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms
```

1.5 Konfigurationsschritte im Überblick

Access Point aktivieren

Feld	Menü	Wert
Betriebsmodus	**Wireless LAN** -> **WLAN** -> **Einstellungen Funkmodul** ->	*Access-Point / Bridge Link Master*
Kanal	**Wireless LAN** -> **WLAN** -> **Einstellungen Funkmodul** ->	z. B. *11*

Drahtlosnetzwerke einrichten

Feld	Menü	Wert
Netzwerkname (SSID)	**Wireless LAN** -> **WLAN** -> **Drahtlosnetzwerke (VSS)** -> **Neu**	*Management*; **Sichtbar** bleibt aktiviert
Sicherheitsmodus	**Wireless LAN** -> **WLAN** -> **Drahtlosnetzwerke (VSS)** -> **Neu**	*WPA-PSK*
Preshared Key	**Wireless LAN** -> **WLAN** -> **Drahtlosnetzwerke (VSS)** -> **Neu**	z. B. *Schluessel-Admin*
Aktion	**Wireless LAN** -> **WLAN** -> **Drahtlosnetzwerke (VSS)** -><**Management**>	
Netzwerkname (SSID)	**Wireless LAN** -> **WLAN** -> **Drahtlosnetzwerke (VSS)** -> **Neu**	*Development*; **Sichtbar** bleibt aktiviert
Sicherheitsmodus	**Wireless LAN** -> **WLAN** -> **Drahtlosnetzwerke (VSS)** -> **Neu**	*WPA-PSK*
Preshared Key	**Wireless LAN** -> **WLAN** -> **Drahtlosnetzwerke (VSS)** -> **Neu**	z. B. *Schluessel-Devs*
Aktion	**Wireless LAN** -> **WLAN** -> **Drahtlosnetzwerke (VSS)** -><**Development**>	
Netzwerkname (SSID)	**Wireless LAN** -> **WLAN** ->	*Public*;

Feld	Menü	Wert
	Drahtlosnetzwerke (VSS) -> Neu	**Sichtbar** bleibt aktiviert
Sicherheitsmodus	**Wireless LAN -> WLAN -> Drahtlosnetzwerke (VSS) -> Neu**	*WPA-PSK*
Preshared Key	**Wireless LAN -> WLAN -> Drahtlosnetzwerke (VSS) -> Neu**	z. B. *Schluessel-Alle*
Aktion	**Wireless LAN -> WLAN -> Drahtlosnetzwerke (VSS) -> <Public>**	^

VLANs konfigurieren

Feld	Menü	Wert
VLAN Identifier	**LAN -> VLAN -> VLANs -> Neu**	z. B. *2*
VLAN-Name	**LAN -> VLAN -> VLANs -> Neu**	z. B. *Development*
VLAN-Mitglieder	**LAN -> VLAN -> VLANs -> Neu**	mit **Hinzufügen** z. B. *vss2-1*
Ausgehende Regel	**LAN -> VLAN -> VLANs -> Neu**	*Untagged* für *vss2-1*
VLAN-Mitglieder	**LAN -> VLAN -> VLANs -> Neu**	mit **Hinzufügen** z. B. *en1-0*
Ausgehende Regel	**LAN -> VLAN -> VLANs -> Neu**	*Tagged* für *en1-0*
VLAN Identifier	**LAN -> VLAN -> VLANs -> Neu**	z. B. *3*
VLAN-Name	**LAN -> VLAN -> VLANs -> Neu**	z. B. *Public*
VLAN-Mitglieder	**LAN -> VLAN -> VLANs -> Neu**	mit **Hinzufügen** z. B. *vss2-2*
Ausgehende Regel	**LAN -> VLAN -> VLANs -> Neu**	*Untagged* für *vss2-2*
VLAN-Mitglieder	**LAN -> VLAN -> VLANs -> Neu**	mit **Hinzufügen** z. B. *en1-0*
Ausgehende Regel	**LAN -> VLAN -> VLANs -> Neu**	*Tagged* für *en1-0*

Port VLAN Identifier (PVID) festlegen

Feld	Menü	Wert
Port VLAN Identifier (PVID)	**LAN** -> **VLAN** -> **Portkonfiguration**	bei **Schnittstelle** *vss2-1* z. B. *Development* ; bei **Schnittstelle** *vss2-2* z. B. *Public*
Nicht-Mitglieder verwerfen	**LAN** -> **VLAN** -> **Portkonfiguration**	Haken setzen bei Schnittstelle *en1-0* und *en1-1*

Ports aus VLAN Management entfernen

Feld	Menü	Wert
VLAN-Mitglieder	**LAN** -> **VLAN** -> **VLANs** -> **<Management>**->	bei **Schnittstelle** *vss2-1* und *vss2-2*

VLANs aktivieren

Feld	Menü	Wert
VLAN aktiveren	**LAN** -> **VLAN** -> **Verwaltung**	*Aktiviert*

Kapitel 2 WLAN - bintec Hotspot Solution

2.1 Einleitung

Die **bintec Hotspot Solution** ermöglicht die Bereitstellung von öffentlichen Internetzugängen. Die Lösung ist geeignet zum Aufbau kleinerer und größerer Hotspot-Lösungen für Cafes, Hotels, Unternehmen, Wohnheime, Campingplätze usw.

Die **bintec Hotspot Solution** besteht aus einem vor Ort installierten Gerät **bintec RS353xx**, **bintec RXL12x00** oder **be.IP**, das als Gateway dient, und aus dem Hotspot-Server, der zentral in einem Rechenzentrum steht. Über einen PC mit Internetzugang (z. B. dem Rezeptions-PC im Hotel) wird das Betreiber-Konto auf dem Server verwaltet, wie z. B. Erfassung von Registrierungen, Erzeugung von Tickets, statistische Auswertung usw.

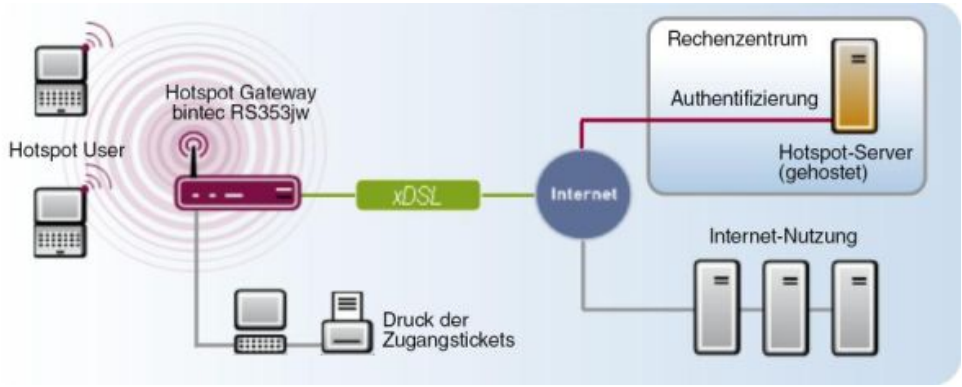


Abb. 12: Funktionsweise

Ablauf der Anmeldeprozedur am Hotspot-Server

- Wenn sich ein neuer Benutzer mit dem Hotspot verbindet, bekommt er über DHCP automatisch eine IP-Adresse zugewiesen.
- Sobald er versucht, eine beliebige Internetseite mit seinem Browser zu öffnen, wird der Benutzer auf die Start/Login-Seite umgeleitet.
- Nachdem der Benutzer die Anmeldedaten (Benutzer/Passwort) eingegeben hat, werden diese als RADIUS-Anmeldung an den zentralen RADIUS-Server (Hotspot-Server) gesendet.
- Nach erfolgreicher Anmeldung gibt das Gateway den Internetzugang frei.
- Das Gateway sendet für jeden Benutzer regelmäßig Zusatzinformationen an den RADI-

US-Server, um das Accounting zu realisieren.

- Nach Ablauf des Tickets wird der Benutzer automatisch abgemeldet und wieder auf die Start/Login-Seite umgeleitet.

Voraussetzungen

Um einen Hotspot betreiben zu können, benötigt der Kunde:

- einen Router der be.IP-, RS-Serie (z. B. **bintec RS353xx**) oder der RXL-Serie (z. B. **bintec RXL12100**)
- **bintec Hotspot Hosting** (Artikelnummer 5510000198 oder 5510000197)
- Zugangsdaten
- Dokumentation
- Software-Lizenzierung

  Beachten Sie bitte, dass Sie die Lizenz zuerst freischalten müssen.

  - Gehen Sie auf *www.bintec-elmeg.com* zu **Service & Support**->**Produkt Lizenzierung**-> **HotSpot Lizenzierung** .

  - Tragen Sie die erforderlichen Daten ein (beachten Sie dazu die Erläuterung auf dem Lizenzblatt) und folgen Sie den Anweisungen der Online-Lizenzierung.

  - Sie erhalten daraufhin die Login-Daten des Hotspot-Servers.

Hinweis

Die Freischaltung kann etwa 2 - 3 Werktage in Anspruch nehmen.

Zugangsdaten zur Konfiguration des Gateways

RADIUS-Server IP	62.245.165.180
RADIUS-Server Password	funkwerk-ec
Domain	Wird kundenindividuell vom Kunden / Fachhändler festgelegt
Walled Network	Wird kundenindividuell vom Kunden / Fachhändler festgelegt
Walled Server URL	Die vom Hotspot-Server festgelegte URL muss hier eingetragen werden.
Terms & Condition URL	Wenn die AGB auf den Hotspot-Server geladen

	werden, legt dieser eine URL für sie fest. Diese muss hier eingetragen werden.

Zugangsdaten zur Konfiguration des Hotspot Servers

Admin URL	https://hotspot.bintec-elmeg.com/
Username	Wird von der bintec elmeg GmbH individuell festgelegt
Password	Wird von der bintec elmeg GmbH individuell festgelegt

2.2 Leistungsmerkmale

2.2.1 Merkmale der Hotspot Solution

- Alternativ als Free-Service oder mit einem zeit- oder volumenbasierten Ticketsystem
- Freie Werbe-Webseiten, die ohne Registrierung erreichbar sind (Walled Garden Pages)
- Sowohl für WLAN als auch für drahtgebundene LAN-Benutzer einsetzbar
- Das System ist filialfähig, das bedeutet, dass z. B. eine Cafe- oder Restaurantkette das System an verschiedenen Standorten anbieten und dabei zentral verwalten kann. Dabei kann ein ausgestelltes Ticket an einem anderen Standort weiterverwendet werden.

2.2.2 Merkmale des Gateways

- Benutzer-Anmeldung einfach per Webbrowser
- Umleitung auf eine Login-Seite beim ersten Zugriff
- Anmeldung über RADIUS-Authentifizierung
- Mehrfach-Anmeldungen eines Benutzers sind konfigurierbar
- Zeitguthaben bleiben erhalten, wenn der Benutzer sich abmeldet oder die Verbindung unterbricht.
- Automatisches Ausloggen der Hotspot-Benutzer bei Inaktivtät oder wenn vergessen wird, sich abzumelden.
- Der Benutzer muss bei der Anmeldung die allgemeinen Geschäftsbedingungen (AGB) aktiv bestätigen. Muster-AGB finden Sie im Downloadbereich der **bintec Hotspot Solution** unter *www.bintec-elmeg.com* .

2.2.3 Merkmale des Hotspot-Servers

- Für jeden Kunden können mehrere Standorte eingerichtet werden (Filial-Unterstützung).
- Für jeden Kunden können mehrere Tarife eingerichtet werden (z. B. Tagesticket, Stundenticket, Volumenticket).
- Jeder Kunde hat einen eigenen Administrationsbereich zum Erstellen und Verwalten der Tickets.

2.3 Konfiguration

Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- ein Router der be.IP-, RS- (z. B. **bintec RS353xx**) oder RXL-Serie (z. B. **RXL12100**)
- Internetzugang, entweder über LAN, DSL oder andere Anbindungen
- Freigeschalteter Account auf dem zentralen **bintec Hotspot Server**

2.3.1 Konfiguration des bintec Hotspot-Gateways

Die Konfiguration Ihres Geräts wird mit dem Graphical User Interface (GUI) durchgeführt.

Aktualisierung der Software auf dem Gateway

Ihr Gerät ist mit der zum Zeitpunkt der Fertigung verfügbaren Version der Systemsoftware ausgestattet, von der es aktuell ggf. neuere Versionen gibt. Eine Aktualisierung können Sie bequem mit dem GUI im Menü **Software & Konfiguration** vornehmen.

(1) Gehen Sie zu **Wartung** -> **Software & Konfiguration** -> **Optionen**.

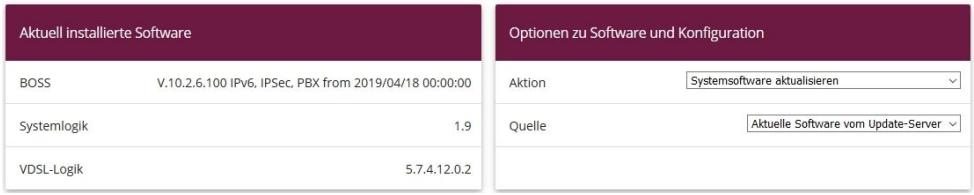


Abb. 13: **Wartung** -> **Software & Konfiguration** -> **Optionen**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie bei **Aktion** `Systemsoftware aktualisieren` aus.

(2) Wählen Sie bei **Quelle** *Aktuelle Software vom Update-Server* aus.

(3) Klicken Sie auf **Start**, um die Aktualisierung auszuführen.

Sprache konfigurieren (Reseller / Partner)

Die Sprache für die Start/Login-Seite für Reseller / Partner können Sie im Menü **Lokale Dienste** -> **Hotspot-Gateway** -> **Hotspot-Gateway** -> **Neu** auswählen.

Die Sprache kann auf der Start/Login-Seite jederzeit umgestellt werden.

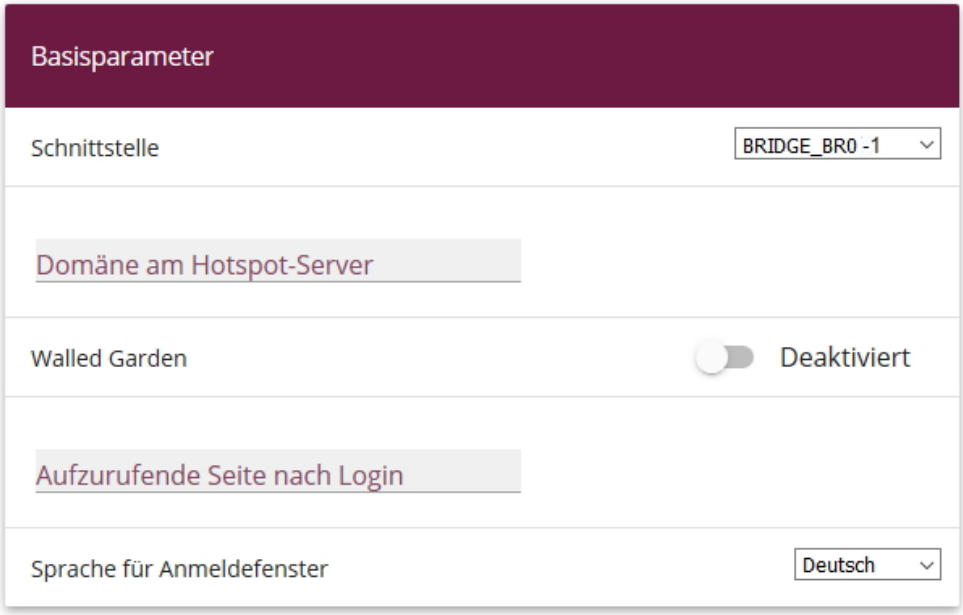


Abb. 14: **Lokale Dienste** -> **Hotspot-Gateway** -> **Hotspot-Gateway** -> **Neu**

Zeitzone einstellen

Die Systemzeit benötigen Sie u. a. für korrekte Zeitstempel bei Systemmeldungen oder Gebührenerfassung. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **Systemverwaltung** -> **Globale Einstellungen** -> **Datum und Uhrzeit**.

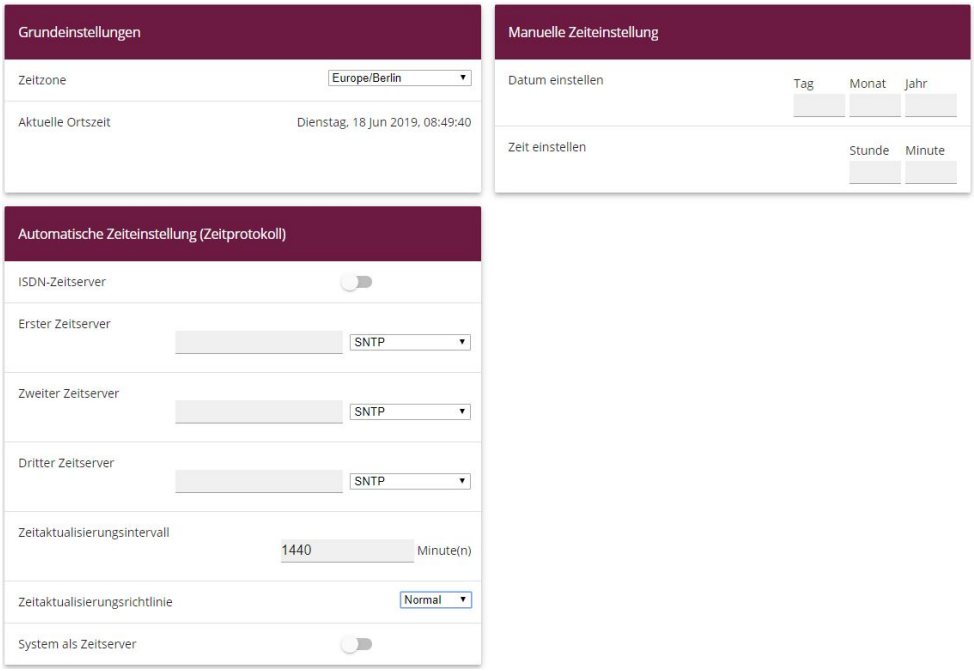


Abb. 15: **Systemverwaltung** -> **Globale Einstellungen** -> **Datum und Uhrzeit**

Hinweis

Wenn auf dem Gerät eine Methode zum automatischen Beziehen der Zeit festgelegt ist, haben die auf diese Weise erhaltenen Werte die höhere Priorität. Eine evtl. manuell eingegebene Systemzeit wird überschrieben.

Gehen Sie folgendermaßen vor, um die Zeitzone einzustellen:

(1) Wählen Sie im Feld **Zeitzone** `Europe/Berlin` aus. Um eine synchrone Systemzeit zu garantieren, ist eine aktuelle Systemzeit für den Betrieb notwendig.

(2) Deaktivieren Sie **ISDN-Zeitserver**.

(3) Deaktivieren Sie **System als Zeitserver**. Zeitanfragen eines Clients werden nicht beantwortet.

(4) Bestätigen Sie mit **OK**.

Deaktivieren der lokalen Kommunikation

Wenn ein Wireless LAN Controller mehrere Access Points verwaltet oder wenn ein Access Point stand-alone betrieben wird, können Sie die Kommunikation der Hotspot-Benutzer untereinander am selben Access Point verhindern.

Gehen Sie bei Verwendung eines Wireless LAN Controllers folgendermaßen vor:

(1) Gehen Sie zu **Wireless LAN Controller**->**Slave-AP-Konfiguration**-> **Drahtlosnetzwerke (VSS)** -> ✎

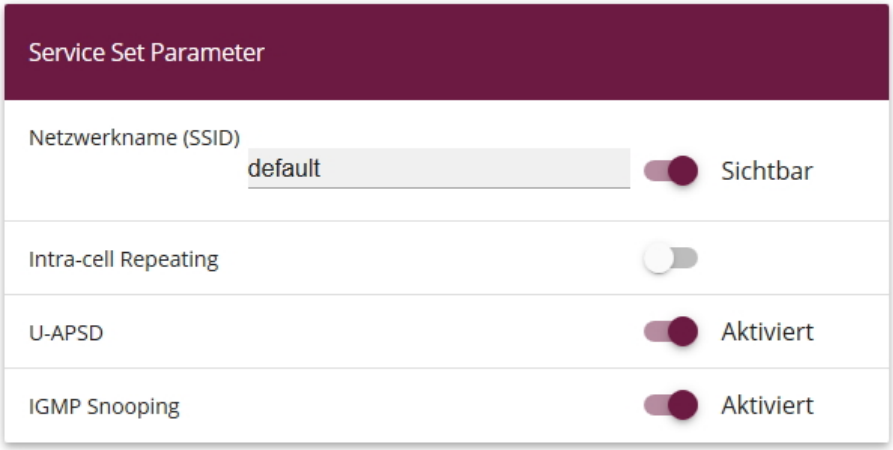


Abb. 16: **Wireless LAN Controller**->**Slave-AP-Konfiguration**-> **Drahtlosnetzwerke (VSS)** -> ✎

(2) Deaktivieren Sie **Intra-cell Repeating**.

(3) Bestätigen Sie mit **OK**.

Wenn Sie Ihren Access Point stand-alone im Access-Point-Modus betreiben (**Wireless LAN** -> **WLAN** -> **Einstellungen Funkmodul** -> ✎ mit **Betriebsmodus** = `Access-Point`), können Sie im Menü **Wireless LAN** -> **WLAN** -> **Drahtlosnetzwerke (VSS)** -> **Neu** neue Drahtlosnetzwerke einrichten.

Im Folgenden wird die Kommunikation zwischen Hotspot-Benutzern, die an einem stand-alone Access Point registriert sind, unterbunden.

Gehen Sie dazu folgendermaßen vor:

(1) Gehen Sie zu **Wireless LAN** -> **WLAN** -> **Drahtlosnetzwerke (VSS)** -> ✎

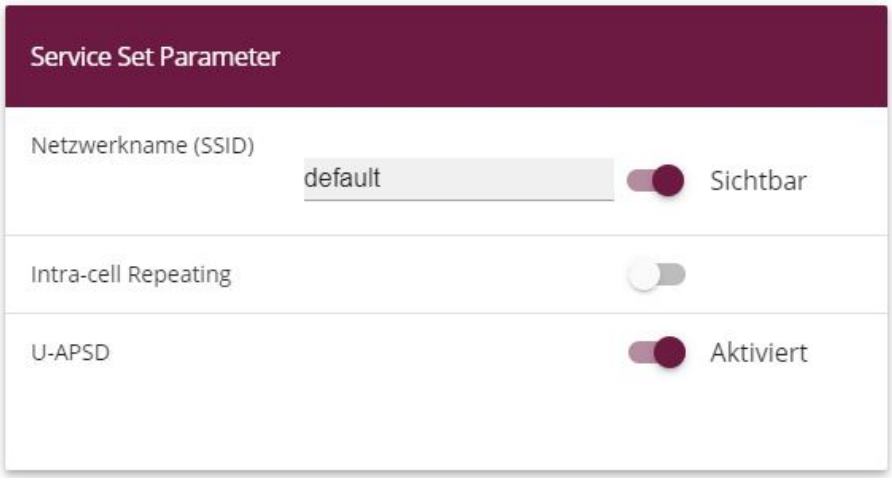


Abb. 17: **Wireless LAN** -> **WLAN** -> **Drahtlosnetzwerke (VSS)** ->

(2) Deaktivieren Sie **Intra-cell Repeating**.

(3) Bestätigen Sie mit **OK**.

RADIUS-Server-Zugriff konfigurieren

Für den Zugang zum RADIUS-Server müssen zwei Einträge erzeugt werden. Der RADUIS-Server ist Bestandteil des zentralen **bintec** Hotspot Servers. Verwenden Sie für die RADIUS-Server-Anmeldung die IP-Adresse `62.245.165.180` und das Passwort `funkwerk-ec`.

Im Menü **Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** wird eine Liste aller eingetragenen RADIUS-Server angezeigt.

Um den ersten Eintrag zu konfigurieren, gehen Sie in folgendes Menü:

(1) Gehen Sie zu **Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**.

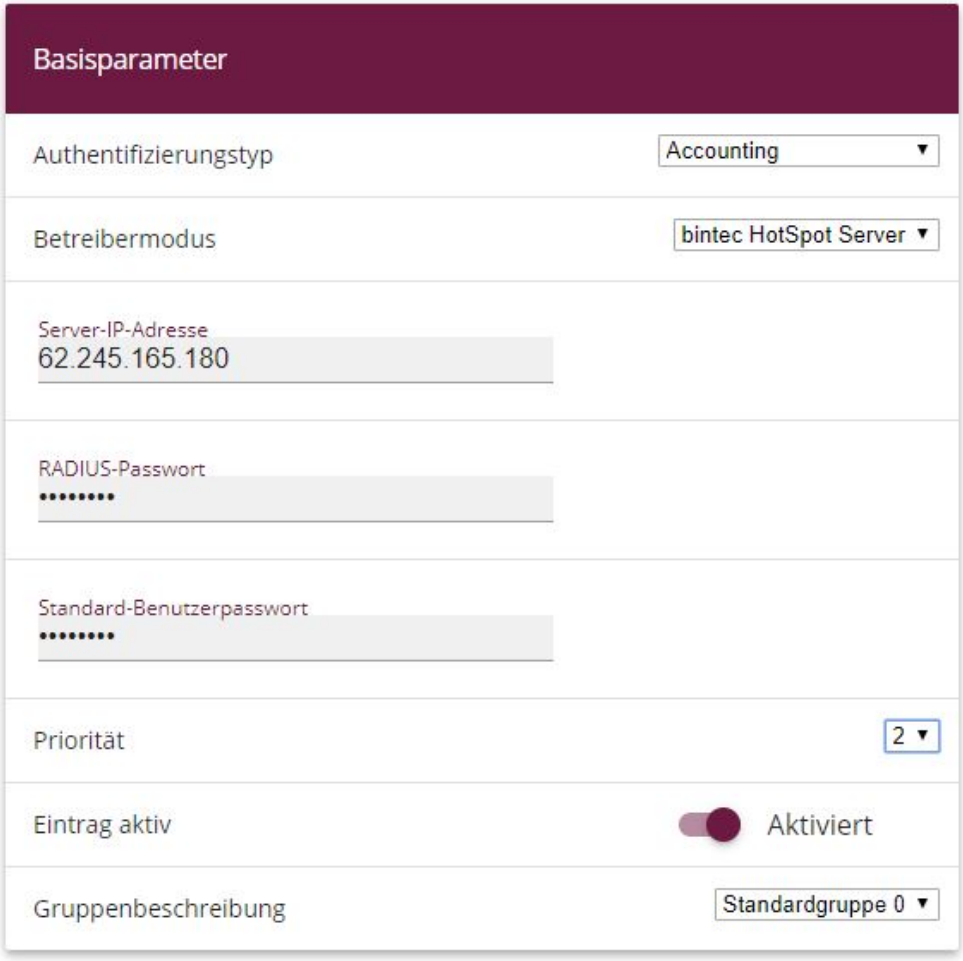


Abb. 18: **Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**

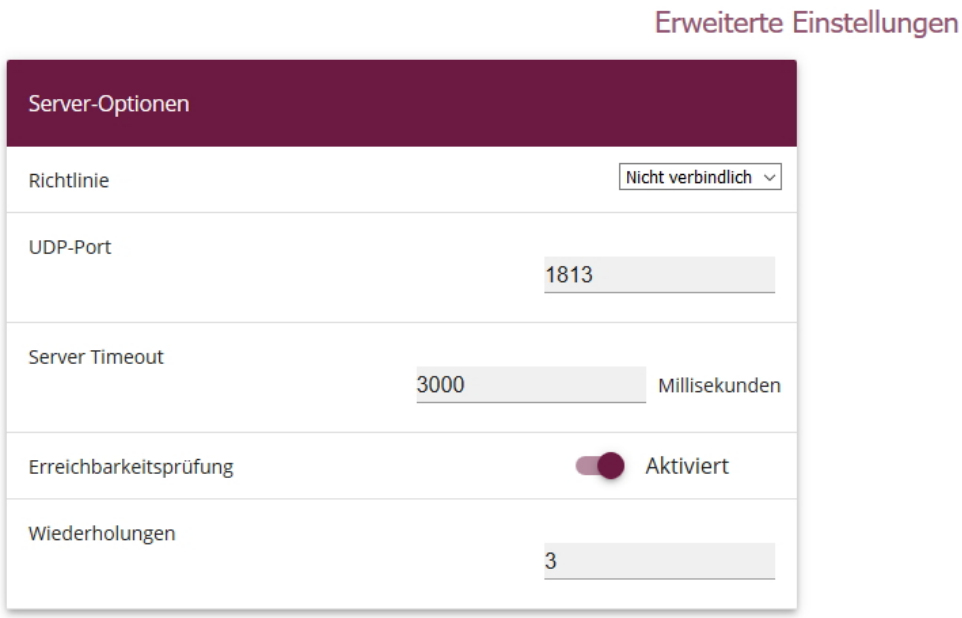


Abb. 19: **Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**->**Erweiterte Einstellungen**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie bei **Authentifizierungstyp** *Accounting* aus.

(2) Wählen Sie bei **Betreibermodus** den Anbieter *bintec HotSpot Server* aus.

(3) Tragen Sie die **Server-IP-Adresse** *62.245.165.180* des RADIUS-Servers ein.

(4) Tragen Sie das **RADIUS-Passwort** *funkwerk-ec* ein.

(5) Setzen Sie die **Priorität** auf *2*. Der Server mit der obersten Priorität wird als erstes verwendet.

(6) Klicken Sie auf **Erweiterte Einstellungen**.

(7) Wählen Sie bei **Richtlinie** *Nicht verbindlich* aus.

(8) Setzen Sie **Server Timeout** auf *3000*.

(9) Setzen Sie die **Wiederholungen** auf *3*.

(10) Bestätigen Sie mit **OK**.

Um den zweiten Eintrag zu konfigurieren, gehen Sie erneut in das Menü:

(1) Gehen Sie zu **Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**.

Gehen Sie folgendermaßen vor:

(1) Wählen Sie bei **Authentifizierungstyp** *Login-Authentifizierung* aus.

(2) Tragen Sie die **Server-IP-Adresse** *62.245.165.180* ein.

(3) Tragen Sie das **RADIUS-Passwort** *funkwerk-ec* ein.

(4) Setzen Sie die **Priorität** auf *1*.

(5) Klicken Sie auf **Erweiterte Einstellungen**.

(6) Wählen Sie bei **Richtlinie** *Nicht verbindlich* aus.

(7) Setzen Sie **Server Timeout** auf *3000*.

(8) Setzen Sie die **Wiederholungen** auf *3*.

(9) Bestätigen Sie mit **OK**.

2.3.2 Konfiguration des bintec Hotspot-Servers durch einen Fachhändler

Ein Fachhändler / Dienstleister, der einen **bintec** Hotspot-Dienst einrichten möchte, erhält bei Bestellung die Zugangsdaten für einen Administratorzugang. Dieser Zugang ermöglicht es dem Dienstleister, alle relevanten Konfigurationen und Voreinstellungen für seine Kunden vorzunehmen.

Folgende Einstellungen und Konfigurationen müssen Sie als Fachhändler festlegen:

- Mandanten-Profil ergänzen
- Benutzer anlegen
- Die gewünschten Tarife anlegen
- Standort bearbeiten

Mandanten-Profil ergänzen

(1) Starten Sie einen Webbrowser und rufen Sie die Seite *https://hotspot.bintec-elmeg.com* auf.

(2) Geben Sie Ihren Benutzernamen in das Feld **Benutzername** des Eingabefensters ein.

(3) Geben Sie Ihr Passwort in das Feld **Passwort** des Eingabefensters ein.

(4) Klicken Sie auf die **Login**-Schaltfläche.

Abb. 20: Login

Gehen Sie folgendermaßen vor, um das Mandanten-Profil zu bearbeiten:

(1) Gehen Sie zu **Mandant**->**Übersicht**.

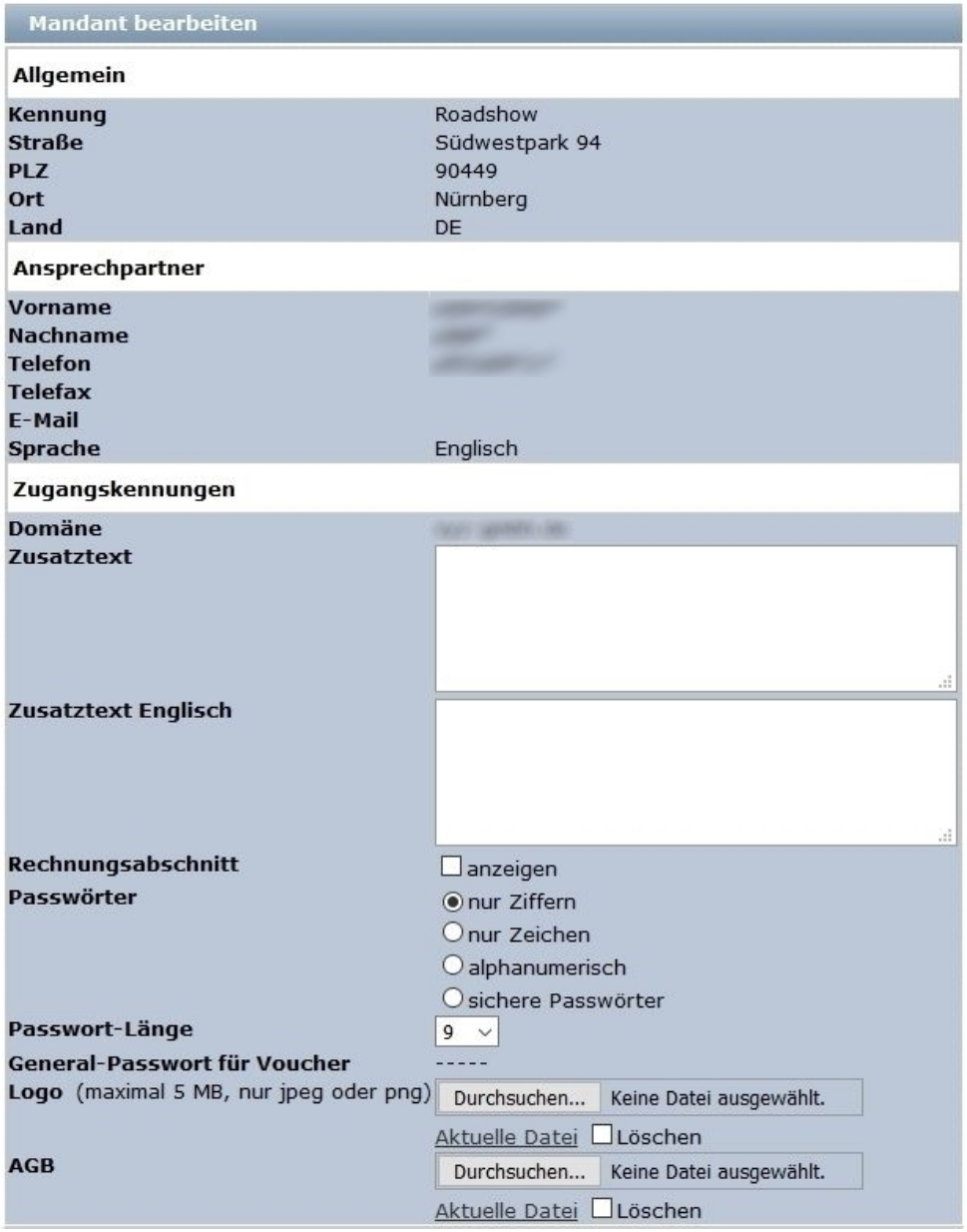


Abb. 21: **Mandant** -> **Mandant bearbeiten**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie bei **Logo** die Datei mit **Durchsuchen** über den Dateibrowser aus. Unter Logo können Sie Ihr Firmenlogo im PNG-Format hinterlegen. Dieses Logo wird auf jedem Ausdruck abgebildet. (Das Logo auf der Benutzer-Startseite kann über das Tem-

plate Bearbeitung festgelegt werden.)

(2) Unter **AGB** hinterlegen Sie Ihre firmenspezifischen, allgemeinen Geschäftsbedingungen (AGB) für den Hotspot-Dienst, falls Sie Default Free Service verwenden. Andernfalls legen Sie die allgemeinen Geschäftsbedingungen auf Ihrem eigenen Webspace ab (siehe **Standort**->**Übersicht**->**Upload Manager**).

(3) Bestätigen Sie mit **speichern**.

Hinweis

Wir empfehlen Ihnen, für **Passwörter** den Parameter *nur Ziffern* zu verwenden, um die Eingabe des Passworts auf Tablet-PCs oder mit verschiedenen Tastatur-Layouts zu erleichtern.

Benutzer anlegen

Im Menü **Benutzer** -> **Übersicht** wird eine Liste aller Benutzer angezeigt. Als Fachhändler können Sie Benutzer anlegen. Gehen Sie dazu folgendermaßen vor:

(1) Gehen Sie zu **Benutzer** -> **Neuer Benutzer**.

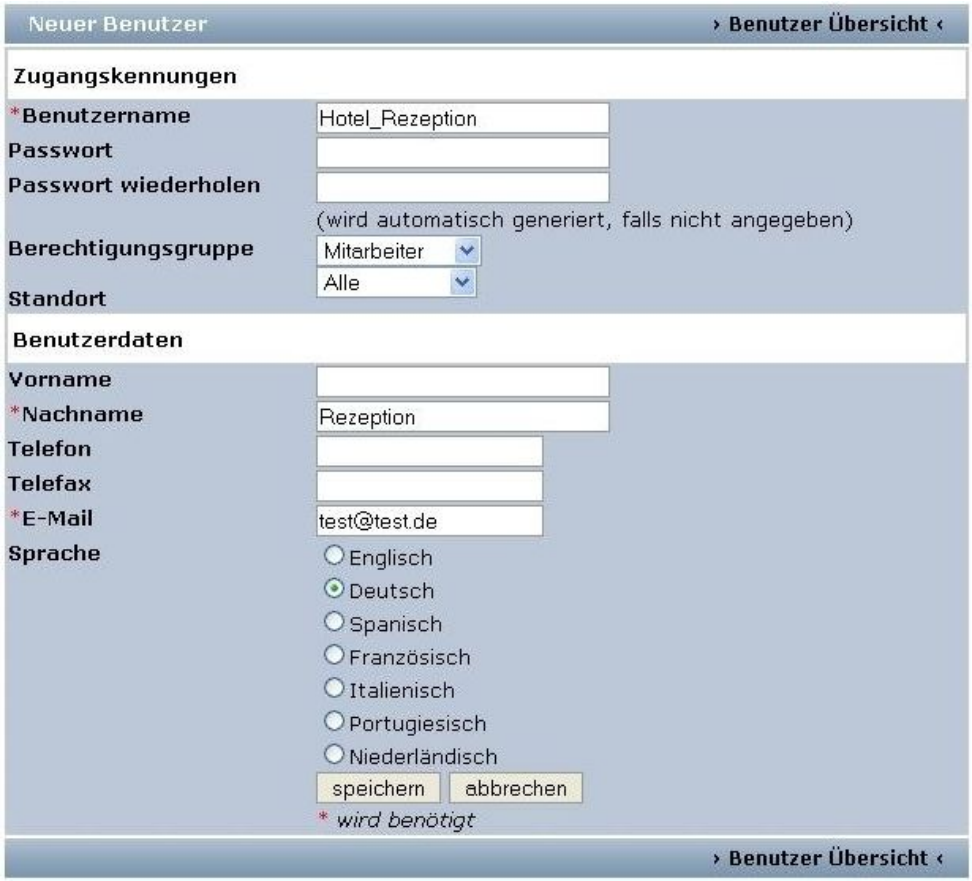


Abb. 22: **Benutzer** -> **Neuer Benutzer**

Die Felder **Benutzername**, **Nachname** und **E-Mail** sind Pflichtfelder.

Gehen Sie folgendermaßen vor:

(1) Tragen Sie bei **Benutzername** z. B. *Hotel_Rezeption* ein.

(2) Wählen Sie bei **Berechtigungsgruppe** *Mitarbeiter* aus. Der Mitarbeiter kann nur Accounts verwalten. Diese Einstellung ist zum Beispiel für die Rezeption eines Hotels geeignet. Der Administrator kann Standorte, Benutzer, Tarife und Accounts verwalten, aber keine neuen Mandanten anlegen.

(3) Wählen Sie einen **Standort** aus, falls mehrere Standorte vorhanden sind.

(4) Tragen Sie bei **Nachname** eine Bezeichnung des Benutzers ein, z. B. *Rezeption*.

(5) Tragen Sie die **E-Mail**-Adresse des Benutzers ein, z. B. *test@test.de*. Die Zugangsdaten werden automatisch an die angebene E-Mail-Adresse versendet.

(6) Bestätigen Sie mit **speichern**.

Tarife anlegen

Im Menü **Tarif** -> **Übersicht** wird eine Liste aller angelegten Tarife angezeigt. Sie können die vorhandenen Tarife bearbeiten oder neue Tarife anlegen.

(1) Gehen Sie zu **Tarif** -> **Neuer Tarif**, um einen neuen Tarif anzulegen.

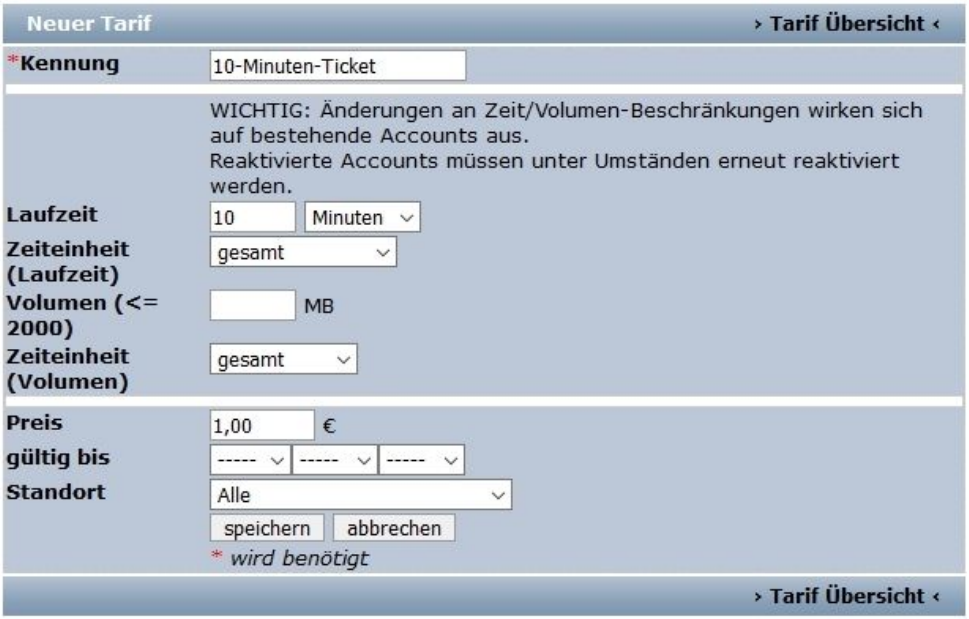


Abb. 23: **Tarif** -> **Neuer Tarif**

Das Feld **Kennung** ist Pflichtfeld.

Um einen neuen Tarif anzulegen, gehen Sie folgendermaßen vor:

(1) Tragen Sie bei **Kennung** eine Bezeichnung für den Tarif ein, z. B. *10-Minuten-Ticket* ein.

(2) Tragen Sie die **Laufzeit** des Tarifs ein, z. B. *10* Minuten.

(3) Wählen Sie bei **Zeiteinheit (Laufzeit)** *gesamt* aus.

Hinweis

Beachten Sie, dass die zur Verfügung gestellt Zeit läuft, sobald der Benutzer sich zum ersten Mal eingeloggt hat. Auch bei Inaktivität oder Ausloggen wird die verfügbare Zeitspanne weiter heruntergezählt. *Gesamt* bedeutet, dass dieser Zeitraum insgesamt verfügbar ist, während z. B. bei der Einstellung *täglich* der angegebene Zeitraum jeden Tag erneut zur Verfügung steht.

Der Preis hat nur symbolischen Wert und erscheint auf dem Ausdruck.

(4) Tragen Sie ggf. den **Preis** in Euro ein, z. B. `1,00`.

(5) Geben Sie ein Enddatum für die Laufzeit des Zeit- bzw. Volumentarifs an.

(6) Wählen Sie bei **Standort** `Alle` aus, wenn das Ticket an allen Standorten gültig sein soll.

(7) Bestätigen Sie mit **speichern**.

Tipp

Wenn Sie eine Dauerflatrate einrichten möchten, geben Sie bei **Laufzeit** `1440` Minuten ein und wählen Sie bei **Zeiteinheit (Laufzeit)** `täglich` aus.

Standort bearbeiten

Beim gewünschten Anmeldeverfahren können Sie unter **Standort**-> **Übersicht**-> **<Standort bearbeiten>** den Standort bearbeiten. Mit dem Upload Manager können Sie dort auch Ihre AGB hochladen und im dafür vorgesehenen Home-Verzeichnis ablegen.

Wenn Sie zusätzliche Standorten einrichten wollen, können Sie nach dem Erwerb einer entsprechenden Lizenz auf der Seite *www.bintec-elmeg.com* unter **Hotspot Lizenzierung** Ihre Daten eintragen und den neuen Standort aktivieren.

2.3.3 Verwaltung von Hotspot Accounts

Vor Ort können Sie Hotspot Accounts über *https://hotspot.bintec-elmeg.com/* verwalten. Die Anmeldedaten haben Sie per E-Mail erhalten.

Erzeugen eines Accounts

Sie können ein neues Ticket für einen Hotspot-Benutzer erzeugen. Hier können Sie zwischen einfacher Eingabe und erweiterter Eingabe wählen.

(1) Gehen Sie zu **Account** -> **Neuer Account (einfach)**.

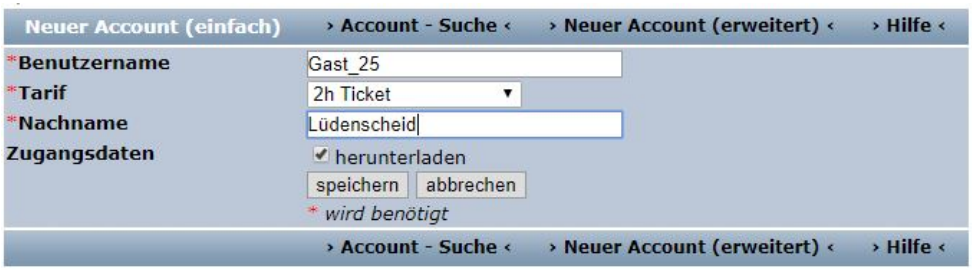


Abb. 24: **Account** -> **Neuer Account (einfach)**

Die Felder **Benutzername**, **Tarif** und **Nachname** sind Pflichtfelder.

Gehen Sie folgendermaßen vor:

(1) Tragen Sie bei **Benutzername** z. B. `Gast_25` ein.

(2) Wählen Sie einen **Tarif** aus, z. B. `2h Ticket`. Die Tarifauswahl kann von Ihrem Administrator erweitert werden.

(3) Tragen Sie bei **Nachname** z. B. `Lüdenscheid` ein.

(4) Bestätigen Sie mit **speichern**.

Für weitere Informationen klicken Sie auf **>Hilfe<** .

Für die erweiterte Eingabe gehen Sie in folgendes Menü:

(1) Gehen Sie zu **Account** -> **Neuer Account (erweitert)**.

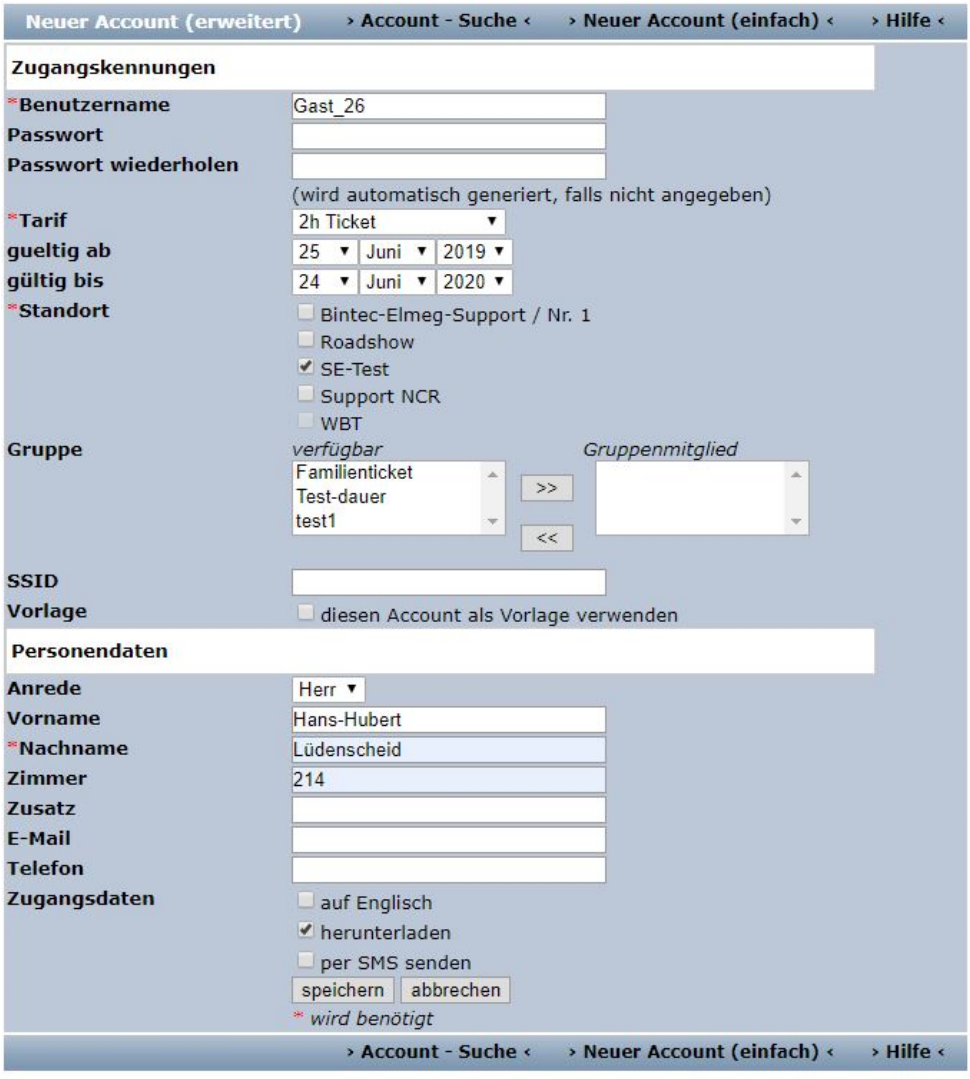


Abb. 25: **Account** -> **Neuer Account (erweitert)**

Die Felder **Benutzername**, **Nachname**, **Tarif** und **Standort** sind Pflichtfelder.

Gehen Sie folgendermaßen vor:

(1) Tragen Sie bei **Benutzername** z. B. `Gast_26` ein.

(2) Wählen Sie einen **Tarif** aus, z. B. `2h Ticket`. Die Tarifauswahl kann von Ihrem Administrator erweitert werden.

(3) Wählen Sie ein **Standort** aus, z. B. `SE-Test`.

(4) Unter **Gruppe** können Sie mehrere Tickets zu einer Gruppe zusammenfassen und

dieser Gruppe während eines bestimmten Zeitraums den Zugang zum Internet untersagen.

Unter **Account**->**Gruppe** werden die vorhandenen Gruppen angezeigt. Sie können einer Gruppe den Zugang zum Internet temporär verwehren. Dazu klicken Sie bei der gewünschten Gruppe in der Spalte **Aktion** auf die angezeigte Zahl und danach auf **Neue Aktion**. Im Fenster **Neue Gruppenaktion** können Sie die Zeitspanne für das Blockieren des Internetzugangs festlegen. Das ist zum Beispiel nützlich, um für die Schüler einer Schulklasse während einer Klassenarbeit den Zugang zum Internet zu unterbinden.

(5) Das Feld **SSID** ist optional und wird auf dem Ticket ausgedruckt.

(6) Tragen Sie bei **Vorname** z. B. *Hans-Hubert* ein.

(7) Tragen Sie bei **Nachname** z. B. *Lüdenscheid* ein.

(8) Tragen Sie bei **Zimmer** z. B. *214* ein.

(9) Bestätigen Sie mit **speichern**.

Für weitere Informationen klicken Sie auf **>Hilfe<** .

Account verwalten

Unter **Accout** können Sie ein neues Ticket für einen Hotspot-Benutzer aktivieren, Konten löschen und die Restlaufzeit ablesen. Sie können außerdem die Zugangsdaten für Ihren Kunden ausdrucken oder eine PDF-Datei erzeugen.

(1) Gehen Sie zu **Account** -> **Übersicht**, um ein neues Ticket zu aktivieren.

Um einen neu angelegten Benutzer zu aktivieren, müssen Sie auf den **Betrag** klicken. Die Anzeige wechselt dann auf *bezahlt*.

Für weitere Informationen klicken Sie auf **>Hilfe<** .

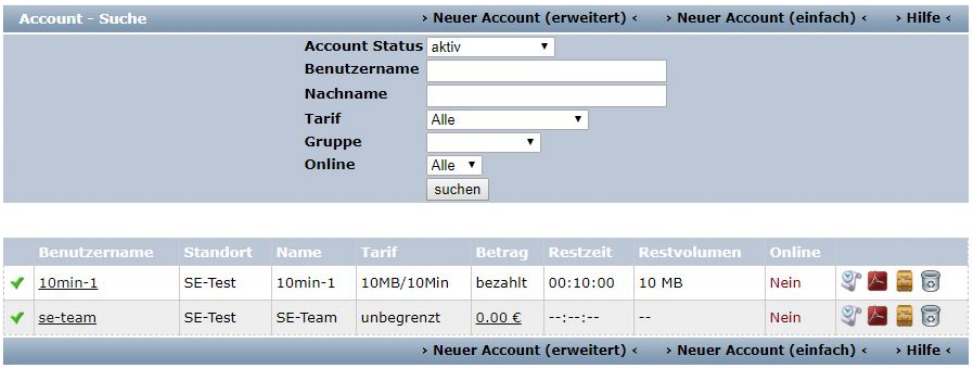


Abb. 26: **Account** -> **Übersicht**

2.3.4 Betrieb an mehreren Standorten

Die **bintec Hotspot Solution** erlaubt den standortübergreifenden Betrieb eines Hotspots. Dabei können die Hotspot-Benutzertickets zentral oder dezentral verwaltet werden. Es ist möglich Tickets zu erzeugen, die nur für einen bestimmten Standort gelten, und es ist möglich Tickets zu erzeugen, die für alle Standorte gültig sind.

Bekanntlich ist der Hotspot-Server zentral angesiedelt und für alle **bintec** Kunden (Mandanten) identisch. Die Erkennung, welcher Mandant mit dem RADIUS-Server des Hotspot-Server kommuniziert, wird über die sogenannte Domain realisiert. Diese Domain wird bei Aktivierung der Lizenz über das Lizenzportal *(www.bintec-elmeg.com* **Service & Support**->**Produkt Lizenzierung**-> **HotSpot Lizenzierung**) vergeben und bei der Konfiguration des **bintec RS353xx** eingetragen. Bei einer Lösung mit mehreren Standorten ist diese Domain für alle Standorte identisch.

Um die Standorte zu unterscheiden, wird der Parameter `RadiusNasId` eingeführt.

Konfiguration des bintec Hotspot-Servers

Nachdem Sie sich mit den Zugangsdaten unter *https://hotspot.bintec-elmeg.com* eingeloggt haben, werden Ihnen im Menü **Standort** -> **Übersicht** alle eingerichteten Standorte angezeigt.

Abb. 27: **Standort** -> **Übersicht**

Upload Manager

Klicken Sie im Menü **Standort** auf **Upload Manager**, um zum Beispiel Ihre AGB hochzuladen.

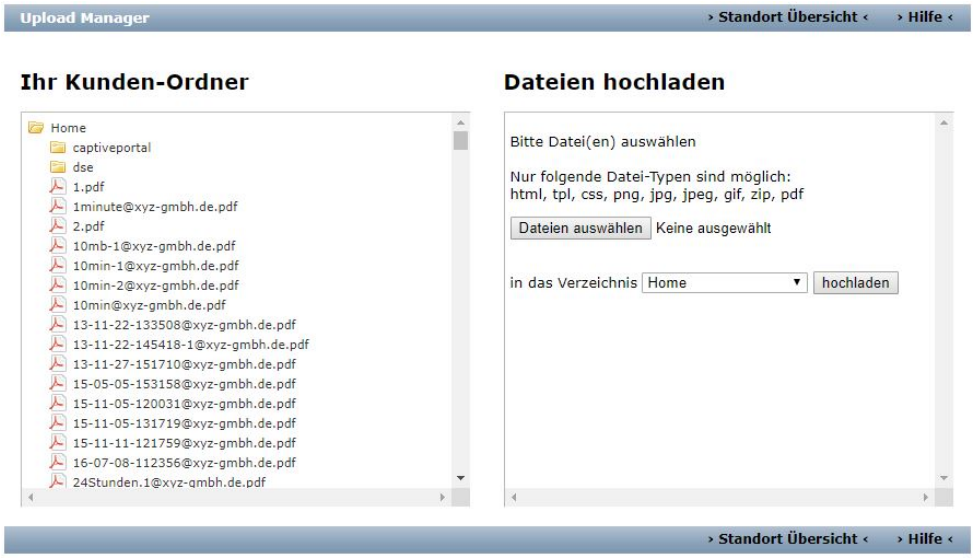


Abb. 28: **Upload Manager**

Für Informationen zur Verwendung des Upload Managers klicken Sie auf **>Hilfe<** .

Standort bearbeiten

Wählen Sie in der **Standort Übersicht** einen `Standort` aus. Sie sehen jetzt eine Detailansicht des Standorts. Hier können Sie den **Standort** bearbeiten.

Abb. 29: **Standort bearbeiten**

Im Menü **Standort bearbeiten** können Sie zur **Host Übersicht** wechseln.

(1) Gehen Sie zu **Host Übersicht**.

Abb. 30: **Host Übersicht**

Hier wird der **NAS-Identifier** angezeigt, der bei der Konfiguration des **bintec RS353xx** im Menü **Lokale Dienste**->**Hotspot-Gateway**->**Optionen** für den Parameter **Host für mehrere Standorte** benötigt wird.

Hinweis

Beachten Sie, dass Sie einen bestimmten Tarif für einen Standort nur dann verwenden können, wenn hier ein NAS-Identifier definiert und im Gateway eingetragen ist.

Sollte kein **NAS-Identifier** angezeigt werden, können Sie diesen unter **Neuer Host** festlegen.

Wenn Sie einen **Account** oder einen **Gutschein** erzeugen, haben Sie unter **Standort** die Wahl zwischen den Standorten und `Alle`.

Wenn Sie hier `Alle` auswähen, ist der Account für alle Standorte gültig.

(1) Gehen Sie zu **Gutschein** -> **Neuer Gutschein**, um einen Gutschein zu erzeugen.

Abb. 31: Neuer Gutschein

Die Felder **Anzahl**, **Tarif** und **Standort** sind Pflichtfelder.

Gehen Sie folgendermaßen vor:

(1) Tragen Sie bei **Anzahl** z. B. *100* ein.

(2) Wählen Sie einen **Tarif** aus, z. B. *2h Ticket*. Die Tarifauswahl kann von Ihrem Administrator erweitert werden.

(3) Wählem Sie bei **Standort** *Alle* aus.

(4) Bestätigen Sie mit **speichern**.

2.4 Anmeldeverfahren konfigurieren

Die Anmeldeseite für den Hotspot wird vom Hotspot-Server bereitgestellt.

Merkmale

- Drei Designs stehen zur Verfügung (Standard blau, Standard grau, Benutzerdefiniert).
- Das Design der Anmeldeseite ist für PC, Tablet PC und Smartphones optimiert. Die Darstellung wird je nach Gerät automatisch angepasst.
- Die Sprachauswahl funktioniert automatisch und entspricht der Browser-Sprache.
- Ein einmal angemeldeter Gast wird automatisch wieder eingeloggt (Cookie basierend).

Authentifizierungsmethoden

Folgende Authentifizierungsmethoden können zur Anmeldung am Hotspot verwendet werden:

- Anonym
- 1-Click
- SMS
- PayPal

Im Folgenden erfahren Sie, wie Sie die jeweilige Authentisierungsmethode für die Anmeldung am Hotspot konfigurieren.

2.4.1 Anonym

Mit dieser Authentifizierungsmethode kann sich ein Benutzer durch Akzeptieren der AGB kostenlos an einem Hotspot anmelden.

Abb. 32: Anonyme Anmeldung

bintec Hotspot-Server konfigurieren

Konfigurieren Sie zuerst die Authentifizierungsmethode auf dem Hotspot-Server.

(1) Starten Sie einen Webbrowser, rufen Sie die Seite *https://hotspot.bintec-elmeg.com* auf und geben Sie Ihre Anmeldedaten ein.

(2) Gehen Sie zu **Standort** -> **<Standort bearbeiten>**.

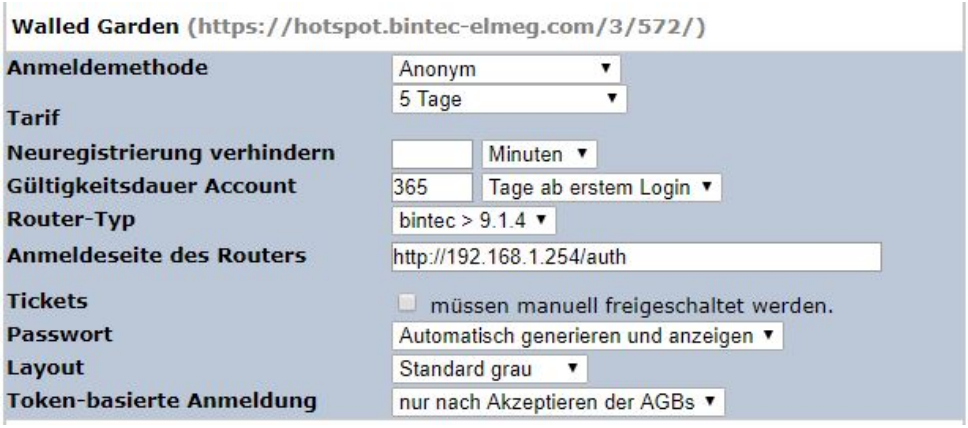


Abb. 33: **Standort** -> **<Standort bearbeiten>**

Gehen Sie folgendermaßen vor, um einen neuen Standort anzulegen:

(1) Bei **Anmeldemethode** wählen Sie `Anonym` aus.

(2) Wählen Sie einen **Tarif** aus, z. B. `5 Tage`.

(3) Die **Anmeldeseite des Routers** ist die lokale IP-Adresse des Hotspot-Gateways, hier z. B. `http://192.168.1.254/auth`.

Hinweis

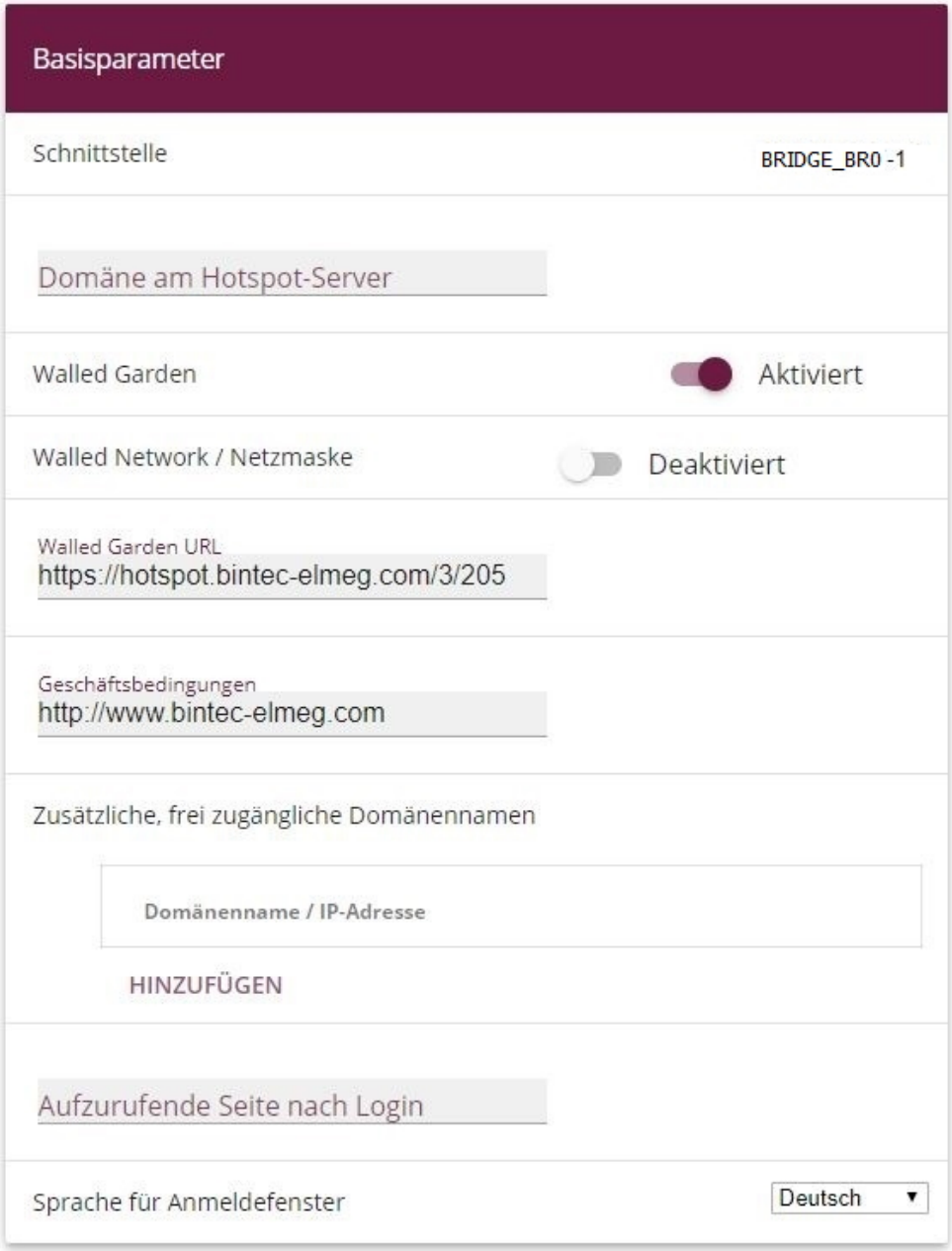
Beachten Sie, dass der Zusatz zur IP-Adresse `/auth` an dieser Stelle unverzichtbar ist.

(4) Bestätigen Sie Ihre Angaben mit **speichern**.

bintec-Gateway konfigurieren

Starten Sie eine Web-Verbindung zum bintec-Gateway (z. B. **bintec RS353xx**).

(1) Gehen Sie zu **Lokale Dienste** -> **Hotspot-Gateway** -> **Hotspot-Gateway** -> **BRIDGE_BR0-1** .


Basisparameter
Schnittstelle
BRIDGE_BR0 -1
Domäne am Hotspot-Server
Walled Garden
Aktiviert
Walled Network / Netzmaske
Deaktiviert
Walled Garden URL
https://hotspot.bintec-elmeg.com/3/205
Geschäftsbedingungen
http://www.bintec-elmeg.com
Zusätzliche, frei zugängliche Domänennamen
Domänenname / IP-Adresse
HINZUFÜGEN
Aufzurufende Seite nach Login
Sprache für Anmeldefenster
Deutsch

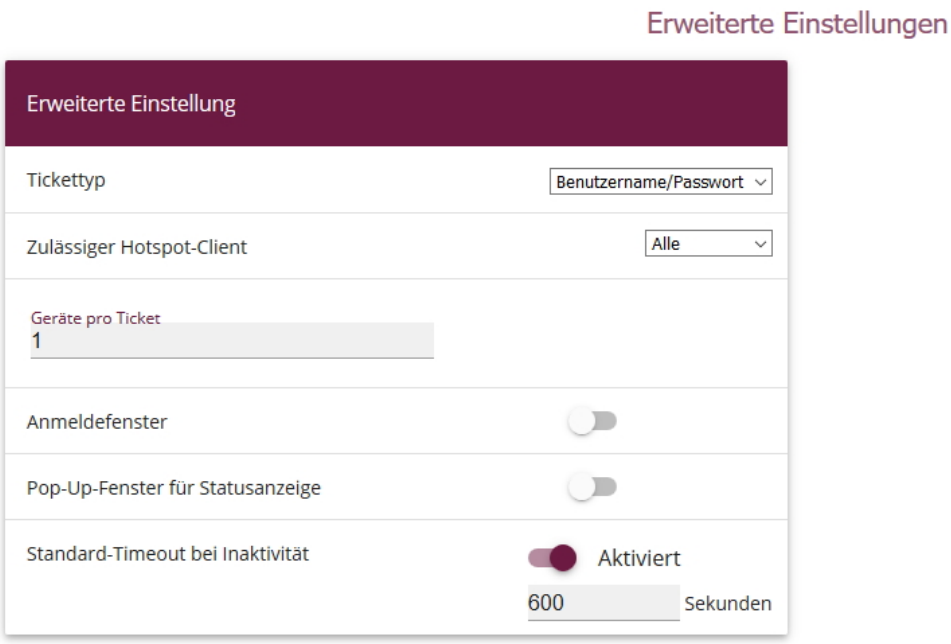


Abb. 35: **Lokale Dienste** -> **Hotspot-Gateway** -> **Hotspot-Gateway** -> **BRIDGE_BR0-1**

Gehen Sie folgendermaßen vor, um das Hotspot-Gateway zu konfigurieren:

(1) Aktivieren Sie die Funktion **Walled Garden,** damit Sie einen kostenfreien Bereich von Webseiten (Intranet) definieren können.

(2) Als **Walled Garden URL** geben Sie die von Hotspot-Server bereitgestellte Anmeldeseite an, hier z. B. `https://hotspot.bintec-elmeg.com/3/205/`.

(3) Tragen Sie in das Eingabefeld **Geschäftsbedingungen** die Adresse der AGB auf dem Intranet-Server bzw. auf einem öffentlichen Server ein, z. B. `http://www.bintec-elmeg.com`. Die Seite muss im Adressraum des Walled Garden-Networks liegen.

(4) Deaktivieren Sie die Funktion **Anmeldefenster**. Wenn die Funktion deaktiviert ist, wird nur die Webseite mit Informationen, Werbung und/oder Links zu frei zugänglichen Webseiten angezeigt.

(5) Bestätigen Sie mit **OK**.

2.4.2 1-Click

Mit dieser Authentifizierungsmethode kann sich ein Benutzer unter Angabe seiner E-Mail-Adresse kostenlos an einem Hotspot anmelden.

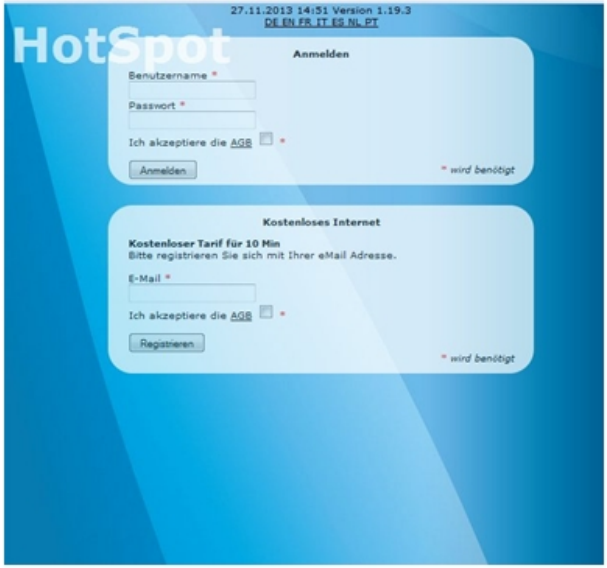


Abb. 36: Anmeldung 1-Click

Der Benutzer muss seine E-Mail-Adresse eingeben und die allgemeinen Geschäftsbedingungen (AGB) akzeptieren. Damit wird er als Gast angemeldet. Er erhält eine E-Mail mit Zugangsdaten, um sich bei Bedarf mit einem Zweitgerät anzumelden.

bintec Hotspot-Server konfigurieren

Konfigurieren Sie zuerst die Authentifizierungsmethode auf dem Hotspot-Server.

(1) Starten Sie einen Webbrowser, rufen Sie die Seite *https://hotspot.bintec-elmeg.com* auf und geben Sie Ihre Anmeldedaten ein.

(2) Gehen Sie in das Menü **Standort** ->**Überblick**-> **<Standort bearbeiten>**.

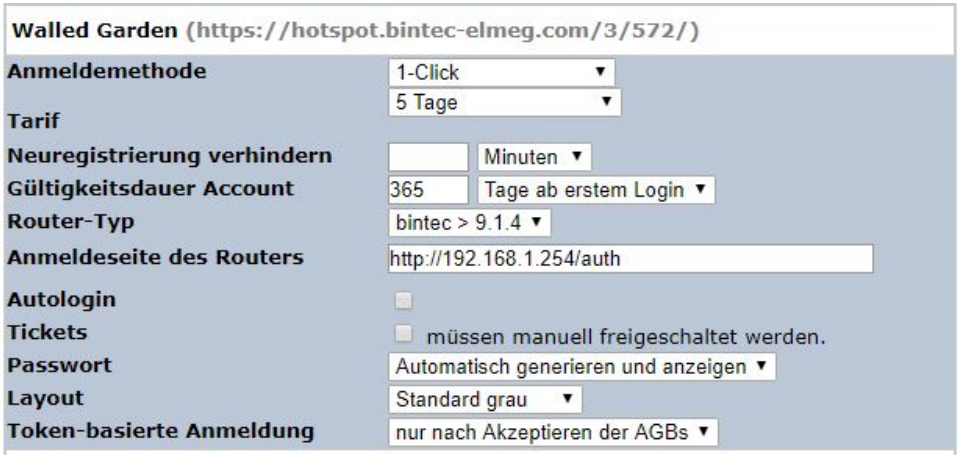


Abb. 37: **Standort** ->**Überblick** ->**<Standort bearbeiten>**

Gehen Sie folgendermaßen vor, um einen Standort zu bearbeiten:

(1) Als **Walled Garden** URL wird die vom Hotspot-Server bereitgestellte Seite angezeigt.

(2) Wählen Sie hier die **Anmeldemethode** `1-Click` aus.

(3) Wählen Sie einen **Tarif** aus, z. B. `5 Tage`.

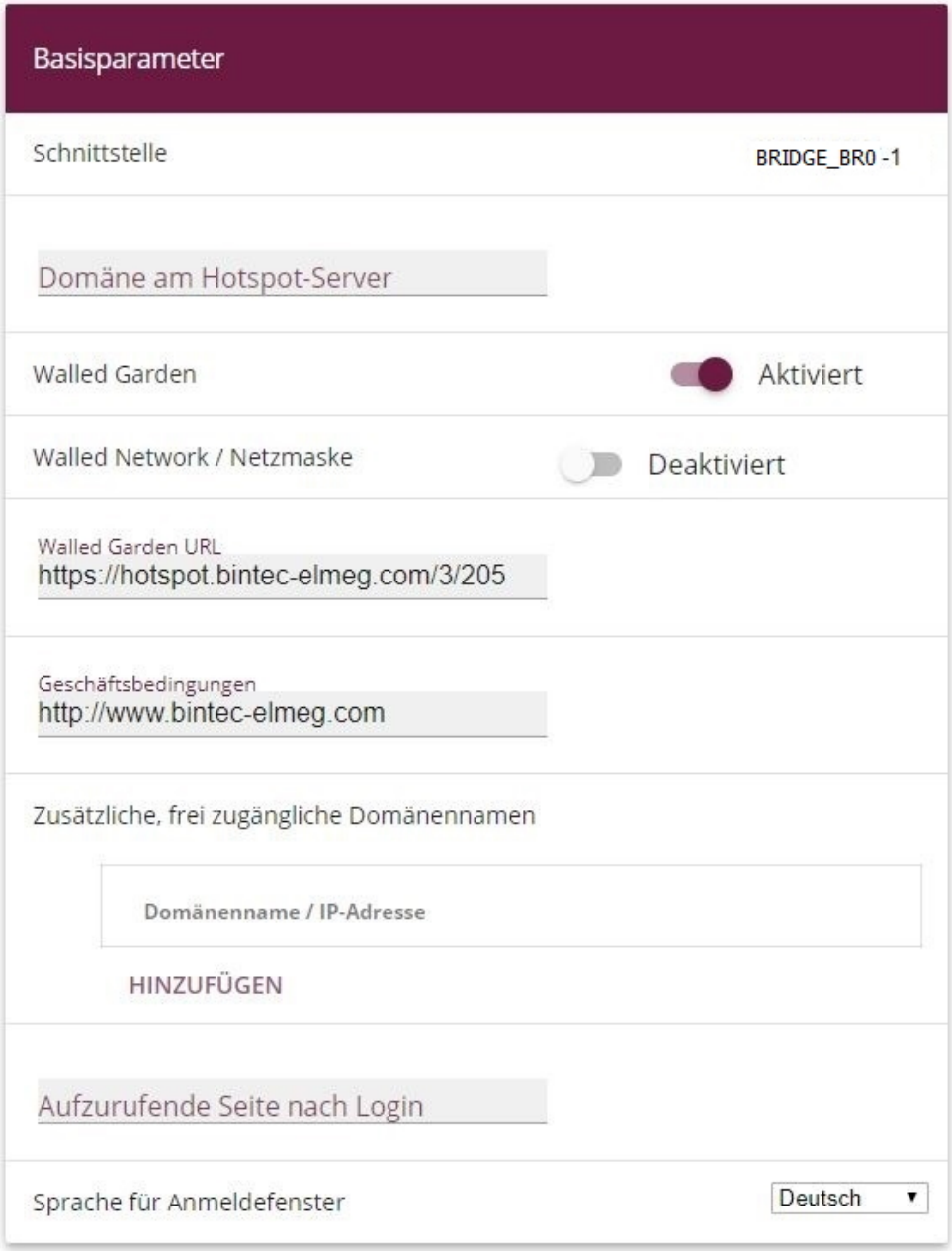
(4) Die **Anmeldeseite des Routers** ist die lokale IP-Adresse des Hotspot-Gateways, hier z. B. `http://192.168.1.254/auth`.

(5) Bestätigen Sie Ihre Angaben mit **Speichern**.

bintec Hotspot-Gateway konfigurieren

Öffnen Sie einen Webbrowser und starten Sie eine Verbindung zum bintec-Gateway (z. B. **bintec RS353xx**).

(1) Gehen Sie zu **Lokale Dienste** -> **Hotspot-Gateway** -> **Hotspot-Gateway** -> **BRIDGE_BR0-1** .


Basisparameter
Schnittstelle
BRIDGE_BR0 -1
Domäne am Hotspot-Server
Walled Garden
Aktiviert
Walled Network / Netzmaske
Deaktiviert
Walled Garden URL
https://hotspot.bintec-elmeg.com/3/205
Geschäftsbedingungen
http://www.bintec-elmeg.com
Zusätzliche, frei zugängliche Domänennamen
Domänenname / IP-Adresse
HINZUFÜGEN
Aufzurufende Seite nach Login
Sprache für Anmeldefenster
Deutsch

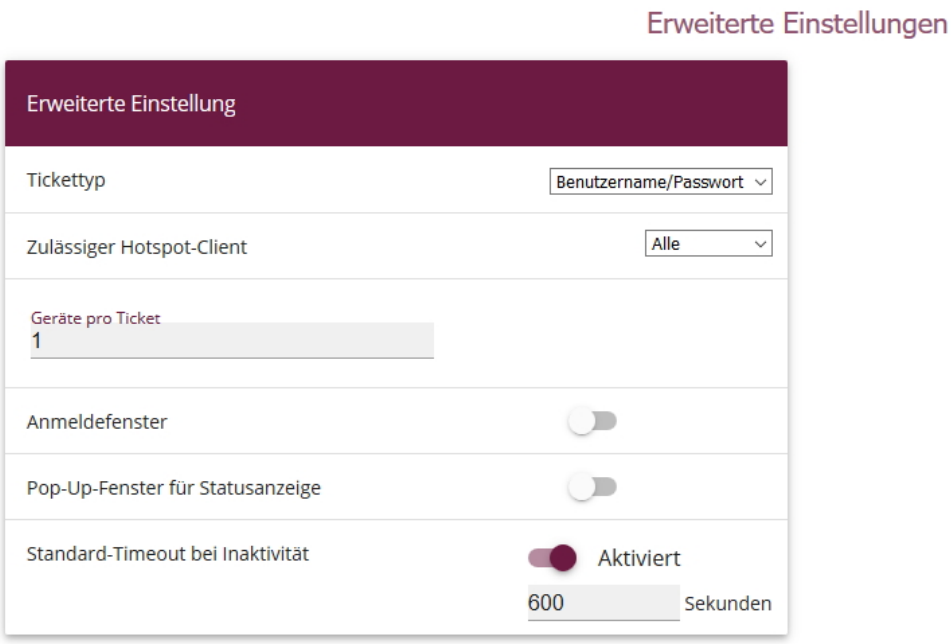


Abb. 39: **Lokale Dienste** -> **Hotspot-Gateway** -> **Hotspot-Gateway** -> **BRIDGE_BR0-1**

Gehen Sie folgendermaßen vor, um das Hotspot-Gateway zu konfigurieren:

(1) Aktivieren Sie die Funktion **Walled Garden**, damit Sie einen kostenfreien Bereich von Webseiten (Intranet) definieren können.

(2) Als **Walled Garden URL** geben Sie die vom Hotspot-Server bereitgestellte Anmeldeseite an, hier z. B. *https://hotspot.bintec-elmeg.com/3/205/*.

(3) Tragen Sie in das Eingabefeld **Geschäftsbedingungen** die Adresse der AGB´s auf dem Intranet-Server bzw. auf einem öffentlichen Server ein, z. B. *http://www.bintec-elmeg.com*. Die Seite muss im Adressraum des Walled-Garden-Networks liegen.

(4) Deaktivieren Sie die Funktion **Anmeldefenster**. Wenn die Funktion deaktiviert ist, wird nur die Webseite mit Informationen, Werbung und/oder Links zu frei zugänglichen Webseiten angezeigt.

(5) Bestätigen Sie mit **OK**.

2.4.3 SMS

Mit dieser Authentifizierungsmethode kann sich ein Benutzer unter Angabe seiner Mobilfunkrufnummer kostenlos an einem Hotspot registrieren. Er erhält eine SMS mit den Zugangsdaten, die er auf der Anmeldeseite eingeben muss. Zusätzlich muss er die allgemeinen Geschäftsbedingungen (AGB) akzeptieren.

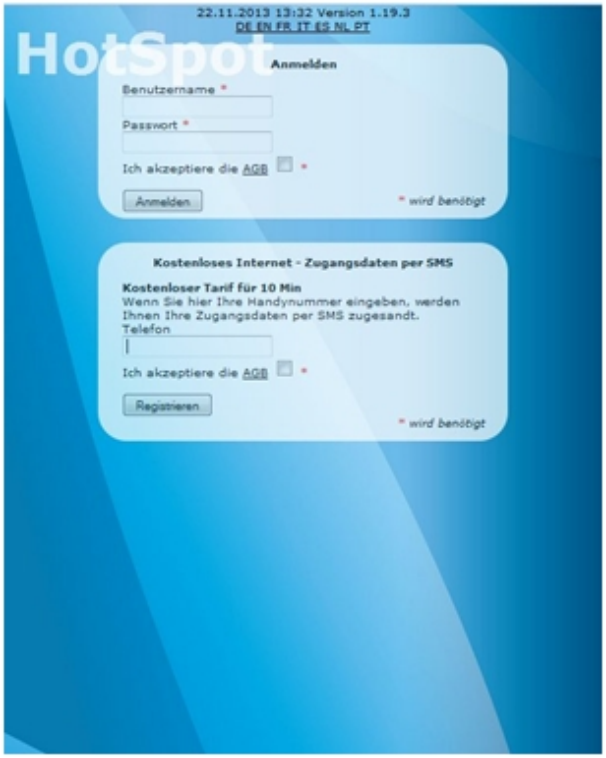


Abb. 40: SMS-Anmeldung

Der Dienst verwendet einen SMS-Dienstleister als SMS-Versender, z. B. *www.lox24.de* . Zunächst muss ein Konto bei *www.lox24.de* oder bei *www.lox24.eu* eingerichtet werden. **LOX24** bietet verschiedene Tarife an, zum Beispiel **Economy**. Fürs Erste kann der Benutzer einen Test-Account bei **LOX24** einrichten.

bintec Hotspot-Server konfigurieren

Konfigurieren Sie zuerst die Authentifizierungsmethode auf dem Hotspot-Server.

(1) Starten Sie einen Webbrowser, rufen Sie die Seite *https://hotspot.bintec-elmeg.com* auf und geben Sie Ihre Anmeldedaten ein.

(2) Gehen Sie in das Menu **Mandant** -> **<Mandant bearbeiten>** .

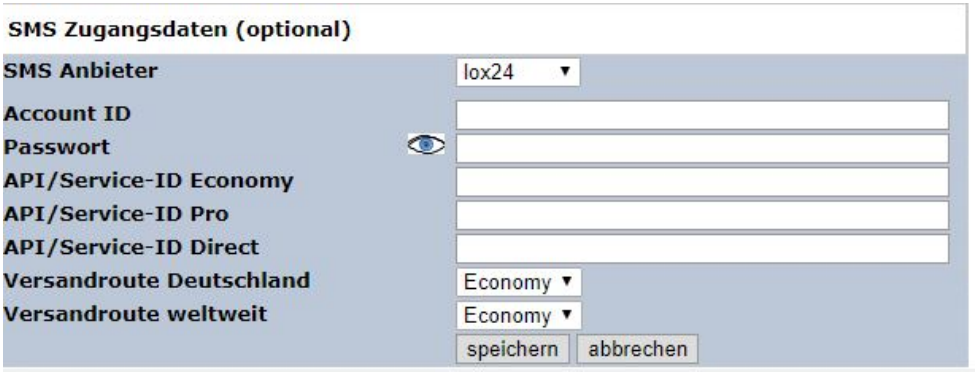


Abb. 41: **Mandant** -> **<Mandant bearbeiten>**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie unter **SMS Zugangsdaten** den **SMS-Anbieter** `lox24` aus.

Hinweis

Beachten Sie, dass **smstrade** zwar ebenfalls ausgewählt, aber für Neuinstallationen nicht mehr verwendet werden kann.

(2) Wählen Sie bei **Versandroute Deutschland** den Tarif aus, z. B. `Economy`.

(3) Bestätigen Sie Ihre Angaben mit **speichern**.

Wählen Sie nun die **Anmeldemethode** aus.

(1) Gehen Sie in das Menü **Standort** -> **<Standort bearbeiten>**.

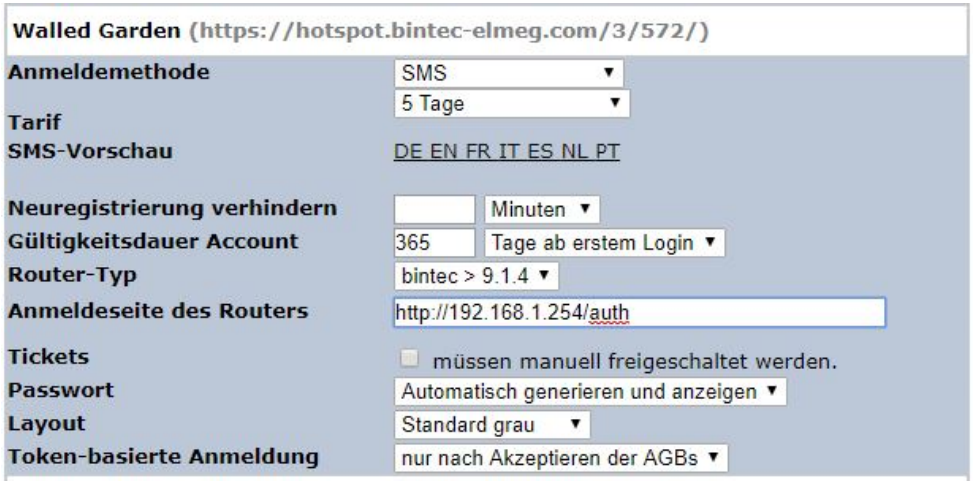


Abb. 42: **Standort** -> **<Standort bearbeiten>**

Gehen Sie folgendermaßen vor, um den Standort zu bearbeiten:

(1) Als **Walled Garden URL** wird die vom Hotspot-Server bereitgestellte Seite angezeigt.

(2) Wählen Sie hier die **Anmeldemethode** *SMS* aus.

(3) Wählen Sie einen **Tarif** aus, z. B. *5 Tage*.

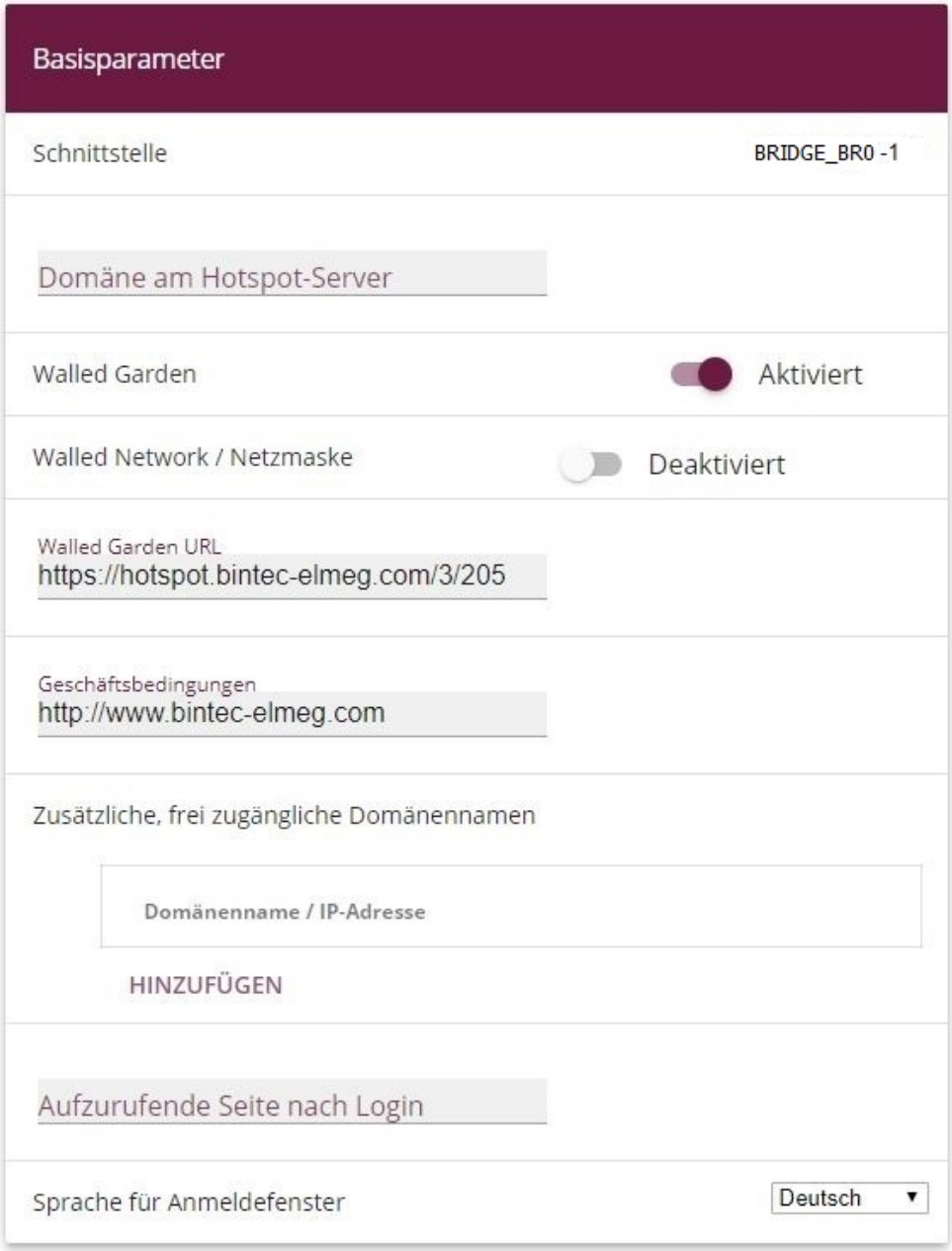
(4) Die **Anmeldeseite des Routers** ist die lokale IP-Adresse des Hotspot-Gateways, hier z. B. *http://192.168.1.254/auth*.

(5) Bestätigen Sie Ihre Angaben mit **Speichern**.

bintec Hotspot-Gateway konfigurieren

Starten Sie eine Web-Verbindung zum bintec-Gateway (z. B. **bintec RS353xx**).

(1) Gehen Sie zu **Lokale Dienste** -> **Hotspot-Gateway** -> **Hotspot-Gateway** ->**BRIDGE_BR0-1** .


Basisparameter
Schnittstelle
BRIDGE_BR0 -1
Domäne am Hotspot-Server
Walled Garden
Aktiviert
Walled Network / Netzmaske
Deaktiviert
Walled Garden URL
https://hotspot.bintec-elmeg.com/3/205
Geschäftsbedingungen
http://www.bintec-elmeg.com
Zusätzliche, frei zugängliche Domänennamen
Domänenname / IP-Adresse
HINZUFÜGEN
Aufzurufende Seite nach Login
Sprache für Anmeldefenster
Deutsch

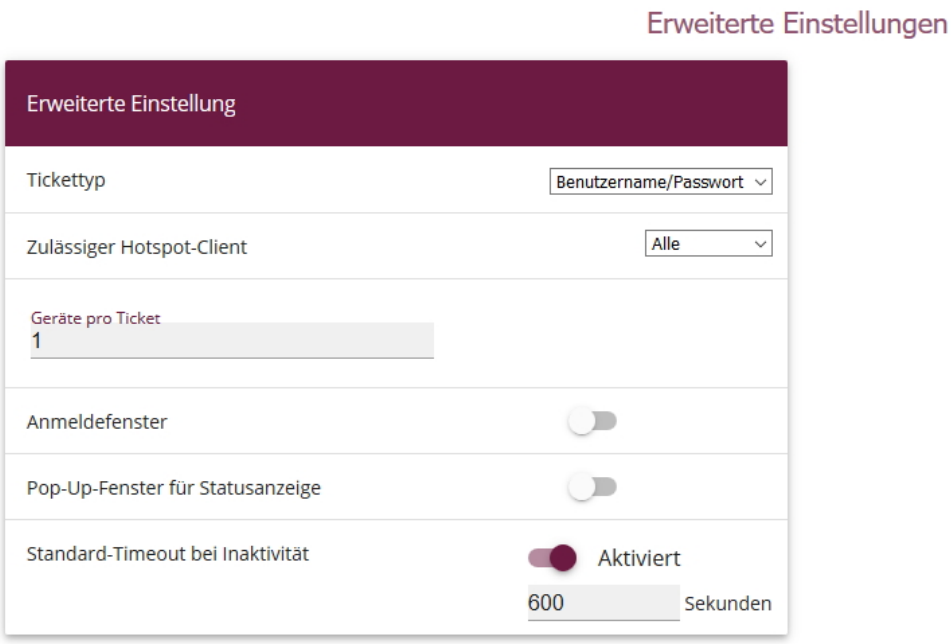


Abb. 44: **Lokale Dienste** -> **Hotspot-Gateway** -> **Hotspot-Gateway** -> **BRIDGE_BR0-1**

Gehen Sie folgendermaßen vor, um das Hotspot-Gateway zu konfigurieren:

(1) Aktivieren Sie die Funktion **Walled Garden,** damit Sie einen kostenfreien Bereich von Webseiten (Intranet) definieren können.

(2) Als **Walled Garden URL** geben Sie die vom Hotspot-Server bereitgestellte Anmeldeseite an, hier z. B. `https://hotspot.bintec-elmeg.com/3/205/`.

(3) Tragen Sie in das Eingabefeld **Geschäftsbedingungen** die Adresse der AGB auf dem Intranet-Server bzw. auf einem öffentlichen Server ein, z. B. `http://www.bintec-elmeg.com`. Die Seite muss im Adressraum des Walled Garden-Networks liegen.

(4) Deaktivieren Sie die Funktion **Anmeldefenster**. Wenn die Funktion deaktiviert ist, wird nur die Webseite mit Informationen, Werbung und/oder Links zu frei zugänglichen Webseiten angezeigt.

(5) Bestätigen Sie mit **OK**.

2.4.4 PayPal

Mit der Authentifizierungsmethode PayPal ist es möglich, einen kostenpflichtigen Hotspot-Dienst einzurichten.

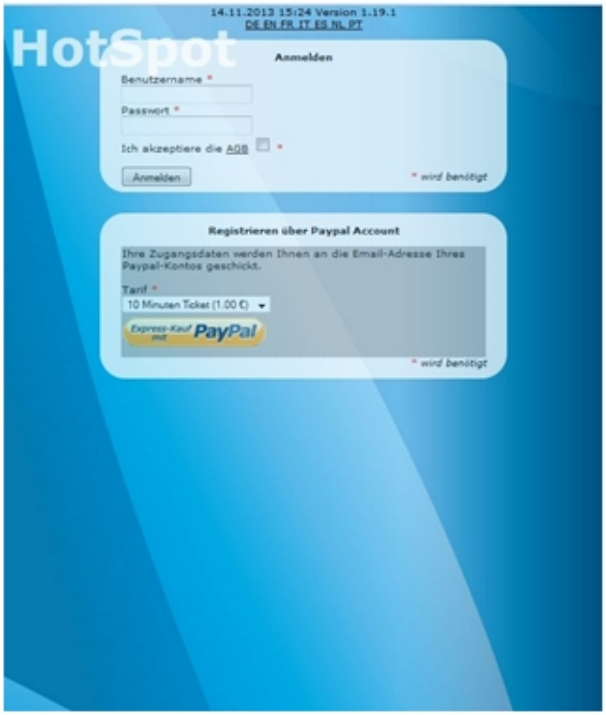


Abb. 45: Anmeldung PayPal

Der Benutzer wählt einen **Tarif**, z. B. `10-Minuten-Ticket (1.00 €)`, aus und klickt auf die Schaltfläche **Express Kauf PayPal**. Danach wird die PayPal-Zahlungsseite angezeigt. Nach Abschluss der Zahlung wird der Benutzer automatisch angemeldet. Zusätzlich erhält er an die E-Mail Adresse seines PayPal-Kontos eine E-Mail mit den Zugangsdaten, um sich bei Bedarf mit einem anderen Gerät anzumelden.

Zur Nutzung des Dienstes wird ein PayPal-Händlerkonto benötigt. Die Registrierung eines solchen Kontos ist kostenfrei. PayPal erhebt auf die eingezogenen Geldbeträge eine Gebühr. Details kann der Benutzer den PayPal-Webseiten entnehmen.

bintec Hotspot-Server konfigurieren

Geben Sie zuerst die API-Anmeldedaten auf dem Hotspot-Server ein.

(1) Starten Sie einen Webbrowser, rufen Sie die Seite *https://hotspot.bintec-elmeg.com* auf und geben Sie Ihre Anmeldedaten ein.

(2) Gehen Sie in das Menü **Mandant** -> **<Mandant bearbeiten>**.

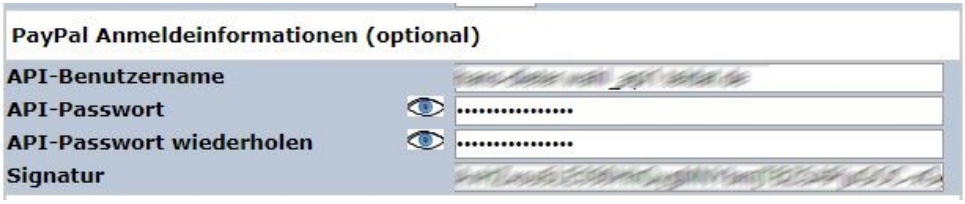


Abb. 46: **Mandant** -> **<Mandant bearbeiten>**

Geben Sie die API-Anmeldedaten (**API-Benutzername**, **API-Passwort** und die **Signatur**) ein. Die Daten können Sie über Ihr PayPal-Händlerkonto (Mein_Profil/mehr/Verkäufer_Händler/API-Zugriff) abrufen.

Wählen Sie nun die **Anmeldemethode** aus.

(1) Gehen Sie auf die Seite des Hotspot-Servers unter **Standort** -> **<Standort bearbeiten>**.

Abb. 47: **Standort** -> **<Standort bearbeiten>**

Gehen Sie folgendermaßen vor, um einen neuen Standort anzulegen:

(1) Als **Walled Garden URL** wird die vom Hotspot-Server bereitgestellte Seite angezeigt.

(2) Wählen Sie hier die **Anmeldemethode** `Paid Service` aus.

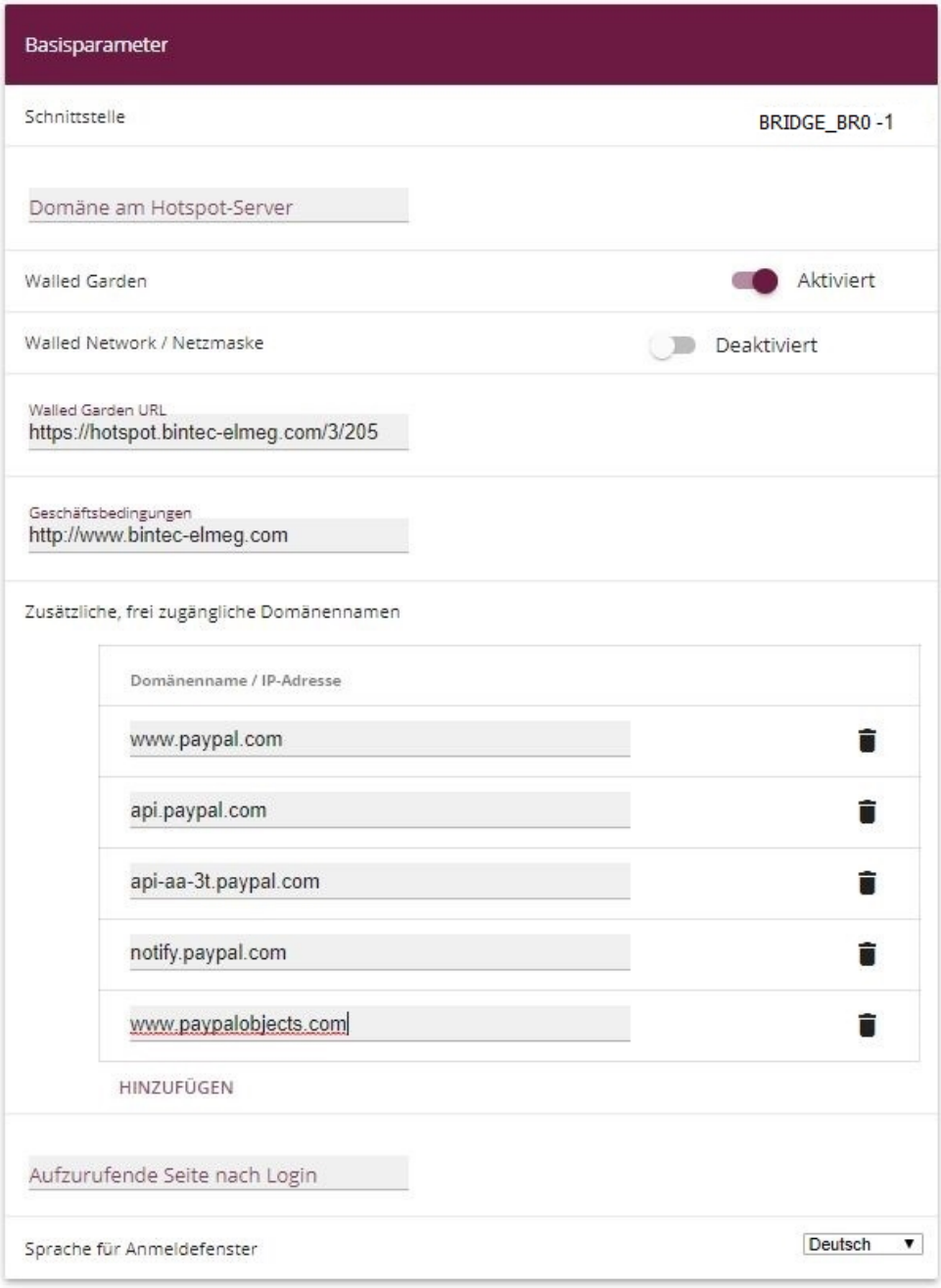
(3) Die **Anmeldeseite des Routers** ist die lokale IP-Adresse des Hotspot-Gateways, hier z. B. `http://192.168.1.254/auth`.

(4) Bestätigen Sie Ihre Angaben mit **speichern**.

bintec Hotspot-Gateway konfigurieren

Zur Konfiguration des Hotspot-Gateways starten Sie eine Web-Verbindung zum bintec-Gateway (z. B. **bintec RS353xx**).

(1) Gehen Sie zu **Lokale Dienste** -> **Hotspot-Gateway** -> **Hotspot-Gateway** -> **BRIDGE_BR0-1** .



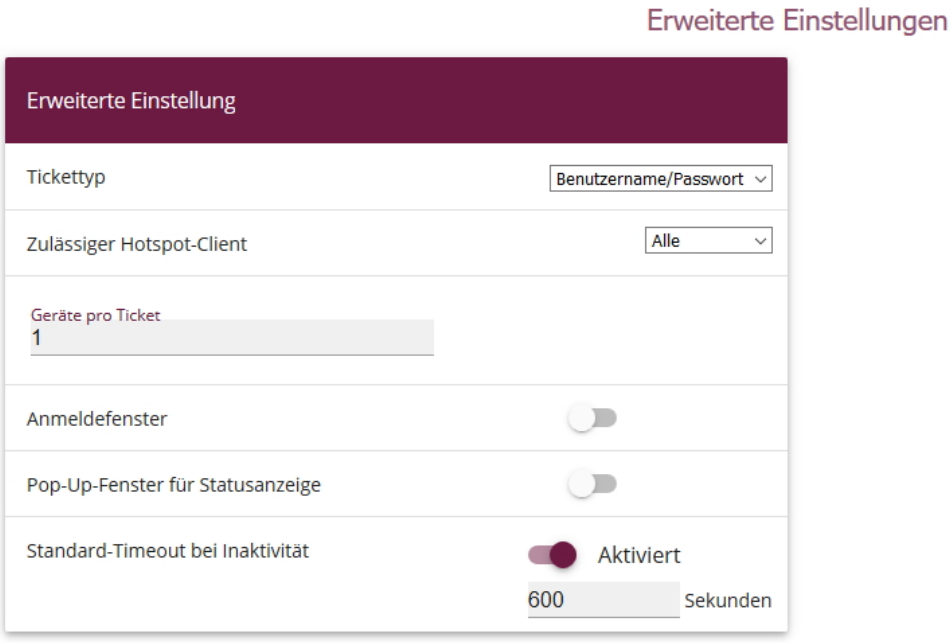


Abb. 49: **Lokale Dienste** -> **Hotspot-Gateway** -> **Hotspot-Gateway** ->**BRIDGE_BR0-1**

Gehen Sie folgendermaßen vor, um das Hotspot-Gateway zu konfigurieren:

(1) Aktivieren Sie die Funktion **Walled Garden**, damit Sie einen kostenfreien Bereich von Webseiten (Intranet) definieren können.

(2) Als **Walled Garden URL** geben Sie die vom Hotspot-Server bereitgestellte Anmeldeseite an, hier z. B. *https://hotspot.bintec-elmeg.com/3/205/*.

(3) Tragen Sie in das Eingabefeld **Geschäftsbedingungen** die Adresse der AGB auf dem Intranet-Server bzw. auf einem öffentlichen Server ein, z. B. *http://www.bintec-elmeg.com*. Die Seite muss im Adressraum des Walled-Garden-Networks liegen.

(4) Deaktivieren Sie die Funktion **Anmeldefenster**. Wenn die Funktion deaktiviert ist, wird nur die Webseite mit Informationen, Werbung und/oder Links zu frei zugänglichen Webseiten angezeigt.

(5) Bestätigen Sie mit **OK**.

Tipp

Der Aufbau der Anmeldeseite und der Paypal Zahlungsseiten kann je nach Tageszeit recht langsam erfolgen, dies hat mit der hohen Belastung der Paypal.com Webseite zu tun. Davon ist auch das Paypal Logo auf der Anmeldeseite betroffen, da dieses immer vom Paypal.com geladen wird.

Die Sicherheitswarnung, die bei manchen Browsern angezeigt wird, lässt sich vermeiden, wenn Sie die **Anmeldeseite des Routers** über https aufrufen; dazu ist ein SSL-Zertifikat notwendig.

2.4.5 Default Free Service

Default Free Service kann für bestehende Installationen weiterverwendet werden. Für neue Installationen ist **Default Free Service** nicht mehr verfügbar.

2.5 Hinweise für den sicheren Betrieb

2.5.1 Mehrfaches Anmelden

Bei entsprechender Konfiguration kann sich ein Benutzer mit einem Coupon (Benutzername, Passwort) mehrfach anmelden (siehe **Geräte pro Ticket** im Gateway Menu **Lokale Dienste**->**Hotspot-Gateway**->**Hotspot-Gateway**->**Neu**->**Erweiterte Einstellungen**.)

Dies ist nützlich, wenn er neben einem Smartphone noch andere Geräte wie zum Beispiel ein Tablet verwenden will oder wenn innerhalb einer Familie mehrere Geräte in Betrieb sind.

2.5.2 Verhindern der Sichtbarkeit der Teilnehmer untereinander

In einem LAN oder WLAN sind alle Teilnehmer auf der IP-Ebene miteinander verbunden. Bei einem Hotspot-System muss dies natürlich verhindert werden.

Hotspot mit nur einem WLAN Access Point

Hier wird nur ein **bintec RS353xw** als Hotspot-Gateway eingesetzt. Alle Benutzer sind ausschließlich über WLAN angemeldet. Kabelgebundes LAN wird nicht verwendet. Der Internetzugang erfolgt über ein lokales Netzwerk oder über ADSL.

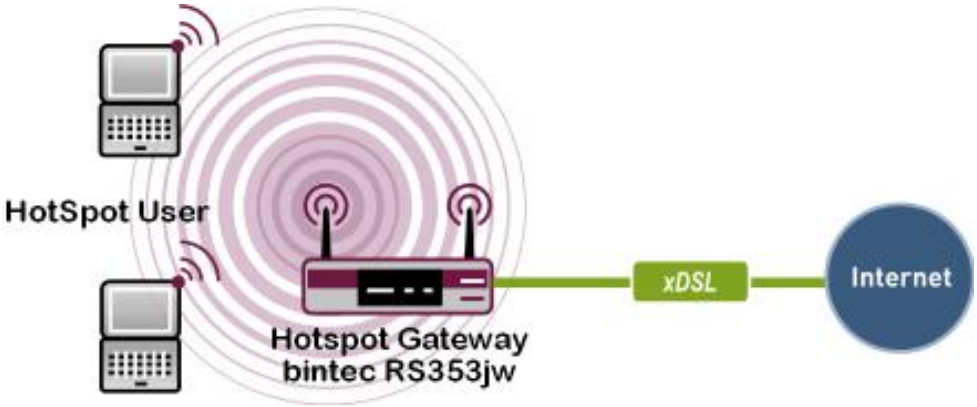


Abb. 50: Hotspot mit einem WLAN Access Point

Um die interne Kommunikation zwischen den Hotspot-Benutzern (WLAN-Clients) zu verhindern, muss im Menu **Wireless LAN** -> **WLAN** -> **Drahtlosnetzwerke (VSS)** -> ✎ die Option **Intra-cell Repeating** deaktiviert werden.

Hotspot mit mehreren WLAN Access Points

Hier werden mehrere WLAN Access Points eingesetzt, die über LAN mit dem **bintec RS353xw** Gateway verbunden sind. Der Internetzugang erfolgt über ein lokales Netzwerk oder über xDSL.

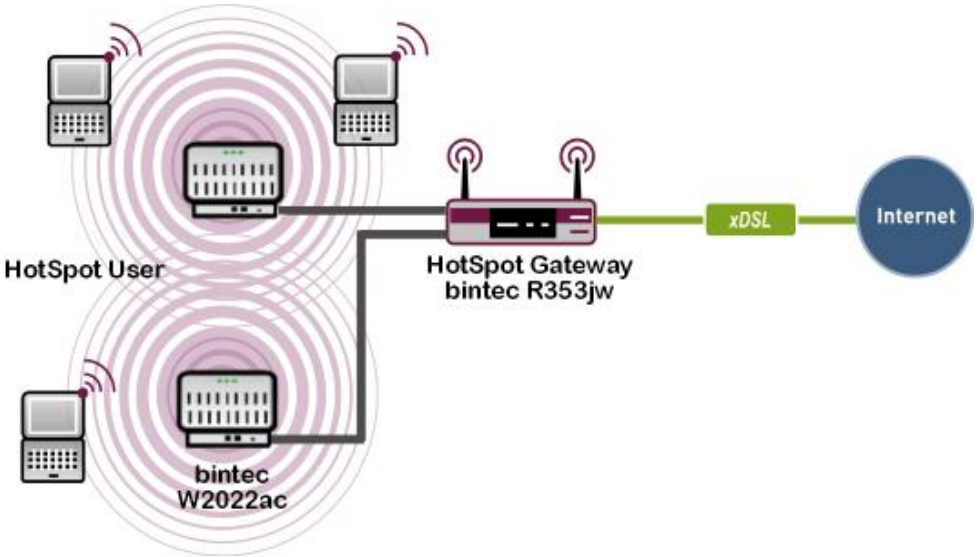


Abb. 51: Hotspot mit mehreren WLAN Access Points

Um die Sichtbarkeit zwischen den einzelnen Hotspot-Benutzern zu verhindern, muss an allen WLAN-Arbeitsplätzen im Menu **Wireless LAN** -> **WLAN** -> **Drahtlosnetzwerke (VSS)** -> die Option **Intra-cell Repeating** deaktiviert werden. Darüber hinaus ist für jeden WLAN Access Point ein eigenes VLAN einzurichten, um die interne Kommunikation zwischen Teilnehmer, die an verschiedenen Access Points angemeldet sind, zu verhindern.

Hotspot mit Ethernet-LAN-Clients

Hier sind mehrere Hotspot-Benutzer über ein LAN an das Hotspot-Gateway angeschlossen. Der Internetzugang erfolgt über ein lokales Netzwerk oder über xDSL.

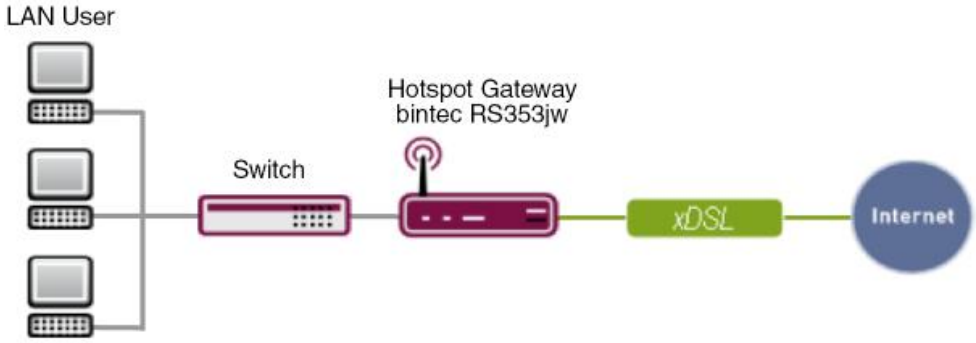


Abb. 52: Hotspot mit Ethernet-LAN-Client

Der PC eines Hotspot-Benutzers wird an einen VLAN-fähigen Switch angeschlossen. Dabei erhält jeder physikalische Port des Switches ein eigenes VLAN.

2.5.3 Verschlüsselte / Unverschlüsselte WLAN-Verbindung

Um die Anmeldung der Benutzer an den Hotspot zu erleichtern, arbeiten die meisten Hotspots unverschlüsselt.

Dies hat folgende Nachteile:

- Jeglicher WLAN Traffic kann von Leuten mit technischem Know-How und einigen Hilfsmitteln mitgelesen werden.

  - Die Coupon-/ Anmeldedaten zur Anmeldung eines Benutzers an den Hotspot.

  - Alle aufgerufenen Webseiten, sofern diese nicht SSL-verschlüsselt sind, z. B. https-Webseiten. Webseiten von Banken sind i. d. R. nicht betroffen, da diese SSL-verschlüsselt sind.

- E-Mails, die nicht SSL-verschlüsselt sind.

- Anmeldedaten zu E-Mail-Konten, die nicht SSL verschlüsselt sind.

Hinweis

Es ist wichtig, dass auf diesen Umstand in den AGB hingewiesen wird.

2.5.4 WPA-Verschlüsselung

Um die obigen Nachteile zu umgehen, kann man die WLAN-Schnittstelle z. B. mit WPA-PSK verschlüsseln. Der Sicherheitsgewinn ist jedoch nicht sehr groß, da jeder diesen Schlüssel kennen muss.

2.5.5 IP/ARP Spoofing

Wird bei der Konfiguration des Gateways der Parameter **Zulässiger Hotspot-Client** auf *DHCP-Client* gesetzt, werden eingehende Pakete zusätzlich auf die IP- bzw. MAC-Adresse des Absenders hin überprüft. Eine gefälschte („gespoofte“) Absender-IP- bzw. MAC-Adresse führt bei IPv4 zu einem Adresskonflikt. Dieses Szenario wird folglich nicht abgefangen.

2.6 Konfigurationsschritte im Überblick

Software auf dem Gateway aktualisieren

Feld	Menü	Wert
Aktion	**Wartung** -> **Software & Konfiguration** -> **Optionen**	*Systemsoftware aktualisieren*
Quelle	**Wartung** -> **Software & Konfiguration** -> **Optionen**	*Aktuelle Software vom Update-Server*

Sprache konfigurieren

Feld	Menü	Wert
Sprache für Anmeldefenster	**Lokale Dienste** -> **Hotspot-Gateway** -> **Hotspot-Gateway** -> **Neu**	z. B. *Deutsch*

Zeitzone einstellen

Feld	Menü	Wert
Zeitzone	**Systemverwaltung** -> **Globale Ein-**	*Europe/Berlin*

Feld	Menü	Wert
	stellungen -> Datum und Uhrzeit	
ISDN-Zeitserver	**Systemverwaltung -> Globale Einstellungen -> Datum und Uhrzeit**	Deaktiviert
System als Zeitserver	**Systemverwaltung -> Globale Einstellungen -> Datum und Uhrzeit**	Deaktiviert

Deaktivieren der lokalen Kommunikation

Feld	Menü	Wert
Intra-cell Repeating	**Wireless LAN Controller->Slave-AP-Konfiguration ->Drahtlosnetzwerke (VSS)->**	Deaktiviert
Intra-cell Repeating	**Wireless LAN -> WLAN ->Drahtlosnetzwerke (VSS)->**	Deaktiviert

RADIUS-Server Zugriff konfigurieren 1

Feld	Menü	Wert
Authentifizierungstyp	**Systemverwaltung -> Remote Authentifizierung -> RADIUS-> Neu**	*Accounting*
Betreibermodus	**Systemverwaltung -> Remote Authentifizierung -> RADIUS-> Neu**	*bintec HotSpot Server*
Server-IP-Adresse	**Systemverwaltung -> Remote Authentifizierung -> RADIUS-> Neu**	z. B. *62.245.165.180*
RADIUS-Passwort	**Systemverwaltung -> Remote Authentifizierung -> RADIUS-> Neu**	*funkwerk-ec*
Priorität	**Systemverwaltung -> Remote Authentifizierung -> RADIUS-> Neu**	*2*
Richtlinie	**Systemverwaltung -> Remote Authentifizierung -> RADIUS-> Neu->Erweiterte Einstellungen**	*Nicht verbindlich*
Server Timeout	**Systemverwaltung -> Remote Authentifizierung -> RADIUS-> Neu->Erweiterte Einstellungen**	*3000*
Wiederholungen	**Systemverwaltung -> Remote Authentifizierung -> RADIUS-> Neu->Erweiterte Einstellungen**	*3*

RADIUS-Server Zugriff konfigurieren 2

Feld	Menü	Wert
Authentifizierungstyp	**Systemverwaltung -> Remote Authentifizierung -> RADIUS-> Neu**	*Login-Authentifizierung*
Server-IP-Adresse	**Systemverwaltung -> Remote Authentifizierung -> RADIUS-> Neu**	z. B. *62.245.165.180*
RADIUS-Passwort	**Systemverwaltung -> Remote Authentifizierung -> RADIUS-> Neu**	*funkwerk-ec*
Priorität	**Systemverwaltung -> Remote Authentifizierung -> RADIUS-> Neu**	*1*
Richtlinie	**Systemverwaltung -> Remote Authentifizierung -> RADIUS-> Neu->Erweiterte Einstellungen**	*Nicht verbindlich*
Server Timeout	**Systemverwaltung -> Remote Authentifizierung -> RADIUS-> Neu->Erweiterte Einstellungen**	*3000*
Wiederholungen	**Systemverwaltung -> Remote Authentifizierung -> RADIUS-> Neu->Erweiterte Einstellungen**	*3*

Mandanten-Profil bearbeiten

Feld	Menü	Wert
Logo	**Mandant -> Mandant bearbeiten**	*Datei auswählen*
AGB	**Mandant -> Mandant bearbeiten**	*Datei auswählen*

Benutzer anlegen

Feld	Menü	Wert
Benutzername	**Benutzer -> Neuer Benutzer**	z. B. *Hotel_Rezeption*
Berechtigungsgruppe	**Benutzer -> Neuer Benutzer**	*Mitarbeiter*
Standort	**Benutzer -> Neuer Benutzer**	*Alle*
Nachname	**Benutzer -> Neuer Benutzer**	z. B. *Rezeption*
E-Mail	**Benutzer -> Neuer Benutzer**	z. B. *test@test.de*

Tarife anlegen

Feld	Menü	Wert
Kennung	**Tarif -> Neuer Tarif**	z. B. *10-Minuten-Ticket*
Laufzeit	**Tarif -> Neuer Tarif**	*10* Minuten

Feld	Menü	Wert
Zeiteinheit (Laufzeit)	**Tarif -> Neuer Tarif**	*gesamt*
Preis	**Tarif -> Neuer Tarif**	z. B. *1,00* Euro
Standort	**Tarif -> Neuer Tarif**	*Alle*

Account erzeugen (einfach)

Feld	Menü	Wert
Benutzername	**Account -> Neuer Account (einfach)**	z. B. *Gast_25*
Tarif	**Account -> Neuer Account (einfach)**	z. B. *2h Ticket*
Nachname	**Account -> Neuer Account (einfach)**	z. B. *Lüdenscheid*

Account erzeugen (erweitert)

Feld	Menü	Wert
Benutzername	**Account -> Neuer Account (erweitert)**	z. B. *Gast_26*
Tarif	**Account -> Neuer Account (erweitert)**	z. B. *2h Ticket*
Standort	**Account -> Neuer Account (erweitert)**	z. B. *SE-Test*
Vorname	**Account -> Neuer Account (erweitert)**	z. B. *Hans-Hubert*
Nachname	**Account -> Neuer Account (erweitert)**	z. B. *Lüdenscheid*
Zimmer	**Account -> Neuer Account (erweitert)**	z. B. *214*

Account verwalten

Feld	Menü	Wert
Betrag	**Account -> Übersicht**	*Betrag* anklicken

Upload Manager verwenden

Feld	Menü	Wert
Standort	**Standort -> Übersicht**	*Standort*
Upload Manager	**StandortUpload Manager**	*Datei hochladen / Hilfe aufrufen*

Gutschein erzeugen

Feld	Menü	Wert
Anzahl	**Gutschein -> Neuer Gutschein**	z. B. *100*
Tarif	**Gutschein -> Neuer Gutschein**	z. B. *2h Ticket*
Standort	**Gutschein -> Neuer Gutschein**	*Alle*

Anmeldeverfahren konfigurieren

Anonym

Feld	Menü	Wert
Anmeldemethode	**Standort -> <Standort bearbeiten>**	*Anonym*
Tarif	**Standort -> <Standort bearbeiten>**	z. B. *5 Tage*
Anmeldeseite des Router	**Standort -> <Standort bearbeiten>**	*http://192.168.1.254/auth*
Walled Garden	**Lokale Dienste -> Hotspot-Gateway -> Hotspot-Gateway -> BRIDGE_BR0-1 ->**	*Aktiviert*
Walled Garden URL	**Lokale Dienste -> Hotspot-Gateway -> Hotspot-Gateway -> BRIDGE_BR0-1 ->**	z. B. *https://www.hotspot.bintec-elmeg.com/3/205*
Geschäftsbedingungen	**Lokale Dienste -> Hotspot-Gateway -> Hotspot-Gateway -> BRIDGE_BR0-1 ->**	z. B. *http://www.hotspot.bintec-elmeg.com*
Anmeldefenster	**Lokale Dienste -> Hotspot-Gateway -> Hotspot-Gateway -> BRIDGE_BR0-1 -> ->Erweiterte Einstellungen**	*Deaktiviert*
Pop-Up-Fenster für Statusanzeige	**Lokale Dienste -> Hotspot-Gateway -> Hotspot-Gateway -> BRIDGE_BR0-1 -> ->Erweiterte Einstellungen**	*Deaktiviert*

1-Click

Feld	Menü	Wert
Walled Garden	**Standort ->Überblick -><Standort bearbeiten>**	URL wird angezeigt

Feld	Menü	Wert
Anmeldemethode	**Standort ->Überblick -><Standort bearbeiten>**	*1-Click*
Tarif	**Standort ->Überblick -><Standort bearbeiten>**	z. B. *5 Tage*
Anmeldeseite des Routers	**Standort ->Überblick -><Standort bearbeiten>**	z. B. *http://192.168.1.254/auth*
Walled Garden	**Lokale Dienste -> Hotspot-Gateway -> Hotspot-Gateway -> BRIDGE_BR0-1 ->**	*Aktiviert*
Walled Garden URL	**Lokale Dienste -> Hotspot-Gateway -> Hotspot-Gateway -> BRIDGE_BR0-1 ->**	z. B. *https://hotspot.bintec-elmeg.com/3/205*
Geschäftsbedingungen	**Lokale Dienste -> Hotspot-Gateway -> Hotspot-Gateway -> BRIDGE_BR0-1 ->**	z. B. *http://www.bintec-elmeg.com*
Anmeldefenster	**Lokale Dienste -> Hotspot-Gateway -> Hotspot-Gateway -> BRIDGE_BR0-1 -> ->Erweiterte Einstellungen**	*Deaktiviert*
Pop-Up-Fenster für Statusanzeige	**Lokale Dienste -> Hotspot-Gateway -> Hotspot-Gateway -> BRIDGE_BR0-1 -> ->Erweiterte Einstellungen**	*Deaktiviert*

SMS

Feld	Menü	Wert
SMS Anbieter	**Mandant -> <Mandant bearbeiten>**	*lox24*
Account ID	**Mandant -> <Mandant bearbeiten>**	xxxxxxxxxxxxxxxxx
Versandroute Deutschland	**Mandant -> <Mandant bearbeiten>**	z. B. *Economy*
Anmeldemethode	**Standort -> <Standort bearbeiten>**	*SMS*
Tarif	**Standort -> <Standort bearbeiten>**	z. B. *5 Tage*
Anmeldeseite des Routers	**Standort -> <Standort bearbeiten>**	z. B. *http://192.168.1.254/auth*
Walled Garden	**Lokale Dienste -> Hotspot-Gateway**	*Aktiviert*

Feld	Menü	Wert
	-> Hotspot-Gateway -> BRIDGE_BR0-1 ->	
Walled Garden URL	**Lokale Dienste -> Hotspot-Gateway -> Hotspot-Gateway -> BRIDGE_BR0-1 ->**	z. B. *https://hotspot.bintec-elmeg.com/3/205*
Geschäftsbedingungen	**Lokale Dienste -> Hotspot-Gateway -> Hotspot-Gateway -> BRIDGE_BR0-1 ->**	z. B. *http://www.bintec-elmeg.com*
Anmeldefenster	**Lokale Dienste -> Hotspot-Gateway -> Hotspot-Gateway ->BRIDGE_BR0-1 -> ->Erweiterte Einstellungen**	*Deaktiviert*
Pop-Up-Fenster für Statusanzeige	**Lokale Dienste -> Hotspot-Gateway -> Hotspot-Gateway -> BRIDGE_BR0-1 -> ->Erweiterte Einstellungen**	*Deaktiviert*

PayPal

Feld	Menü	Wert
API-Benutzername	**Mandant -> <Mandant bearbeiten>**	xxxxxxxxxxxxxxxxx
API-Passwort	**Mandant -> <Mandant bearbeiten>**	z. B. *supersecret*
API-Passwort wiederholen	**Mandant -> <Mandant bearbeiten>**	z. B. *supersecret*
Signatur	**Mandant -> <Mandant bearbeiten>**	xxxxxxxxxxxxxxxxx
Anmeldemethode	**Standort -> <Standort bearbeiten>**	*Paid Service*
Tarif	**Standort -> <Standort bearbeiten>**	z. B. *Alle*
Anmeldeseite des Routers	**Standort -> <Standort bearbeiten>**	z. B. *http://192.168.1.254/auth*
Walled Garden	**Lokale Dienste -> Hotspot-Gateway -> Hotspot-Gateway -> BRIDGE_BR0-1 ->**	*Aktiviert*
Walled Garden URL	**Lokale Dienste -> Hotspot-Gateway -> Hotspot-Gateway -> BRIDGE_BR0-1 ->**	z. B. *https://hotspot.bintec-elmeg.com/3/205*
Geschäftsbedingungen	**Lokale Dienste -> Hotspot-Gateway -> Hotspot-Gateway ->**	z. B. *http://www.bintec-*

Feld	Menü	Wert
	BRIDGE_BR0-1 ->	*elmeg.com*
Anmeldefenster	**Lokale Dienste** -> **Hotspot-Gateway** -> **Hotspot-Gateway** -> **BRIDGE_BR0-1** -> ->**Erweiterte Einstellungen**	*Deaktiviert*
Pop-Up-Fenster für Statusanzeige	**Lokale Dienste** -> **Hotspot-Gateway** -> **Hotspot-Gateway** -> **BRIDGE_BR0-1** -> ->**Erweiterte Einstellungen**	*Deaktiviert*

Kapitel 3 WLAN - 802.1x Authentifizierung unter Nutzung eines Microsoft Servers 2008

3.1 Einleitung

Im Folgenden wird die Anbindung von WLAN-Clients unter Nutzung des 802.1x (EAP-PEAP) Protokolls an einen Windows-Server 2008 beschrieben.

Die WLAN-Authentifizierung wird von einem RADIUS-Server durchgeführt. Dabei werden die Authentifizierungsdaten (Benutzername/Passwort/Zertifikate) auf dem zentralen Windows-Server verwaltet. Hierfür wird ein Windows 2008 Server verwendet, der folgende Server-Rollen zur Verfügung stellt:

- Active Directory-Domänendienste (ADS)
- Active Directory-Zertifikatsdienste (CA)
- Netzwerkrichtlinien und Zugriffsdienste (NPS)

Der Workshop zeigt die Konfiguration des Servers als Zertifizierungsstelle (CA) und die Einrichtung des RADIUS-Servers (Network Policy Server (NPS)). Anschließend wird die Konfiguration eines Access Points beschrieben. Bei der Anbindung eines WLAN-Clients unter Windows7 werden Bordmittel verwendet.

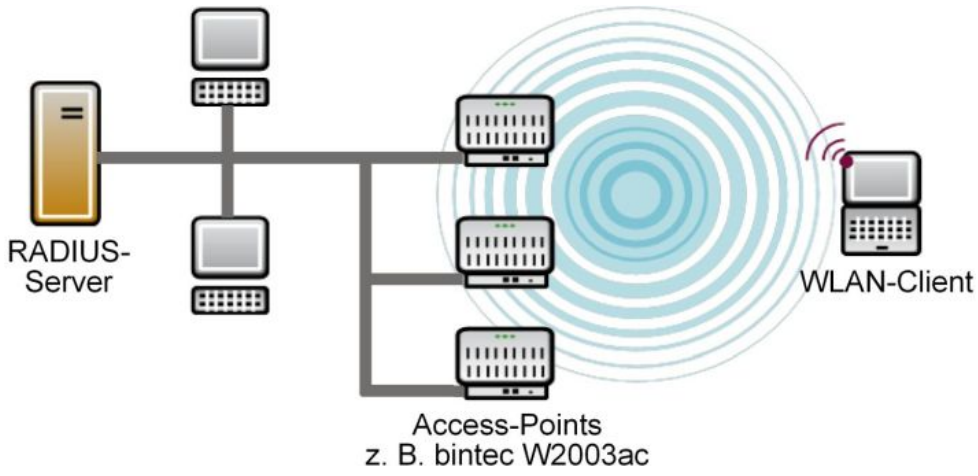


Abb. 53: Beispielszenario

Voraussetzungen

- Ein Microsoft Windows Server 2008 (z. B. Windows Server 2008 R2 Standard)
- Die Active Directory Konfiguration wird vorausgesetzt
- Es wird ein DHCP-Server im Netzwerk vorausgesetzt (z. B Windows DHCP-Server)
- Ein oder mehrere **bintec** Access Points (z. B. **bintec W2003ac**)
- Ein- oder mehrere WLAN-Clients (z. B. Windows 7 WLAN Supplicant)

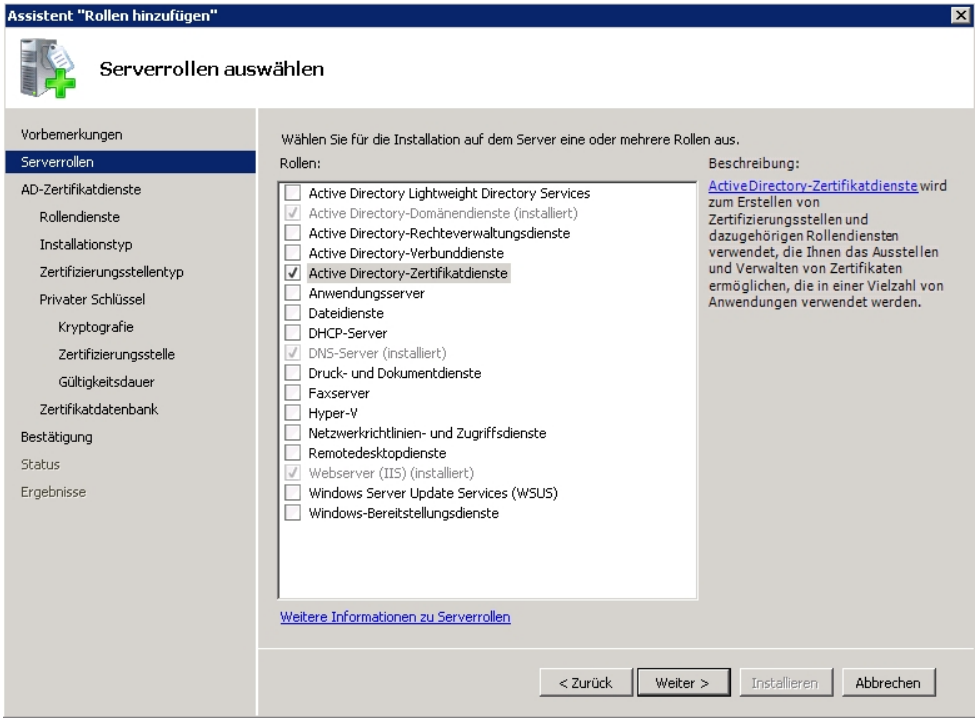
3.2 Server Konfiguration

3.2.1 Konfiguration der Active Directory-Zertifikatsdienste

Die Authentifzierung von WLAN-Clients am RADIUS-Server wird über eine gesicherte Transportverbindung durchgeführt. Hierzu wird das Zertifikat einer Zertifizierungsstelle (CA Zertifikat) benötig. Zum Hinzufügen der **Serverrolle** wird der Server-Manager verwendet.

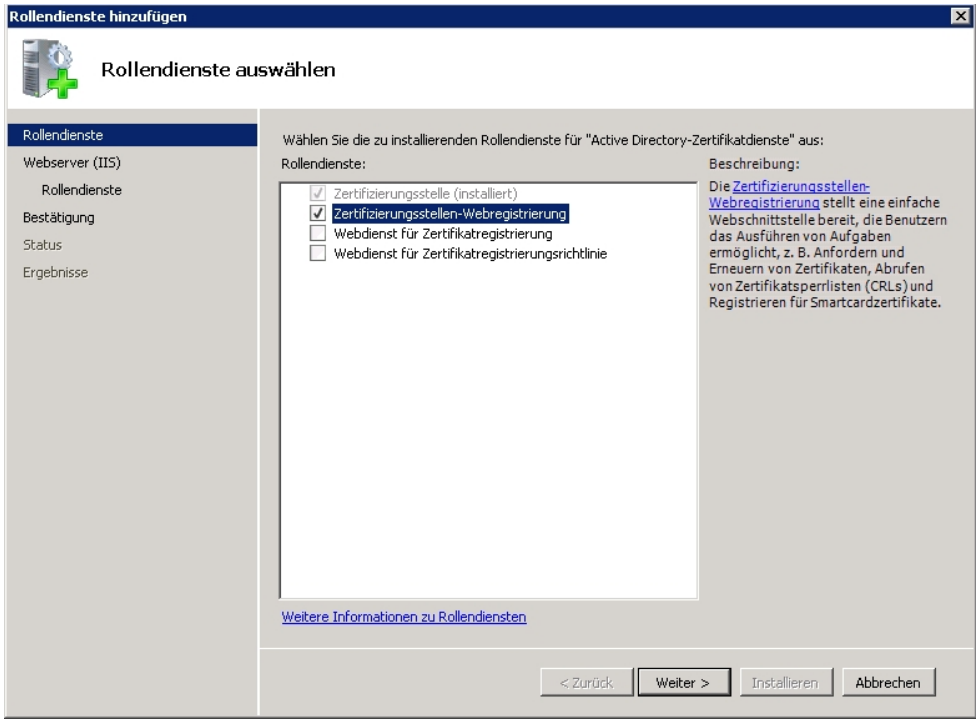
(1) Gehen Sie zu **Assistent "Rollen hinzufügen"** -> **Serverrollen**.

In diesem Workshop werden die *Active Directory-Zertifikatsdienste* des Windows-Servers verwendet.



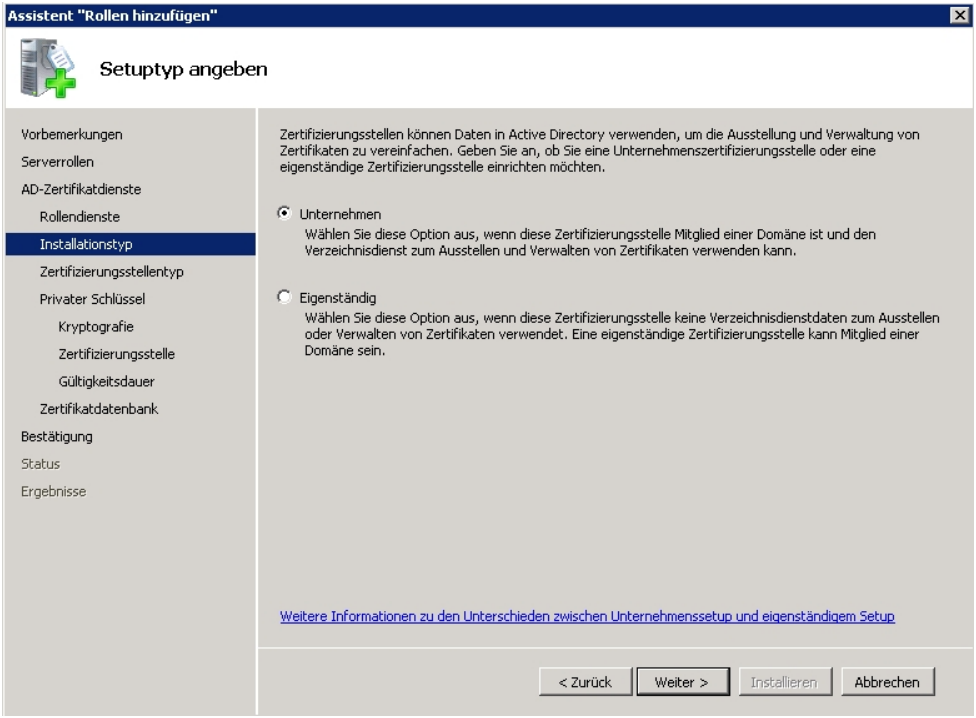
Der Zugriff auf die Zertifikate soll über eine Webschittstelle erfolgen.

Hierzu wird neben der Zertifizierungsstelle selbst der **Rollendienst** *Zertifizierungsstellen-Webregistrierung* installiert.

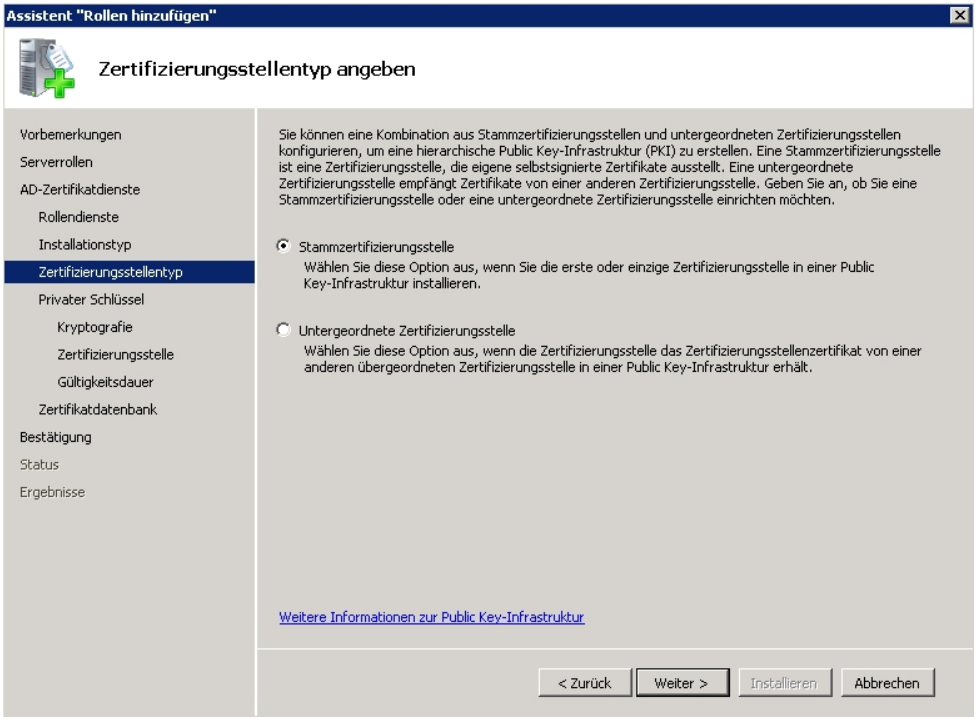


In den nächsten Schritten des Assistenten zum Anlegen der Serverrolle *Active Directory-Zertifikatsdienste* wird der **Installationstyp** der Zertifizierungsstelle gewählt.

Wählen Sie die Option *Unternehmen* aus.

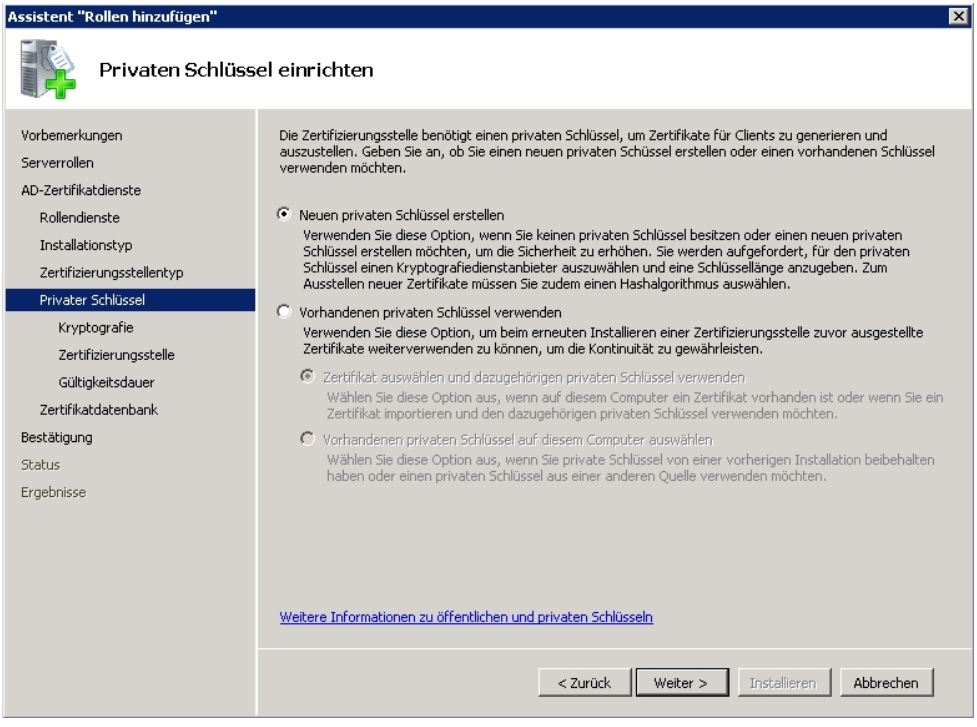


Im Menü **Zertifizierungsstellentyp** wählen Sie die Option *Stammzertifizierungsstelle* aus.

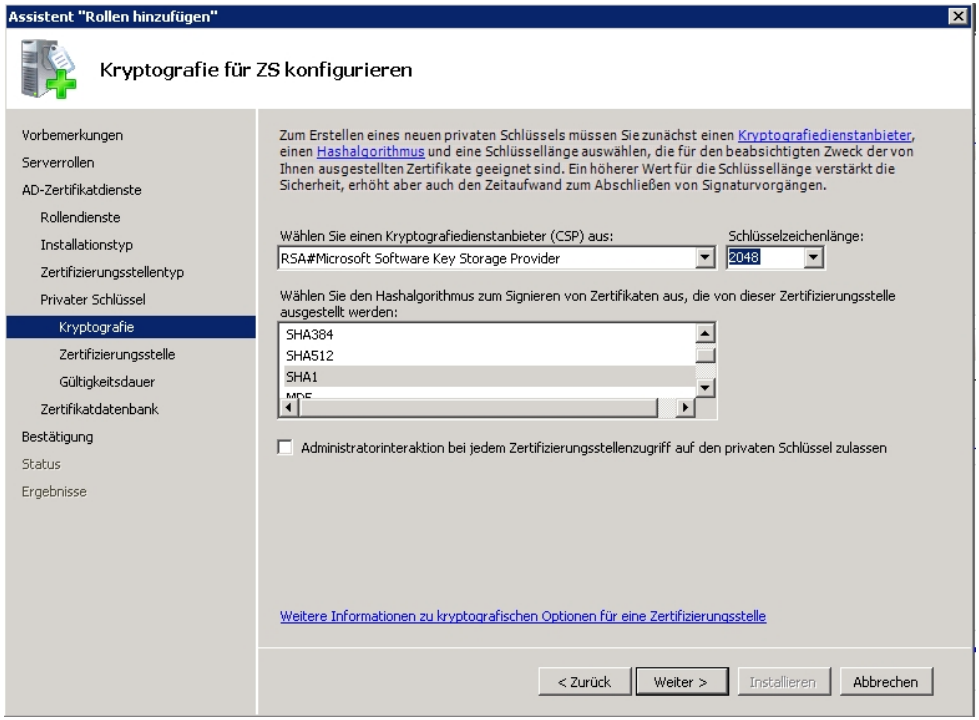


In unserem Beispiel wird bei der Erstinstallation der Zertifizierungsstelle auch ein neuer **Privater Schlüssel** erstellt.

Wählen Sie die Option *Neuen privaten Schlüssel erstellen* aus.



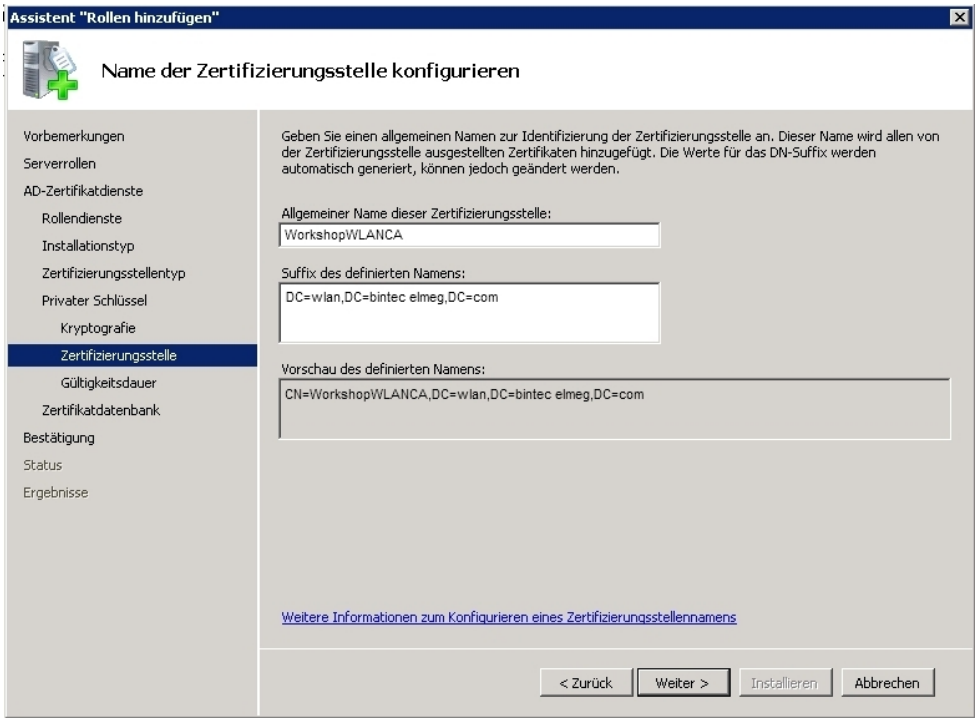
Im Menü **Kryptografie** wählen Sie den Hash Algorythmus *SHA1* und eine **Schlüsselzeichenlänge** von *2048* bit aus.



Im nächsten Schritt wird im Menü **Zertifizierungsstelle** die Bezeichnung des Zertifizierungsstellenzertifikats sowie der Distinguished Name (DN) angegeben.

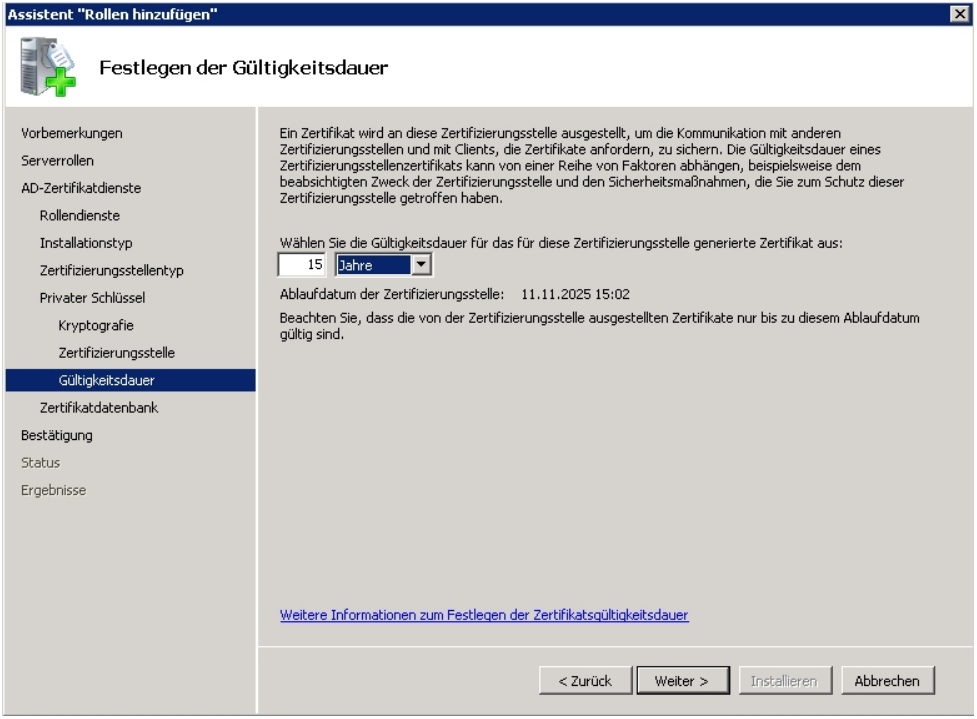
Als **Allgemeiner Name dieser Zertifizierungsstelle** geben Sie z. B. *WorkshopWLANCA* ein.

Als **Suffix des definierten Namens** geben Sie z. B. *DC=wlan,DC=bintec elmeg,DC=com* ein.

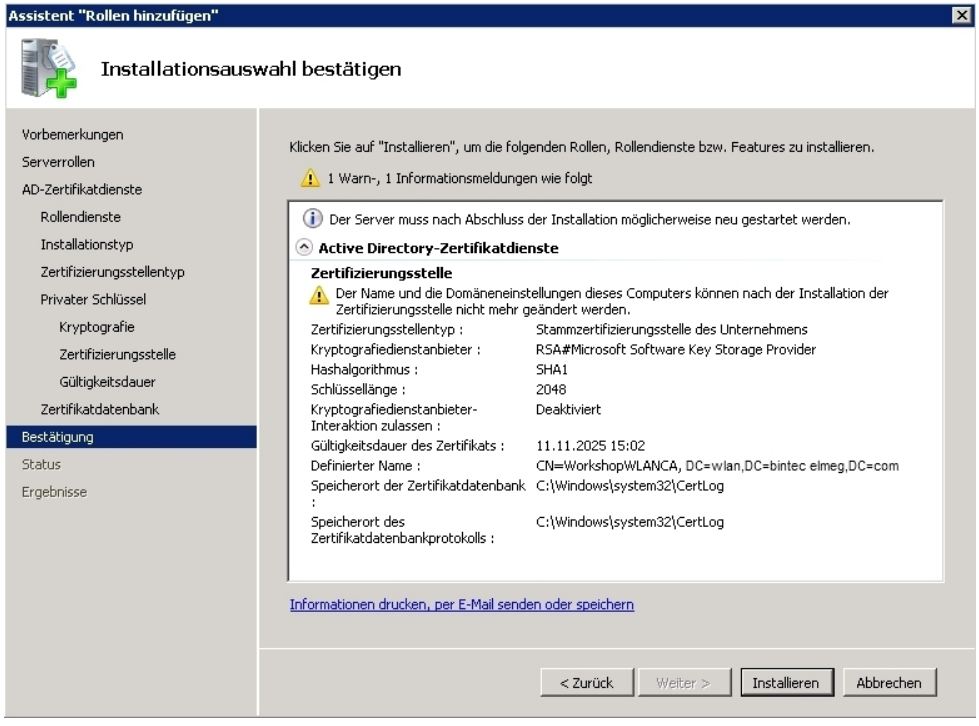


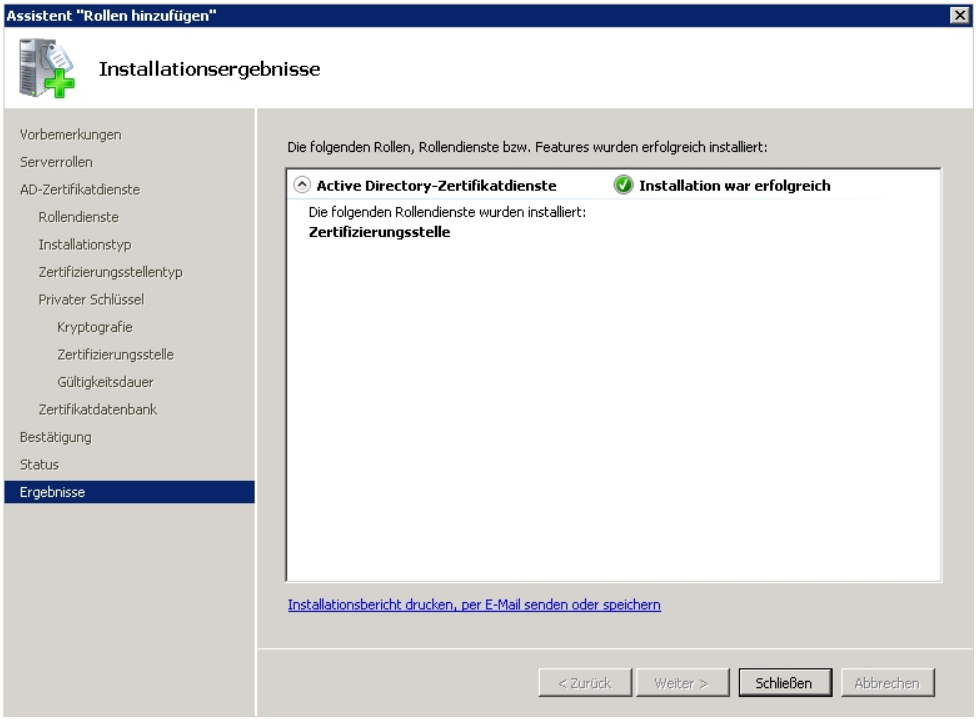
Wählen Sie noch die **Gültigkeitdauer** des Zertifizierungsstellenzertifikats aus.

In unserem Beispiel wird die Gültigkeitsdauer auf *15 Jahre* gesetzt.



Zum Abschluss der Installation der Serverrolle **Active Directory-Zertifikatsdienste** wird eine Zusammenfassung sowie das Ergebnis der Installation angezeigt.


Assistent "Rollen hinzufügen"
Installationsauswahl bestätigen
Vorbemerkungen
Serverrollen
AD-Zertifikatdienste
Rollendienste
Installationstyp
Zertifizierungsstellentyp
Privater Schlüssel
Kryptografie
Zertifizierungsstelle
Gültigkeitsdauer
Zertifikatdatenbank
Bestätigung
Status
Ergebnisse
Klicken Sie auf "Installieren", um die folgenden Rollen, Rollendienste bzw. Features zu installieren.
1 Warn-, 1 Informationsmeldungen wie folgt
Der Server muss nach Abschluss der Installation möglicherweise neu gestartet werden.
Active Directory-Zertifikatdienste
Zertifizierungsstelle
Der Name und die Domäneneinstellungen dieses Computers können nach der Installation der Zertifizierungsstelle nicht mehr geändert werden.
Zertifizierungsstellentyp : Stammzertifizierungsstelle des Unternehmens
Kryptografiedienstanbieter : RSA#Microsoft Software Key Storage Provider
Hashalgorithmus : SHA1
Schlüssellänge : 2048
Kryptografiedienstanbieter-Interaktion zulassen : Deaktiviert
Gültigkeitsdauer des Zertifikats : 11.11.2025 15:02
Definierter Name : CN=WorkshopWLANCA, DC=wlan,DC=bintec elmeg,DC=com
Speicherort der Zertifikatdatenbank : C:\Windows\system32\CertLog
Speicherort des Zertifikatdatenbankprotokolls : C:\Windows\system32\CertLog
Informationen drucken, per E-Mail senden oder speichern
< Zurück
Weiter >
Installieren
Abbrechen

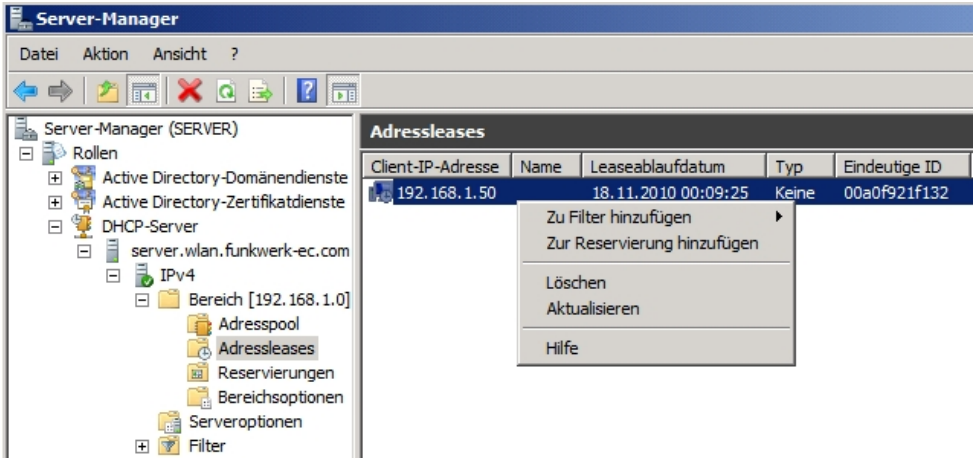


3.2.2 Reservierung der Access Point IP-Adressen am DHCP-Server (Windows Server 2008)

Die verwendeten **bintec** Access Points (z. B. **bintec W2003n**) werden mit dem DHCP-Client Mechanismus in das Netzwerk eingebunden. In diesem Workshop arbeitet der Windows-Server als DHCP-Server und verwaltet unter anderem die IP-Adressen der Access Points. Um zu gewährleisten, dass die Access Points immer unter der selben IP-Adresse erreichbar sind und stets die gleiche IP-Adresse für die RADIUS-Authentifzierung verwenden, werden deren IP-Adressen am DHCP- Server reserviert.

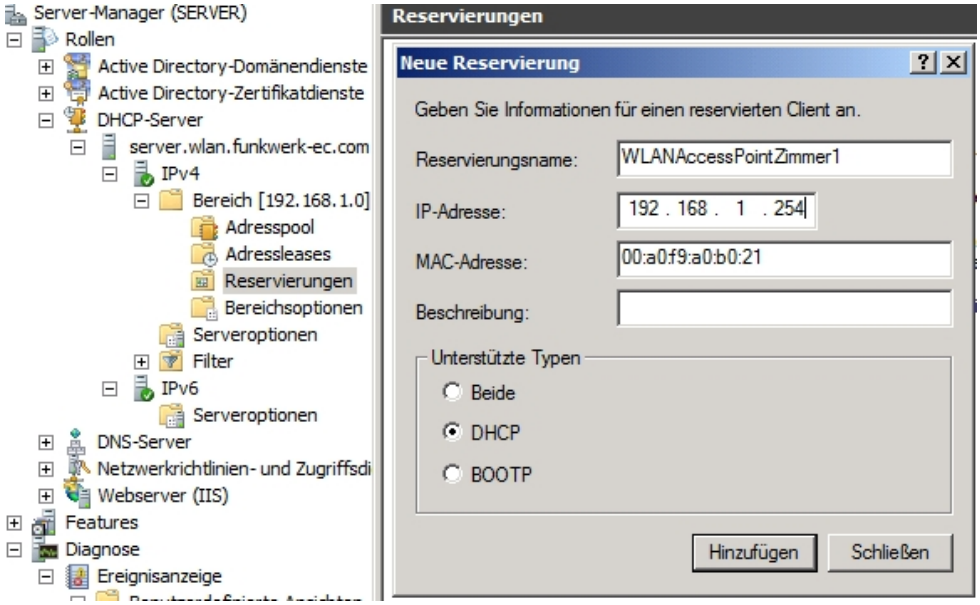
Bereits vergebene IP-Adressen werden im Menü **Adressleases** des Windows 2008 Server-Managers gelistet. Mit Hilfe des Kontext-Menüs können die Adressen der Access Points als **Reservierungen** hinzugefügt werden.

(1) Gehen Sie zu **Server-Manager** -> **DHCP-Server** -> **Adressleases**.



WLAN Access Points ohne aktive **Addressleases** (keine IP-Adresse zugewiesen) können über das Kontext-Menü **Neue Reservierung** angelegt werden. Hierzu muss die Ethernet MAC-Adresse des jeweiligen Access Points hinterlegt werden.

(1) Gehen Sie zu **Server-Manager** -> **DHCP-Server** -> **Reservierungen**.



Gehen Sie folgendermaßen vor, um die Informationen für einen reservierten Client anzugeben:

(1) Als **Reservierungsname** geben Sie z. B. *WLANAccessPointZimmer1* ein.

(2) Geben Sie die **IP-Adresse** z. B. *192.168.1.254* ein.

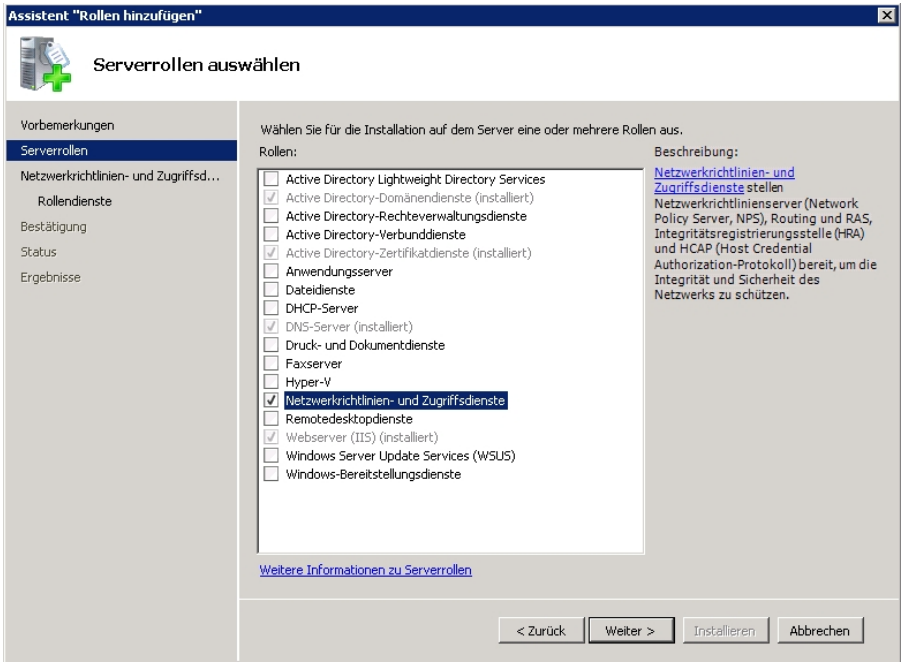
(3) Bei **MAC-Adresse** geben Sie z. B. *00:a0:f9:a0:b0:21* ein.

3.2.3 Installation der Netzwerkrichtlinien- und Zugriffsdienste (NPS / RADIUS-Server)

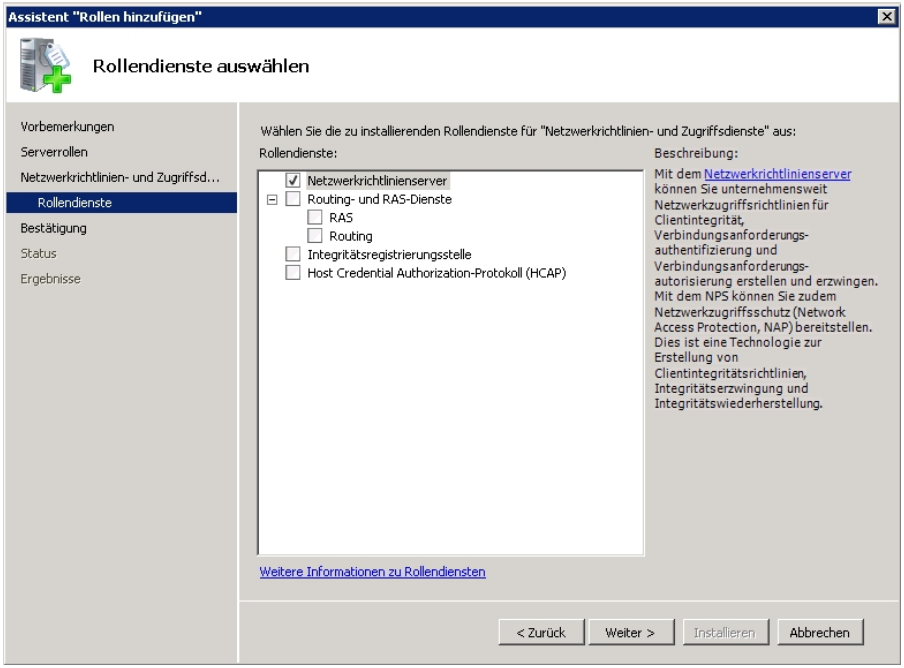
Mit der Installation der *Netzwerkrichtlinien- und Zugriffsdienste (NPS)* wird der RADIUS-Server des Windows 2008 Servers installiert. Hierzu wird die Funktion **Rollen Hinzufügen** des Server-Managers verwendet. Gehen Sie folgendermaßen vor:

(1) Gehen Sie zu **Assistent "Rollen hinzufügen"** -> **Serverrollen**.

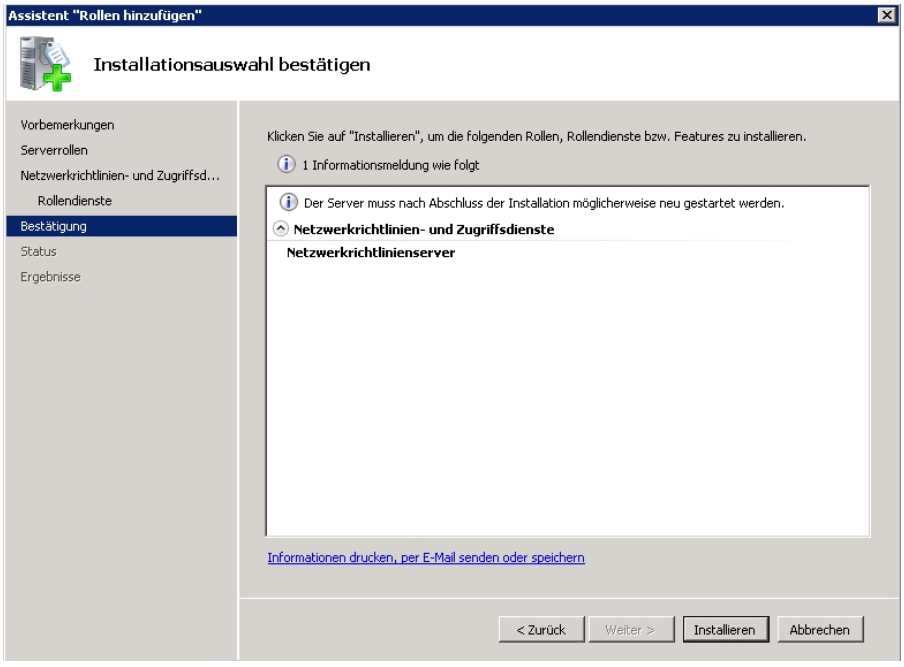
(2) Wählen Sie die Option *Netzwerkrichtlinien- und Zugriffsdienste* aus.



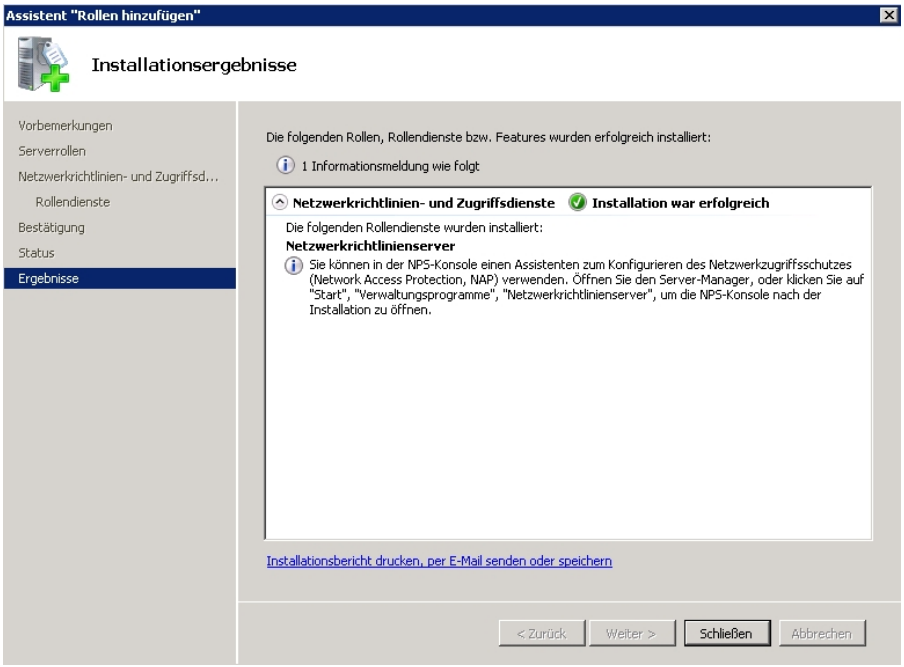
(3) Gehen Sie zu **Rollendienste**.
Aktivieren Sie die Option *Netzwerkrichtlinienserver*.



(4) Klicken Sie auf **Installieren**. Die Rollen werden installiert.



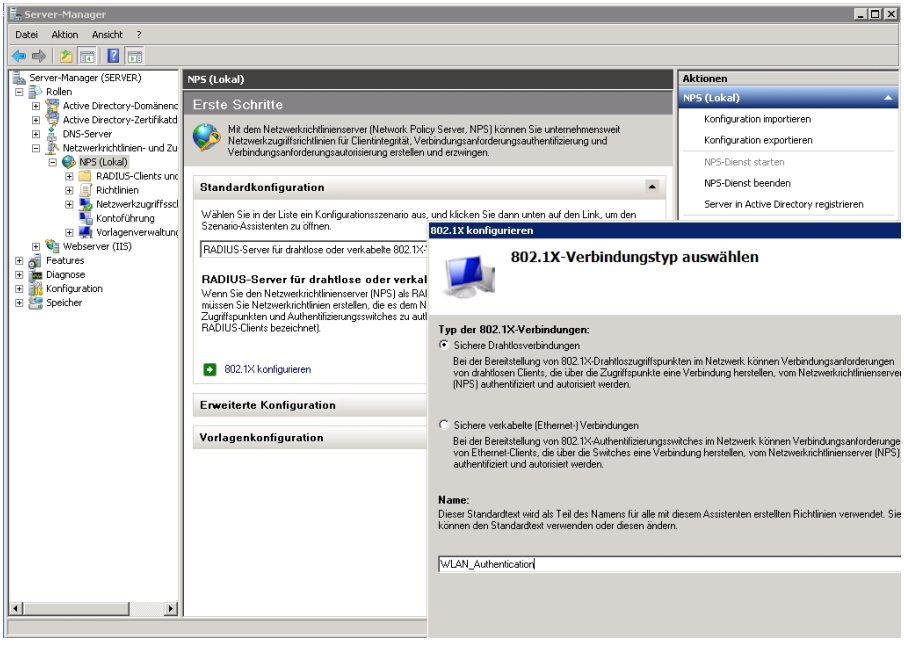
(5) Unter **Ergebnisse** sehen Sie, ob die Rollen erfolgreich installiert wurden.



3.2.4 Konfiguration der Netzwerkrichtlinien- und Zugriffsdienste (NPS / RADIUS-Server)

Der RADIUS-Server für die 802.1x WLAN-Authentifzierung wird im Menü **Network Policy Servers (NPS)** konfiguriert.

(1) Gehen Sie zu **Server-Manager** -> **Netzwerkrichtlinien- und Zugriffsdienste (NPS)** -> **NPS (Lokal)**.

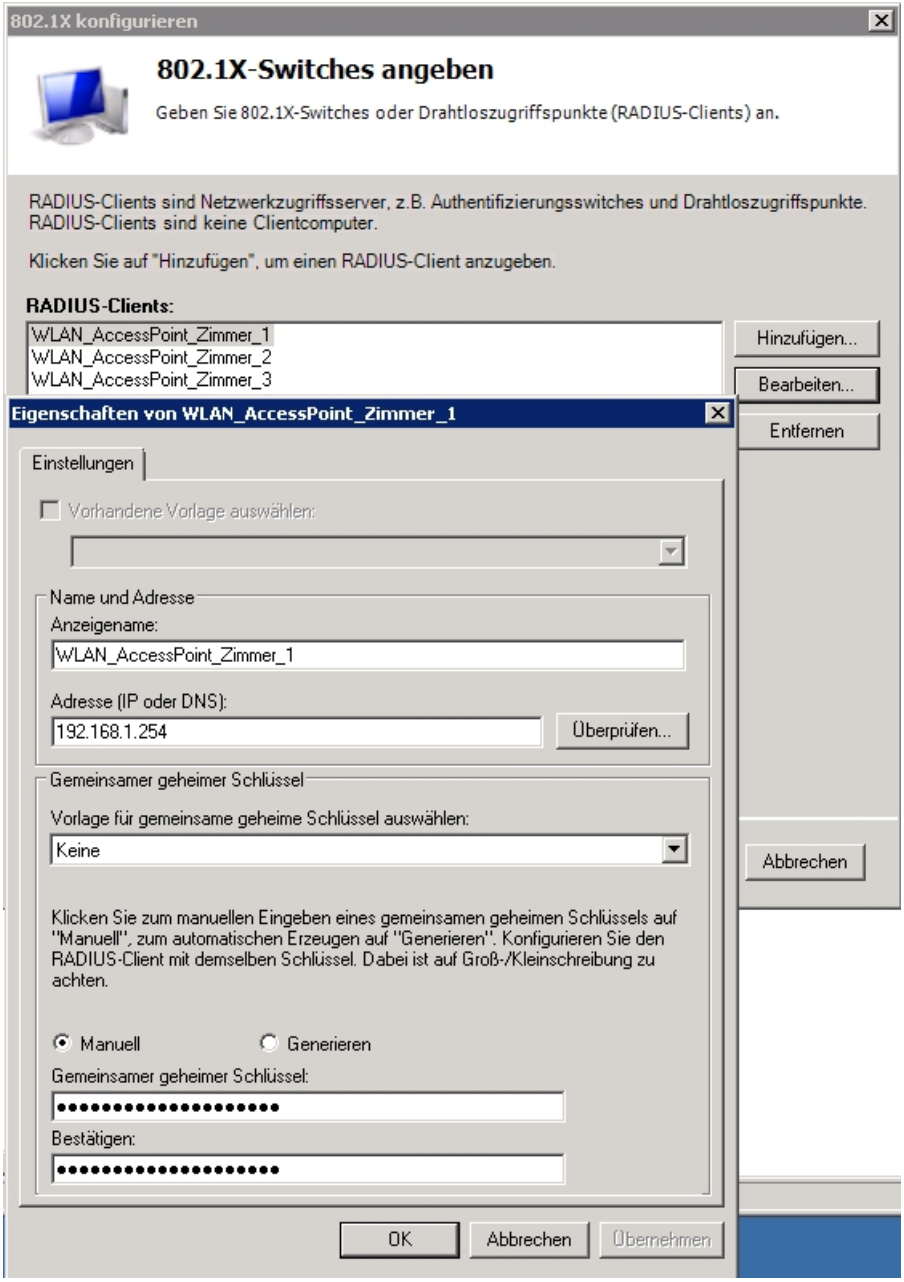


(2) Wählen Sie ein Konfigurationsszenario aus.

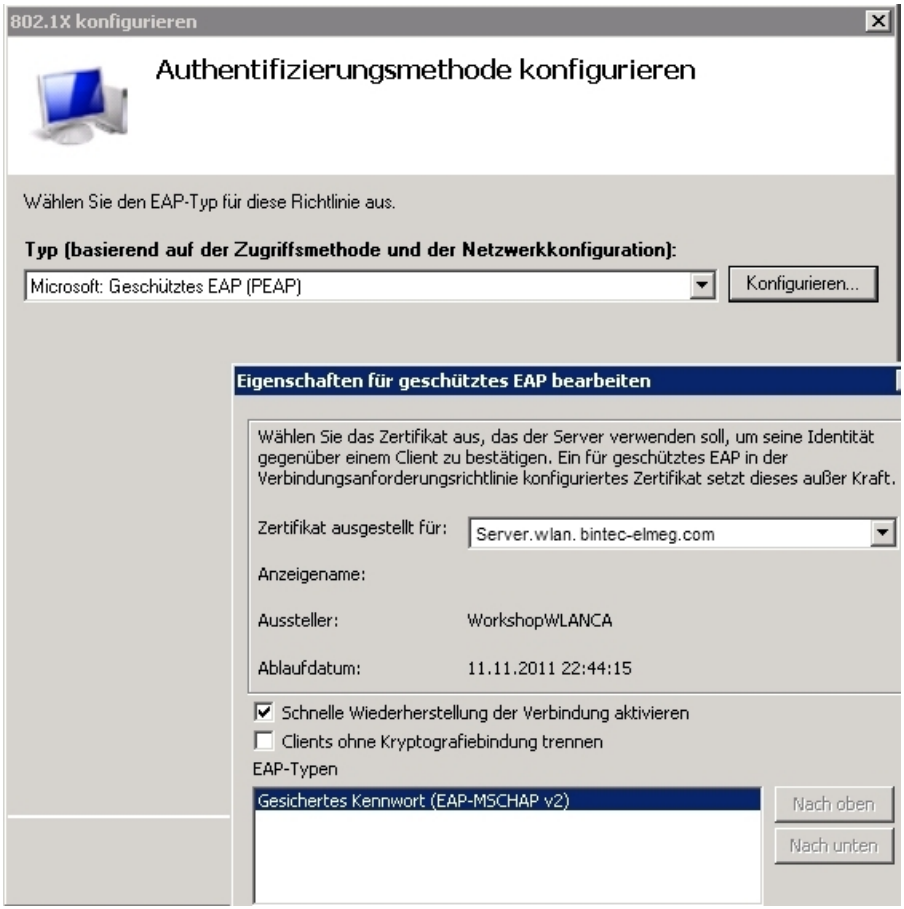
(3) Klicken Sie auf den Link **802.1X konfigurieren**, um den Szenario-Assistenten zu öffnen.

(4) Im ersten Schritt wird der **Typ der 802.1x-Verbindungen** *Sichere Drahtlosverbindungen* gewählt und ein **Name** vergeben, z. B. *WLAN_Authentication*.

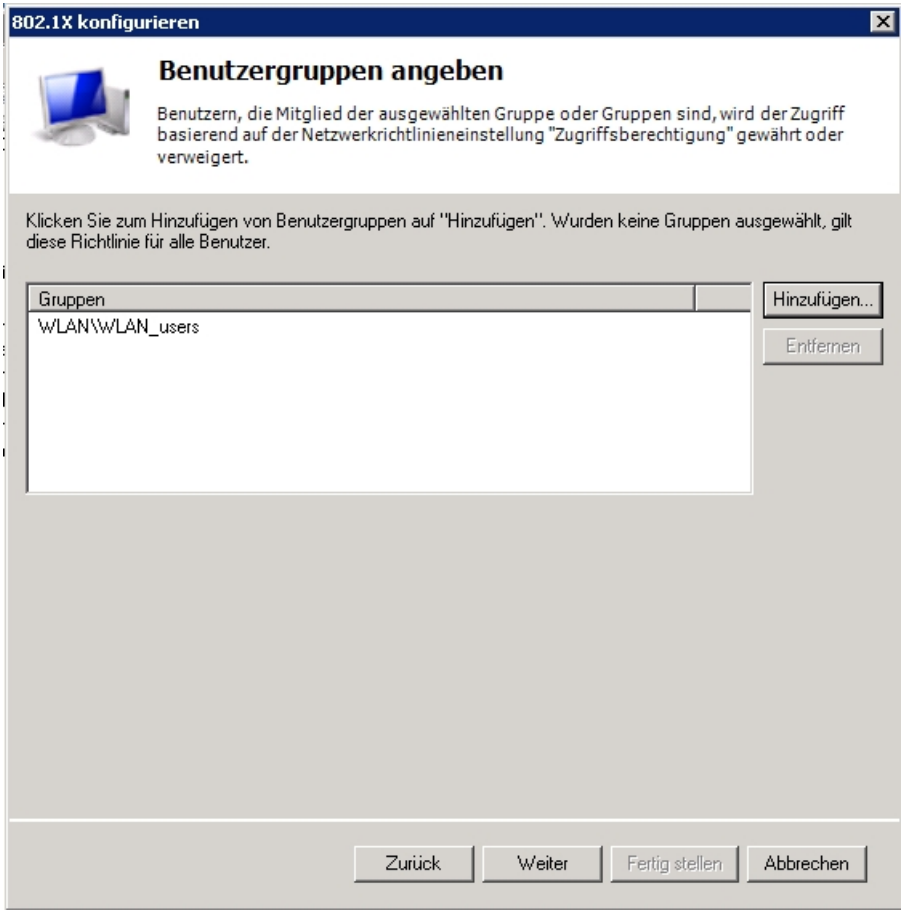
(5) Im zweiten Schritt des Assistenten werden alle Access Points als RADIUS-Client konfiguriert. Die Access Points senden bei der Anmeldung eines WLAN-Clients Authentifizierungsanfragen an den RADIUS-Server (Netzwerkrichtlinien- und Zugriffsdienste, NPS). Beim Anlegen der RADIUS-Clients (Access Points) wird deren IP-Adresse und ein Passwort zum Schutz der RADIUS-Authentifizierung vergeben.



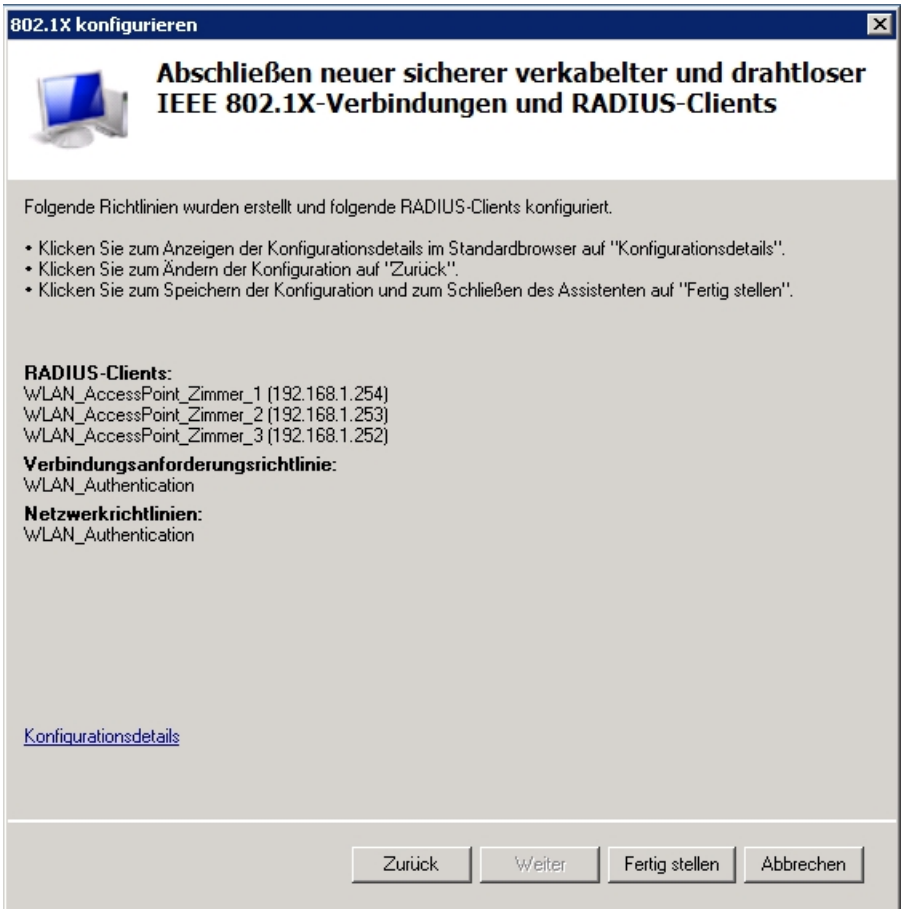
(6) Anschließend wird der **EAP-Typ** (Extensible Authentication Protocol) zur Authentifizierung der WLAN-Clients gewählt. In diesem Workshop wird *EAP-PEAP* verwendet. Im Konfigurationsdialog der EAP-PEAP Option muss das Serverzertifkat zur Identifikation gegenüber dem WLAN-Client gewählt werden.



(7) Im nächsten Schritt kann der WLAN-Zugriff auf einzelne Benutzergruppen beschränkt werden. In diesem Workshop wird den Mitgliedern der Benutzergruppe **WLAN** der Zugriff ermöglicht.



(8) Zum Abschluss des Assistenten wird eine Zusammenfassung angezeigt und die Konfiguration des Network Policy Servers (NPS) erstellt.



3.3 RADIUS-Konfiguration des Access Points

Bei der Anmeldung eines WLAN-Clients leitet der Access Point die Authentifizierungsanfrage in Form einer RADIUS-Anfrage an den RADIUS-Server (Windows 2008 NPS) weiter. Der RADIUS-Server wird am **bintec** Access Point mit Hilfe des **GUI** konfiguriert.

(1) Gehen Sie zu **Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**.

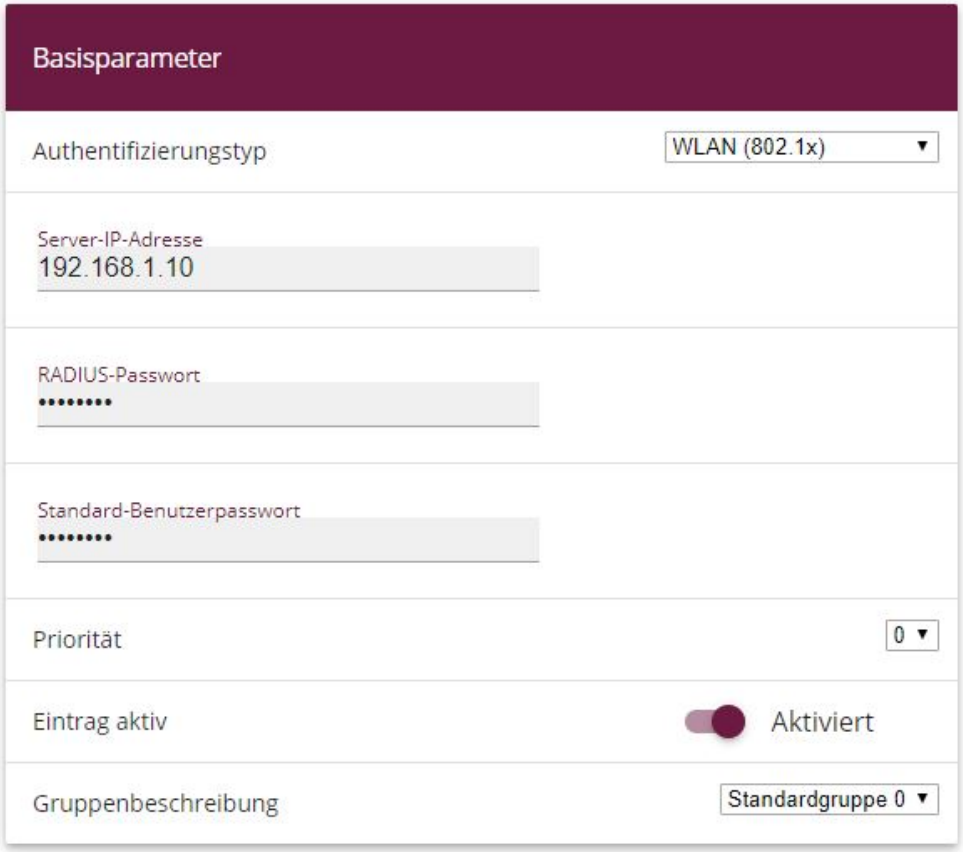


Abb. 54: **Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**

Gehen Sie folgendermaßen vor, um den RADIUS-Server zu konfigurieren:

(1) Um den Zugang zu einem WLAN-Netzwerk zu regeln, ist es notwendig, den **Authentifizierungstyp** auf den Wert *WLAN (802.1x)* zu setzen.

(2) Tragen Sie die **IP-Adresse** des Windows 2008 Servers ein, z. B. *192.168.1.10*.

(3) Die Kommunikation mit dem RADIUS-Server wird mit einem **RADIUS-Passwort** geschützt. Bitte verwenden Sie hier das am RADIUS-Server hinterlegte Kennwort.

(4) Bestätigen Sie Ihre Angaben mit **OK**.

3.4 WLAN-Konfiguration des Access Points

Die Einstellungen des WLAN-Funkmoduls können nach Bedarf gesetzt werden. In unserem Beispiel wird das 2.4 GHz Band mit automatischer Kanalwahl verwendet.

(1) Gehen Sie zu **Wireless LAN** -> **WLAN** -> **Einstellungen Funkmodul** -> .

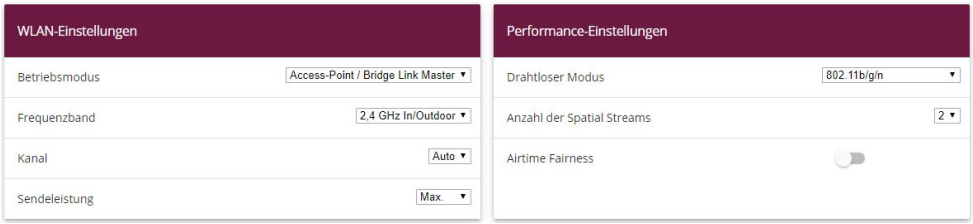


Abb. 55: **Wireless LAN** -> **WLAN** -> **Einstellungen Funkmodul** ->

Gehen Sie folgendermaßen vor, um den Access Point zu konfigurieren:

(1) Wählen Sie den **Betriebsmodus** *Access-Point / Bridge Link Master* aus.

(2) Als **Frequenzband** wählen Sie *2.4 GHz In/Outdoor* aus.

(3) Den **Kanal** setzen Sie auf *Auto*.

(4) Belassen Sie die restlichen Einstellungen und bestätigen Sie mit **OK**.

Mit der Konfiguration der Drahtlosnetzwerke (VSS) werden die Authentifizierungsanfragen eines WLAN-Clients an den konfigurierten RADIUS-Server weitergeleitet.

(1) Gehen Sie zu **Wireless LAN** -> **WLAN** -> **Drahtlosnetzwerke (VSS)** -> **Neu**.

Abb. 56: **Wireless LAN** -> **WLAN** -> **Drahtlosnetzwerke (VSS)** -> **Neu**

Gehen Sie folgendermaßen vor, um die Drahtlosnetzwerke zu konfigurieren:

(1) Geben Sie den **Netzwerknamen (SSID)** ein, z. B. *workshop*.

(2) Als **Sicherheitsmodus** muss der Sicherheitsmodus *WPA-Enterprise* verwendet werden.

(3) Als **WPA-Modus** wählen Sie *WPA und WPA2* aus.

(4) Bei **WPA Cipher** wählen Sie die Verschlüsselung *AES und TKIP* aus.

(5) Bei **WPA2 Cipher** wählen Sie die Verschlüsselung *AES und TKIP* aus.

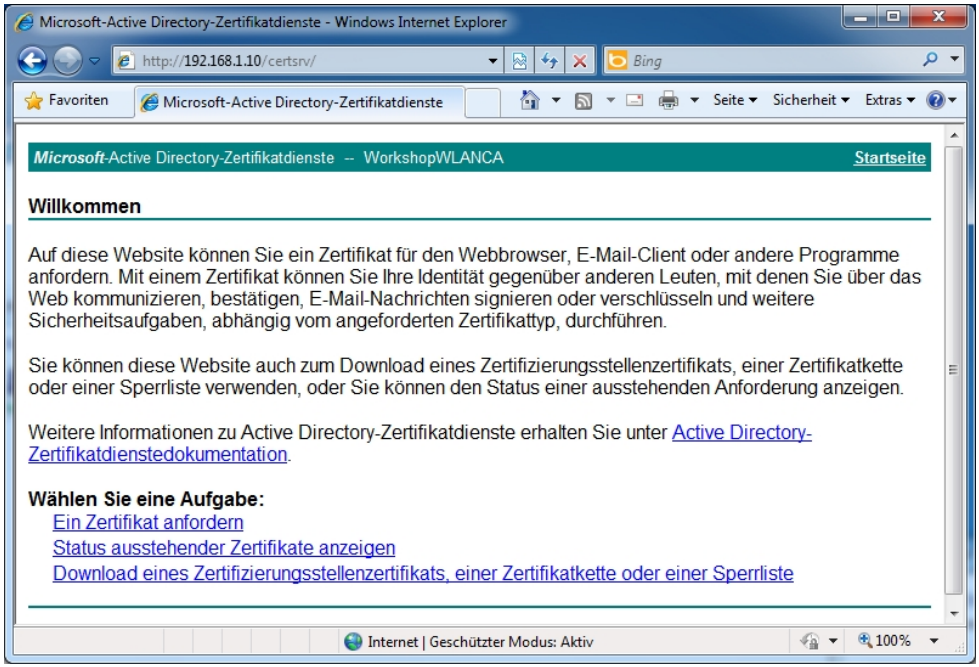
(6) Belassen SIe die restlichen Einstellungen und bestätigen Sie mit **OK**.

3.5 Anbindung eines Windows 7 WLAN-Clients

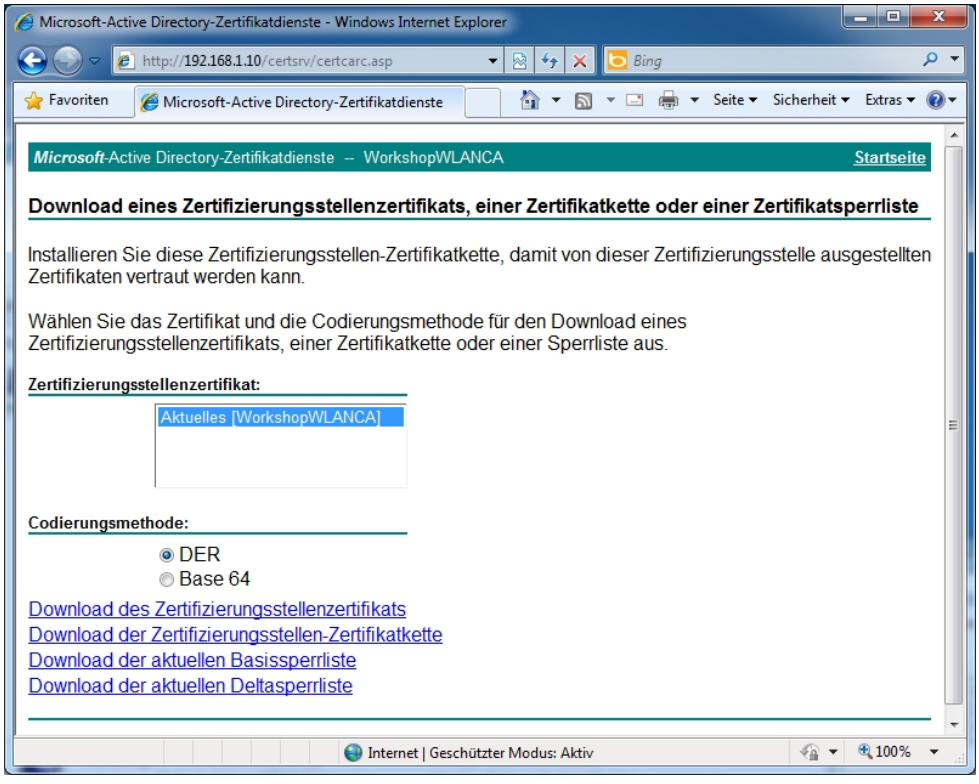
3.5.1 Importieren des Zertifikats der Zertifizierungsstelle (CA Zertifikat)

Bei der gewählten Authentifizierungsmethode *802.1x / EAP-PEAP* wird zur Übertragung der Logininformationen eine gesicherte Transportverbindung hergestellt. Um sicherzustellen, dass dieser Tunnel zur richtigen Gegenstelle aufgebaut wird, identifiziert der WLAN-Client den Server mit Hilfe des ausgestellten Zertifikats. Deshalb muss das Zertifikat der Zertifizierungsstelle auf jedem WLAN-Client installiert werden.

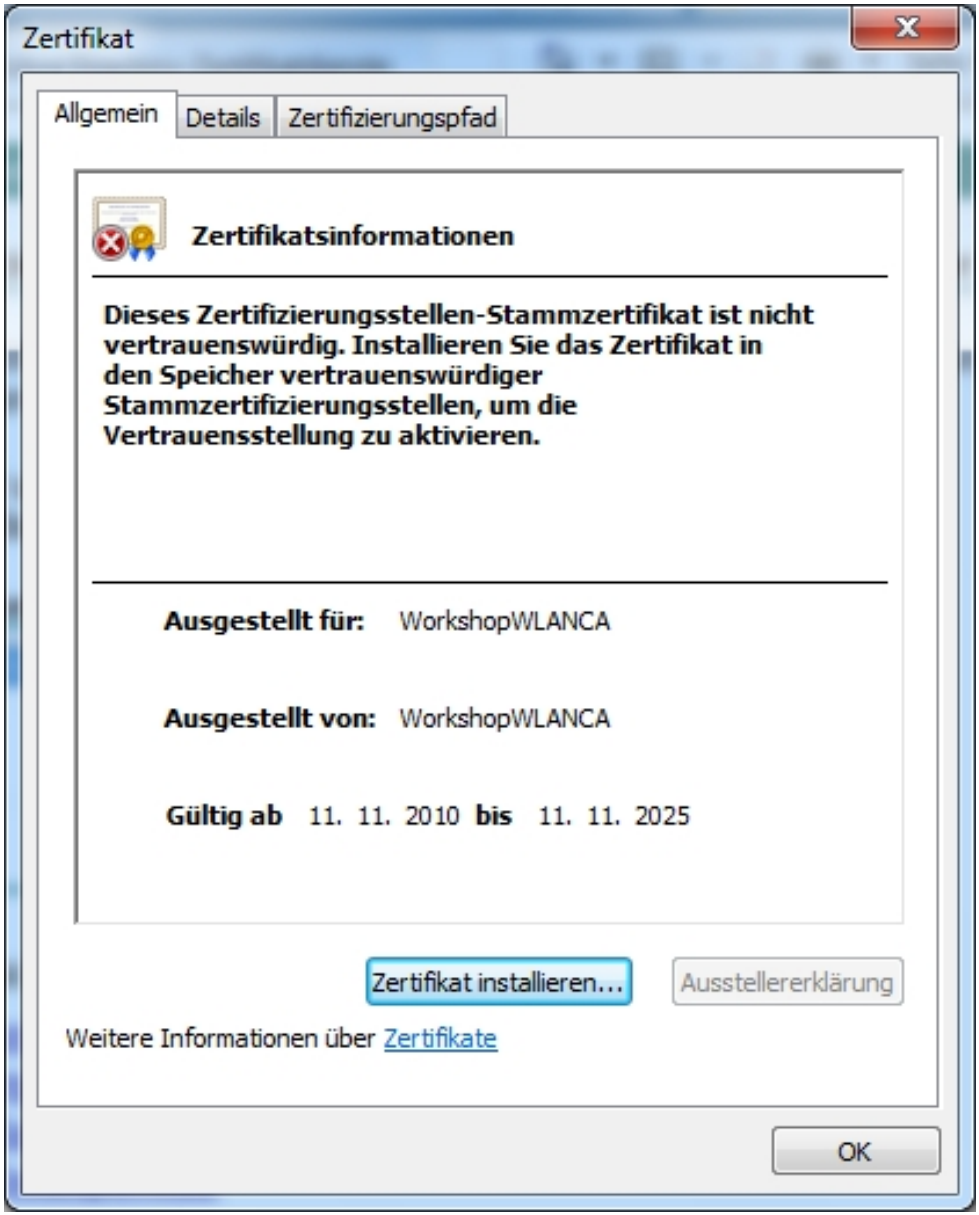
In diesem Workshop wird die Web-Schnittstelle des Zertifkatsservers zur Installation des Zertifizierungstellenzertifikats (CA Zertifikat) verwendet. Hierzu wird das anzubindende Notebook zunächst per Ethernet mit dem Netzwerk des Windows-Servers verbunden. Die Webschnittstelle des Zertifikatsservers ist über folgende URL erreichbar "http://SERVER_IP_Adresse/certsrv/" (z. B. http://192.168.1.10/certsrv/).



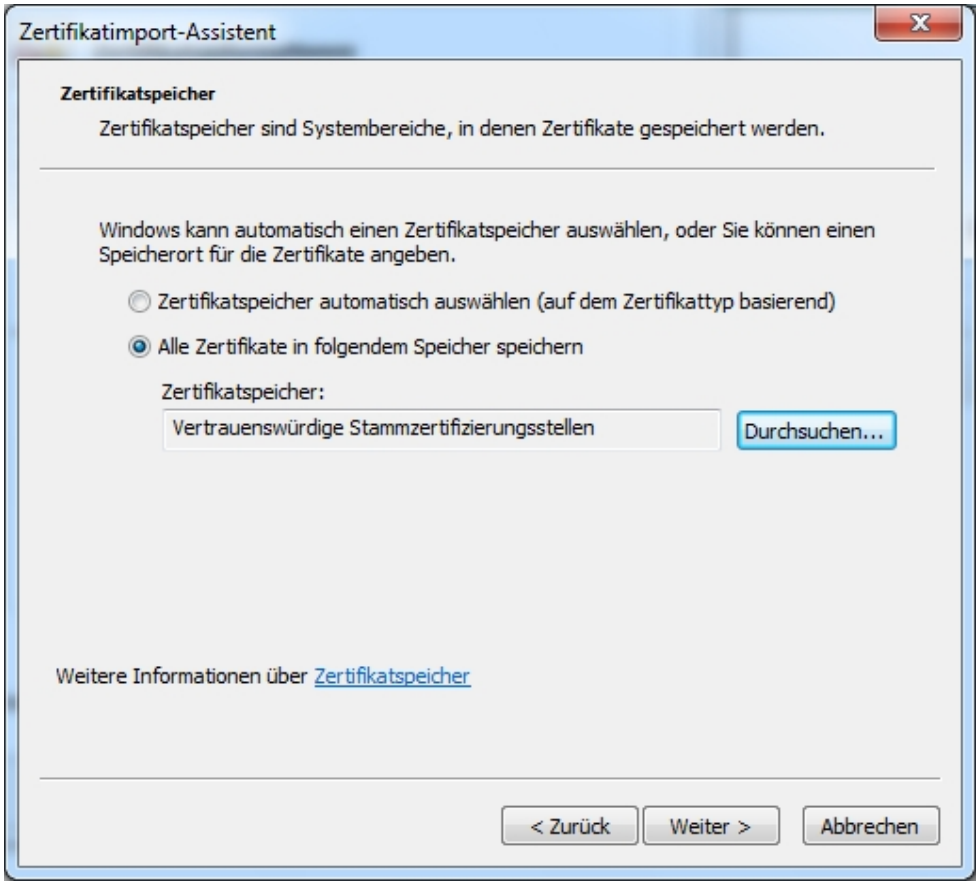
Mit der Option **Download eines Zertifizierungsstellenzertifikats** kann das Root-Zertifikat auf das Notebook (WLAN-Client) übertragen werden.



Anschließend wird das Zertifikat installiert.

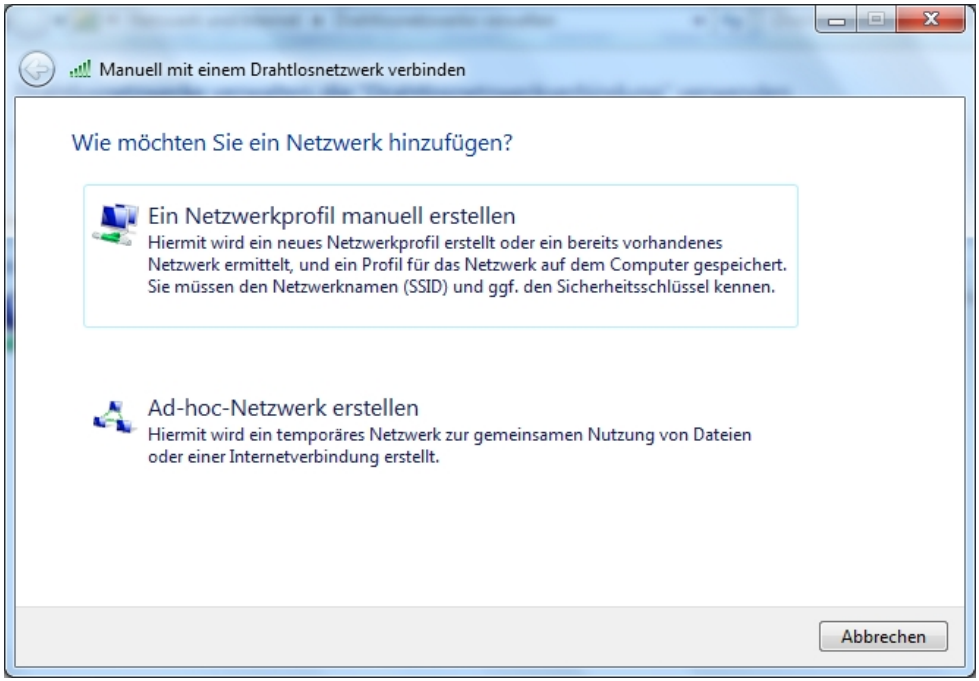


Wählen Sie den Speicherort des Zertifikats manuell aus.

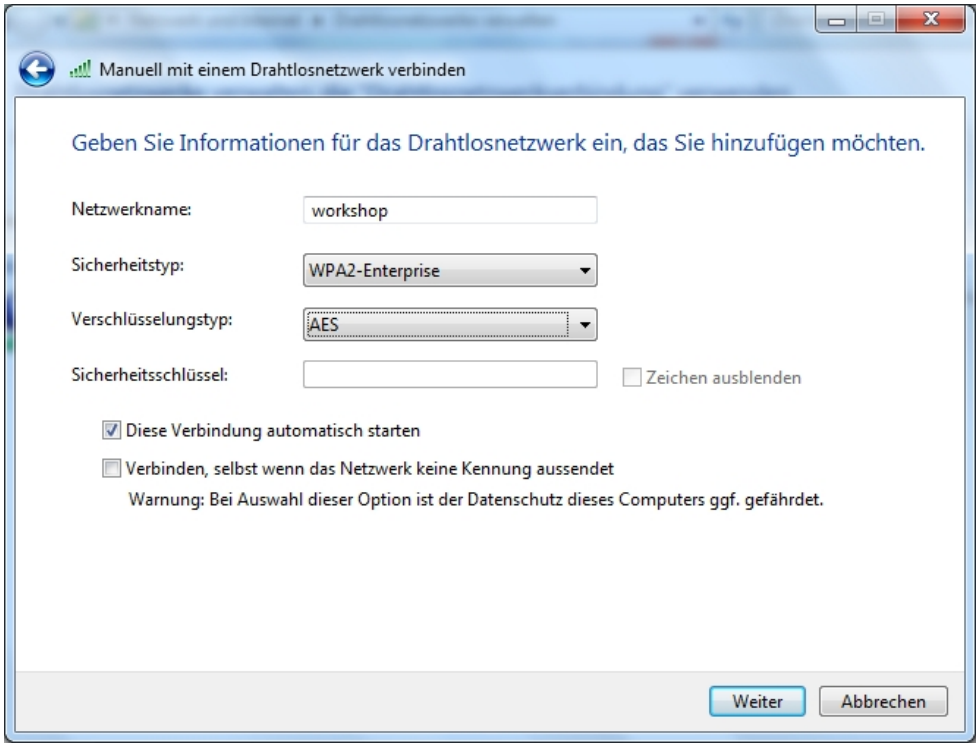


3.5.2 Konfiguration des Windows 7 WLAN Clients

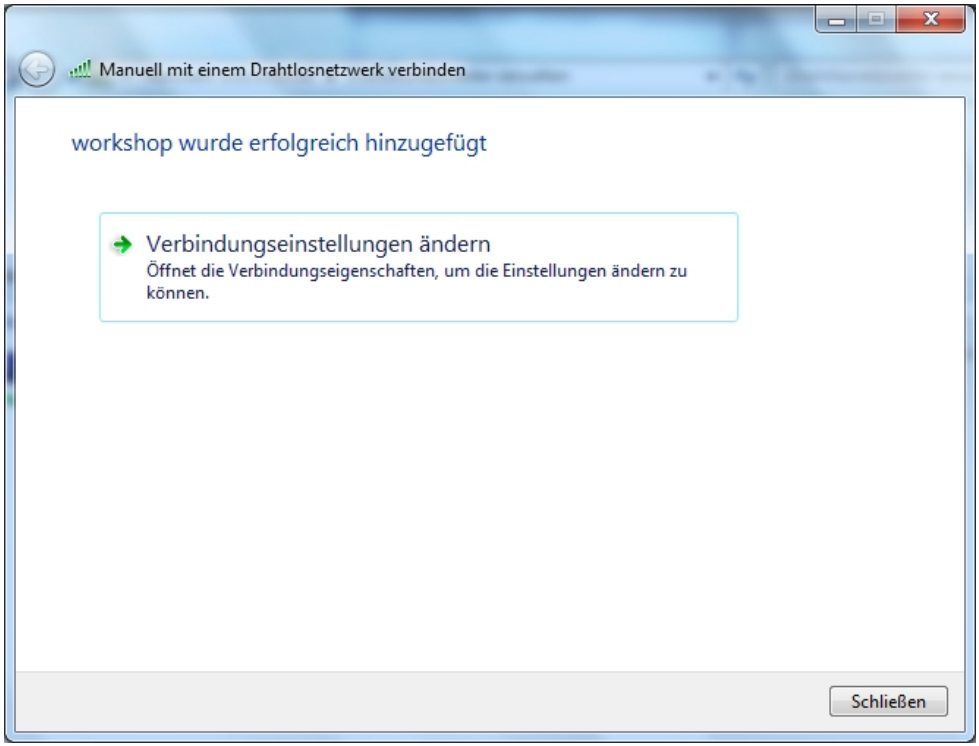
Die WLAN-Konfiguration wird am Beispiel eines Windows 7 Clients gezeigt. Dabei wird mit Hilfe des Dialogs **Drahtlosnetzwerke Verwalten** eine neue Drahtlosverbindung hinzugefügt.



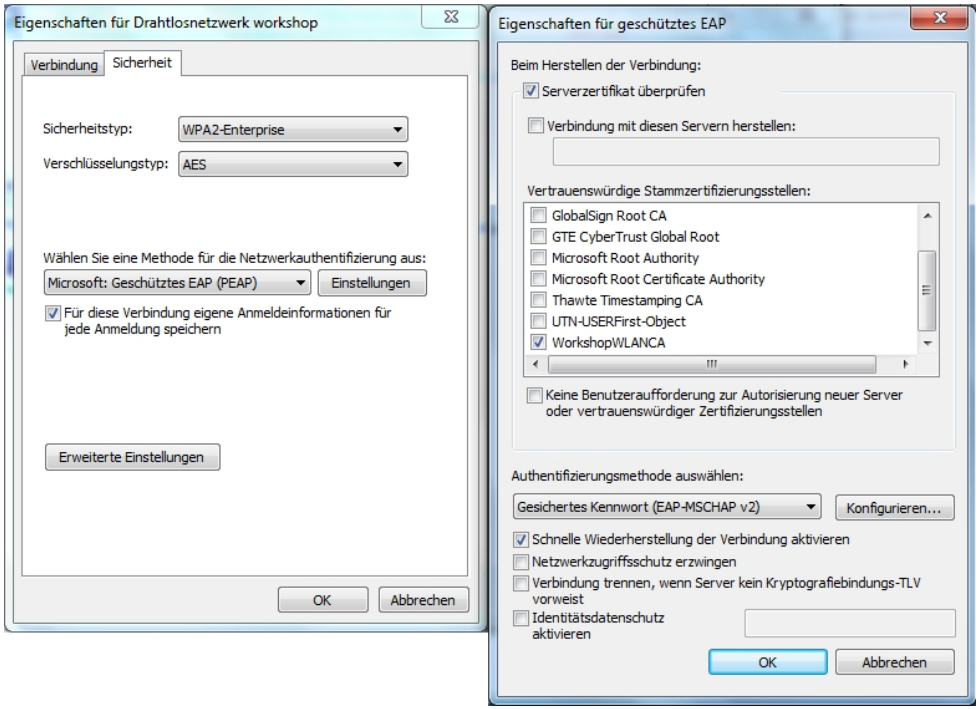
Der **Netzwerkname** sowie der **Sicherheitstyp** und der **Verschlüsselungstyp** werden im Assistenten manuell hinterlegt.



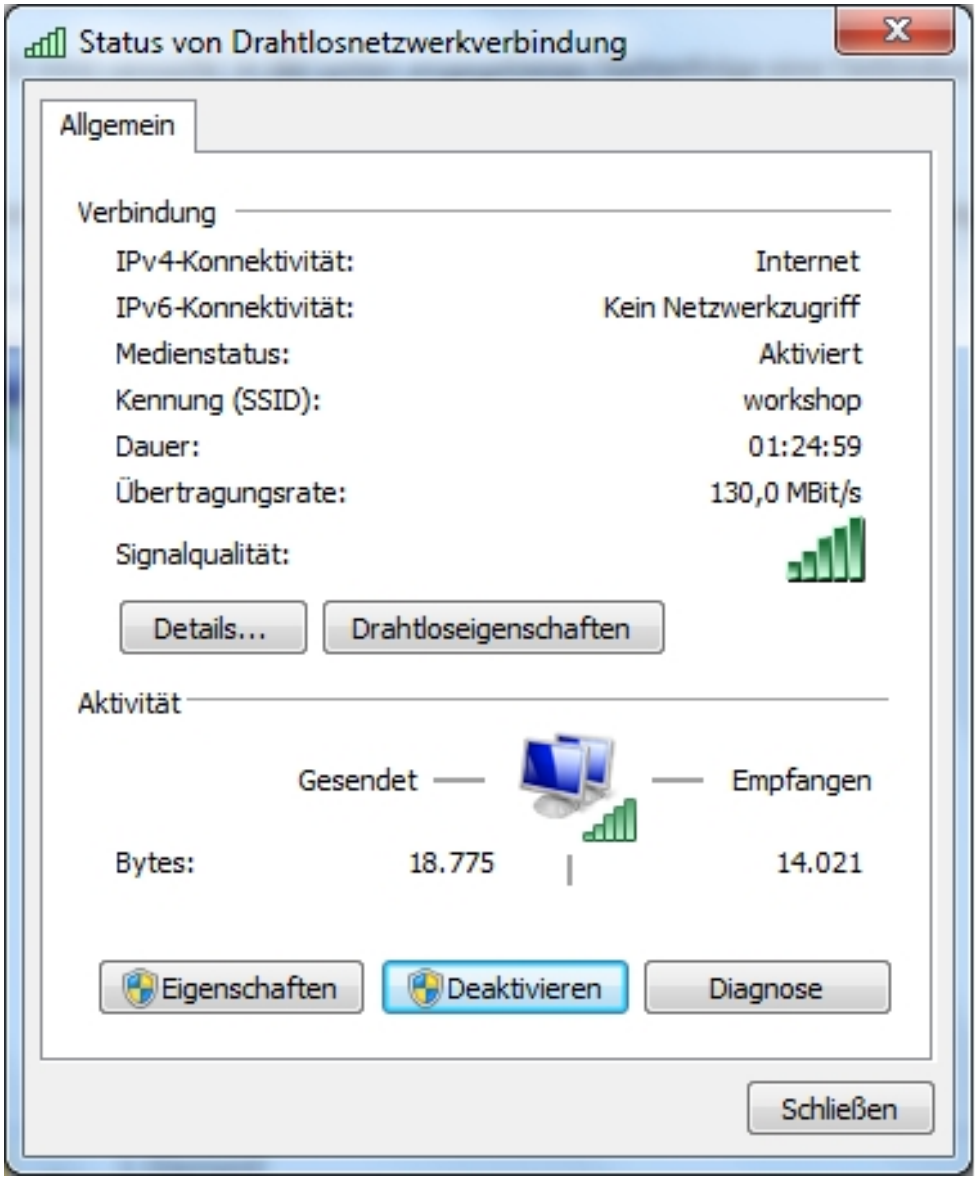
Nachdem die neue Verbindung mit Hilfe des Assistenten hinzugefügt wurde, müssen die Verbindungseinstellungen weiter angepasst werden.



Dabei wird in den Einstellungen der Sicherheitsmethode *Geschütztes EAP(PEAP)* das bereits installierte Zertifikat der Zertifizierungsstelle als vertrauenswürdiges Zertifikat ausgewählt. Mit diesem Konfigurationsschritt wird der Windows 2008 RADIUS-Server als Vertrauenswürdige Gegenstelle definiert.



Beim Aufbau der WLAN-Verbindung wird mit Hilfe des erstellten Zertifikates eine gesicherte Verbindung zwischen dem WLAN-Client und dem Windows 2008-Server hergestellt. Über diese Verbindung werden die Windows Anmeldedaten (Benutzer- oder Computerauthentifzierung) zum Microsoft Network Policy Server (RADIUS-Server) übertragen.


Status von Drahtlosnetzwerkverbindung
Allgemein
Verbindung
IPv4-Konnektivität:
Internet
IPv6-Konnektivität:
Kein Netzwerkzugriff
Medienstatus:
Aktiviert
Kennung (SSID):
workshop
Dauer:
01:24:59
Übertragungsrate:
130,0 MBit/s
Signalqualität:
Details...
Drahtloseigenschaften
Aktivität
Gesendet
Empfangen
Bytes:
18.775
14.021
Eigenschaften
Deaktivieren
Diagnose
Schließen

3.6 Konfigurationsschritte im Überblick

Konfiguration der Active Directory-Zertifikatsdienste

Feld	Menü	Wert
Active Directory-Zertifikadtsdienste	**Assistent "Rollen hinzufügen"** -> **Serverrollen**	Aktivieren
Zertifizierungsstellen-Webregistrierung	**Assistent "Rollen hinzufügen"** -> **Rollendienste**	Aktivieren
Unternehmen	**Assistent "Rollen hinzufügen"** -> **Installationstyp**	Aktivieren
Stammzertifizierungsstelle	**Assistent "Rollen hinzufügen"** -> **Zertifizierungsstellentyp**	Aktivieren
Neuen privaten Schlüssel erstellen	**Assistent "Rollen hinzufügen"** -> **Privater Schlüssel**	Aktivieren
Schlüsselzeichenlänge	**Assistent "Rollen hinzufügen"** -> **Kryptografie**	*2048*
Hashalgorithmus	**Assistent "Rollen hinzufügen"** -> **Kryptografie**	*SHA1*
Allgemeiner Name der Zertifizierungsstelle	**Assistent "Rollen hinzufügen"** -> **Zertifizierungsstelle**	z. B. *WorkshopWLANCA*
Suffix des definierten Namen	**Assistent "Rollen hinzufügen"** -> **Zertifizierungsstelle**	z. B. *DC=wlan,DC=bintec elmeg,DC=com*
Gültigkeitsdauer	**Assistent "Rollen hinzufügen"** -> **Gültigkeitsdauer**	*15 Jahre*

Reservierung der Access Point IP-Adressen am DHCP-Server

Feld	Menü	Wert
Adressleases	**Server-Manager** -> **DHCP-Server** -> **Adressleases**	*Zur Reservierung hinzufügen*
Reservierungsname	**Server-Manager** -> **DHCP-Server** -> **Adressleases**	z. B. *WLANAccess-PointZimmer1*
IP-Adresse	**Server-Manager** -> **DHCP-Server** -> **Adressleases**	z. B. *192.168.1.254*
MAC-Adresse	**Server-Manager** -> **DHCP-Server** -> **Adressleases**	z. B. *00:a0:f9:a0:b2:21*

Installation der Netzwerkrichtlinien- und Zugriffsdienste

Feld	Menü	Wert
Netzwerkrichtlinien- und Zugriffsdienste	**Assistent "Rollen hinzufügen"** -> **Serverrollen**	Aktivieren
Netzwerkrichtlinienserver	**Assistent "Rollen hinzufügen"** -> **Rollendienste**	Aktivieren

Konfiguration der Netzwerkrichtlinien- und Zugriffsdienste

Feld	Menü	Wert
802.1X konfigurieren	**Server-Manager** -> **Netzwerkrichtlinien- und Zugriffsdienste (NPS)** -> **NPS (Lokal)**	Starten
Sichere Drahtlosverbindungen	**Server-Manager** -> **Netzwerkrichtlinien- und Zugriffsdienste (NPS)** -> **NPS (Lokal)**	Aktivieren
Name	**Server-Manager** -> **Netzwerkrichtlinien- und Zugriffsdienste (NPS)** -> **NPS (Lokal)**	z. B. *WLAN_Authentication*
Anzeigename	**802.1X konfigurieren** -> **802.1X-Switches angeben**	z. B. *WLAN_AccessPoint_Zimmer_1*
Adresse (IP oder DNS)	**802.1X konfigurieren** -> **802.1X-Switches angeben**	z. B. *192.168.1.254*
Gemeinsamer geheimer Schlüssel	**802.1X konfigurieren** -> **802.1X-Switches angeben**	z. B. *supersecret*
Typ	**802.1X konfigurieren** -> **Authentifizierungsmethode konfigurieren**	*Microsoft:Geschütztes EAP (PEAP)*
Zertifikat ausgestellt für:	**802.1X konfigurieren** -> **Authentifizierungsmethode konfigurieren**	*Server.wlan.bintec-elmeg.com*
WLAN\WLAN_users	**802.1X konfigurieren** -> **Benutzergruppen angeben**	Hinzufügen

Radius Konfiguration des Access Points

Feld	Menü	Wert
Authentifizierungstyp	**Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**	WLAN (802.1x)
Server-IP-Adresse	**Systemverwaltung** -> **Remote Au-**	z. B. *192.168.1.10*

Feld	Menü	Wert
	thentifizierung -> RADIUS -> Neu	
RADIUS-Passwort	**Systemverwaltung -> Remote Authentifizierung -> RADIUS -> Neu**	z. B. *supersecret*

WLAN-Konfiguration des Access Points

Feld	Menü	Wert
Betriebsmodus	**Wireless LAN -> WLAN -> Einstellungen Funkmodul ->**	*Access-Point / Bridge Link Master*
Frequenzband	**Wireless LAN -> WLAN -> Einstellungen Funkmodul ->**	*2.4GHz In/Outdoor*
Kanal	**Wireless LAN -> WLAN -> Einstellungen Funkmodul ->**	*Auto*
Netzwerkname (SSID)	**Wireless LAN -> WLAN -> Drahtlosnetzwerke (VSS) -> Neu**	z. B. *workshop*
Sicherheitsmodus	**Wireless LAN -> WLAN -> Drahtlosnetzwerke (VSS) -> Neu**	*WPA-Enterprise*
WPA-Modus	**Wireless LAN -> WLAN -> Drahtlosnetzwerke (VSS) -> Neu**	*WPA und WPA2*
WPA Cipher	**Wireless LAN -> WLAN -> Drahtlosnetzwerke (VSS) -> Neu**	*AES und TKIP*
WPA2 Cipher	**Wireless LAN -> WLAN -> Drahtlosnetzwerke (VSS) -> Neu**	*AES und TKIP*

Anbindung eines Windows 7 WLAN-Clients

Feld	Menü	Wert
Download eines Zertifizierungsstellenzertifikats	**Explorer 192.168.1.10**	Aktivieren
Zertifizierungsstellenzertifikat	**Explorer 192.168.1.10**	*Aktuelles (WorkshopWLANCA)*
Zertifikat	**Explorer 192.168.1.10**	Zertifikat installieren
Zertifikatspeicher	**Explorer 192.168.1.10**	Alle Zertifikate in folgendem Speicher speichern

Konfiguration des Windows 7 WLAN-Clients

Feld	Menü	Wert
Drahtlosverbindung	**Drahtlosnetzwerke verwalten**	Hinzufügen
Netzwerkname	**Drahtlosnetzwerke verwalten**	z. B. *workshop*

Feld	Menü	Wert
Sicherheitstyp	**Drahtlosnetzwerke verwalten**	*WPA2-Enterprise*
Verschlüsselungstyp	**Drahtlosnetzwerke verwalten**	*AES*
Verbindungseinstellungen ändern	**Drahtlosnetzwerke verwalten**	Aktivieren
Authentifizierungsmethode auswählen	**Drahtlosnetzwerke verwalten**	Gesichertes Kennwort (EAP-MSCHAP v2)

Kapitel 4 WLAN - Einführung in den bintec-WLAN-Controller

4.1 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

4.2 Projektplanung

4.2.1 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 2,4 GHz-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 stattdessen die Access Points (AP) unter Berücksichtigung der räumlichen Gegebenheiten und der Kundenwünsche 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.

4.2.2 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 230 V-Steckdose und vereinfacht die Montage erheblich.

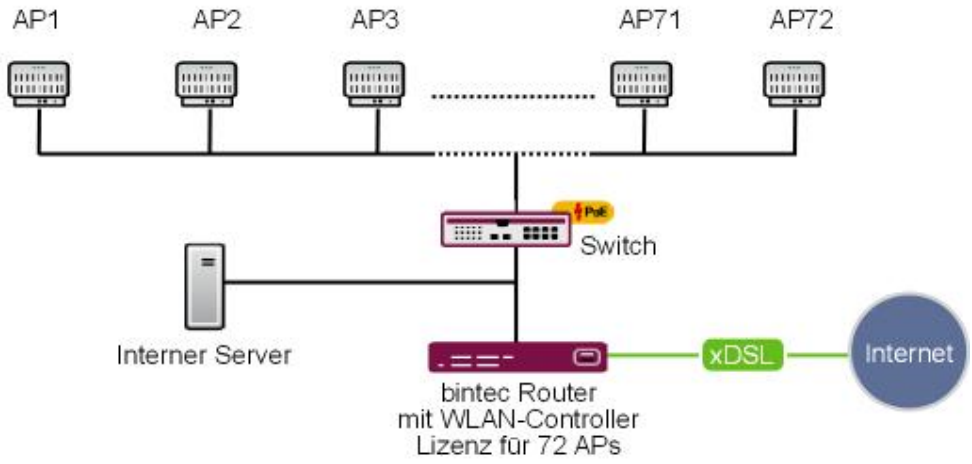


Abb. 57: WLAN-Infrastruktur

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.

4.3 Systemanforderungen

4.3.1 WLAN-Controller-Hardware

Folgende Geräte, deren Firmwareversion 10.1.21 oder höher ist, können als WLAN-Controller verwendet werden (unterstützte Geräte, deren Firmwareversion älter als 10.1.21 ist, müssen vor der Installation aktualisiert werden):

- **bintec Access-Points (W1001n, W1003n, W2003ac/ext, W2022 ac/ext., WI1003n, WO1003ac, WO2003ac)**
- **bintec Medium Router (RS123-Serie, RS353-Serie)**
- **bintec be.IP , be.IP plus**
- **bintec RXL12100**: Central Router, Hochleistungs-Multiplex-VPN-Gateway
- **bintec RXL12500**: Central Router, Hochleistungs-Central-Site-VPN-Gateway

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 **bintec Router** als WLAN-Controller-Hardware notwendig.

4.3.2 Access-Point-Hardware

Der WLAN-Controller kann die bintec Access-Points verwalten. Diese benötigen mindestens die Firmwareversion 10.1.21.

4.3.3 WLAN-Controller-Lizenzen

Bei jedem unterstützten Gerät ist der WLAN-Controller zu Testzwecken in der Software bereits freigeschaltet, allerdings kann lediglich ein einziger Access Point verwaltet werden. Für den Produktivbetrieb muss auf dem Controller eine WLAN-Controller-Lizenz installiert werden. Die WLAN-Controller-Lizenzen finden Sie auf unserer Homepage unter *https://www.bintec-elmeg.com/service-support/produkt-lizenzierung/*

4.4 Netzwerk-Konfiguration

4.4.1 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.

4.4.2 DHCP-Server

4.4.2.1 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 108 wechseln und die WLAN-Installation beginnen, da der Assistent des WLAN-Controllers alle benötigten Einstellungen für den DHCP-Server bereits richtig konfiguriert.

4.4.2.2 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 den 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.

4.4.2.3 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 114 beschrieben.

4.5 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.

4.5.1 Schritt 1 im Assistenten

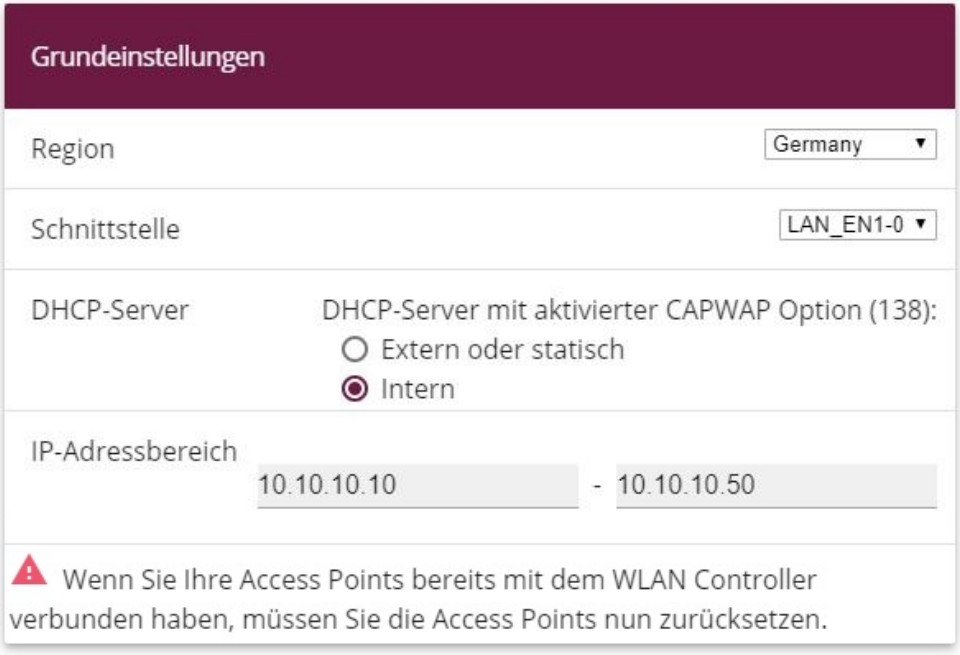


Abb. 58: **Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard**

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) **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.)

(3) **DHCP-Server**: Legt fest, ob der DHCP-Server *Intern* oder *Extern oder statisch* 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 114.

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

(5) Klicken Sie auf **Weiter**.

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.

4.5.2 Schritt 2 im Assistenten

Abb. 59: **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-Radio Profil vorhanden. Weitere Funkprofile lassen sich über das Menü **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Funkmodulprofile** anlegen.

Klicken SIe auf **Weiter**.

4.5.3 Schritt 3 im Assistenten

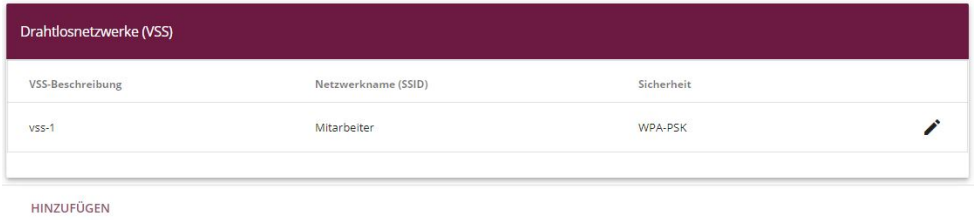


Abb. 60: **Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard**

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

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

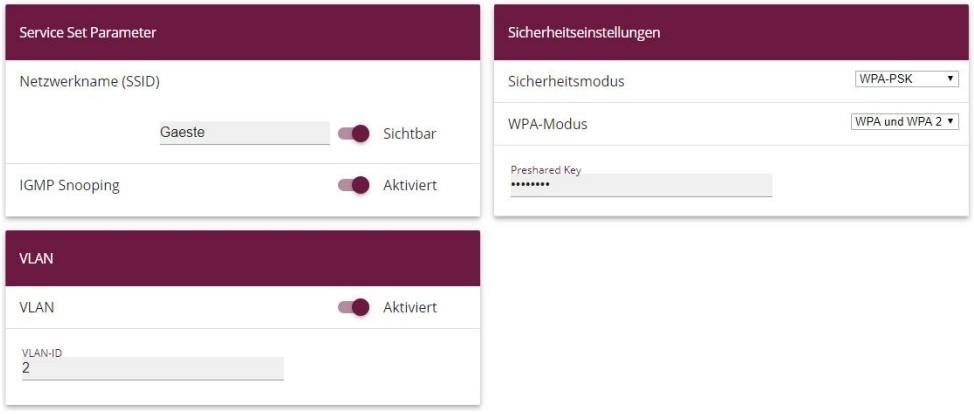


Abb. 61: **Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard**

(1) Für das neue Wireless-Network-Profil (VSS) wird ein **Netzwerkname (SSID)** vergeben.

(2) Wählen Sie den **Sicherheitsmodus** *WPA-PSK* aus.

(3) 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.

(4) Klicken Sie auf **OK**.

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.

4.5.4 Schritt 4 im Assistenten

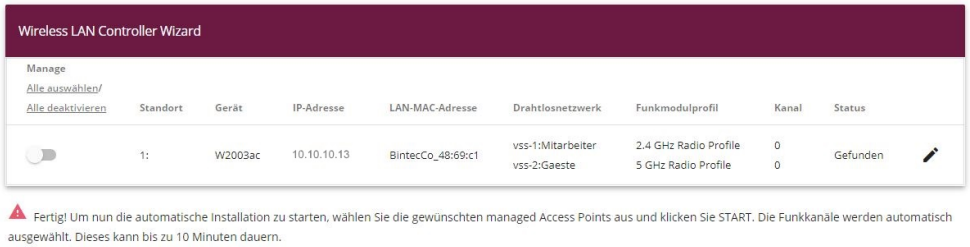


Abb. 62: **Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard**

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 -Symbol 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.

4.5.5 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.

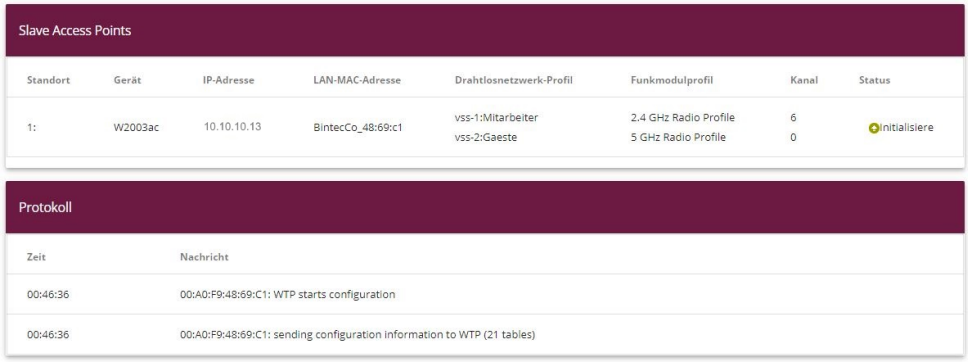


Abb. 63: **Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard**

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.

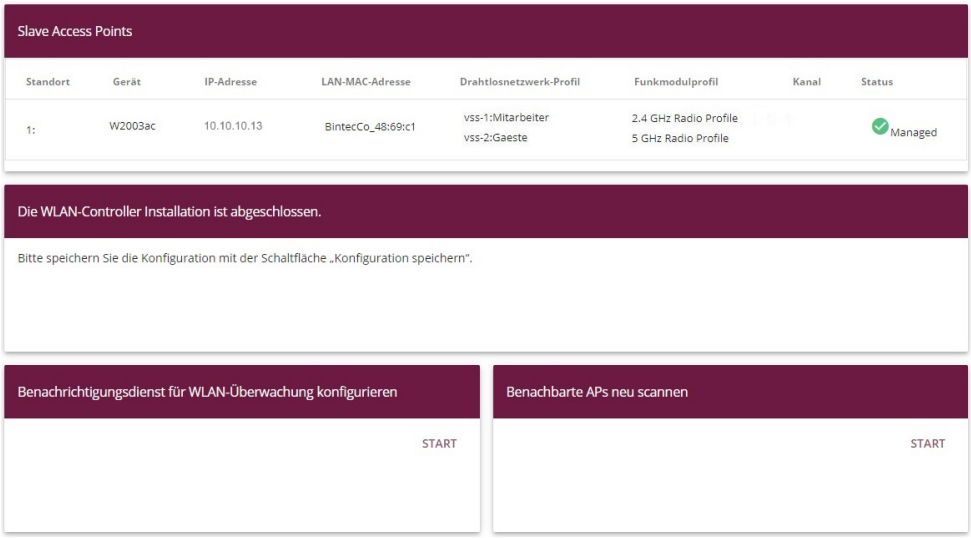


Abb. 64: **Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard**

Die Konfiguration der Access Points sollte nun auf dem WLAN-Controller durch einen Klick auf die Schaltfläche **Konfiguration speichern** (oben rechts) 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 einem 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.

Klicken Sie im Bereich **Benachrichtigungsdienst für WLAN-Überwachung konfigurieren** auf **Start**, um Ihre Managed APs überwachen zu lassen. Zur Konfiguration werden Sie in das Menü **Externe Berichterstellung** ->**Benachrichtigungsdienst** -> **Benachrichtigungsempfänger** mit der Voreinstellung **Ereignis** = *`Verwalteter AP offline`* geleitet. Sie können festlegen, dass Sie mittels E-Mail informiert werden, wenn das Ereignis *`Verwalteter AP offline`* eintritt.

4.6 Anhang

4.6.1 E-Mail-Benachrichtigung bei Ausfall eines Access Points

Sie können sich eine E-Mail vom WLAN-Controller schicken 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 **Benachrichtigungseinstellungen** werden hier nicht beschrieben).

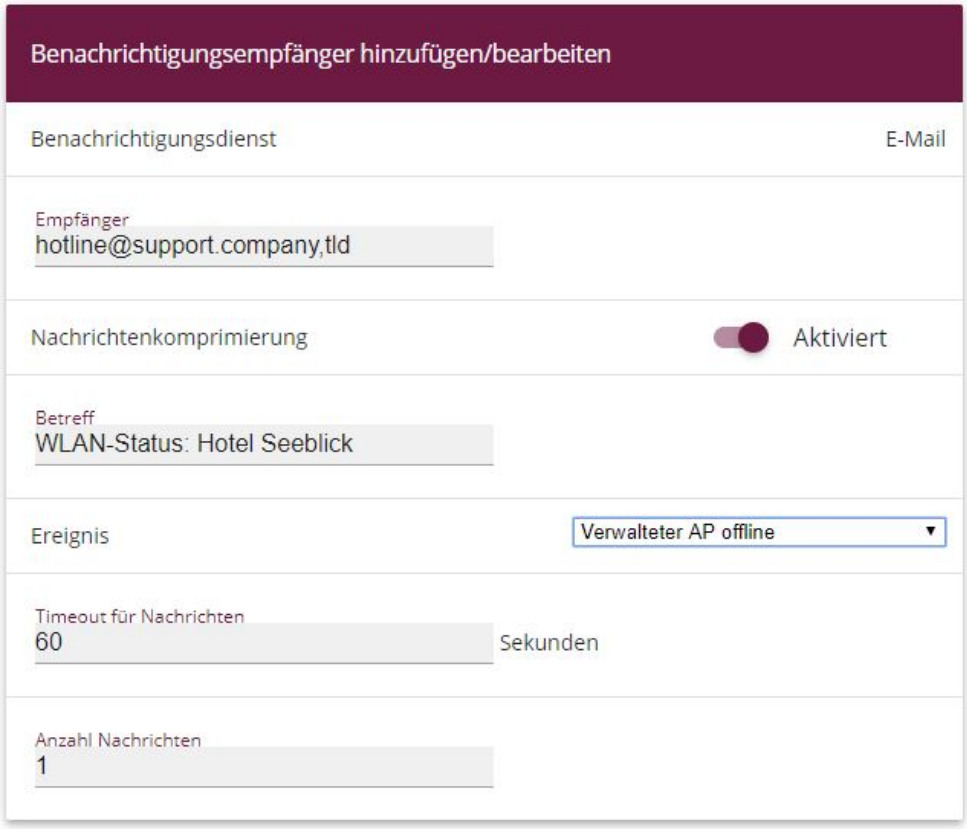


Abb. 65: **Externe Berichterstellung** -> **Benachrichtigungsdienst** -> **Benachrichtigungsempfänger**

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

Benötigt wird ein bintec-Router mit dem Software-Release 10.1.21 oder höher.

Zunächst müssen Sie im Menü **Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu** einen IP-Adresspool definieren.

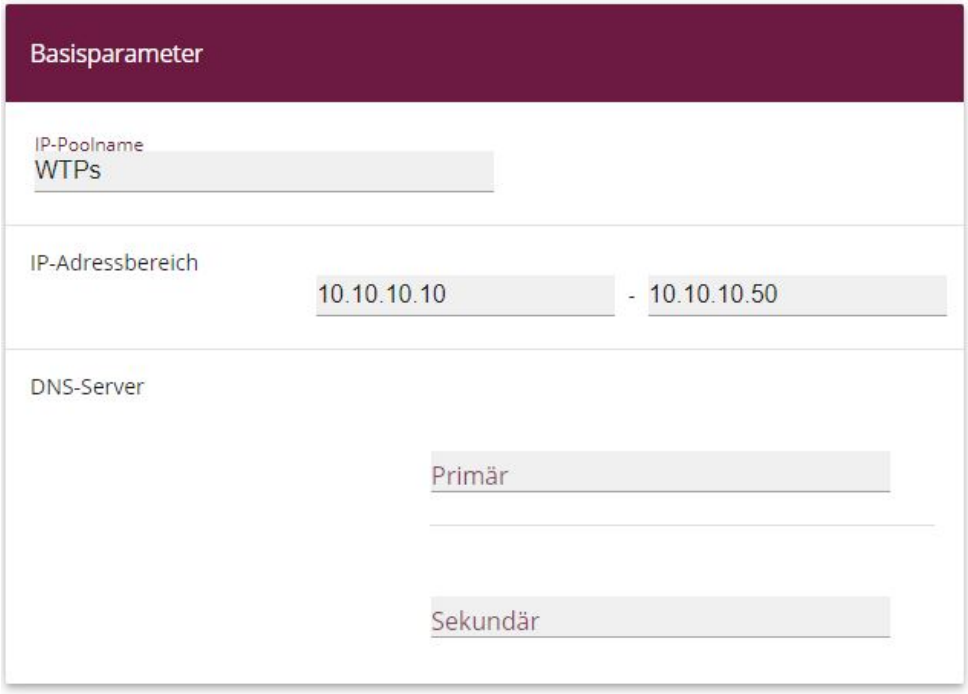


Abb. 66: **Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu**

(1) Geben Sie bei **IP-Poolname** eine beliebige Beschreibung, z. B. `WTPs` ein.

(2) Bei **IP-Adressbereich** geben Sie die erste und die letzte IP-Adresse des IP-Adress-Pools ein, z. B. `10.10.10.10` - `10.10.10.50`.

(3) Bestätigen Sie mit **OK**.

Im Menü **Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu** können Sie nun die weitere Konfiguration vornehmen.

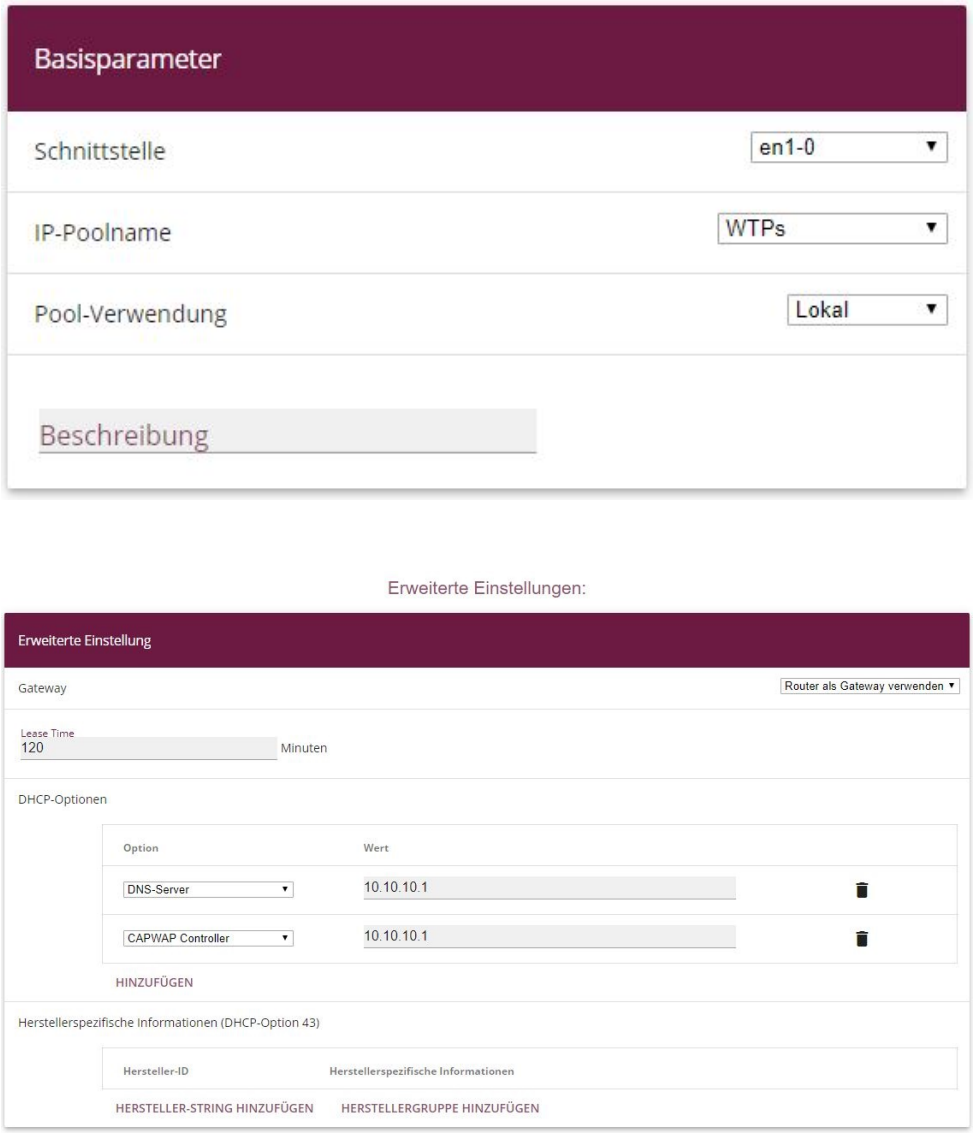


Abb. 68: **Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**

(1) Wählen Sie die **Schnittstelle** aus, über welche die in **IP-Adressbereich** definierten Adressen an anfragende DHCP-Clients vergeben werden.

(2) Unter **IP-Poolname** wählen Sie einen konfigurierten **IP-Pool** aus.

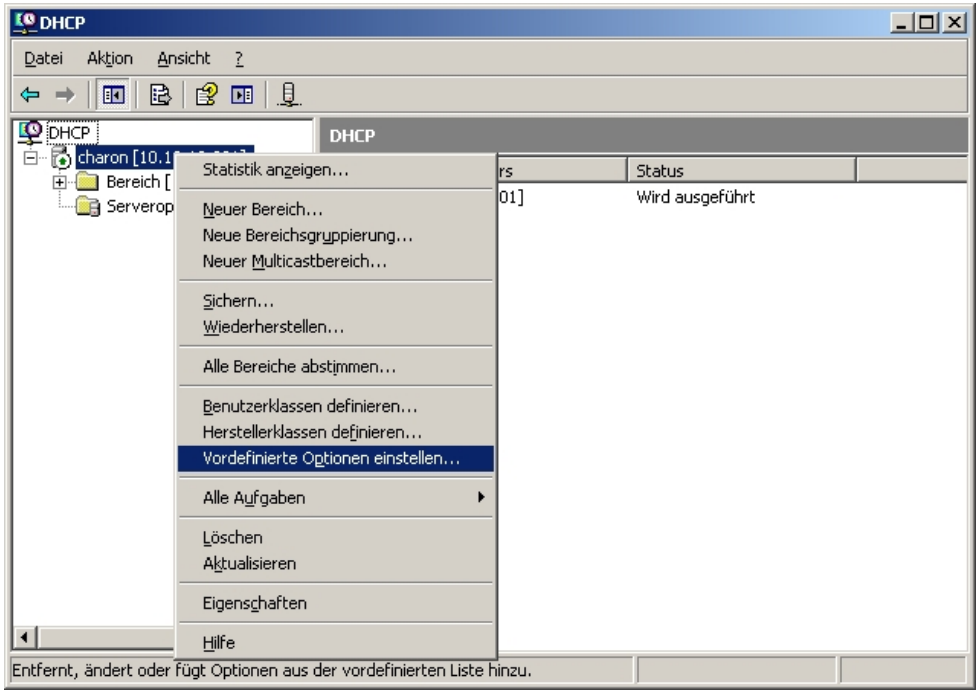
(3) Unter **Erweiterte Einstellungen** im Menü **DHCP-Optionen** fügen Sie mit **Hinzufügen** die Option `CAPWAP Controller` hinzu und im Feld **Wert** tragen Sie die IP-Adresse des WLAN-Controllers ein.

(4) Klicken Sie auf **OK**.

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

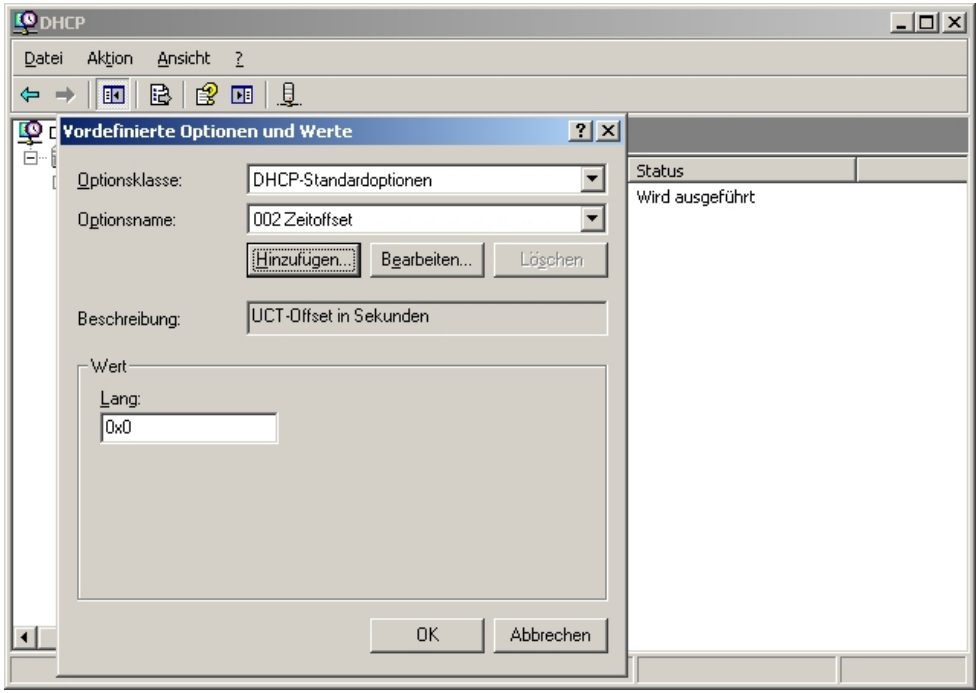
Zunächst sollten Sie Ihren Windows-DHCP-Serverdienst grundlegend einrichten, also den DHCP-IP-Adressbereich definieren, Standardoptionen wie DNS-Server und Standard-Gateway entsprechend der eigenen Netzwerkinfrastruktur konfigurieren.

4.6.3.1 1. Schritt



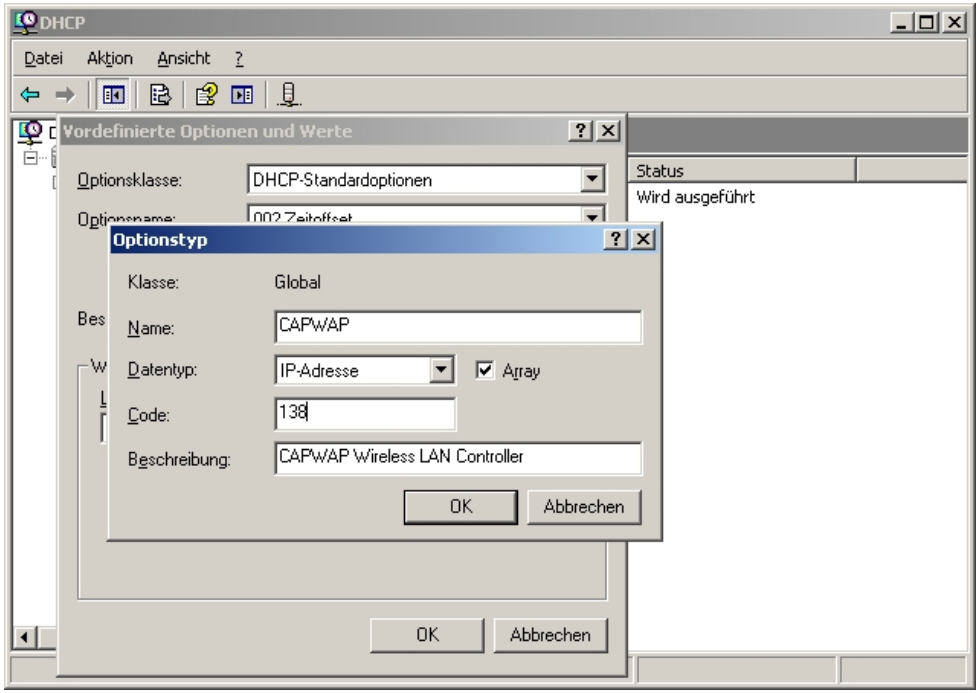
Im Verwaltungsfenster des DHCP-Dienstes (zu erreichen über die Systemsteuerung und dort unter Verwaltung) führen Sie einen Rechtsklick auf die bestehende DHCP-Dienstinstanz aus und klicken im aufklappenden Kontextmenü auf **Vordefinierte Optionen einstellen** (Der Name der Dienstinstanz setzt sich zusammen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

4.6.3.2 2. Schritt



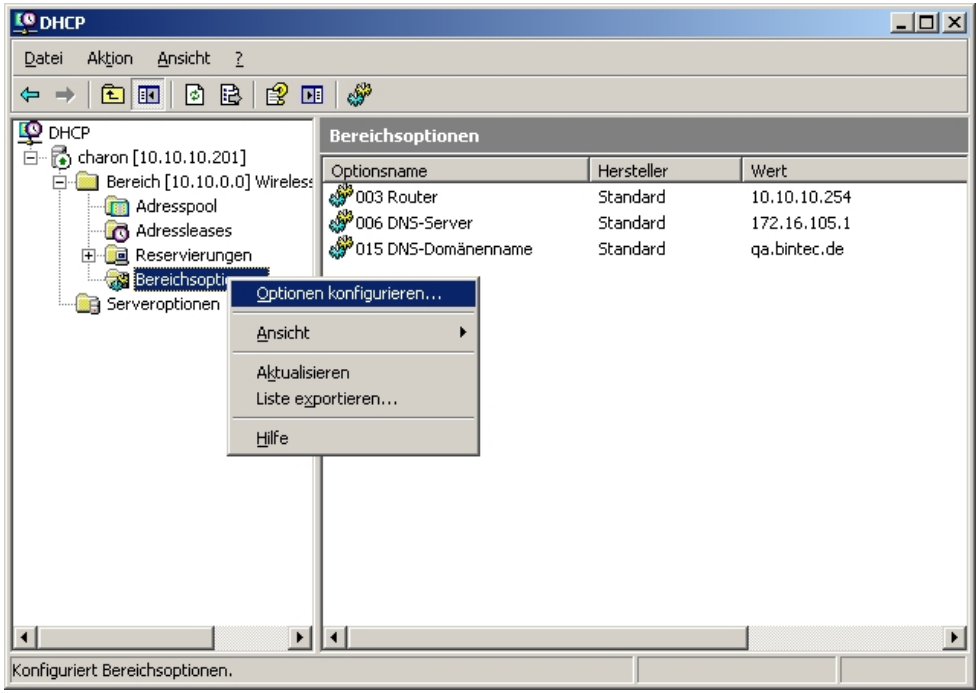
In dem sich nun öffnenden Fenster auf **Hinzufügen** klicken, um die standardmäßig nicht vordefinierte CAPWAP-Option hinzuzufügen.

4.6.3.3 3. Schritt



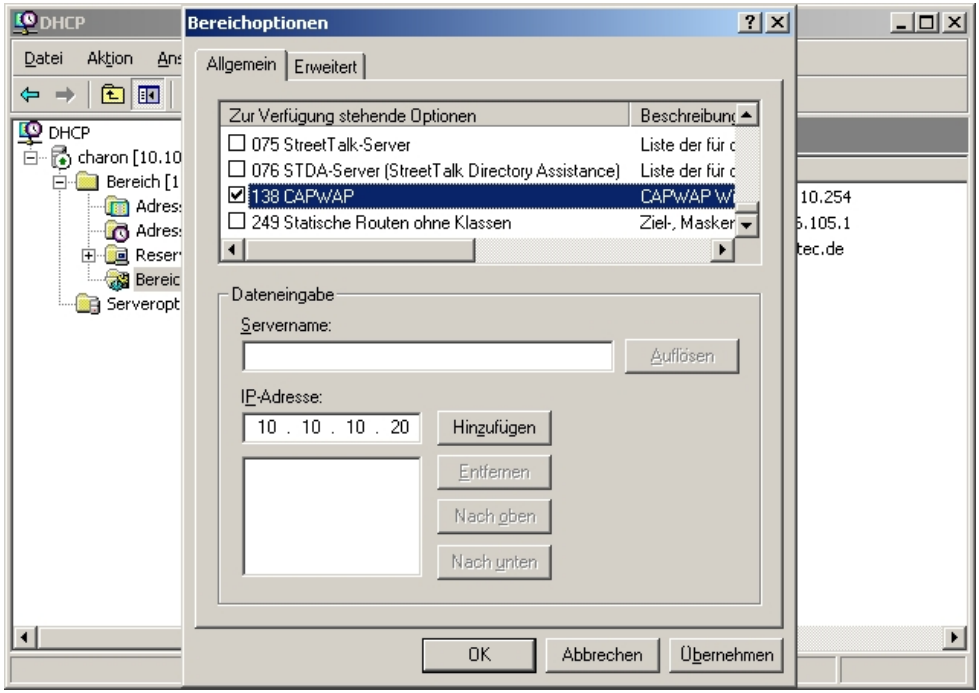
Im neuen Dialogfenster **Optionstyp** wird jetzt die CAPWAP-Option definiert (nicht aktiviert). **Name** und **Beschreibung** sind dabei frei wählbar, sollten aber eingängig benannt werden. Der Datentyp muss auf *IP Adresse* eingestellt und der Haken vor **Array** muss gesetzt sein. Ebenso muss der **Code** 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 dieser zuvor gelöscht werden. Verlassen Sie den Dialog und das vorherige Fenster anschließend mit **OK**.

4.6.3.4 4. Schritt



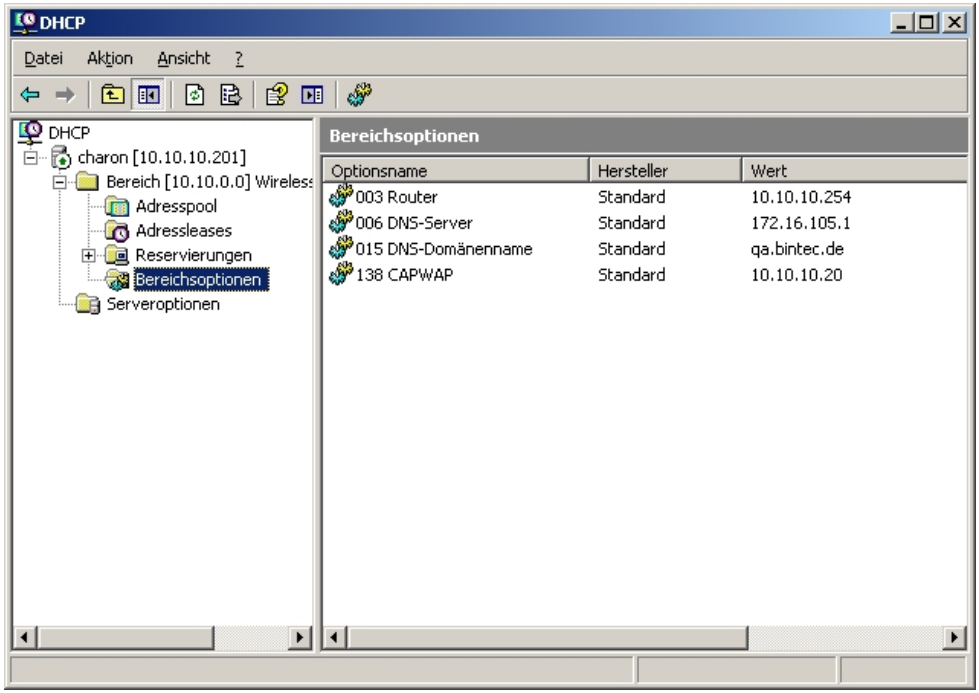
Führen Sie einen Rechtsklick im bereits vorkonfigurierten IP-Adressbereich des DHCP-Dienstes für die künftigen Slave-Access-Points auf **Bereichsoptionen** aus und wählen Sie im Kontextmenü **Optionen konfigurieren** aus.

4.6.3.5 5. Schritt



Im nun aufklappenden Dialogfenster in der Liste der **Zur Verfügung stehenden Optionen** die Option *138 CAPWAP* 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.

4.6.3.6 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 in dem Netz, in dem der soeben eingerichtete DHCP-Dienst erreichbar ist, in Betrieb genommen werden.

4.6.4 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.

4.6.5 Betrieb der APs mit statischen IP-Adressen

Wie im Kapitel *DHCP-Server* auf Seite 107 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. Sie finden im Menü **Systemverwaltung** -> **Globale Einstellungen** -> **System** auf den APs das dazu benötigte Feld **Manuelle IP-Adresse des WLAN-Controller**.

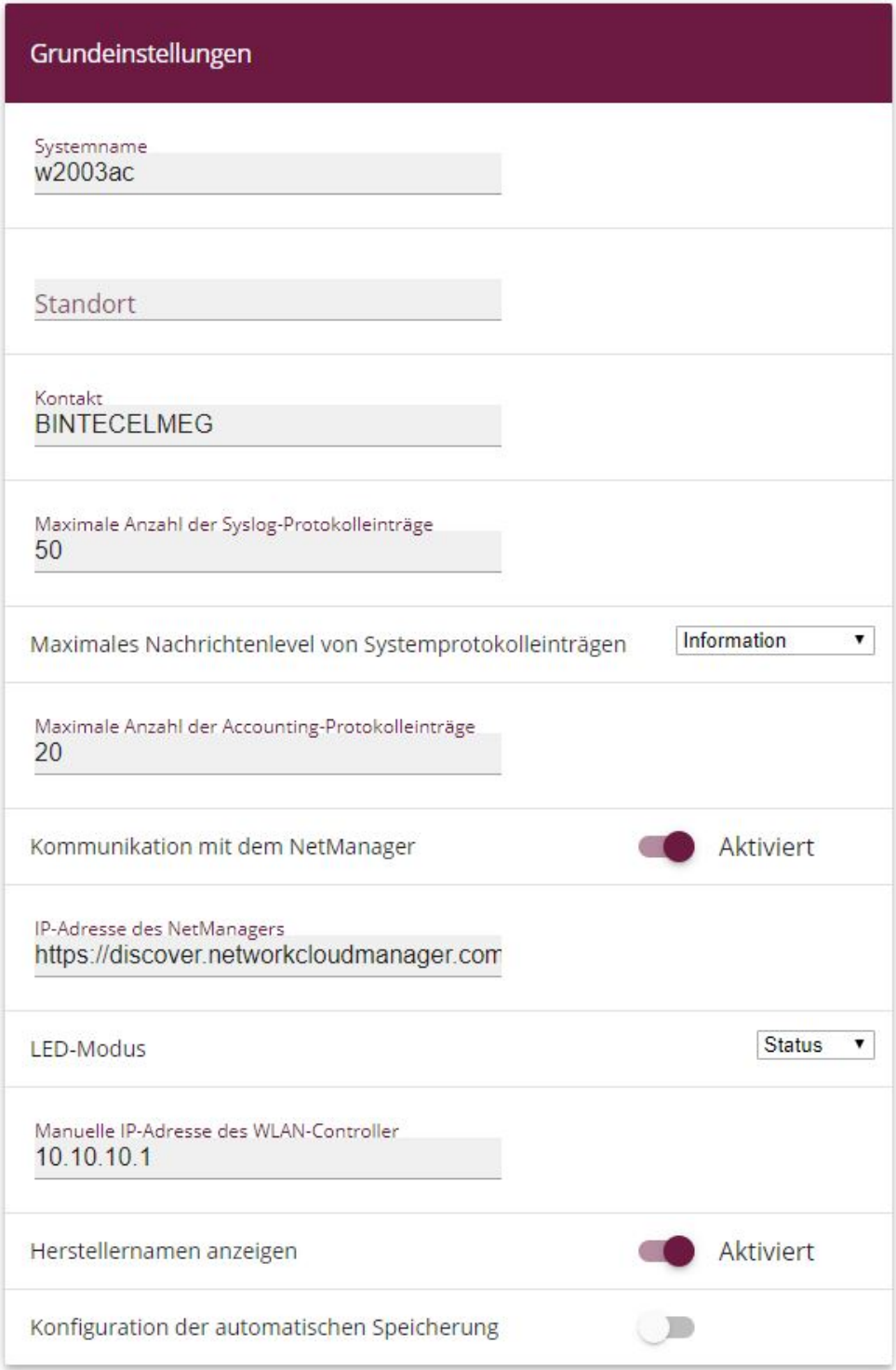

Grundeinstellungen
Systemname
w2003ac
Standort
Kontakt
BINTECELMEG
Maximale Anzahl der Syslog-Protokolleinträge
50
Maximales Nachrichtenlevel von Systemprotokolleinträgen
Information
Maximale Anzahl der Accounting-Protokolleinträge
20
Kommunikation mit dem NetManager
Aktiviert
IP-Adresse des NetManagers
https://discover.networkcloudmanager.com
LED-Modus
Status
Manuelle IP-Adresse des WLAN-Controller
10.10.10.1
Herstellernamen anzeigen
Aktiviert
Konfiguration der automatischen Speicherung

Abb. 69: **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.

4.7 Konfigurationsschritte im Überblick

WLAN-Installation: Schritt 1

Feld	Menü	Wert
Region	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard** ->**Schritt 1**	z. B. *Germany*
Schnittstelle	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard** ->**Schritt 1**	z. B. *LAN_EN1-0*
DHCP-Server	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard** ->**Schritt 1**	z. B. *Intern*
IP-Adressbereich	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard** ->**Schritt 1**	z. B. *10.10.10.10 - 10.10.10.50*

WLAN-Installation: Schritt 2

Feld	Menü	Wert
Funkmodulprofil für Modul 1	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard** ->**Schritt 2**	z. B. *2,4 GHz Radio Profile*
Funkmodulprofil für Modul 2	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard** ->**Schritt 2**	z. B. *5 GHz Radio Profile*

WLAN-Installation: Schritt 3

Feld	Menü	Wert
Netzwerkname (SSID)	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard** ->**Schritt 3**	z. B. *Mitarbeiter*
Netzwerkname (SSID)	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard** ->**Schritt 3** ->**Hinzufügen**	z. B. *Gaeste*

Feld	Menü	Wert
Sicherheitsmodus	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard** ->**Schritt 3** ->**Hinzufügen**	*WPA-PSK*
Preshared Key	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard** ->**Schritt 3** ->**Hinzufügen**	z. B. *supersecret*
VLAN	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard** ->**Schritt 3** ->**Hinzufügen**	*Aktiviert*
VLAN-ID	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard** ->**Schritt 3** ->**Hinzufügen**	z. B. *2*

WLAN-Installation: Schritt 4

Feld	Menü	Wert
Gerät auswählen	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard** ->**Schritt 4**	*Aktiviert*
Benachrichtigungsdienst für WLAN-Überwachung konfigurieren	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard** ->**Schritt 4**	*START*

E-Mail-Benachrichtigung

Feld	Menü	Wert
Empfänger	**Externe Berichterstellung** -> **Benachrichtigungsdienst** -> **Benachrichtigungsempfänger**	z. B. *hotline@support.company.ltd*
Betreff	**Externe Berichterstellung** -> **Benachrichtigungsdienst** -> **Benachrichtigungsempfänger**	z. B. *WLAN-Status: Hotel Seebliick*
Ereignis	**Externe Berichterstellung** -> **Benachrichtigungsdienst** -> **Benachrichtigungsempfänger**	*Verwalteter AP offline*

Konfiguration eines DHCP-Servers auf einem anderen Router

Feld	Menü	Wert
IP-Poolname	**Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu**	z. B. *WTPs*

Feld	Menü	Wert
IP-Adressbereich	**Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu**	z. B. *10.10.10.10 - 10.10.10.50*
Schnittstelle	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	z. B. *en1-0*
IP-Poolname	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	z. B. *WTPs*
Pool-Verwendung	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	*Lokal*
DHCP-Optionen	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu** ->**Erweiterte Einstellungen**	**Option***CAPWAP Controller*, **Wert** z. B. *10.10.10.1*

Betrieb mit statischer IP-Adresse

Feld	Menü	Wert
Manuelle IP-Adresse des WLAN-Controller	**Systemverwaltung** -> **Globale Einstellungen** -> **System**	z. B. *10.10.10.1*

Kapitel 5 WLAN - VoWLAN Grundlagen und Konfiguration

5.1 Allgemein

Beim schnurlosen Telefonieren erwartet der Anwender eine möglichst gute Sprachqualität und hohe Zuverlässigkeit.

Der DECT (Digital Enhanced Cordless Telecommunications) Standard hat eine hohe Akzeptanz und erfüllt die oben genannten Voraussetzungen. Im Gegensatz zu WLAN verwendet DECT einen eigenen reservierten Frequenzbereich. Da DECT im 1,9 GHz Bereich arbeitet, ist die Hochfrequenz-Ausbreitungscharakteristik günstiger als bei WLAN, dies führt zu einer höheren Reichweite. Daher werden auch bei VoWLAN mehr Basisstationen (Access Points) als bei DECT benötigt. WLAN ist ursprünglich für Datenübertragung von Endgeräten entwickelt worden, deren Standort sich nicht verändert. Bei VoWLAN verändert sich der Standort des Wifi Telefons aber permanent. VoWLAN muss also in der Lage sein, die Verbindung von einem Access Point zum nächsten Access Point zu übergeben (Handover/Roaming). Das muss ohne merkliche Unterbrechung der Verbindung möglich sein (Seamless Handover). Dieses Merkmal ist besonders bei Installationen in größeren Unternehmen wichtig, bei denen mehrere Access Points zum Einsatz kommen.

In den nachfolgenden Kapiteln wird gezeigt, wie ein derartiges VoWLAN-Netz konfiguriert und aufgebaut werden muss, damit die wichtigsten Qualitätsmerkmale erfüllt werden können, die von drahtloser Telefonie erwartet werden. Es kommen dabei die **bintec be.IP** oder **be.IP plus**, mehrere WLAN-Access Points z. B. **bintec W2003ac-ext**, ein **bintec RS123w** als WLAN-Controller sowie das von bintec elmeg zertifizierte **Ascom i62** VoWLAN-Telefon zum Einsatz.

5.2 WLAN Infrastruktur

5.2.1 WLAN Funkausleuchtung

Gegenüber einer WLAN-Infrastruktur für Datenübertragung muss das WLAN-Netz für VoWLAN engmaschiger ausgelegt werden. Bei der Planung ist auch auf die WLAN-Versorgung von Nebenräumen zu achten, damit beispielsweise auch in der Kaffeeküche telefoniert werden kann. Damit das Roaming perfekt funktioniert, und zur Erzielung einer guten Sprachqualität ist eine Versorgung mit mindestens -70 dBm innerhalb einer Zelle zu gewährleisten. Darüber hinaus sollen sich die Funkzellen gegenseitig um 6-10 dBm überlappen. Die VoWLAN-Telefone und die Access Points sollen dabei auf maximale Sendeleistung (20 dBm/100 mW) eingestellt sein.

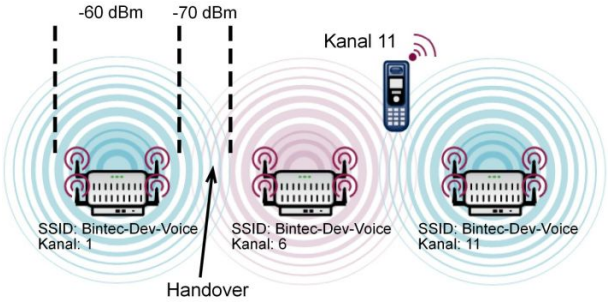


Abb. 70: Darstellung der Mindestanforderungen an die WLAN-Ausleuchtung für VoWLAN

Bei größeren Gebäuden wird man die zur Verfügung stehenden drei überlappungsfreien Funkkanäle (z. B. 1, 6, 11) mehrfach vergeben müssen. Damit es zu keinen Einschränkungen bei der Performance kommt, sollte gewährleistet sein, dass innerhalb einer Funkzelle auf dem gleichen Kanal keine Access Points arbeiten, die ein stärkeres Signal als -80 dBm liefern.

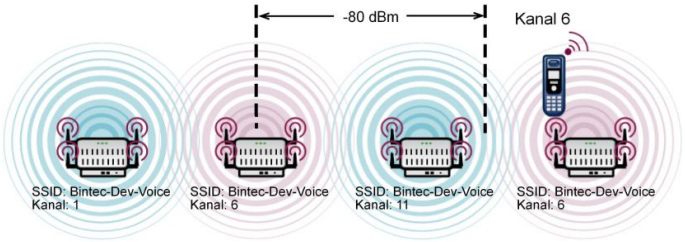


Abb. 71: Mindestabstand zweier WLAN Access Points auf dem gleichen Sendekanal

Die Ausleuchtung des Gebäudes und die Festlegung der Standorte der Access Points sollen bei einer VoWLAN-Installation unbedingt durch ein **Ekahau Site Survey** (www.ekahau.de) geplant werden. Bei einem **Site Survey** wird mit einer computergestützten Planungssoftware eine Begehung des Gebäudes durchgeführt und eine flächende-

ckende Ausleuchtung errechnet. Dabei werden auch die optimalen Standorte der WLAN Access Points festgelegt.

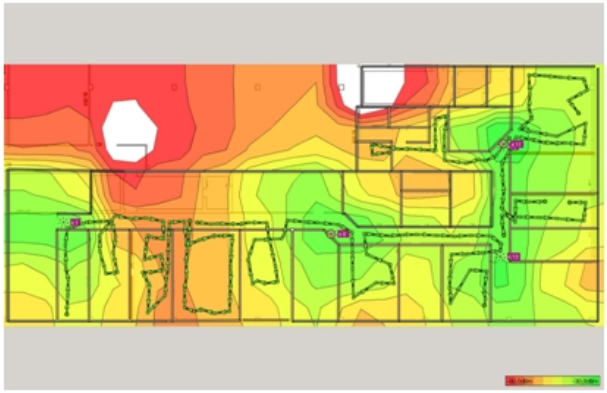


Abb. 72: Typisches Ergebnis eines Site Survey

5.2.2 Handover zwischen den Access Points

Damit das Handover zwischen den Access Points richtig funktioniert, ist es notwendig, dass alle Access Points die gleiche SSID verwenden. Vorzugsweise soll für die Sprachkommunikation eine eigene SSID verwendet werden.

Bei Netzen mit 802.11g und 802.11n (20 MHz) müssen die Funkkanäle einen Kanalabstand von 5 Kanälen haben. Daher können z. B. nur die Kanäle 1, 6 und 11 überlappungsfrei belegt werden.

Zur Optimierung des Handover zwischen den Access Points kann bei manchen VoWLAN-Telefonen (z. B. Ascom) ein Kanalplan (z. B. Kanal 1, 6, 11) eingegeben werden. Dies bewirkt dann, dass das Telefon bei schwachem WLAN-Signal nur auf den Kanälen des Kanalplanes nach einem neuen Access Point sucht. Dieses Verfahren ermöglicht ein etwas schnelleres Handover. Wichtig ist nur, dass bei der Konfiguration darauf geachtet wird, dass der Kanalplan des Telefons identisch mit den im WLAN-Netz verwendeten Kanälen ist.

5.2.3 Bandbreitenbedarf

Die maximal erreichbare Bruttodatenrate einer WLAN-Verbindung hängt zunächst von der verwendeten 802.11-Betriebsart ab. Es ist aber zu beachten, dass bei größerer Entfernung zwischen Access Point und Endgerät diese Bruttorate leicht auf die minimale Bruttorate abfallen kann. Die tatsächliche Nettorate liegt jedoch nur bei etwa 40-50 % der Bruttorate.

802.11 Betriebsart	Maximale Bruttorate	Minimale Bruttorate
802.11b	11 Mbit/s	1 Mbit/s
802.11bg	54 Mbit/s	6 Mbit/s
802.11n (1stream/20 MHz)	72,2 Mbit/s	7,2 Mbit/s

Ein Sprachkanal benötigt etwa 100 kbit/s, bei der Kapazitätsplanung ist jedoch davon auszugehen, dass genügend Reserven im Nutzkanal vorhanden sind, damit jedes RTP-Paket auch sofort versendet werden kann.

802.11g und 802.11n sind untereinander 100-prozentig kompatibel und ein WLAN-Netz kann daher bedenkenlos im Mischbetrieb laufen. Bei 802.11b (11 Mbit/s) gibt es aber die Besonderheit, dass bereits ein Gerät mit 802.11b (11 Mbit/s) ein komplettes Netz auf diese niedrige Bitrate zieht. 802.11b-Geräte sind kaum noch verbreitet, daher wird dringend empfohlen, eine Betriebsart zu verwenden, die 802.11b nicht zulässt. Wir empfehlen daher, *802.11g/n* als 802.11-Betriebsart einzustellen, um 802.11b-Geräte nicht zuzulassen.

5.2.4 Der Sicherheitsstandard und das Handover

WLAN ist ursprünglich für die Datenübertragung von Endgeräten entwickelt worden, deren Standort sich nicht verändert. Bei VoWLAN verändert sich der Standort des WLAN-Telefons aber permanent. Eine VoWLAN-Installation muss also in der Lage sein, die Verbindung von einem Access Point zum nächsten Access Point zu übergeben (Handover), ohne dass es zu einer merklichen Unterbrechung der Verbindung (Seamless Handover) kommt. Dieses Merkmal ist besonders bei Installationen in größeren Unternehmen wichtig, bei denen mehrere Access Points zum Einsatz kommen. Gerade einfache, preiswerte Access Points aus dem Konsumbereich und auch ältere Endgeräte haben hier oft Probleme.

Das gewählte WLAN-Security-Verfahren hat darüber hinaus entscheidenden Einfluss auf die Handover-Performance. Beim Handover von einem Access Point auf einen anderen Access Point mit besserem WLAN-Signal muss nach dem Herstellen der Verbindung die WLAN-Security wiederhergestellt werden, bevor das nächste Sprachdatenpaket übertragen werden kann. Wir empfehlen WPA2-PSK, da hier eine hohe Sicherheit erreicht wird bei gleichzeitig hervorragenden Handover-Zeiten (<40 ms).

Von der Verwendung von 802.1x bzw. WPA2-Enterprise in drahtlosen VoWLAN-Netzen wird abgeraten, da die Wiederherstellung der Security nach einem Handover auf einen neuen Access Point deutlich länger dauert als bei WPA2-PSK. Dies führt dann möglicherweise zu hörbaren Unterbrechungen und Störgeräuschen.

5.2.5 QoS, WMM und U-APSD

Damit die Endgeräte eine lange Gesprächszeit und hohe Standby-Zeiten mit einer Akkuladung erreichen, ist es notwendig, dass sowohl die Endgeräte als auch die Access Points entsprechende Stromsparmechanismen unterstützen. U-APSD (Unscheduled Automatic Power Save Delivery) sorgt dafür, dass das Endgerät nur dann sendet, wenn es notwendig ist. Während der Schlafphase des Endgerätes sorgt der Access Point dafür, dass Datenpakete, die an das Telefon gesendet werden sollen, zwischengespeichert werden und dass das Telefon auch rechtzeitig aufgeweckt wird. Ob U-APSD richtig funktioniert, hängt von der signalisierten QoS-Klasse ab, da U-APSD immer einen Bezug zur QoS-Klasse hat. Bei der Konfiguration sollte man sich daher an die Herstellerempfehlung halten.

Die Sprachdaten werden als RTP (Real-Time-Transport-Protocol) Daten übermittelt. Um die Übermittlung der RTP-Sprachdatenpakete zwischen der IP-TK- Anlage und dem VoWLAN-Telefon mit geringen Latenzzeiten zu realisieren, ist es notwendig, die Sprachdaten gegenüber den normale Daten zu priorisieren.

In diesem Kapitel wird beschrieben, wie die Priorisierung der Sprachdaten im LAN und im WLAN funktioniert und welchen Zusammenhang es mit dem Stromsparmechanismus U-APSD gibt.

5.2.5.1 WMM Priority Classes und COS (Layer 2) Mapping

Der 802.11e-Standard definiert vier WMM-Access-Categories (ACs), um den Datenverkehr entsprechend der QoS-Anforderungen zu behandeln.

- AC_BK (background)
- AC_BE (best effort)
- AC_VI (video)
- AC_VO (voice)

Ergänzend legt 802.11e ein Mapping zwischen dem Layer 2 (802.1d) Class of Service des LANs und den WMM-Access-Categories des WLANs fest.

Mapping Tabelle nach 802.11e

Priority	Layer 2 COS	WMM-Access-Category
Lowest	1	AC_BK (background)
	2	AC_BK (background)
	0	AC_BE (best effort)
	3	AC_BE (best effort)
	4	AC_VI (video)

Priority	Layer 2 COS	WMM-Access-Category
	5	AC_VI (video)
	6	AC_VO (voice)
Highest	7	AC_VO (voice)

Die Access Points (z. B. **bintec W2003ac-ext**, **bintec WI1003n**) haben das Mapping entsprechend des 802.11e-Standards implementiert. Der WLAN-Treiber der Access Points führt das Mapping zwischen der Layer 2-Priorität des LAN und der WMM-Klasse des WLAN durch und zwar in beiden Richtungen.

In vielen IP-Netzwerken (kein VLAN oder VLAN ohne Layer 2 Priority) werden die QoS-Requirements für die Datenübertragung mittels Layer 3-Priority (TOS/DSCP) signalisiert. Deshalb ist es notwendig, dass die WLAN Access Points Layer3 <- -> Layer 2 Mapping unterstützen.

Layer 3 / Layer 2 / WMM-Mapping

DSCP Field Hex/Bin/Dec	Layer 2 Prio	Traffic Type	Acronym	WMM-Access-Category
0x38 / 111000 / 56	7	Network Control	NC	AC_VO
0x30 / 110000 / 48	6	Voice	VO	AC_VO
0x28 / 101000 / 40	5	Video	VI	AC_VI
0x20 / 100000 / 32	4	Controlled Load	CL	AC_VI
0x18 / 011000 / 24	3	Excellent Effort	EE	AC_BE
0x10 / 010000 / 16	2	Spare		AC_BK
0x08 / 001000 / 8	1	Background	BK	AC_BK
0x00 / 000000 / 0	0	Best Effort	BE	AC_BE

Das obige Mapping berücksichtigt nur die oberen drei Bits des TOS/DSCP-Feldes; es ist daher relativ unscharf und führt zu Problemen mit VoWLAN-Geräten.

Die meisten VoWLAN-Geräte benutzten aber als Class of Service Expedited Forwarding (EF) mit DSCP Value (0x2E / 101110 / 46) entsprechend RFC 4594. Die obige Mapping-Tabelle würde diese Klasse in die WMM Class 'AC_VI' mappen. Dies ist aber nicht korrekt, da

das VoWLAN-Telefon für die Gegenrichtung „WMM AC 'AC_VO“ verwendet.

Um dieses Problem zu vermeiden, mappen bintec Access Points Daten, die mit “EF” getagged sind, auf folgende Weise:

DSCP Field Hex/Bin/Dec	Layer 2 Prio	Traffic Type	Acronym	WMM-Access-Category
0x2E / 101110 / 46	6	Voice	VO	AC_VO

Merke: Bei der Installation muss der Anwender lediglich darauf achten, dass das VoWLAN-Telefon und die IP-TK-Anlage als Class of Service Expedited Forwarding (EF) mit DSCP Value (0x2E / 101110 / 46) verwenden. Dieser Wert ist bei der **bintec be.IP plus** voreingestellt.

5.2.5.2 U-APSD (Unscheduled Automatic Power Save Delivery)

U-APSD ist Bestandteil von 802.11e und trägt maßgeblich zur Erhöhung der Akkulaufzeit von VoWLAN-Endgeräten bei. U-APSD muss sowohl vom VoWLAN-Endgerät als auch vom WLAN Access Point unterstützt werden. U-APSD funktioniert immer nur für die jeweilige WMM-Access-Categorie. Daher ist wichtig, dass die im obigen Kapitel gemachten Voraussetzungen geschaffen werden.

Der grobe Ablauf funktioniert wie folgt:

- VoWLAN-Endgerät meldet sich mit Class of Service Expedited Forwarding (EF) und U-APSD beim WLAN Access Point an.
- Das VoWLAN-Endgerät schaltet danach in den Power-Save-Mode.
- Falls der WLAN Access Point Datenpakete für das betreffende VoWLAN-Endgerät mit dem Class of Service Expedited Forwarding (EF) erhält, speichert der Access Point diese Daten kurzzeitig zwischen und wartet bis das VoWLAN-Endgerät wieder aufgeweckt ist. Erst jetzt werden die Daten versendet.
- Der Vorgang funktioniert derart schnell, dass das Endgerät selbst im Gesprächszustand noch genug Zeit für den Power-Save-Mode hat.

Neben der längeren Akkulaufzeit gibt es einen weiteren positiven Effekt von U-APSD. VoWLAN-Endgeräte mit funktionierenden U-APSD sind bei längeren Gesprächen deutlich kühler als Geräte, die kein U-APSD unterstützen.

U-APSD wird von den Access Points (z. B. **bintec W2003ac-ext**, **bintec WI1003n**) ab Release 10.1.9 unterstützt.

5.2.6 WLAN Controller – Ein Muss in einem VoWLAN-Netz?

Um das Handover zu optimieren, verwalten die Lösungen einiger Hersteller die WLAN-Daten zentral im WLAN-Controller. Diese Lösungen bedienen sich dann sogenannter Thin-APs, das sind Access Points ohne eigene Intelligenz. Der Nachteil dieser Lösungen ist, dass der gesamte Datenverkehr zentral ausgekoppelt wird und damit die Netze belastet. Mit Einführung der 802.11n-Technik ist die Datenmenge beträchtlich gestiegen, damit verlieren Lösungen mit Thin-APs weiter an Bedeutung gegenüber Lösungen mit intelligenten FAT-APs. Seit Einführung des Sicherheitsstandards WPA2-PSK und dem Fast-Roaming nach 802.11r ist nun auch die Handover-Problematik bei WLAN-Lösungen mit FAT-APs gelöst.

Die **bintec WLAN Controller**-Lösung arbeitet mit intelligenten Access Points (FAT-APs), die die Nutzdaten lokal verwalten. Dieses Szenario hat gegenüber Thin-Client Lösungen erhebliche Performance-Vorteile. Der **bintec WLAN Controller** ist kein Muss für eine VoWLAN-Installation, erleichtert aber die Installation erheblich und vereinfacht die Überwachung des Systems.

5.2.7 Mögliche Störquellen

Das 2,4-GHz-Band wird neben WLAN von verschiedensten Funkdiensten genutzt. Die meisten dieser Dienste sind auf kleine Sendeleistungen beschränkt und haben nur eine geringe Reichweite. So haben zum Beispiel die meisten Bluetooth-Geräte, die wir in Büroumgebungen häufig finden, meist nur eine Sendeleistung von 1 mW und sind somit für VoWLAN kein echtes Problem. Wichtig für störungsfreien VoWLAN-Betrieb ist darüber hinaus natürlich auch, dass sich möglichst wenige, fremde Access Points (Nachbarn) in der Nähe befinden. Diese fremden Access Points stören zwar zunächst nicht, reduzieren aber die Nettobandbreite. Verbesserung bringt hier z. B. ein geänderter Kanalplan, um so am Nachbar-Access-Point „vorbei zu funken“. Besonders dann, wenn ein VoWLAN-Netz für eine hohe Anzahl von Teilnehmern geplant wird, kann es auch hilfreich sein, ein zweites WLAN-Netz mit 5 GHz zu installieren, um so die Datenanwendungen auf das freie 5-GHz-Netz zu bringen.

Nach unserer Erfahrung sind unbekannte Störquellen in VoWLAN-Anwendungen selten, wenn die hier beschriebenen Grundregeln bei der Installation eingehalten werden. Eventuelle, breitbandige Störquellen oder Nachbarschafts-Access-Points, die später zu Problemen führen können, werden darüber hinaus bei einer Site-Survey-Begehung des Gebäudes bereits im Vorfeld erkannt und es können vorab Gegenmaßnahmen ergriffen werden.

5.3 Beispielkonfiguration

5.3.1 Netzwerkplan

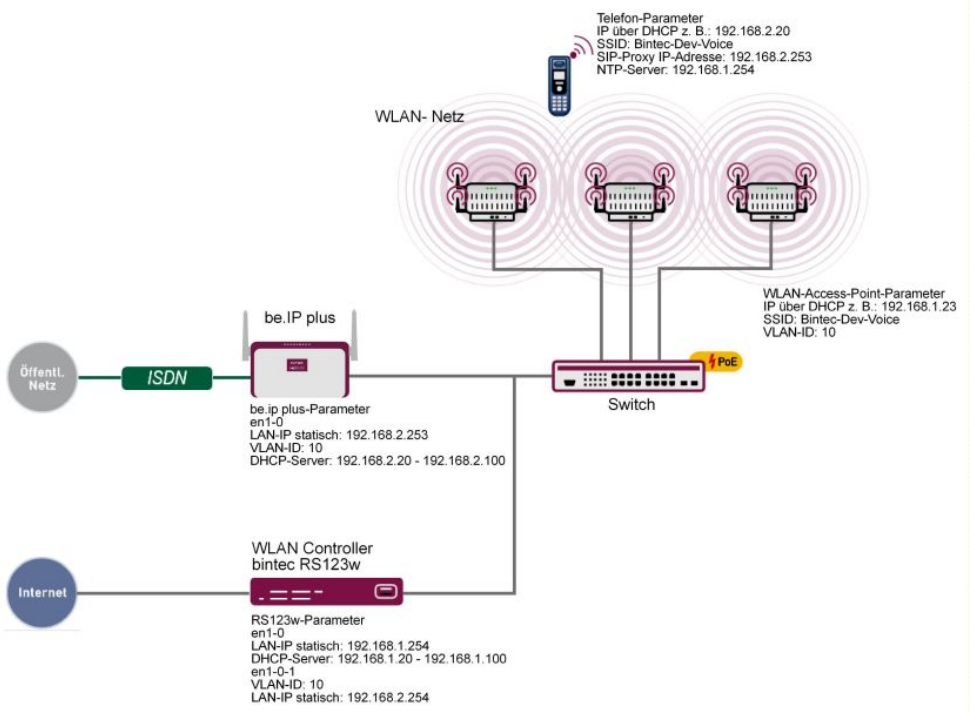


Abb. 73: Beispielszenario

Die obige Beispielkonfiguration zeigt ein kleines Anwendungsszenario, bestehend aus einer **bintec be.IP plus**, einem **bintec RS123w** als WLAN Controller, drei **bintec W2003ac-ext** Access Points und einem **Ascom i62** VoWLAN-Telefon.

Das LAN besteht aus zwei Netzen: Zum einen aus dem Netz 192.168.1.0/24, dieses Netz dient der Kommunikation zwischen dem WLAN Controller (**bintec RS123w**) und den Access Points.

Das zweite Netz 192.168.2.0/24 ist hier mit der **VLAN-ID** *10* getagged und dient zum Transport der Voice-Daten. Die **SSID** *Bintec-Dev-Voice* ist der **VLAN-ID** *10* zugeordnet. Dadurch werden nur die Voice-Daten zwischen dem VoWLAN-Telefon und der hybird über die WLAN-Strecke übertragen.

bintec RS123w arbeitet als WLAN Controller und stellt darüberhinaus für die VoWLAN-Telefone zusätzlich noch den NTP-Zeitserver (192.168.1.254) zur Verfügung.

5.3.2 WLAN Konfiguration mit oder ohne WLAN Controller

Ein VoWLAN-Netz kann sowohl über einen WLAN Controller als auch manuell konfiguriert und betrieben werden. Da der Handling-Aufwand für eine größere Installation bei Verwendung eines WLAN Controller deutlich geringer ist und zudem auch mehr Komfort bei der Überwachung bietet, empfehlen wir bei Installationen mit mehr als drei Access Points den Einsatz eines WLAN Controllers.

Zur Konfiguration wird das **GUI** (Graphical User Interface) verwendet.

Um auf die Konfigurationsoberfläche zu gelangen, geben Sie im Web-Browser die IP-Adresse des **bintec RS123w** an.

Gehen Sie zu **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Funkmodulprofile** -> **Neu**.

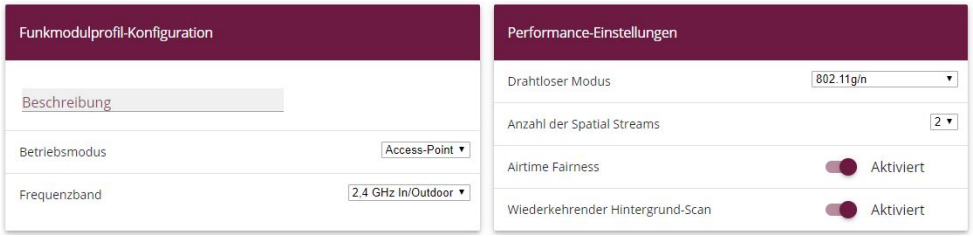


Abb. 74: **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Funkmodulprofile** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Bei **Betriebsmodus** legen Sie fest, in welchem Modus das Funkmodulpofil betrieben werden soll, hier *Access-Point*.

(2) Wählen Sie das **Frequenzband** des Funkmodulprofils *2,4 GHz In/Outdoor* aus.

(3) Bei **Anzahl der Spatial Streams** wählen Sie aus, wieviele Datenströme parallel verwendet werden sollen, z. B. *2* (Standardwert): Zwei Datenströme werden verwendet.

(4) Wählen Sie bei **Drahtloser Modus** die Wireless-Technologie aus, die der Access Point anwenden soll, hier *802.11 g/n*.

(5) Klicken Sie auf **Erweiterte Einstellungen**.

(6) Wählen Sie die **Max. Übertragungsrate** aus. Mit *Auto* (Standardwert) wird die Übertragungsgeschwindigkeit automatisch ermittelt.

(7) Bestätigen Sie mit **OK**.

Legen Sie anschließend die Drahtlosnetzwerk-Einträge an.

Gehen Sie zu **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)** -> **Neu**.

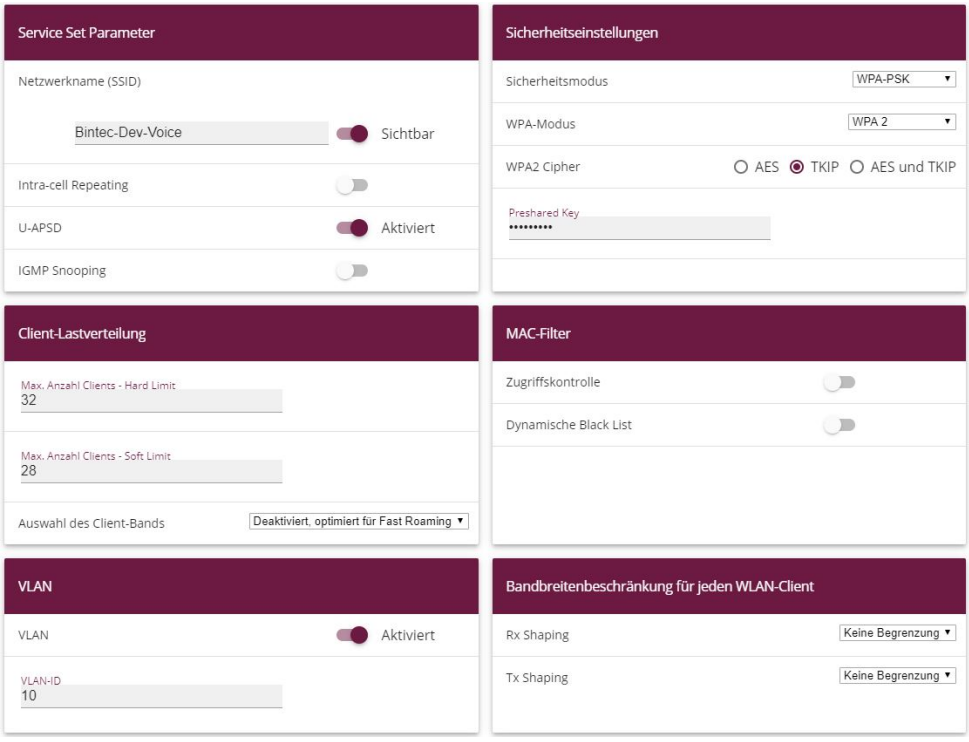


Abb. 75: **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Geben Sie den **Netzwerknamen (SSID)** des Drahtlosnetzwerks, z. B. *Bintec-Dev-Voice* ein.

(2) Deaktivieren Sie das **Intra-cell Repeating**. Die Kommunikation zwischen den WLAN-Clients innerhalb einer Funkzelle ist nicht erlaubt.

(3) Wählen Sie den **Sicherheitsmodus** *WPA-PSK* aus.

(4) Bei **WPA-Modus** wählen Sie aus, welche Verschlüsselung angewendet werden soll, hier *WPA2*.

(5) Wählen Sie bei **WPA2 Cipher** aus, mit welcher Verschlüsselung Sie WPA anwenden wollen, hier *TKPI* und *AES*.

(6) Geben Sie bei **Preshared Key** das WPA-Passwort ein, z. B. *supersecret*. Solange der Key nicht geändert wurde, ist ihr Gerät nicht gegen einen unautorisierten Zugriff geschützt!

(7) Deaktivieren Sie **ACL-Modus**. Für dieses Drahtlosnetzwerk werden alle Clients zugelassen.

(8) Wählen Sie bei **VLAN-ID** den Zahlenwert ein, der das VLAN identifiziert, hier *10*.

(9) Bestätigen Sie mit **OK**.

5.4 Ascom i62 Talker Konfiguration

5.4.1 Vorrausetzungen

Folgende Geräte bzw. Software benötigen Sie zur Konfiguration des **Ascom i62**:

- **Ascom i62** Talker (EH1-AAAA/1A)
- Ascom Desktop Programmer (DP1-AAAA)
- Ascom WinPDM Version 3.8.1 oder höher
- Softwarestand 2.1.20 oder höher
- Parameterversion 13.3 oder höher

5.4.2 Konfiguration

5.4.2.1 Neues Telefon anlegen

(1) Öffnen Sie das Ascom WinPDM-Programm.

(2) Zum Anlegen eines neuen Teilnehmers gehen Sie zu **Numbers** -> **New**.

(3) Tragen Sie in das Feld **Call number** die SIP-Rufnummer ein, z. B. *2011*.

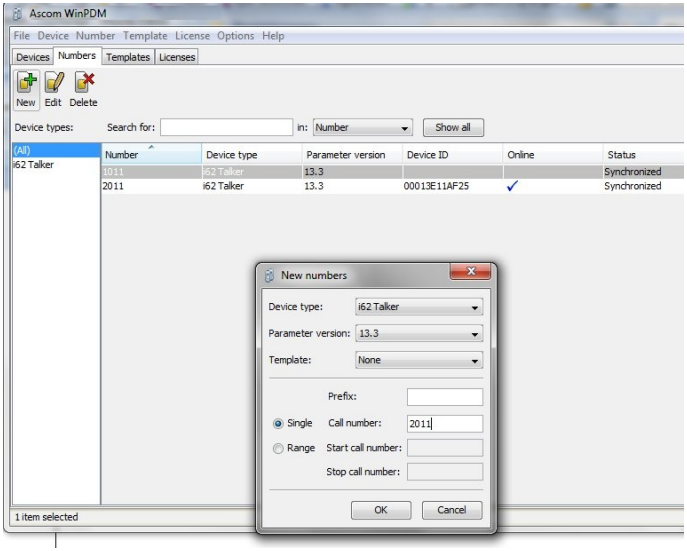


Abb. 76: **Numbers** -> **New**

Netzwerk definieren

Beim **Ascom i62** kann man vier WLAN-Netzwerke (Network A bis D) definieren.

Gehen Sie zu **Network** -> **Network B**.

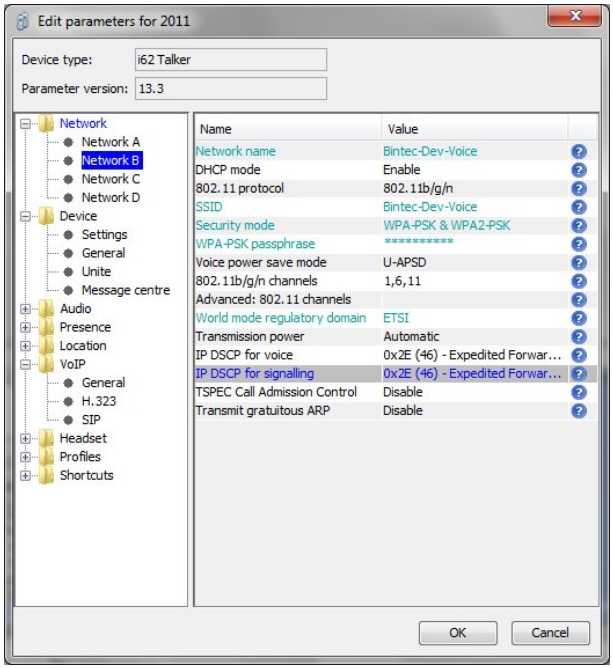


Abb. 77: **Network** -> **Network B**

Zum Betrieb sind folgende Einträge nötig:

Name	Wert
DHCP mode	Enable
SSID	Bintec-Dev_Voice
Security mode	WPA-PSK & WPA2-PSK
WPA-PSK passphrase	z. B. supersecret
Voice power save mode	U-APSD
802.11b/g/n channels	1, 6, 11
IP DSCP for voice	0x2E (46)
IP DSCP for signaling	0x2E (46)

Geräte-Einstellungen

Gehen Sie zu **Device** -> **Settings**.

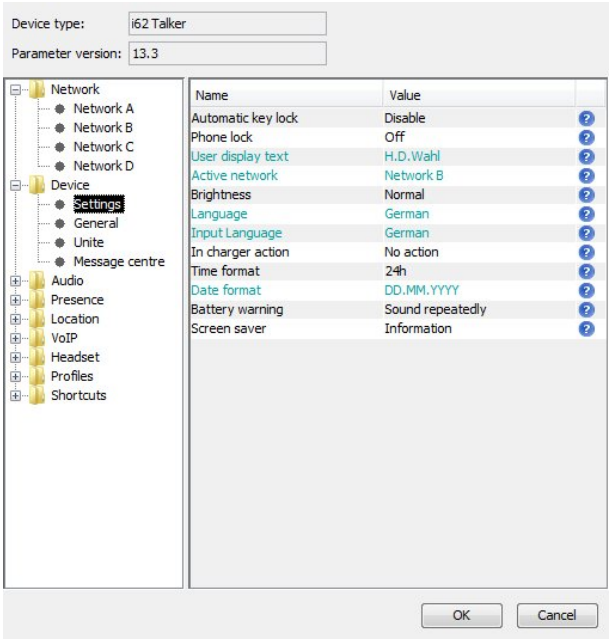


Abb. 78: **Device** -> **Settings**

Zum Betrieb sind folgende Einträge nötig:

Name	Wert
User display text	z. B. bintec elmeg
Active Network	Network B

Allgemeine Geräte-Einstellungen

Gehen Sie zu **Device** -> **General**.

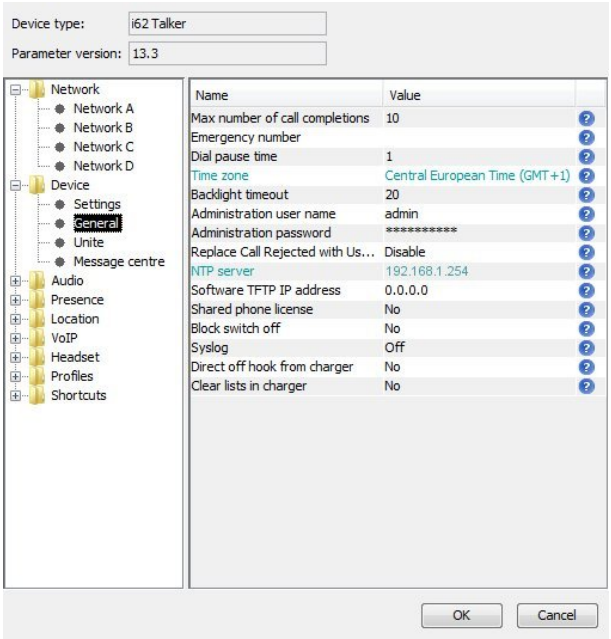


Abb. 79: **Device** -> **General**

Zum Betrieb sind folgende Einträge nötig:

Name	Wert
Time zone	Central European Time (GMT+1)
NTP server	192.168.1.254

Allgemeine VoIP-Einstellungen

Gehen Sie zu **VoIP** -> **General**.

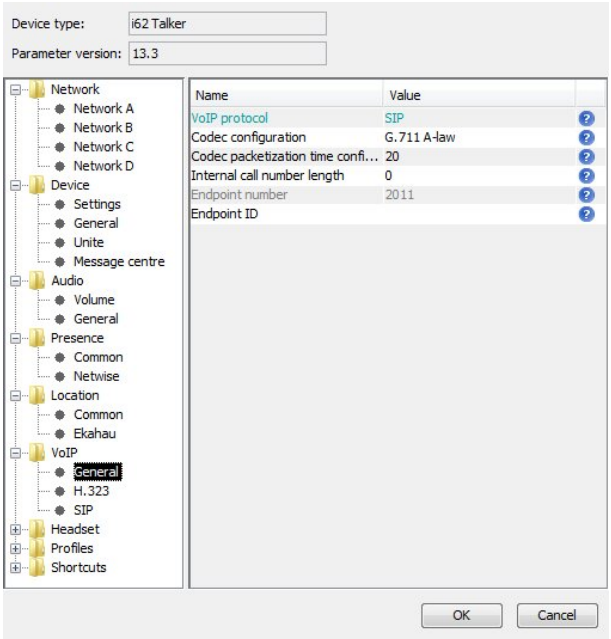


Abb. 80: **VoIP** -> **General**

Zum Betrieb sind folgende Einträge nötig:

Name	Wert
VoIP protocol	SIP
Endpoint number	Stellt die Rufnummer des Gerätes dar und ist hier nicht veränderbar. Die Rufnummer wird bereits bei Erzeugung des Geräte-parametersatzes festgelegt.

SIP-Konfiguration

Gehen Sie zu **VoIP** -> **SIP**.

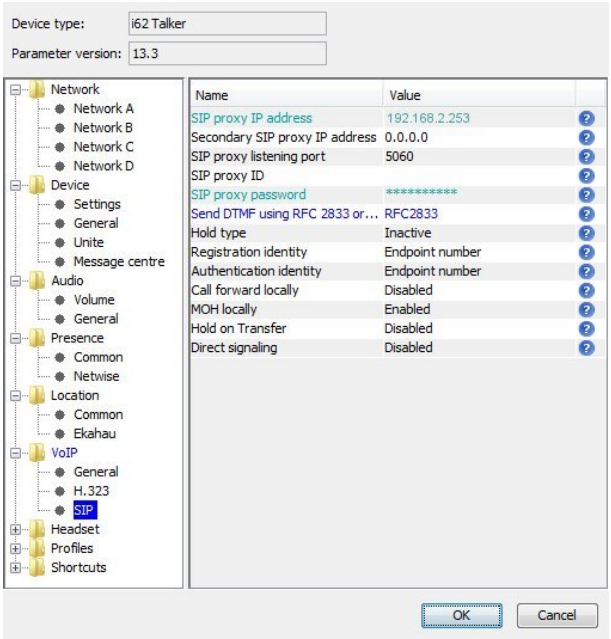


Abb. 81: **VoIP** -> **SIP**

Zum Betrieb sind folgende Einträge nötig:

Name	Wert
SIP proxy IP address	192.168.2.253
SIP proxy password	z. B. supersecret
Authentication identity	Endpoint number (die Rufnummer wird als SIP username verwendet)

5.4.3 Testbefehle am Ascom i62

Das **Ascom i62** hat einige Testbefehle die bei der Installation und Fehlersuche hilfreich sind:

*#76# Schaltet die RSSID-Anzeige ein/aus

*#77# Schaltet die Site Survey Tools ein

5.5 Konfiguration der bintec be.IP plus

5.5.1 Konfiguration

Für das VoWLAN-Telefon muss ein SIP-Teilnehmer eingerichtet werden. Die unbedingt notwendige Einstellung des DSCP-Wertes auf 0x2E / 101110 / 46 ist bereits als Standard-Einstellung berücksichtigt, so dass hier keine Änderung notwendig ist.

Die Netzwerkschnittstelle der **bi.IP plus** muss in unserem Anwendungsbeispiel mit **VLAN-ID** *10* getaggt werden.

Um auf die Konfigurationsoberfläche zu gelangen, geben Sie im Web-Browser die IP-Adresse der **bi.IP plus** an.

Gehen Sie zu **LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **Neu**.

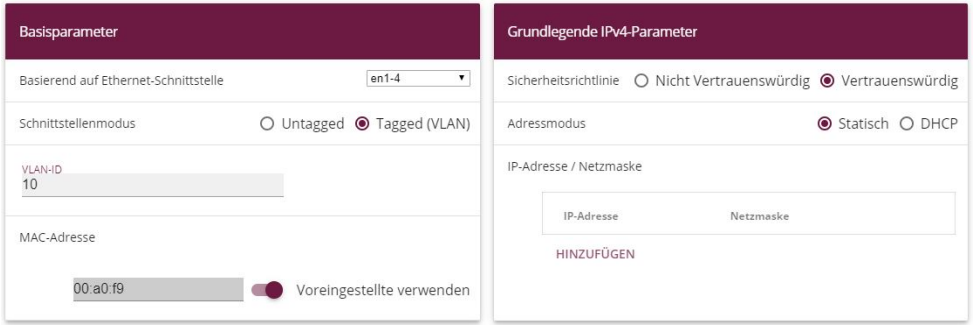


Abb. 82: **LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Bei **Basierend auf Ethernet-Schnittstelle** wählen Sie die virtuelle Schnittstelle aus, z. B. *en1-4*.

(2) Bei **Schnittstellenmodus** wählen Sie *Tagged (VLAN)* aus.

(3) Bei **VLAN-ID** geben Sie *10* ein.

(4) Bestätigen Sie mit **OK**.

5.5.2 Betriebsfall: WLAN-Telefon nicht erreichbar

Ein Ruf auf das WLAN-Telefon kann fehlschlagen, wenn der Teilnehmer sich zum Beispiel außerhalb der Reichweite eines Access Points befindet, das Telefon ausgeschaltet ist oder wenn der Akku leer ist. Damit dennoch keine Rufe verloren gehen ist es sinnvoll, eine **Anrufweiterschaltung (AWS)** *Bei Besetzt/Bei Nichtmelden* in der **bi.IP plus** für die betreffende Nebenstelle einzurichten.

Gehen Sie zu **Anrufkontrolle** -> **Ausgehende Dienste** -> **Anrufweiterschaltung (AWS)** -

> **Neu**.

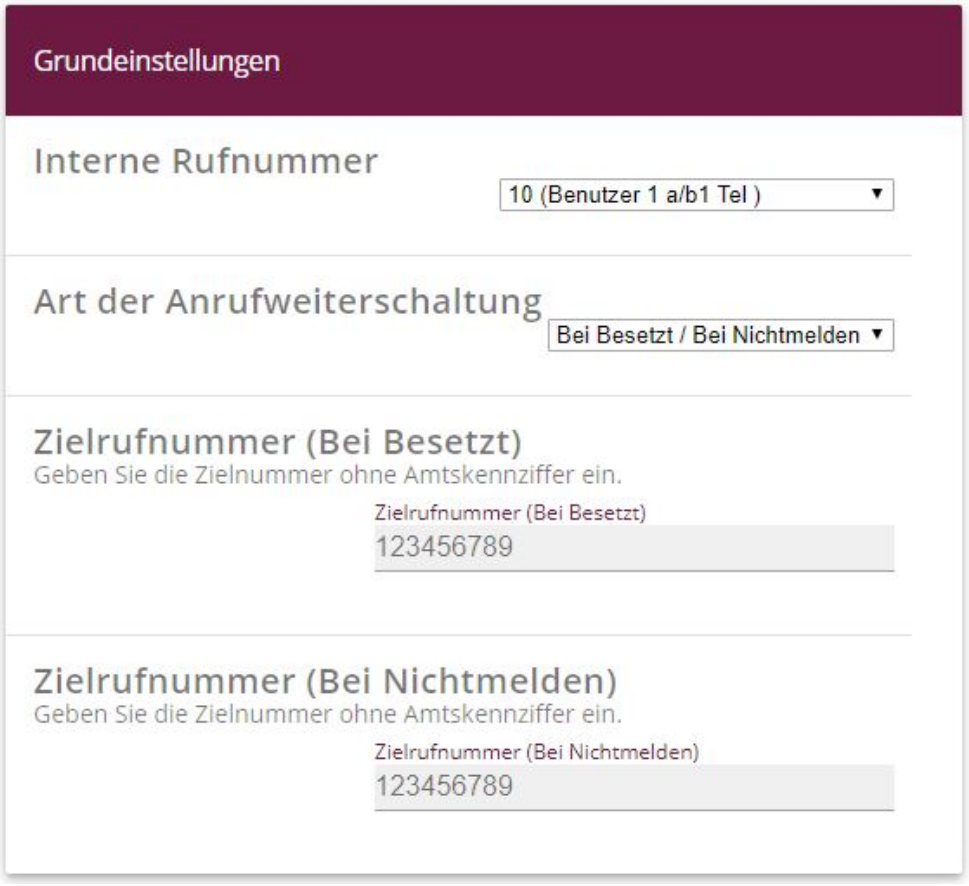


Abb. 83: **Anrufkontrolle** -> **Ausgehende Dienste** -> **Anrufweiterschaltung (AWS)** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie eine **Interne Rufnummer** aus, für die kommende Anrufe weitergeschaltet werden sollen.

(2) Bei **Art der Anrufweiterschaltung** wählen Sie *Bei Besetzt/Bei Nichtmelden* aus.

(3) Geben Sie eine **Zielrufnummer** ein, auf die kommende Anrufe bei Besetzt oder bei Nichtmelden weitergeschaltet werden sollen.

(4) Bestätigen Sie mit **OK**.

5.6 Verwendung anderer WLAN-Telefone

Neben dem von uns zertifizierten und empfohlenen **Ascom i62** VoWLAN-Endgerät können natürlich auch Geräte anderer Anbieter verwendet werden. Auch Smart Phones, wie z. B. ein **Apple iPhone**, sind einsetzbar. Leider gibt es jedoch hier kleine Unterschiede in der Performance, so haben einige Geräte kein U-APSD implementiert oder die Roaming Performance lässt zu wünschen übrig.

Mit den hier aufgeführten Geräten haben wir gute Ergebnisse erzielt:

- **Apple iPhone 4** mit bintec SIP APP (kein U-APSD)
- **Nokia 6710**

5.7 Konfigurationsschritte im Überblick

Funkmodulprofile konfigurieren

Aktion	Menü	Wert
Betriebsmodus	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Funkmodulprofile** -> **Neu**	*Access-Point*
Frequenzband	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Funkmodulprofile** -> **Neu**	*2,4 GHz In/Outdoor*
Anzahl der Spatial Streams	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Funkmodulprofile** -> **Neu**	*2*
Drahtloser Modus	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Funkmodulprofile** -> **Neu**	*802.11 g/n*
Max. Übertragungsrate	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Funkmodulprofile** -> **Neu**	*Auto*

Funkmodulprofile konfigurieren

Aktion	Menü	Wert
Netzwername (SSID)	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)** -> **Neu**	z. B. *Bintec-Dev-Voice*
Intra-cell Repeating	**Wireless LAN Controller** -> **Slave-**	*Deaktiviert*

Aktion	Menü	Wert
	AP-Konfiguration -> **Drahtlosnetzwerke (VSS)** -> **Neu**	
Sicherheitsmodus	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)** -> **Neu**	*WPA-PSK*
WPA-Modus	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)** -> **Neu**	*WPA2*
WPA2 Cipher	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)** -> **Neu**	*AES und TKIP* aktiviert
Preshared Key	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)** -> **Neu**	z. B. *supersecret*
ACL-Modus	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)** -> **Neu**	*Deaktiviert*
VLAN-ID	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)** -> **Neu**	*10*

Ascom i62 konfigurieren

Feld	Menü	Wert
Call number	**Numbers** -> **New**	z. B. *2011*
DHCP mode	**Network** -> **Network B**	*Enable*
SSID	**Network** -> **Network B**	z. B. *Bintec-Dev-Voice*
Security mode	**Network** -> **Network B**	*WPA-PSK & WPA2-PSK*
WPA-PSK passphase	**Network** -> **Network B**	z. B. *supersecret*
Voice power save mode	**Network** -> **Network B**	*U-APSD*
802.11b/g/n channels	**Network** -> **Network B**	*1,6,11*
IP DSCP for voice = 0x2E (46)	**Network** -> **Network B**	*0x2E (46)*
IP DSCP for signaling = 0x2E (46)	**Network** -> **Network B**	*0x2E (46)*
User display text	**Device** -> **Settings**	z. B. *bintec elmeg*

Feld	Menü	Wert
Active network	**Device -> Settings**	*Network B*
Time zone	**Device -> General**	*Central European Time (GMT+1)*
NTP server	**Device -> General**	z. B. *192.168.1.254*
VoIP protocol	**VoIP -> General**	SIP
SIP proxy IP address	**VoIP -> SIP**	z. B. *192.168.2.253*
SIP proxy password	**VoIP -> SIP**	z. B. *supersecret*
Authentication identity	**VoIP -> SIP**	*Endpoint number*

Schnittstelle konfigurieren

Feld	Menü	Wert
Basierend auf Ethernet-Schnittstelle	**LAN -> IP-Konfiguration -> Schnittstellen -> Neu**	z. B. *en1-4*
Schnittstellenmodus	**LAN -> IP-Konfiguration -> Schnittstellen -> Neu**	*Tagged (VLAN)*
VLAN-ID	**LAN -> IP-Konfiguration -> Schnittstellen -> Neu**	*10*

Anrufweiterschaltung konfigurieren

Feld	Menü	Wert
Interne Rufnummer	**Anrufkontrolle -> Ausgehende Dienste -> Anrufweiterschaltung (AWS) -> Neu**	Interne Nummer
Art der Anrufweiterschaltung	**Anrufkontrolle -> Ausgehende Dienste -> Anrufweiterschaltung (AWS) -> Neu**	*Bei Besetzt/Bei Nichtmelden*
Zielnummer (Bei Besetzt)	**Anrufkontrolle -> Ausgehende Dienste -> Anrufweiterschaltung (AWS) -> Neu**	Zielnummer
Zielnummer (Bei Nichtmelden)	**Anrufkontrolle -> Ausgehende Dienste -> Anrufweiterschaltung (AWS) -> Neu**	Zielnummer

Kapitel 6 WLAN - Management für mehrere Standorte: WLAN Controller über VPN

6.1 Einleitung

Im Folgenden wird die Konfiguration eines bintec-Routers der **RS**-Serie als zentraler WLAN Controller für eine über mehrere Standorte verteilte WLAN-Infrastruktur (**bintec W2003ac**-Access-Points) beschrieben. Ein bintec-Router der **RS**-Serie dient dabei am jeweiligen Standort als Gateway für den Internetzugang.

Zur Konfiguration wird das **GUI** (Graphical User Interface) verwendet.

Aufgabenprofil des Workshops:

- Mehrere Standorte eines Unternehmens sollen mit WLAN ausgestattet werden. Das WLAN soll anschließend allen Mitarbeitern zur Verfügung stehen und zentral verwaltet werden können.
- Die Geräte der Mitarbeiter sollen automatisch per DHCP in das Firmennetzwerk integriert werden.
- Die Mitarbeiter sollen über das WLAN sowohl auf das Internet als auch auf das Intranet der Firma zugreifen können. Der Zugang zum Firmenintranet in der Zentrale sowie in den Außenstellen erfolgt dabei über das Internet mittels eines durch IPSec-gesicherten VPNs.

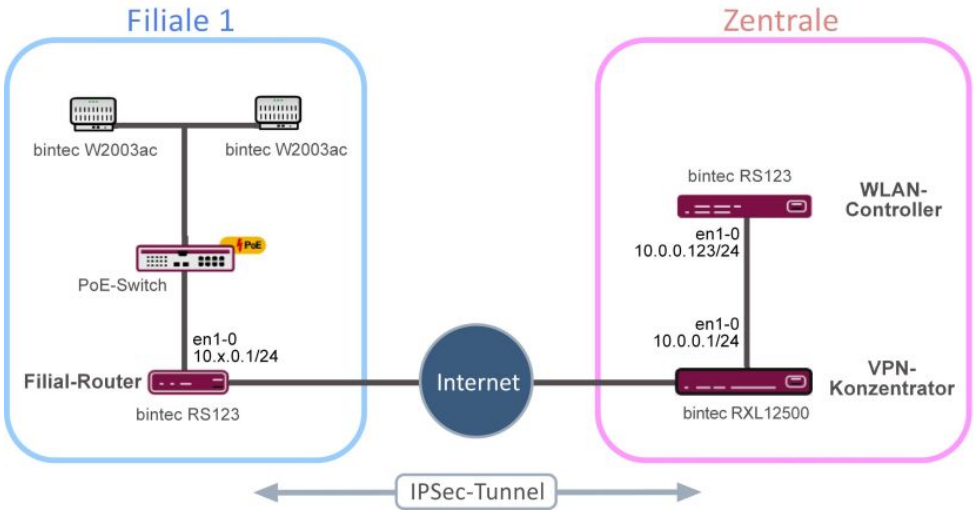


Abb. 84: Beispielszenario

6.1.1 Voraussetzungen

In der Firmenzentrale:

- Zwei bintec-Router der **RS**- oder **RXL**-Serie, **bintec be.IP** oder **be.IP plus** deren Firmware-Version mindestens **10.1.9** entspricht.

  Im Workshop wird exemplarisch ein **bintec RS123** als WLAN-Controller und ein **bintec RXL12500** als VPN-Konzentrator verwendet.

In der Filiale:

- Ein bintec-Router mit einer Firmware, die mindestens der Version **10.1.9** entspricht. Für den Internetzugang der Filiale können Router der **RS**-Serie, be.IP oder be.IP plus verwendet werden.

  Im Beispiel wird ein **bintec RS123** als Filialrouter eingesetzt.

- Ein oder mehrere bintec-Access-Points der Geräteklassen **bintec W2003ac** oder **bintec WI1003n** mit mindestens Firmware-Version **10.1.9**. Die minimal benötigte Anzahl an Access Points richtet sich nach der Größe und Gebäudestruktur des Firmenstandorts und kann durch eine im Vorfeld erfolgte WLAN-Ausleuchtung genau festgelegt werden. Für zusätzliche Informationen lesen Sie bitte in *WLAN - Einführung in den bintec-WLAN-Controller* auf Seite 104 nach.

  In diesem Workshop werden für den Fall einer Beispielfiliale vier **bintec W2003ac**-Access-Points verwendet.

- Ein Internetzugang

- Ein PoE-Switch für die Access Points (optional).

6.1.2 Hinweise zum Test-Setup

An dieser Stelle finden Sie eine Übersicht hinsichtlich der Belegung der Schnittstellen in den einzelnen Routern.

Router	Schnittstelle	Beschreibung	IP-Adresse / -Adressbereich
Router der x-ten Filiale	en1-0	LAN-Anbindung der Filiale	10.x.0.1/24
	en1-0	DHCP-Server für Access Points und WLAN-Geräte der Filiale	10.x.0.10 bis 10.x.0.254
VPN-Konzentrator in der Zentrale	en1-0	LAN-Anbindung der Zentrale	10.0.0.1/24
WLAN-Controller in der Zentrale	en1-0	IP-Adresse des WLAN-Controllers, die im gesamten VPN erreichbar sein muss	10.0.0.123/24
	en1-0	Standardroute auf den VPN-Konzentrator	10.0.0.1
	en1-0	WLAN-Controller für alle Access Points aller Filialen	

6.2 Konfiguration

6.2.1 Voreinstellungen

Im Vorfeld muss zwischen dem VPN-Konzentrator in der Zentrale (im Workshop **bintec RXL12500**) und einem Filialrouter oder mehreren Filialroutern (im Workshop **bintec RS123**) ein funktionierendes VPN eingerichtet werden. Zur Installation eines VPN verweisen wir Sie auf den IP-Workshop "Routing-Protokoll RIPv2 über IPSec-Verbindung". In den Einstellungen dieses Workshops müssen Sie die IP-Adressbereiche der jeweiligen LAN-Segmente durch die Werte aus der obigen Tabelle ersetzen. Die restlichen Einstellungen belassen Sie bitte unverändert.

Die Verwendung von RIPv2 bietet Ihnen folgende Vorteile:

- Alle oben aufgeführten Router für den Einsatz in der Filiale können eingesetzt werden.
- Die verwendeten Geräte sind verhältnismäßig leicht einzurichten.
- Die Konfiguration kann im laufenden Betrieb problemlos um neue Standorte erweitert werden.

6.2.2 Konfiguration des Routers in der Außenstelle

6.2.2.1 IP-Konfiguration

Ergänzend zum IP-Workshop "Routing-Protokoll RIPv2 über IPSec-Verbindung" wird die IP-Schnittstelle des ersten Filialrouters folgendermaßen konfiguriert.

(1) Gehen Sie in das Menü **LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>** .

Abb. 85: **LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie bei **Adressmodus** `Statisch` aus.

(2) Tragen Sie im jeweiligen Feld die **IP-Adresse / Netzmaske** z. B. `10.1.0.1` des ersten Filialrouters ein. Die IP-Adressen für die zweite, dritte, usw. Filiale lauten folglich `10.2.0.1`, `10.3.0.1`, usw. Als **Netzmaske** wählen Sie in diesem Fall

255.255.255.0.

(3) Belassen Sie den **Schnittstellenmodus** auf *Untagged*.

(4) Belassen Sie den Haken bei der **MAC-Adresse** für *Voreingestellte verwenden*.

(5) Bestätigen Sie mit **OK**.

6.2.2.2 DHCP-Pool konfigurieren

Anschließend müssen Sie einen DHCP-Pool auf der entsprechenden Schnittstelle für alle Geräte im LAN, wie die Slave-Access-Points oder die später über das WLAN angebundenen Mitarbeitergeräte, anlegen.

(1) Gehen Sie dazu in das Menü **Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu**.

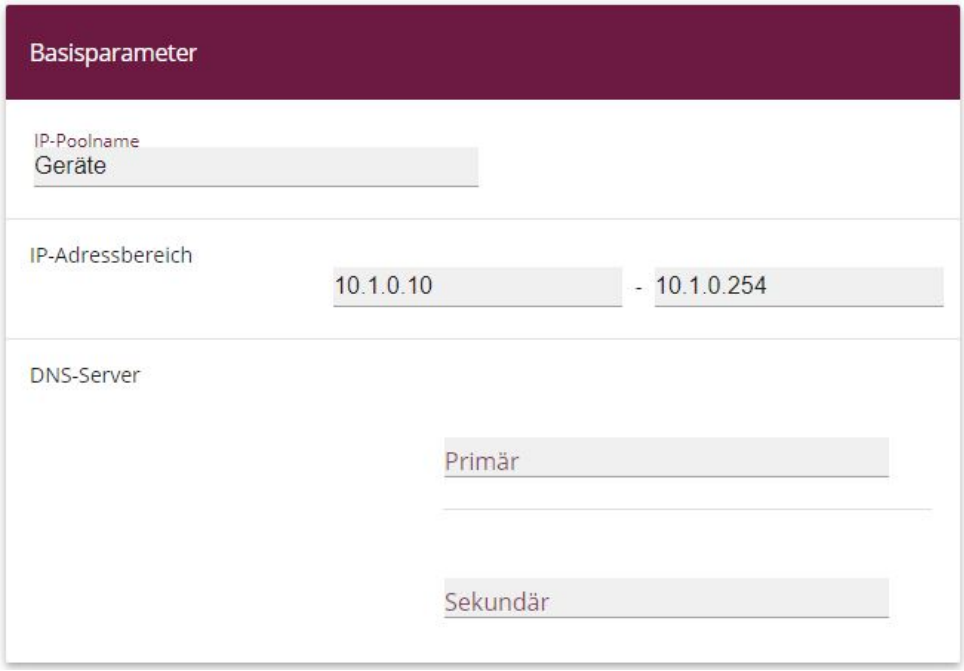


Abb. 86: **Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Für den **IP-Poolnamen** können Sie z. B. *Geräte* verwenden.

(2) Für den **IP-Adressbereich** des ersten Filialrouters verwenden Sie z. B. *10.1.0.10* bis *10.1.0.254*. Dadurch sind in diesem Fall noch acht Adressen unterhalb von 10.1.0.10 für weitere statisch konfigurierte Geräte im selben Netz frei.

(3) Bestätigen Sie Ihre Eingaben mit **OK**.

Im Menü **Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu** können Sie nun die weitere Konfiguration vornehmen.

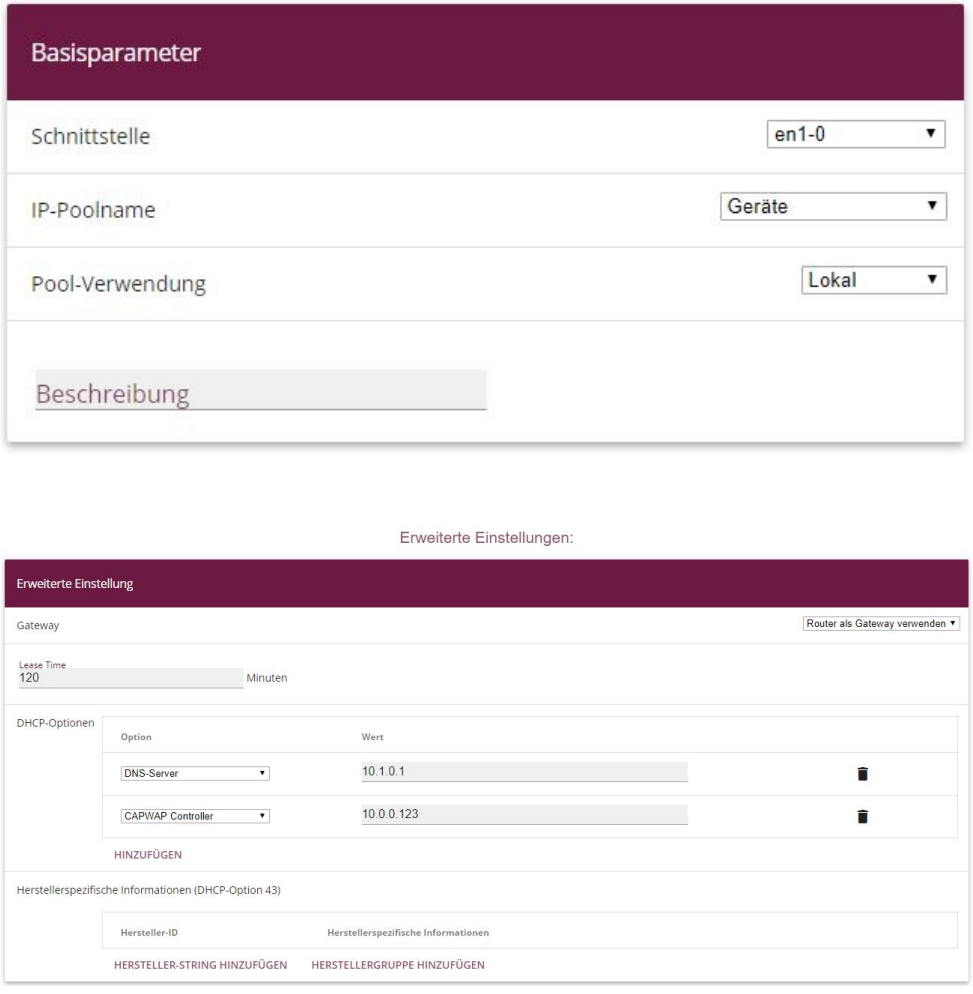


Abb. 88: **Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie die **Schnittstelle** `en1-0` aus.

(2) Wählen Sie einen gültigen **IP-Pool** aus, hier z. B. `Geräte`.

(3) Die **Pool-Verwendung** wird auf `Lokal` gesetzt.

(4) Klicken Sie auf **Erweiterten Einstellungen**.

(5) Dort wird unter **Gateway** die Einstellung `Router als Gateway verwenden` beibehalten. Dadurch erreichen alle DHCP-fähigen Geräte im Netzwerk das Standard-Gate-

way unter der momentanen IP-Adresse der Schnittstelle en1-0.

(6) Die **Lease Time** wird auf *120* Minuten eingestellt.

(7) Bei **DHCP-Optionen** klicken Sie auf **Hinzufügen**.

(8) Legen Sie als erstes die IP-Adresse des DNS-Server fest. Wählen Sie dazu unter **Option** *DNS-Server* aus und tragen Sie unter **Wert** die IP-Adresse der Schnittstelle *en1-0* z. B. *10.1.0.1* ein.

(9) Klicken Sie auf **Hinzufügen**.

(10) Wählen Sie unter **Option** *CAPWAP-Controller* aus und tragen Sie unter **Wert** die IP-Adresse des WLAN-Controllers in der Zentrale ein, in unserem Fall also *10.0.0.123*.

(11) Bestätigen Sie Ihre Eingaben mit **OK**.

Hinweis

Die Einrichtung weiterer DHCP-Optionen ist für die Slave-Access-Points und WLAN-Geräte nicht zwingend notwendig. Die Konfiguration des *DNS-Domänenname*, *Zeitserver* , usw. kann aber hilfreich sein und richtet sich nach der vorgegebenen Infrastruktur.

Hinweis

Es wird nicht empfohlen, auf dem Filialrouter an Stelle des lokalen DHCP-Servers ein sogenanntes **DHCP-Relay** zu einem in der Zentrale befindlichen DHCP-Server einzurichten. Denn dann ist in der Zentrale nicht mehr unmittelbar über den IP-Adressbereich der Slave-Access-Points und der Mitarbeitergeräte ersichtlich, in welcher Filiale sich das jeweilige Gerät befindet. Darüber hinaus könnten sich bei einem Einsatz von **DHCP-Relay** und dem Ausfall des Internetzugangs oder des VPNs die Mitarbeitergeräte nicht mehr in das lokale Netz des jeweiligen Standorts einbuchen, da sie keine IP-Adresse mehr per DHCP erhalten.

Die Konfiguration des Filialrouters ist somit abgeschlossen. Speichern Sie die Konfiguration mit **Konfiguration speichern** und bestätigen Sie die Auswahl mit **OK**.

6.2.3 Konfiguration des VPN-Konzentrators in der Zentrale

Ergänzend zum IP-Workshop "Routing-Protokoll RIPv2 über IPSec-Verbindung" wird die IP-Schnittstelle des VPN-Konzentrators in der Zentrale wie folgt eingerichtet.

(1) Gehen Sie in das Menü **LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>** .

Abb. 89: **LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie für den **Adressmodus** `Statisch` aus.

(2) Tragen Sie im Feld die **IP-Adresse** z. B. `10.0.0.1` und die **Netzmaske** `255.255.255.0` ein.

(3) Belassen Sie den **Schnittstellenmodus** auf `Untagged`.

(4) Bestätigen Sie mit **OK**.

6.2.4 Konfiguration des WLAN-Controllers in der Zentrale

6.2.4.1 IP-Konfiguration

Zuerst werden die IP-Parameter des WLAN-Controllers eingestellt.

(1) Gehen Sie zu **LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>**.

Abb. 90: **LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie für den **Adressmodus** `Statisch` aus.

(2) Tragen Sie im Feld die **IP-Adresse** z. B. `10.0.0.123` und die **Netzmaske**

`255.255.255.0` ein.

(3) Belassen Sie den **Schnittstellenmodus** auf `Untagged`.

(4) Bestätigen Sie mit **OK**.

6.2.4.2 Einrichtung der Standardroute

Anschließend wird auf dem WLAN-Controller die Standardroute über die Schnittstelle `en1-0` zur IP-Adresse des VPN-Konzentrators eingerichtet.

(1) Gehen Sie zu **Netzwerk** -> **Routen** -> **Konfiguration von IPv4-Routen** -> **Neu**.

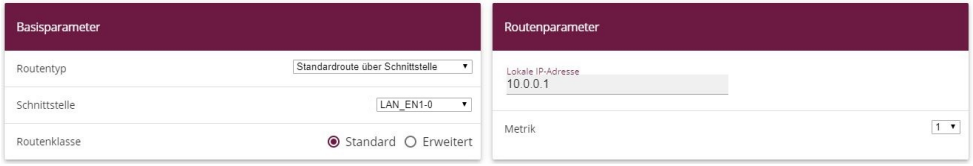


Abb. 91: **Netzwerk** -> **Routen** -> **Konfiguration von IPv4-Routen** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Den **Routentyp** setzen Sie auf `Standardroute über Schnittstelle`.

(2) Als **Schnittstelle** wählen Sie `LAN_EN1-0`.

(3) Geben Sie unter **Lokale IP-Adresse** die IP-Adresse des Hosts ein, an die Ihr Gerät die IP-Pakete weitergeben soll, hier die LAN-IP-Adresse `10.0.0.1` des VPN-Konzentrators.

(4) Setzen Sie die **Metrik** der Route z. B. auf `1`, um die Priorität der Route zu wählen. Je niedriger Sie den Wert setzen, desto höhere Priorität besitzt die Route.

(5) Bestätigen Sie ihre Eingaben mit **OK**.

Die Übersicht der IP-Routen sieht im Anschluss folgendermaßen aus:

Abb. 92: **Netzwerk** -> **Routen** -> **Konfiguration von IPv4-Route**

Die VPN-Konzentrator-Konfiguration ist somit abgeschlossen. Speichern Sie die Konfiguration mit **Konfiguration speichern** und bestätigen Sie die Auswahl mit **OK**.

6.2.4.3 WLAN-Controller konfigurieren

Nun kann der eigentliche WLAN-Controller aktiviert werden.

(1) Gehen Sie zu **Wireless LAN Controller** -> **Controller-Konfiguration** -> **Allgemein**.

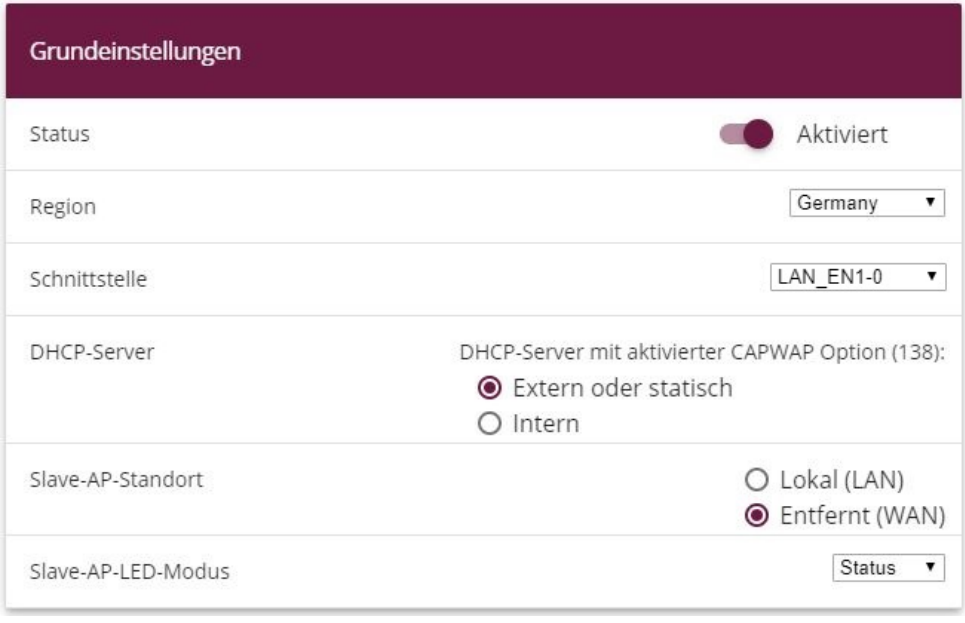


Abb. 93: **Wireless LAN Controller** -> **Controller-Konfiguration** -> **Allgemein**

Gehen Sie folgendermaßen vor:

(1) Die **Region** muss passend zum Standort der Access Points eingerichtet werden, z. B. `Germany`. Diese Einstellung bewirkt den Betrieb des WLAN-Funkmoduls der Access Points nur innerhalb des gesetzlich erlaubten Rahmens des jeweiligen Landes.

(2) Als **Schnittstelle** des WLAN-Controllers wird `LAN_EN1-0` ausgewählt.

(3) Die **DHCP-Server**-Einstellung muss auf `Extern oder statisch` belassen werden, da der DHCP-Server bereits auf den Filialroutern eingerichtet wurde.

(4) Der **Slave-AP-Standort** muss auf `Entfernt (WAN)` geändert werden. Dies hat zur Folge, dass verwaltete Slave-Access-Points bei einem eventuellen Netzwerkausfall autonom weiterlaufen (und somit wenigstens das lokale WLAN des betroffenen Standorts weiterhin funktioniert) und erst nach erneuter Verbindung zum WLAN-Controller reinitialisiert werden. Ebenso werden mit diesem Schalter wechselseitige Wartezeiten von Slave-Access-Points und WLAN-Controller an typische Gegebenheiten von WANs angepasst (zum Beispiel kurze Netzunterbrechungen durch DSL-Zwangstrennung).

(5) Bestätigen Sie mit **OK**.
Die Einstellungen sind jetzt aktiv und der WLAN Controller wird gestartet.

6.2.4.4 Drahtlosnetzwerk-Profil konfigurieren

Anschließend wird das standardmäßig vorhandene Profil für ein **Drahtlosnetzwerk (VSS)** wie folgt modifiziert.

(1) Gehen Sie zu **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)**.

Klicken Sie dazu bei dem vorhandenen Eintrag **<vss-1>** auf das -Symbol.

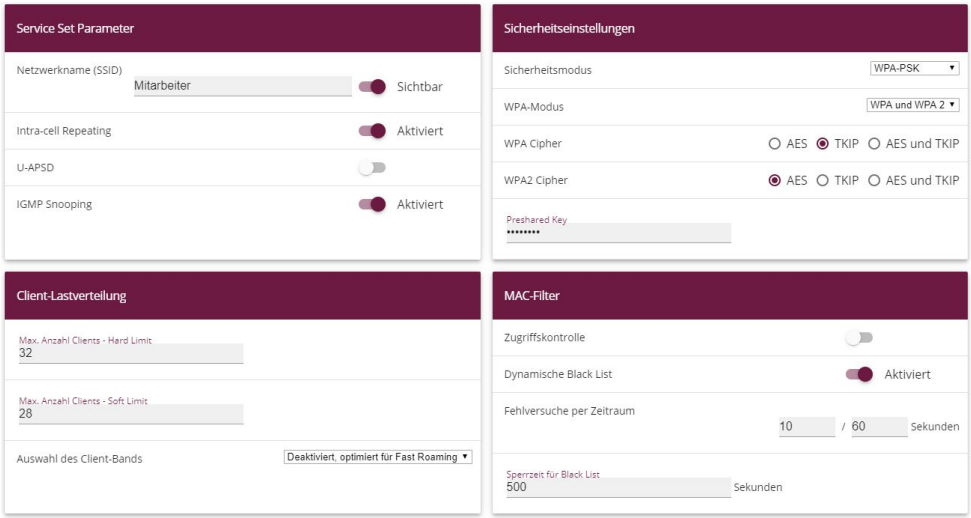


Abb. 94: **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)** -> **<vss-1>**

Gehen Sie folgendermaßen vor:

(1) Der **Netzwerkname (SSID)** wird z. B. auf `Mitarbeiter` geändert.

(2) Für **Intra-cell Repeating** und **Max. Clients** werden die Standardeinstellungen belassen.

(3) Als **Sicherheitsmodus** wählen Sie `WPA-PSK` aus.

(4) Daraufhin können Sie den **WPA-Modus** auf `WPA und WPA 2` belassen.

(5) Bei **WPA-Cipher** wird `TKIP` und bei **WPA2-Cipher** `AES` aktiv gesetzt.

(6) Das **Preshared Key** ist das WLAN-Zugangspasswort für alle Mitarbeiter. Geben Sie eine ASCII-Zeichenfolge mit 8 - 63 Zeichen ein.

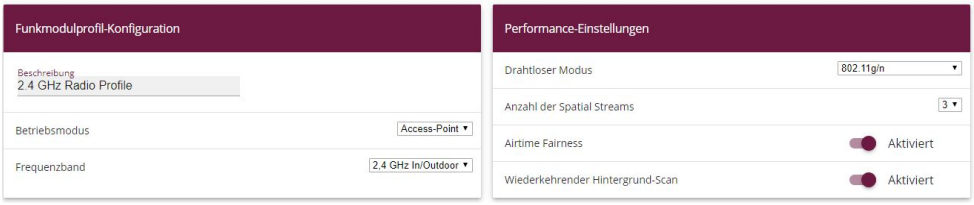
(7) Bestätigen Sie mit **OK**.

6.2.4.5 Funkmodulprofile konfigurieren

Im nächsten Schritt werden die **Funkmodulprofile** bearbeitet. Konfigurieren Sie die **Funkmodulprofile**, indem Sie den Standardeintrag bearbeiten.

(1) Gehen Sie zu **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Funkmodulprofile**.

(2) Klicken Sie bei dem vorhandenen Eintrag **<2.4 GHz Radio Profile>** auf das -Symbol.



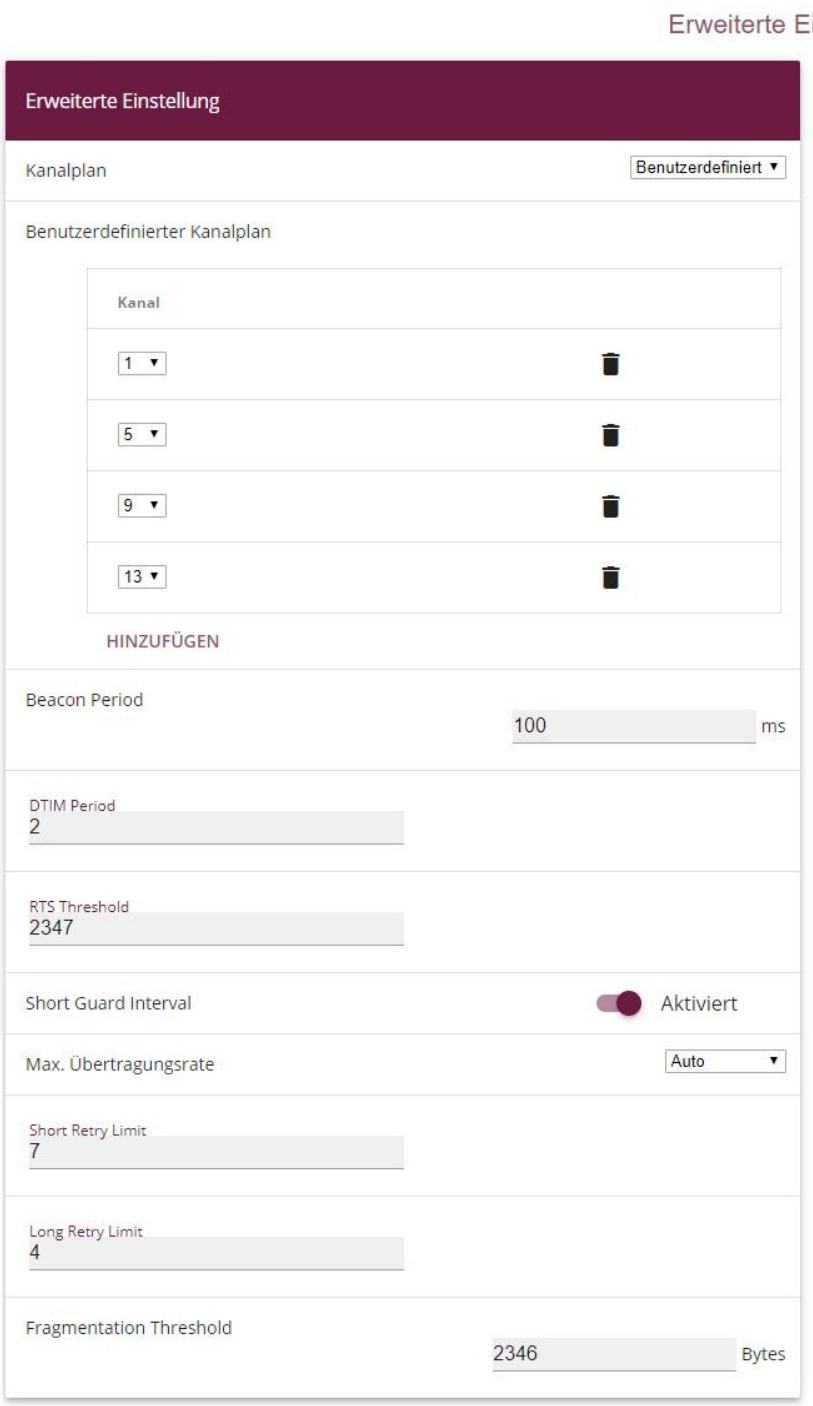


Abb. 96: **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Funkmodulprofile** ->

>2.4 GHz Radio Profile> 

Gehen Sie folgendermaßen vor:

(1) Das **Frequenzband** des Funkmodulprofils wird auf *2,4 GHz In/Outdoor* belassen.

(2) Ändern Sie den **Drahtlosen Modus** auf *802.11g/n*.

Hinweis

Die Änderung des Drahtlosmodus bewirkt, dass veraltete WLAN-Geräte, die nur auf dem 802.11b-Übertragungsstandard beruhen, das WLAN nicht mehr nutzen können. Der größte Vorteil dieser Maßnahme ist jedoch die Vermeidung einer automatischen Reduktion der Bandbreite, sobald ein 802.11b-Gerät angeschlossen wird.

(3) Aktivieren Sie die Option **Burst-Mode**, um die Übertragungsgeschwindigkeit zu erhöhen.

(4) Klicken Sie auf **Erweiterte Einstellungen**.

(5) Wählen Sie den gewünschten **Kanalplan** aus. Mit *Benutzerdefiniert* können Sie die gewünschten Kanäle selbst auswählen.

(6) Unter **Benutzerdefiniert** wählen Sie als erlaubten Kanäle *1*, *5*, *9* und *13* aus. Dieser Kanalplan ist für alle Länder in denen die Kanäle 1 bis 13 erlaubt sind als optimaler Kanalplan empfohlen und hat bei 802.11g/n keine (nennenswerte) Frequenzüberlappung. Die Access Points haben somit mehr Auswahlmöglichkeiten einen möglichst störungsfreien Kanal zu nutzen, was die Leistungsfähigkeit und Zuverlässigkeit des gesamten WLANs steigert.

(7) Aktivieren Sie die Funktion **Short Guard Interval**, um das Guard Interval (= Zeit zwischen der Übertragung von zwei Datensymbolen) von 800 ns auf 400 ns zu verkürzen.

(8) Die restlichen Einstellungen bleiben unverändert und das Konfigurationsmenü wird mit **OK** gespeichert und verlassen.

Somit sind alle benötigten Profile im WLAN-Controller eingerichtet.

6.2.4.6 Access Points konfigurieren

Jetzt werden die Access Points aktiviert und eingerichtet.

(1) Gehen Sie zu **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Slave Access Points**.

In dieser Übersicht sollten alle vorhandenen Access Points als *Gefunden* markiert sein. Sollte dies nicht der Fall sein, empfiehlt es sich, nochmals die DHCP-Server-Einstellungen auf dem Filialrouter zu überprüfen. Insbesondere sollte kontrolliert werden, ob die CAPWAP-Option korrekt eingerichtet ist. Auch die VPN-Netzwerkverbindung von der Zentrale

in die Filiale kann eine mögliche Fehlerursache sein. Sofern diese Fehlerquellen ausgeschlossen werden können, kann ein versehentlich aktivierter DHCP-Server auf einem Gerät in der Filiale die Störung verursachen. Dieser Server muss deaktiviert und alle Access Points in der Filiale vom Stomnetz getrennt werden, um eine neue Netzwerkkonfiguration vom DHCP-Server zu beziehen. Alternativ kann auch der Ablauf der sogenannten DHCP-Lease-Time abgewartet werden.

Jetzt können die zuvor konfigurierten Funk- und VSS-Profile auf den gefundenen Access Points eingerichtet werden. Im Folgenden wird die Anpassung eines Access Points für den Standort "Nbg - Geschäft" beschrieben.

(1) Gehen Sie zu **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Slave Access Points** .

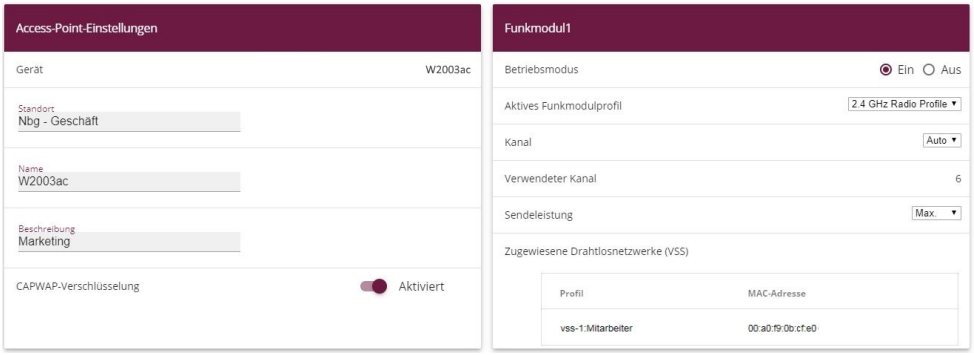


Abb. 97: **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Slave Access Points**

Gehen Sie folgendermaßen vor:

(1) Als **Standort** wird eine möglichst eindeutige Bezeichnung vergeben, z. B. *Nbg - Geschäft*.

(2) Der **Betriebsmodus** des Funkmoduls muss zwingend auf *Ein* belassen werden. Damit wird der Betriebsmodus vom verwendeten Funkmodulprofil bestimmt.

(3) Als nächstes wird als **Aktives Funkmodulprofil** hier das zuvor konfigurierte *2.4 GHz Radio Profile* ausgewählt.

(4) Der **Kanal** wird auf *Auto* belassen und wird somit anhand des Kanalplans des Funkprofils sowie der WLAN-Umgebung dynamisch bestimmt.

(5) Zuletzt wird unter **Zugewiesene Drahtlosnetzwerke (VSS)** mithilfe der Schaltfläche **Hinzufügen** das konfigurierte Drahtlosnetzwerk *Mitarbeiter* dem Funkmodul zugewiesen.

(6) Die restlichen Einstellungen werden unverändert übernommen. Bestätigen Sie mit **OK**.

Hinweis

Bei einem Access Point mit zwei Funkmodulen erscheinen zwei Konfigurationsmasken für **Funkmodul1** und **Funkmodul2**. Die Einstellung erfolgt entsprechend den Vorgaben des vorangegangenen Beispiels.

Die übrigen Access Points der Übersichtsliste werden genauso wie der Erste konfiguriert. Für jeden Access Point muss nur eine eindeutige Standortbezeichnung vergeben werden, andernfalls können die Access Points, z. B. beim WLAN-Netz-Monitoring (im Menü **Wireless LAN Controller** -> **Monitoring**) nicht mehr unterschieden werden.

Nachdem die Access Points alle eingerichtet sind, werden sie nach einer kurzen Initialisierungsphase in der Übersicht unter **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Slave Access Points** mit dem Status *Managed* gekennzeichnet und sind somit nun in Betrieb. Zudem sind sie durch den WLAN-Controller gegen jede Art eines externen Konfigurationszugriffs gesperrt.

Durch Klicken auf die ⌃-Schaltfläche oder die ⌄-Schaltfläche in der Spalte **Aktion** wählen Sie aus, ob der gewählte Access Point vom WLAN Controller verwaltet werden soll.

Sie können einen Access Point vom WLAN Controller trennen und ihn somit aus Ihrer WLAN-Infrastruktur entfernen, indem Sie auf die ⌄-Schaltfläche klicken. Der Access Point bekommt dann den Status *Gefunden*, aber nicht mehr *Managed*.

Die im Menü **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Slave Access Points** angezeigten WLAN-Kanäle sind jedoch unter Umständen noch nicht ideal, z. B. bezüglich der Mehrfachbelegung eines Kanals. Die Access Points konnten sich während der Inbetriebnahme nur auf die allgemeine WLAN-Umgebung abstimmen, aber noch nicht aufeinander. Dies kann auf zwei unterschiedlichen Wegen nachträglich korrigiert werden: Entweder indem für alle verwalteten Access Points aller Standorte die Aktion **Neue Kanalfestlegung** über die Schaltfläche **START** angestoßen wird oder indem individuell durch Betätigen des Aktualisierungssymbols in der Spalte **Kanalsuche** die Kanalsuche speziell für einen betroffenen Access Point neu angestoßen wird.

Wenn die Kanalfestlegung abgeschlossen ist, sollten jeweils direkt benachbarte Access Points eines Standorts auf unterschiedlichen Kanälen senden.

Die Liste der konfigurierten Access Points sieht nun wie folgt aus:

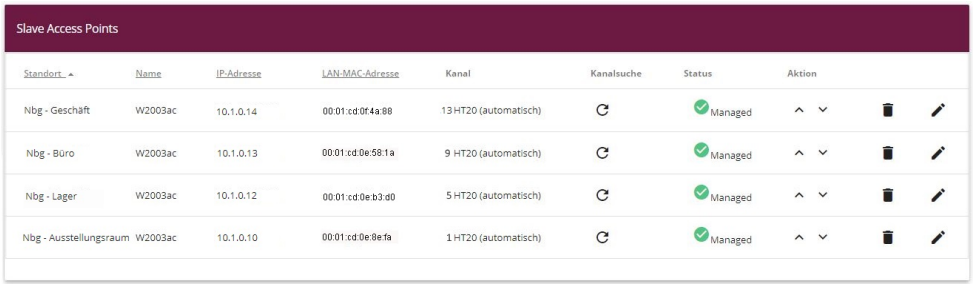


Abb. 98: **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Slave Access Points**

6.2.4.7 E-Mail-Benachrichtigung einrichten

Abschließend wird ein E-Mail-Alarm für die Slave-Access-Points eingerichtet. Die zuständigen Systemadministratoren werden damit unverzüglich und automatisch über (WLAN-) Netzprobleme der einzelnen Standorte informiert, inklusive (indirekter) Fehler durch Internetzugangs- und VPN-Ausfall. Die Access Points sind bei Netzstörungen nicht mehr für den WLAN-Controller sichtbar und werden nach einer bestimmten Zeitspanne automatisch als `offline` deklariert, auch wenn sie immer noch autonom vor Ort ihren Dienst verrichten.

Um den E-Mail-Alarm nutzen zu können, muss zuerst ein E-Mail-Server und anschließend ein Empfänger für die Alarm-Mitteilung eingerichtet werden.

(1) Gehen Sie zu **Externe Berichterstellung** -> **Benachrichtigungsdienst** ->**Benachrichtigungseinstellungen**.

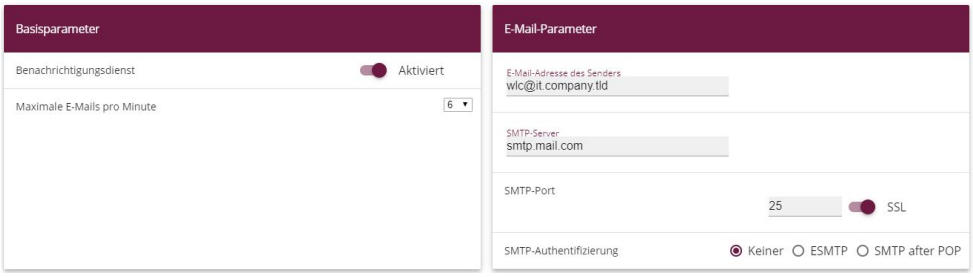


Abb. 99: **Externe Berichterstellung** -> **Benachrichtigungsdienst** ->**Benachrichtigungseinstellungen**

Gehen Sie folgendermaßen vor:

(1) Der **Benachrichtigungsdienst** muss aktiviert sein.

(2) Über den Wert bei **Maximale E-Mails pro Minute** können Sie die Anzahl der ausgehenden Mails pro Minute begrenzen, z. B. `6`.

(3) Tragen Sie eine Adresse ein, die in das Absenderfeld der E-Mail eingetragen wird, z.

B. `wlc@it.company.tld`.

(4) Geben Sie die IP-Adresse oder den DNS-Namen des **SMTP-Server**s ein, der zum Versenden der Mails verwendet werden soll, z. B. `smtp.mail.com`.

(5) Wählen Sie gegebenenfalls eine Authentifizierungsmethode für den SMTP-Server.

(6) Bestätigen Sie mit **OK**.

Als Letztes wird ein E-Mail-Alarm für die Slave-Access-Points eingerichtet.

(1) Gehen Sie zu **Externe Berichterstellung** -> **Benachrichtigungsdienst** ->**Benachrichtigungsempfänger**-> **Neu**.

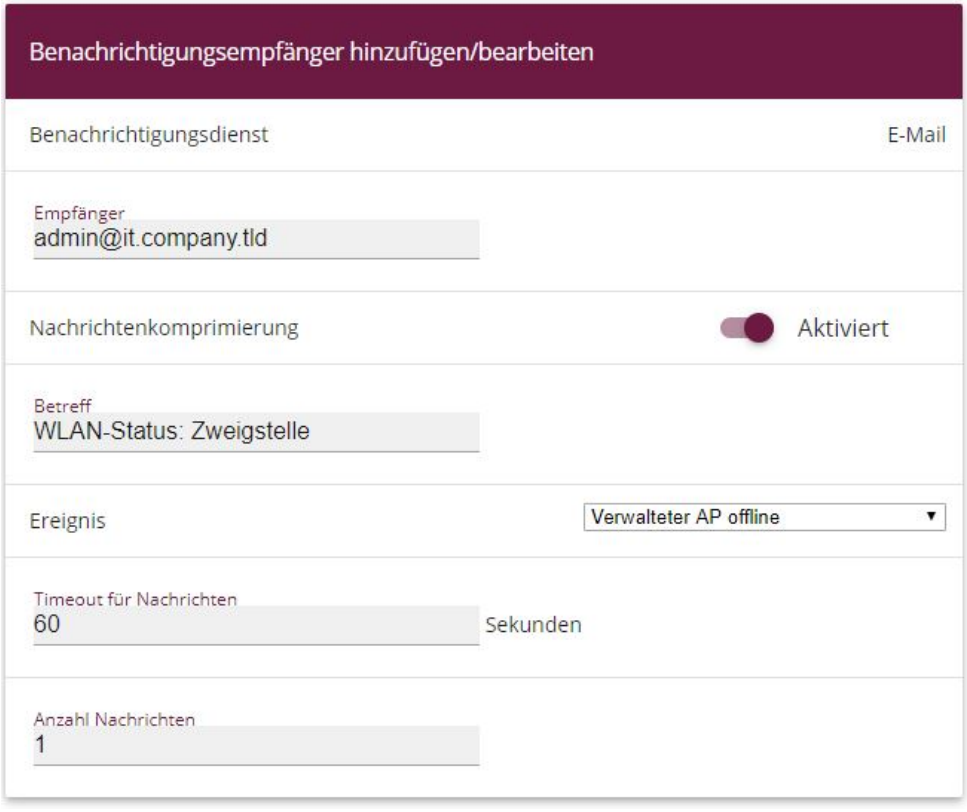


Abb. 100: **Externe Berichterstellung** ->**Benachrichtigungsdienst** ->**Benachrichtigungsempfänger**-> **Neu**

Gehen Sie folgendermaßen vor:

(1) Als **Empfänger** wird die E-Mail-Kontaktadresse der für dieses WLAN zuständigen Systemadministratoren eingegeben, z. B. `admin@it.company.tld`.

(2) Als **Betreff** wird eine möglichst prägnante kurze Information angegeben, z. B. `WLAN-Status: Zweigstellen`.

Hinweis

Der Inhalt einer Alarm-E-Mail enthält weitere Informationen, wie Grund des Alarms, Zeitpunkt des Ereignisses und das betroffene Gerät.

(3) Als **Ereignis** muss *Verwalteter AP offline* ausgewählt werden.

(4) Belassen Sie die übrigen Einstellungen und bestätigen Sie mit **OK**.

Die WLAN Controller-Konfiguration ist somit abgeschlossen. Speichern Sie die Konfiguration mit **Konfiguration speichern** und bestätigen Sie die Auswahl mit **OK**.

6.3 Konfigurationsschritte im Überblick

Konfiguration des Routers in der Außenstelle - IP-Konfiguration

Feld	Menü	Wert
Adressmodus	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>**	*Statisch*
IP-Adresse / Netzmaske	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>**	IP-Adresse: z. B. *10.1.0.1* Netzmaske: z. B. *255.255.255.0*
Schnittstellenmodus	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>**	*Untagged*
MAC-Adresse	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>**	*Voreingestellte verwenden*

Konfiguration des Routers in der Außenstelle - DHCP-Pool

Feld	Menü	Wert
IP-Poolname	**Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu**	z. B. *Geräte*
IP-Adressbereich	**Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu**	z. B. *10.1.0.10 - 10.1.0.254*
Schnittstelle	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguartion** -> **Neu**	*en1-0*
IP-Poolname	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	z. B. *Geräte*
Pool-Verwendung	**Lokale Dienste** -> **DHCP-Server** ->	*Lokal*

Feld	Menü	Wert
	DHCP-Konfiguration -> **Neu**	
Gateway	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	*Router als Gateway verwenden*
Lease-Time	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	z. B. *120*
DHCP-Optionen	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**-> **Hinzufügen**	*DNS-Server*: z. B. *10.1.0.1* *CAPWAP-Controller*: z. B. *10.0.0.123*

Konfiguration des VPN-Konzentrators in der Zentrale

Feld	Menü	Wert
Adressmodus	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>**	*Statisch*
IP-Adresse / Netzmaske	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>**	*IP-Adresse*: z. B. *10.0.0.1* *Netzmaske*: z. B. *255.255.255.0*
Schnittstellenmodus	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>**	*Untagged*
MAC-Adresse	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>**	*Voreingestellte verwenden*

Konfiguration des WLAN-Controllers in der Zentrale - IP-Konfiguration

Feld	Menü	Wert
Adressmodus	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>**	*Statisch*
IP-Adresse / Netzmaske	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>**	*IP-Adresse*: z. B. *10.0.0.123* *Netzmaske*: z. B. *255.255.255.0*
Schnittstellenmodus	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>**	*Untagged*
MAC-Adresse	**LAN** -> **IP-Konfiguration** -> **Schnitt-**	*Voreingestellte*

Feld	Menü	Wert
	stellen -> **<en1-0>** 	*verwenden*

Konfiguration des WLAN-Controllers in der Zentrale - Standardroute

Feld	Menü	Wert
Routentyp	**Netzwerk** -> **Routen** -> **Konfiguration von IPv4** -> **Neu**	*Standardroute über Schnittstelle*
Schnittstelle	**Netzwerk** -> **Routen** -> **Konfiguration von IPv4** -> **Neu**	*LAN_EN1-0*
Lokale IP-Adresse	**Netzwerk** -> **Routen** -> **Konfiguration von IPv4** -> **Neu**	z. B. *10.0.0.1*
Metrik	**Netzwerk** -> **Routen** -> **Konfiguration von IPv4** -> **Neu**	z. B. *1*

Konfiguration des WLAN-Controllers in der Zentrale - WLAN-Controller

Feld	Menü	Wert
Region	**Wireless LAN Controller** -> **Controller-Konfiguration** -> **Allgemein**	z. B. *Germany*
Schnittstelle	**Wireless LAN Controller** -> **Controller-Konfiguration** -> **Allgemien**	*LAN_EN1-0*
DHCP-Server	**Wireless LAN Controller** -> **Controller-Konfiguration** -> **Allgemien**	*Extern oder statisch*
Slave-AP-Standort	**Wireless LAN Controller** -> **Controller-Konfiguration** -> **Allgemien**	*Entfernt (WAN)*

Konfiguration des WLAN-Controllers in der Zentrale - Drahtlosnetzwerk-Profil

Feld	Menü	Wert
Netzwerkname (SSID)	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)**	z. B. *Mitarbeiter* (Sichtbar)
Intra-cell Repeating	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)**	*Aktiviert*
ARP Processing	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)**	*Deaktiviert*
WMM	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)**	*Aktiviert*

Feld	Menü	Wert
Max. Clients	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)**	z. B. *32*
Sicherheitsmodus	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)**	*WPA-PSK*
WPA-Modus	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)**	*WPA und WPA 2*
WPA-Cipher	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)**	*TKIP*
WPA2-Cipher	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)**	*AES*
Preshared Key	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)**	Zeichenfolge mit 8 - 63 Zeichen
ACL-Modus	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)**	*Deaktiviert*
Erlaubte Adressen	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)**	*Keine*
VLAN	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)**	*Deaktiviert*

Konfiguration des WLAN-Controllers in der Zentrale - Funkmodulprofile

Feld	Menü	Wert
Beschreibung	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Funkmodulprofile** -> **2.4 GHz Radio Profile**	z. B. *2.4 GHz Radio Profile*
Betriebsmodus	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Funkmodulprofile** -> **2.4 GHz Radio Profile**	*Access-Point*
Frequenzband	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Funkmodulprofile** -> **2.4 GHz Radio Profile**	*2,4 GHz In / Outdoor*

Feld	Menü	Wert
Anzahl der Spatial Streams	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Funkmodul-profile -> 2.4 GHz Radio Profile**	*2*
Drahtloser Modus	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Funkmodul-profile -> 2.4 GHz Radio Profile**	*802.11 g / n*
Max. Übertragungsrate	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Funkmodul-profile -> 2.4 GHz Radio Profile**	*Auto*
Burst-Mode	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Funkmodul-profile -> 2.4 GHz Radio Profile**	*Aktiviert*
Kanalplan	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Funkmodul-profile -> 2.4 GHz Radio Profile**	*Benutzerdefiniert*
Benutzerdefinierter Kanalplan	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Funkmodul-profile -> 2.4 GHz Radio Profile ->Erweiterte Einstellungen**	*1*, *5*, *9*, *13*
Beacon Period	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Funkmodul-profile -> 2.4 GHz Radio Profile ->Erweiterte Einstellungen**	*100* ms
DTIM Period	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Funkmodul-profile -> 2.4 GHz Radio Profile ->Erweiterte Einstellungen**	*2*
RTS Threshold	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Funkmodul-profile -> 2.4 GHz Radio Profile-> Erweiterte Einstellungen**	*2347*
Short Guard Interval	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Funkmodul-profile -> 2.4 GHz Radio Profile-> Erweiterte Einstellungen**	*Aktiviert*
Short Retry Limit	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Funkmodul-profile -> 2.4 GHz Radio Profile->**	*7*

Feld	Menü	Wert
	Erweiterte Einstellungen	
Long Retry Limit	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Funkmodulprofile** -> **2.4 GHz Radio** **Profile**-> **Erweiterte Einstellungen**	*4*
Fragmentation Threshold	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Funkmodulprofile** -> **2.4 GHz Radio** **Profile**-> **Erweiterte Einstellungen**	*2346* Bytes

Konfiguration des WLAN-Controllers in der Zentrale - Access Points

Feld	Menü	Wert
Standort	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Slave Access Points**	z. B. *Nbg - Geschäft*
CAPWAP-Verschlüsselung	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Slave Access Points**	*Aktiviert*
Betriebsmodus	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Slave Access Points**	*Ein*
Aktives Funkmodulprofil	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Slave Access Points**	z. B. *2.4 GHz Radio Profile*
Kanal	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Slave Access Points**	*Auto*
Verwendeter Kanal	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Slave Access Points**	z. B. *13*
Sendeleistung	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Slave Access Points**	*Max.*
Zugewiesene Drahtlosnetzwerke (VSS)	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Slave Access Points**	z. B. *vss-1: Mitarbeiter*

E-Mail-Benachrichtigung einrichten - Einstellungen

Feld	Menü	Wert
Benachrichtigungsdienst	**Externe Berichterstellung ->Benachrichtigungsdienst -> Benachrichtigungseinstellungen**	*Aktiviert*
Maximale E-Mails pro Minute	**Externe Berichterstellung ->Benachrichtigungsdienst -> Benachrichtigungseinstellungen**	z. B. *6*
E-Mail-Adresse des Senders	**Externe Berichterstellung ->Benachrichtigungsdienst -> Benachrichtigungseinstellungen**	z. B. *wlc@itcompany.tld*
SMTP-Server	**Externe Berichterstellung ->Benachrichtigungsdienst -> Benachrichtigungseinstellungen**	z. B. *smtp.mail.com*
SMTP- Authentifizierung	**Externe Berichterstellung ->Benachrichtigungsdienst -> Benachrichtigungseinstellungen**	z. B. *Keine*

E-Mail-Benachrichtigung einrichten - Empfänger

Feld	Menü	Wert
Empfänger	**Externe Berichterstellung -> Benachrichtigungsdienst ->Benachrichtigungsempfänger -> Neu**	z. B. *admin@itcompany.tld*
Nachrichtenkomprimierung	**Externe Berichterstellung -> Benachrichtigungsdienst ->Benachrichtigungsempfänger -> Neu**	*Aktiviert*
Betreff	**Externe Berichterstellung -> Benachrichtigungsdienst ->Benachrichtigungsempfänger -> Neu**	z. B. *WLAN-Status: Zweigstellen*
Ereignis	**Externe Berichterstellung -> Benachrichtigungsdienst ->Benachrichtigungsempfänger -> Neu**	*Verwalteter AP offline*
Timeout für Nachrichten	**Externe Berichterstellung -> Benachrichtigungsdienst ->Benachrichtigungsempfänger -> Neu**	z. B. *60*
Anzahl Nachrichten	**Externe Berichterstellung -> Benachrichtigungsdienst ->Benachrichtigungsempfänger -> Neu**	z. B. *1*

Kapitel 7 WLAN - Wireless LAN Controller als Netzzugangsgateway

7.1 Einleitung

Im Folgenden wird die Konfiguration eines Bintec-Routers als WLAN Controller für die lokale WLAN-Infrastruktur (**bintec W2003ac**-Access Points) und als zentrales Zugangsgateway in das WAN (Internet) mit automatischer Netzeinrichtung und Firewall für Geräte im WLAN und Ethernet-LAN beschrieben.

Zur Konfiguration wird das **GUI** (Graphical User Interface) verwendet.

Ein Firmenstandort soll mit Ethernet-LAN und WLAN nach Mitarbeitern und Gästen getrennt ausgerüstet werden:

- Die Rechner und die sonstigen Geräte beider Benutzergruppen sollen automatisch per DHCP in das Netzwerk integriert werden und auf das Internet zugreifen können.
- Gäste sollen nicht auf das Intranet der Mitarbeiter zugreifen können.
- Mitarbeiter sollen jedoch auf das Intranet der Gäste zugreifen können, um zum Beispiel ausgewählte Dokumente schnell und sicher mit einem vor Ort befindlichen externen Projektpartner entsprechend der Firmenstandards gemeinsam nutzen zu können.
- Zusätzlich soll der Zugriff auf die Netzinfrastruktur auf Systemadministratoren beschränkt werden.

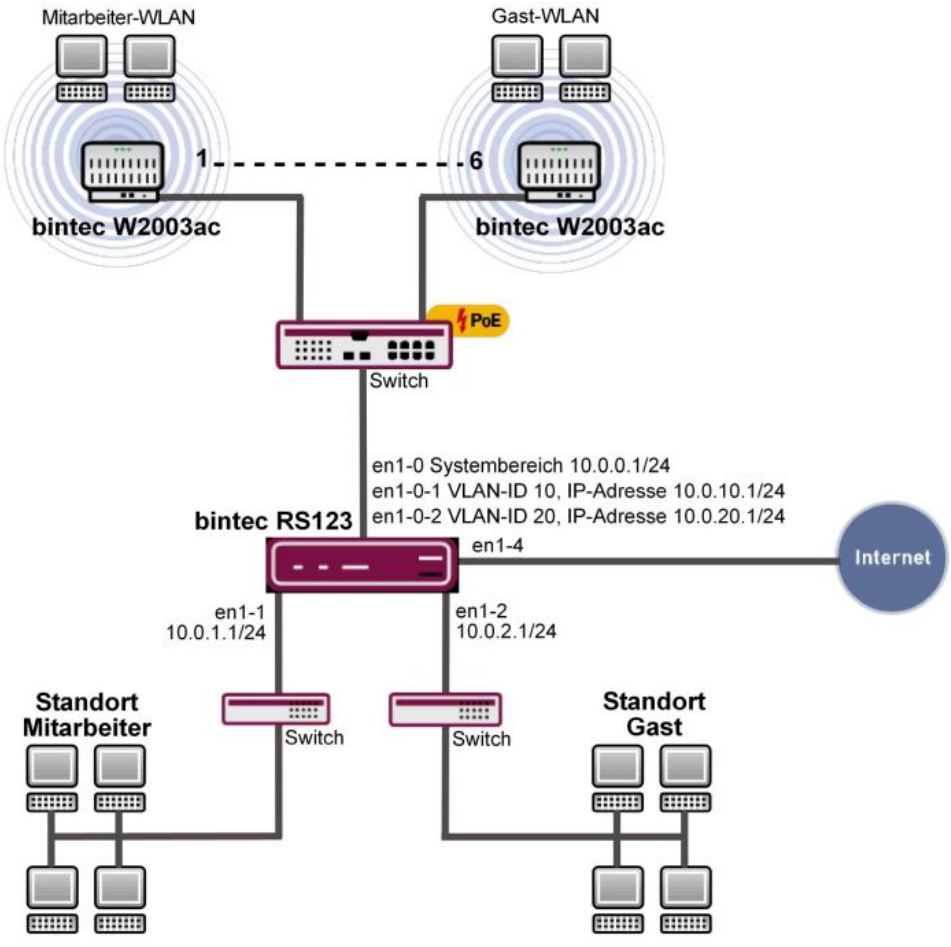


Abb. 101: Beispielszenario

Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Ein Bintec-Router der RS-Serie, der RXL-Serie, eine **be.IP**, oder **be.IP plus**.
- Access Points der **bintec W2003ac**-Serie oder bintec WI-Serie (z. B. **bintec WI1003n**). Die mindestens benötigte Anzahl der Access Points richtet sich nach der Größe und Gebäudestruktur des Firmenstandorts und lässt sich mit einer vorherigen WLAN-Ausleuchtung genau festlegen (siehe dazu auch die WLAN Controller-Einführung). In unserem Beispiel werden 5 **bintec W2003ac** und ein **bintec WI1003n** verwendet.
- Ein Bootimage mit mindestens Version 10.1.9 für den Bintec-Router

- Ein Bootimage mit mindestens Version 10.1.9 für die Access Points
- Ein Internetzugang am Firmenstandort.
- Mindestens ein PoE-Switch für die Access Points und weitere Switche für das LAN.

Hinweise zum Test-Setup

Schnittstellenkonfigurationsübersicht am Bintec-Router:

en1-0	Systembereich	IP-Adresse 10.0.0.1/24: DHCP-Server für Access Points und Schnittstelle des WLAN Controllers
en1-0-1	Mitarbeiter-WLAN	Virtuelle Schnittstelle über en1-0 mit VLAN-ID 10, IP-Adresse 10.0.10.1/24: DHCP-Server und Gateway für das Mitarbeiter-WLAN
en1-0-2	Gast-WLAN	Virtuelle Schnittstelle über en1-0 mit VLAN-ID 20, IP-Adresse 10.0.20.1/24: DHCP-Server und Gateway für das Gast-WLAN
en1-1	Mitarbeiter-Ethernet-LAN	IP-Adresse 10.0.1.1/24: DHCP-Server und Gateway für das Mitarbeiter-Ethernet-LAN
en1-2	Gast-Ethernet-LAN	IP-Adresse 10.0.2.1/24: DHCP-Server und Gateway für das Gast-Ethernet-LAN
en1-4	WAN	Uplink ins Internet

7.2 Konfiguration

Portkonfiguration

Hinweis

Während der gesamten Konfiguration sollte der Rechner, von dem aus der Router konfiguriert wird, am Ethernet-Port 1 angeschlossen sein. Andernfalls sperrt man sich während der Konfiguration wiederholt aus dem Router aus.

Als erstes werden die Ethernet-Ports als getrennte Schnittstellen konfiguriert und jedem Port wird aufsteigend, beginnend mit en1-0, eine eigene Schnittstelle zugewiesen.

(1) Gehen Sie zu **Physikalische Schnittstellen** -> **Ethernet-Ports** -> **Portkonfiguration**.

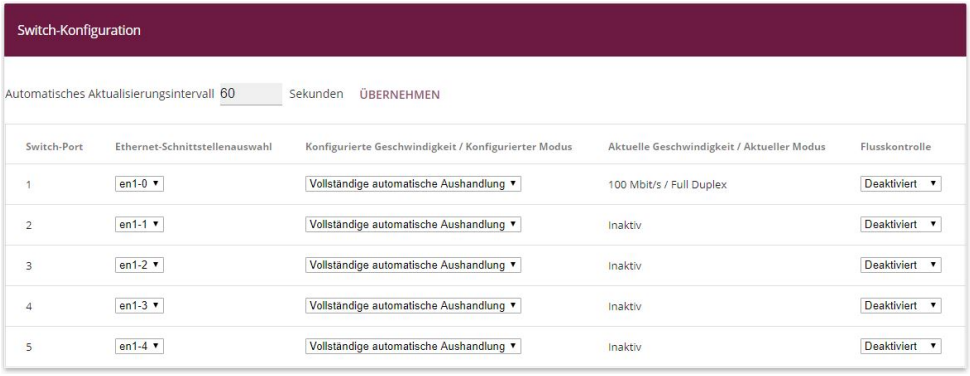


Abb. 102: **Physikalische Schnittstellen** -> **Ethernet-Ports** -> **Portkonfiguration**

Gehen Sie folgendermaßen vor um die Ports den Schnittstellen zuzuordnen:

(1) Wählen Sie bei **Ethernet-Schnittstellenauswahl** für die **Switch-Ports 1** bis **5** *en1-0* bis *en1-4* im Dropdown-Menü aus.

(2) Bestätigen Sie mit **OK**.

Anschließend wird der WAN- bzw. Internetzugang eingerichtet. Zur Konfiguration eines Internetzugangs verfügt das **GUI** über einen **Assistenten**. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **Assistenten** -> **Internet** -> **Internetverbindungen** -> **Neu**.

(2) Wählen Sie bei **Verbindungstyp** den passenden Verbindungstyp Ihres Internetzugangs aus, in unserem Beispiel *Externes Gateway/Kabelmodem*.

(3) Klicken Sie auf **Weiter**, um eine neue Internetverbindung zu konfigurieren.

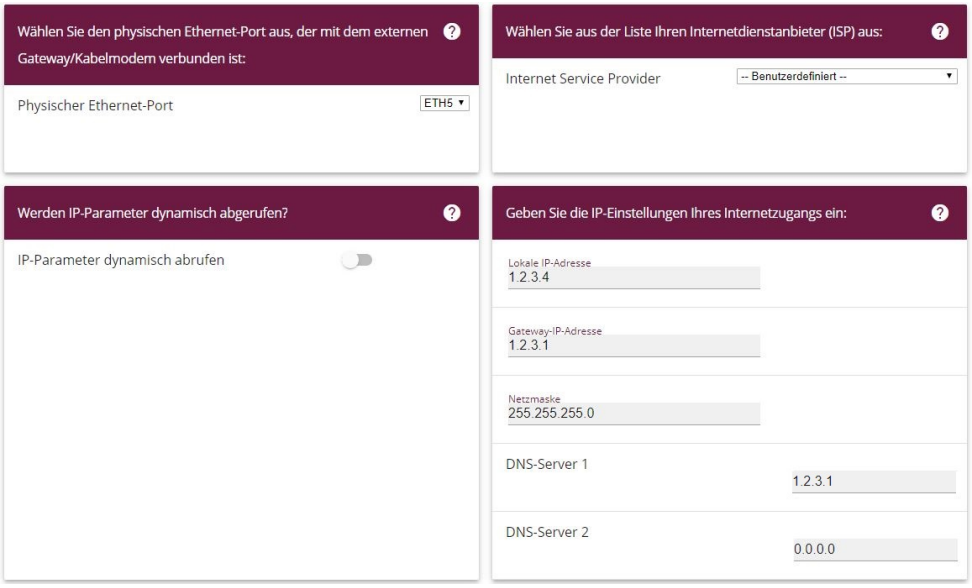


Abb. 103: **Assistenten** -> **Internet** -> **Internetverbindungen** -> **Neu** -> **Weiter**

Im Folgenden wird die Einstellung für ein externes Gateway beschrieben:

(1) Im Menüpunkt **Physischer Ethernet-Port** wählen Sie den physikalischen Ethernet-Port aus, an dem das xDSL-Modem, bzw. der Internet-Uplink angeschlossen ist, hier *ETH5*.

(2) Bei **Internet Service Provider** wählen Sie *-Benutzerdefiniert-* aus.

(3) Deaktivieren Sie die Option **IP-Parameter dynamisch abrufen**.

(4) Geben Sie bei **Lokale IP-Adresse** die Daten Ihres Internetzugangs ein, z. B. *1.2.3.4*.

(5) Bei **Gateway-IP-Adresse** geben Sie die Adresse des Gateways ein, z. B. *1.2.3.1*.

(6) Geben Sie die entsprechende **Netzmaske** ein, z. B. *255.255.255.0*.

(7) Bei **DNS-Server 1** geben Sie die IP-Adresse des Name-Servers ein, z. B. *1.2.3.1*.

(8) Bestätigen Sie Ihre Angaben mit **OK**.

Variante:

(1) Ist der Uplink ein xDSL-Zugang eines Providers, kann man stattdessen im ersten Schritt des Internetzugangsassistenten das *Interne Modem* als **Verbindungstyp** auswählen.

(2) Die interne **Netzwerkschnittstelle** heißt in diesem Fall in der Regel *WAN_Providername* statt *en1-4* und taucht nach abgeschlossener Konfiguration im Menü **Netzwerk** -> **Routen** -> **IP-Routen** als Schnittstelle für das Standardgateway auf. (Im einfachsten Fall ist das der einzige Eintrag mit Ziel-IP-Adresse und Netzmas-

ke gleich `0.0.0.0`.)

(3) Der Name der **Schnittstelle** ist für spätere Konfigurationsschritte in der Firewalleinrichtung relevant.

Hinweis

Diese Schnittstelle darf nicht mit der ebenfalls vorhandenen (zugrundeliegenden) `ethoa`-Schnittstelle verwechselt werden.

Anschließend werden die LAN-Schnittstellen konfiguriert.

Konfigurieren Sie die Ethernet-Schnittstelle, indem Sie den Standardeintrag bearbeiten. Klicken Sie dazu bei dem vorhandenen Eintrag **<en1-0>** auf das -Symbol.

(1) Gehen Sie zu **LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> .

Abb. 104: **LAN** -> **IP-Konfiguration** -> **Schnittstellen** ->

Gehen Sie folgendermaßen vor, um die Ethernet-Schnittstelle zu konfigurieren:

(1) Geben Sie die statische **IP-Adresse** `10.0.0.1` und die **Netzmaske** `255.255.255.0` ein.

(2) Bestätigen Sie mit **OK**.

Hinweis

Nachdem Sie die Konfiguration mit **OK** bestätigt haben, haben Sie sich (einmalig) aus dem Router ausgesperrt. Melden Sie sich auf der soeben neu eingerichteter **IP-Adresse** `10.0.0.1` für `en1-0` erneut an (ggf. muss die Netzkonfiguration des eigenen Rechners zuvor angepasst werden).

(1) Danach wird auf der Ethernet-Schnittstelle `en1-1` die statische **IP-Adresse** `10.0.1.1` mit der **Netzmaske** `255.255.255.0` eingerichtet.

(2) Bestätigen Sie mit **OK**.

(3) Zum Schluss wird noch die Ethernet-Schnittstelle *en1-2* mit der statischen **IP-Adresse** *10.0.2.1* und mit der **Netzmaske** *255.255.255.0* eingerichtet. Die Ethernet-Schnittstelle *en1-3* bleibt ungenutzt.

(4) Bestätigen Sie mit **OK**.

Im nächsten Schritt werden zwei virtuelle Schnittstellen basierend auf *en1-0* hinzugefügt.

(1) Gehen Sie zu **LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **Neu**.

Abb. 105: **LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **Neu**

Gehen Sie folgendermaßen vor, um die erste virtuelle Schnittstelle zu konfigurieren:

(1) Bei **Basierend auf Ethernet-Schnittstelle** wählen Sie die Schnittstelle *en1-0* aus.

(2) Weisen Sie der Schnittstelle die **VLAN-ID** *10* zu.

(3) Bei **IP-Adresse / Netzmaske** klicken Sie auf **Hinzufügen**.

(4) Die erste virtuelle Schnittstelle bekommt die statische **IP-Adresse** *10.0.10.1* und die **Netzmaske** *255.255.255.0*.

(5) Bestätigen Sie mit **OK**.

Konfigurieren Sie die zweite virtuelle Schnittstelle wie folgt:

(1) Bei **Basierend auf Ethernet-Schnittstelle** wählen Sie die Schnittstelle *en1-0* aus.

(2) Weisen Sie der Schnittstelle die **VLAN-ID** *20* zu.

(3) Bei **IP-Adresse / Netzmaske** klicken Sie auf **Hinzufügen**.

(4) Die zweite virtuelle Schnittstelle bekommt die statische **IP-Adresse** *10.0.20.1* und die **Netzmaske** *255.255.255.0*.

(5) Bestätigen Sie mit **OK**.

Ergebnis:

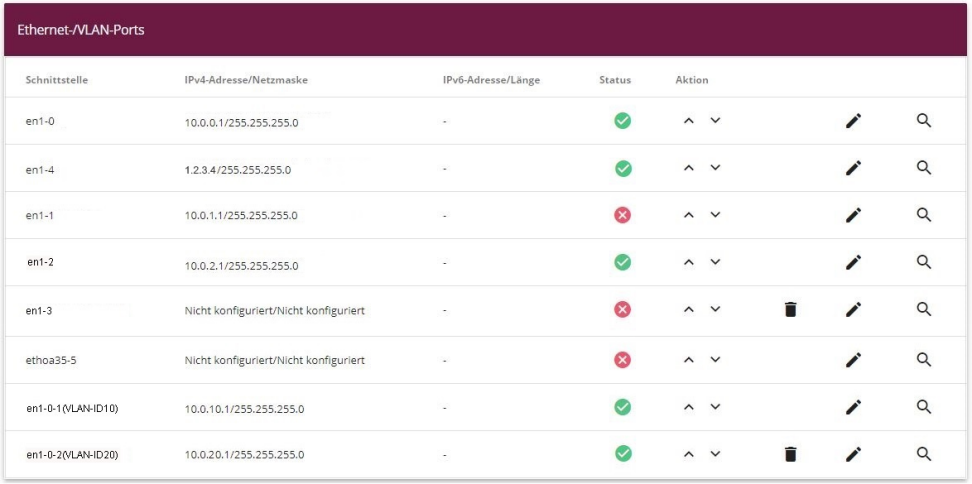


Abb. 106: **LAN** -> **IP-Konfiguration** -> **Schnittstellen**

Systemzugangs- und Firewalleinrichtung

Im Menü **Zugriff** wird der administrativer Zugriff zum Gerät konfiguriert. Zuerst werden alle Konfigurationsdienste des Routers auf die administrative Ethernet-Schnittstelle `en1-0` beschränkt.

(1) Gehen Sie zu **Systemverwaltung** -> **Administrativer Zugriff** -> **Zugriff**.

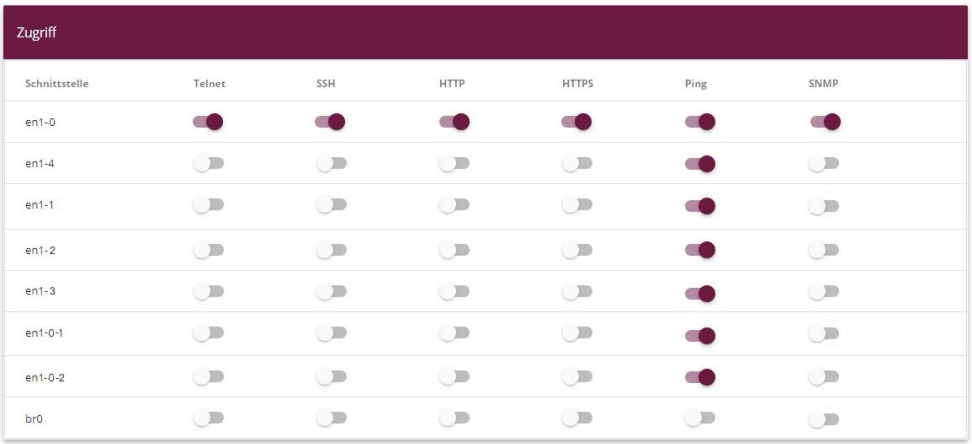


Abb. 107: **Systemverwaltung** -> **Administrativer Zugriff** -> **Zugriff**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie für die **Schnittstelle** `en1-0` die Konfigurationsdienste des Routers `Tel-`

net, *SSH*, *HTTP*, *HTTPS*, *Ping* und *SNMP* aus.

(2) Auf allen anderen Schnittstellen soll nur *Ping* erlaubt sein. Es wird nicht empfohlen, Ping ebenfalls zu sperren, da dadurch die Fehlersuche im LAN unnötig (ohne Sicherheitsgewinn) erschwert wird.

(3) Klicken Sie auf **OK**.

Auch das Einstellen der **Passwörter** gehört zu den grundlegenden Systemeinstellungen. Ändern Sie unbedingt die Passwörter, um unberechtigten Zugriff auf das Gerät zu verhindern.

(1) Gehen Sie zu **Systemverwaltung** -> **Globale Einstellungen** -> **Passwörter**.

(2) Geben Sie das Passwort für den Benutzernamen *admin* an.

(3) Bestätigen Sie das Passwort, indem Sie es erneut angeben.

(4) Klicken Sie auf **OK**.

Anschließend wird die **Firewall** für das LAN eingerichtet. Definieren Sie eine Gruppe, die alle Dienste beinhaltet, die vom Router selbst im LAN angeboten werden dürfen.

(1) Gehen Sie zu **Firewall** -> **Dienste** -> **Gruppen** -> **Neu**.

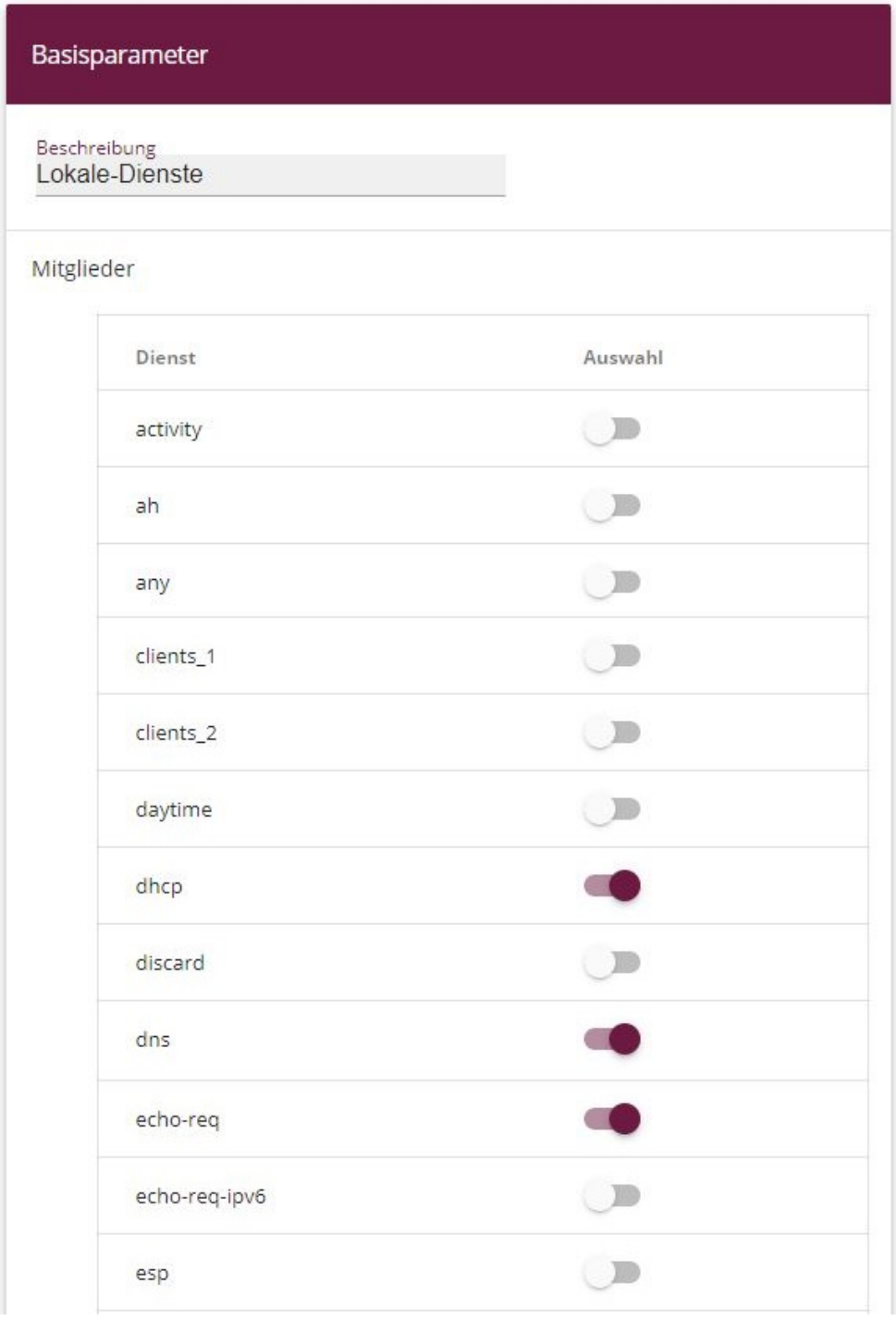

Basisparameter
Beschreibung
Lokale-Dienste
Mitglieder
Dienst
Auswahl
activity
ah
any
clients_1
clients_2
daytime
dhcp
discard
dns
echo-req
echo-req-ipv6
esp

Abb. 108: **Firewall** -> **Dienste** -> **Gruppen** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Geben Sie bei **Beschreibung** `Lokale-Dienste` für die Gruppe ein.

(2) Wählen Sie die **Mitglieder** der Gruppe aus, z. B. `echo`, `dns`, `dhcp`, `ntp`. Aktivieren Sie dazu das Feld in der Spalte **Mitglieder**.

(3) Bestätigen Sie mit **OK**.

Im nächsten Schritt werden die Adresslisten der Firewall definiert. Standardmäßig ist nur der Eintrag `ANY` vorhanden.

(1) Gehen Sie zu **Firewall** -> **Adressen** -> **Adressliste** -> **Neu**.

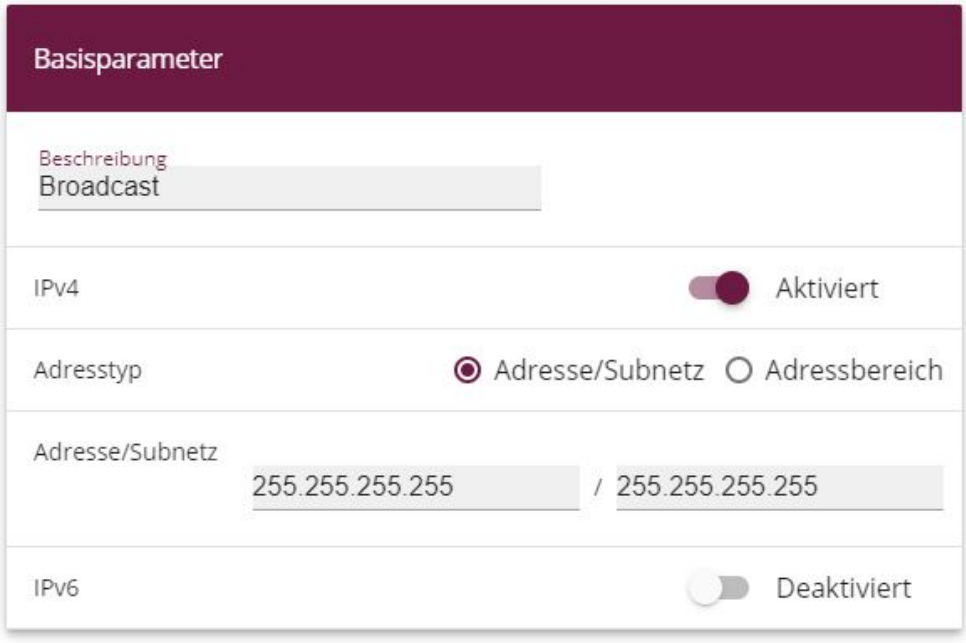


Abb. 109: **Firewall** -> **Adressen** -> **Adressliste** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Geben Sie bei **Beschreibung** `Broadcast` ein.

(2) Geben Sie als **IP-Adresse** und **Netzmaske** `255.255.255.255` und `255.255.255.255` ein.

(3) Bestätigen Sie mit **OK**.

Definieren Sie weitere LAN-IP-Adresslisten.

(1) Für `Mitarbeiter-LAN-GW` (en1-1) die **IP-Adresse** `10.0.1.1` mit der **Netzmaske** `255.255.255.255`.

(2) Bestätigen Sie mit **OK**.

(3) Für *Gast-LAN-GW* (en1-2) die **IP-Adresse** *10.0.2.1* mit der **Netzmaske** *255.255.255.255*.

(4) Bestätigen Sie mit **OK**.

(5) Für *Mitarbeiter-WLAN-GW* (en1-0-1) die **IP-Adresse** *10.0.10.1* mit der **Netzmaske** *255.255.255.255*.

(6) Bestätigen Sie mit **OK**.

(7) Und für *Gast-WLAN-GW* (en1-0-2) die **IP-Adresse** *10.0.20.1* mit der **Netzmaske** *255.255.255.255*.

(8) Bestätigen Sie mit **OK**.

Hinweis

Die IP-Adressen in der Firewall müssen zur IP-Konfiguration der jeweiligen Schnittstellen passen (und bei Konfigurationsänderung angepasst werden). Die Maske muss immer 255.255.255.255 sein und hat nichts mit der Netzmaske der jeweiligen Netze zu tun. Die Maske schränkt den Bereich der jeweiligen Adressliste auf genau die eine angegebene IP-Adresse ein.

Die Liste der konfigurierten Adressen sieht nun wie folgt aus:

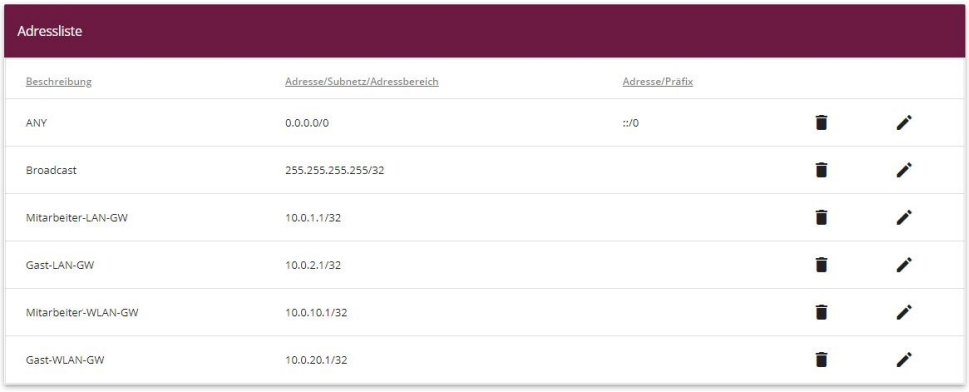


Abb. 110: **Firewall** -> **Adressen** -> **Adressliste**

Jetzt müssen Sie noch die Schnittstellen für die einzelnen Benutzergruppen definieren.

(1) Gehen Sie zu **Firewall** -> **Schnittstellen** -> **IPv4-Gruppen** -> **Neu**.

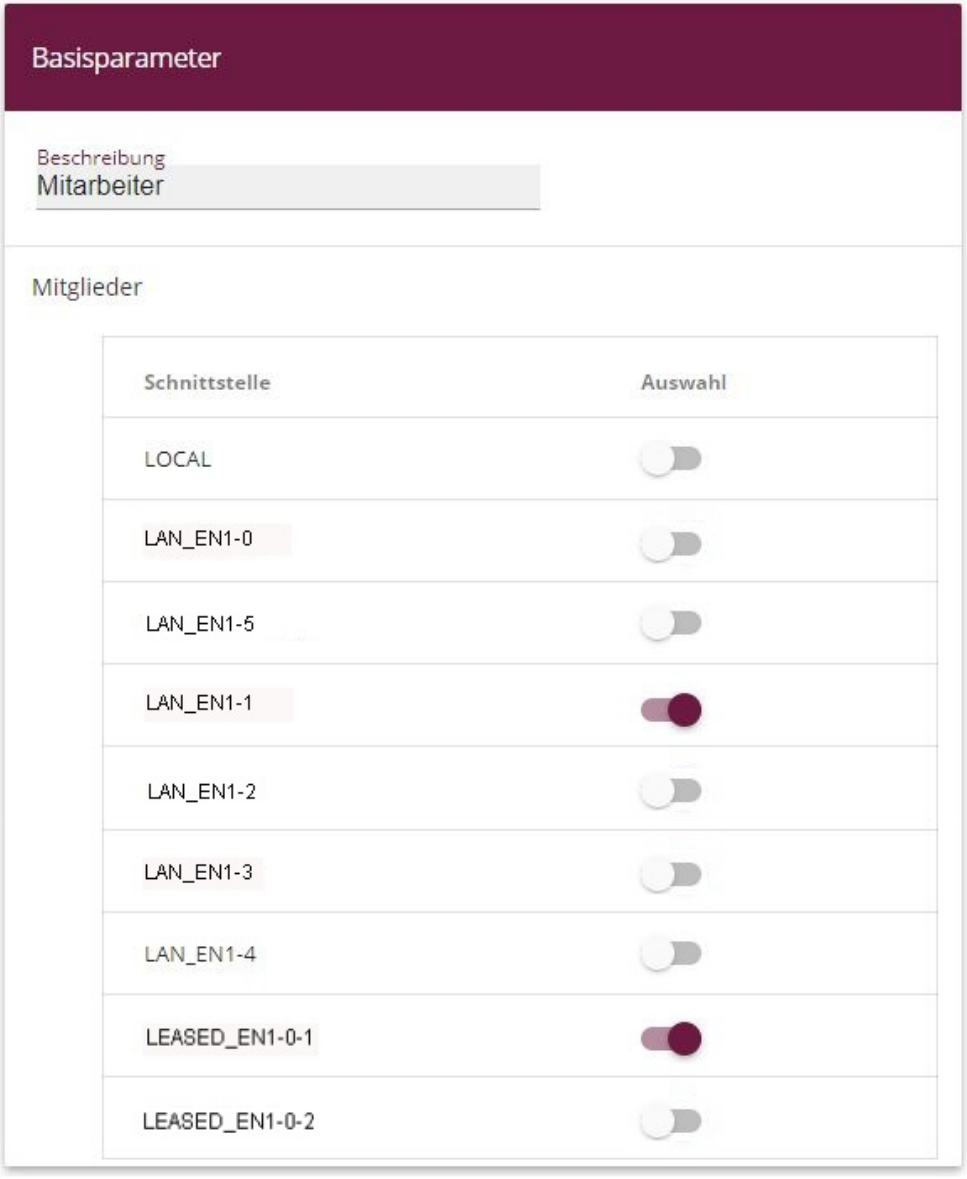


Abb. 111: **Firewall** -> **Schnittstellen** -> **IPv4-Gruppen** -> **Neu**

Gehen Sie folgendermaßen vor, um die Gruppe `Mitarbeiter` einzurichten:

(1) Geben Sie als **Beschreibung** der Gruppe `Mitarbeiter` ein.

(2) Wählen Sie aus den konfigurierten Schnittstellen als **Mitglieder** der Gruppe `LAN_EN1-1` und `LEASED_EN1-0-1` aus.

(3) Bestätigen Sie mit **OK**.

Definieren Sie eine weitere Gruppe *Gast* wie folgt:

(1) Geben Sie als **Beschreibung** der Gruppe *Gast* ein.

(2) Wählen Sie als **Mitglieder** der Gruppe *LAN_EN1-2* und *LEASED_EN1-0-2* aus.

(3) Bestätigen Sie mit **OK**.

Einrichtung Schnittstellen-Gruppe *Benutzer* (Mitarbeiter und Gäste).

(1) Geben Sie als **Beschreibung** der Gruppe *Benutzer* ein.

(2) Wählen Sie als **Mitglieder** der Gruppe *LAN_EN1-1*, *LAN_EN1-2*, *LEASED_EN1-0-1* und *LEASED_EN1-0-2* aus.

(3) Bestätigen Sie mit **OK**.

Die Liste der konfigurierten Gruppen sieht nun wie folgt aus:

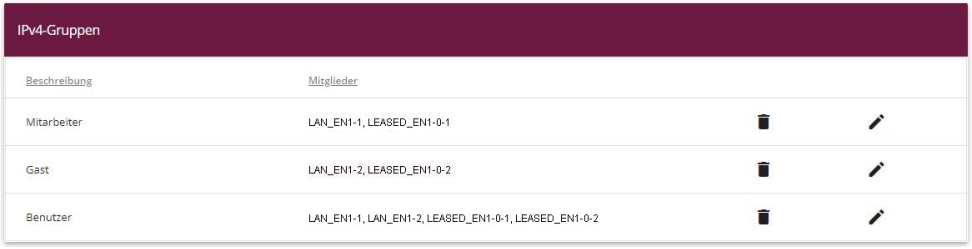


Abb. 112: **Firewall** -> **Schnittstellen** -> **IPv4-Gruppen**

Nun können basierend auf diesen Definitionen die eigentlichen Firewallregeln erstellt werden. Als Erstes muss die Regel für den Administratorenbereich auf *en1-0* definiert werden (andernfalls sperrt man sich sofort komplett aus).

(1) Gehen Sie zu **Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**.

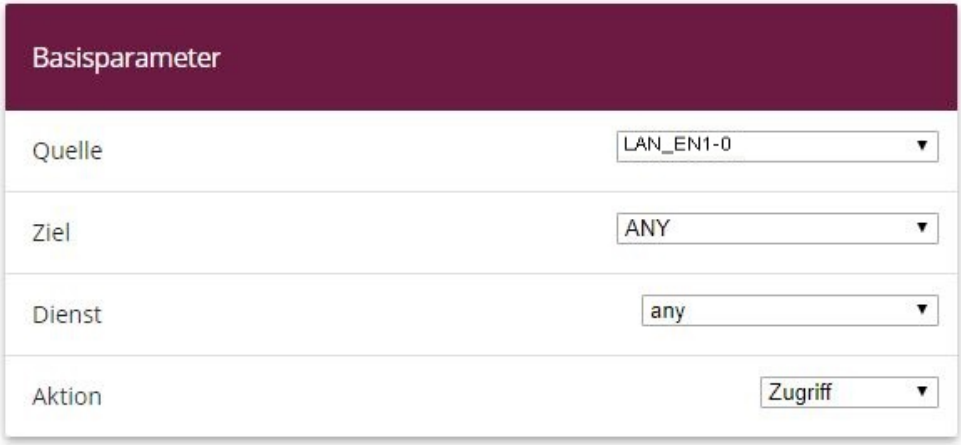


Abb. 113: **Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie die **Quelle** des Pakets aus, hier *LAN_EN1-0*.

(2) Wählen Sie als **Ziel** *ANY* aus. Weder Ziel-Schnittstelle noch Ziel-Adresse werden überprüft.

(3) Bei **Dienste** wählen Sie *any* (alle Dienste) aus.

(4) Wählen Sie die **Aktion** aus die angewendet werden soll, hier *Zugriff*. Die Pakete werden entsprechend den Angaben weitergeleitet.

(5) Bestätigen Sie mit **OK**.

(6) Als nächste Regel darf die **Quellgruppe** *Mitarbeiter* auf die **Zielgruppe** *Benutzer* über **Dienste** *any* zugreifen.

(7) Bestätigen Sie mit **OK**.

(8) Daran anschließend wird eine Regel erstellt, mit der von der **Quellgruppe** *Gast* auf die **Zielgruppe** *Gast* über **Dienste** *any* zugegriffen werden darf.

(9) Bestätigen Sie mit **OK**.

(10) Mit einer weiteren Regel sollen alle *Benutzer* auf das Internet zugreifen können: Wählen Sie als **Quelle** *Benutzer*, als **Ziel** *LAN_EN1-4* , und als **Dienst** *any* aus.

(11) Bestätigen Sie mit **OK**.

Hinweis

Falls ein Internetzugang über ein internes xDSL-Modem eingerichtet wurde, muss die entsprechende WAN-Schnittstelle (*WAN_Providername*) statt *LAN_EN1-4* als **Ziel** ausgewählt werden.

Bis jetzt sind lediglich Zugriffsregeln für über den Router verbundene Netzbereiche definiert und niemand außer dem Systembereich an der Schnittstelle *en1-0* darf auf lokal im Router definierte IP-Adressen zugreifen.

Um grundlegende Dienste wie zum Beispiel *dns*, *dhcp* usw. nutzen zu können, muss der **Zugriff** auf die auf dem Router gebundene IP-Adresse der jeweiligen Schnittstelle explizit erlaubt werden.

(1) Gehen Sie zu **Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**.

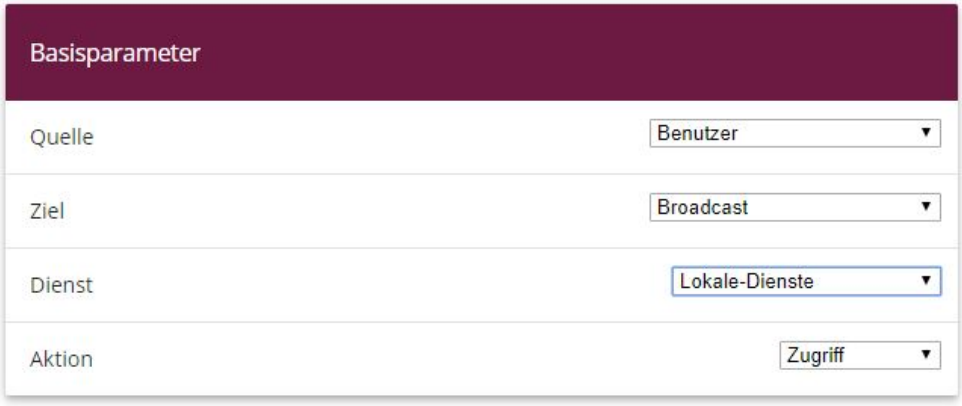


Abb. 114: **Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie als **Quelle** des Pakets die Gruppe *Benutzer* aus.

(2) Wählen Sie als **Ziel** die zuvor definierte Adresse *Broadcast* aus.

(3) Bei **Dienste** wählen Sie die Dienstgruppe aus, auf die die Benutzer zugreifen dürfen, hier *Lokale-Dienste*.

(4) Wählen Sie die **Aktion** aus, die angewendet werden soll, hier *Zugriff*. Die Pakete werden entsprechend den Angaben weitergeleitet.

(5) Bestätigen Sie mit **OK**.

(6) In der nächsten Regel wählen Sie als **Quelle** *LAN_EN1-1* aus. Wählen Sie als **Ziel** die zuvor definierte Adresse *Mitarbeiter-LAN-GW*, als **Dienst** wählen Sie *Lokale-Dienste* und als **Aktion** *Zugriff* aus.

(7) Bestätigen Sie mit **OK**.

(8) In der darauffolgenden Regel wählen Sie die **Quelle** *LAN_EN1-2* aus. Wählen Sie als **Ziel** die zuvor definierte Adresse *Gast-LAN-GW*, als **Dienst** wählen Sie *Lokale-Dienste* und die **Aktion** *Zugriff* aus.

(9) Bestätigen Sie mit **OK**.

(10) Als nächste Regel wählen Sie als **Quelle** *LEASED_EN1-0-1* , als **Ziel** die zuvor definierte Adresse *Mitarbeiter-WLAN-GW* , als **Dienst** *Lokale-Dienste* und als **Aktion** *Zugriff* aus.

(11) Bestätigen Sie mit **OK**.

(12) In der letzten Regel wählen Sie die **Quelle** *LEASED_EN1-0-2* aus. Wählen Sie als **Ziel** die zuvor definierte Adresse *Gast-WLAN-GW* , als **Dienst** wählen Sie *Lokale-Dienste* und die **Aktion** *Zugriff* aus.

(13) Bestätigen Sie mit **OK**.

Die Liste der konfigurierten Filterregeln sieht nun wie folgt aus:

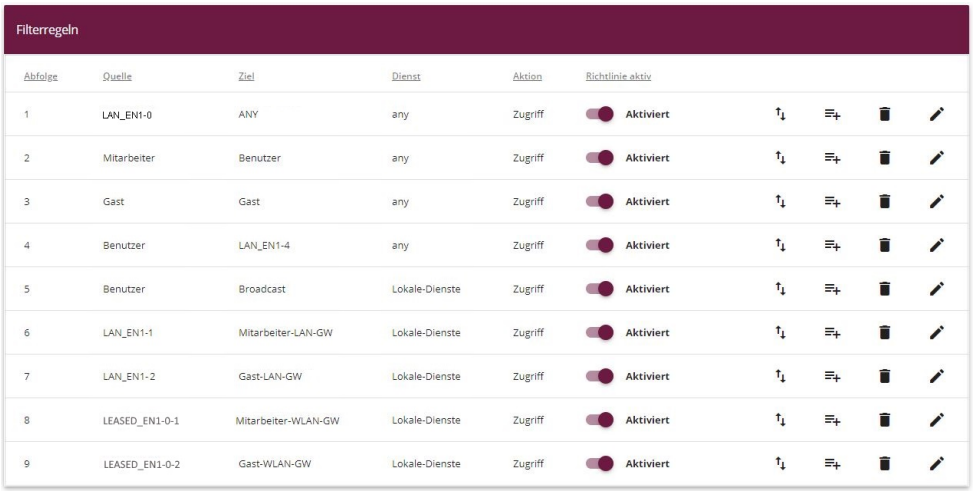


Abb. 115: **Firewall** -> **Richtlinien** -> **IPv4-Filterregeln**

Alle übrigen Daten, die nicht zu den obigen Regeln passen, werden von der Firewall automatisch verworfen. Es muss also keine explizite Schlussregel angelegt werden, welche den übrigen Datenverkehr verwirft. Dies bedeutet auch, dass mit der bestehenden Firewallkonfiguration jeglicher vom WAN/Internet (in unserem Beispiel *en1-4*) initiierte IP-Datenverkehr auf den Router und ins LAN unterbunden ist. Ist ein Zugriff von außen erwünscht, müssen hierzu eigene Firewallregeln mit der WAN-Schnittstelle (hier *LAN_EN1-4*) als Quelle definiert werden.

Zum Schluss überprüfen Sie noch, ob die Firewall eingeschaltet ist. Gehen Sie dazu in folgendes Menü:

(1) Gehen Sie zu **Firewall** -> **Richtlinien** -> **Optionen**.

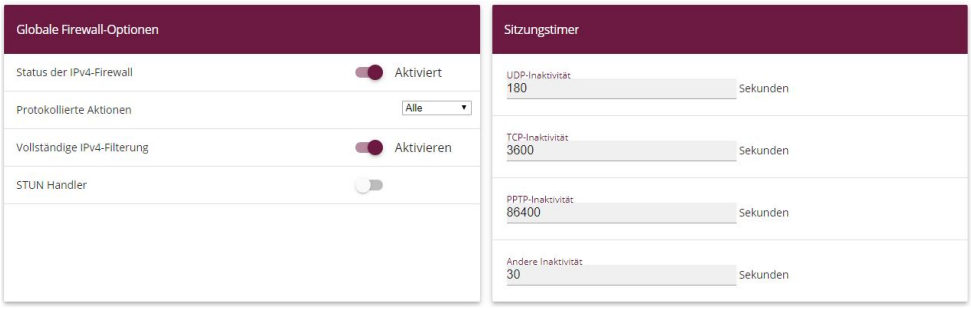


Abb. 116: **Firewall** -> **Richtlinien** -> **Optionen**

Die Option **Status der IPv4-Firewall** muss auf `Aktiviert` gesetzt sein.

DHCP-Server-Konfiguration

Im Anschluss müssen nun insgesamt 5 DHCP-Server passend zum Netz der jeweiligen Schnittstelle konfiguriert werden.

(1) Gehen Sie zu **Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu**.

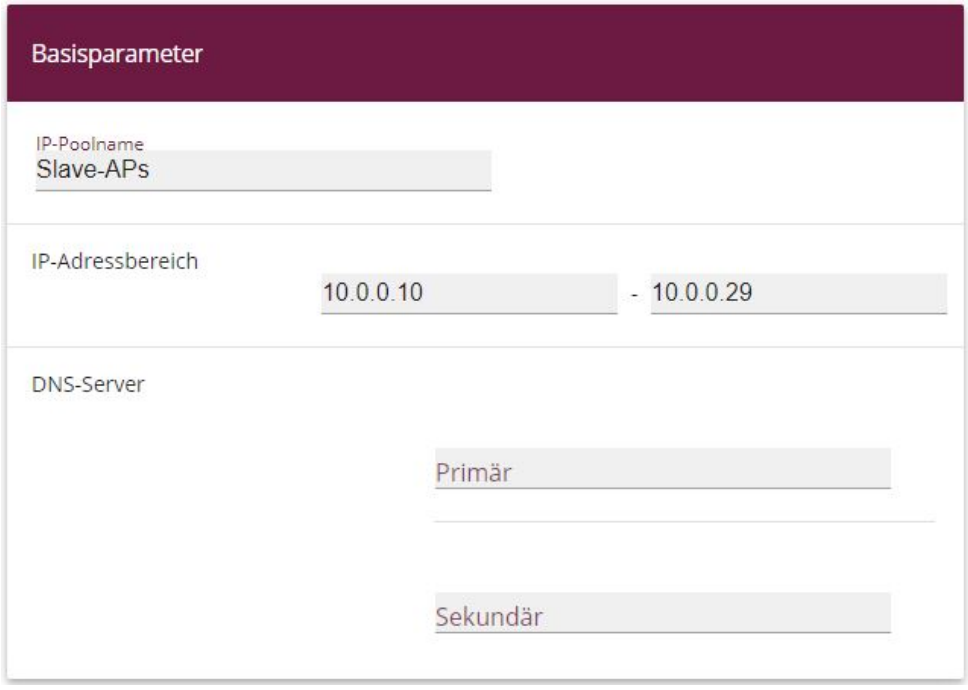


Abb. 117: **Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu**

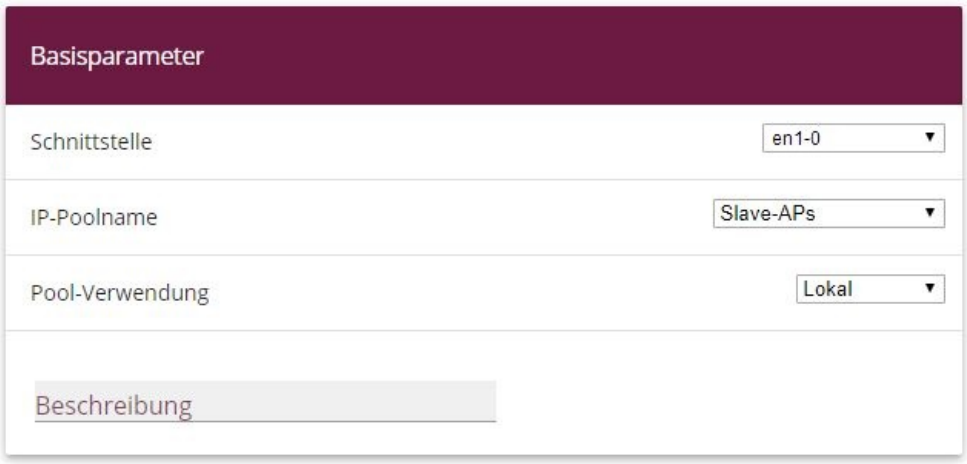
Gehen Sie folgendermaßen vor, um den IP-Adress-Pool für die Slave-APs einzurichten:

(1) Geben Sie einen **IP-Poolnamen** ein, um den IP-Pool eindeutig zu benennen, z. B. *Slave-APs*.

(2) Geben Sie einen **IP-Adressbereich** an. In unserem Beispiel nehmen wir den IP-Adressbereich von *10.0.0.10* bis *10.0.0.29*. Die Größe des IP-Adressbereichs richtet sich nach der Anzahl der maximal benötigten Access Points (in unserem Beispiel 6 plus Reserve). Die übrigen Adressen können somit für andere Infrastruktur im selben Netz verwendet werden.

(3) Bestätigen Sie Ihre Angaben mit **OK**.

Im Menü **Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu** können Sie nun die weitere Konfiguration vornehmen.



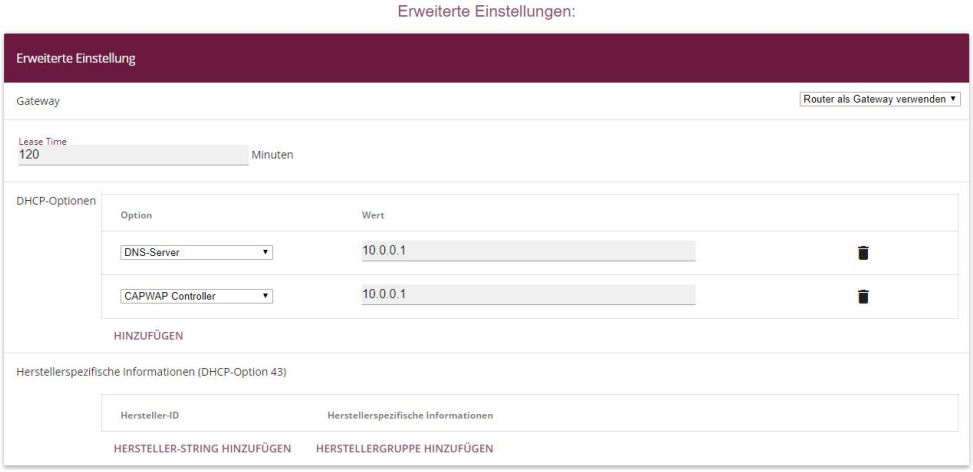


Abb. 119: **Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Bei **Schnittstelle** wählen Sie die logische Schnittstelle *en1-0* aus.

(2) Wählen Sie einen gültigen **IP-Pool** aus, hier z. B. *Slave-APs* .

(3) Klicken Sie auf **Erweiterte Einstellungen**.

(4) Für das **Gateway** belassen Sie die Einstellung *Router als Gateway verwenden*. Die momentane IP-Adresse der Schnittstelle *en1-0* wird als Standardgateway an die DHCP-Geräte propagiert.

(5) Bei **DHCP-Optionen** klicken Sie auf **Hinzufügen**.

(6) Wählen Sie die Option *DNS-Server* aus, und geben Sie die IP-Adresse der Schnittstelle *en1-0* ein, hier *10.0.0.1*.

(7) Klicken Sie erneut auf **Hinzufügen**.

(8) Wählen Sie die Option *CAPWAP Controller* aus, und geben Sie die IP-Adresse der Schnittstelle *en1-0* ein, hier *10.0.0.1*.

(9) Bestätigen Sie Ihre Angaben mit **OK**.

Weitere DHCP-Optionen sind für den korrekten Betrieb der Slave-Access Points nicht notwendig.

Im nächsten Schritt wird der **DHCP Pool** *Mitarbeiter-WLAN* eingerichtet.

Gehen Sie zu **Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu**.

(1) Geben Sie einen **IP-Poolnamen** ein, um den IP-Pool eindeutig zu benennen, z. B. *Mitarbeiter-WLAN*.

(2) Geben Sie einen **IP-Adressbereich** an, in unserem Beispiel den IP-Adressbereich von *10.0.10.10* bis *10.0.10.254* . Die noch freien 8 Adressen unterhalb von

10.0.10.10 können somit für weitere statisch konfigurierte Infrastruktur im selben Netz verwendet werden.

(3) Bestätigen Sie Ihre Angaben mit **OK**.

(4) Gehen Sie in das Menü **Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**.

(5) Bei **Schnittstelle** wählen Sie die Schnittstelle *en1-0-1* aus.

(6) Wählen Sie einen gültigen **IP-Pool** aus, hier z. B. *Mitarbeiter-WLAN* .

(7) Klicken Sie auf **Erweiterte Einstellungen**.

(8) Für das **Gateway** belassen Sie die Einstellung *Router als Gateway verwenden*.

(9) Bei **DHCP-Optionen** klicken Sie auf **Hinzufügen**.

(10) Wählen Sie die Option *DNS-Server* aus, und geben Sie die IP-Adresse der Schnittstelle *en1-0* ein, hier *10.0.10.1*.

(11) Bestätigen Sie Ihre Angaben mit **OK**.

Gehen Sie folgendermaßen vor, um einen weiteren IP-Adress-Pool für den *Gast-WLAN* einzurichten:

Gehen Sie zu **Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu**.

(1) Geben Sie einen **IP-Poolnamen** ein, z. B. *Gast_WLAN*.

(2) Geben Sie einen **IP-Adressbereich** an, in unserem Beispiel den IP-Adressbereich von *10.0.20.10* bis *10.0.20.254* .

(3) Bestätigen Sie mit **OK**.

(4) Gehen Sie in das Menü **Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**.

(5) Bei **Schnittstelle** wählen Sie die Schnittstelle *en1-0-2* aus.

(6) Wählen Sie einen gültigen **IP-Pool** aus, hier z. B. *Gast-WLAN* .

(7) Klicken Sie auf **Erweiterte Einstellungen**.

(8) Für das **Gateway** belassen Sie die Einstellung *Router als Gateway verwenden*.

(9) Bei **DHCP-Optionen** klicken Sie auf **Hinzufügen**.

(10) Wählen Sie die Option *DNS-Server* aus, und geben Sie die IP-Adresse der Schnittstelle, hier *10.0.20.1* , ein.

(11) Bestätigen Sie Ihre Angaben mit **OK**.

Verfahren Sie analog, um den **DHCP Pool** für das *Mitarbeiter-Ethernet* zu konfigurieren.

Gehen Sie zu **Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu**.

(1) Geben Sie einen **IP-Poolnamen** ein, z. B. *Mitarbeiter-Ethernet*.

(2) Geben Sie einen **IP-Adressbereich** an, in unserem Beispiel den IP-Adressbereich von *10.0.1.10* bis *10.0.1.254* .

(3) Bestätigen Sie mit **OK**.

(4) Gehen Sie in das Menü **Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**.

(5) Bei **Schnittstelle** wählen Sie die Schnittstelle *en1-1* aus.

(6) Wählen Sie einen gültigen **IP-Pool** aus, hier z. B. *Mitarbeiter-Ethernet* .

(7) Klicken Sie auf **Erweiterte Einstellungen**.

(8) Für das **Gateway** belassen Sie die Einstellung *Router als Gateway verwenden*.

(9) Bei **DHCP-Optionen** klicken Sie auf **Hinzufügen**.

(10) Wählen Sie die Option *DNS-Server* aus, und geben Sie die IP-Adresse der Schnittstelle, hier *10.0.1.1* , ein.

(11) Bestätigen Sie Ihre Angaben mit **OK**.

Am Schluss konfigurieren Sie noch den **DHCP Pool** für das *Gast-Ethernet*.

Gehen Sie zu **Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu**.

(1) Geben Sie einen **IP-Poolnamen** ein, z. B. *Gast-Ethernet*.

(2) Geben Sie einen **IP-Adressbereich** an. In unserem Beispiel den IP-Adressbereich von *10.0.2.10* bis *10.0.2.254* .

(3) Bestätigen Sie mit **OK**.

(4) Gehen Sie in das Menü **Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**.

(5) Bei **Schnittstelle** wählen Sie die Schnittstelle *en1-2* aus.

(6) Wählen Sie einen gültigen **IP-Pool** aus, hier z. B. *Gast-Ethernet* .

(7) Klicken Sie auf **Erweiterte Einstellungen**.

(8) Für das **Gateway** belassen Sie die Einstellung *Router als Gateway verwenden*.

(9) Bei **DHCP-Optionen** klicken Sie auf **Hinzufügen**.

(10) Wählen Sie die Option *DNS-Server* aus, und geben Sie die IP-Adresse der Schnittstelle, hier *10.0.2.1* ein.

(11) Bestätigen Sie Ihre Angaben mit **OK**.

Die Liste der konfigurierten DHCP Pools sieht nun wie folgt aus:

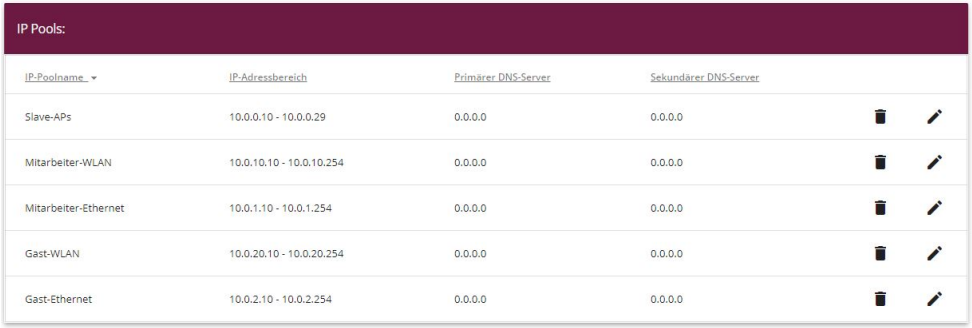


Abb. 120: **Lokale Dienste** -> **DHCP-Server** -> **IP- Pool-Konfiguration**

WLAN Controller-Einrichtung

Nun kann der **Wireless LAN Controller** auf der Schnittstelle `en1-0` aktiviert werden.

(1) Gehen Sie zu **Wireless LAN Controller** -> **Controller-Konfiguration** -> **Allgemein**.

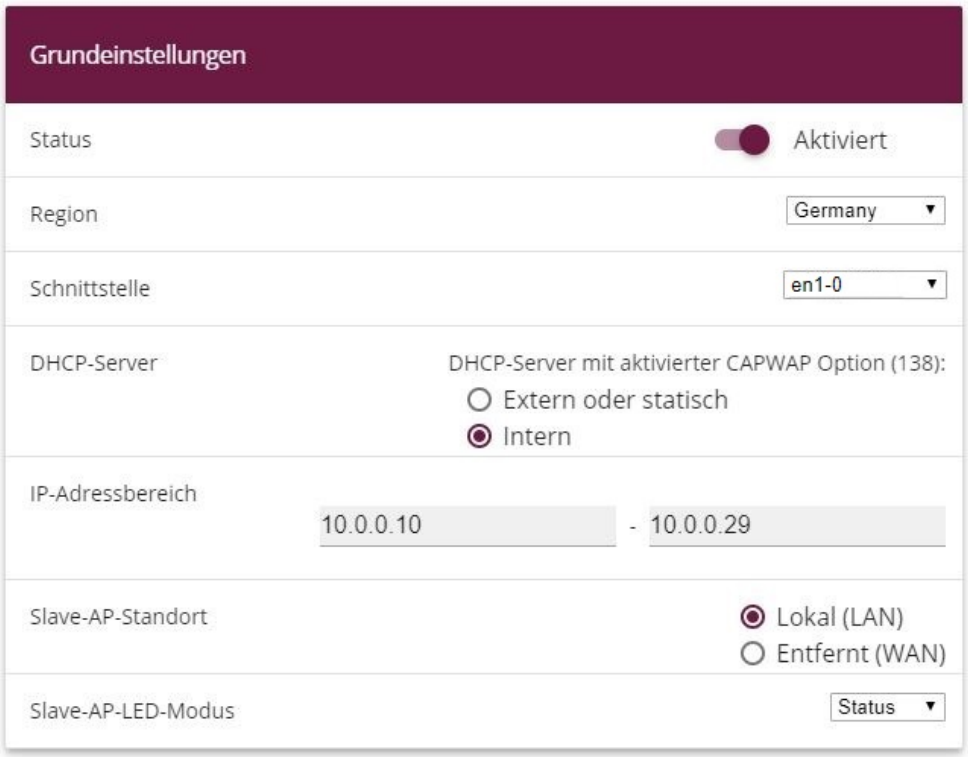


Abb. 121: **Wireless LAN Controller** -> **Controller-Konfiguration** -> **Allgemein**

Gehen Sie folgendermaßen vor:

(1) Die **Region** muss passend zum Standort der Access Points eingerichtet werden, in unserem Beispiel *Germany*. Die WLAN-Funkmodule der Access Points werden damit nur innerhalb des gesetzlich erlaubten Rahmens des jeweiligen Landes betrieben.

(2) Als **Schnittstelle** des WLAN Controllers wählen Sie *en1-0* aus.

(3) Nach der Auswahl der Schnittstelle wechselt die **DHCP-Server**-Einstellungen automatisch auf *Intern* .

(4) Unter **IP-Adressbereich** wird der Adressbereich angezeigt, der im Menü DHCP-Pools auf der Schnittstelle *en1-0* konfiguriert wurde, hier *10.0.0.10* - *10.0.0.29*.

(5) Belassen Sie den **Slave-AP-Standort** auf *Lokal (LAN)*.

(6) Bestätigen Sie mit **OK**.

Die Einstellungen sind jetzt aktiv und der WLAN Controller wird gestartet.

Anschließend werden die **Drahtlosnetzwerke (VSS)** bearbeitet.

Gehen Sie in folgendes Menü, um Ihr WLAN-Netzwerk zu erstellen:

(1) Gehen Sie zu **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)**.

Konfigurieren Sie die WLAN-Verbindung, indem Sie den Standardeintrag bearbeiten. Klicken Sie dazu bei dem vorhandenen Eintrag **<vss-1>** auf das -Symbol.

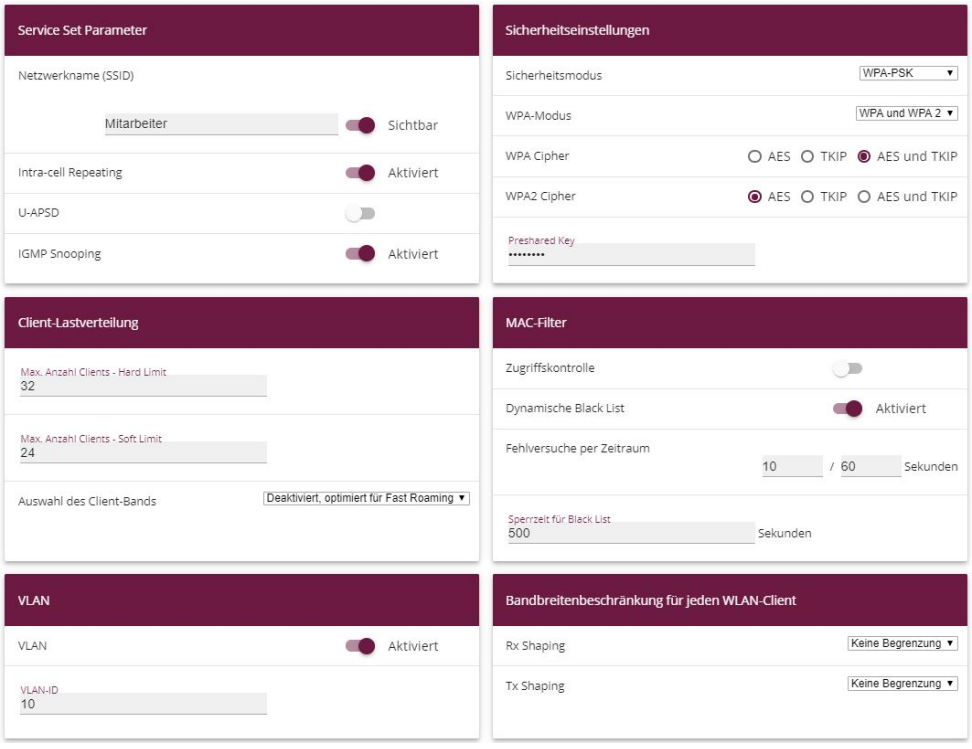


Abb. 122: **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)** -> **<vss-1>**

Gehen Sie folgendermaßen vor:

(1) Unter **Netzwerkname (SSID)** tragen Sie z. B. *Mitarbeiter* ein. Die Option **Sichtbar** bleibt aktiviert.

(2) Den **Sicherheitsmodus** stellen Sie auf *WPA-PSK*.

(3) Den **WPA-Modus** lassen Sie auf *WPA und WPA2*.

(4) Der **WPA Cipher** wird auf *TKIP* gesetzt.

(5) Setzen Sie den **WPA2 Cipher** auf *AES*.

(6) Der **Preshared Key** ist das WLAN-Zugangspasswort für alle Mitarbeiter. Geben Sie eine ASCII-Zeichenfolge mit 8 - 63 Zeichen ein.

(7) Aktivieren Sie die Option **VLAN**.

(8) Geben Sie die **VLAN-ID** *10* ein.
Dies bewirkt, dass alle Daten der später mit der SSID *Mitarbeiter* verbundenen WLAN-Geräte von den Slave-Access Points im Ethernet mit der **VLAN-ID** *10* markiert werden. Somit ist der Mitarbeiterdatenverkehr zwischen Router und Access Points auch auf Ethernet-Ebene (Layer 2) ein eigenständiger Netzbereich.

(9) Bestätigen Sie mit **OK**.

Wählen Sie die Schaltfläche **Neu**, um ein Drahtlosnetzwerk für den Gastzugang zu konfigurieren.

(1) Gehen Sie zu **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)** -> **Neu**.

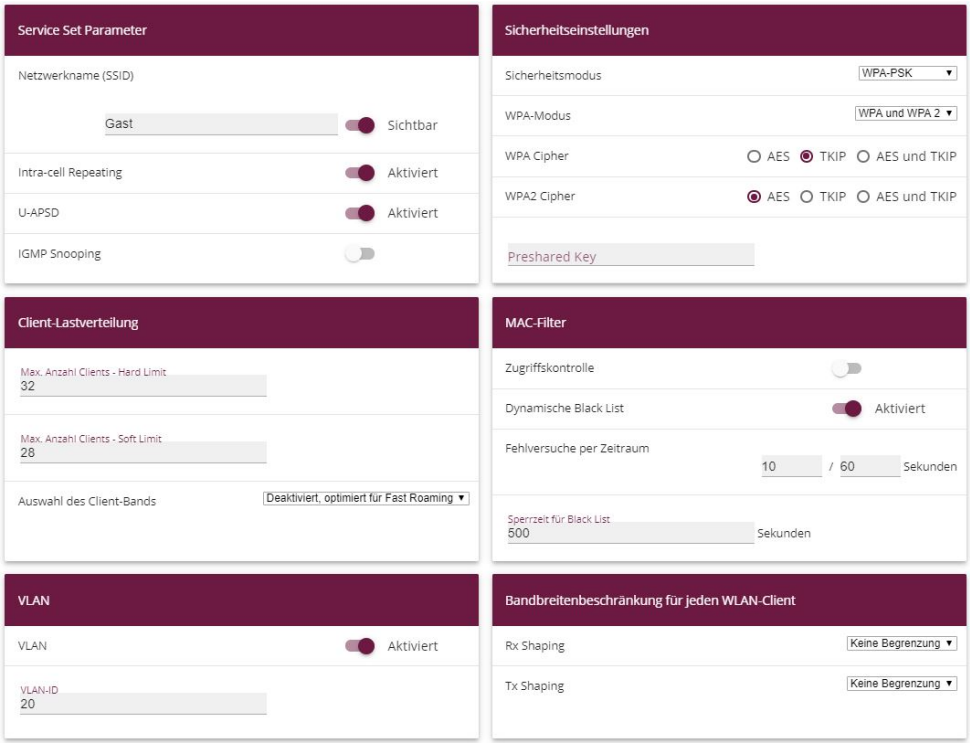


Abb. 123: **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetzwerke (VSS)** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Unter **Netzwerkname (SSID)** tragen Sie z. B. `Gast` ein. Die Option **Sichtbar** bleibt aktiviert.

(2) Den **Sicherheitsmodus** stellen Sie auf `WPA-PSK`.

(3) Den **WPA-Modus** lassen Sie auf `WPA und WPA2`.

(4) Der **WPA Cipher** wird auf `TKIP` gesetzt.

(5) Setzen Sie den **WPA2 Cipher** auf `AES`.

(6) Das **Preshared Key** ist das WLAN-Zugangspasswort für alle Gäste. Geben Sie eine ASCII Zeichenfolge mit 8 - 63 Zeichen ein.

(7) Aktivieren Sie die Option **VLAN**.

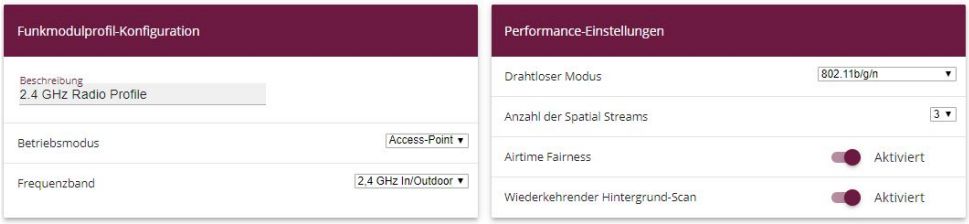
(8) Geben Sie die **VLAN-ID** *20* ein.

(9) Bestätigen Sie mit **OK**.

Im nächsten Schritt werden die **Funkmodulprofile** bearbeitet. Konfigurieren Sie die **Funkmodulprofile**, indem Sie den Standardeintrag bearbeiten.

(1) Gehen Sie zu **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Funkmodulprofile** .

(2) Klicken Sie bei dem vorhandenen Eintrag **<2.4 GHz Radio Profile>** auf das -Symbol.



Gehen Sie folgendermaßen vor:

(1) Belassen Sie die Einstellung **Frequenzband** = *2.4 GHz In/Outdoor*.

(2) Wählen Sie bei **Drahtloser Modus** *802.11 g/n* aus. Die Änderung des **Drahtlosen Modus** bewirkt, dass alte relativ rar gewordene WLAN-Geräte, die nur 802.11b sprechen, das WLAN nicht mehr nutzen können. Der große Vorteil nur 802.11g/n zu erlauben besteht darin, dass der Datendurchsatz für alle angeschlossenen WLAN-Geräte nicht mehr automatisch drastisch reduziert wird, sobald ein WLAN-Gerät versucht im 802.11b-Modus ins WLAN-Netz zu gelangen.

(3) Aktivieren Sie die Option **Burst-Mode**, um die Übertragungsgeschwindigkeit zu erhöhen.

(4) Klicken Sie auf **Erweiterte Einstellungen**.

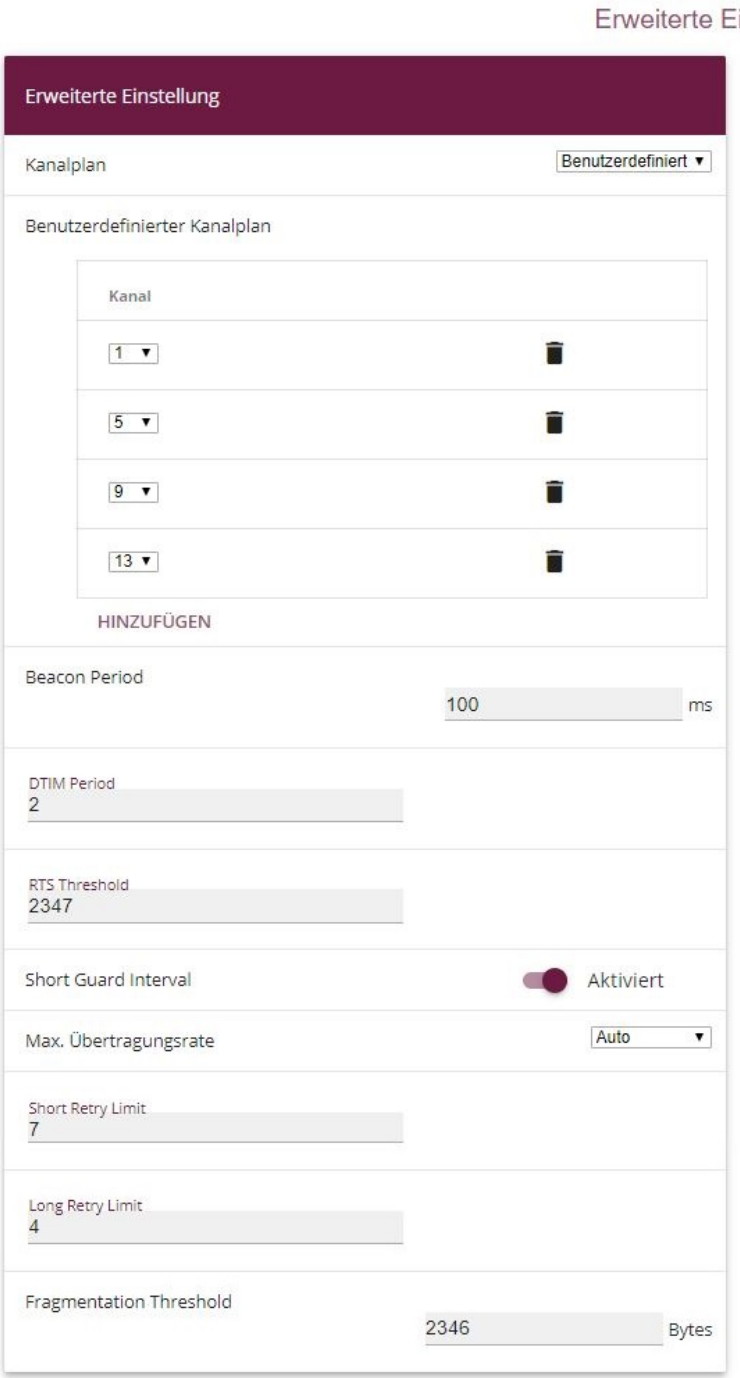


Abb. 125: **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Funkmodulpro-**

file -> **<2.4 GHz Radio Profile>**

(5) Wählen Sie den gewünschten **Kanalplan** aus. Mit *Benutzerdefiniert* können Sie die gewünschten Kanäle selbst auswählen.

(6) Unter **Benutzerdefinierter Kanalplan** wählen Sie die erlaubten Kanäle, *1*, *5*, *9* und *13* aus. Dieser Kanalplan ist für alle Länder, in denen die Kanäle 1 bis 13 erlaubt sind, als optimaler Kanalplan empfohlen und hat bei 802.11g/n keine (nennenswerte) Frequenzüberlappung. Die Access Points haben somit mehr Auswahlmöglichkeiten, einen möglichst störungsfreien Kanal zu nutzen, was die Leistungsfähigkeit und Zuverlässigkeit des gesamten WLANs steigert.

(7) Aktivieren Sie die Funktion **Short Guard Interval**, um das Guard Interval (= Zeit zwischen der Übertragung von zwei Datensymbolen) von 800 ns auf 400 ns zu verkürzen.

(8) Belassen Sie die übrigen Einstellungen und bestätigen Sie mit **OK**.

Somit sind alle benötigten Profile im WLAN Controller eingerichtet.

Jetzt werden die Access Points aktiviert und eingerichtet. Im Menü **Slave Access Points** wird eine Liste aller mit Hilfe des **Wizard** gefundenen APs angezeigt, hier z. B. eine **bintec W2003ac**.

(1) Gehen Sie zu **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Slave Access Points**.

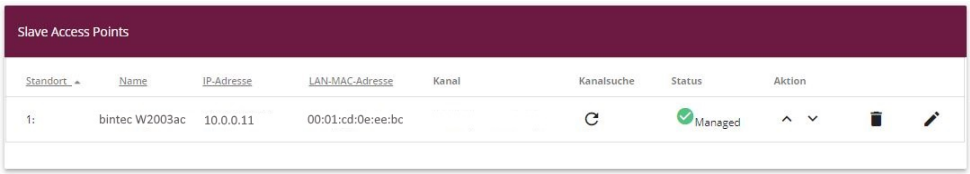


Abb. 126: **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Slave Access Points**

Hinweis

Wenn keine Access Points angezeigt werden, empfiehlt es sich, nochmals die DHCP-Server-Einstellungen für den **DHCP-Pool** *Slave-APs* zu überprüfen, ob er auf die korrekte Schnittstelle (hier *en1-0*) gebunden ist und die CAPWAP-Option korrekt (hier *10.0.0.1*) eingerichtet ist. Überprüfen Sie auch, ob im Systembereich auf einem anderen Gerät versehentlich ein weiterer DHCP-Server aktiv ist. Schalten Sie alle Access Points aus und wieder ein, damit sie nochmal die Netzkonfigurationseinstellungen vom DHCP-Server beziehen.

Zum Schluss werden die zuvor konfigurierten **Funkmodulprofile** und **Drahtlosnetzwerke** für jeden Access Point eingerichtet.

(1) Gehen Sie zu **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Slave Access Points** .

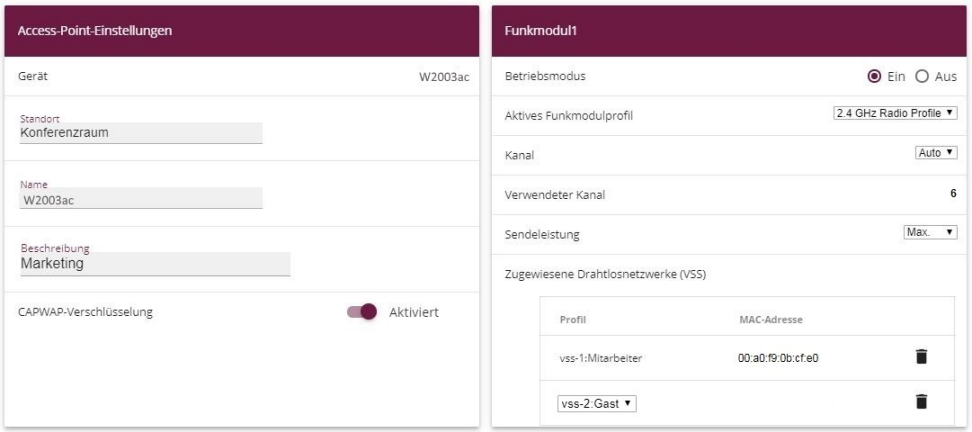


Abb. 127: **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Slave Access Points**

Gehen Sie folgendermaßen vor:

(1) Bei **Standort** geben Sie z. B. `Konferenzraum` ein.

(2) Bei **Beschreibung** geben Sie z. B. `Marketing` ein.

(3) Bei **CAPWAP-Verschlüsselung** belassen Sie `Aktiviert` .

(4) Bei **Betriebsmodus** belassen Sie `Ein` . Dies bewirkt, dass alle Einstellungen in den gewählten Funkmodulprofilen verwendet werden.

(5) Als **Aktives Funkmodulprofil** wählen Sie das zuvor konfigurierte Funkmodulprofil, hier `2.4 GHz Radio Profile` aus.

(6) Den **Kanal** belassen Sie auf `Auto` (er wird somit anhand des Kanalplan des Funkprofils und der WLAN-Umgebung dynamisch bestimmt).

(7) Bei **Zugewiesen Drahtlosnetzwerke (VSS)** werden die beiden konfigurierten Drahtlosnetzwerke `Mitarbeiter` und `Gast` dem Funkmodul zugewiesen.

(8) Bestätigen Sie mit **OK**.

Konfigurieren Sie analog dazu alle gefundenen Access-Points.

Hinweis

Jeder Access Point muss eine eindeutige Standortbezeichnung bekommen. Andernfalls wird man im laufenden Betrieb die Access Points nicht mehr voneinander unterscheiden können.

Die Liste der konfigurierten Access Points (hier z. B. eine **w2003ac**) sieht nun wie folgt aus:

Abb. 128: **Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Slave Access Points**

Nachdem alle Access Points eingerichtet sind, werden sie nach einer kurzen Initialisierungsphase mit dem Status `Managed` gekennzeichnet und sind somit nun in Betrieb. Zudem sind sie durch den WLAN-Controller gegen jede Art eines externen Konfigurationszugriffs gesperrt.

Durch Klicken auf die ^-Schaltfläche oder die v-Schaltfläche in der Spalte **Aktion** wählen Sie aus, ob der gewählte Access Point vom WLAN Controller verwaltet werden soll.

Sie können einen Access Point vom WLAN Controller trennen und ihn somit aus Ihrer WLAN-Infrastruktur entfernen, indem Sie auf die v-Schaltfläche klicken. Der Access Point bekommt dann den Status `Gefunden`, aber nicht mehr `Managed`.

Die auf der Übersichtsseite angezeigten momentan verwendeten WLAN-Kanäle sind noch nicht optimal, da sich die Access Points während der initialen Inbetriebnahme nur auf die allgemeine WLAN-Umgebung abstimmen konnten.

Klicken Sie unter **Neue Kanalfestlegung** auf die Schaltfläche **START**, um die zugewiesenen Kanäle optimal gegenseitig abstimmen zu lassen.

Wenn die Kanalfestlegung abgeschlossen ist, sollten jeweils direkt benachbarte Access Points unterschiedliche Kanäle haben.

Die WLAN Controller-Konfiguration und die Konfiguration des Routers als Zugangsgateway ist somit abgeschlossen. Speichern Sie die Konfiguration mit **Konfiguration speichern** und bestätigen Sie die Auswahl mit **OK**.

Hinweis

In manchen Fällen kann es passieren, dass auch nach der neuen Kanalfestlegung einzelne benachbarte Access Points dennoch denselben Kanal belegen. Dies passiert immer dann, wenn sich benachbarte Access Points nur unzureichend oder gar nicht gegenseitig per WLAN erkennen können. Bei korrekten Abständen der Access Points sind starke lokale Störeinflüsse durch fremde Access Points eine häufige Ursache hierfür oder eine schwierige Gebäudestruktur wie (zumeist geschlossene) Feuerschutztüren aus Stahl zwischen zwei unmittelbar benachbarten Gebäudebereichen. In diesem Fall empfiehlt es sich, für diese einzelnen betroffenen Access Points paarweise manuell einen fixen Kanal (passend zum Kanalplan) für die Funkmodule zu setzen und die Kanalneusuche erneut zu starten. Dadurch werden für die übrigen mit automatischer Kanalwahl konfigurierten Access Points die Kanäle passend zur Umgebung der fix eingerichteten Access Points vergeben.

7.3 Konfigurationsschritte im Überblick

Schnittstellen zuweisen

Field	Menu	Value
Switch-Port 1 bis 5	**Physikalische Schnittstellen** -> **Ethernet-Ports** -> **Portkonfiguration**	*en1-0* bis *en1-4*

Internetzugang einrichten

Field	Menu	Value
Verbindungstyp	**Assistenten** -> **Internetzugang** -> **Internetverbindungen** -> **Neu**	*Externes Gateway/ Kabelmodem*
Physischer Ethernet-Port	**Assistenten** -> **Internetzugang** -> **Internetverbindungen** -> **Weiter**	*ETH5*
Internet Service Provider	**Assistenten** -> **Internetzugang** -> **Internetverbindungen** -> **Weiter**	*-Benutzerdefiniert-*
IP-Parameter dynamisch abrufen	**Assistenten** -> **Internetzugang** -> **Internetverbindungen** -> **Weiter**	Deaktiviert
Lokale IP-Adresse	**Assistenten** -> **Internetzugang** -> **Internetverbindungen** -> **Weiter**	z. B. *1.2.3.4*
Gateway-IP-Adresse	**Assistenten** -> **Internetzugang** -> **Internetverbindungen** -> **Weiter**	z. B. *1.2.3.1*
Netzmaske	**Assistenten** -> **Internetzugang** -> **Internetverbindungen** -> **Weiter**	*255.255.255.0*

Field	Menu	Value
DNS-Server 1	**Assistenten** -> **Internetzugang** -> **Internetverbindungen** -> **Weiter**	z. B. *1.2.3.1*

Schnittstellen konfigurieren

Field	Menu	Value
IP-Adresse/Netzmaske	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>**	*10.0.0.1* und *255.255.255.0*
IP-Adresse/Netzmaske	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-1>**	*10.0.1.1* und *255.255.255.0*
IP-Adresse/Netzmaske	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-2>**	*10.0.2.1* und *255.255.255.0*
Basierend auf Ethernet-Schnittstelle	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **Neu**	*en1-0*
Adressmodus	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **Neu**	*Statisch*
IP-Adresse/Netzmaske	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **Neu**	*10.0.10.1* und *255.255.255.0*
Schnittstellenmodus	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **Neu**	*Tagged (VLAN)*
VLAN-ID	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **Neu**	*10*
Basierend auf Ethernet-Schnittstelle	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **Neu**	*en1-0*
Adressmodus	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **Neu**	*Statisch*
IP-Adresse/Netzmaske	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **Neu**	*10.0.20.1* und *255.255.255.0*
Schnittstellenmodus	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **Neu**	*Tagged (VLAN)*
VLAN-ID	**LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **Neu**	*20*

Zugriff einrichten

Field	Menu	Value
en1-0	**Systemverwaltung** -> **Administrativer Zugriff** -> **Zugriff**	*Telnet*, *SSH*, *HTTP*, *HTTPS*, *Ping*, *SNMP*
en1-1 bis en1-4	**Systemverwaltung** -> **Administrati-**	*Ping*

Field	Menu	Value
	ver Zugriff -> **Zugriff**	

Passwort ändern

Field	Menu	Value
Systemadministrator-Passwort	**Systemverwaltung** -> **Globale Einstellungen** -> **Passwörter**	z. B. *test12345*
Systemadministrator-Passwort bestätigen	**Systemverwaltung** -> **Globale Einstellungen** -> **Passwörter**	z. B. *test12345*

Firewall einrichten

Field	Menu	Value
Beschreibung	**Firewall** -> **Dienste** -> **Gruppen** -> **Neu**	*Lokale-Dienste*
Mitglieder	**Firewall** -> **Dienste** -> **Gruppen** -> **Neu**	z. B. *echo*, *dns*, *dhcp*, *ntp*

Adressen definiern

Field	Menu	Value
Beschreibung	**Firewall** -> **Adressen** -> **Adressliste** -> **Neu**	*Broadcast*
Adresse/Subnetz	**Firewall** -> **Adressen** -> **Adressliste** -> **Neu**	*255.255.255.255* / *255.255.255.255*
Beschreibung	**Firewall** -> **Adressen** -> **Adressliste** -> **Neu**	z. B. *Mitarbeiter-LAN-GW*
Adresse/Subnetz	**Firewall** -> **Adressen** -> **Adressliste** -> **Neu**	*10.0.1.1* / *255.255.255.255*
Beschreibung	**Firewall** -> **Adressen** -> **Adressliste** -> **Neu**	*Gast-LAN-GW*
Adresse/Subnetz	**Firewall** -> **Adressen** -> **Adressliste** -> **Neu**	*10.0.2.1* / *255.255.255.255*
Beschreibung	**Firewall** -> **Adressen** -> **Adressliste** -> **Neu**	*Mitarbeiter-WLAN-GW*
Adresse/Subnetz	**Firewall** -> **Adressen** -> **Adressliste** -> **Neu**	*10.0.10.1* / *255.255.255.255*
Beschreibung	**Firewall** -> **Adressen** -> **Adressliste** -> **Neu**	*Gast-WLAN-GW*
Adresse/Subnetz	**Firewall** -> **Adressen** -> **Adressliste** -> **Neu**	*10.0.20.1* / *255.255.255.255*

Gruppen definiern

Field	Menu	Value
Beschreibung	**Firewall** -> **Schnittstellen** -> **IPv4-Gruppen** -> **Neu**	*Mitarbeiter*
Mitglieder	**Firewall** -> **Schnittstellen** -> **IPv4-Gruppen** -> **Neu**	*LAN_EN1-1*, *LEASED_EN1-0-1*
Beschreibung	**Firewall** -> **Schnittstellen** -> **IPv4-Gruppen** -> **Neu**	*Gast*
Mitglieder	**Firewall** -> **Schnittstellen** -> **IPv4-Gruppen** -> **Neu**	*LAN_EN1-2*, *LEASED_EN1-0-2*
Beschreibung	**Firewall** -> **Schnittstellen** -> **IPv4-Gruppen** -> **Neu**	*Benutzer*
Mitglieder	**Firewall** -> **Schnittstellen** -> **IPv4-Gruppen** -> **Neu**	*LAN_EN1-1*, *LAN_EN1-2*, *LEASED_EN1-0-1*, *LEASED_EN1-0-2*

Richtlinien erstellen (über den Router verbundene Netzbereiche)

Field	Menu	Value
Quelle	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*LAN_EN1-0*
Ziel	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*ANY*
Dienst	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*any*
Aktion	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Zugriff*
Quelle	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Mitarbeiter*
Ziel	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Benutzer*
Dienst	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*any*
Aktion	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Zugriff*
Quelle	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Gast*
Ziel	**Firewall** -> **Richtlinien** ->	*Gast*

Field	Menu	Value
	IPv4-Filterregeln -> **Neu**	
Dienst	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*any*
Aktion	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Zugriff*
Quelle	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Benutzer*
Ziel	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*LAN_EN1-4*
Dienst	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*any*
Aktion	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Zugriff*

Richtlinien erstellen (auf den Router gebundene IP-Adressen)

Field	Menu	Value
Quelle	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Benutzer*
Ziel	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Broadcast*
Dienst	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Lokale-Dienste*
Aktion	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Zugriff*
Quelle	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*LAN_EN1-1*
Ziel	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Mitarbeiter-LAN-GW*
Dienst	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Lokale-Dienste*
Aktion	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Zugriff*
Quelle	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*LAN_EN1-2*
Ziel	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Gast-LAN-GW*
Dienst	**Firewall** -> **Richtlinien** ->	*Lokale-Dienste*

Field	Menu	Value
	IPv4-Filterregeln -> **Neu**	
Aktion	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Zugriff*
Quelle	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*LEASED_EN1-0-1*
Ziel	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Mitarbeiter-WLAN-GW*
Dienst	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Lokale-Dienste*
Aktion	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Zugriff*
Quelle	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*LEASED_EN1-0-2*
Ziel	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Gast-WLAN-GW*
Dienst	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Lokale-Dienste*
Aktion	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Zugriff*

DHCP-Konfiguration

Field	Menu	Value
IP-Poolname	**Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu**	z. B. *Slave-APs*
IP-Adressbereich	**Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu**	*10.0.0.10* - *10.0.0.29*
Schnittstelle	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	*en1-0*
IP-Poolname	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	z. B. *Slave-APs*
Pool-Verwendung	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	*Lokal*
Gateway	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	*Router als Gateway verwenden*
DHCP-Optionen	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	*DNS-Server* / *10.0.0.1* und *CAPWAP Controller* /

Field	Menu	Value
		10.0.0.1
IP-Poolname	**Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu**	z. B. *Mitarbeiter-WLAN*
IP-Adressbereich	**Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu**	*10.0.10.10* - *10.0.10.254*
Schnittstelle	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	*en1-0-1*
IP-Poolname	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	z. B. *Mitarbeiter-WLAN*
Pool-Verwendung	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	*Lokal*
Gateway	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	*Router als Gateway verwenden*
DHCP-Optionen	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	*DNS-Server* / *10.0.10.1*
IP-Poolname	**Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu**	z. B. *Gast-WLAN*
IP-Adressbereich	**Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu**	*10.0.20.10* - *10.0.20.254*
Schnittstelle	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	*en1-0-2*
IP-Poolname	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	z. B. *Gast-WLAN*
Pool-Verwendung	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	*Lokal*
Gateway	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	*Router als Gateway verwenden*
DHCP-Optionen	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	*DNS-Server* / *10.0.20.1*
IP-Poolname	**Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu**	z. B. *Mitarbeiter-Ethernet*
IP-Adressbereich	**Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu**	*10.0.1.10* - *10.0.1.254*
Schnittstelle	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	*en1-1*
IP-Poolname	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	z. B. *Mitarbeiter-Ethernet*

Field	Menu	Value
Pool-Verwendung	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	*Lokal*
Gateway	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	*Router als Gateway verwenden*
DHCP-Optionen	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	*DNS-Server* / *10.0.1.1*
IP-Poolname	**Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu**	z. B. *Gast-Ethernet*
IP-Adressbereich	**Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu**	*10.0.2.10* - *10.0.2.254*
Schnittstelle	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	*en1-2*
IP-Poolname	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	z. B. *Gast-Ethernet*
Pool-Verwendung	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	*Lokal*
Gateway	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	*Router als Gateway verwenden*
DHCP-Optionen	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	*DNS-Server* / *10.0.2.1*

Wireless LAN Controller konfigurieren

Field	Menu	Value
Region	**Wireless LAN Controller** -> **Controller-Konfiguration** -> **Allgemein**	*Germany*
Schnittstelle	**Wireless LAN Controller** -> **Controller-Konfiguration** -> **Allgemein**	*LAN_EN1-0*
DHCP-Server	**Wireless LAN Controller** -> **Controller-Konfiguration** -> **Allgemein**	*Intern*
IP-Adressbereich	**Wireless LAN Controller** -> **Controller-Konfiguration** -> **Allgemein**	*10.0.0.10* - *10.0.0.29*
Slave-AP-Standort	**Wireless LAN Controller** -> **Controller-Konfiguration** -> **Allgemein**	*Lokal (LAN)*

Drahtlosnetzwerke bearbeiten

Field	Menu	Value
Netzwerkname (SSID)	**Wireless LAN Controller** -> **Slave-AP-Konfiguration** -> **Drahtlosnetz-**	z. B. *Mitarbeiter*

Field	Menu	Value
	werke (VSS) -> <vss-1>	
Sicherheitsmodus	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Drahtlosnetzwerke (VSS) -> <vss-1>**	*WPA-PSK*
WPA-Modus	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Drahtlosnetzwerke (VSS) -> <vss-1>**	*WPA und WPA 2*
WPA Cipher	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Drahtlosnetzwerke (VSS) -> <vss-1>**	*TKIP*
WPA2 Cipher	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Drahtlosnetzwerke (VSS) -> <vss-1>**	*AES*
Preshared Key	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Drahtlosnetzwerke (VSS) -> <vss-1>**	Passwort eingeben
VLAN	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Drahtlosnetzwerke (VSS) -> <vss-1>**	*Aktiviert*
VLAN-ID	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Drahtlosnetzwerke (VSS) -> <vss-1>**	*10*
Netzwerkname (SSID)	**Wireless LAN -> WLAN1 -> Drahtlosnetzwerke (VSS) -> Neu**	z. B. *Gast*
Sicherheitsmodus	**Wireless LAN -> WLAN1 -> Drahtlosnetzwerke (VSS) -> Neu**	*WPA-PSK*
WPA-Modus	**Wireless LAN -> WLAN1 -> Drahtlosnetzwerke (VSS) -> Neu**	*WPA und WPA 2*
WPA Cipher	**Wireless LAN -> WLAN1 -> Drahtlosnetzwerke (VSS) -> Neu**	*TKIP*
WPA2 Cipher	**Wireless LAN -> WLAN1 -> Drahtlosnetzwerke (VSS) -> Neu**	*AES*
Preshared Key	**Wireless LAN -> WLAN1 -> Drahtlosnetzwerke (VSS) -> Neu**	Passwort eingeben
VLAN	**Wireless LAN -> WLAN1 -> Drahtlosnetzwerke (VSS) -> Neu**	*Aktiviert*

Field	Menu	Value
VLAN-ID	**Wireless LAN -> WLAN1 -> Drahtlosnetzwerke (VSS) -> Neu**	*20*

Funkmodulprofile bearbeiten

Field	Menu	Value
Frequenzband	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Funkmodulprofile -> <2.4 GHz Radio Profile>**	*2.4 GHz In/Outdoor*
Drahtloser Modus	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Funkmodulprofile -> <2.4 GHz Radio Profile>**	*802.11g/n*
Burst-Mode	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Funkmodulprofile -> <2.4 GHz Radio Profile>**	*Aktiviert*
Kanalplan	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Funkmodulprofile -> <2.4 GHz Radio Profile>** **-> Erweiterte Einstellungen**	Benutzerdefiniert
Benutzerdefinierter Kanalplan	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Funkmodulprofile -> <2.4 GHz Radio Profile>** **-> Erweiterte Einstellungen**	*1*, *5*, *9*, *13*
Short Guard Interval	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Funkmodulprofile -> <2.4 GHz Radio Profile>** **-> Erweiterte Einstellungen**	*Aktiviert*

Slave Access Points einrichten

Field	Menu	Value
Standort	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points**	z. B. *Konferenzraum*
Beschreibung	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points**	z. B. *Marketing*
CAPWAP-Ver-	**Wireless LAN Controller -> Slave-**	*Aktiviert*

Field	Menu	Value
schlüsselung	**AP-Konfiguration -> Slave Access Points**	
Betriebsmodus	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points**	*Ein*
Aktives Funkmodulprofil	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points**	*2.4 GHz Radio Profile*
Kanal	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points**	*Auto*
Zugewiesene Drahtlosnetzwerke (VSS)	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points**	*vss-1: Mitarbeiter* / *vss-2: Gast*
Standort	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points**	z. B. *Küche*
Standort	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points**	z. B. *Terrasse*
Standort	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points**	z. B. *Flur zum Treppenhaus*
Standort	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points**	z. B. *Flurknick*
Standort	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points**	z. B. *Flurende*

Neue Kanalfestlegung

Field	Menu	Value
Neue Kanalfestlegung	**Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points**	**START**

Kapitel 8 WLAN - Netzwerk mit Gäste-WLAN

8.1 Einleitung

Im Folgenden wird beschrieben, wie Sie einen WLAN-Zugang zum lokalen Netzwerk und ein Gäste-WLAN konfigurieren. Um zusätzliche Access Points einzubinden, wird der Wireless LAN Controller verwendet. Zur Trennung der beiden Netze auf Layer2-Ebene wird für das Gästenetzwerk ein VLAN eingerichtet. Die Nutzer des Gäste-WLANs haben uneingeschränkten Zugriff auf das Internet, aber keinen Zugang zum lokalen Netz.

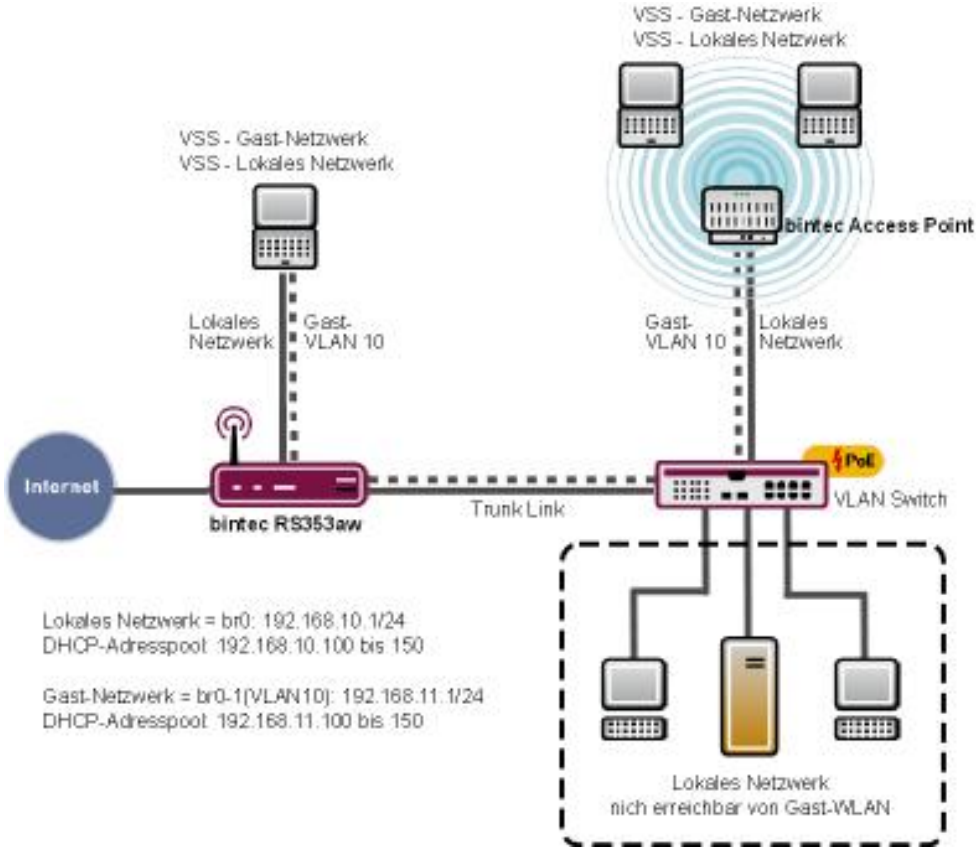


Abb. 129: Beispielszenario WLAN mit Gäste-WLAN

Hinweis

Der Trunk Link (siehe Abbildung) ist mit dem **RS353aw** über einen der vier ETH-Ports (ETH1 bis ETH4) verbunden, die standardmäßig en1-0 zugeordnet sind.

Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Ein Gerät der RS-Serie, eine **be.IP** oder **be.IP plus**
- Ein Bootimage der Version 10.1.9 Patch 3 oder höher
- Switche, die 802.1q VLAN unterstützen

Zur Konfiguration wird das **GUI** (Graphical User Interface) verwendet.

8.2 Konfiguration

8.2.1 IP-Adresse konfigurieren

Konfigurieren Sie eine IP-Adresse auf der LAN-Schnittstelle.

Gehen Sie zu **LAN**->**IP-Konfiguration**->**Schnittstellen**->**<en1-0>**->

Abb. 130: **LAN**->**IP-Konfiguration**->**Schnittstellen**->**<en1-0>**->

Gehen Sie folgendermaßen vor, um die IP-Adresse zu konfigurieren:

(1) Stellen Sie die **Sicherheitsrichtlinie** auf *Vertrauenswürdig*.

(2) Belassen Sie den **Adressmodus** auf *Statisch*.

(3) Geben Sie die **IP-Adresse / Netzmaske** ein, z. B. *192.168.10.1*. Belassen Sie die

Netzmaske `255.255.255.0`.

(4) Bestätigen Sie Ihre Eingaben mit **OK**.

8.2.2 Bridge-Gruppe anlegen und LAN-Schnittstelle zuweisen

Legen Sie eine neue Bridge-Gruppe an und weisen Sie sie der LAN-Schnittstelle zu.

Gehen Sie zu **Systemverwaltung**->**Schnittstellenmodus / Bridge-Gruppen**->**Schnittstellen**.

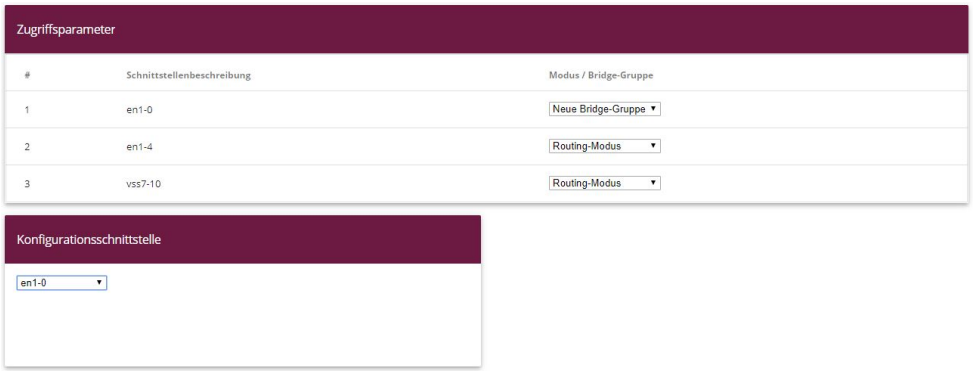


Abb. 131: **Systemverwaltung**->**Schnittstellenmodus / Bridge-Gruppen**->**Schnittstellen**

Gehen Sie folgendermaßen vor, um die LAN-Schnittstelle einer neuen Bridge-Gruppe zuzuweisen und die IP-Adresse der LAN-Schnittstelle auf die Bridge-Gruppe zu übertragen:

(1) Wählen Sie in der Zeile `en1-0` unter **Modus / Bridge-Gruppe** `Neue Bridge-Gruppe` aus.

(2) Wählen Sie als **Konfigurationsschnittstelle** `en1-0`.

Sobald Sie auf **OK** geklickt haben, wird automatisch die Bridge-Gruppe `br0` angelegt und die Schnittstelle `en1-0` dieser Bridge-Gruppe hinzugefügt. Die Bridge-Gruppe `br0` erhält dabei automatisch die IP-Konfiguration der Schnittstelle `en1-0`. Die IP-Konfiguration der Bridge-Gruppe `br0` können Sie im Menü **LAN** -> **IP-Konfiguration** -> **<br0>** -> ✎ überprüfen.

8.2.3 Wireless LAN Controller in Betrieb nehmen

Der IP-Adressbereich, den Sie im Folgenden einrichten, muss zur IP-Adresse der LAN-Schnittstelle passen.

Hinweis

War im Menü **Lokale Dienste**->**DHCP-Server**->**DHCP-Konfiguration** der Schnittstelle *en1-0* bereits ein IP-Pool zugeordnet, so muss dieser Eintrag gelöscht werden.

Gehen Sie in folgendes Menü, um einen IP-Adressbereich einzurichten:

Gehen Sie zu **Wireless LAN Controller**->**Wizard**->**Schritt 1**.

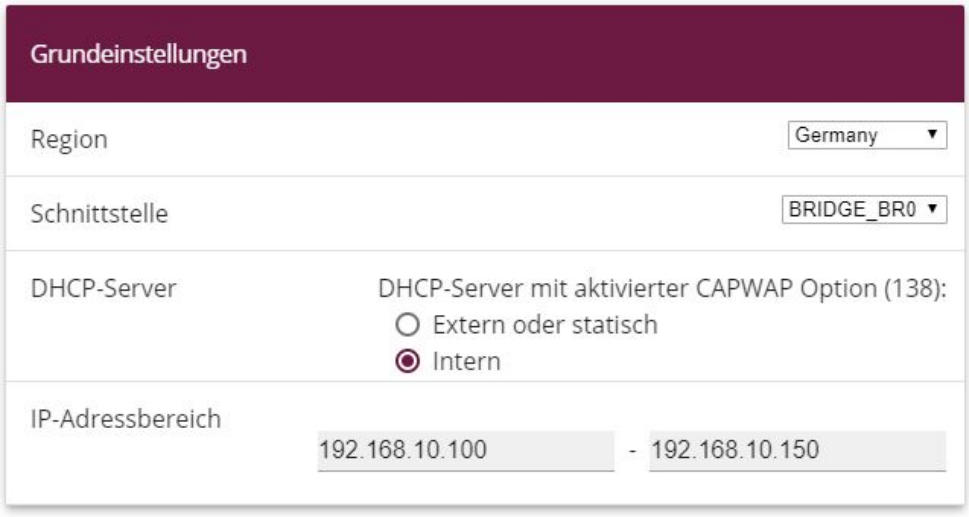


Abb. 132: **Wireless LAN Controller**->**Wizard**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie das Land, in welchem der Wirelless LAN Controller betrieben werden soll. Belassen Sie unter **Region** die Einstellung *Germany*.

(2) Wählen Sie die **Schnittstelle** die für den Wireless Controller verwendet werden soll aus, hier *BRIDGE_BR0*.

(3) Wählen Sie **DHCP-Server** *Intern*.

(4) Geben Sie den ersten und den letzten Wert des **IP-Adressbereichs** ein, z. B. *192.168.10.100* - *192.168.10.150*.

(5) Klicken Sie auf **Weiter**.

8.2.4 Funkmodulprofil auswählen und WLAN-Zugang zum lokalen Netz konfigurieren

Legen Sie fest, welche Funkmodulprofile verwendet werden sollen. Sie sollten **Zwei unabhängige Funkmodulprofile verwenden** aktivieren, wenn in Ihrem Netz Access Points mit zwei 2.4/5 GHz-fähigen Funkmodulen installiert sind.

Schritt 2

Abb. 133: **Wireless LAN Controller->Wizard**

Gehen Sie folgendermaßen vor:

(1) Aktivieren Sie die Option **Zwei unabhängige Funkmodulprofile verwenden**, wenn in Ihrem Netz APs mit zwei Funkmodulen verwendet werden.
Funkmodulprofil für Modul 1 (für alle Access Points) = `2.4 GHz Radio Profile` und **Funkmodulprofil für Modul 2 (nur für APs mit 2 Funkmodulen)** = `5 GHz Radio Profile` wird automatisch ausgewählt und angezeigt.

(2) Klicken Sie auf **Weiter**.
Schritt 3

Abb. 134: **Wireless LAN Controller->Wizard**
Konfigurieren Sie den WLAN-Zugang zu Ihrem lokalen Netz. Klicken Sie dazu bei vss-1 auf das -Symbol.
Schritt 3

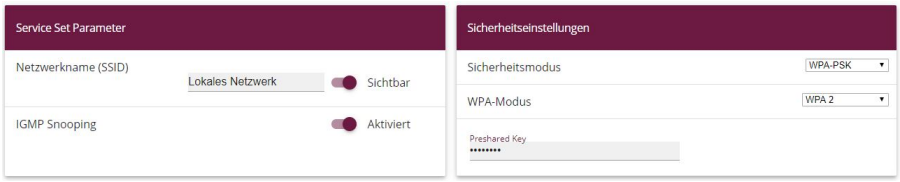


Abb. 135: **Wireless LAN Controller->Wizard-><vss-1>**

(3) Geben Sie einen **Netzwerknamen (SSID)** für Ihr LAN ein, z. B. `Lokaes Netzwerk`.

(4) Geben Sie unter **Preshared Key** ein Passwort, z. B. `supersecret` ein, belassen Sie die Voreinstellungen der übrigen Parameter und klicken Sie auf **OK**.
Sie sehen das lokale Netz, das Sie konfiguriert haben.

8.2.5 Gäste-WLAN konfigurieren

Sie haben einen WLAN-Zugang zu Ihrem lokalen Netz konfiguriert und konfigurieren jetzt ein Gästenetz. Zur Trennung der beiden Netze auf Layer2-Ebene konfigurieren Sie für das Gäste-WLAN ein VLAN, im folgenden Beispiel mit VLAN-ID 10. Alle Datenpakete im Gäste-WLAN sind VLAN 10 getagged, Datenpakete im lokalen WLAN sind untagged.

Hinweis

Beachten Sie, dass die Switche in Ihrem Netz 802.1q VLAN unterstützen müssen, damit die Layer2-Trennung der beiden Netze funktioniert.

Der Wireless LAN Controller konfiguriert Ihre bintec-elmeg Access Points, Ihre Switche müssen Sie selbst entsprechend konfigurieren.

Klicken Sie im **Wireless LAN Controller->Wizard** auf **Hinzufügen**.

Schritt 3

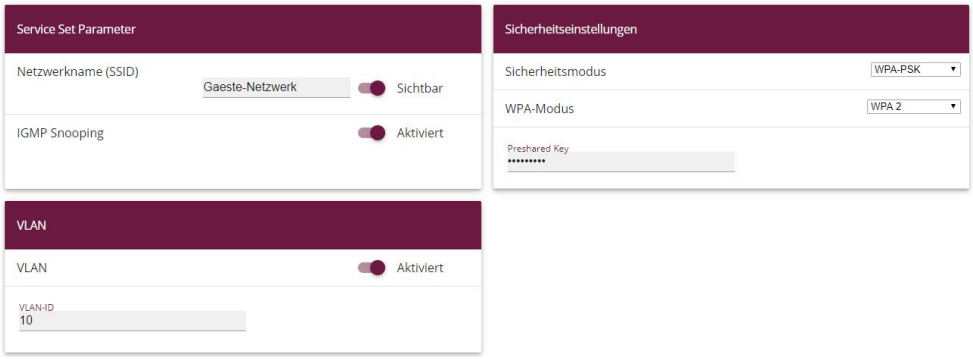


Abb. 136: **Wireless LAN Controller->Wizard->Hinzufügen**

Gehen Sie folgendermaßen vor:

(1) Geben Sie einen **Netzwerknamen (SSID)** für das Gästenetz ein, z. B. *Gaeste-Netzwerk*.

(2) Wählen Sie als **Sicherheitsmodus** *WPA-PSK*.

(3) Wählen Sie als **WPA-Modus** *WPA 2*.

(4) Geben Sie einen **Preshared Key** ein, z. B. *supersecret*

(5) Klicken Sie unter **VLAN** auf *Aktiviert*.

(6) Geben Sie eine **VLAN-ID** ein, z. B. *10*.

(7) Bestätigen Sie mit **OK**.
Sie sehen das lokale Netz zusammen mit dem Gästenetz, das Sie soeben konfiguriert haben.

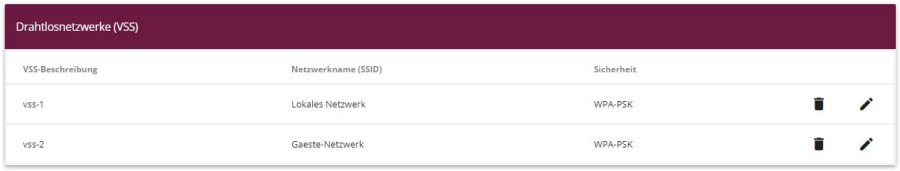


Abb. 137: **Wireless LAN Controller->Wizard**, *mit konfiguriertem Gästenetz*

Klicken Sie auf **Weiter**.

Alle gefundenen Access Points werden angezeigt.

Wählen Sie in der Spalte **Manage** diejenigen Access Points, die Sie vom Wireless LAN Controller automatisch konfigurieren und verwalten lassen wollen.

Schritt 4

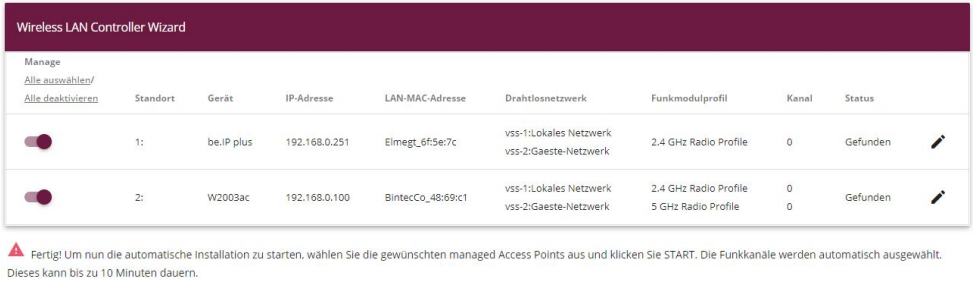


Abb. 138: **Wireless LAN Controller->Wizard**

8.2.6 Access Points mit dem Wireless LAN Controller konfigurieren

Lassen Sie die gewählten Access Points vom Wireless LAN Controller automatisch konfigurieren.

(1) Klicken Sie auf **Start**.
Der Konfigurationsprozess erfolgt schrittweise und kann - je nach Anzahl der installierten Access Points - eine Weile dauern.

(2) Prüfen Sie nach beendeter Konfiguration, ob sich alle gewählten Access Points im **Status** `Managed` befinden. Alle `Managed` Access Points haben vom WLAN Controller eine Konfiguration bekommen und werden von diesem verwaltet.

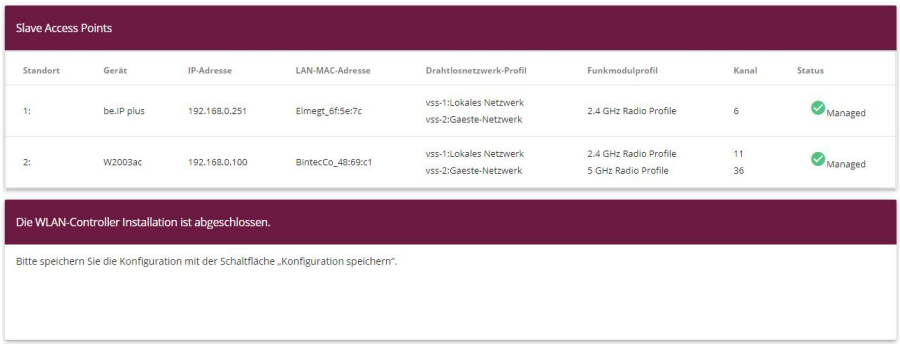


Abb. 139: **Wireless LAN Controller->Wizard**

8.2.7 IP-Adresse für die virtuelle Bridge-Schnittstelle konfigurieren

Konfigurieren Sie eine virtuelle Bridge-Schnittstelle mit VLAN-ID 10, damit die WLAN Clients auf die lokalen Dienste, z. B. DHCP, DNS und Echo, zugreifen können. Konfigurieren Sie für diese Schnittstelle eine IP-Adresse.

Gehen Sie in folgendes Menü:

Gehen Sie zu **LAN**->**IP-Konfiguration**->**Schnittstellen**->**Neu**.

Abb. 140: **LAN**->**IP-Konfiguration**->**Schnittstellen**->**Neu**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie unter **Basierend auf Ethernet-Schnittstelle** `br0`.

(2) Belassen Sie unter **Schnittstellenmodus** die Einstellung `Tagged (VLAN)`.

(3) Geben Sie unter **VLAN-ID** den Wert `10` ein.

(4) Wählen Sie unter **Sicherheitsrichtlinie** `Nicht Vertrauenswürdig`.

(5) Belassen Sie den **Adressmodus** `Statisch`.

(6) Klicken Sie auf **Hinzufügen**. Geben Sie die IP-Adresse ein, z. B. `192.168.11.1`. Belassen Sie die **Netzmaske** `255.255.255.0`.

(7) Bestätigen Sie Ihre Eingaben mit **OK**.

Das Ergebnis Ihrer Konfiguration wird in der Liste in der letzten Zeile angezeigt.

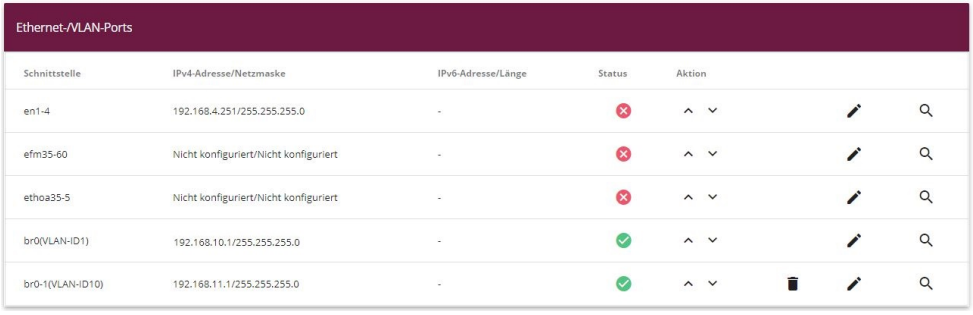


Abb. 141: **LAN**->**IP-Konfiguration**->**Schnittstellen**->**Neu**

8.2.8 IP-Adressbereich für das Gästenetz einrichten

Konfigurieren Sie einen IP-Adessbereich für die IP-Adressvergabe an WLAN-Clients im Gästenetz. Dieser IP-Adessbereich muss zur soeben konfigurierten IP-Adresse der virtuellen Bridge-Schnittstelle passen.

Gehen Sie in folgendes Menü, um einen IP-Adressbereich einzurichten:

Gehen Sie zu **Lokale Dienste**->**DHCP-Server**->**IP-Pool-Konfiguration**->**Neu**.

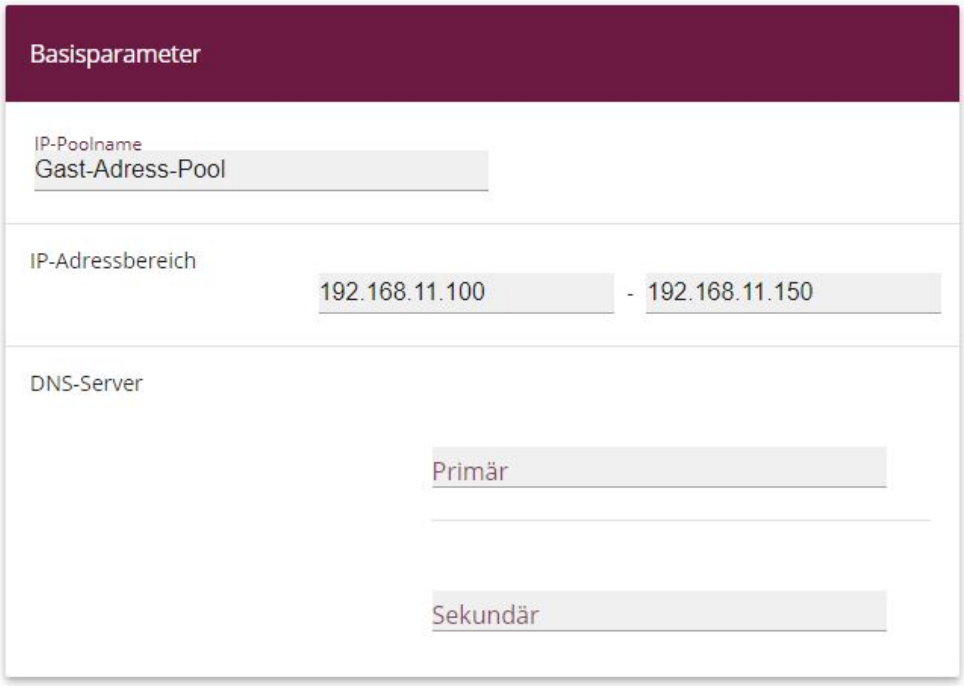


Abb. 142: **Lokale Dienste**->**DHCP-Server**->**IP-Pool-Konfiguration**->**Neu**

Gehen Sie folgendermaßen vor:

(1) Geben Sie unter **IP-Poolname** eine Beschreibung ein, z. B. `Gast-Adress-Pool`.

(2) Geben Sie unter **IP-Adressbereich** den ersten und den letzten Wert des IP-Adressbereichs ein, z. B. `192.168.11.100` - `192.168.11.150`.

(3) Bestätigen Sie Ihre Eingaben mit **OK**.

Sie sehen den neuen IP-Adressbereich in der Liste.

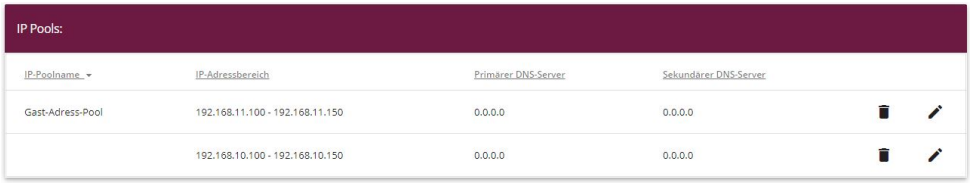


Abb. 143: **Lokale Dienste->DHCP-Server->IP-Pool-Konfiguration**

8.2.9 DHCP-Verwendung konfigurieren

Konfigurieren Sie die Verwendung von DHCP für WLAN-Clients im Gästenetz.

Gehen Sie in folgendes Menü:

Gehen Sie zu **Lokale Dienste->DHCP-Server->DHCP-Konfiguration->Neu**.

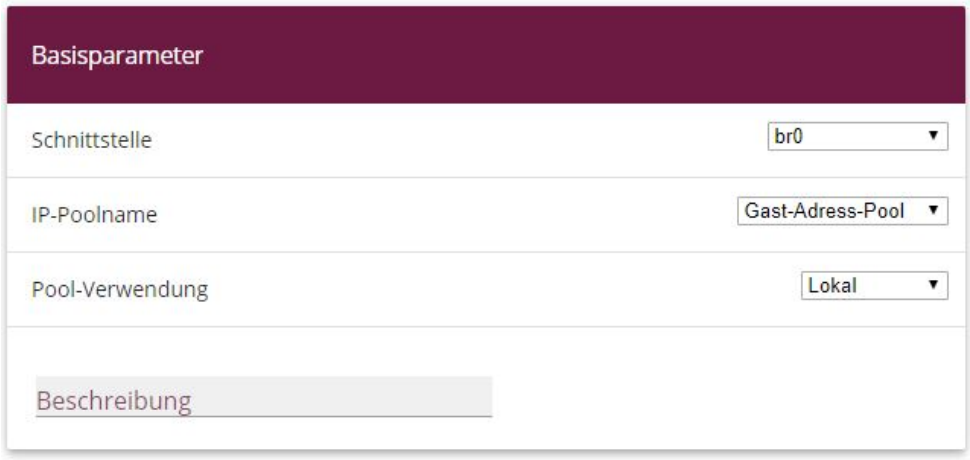


Abb. 144: **Lokale Dienste->DHCP-Server->DHCP-Konfiguration->Neu**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie eine **Schnittstelle** aus, z. B. `br0-1`.

(2) Wählen Sie unter **IP-Poolname** einen IP-Adresspool, z. B. `Gast-Adress-Pool`.

(3) Wählen Sie unter **Pool-Verwendung** aus, für welche DHCP-Anfragen der DHCP-Pool verwendet werden soll, z. B. `Lokal`.

(4) Bestätigen Sie Ihre Eingaben mit **OK**.

Sie sehen die neue DHCP-Konfiguration in der Liste.

Abb. 145: **Lokale Dienste->DHCP-Server->DHCP-Konfiguration**

8.2.10 Firewall einrichten

Die folgende Firewall-Konfiguration ist ein einfaches Beispiel, um die Grundfunktion der Firewall sicherzustellen. Sollten Sie weitere Sicherheitseinstellungen benötigen, so passen Sie das Beispiel bitte an Ihre Bedürfnisse an.

Bridge-Schnittstelle als vertrauenswürdig definieren

Definieren Sie die Schnittstelle `br0` (die Schnittstelle zu Ihrem lokalen Netzwerk) als vertrauenswürdige Schnittstelle.

Gehen Sie zu **Firewall->Richtlinien->IPv4-Filterregeln**. Klicken Sie im Bereich **Standardfilterregeln** bei Vertrauenswürdige Schnittstellen auf das -Symbol.

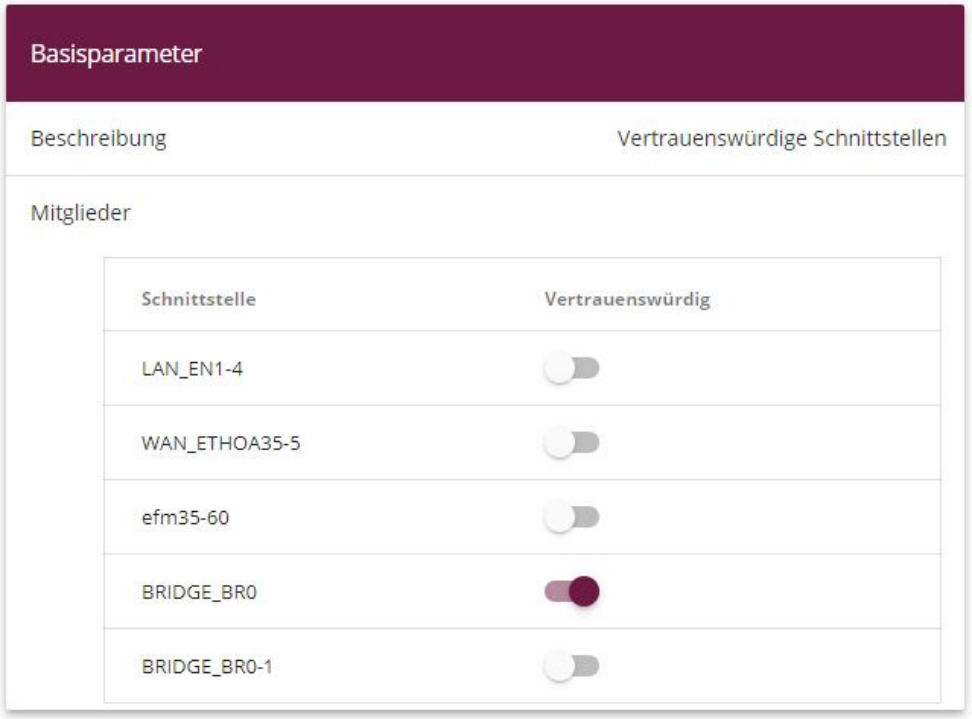


Abb. 146: **Firewall**->**Richtlinien**->**IPv4-Filterregeln**->**Standardfilterregeln**->

Gehen Sie folgendermaßen vor:

(1) Aktivieren Sie die Schnittstelle *BRIDGE_BR0* als vertrauenswürdige Schnittstelle.

(2) Stellen Sie sicher, dass keine weitere Schnittstelle markiert ist.

(3) Bestätigen Sie Ihre Eingaben mit **OK**.

Service-Gruppe anlegen

Legen Sie eine Service-Gruppe mit den Diensten an, die Clients im Gäste-WLAN verwenden wollen.

Gehen Sie zu **Firewall**->**Dienste**->**Gruppen**->**Neu**.

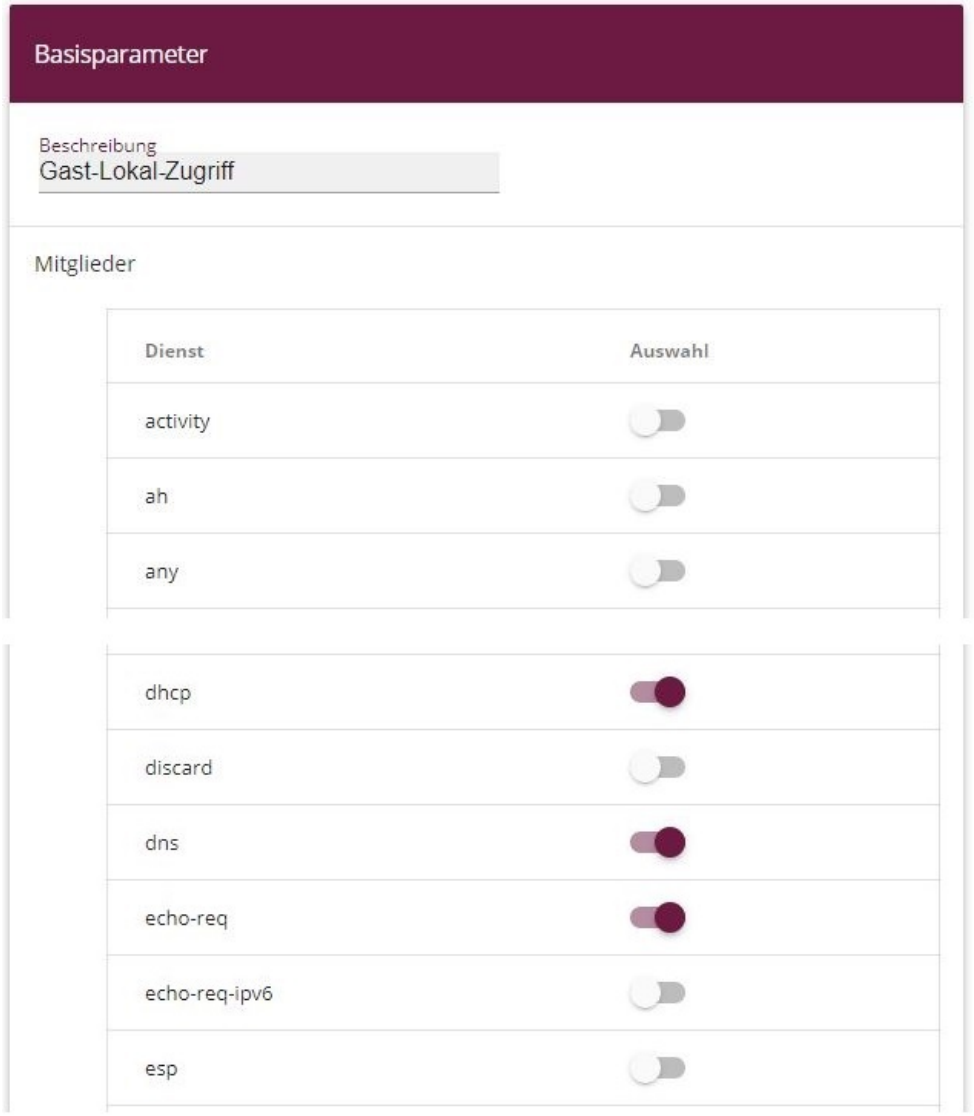


Abb. 147: **Firewall**->**Dienste**->**Gruppen**->**Neu**

Gehen Sie folgendermaßen vor:

(1) Geben Sie eine **Beschreibung** ein, z.B. `Gast-Lokal-Zugriff`.

(2) Wählen Sie die gewünschten **Mitglieder**, z. B. `dhcp`, `dns` und `echo-req`.

(3) Bestätigen Sie Ihre Eingaben mit **OK**.

Die konfigurierte Service-Gruppe wird angezeigt.

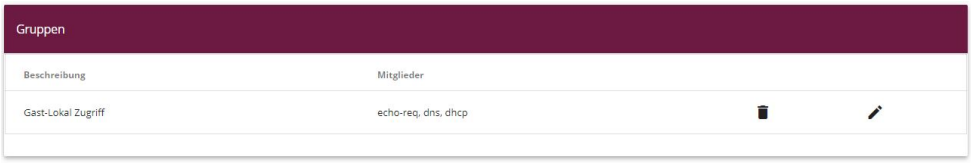


Abb. 148: **Firewall**->**Dienste**->**Gruppen**

IPv4-Filterregeln anlegen

Legen Sie eine Regel an, damit Ihre Gäste die Dienste DHCP, DNS und Echo nutzen können, die Sie in einer Service-Gruppe zusammengefasst haben.

Gehen Sie zu **Firewall**->**Richtlinien**->**IPv4-Filterregeln**->**Neu**.

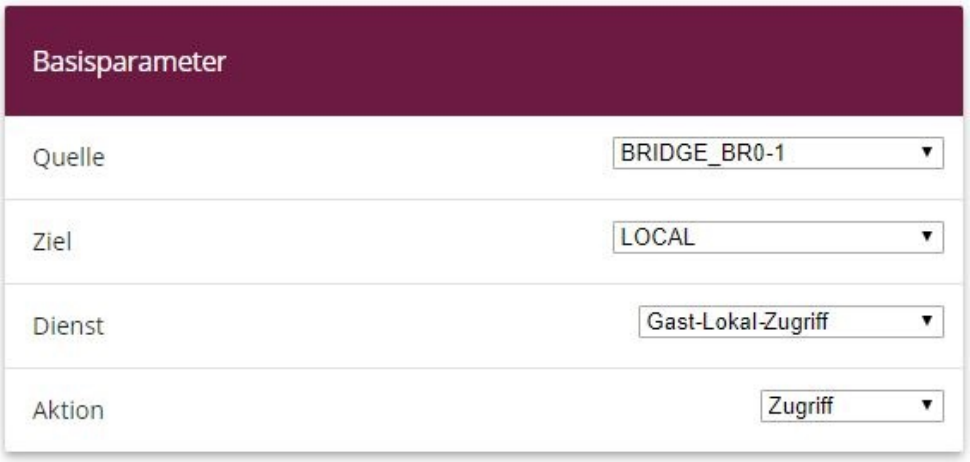


Abb. 149: **Firewall**->**Richtlinien**->**IPv4-Filterregeln**->**Neu**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie als **Quelle** *BRIDGE_BR0-1*.

(2) Wählen Sie als **Ziel** *LOCAL*.

(3) Wählen Sie als Dienst bzw. Dienstgruppe *Gast-Lokal-Zugriff*.

(4) Wählen Sie als **Aktion** *Zugriff*.

(5) Bestätigen Sie Ihre Eingaben mit **OK**.

Legen Sie eine Filterregel für den Zugang Ihrer Gäste in das Internet an.

Gehen Sie zu **Firewall**->**Richtlinien**->**IPv4-Filterregeln**->**Neu**.

Gehen Sie folgendermaßen vor:

(1) Wählen Sie als **Quelle** *BRIDGE_BR0-1*.

(2) Wählen Sie als **Ziel** *WAN_INTERNET*.

(3) Wählen Sie einen Dienst, z. B. *any*.

(4) Wählen Sie als **Aktion** *Zugriff*.

(5) Bestätigen Sie Ihre Eingaben mit **OK**.

Die beiden Filterregeln werden angezeigt.

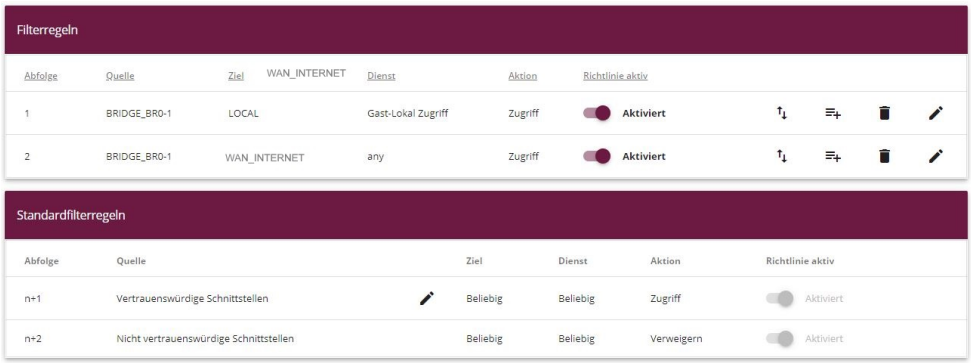


Abb. 150: **Firewall->Richtlinien->IPv4-Filterregeln**

Fügen Sie bei Bedarf weitere Regeln hinzu.

Firewall einschalten

Wenn Sie Ihre Firewall-Konfiguration beendet haben, müssen Sie die Firewall einschalten.

Gehen Sie zu **Firewall->Richtlinien->Optionen**.

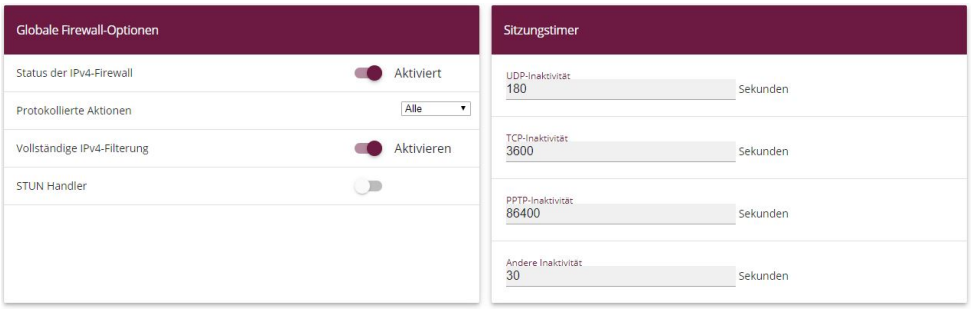


Abb. 151: **Firewall->Richtlinien->Optionen**

Gehen Sie folgendermaßen vor:

(1) Aktivieren Sie den **Status der IPv4-Firewall**.

(2) Bestätigen Sie Ihre Eingaben mit **OK**.

8.3 Ergebnis

Sie haben einen WLAN-Zugang zum lokalen Netz und ein Gäste-WLAN konfiguriert. Ihre Gäste können auf das Internet zugreifen, aber nicht auf das lokale Netz.

8.4 Konfigurationsschritte im Überblick

IP-Adresse konfigurieren

Feld	Menü	Wert
Sicherheitsrichtlinie	**LAN ->IP-Konfiguration-> Schnittstellen -><en1-0->**	*Vertrauenswürdig*
Adressmodus	**LAN ->IP-Konfiguration-> Schnittstellen-> <en1-0->**	*Statisch*
IP-Adresse / Netzmaske	**LAN ->IP-Konfiguration-> Schnittstellen -><en1-0->**	*192.168.10.1 / 255.255.255.0*

Bridge-Gruppe anlegen und LAN-Schnittstelle zuweisen

Feld	Menü	Wert
Schnittstellenbeschreibung	**Systemverwaltung ->Schnittstellenmodus / Bridge-Gruppen ->Schnittstellen**	*en1-0*
Modus / Bridge-Gruppe	**Systemverwaltung ->Schnittstellenmodus / Bridge-Gruppen-> Schnittstellen**	*Neue Bridge-Gruppe*
Konfigurationsschnittstelle	**Systemverwaltung ->Schnittstellenmodus / Bridge-Gruppen ->Schnittstellen**	*en1-0*

Wireless LAN Controller in Betrieb nehmen

Feld	Menü	Wert
Region	**Wireless LAN Controller-> Wizard**	*Germany*
Schnittstelle	**Wireless LAN Controller-> Wizard**	*BRIDGE_BR0*
DHCP-Server	**Wireless LAN Controller ->Wizard**	*Intern*
IP-Adressbereich	**Wireless LAN Controller-> Wizard**	z. B. *192.168.10.100 - 192.168.10.150*

Funkmodulprofil auswählen und WLAN-Zugang zum lokalen Netz konfigurieren

Feld	Menü	Wert
Zwei Unabhängige Funkmodulprofile verwenden	**Wireless LAN Controller-> Wizard ->Weiter**	*Aktiviert*
Funkmodulprofil für Modul 1 (für alle Access Points)	**Wireless LAN Controller ->Wizard ->Weiter**	*2.4 GHz Radio Profile*
Funkmodulprofil für Modul 2 (nur für APs mit 2 Funkmodulen)	**Wireless LAN Controller-> Wizard ->Weiter**	*5 GHz Radio Profile*
Netzwerkname (SSID)	**Wireless LAN Controller-> Wizard ->Weiter -><vss-1>->**	*Lokales Netzwerk*
Preshared Key	**Wireless LAN Controller-> Wizard ->Weiter -><vss-1>->**	z. B. *supersecret*

Gäste-WLAN konfigurieren

Feld	Menü	Wert
Netzwerkname (SSID)	**Wireless LAN Controller-> Wizard ->Weiter ->Hinzufügen**	z. B. *Gaeste-Netzwerk*
Sicherheitsmodus	**Wireless LAN Controller-> Wizard ->Weiter ->Hinzufügen**	*WPA-PSK*
WPA-Modus	**Wireless LAN Controller-> Wizard ->Weiter ->Hinzufügen**	*WPA2*
Preshared Key	**Wireless LAN Controller-> Wizard ->Weiter ->Hinzufügen**	z. B. *Super-Secret-1*
VLAN	**Wireless LAN Controller-> Wizard ->Weiter ->Hinzufügen**	*Aktiviert*
VLAN-ID	**Wireless LAN Controller-> Wizard ->Weiter ->Hinzufügen**	z. B. *10*
Manage	**Wireless LAN Controller ->Wizard ->Weiter**	*Aktiviert*

Access Points mit dem Wireless LAN Controller konfigurieren

Feld	Menü	Wert
Wireless LAN Controller Wizard	**Wireless LAN Controller-> Wizard ->Weiter ->Weiter ->Weiter**	**START**

IP-Adresse für die virtuelle Bridge-Schnittstelle konfigurieren

Feld	Menü	Wert
Basierend auf Ethernet- Schnittstelle	**LAN ->IP-Konfiguration-> Schnittstellen-> Neu**	*br0*
Schnittstellenmodus	**LAN ->IP-Konfiguration-> Schnittstellen-> Neu**	*Tagged (VLAN)*
VLAN-ID	**LAN-> IP-Konfiguration-> Schnittstellen ->Neu**	*10*
Sicherheitsrichtlinie	**LAN ->IP-Konfiguration-> Schnittstellen ->Neu**	*Nicht Vertrauenswürdig*
Adressmodus	**LAN ->IP-Konfiguration-> Schnittstellen ->Neu**	*Statisch*
IP-Adresse / Netzmaske	**LAN-> IP-Konfiguration-> Schnittstellen ->Neu**	*192.168.11.1 / 255.255.255.0*

IP-Adressbereich für das Gästenetz einrichten

Feld	Menü	Wert
IP-Poolname	**Lokale Dienste ->DHCP-Server ->IP-Pool-Konfiguration ->Neu**	*Gast-Adress-Pool*
IP-Adressbereich	**Lokale Dienste ->DHCP-Server-> IP-Pool-Konfiguration-> Neu**	z. B. *192.168.11.100 - 192.168.11.150*

DHCP-Verwendung konfigurieren

Feld	Menü	Wert
Schnittstelle	**Lokale Dienste ->DHCP-Server ->DHCP-Konfiguration-> Neu**	*br0-1*
IP-Poolname	**Lokale Dienste ->DHCP-Server-> DHCP-Konfiguration ->Neu**	*Gast-Adress-Pool*
Pool-Verwendung	**Lokale Dienste-> DHCP-Server ->DHCP-Konfiguration ->Neu**	*Lokal*

Firewall einrichten

Feld	Menü	Wert
BRIDGE_BR0	**Firewall ->Richtlinien-> IPv4-Filterregeln ->Standardfilterregeln->** 	**Vertrauenswürdig** *Aktiviert*
Beschreibung	**Firewall ->Dienste ->Gruppen ->Neu**	z. B. *Gast-Lokal-Zugriff*
Mitglieder	**Firewall ->Dienste ->Gruppen ->Neu**	z. B. *dhcp*, *dns* und *echo-req*

Feld	Menü	Wert
Quelle	**Firewall ->Richtlinien ->IPv4-Filterregeln-> Neu**	*BRIDGE_BR0-1*
Ziel	**Firewall ->Richtlinien ->IPv4-Filterregeln ->Neu**	*LOCAL*
Dienst	**Firewall ->Richtlinien ->IPv4-Filterregeln ->Neu**	*Gast-Lokal-Zugriff*
Aktion	**Firewall ->Richtlinien ->IPv4-Filterregeln ->Neu**	*Zugriff*
Quelle	**Firewall ->Richtlinien ->IPv4-Filterregeln ->Neu**	*BRIDGE_BR0-1*
Ziel	**Firewall ->Richtlinien ->IPv4-Filterregeln ->Neu**	*WAN_INTERNET*
Dienst	**Firewall ->Richtlinien ->IPv4-Filterregeln ->Neu**	z. B. *any*
Aktion	**Firewall ->Richtlinien ->IPv4-Filterregeln ->Neu**	*Zugriff*
Status der IPv4-Firewall	**Firewall ->Richtlinien ->Optionen**	*Aktiviert*

Kapitel 9 VLAN-Einrichtung ESW4000-Switche

Die Ports der **ESW4000**-Switch-Serie sind im Auslieferzustand der Switche für alle nicht getaggten Pakete transparent, getaggte Pakete werden jedoch blockiert. Wenn wir also mit VLAN arbeiten möchten, um z. B. ein für den übrigen Netz getrenntes WLAN-Gastnetz einzurichten, müssen wir neben der Konfiguration der WLAN Access Points und des Routers auch die Konfiguration am Switch anpassen.

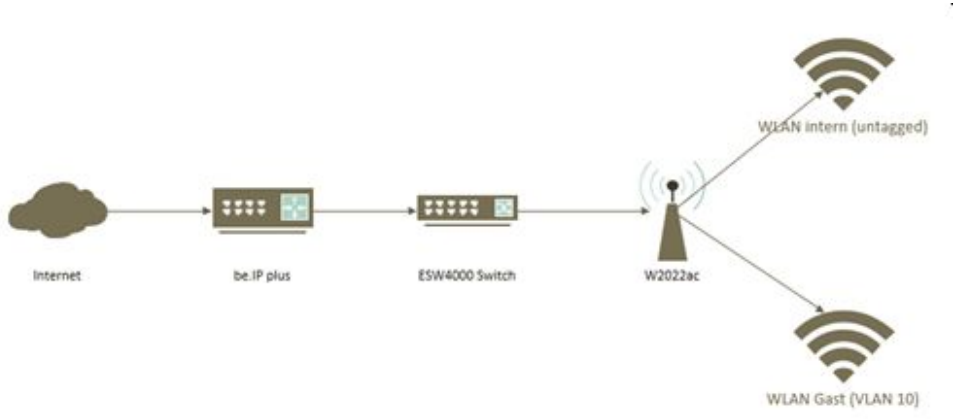


Abb. 152: Aufbaubauspiel

Voraussetzungen

- Ein Router **bintec be.IP** oder **bintec be.IP plus** mit der Firmware Version 10.2.6.102
- Eine **ESW4000** mit der Firmware Version 1.2.24.182
- Ein **bintec W2022ac** mit der Firmware Version 1.12.1.6

9.1 Einrichtung eines Gast-Netzwerks am Router

Einrichtung eines Gäste-WLANs über den WLAN Controller an einem Router finden Sie im Kapitel *WLAN - Netzwerk mit Gäste-WLAN* auf Seite 219 oder auf unserer Homepage unter: *https://www.bintec-elmeg.com/mc/workshops/anwendungs-workshops/*

9.2 Einrichtung am Switch ESW4000

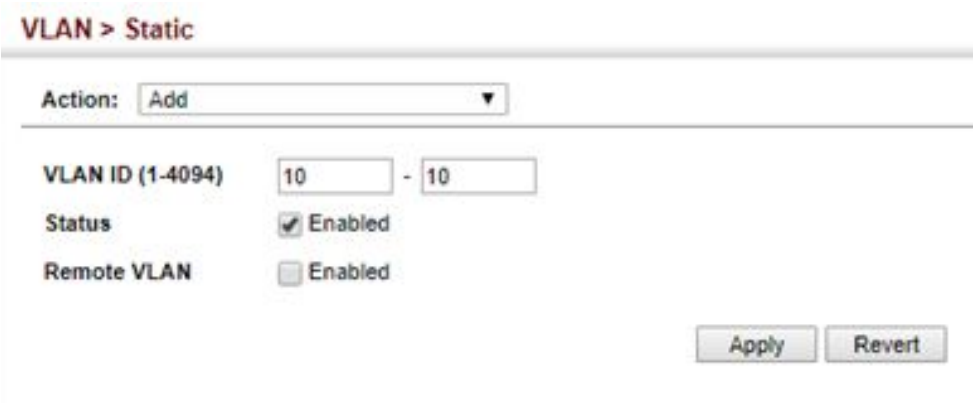
Öffnen Sie einen Webbrowser und geben Sie die Standard-IP-Adresse `192.168.2.10` in das Adressfeld ein.

Melden Sie sich mit den Anmeldedaten

User: `admin`, **Password**: `admin` an. Klicken Sie auf **Login**.

In unserem Beispiel wird das Gäste-WLAN mit VLAN 10 getaggt. Die angelegten Drahtlosnetzwerke finden Sie auf Ihrer **be.IP** im Menü **Wireless LAN Controller**->**Slave-AP-Configuration**->**Drahtlosnetzwerke (VSS)**. Außerdem sind im Menü **LAN**->**IP-Konfiguration** die vorhandenen Ethernet-/VLAN-Ports aufgelistet, z. B. br0(VLAN-ID1), br0-1(VLAN-ID3).

Zur Konfiguration des VLANs gehen Sie in das Menü **VLAN**->**Static**.

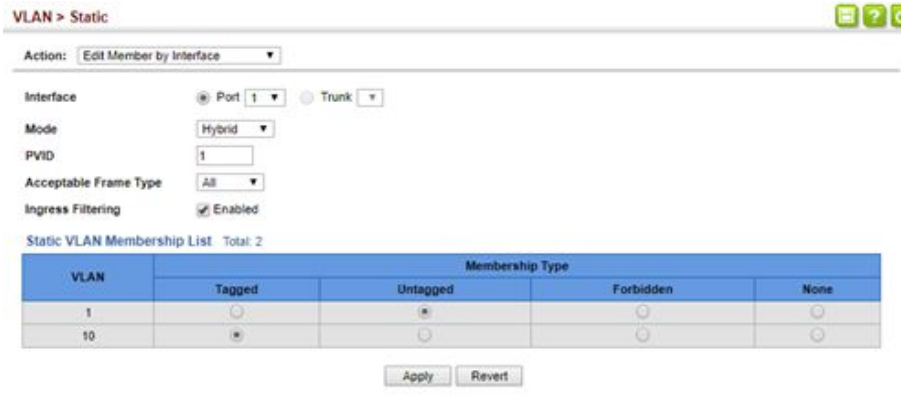


(1) Geben Sie bei **VLAN ID** 10 - 10 ein.

(2) Klicken Sie auf **Apply**.

Im nächsten Schritt richten Sie den Port ein, an dem der Access Point angeschlossen ist.

(1) Wählen Sie im Menü **VLAN**->**Static** bei **Action** die Option *Edit Member by Interface* aus.

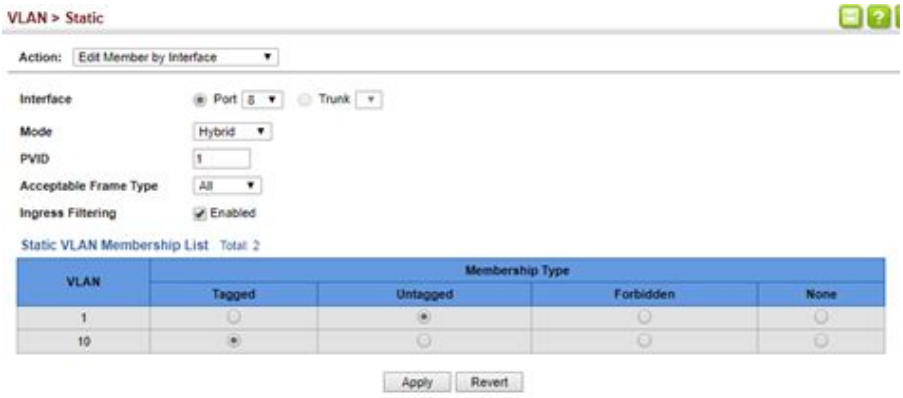


(2) Wählen Sie den **Port** aus, in unserem Beispiel ist das der Port 1.

(3) Bestätigen Sie mit **Apply**.

Für die Einrichtung des Ports an dem die **be.IP plus** angeschlossen ist, gehen Sie erneut in das Menü **VLAN**->**Static**.

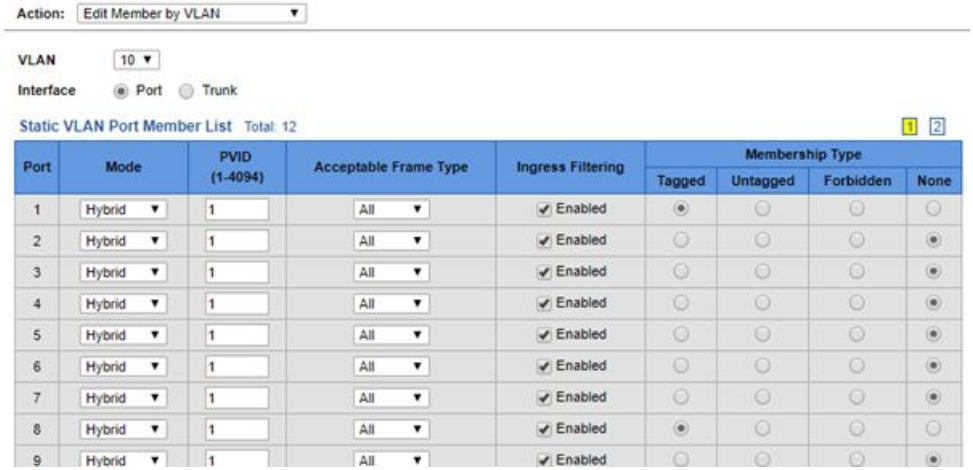
(1) Wählen Sie unter **Action** die Option *Edit Member by Interface*aus.



(2) Wählen Sie den **Port** aus, in unserem Beispiel ist das der Port 8.

(3) Bestätigen Sie mit **Apply**.

Alternativ können Sie im Menü **VLAN**->**Static** unter **Action** die Option *Edit Member by VLAN* auswählen.



In der Übersicht **Statische VLAN-Port-Mitgliederliste** sind alle vorhandenen VLAN-Mitglieder aufgelistet.

Hier können Sie die **Eingangsfilterung** aktivieren/deaktivieren, sowie die **Art der Mitgliedschaft** festlegen.

Kapitel 10 WLAN - WLAN-Controller-Installation mit integrierter HotSpot-Funktionalität

10.1 Einleitung

Es soll ein WLAN-Netz mit Wireless LAN Controller und der **bintec HotSpot Solution** aufgebaut werden. Das WLAN-Netz soll zwei SSIDs bereitstellen. Eine SSID für Mitarbeiter soll Zugriff auf das interne Netz und auf das Internet erhalten. Die zweite SSID ist für Gäste; diese sollen nach Anmeldung über die bintec HotSpot-Lösung ausschließlich Zugang zum Internet haben.

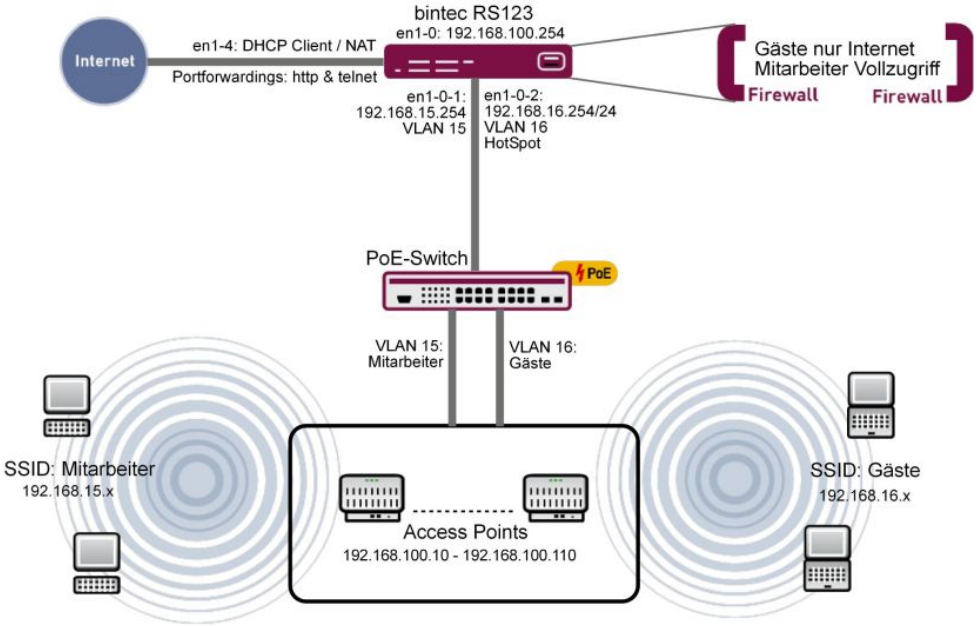


Abb. 158: Beispielszenario

Voraussetzungen

- Ein Router der RS-Serie (z. B. **bintec RS123**) oder ein Gerät der RXL-Serie (z. B. **bintec RXL12500**)
- Ein **bintec W2003ac**

- Software-Lizenzierung für die bintec Router
- WLAN Controller Lizenz
- 6 Access Points
- bintec Hotspot Hosting 2yr1 Location

10.2 Funktion

Der bintec Router (z. B. **bintec RS123**) dient gleichzeitig als Gateway, Firewall, WLAN Controller und als HotSpot-Gateway. Die Access Points stellen zwei SSIDs bereit, diese sind jeweils mit einem eigenen VLAN getagged. Der Router separiert anhand des Taggings die beiden Datenströme und stellt diese intern an zwei virtuellen Ports zur Verfügung.

Der Router stellt drei DHCP-Pools zur Verfügung: einen für die Access Points (192.168.100.10 bis 192.168.100.110); dieser wird automatisch durch den Wireless LAN Controller Wizard angelegt. Der Wireless LAN Controller Wizard berücksichtigt dabei automatisch die Konfiguration der DHCP-Option 138. Das ist die WLAN Controller-Adresse, die die Access Points zur Kommunikation mit dem WLAN Controller benötigen. Die anderen beiden DHCP-Pools werden manuell angelegt. Sie werden jeweils für die SSID *Mitarbeiter* und die SSID *Gäste* verwendet.

Hinweis

In kleinen WLAN-Installationen bis zu 6 Access Points kann man einen **bintec W2003ac** auch als WLAN Controller verwenden. Dies ist hier nicht möglich, da das Gerät gleichzeitig auch die HotSpot-Gateway-Funktionalität übernehmen muss. Dazu sind jedoch Routerfunktionen notwendig, die im **bintec W2003ac** deaktiviert sind, wenn dieser als WLAN Controller arbeitet.

10.3 Konfiguration

10.3.1 Basiskonfiguration

Bevor Sie mit der Konfiguration nach nachstehender Beschreibung beginnen, müssen Sie mit Hilfe der Assistenten einen Internetzugang einrichten. Falls Sie eine WLAN Controller Lizenz erworben haben, müssen Sie diese im Menu **Systemverwaltung** -> **Globale Einstellungen** -> **Systemlizenzen** eintragen. Darüber hinaus ist es notwendig, einen NTP-Zeitserver festzulegen und die Zeitzone einzustellen. Dies ist wichtig für eine zuverlässige Funktion des Hotspots. Richten Sie bitte zunächst keinen DHCP-Pool für den Router ein, da später bei der WLAN Controller-Einrichtung der DHCP-Pool für die WLAN Access Points automatisch eingerichtet wird.

10.3.2 LAN-Konfiguration

Ändern Sie zuerst in Menü **IP-Konfiguration** die IP-Adresse.

(1) Gehen Sie zu **LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>** .

Abb. 159: **LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **<en1-0>**

Gehen Sie folgendermaßen vor:

(1) Den **Schnittstellenmodus** stellen Sie auf *Untagged*.

(2) Geben Sie die **IP-Adresse / Netzmaske** *192.168.100.254* ein.

(3) Bestätigen Sie mit **OK**.

Fügen Sie nun die virtuelle Schnittstelle hinzu.

(1) Gehen Sie zu **LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **Neu**.

Abb. 160: **LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Bei **Basierend auf Ethernet-Schnittstelle** wählen Sie *en1-0* aus.

(2) Wählen Sie bei **Schnittstellenmodus** *Tagged (VLAN)* aus.

(3) Weisen Sie der Schnittstelle eine **VLAN-ID** zu, z. B. *15*.

(4) Fügen Sie mit **Hinzufügen** die **IP-Adresse / Netzmaske** *192.168.15.254* ein.

(5) Bestätigen Sie mit **OK**.
Sie haben eine virtuelle Schnittstelle *en1-0-1* mit der **VLAN-ID** *15* hinzugefügt.

(1) Gehen Sie zu **LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **Neu** um eine weitere Schnittstelle anzulegen.

(2) Bei **Basierend auf Ethernet-Schnittstelle** wählen Sie *en1-0* aus.

(3) Wählen Sie bei **Schnittstellenmodus** *Tagged (VLAN)* aus.

(4) Weisen Sie der Schnittstelle eine **VLAN-ID** zu, z. B. *16*.

(5) Fügen Sie mit **Hinzufügen** die **IP-Adresse / Netzmaske** *192.168.16.254* ein.

(6) Bestätigen Sie mit **OK**.
Sie haben eine virtuelle Schnittstelle *en1-0-2* mit der **VLAN-ID** *16* hinzugefügt.

Nach dieser Konfiguration sieht das Menü **Schnittstellen** folgendermaßen aus.

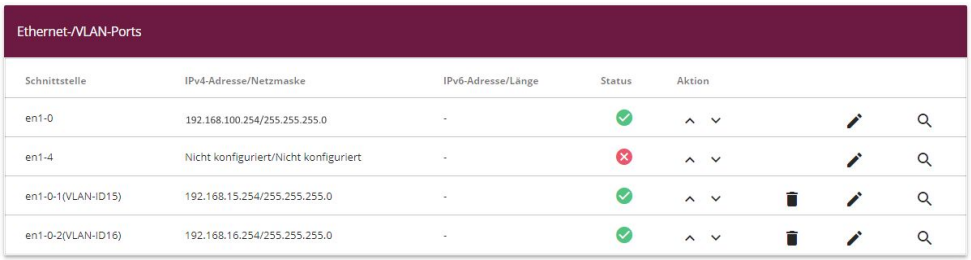


Abb. 161: **LAN** -> **IP-Konfiguration** -> **Schnittstellen**

10.3.3 HotSpot-Konfiguration

Um die Konfiguration vorzubereiten, sollten Sie Ihre Lizenz über das Lizenzportal der bintec elmeg-Webseite *http://www.bintec-elmeg.com* freischalten. Sie erhalten dann kurzfristig Ihre individuellen Zugangsdaten.

Zunächst ist es notwendig einen RADIUS-Server einzutragen.

RADIUS (Remote Authentication Dial In User Service) ist ein Dienst, der es ermöglicht, Authentifizierungs- und Konfigurationsinformationen zwischen Ihrem Gerät und einem RADIUS-Server auszutauschen.

(1) Gehen Sie zu **Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**.

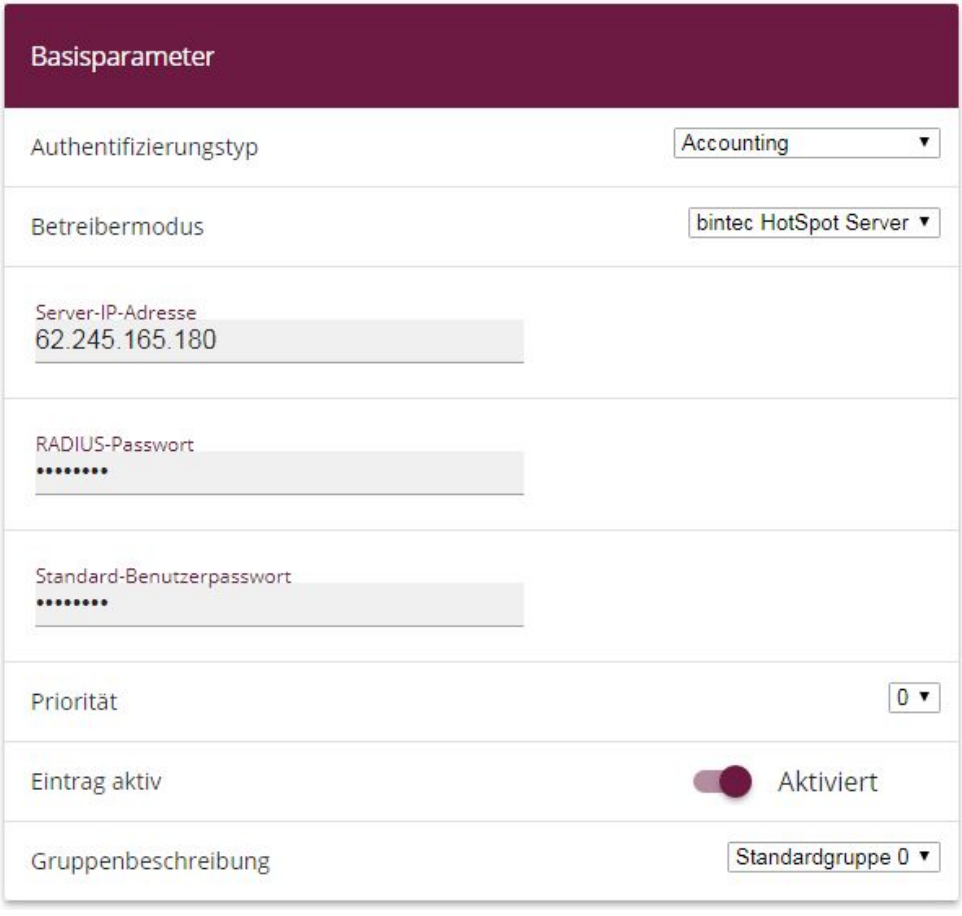


Abb. 162: **Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**

Gehen Sie folgendermaßen vor, um einen RADIUS-Server einzurichten:

(1) Wählen Sie den **Authentifizierungstyp** `Accounting` aus. Der RADIUS-Server wird zur Erfassung statistischer Verbindungsdaten verwendet.

(2) Als **Betreibermodus** wählen Sie `bintec HotSpot Server` aus.

(3) Bei **Server-IP-Adresse** geben Sie die Adresse des zentralen bintec HotSpot Servers ein, hier z. B. `62.245.165.180`.

(4) Das **RADIUS-Passwort** entnehmen Sie Ihren Zugangsdaten.

(5) Das **Standard-Benutzerpasswort** ist identisch mit dem **RADIUS-Passwort**.

(6) Die **Priorität** setzen Sie auf `0` (höchste Priorität).

(7) Bestätigen Sie mit **OK**.

(1) Gehen Sie zu **Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**, um den zweiten RADIUS-Server einzurichten.

(2) Wählen Sie den **Authentifizierungstyp** *Login-Authentifizierung* aus.

(3) Bei **Server-IP-Adresse** geben Sie die Adresse des zentralen bintec HotSpot Servers ein, hier z. B. *62.245.165.180*.

(4) Das **RADIUS-Passwort** entnehmen Sie Ihren Zugangsdaten.

(5) Das **Standard-Benutzerpasswort** ist identisch mit dem **RADIUS-Passwort**.

(6) Die **Priorität** setzen Sie auf *0* (höchste Priorität).

(7) Wählen Sie im Menü **Erweiterte Einstellungen** unter **Richtlinie** *Nicht verbindlich*.

(8) Bestätigen Sie mit **OK**.

Die fertige Konfiguration sieht wie folgt aus:

Abb. 163: **Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS**

Im nächsten Schritt wird ein Hotspot-Netzwerk eingerichten.

(1) Gehen Sie zu **Lokale Dienste** -> **Hotspot-Gateway** -> **Hotspot-Gateway** -> **Neu**.

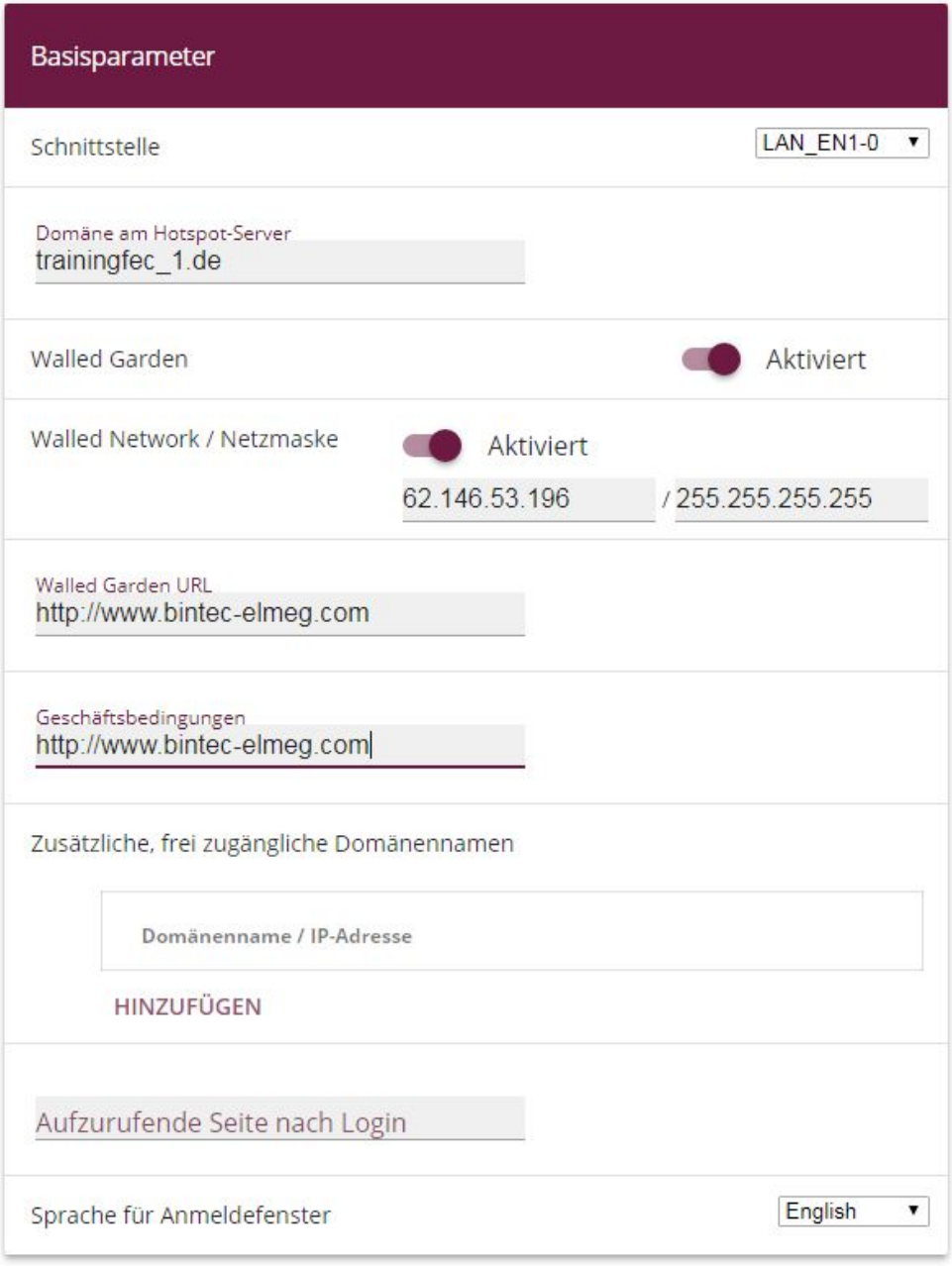


Abb. 164: **Lokale Dienste** -> **Hotspot-Gateway** -> **Hotspot-Gateway** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie die **Schnittstelle** *LAN_EN1-0* aus. Diese korrespondiert später mit der **SSID** *Gäste*.

(2) Unter **Domäne am Hotspot-Server** geben Sie die Domäne an, die Sie mit den Zugangsdaten erhalten haben, z. B. *trainingfec_1.de*.

(3) Aktivieren Sie die Option **Walled Garden**.

(4) Bei **Walled Network / Netzmaske** geben Sie die IP-Adresse an, die Ihre HotSpot-Gäste ohne Anmeldung erreichen dürfen, z. B. *62.146.53.196* und *255.255.255.255*.

(5) Unter **Walled Garden URL** geben Sie die URL an, die Ihren HotSpot Gäste ohne Anmeldung angezeigt werden soll, z. B. *http://www.bintec-elmeg.com*. Die Walled Garden URL muss unter der Walled Network Adresse erreichbar sein.

(6) Unter **Geschäftsbedingungen** geben Sie die URL an, unter der Sie Ihre AGB Webseite abgelegt haben, z. B. *http://www.bintec-elmeg.com*. Die URL muss unter der Walled Network Adresse erreichbar sein.

(7) Bestätigen Sie mit **OK**.

10.3.4 DHCP-Konfiguration

Nun werden die beiden DHCP-Pools für die virtuellen Schnittstellen en1-0-1 (VLAN-ID 15) und en1-0-2 (VLAN-ID 16) angelegt.

(1) Gehen Sie zu **Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu** um den IP-Pool zu konfigurieren.

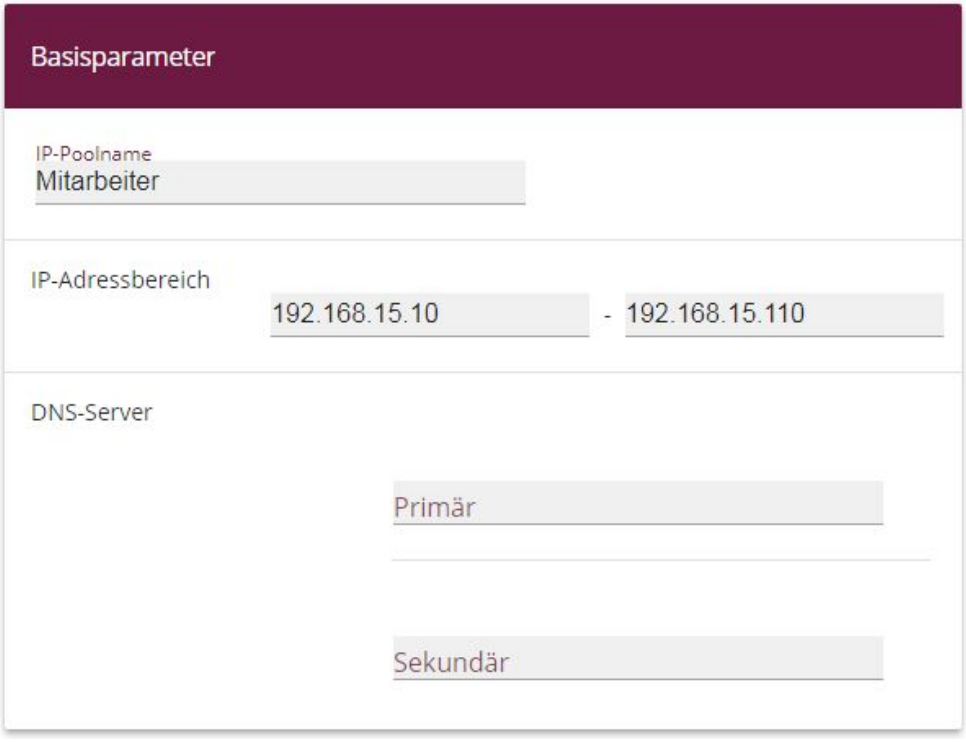


Abb. 165: **Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Geben Sie bei **IP-Poolname** eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen, z. B. `Mitarbeiter`.

(2) Bei **IP-Adressbereich** geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein, z. B. `192.168.15.10` - `192.168.15.110`.

(3) Bestätigen Sie mit **OK**.

Im Menü **Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu** können Sie nun weitere Konfiguration vornehmen.

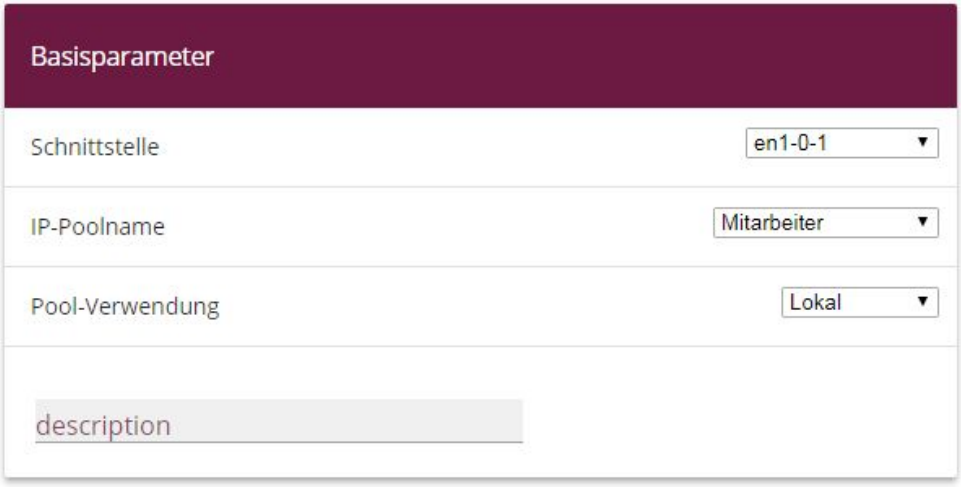


Abb. 166: **Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Wählen Sie die **Schnittstelle** *en1-0-1* aus.

(2) Wählen Sie einen gültigen **IP-Pool** aus, hier z. B. *Mitarbeiter*.

(3) Wählen Sie bei **Pool-Verwendung** *Lokal* aus. Der DHCP-Pool wird nur für DHCP-Anfragen im selben Subnetz verwendet.

(4) Bestätigen Sie mit **OK**.

Nun legen Sie für die zweite virtuelle Schnittstelle en1-0-2 (VLAN-ID 16) einen weiteren DHCP-Pool an.

(1) Gehen Sie zu **Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu**.

(2) Geben Sie bei **IP-Poolname** z. B. *Gäste* ein.

(3) Bei **IP-Adressbereich** geben Sie die IP-Adresse des IP-Adress-Pools ein, z. B. *192.168.16.10* - *192.168.16.110*.

(4) Bestätigen Sie mit **OK**.

(5) Gehen Sie zu **Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**.

(6) Wählen Sie die **Schnittstelle** *en1-0-2* aus.

(7) Wählen Sie einen definierten **IP-Poolnamen** aus, hier z. B. *Gäste*.

(8) Wählen Sie bei **Pool-Verwendung** *Lokal* aus.

(9) Bestätigen Sie mit **OK**.

Die fertige Konfiguration sieht wie folgt aus:

Abb. 167: **Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration**

10.3.5 Wireless LAN Controller Wizard

Mit dem **Wireless LAN Controller** können Sie eine WLAN-Infrastruktur mit mehreren Access Points (APs) aufbauen und verwalten. Der WLAN Controller verfügt über einen Wizard, der Sie bei der Konfiguration Ihrer Access Points unterstützt.

(1) Gehen Sie zu **Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard**.

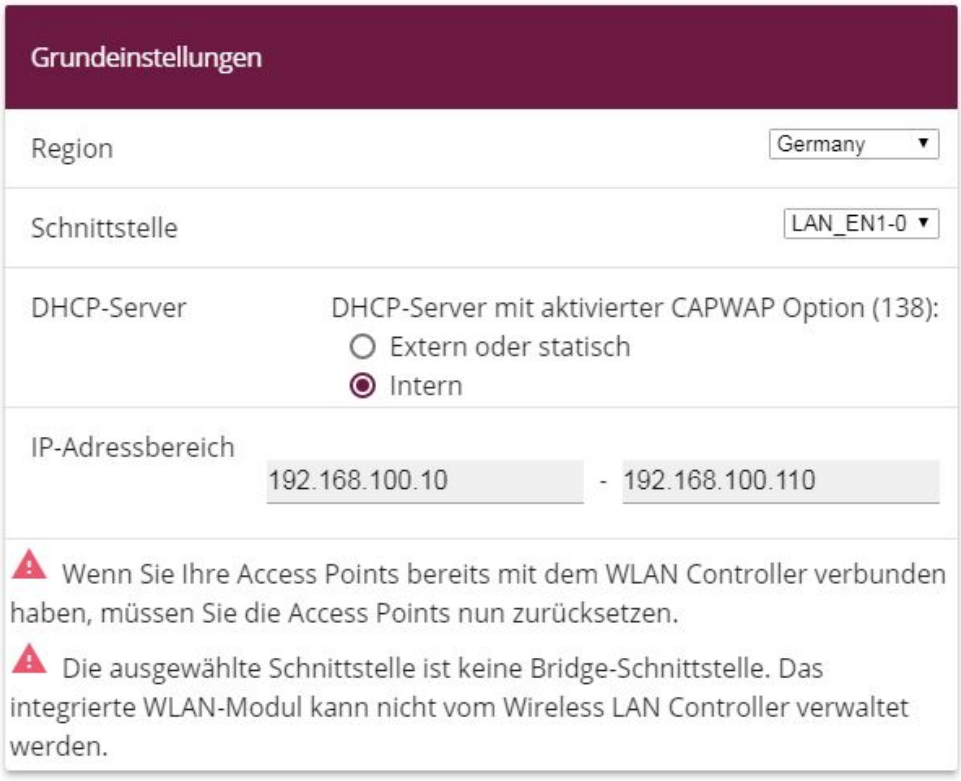


Abb. 168: **Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard**

Gehen Sie folgendermaßen vor:

(1) Bei **Region** wählen Sie *Germany* aus.

(2) Wählen Sie die **Schnittstelle** *LAN_EN1-0* aus.

(3) Bei **DHCP-Server** wählen Sie *Intern* aus.

(4) Geben Sie den **IP-Adressbereich** ein, hier *192.168.100.10* - *192.168.100.110*. Nun wird automatisch ein weiterer DHCP-Pool für die Schnittstelle EN1-0 angelegt. Dabei wird berücksichtigt, dass die IP-Adresse des WLAN Controllers bei jeder DHCP-Anfrage als CAPWAP Option 138 gesendet wird. Hierüber erhalten die Access Points die Adresse des WLAN Controllers mitgeteilt.

(5) Klicken Sie auf **Weiter**.

Im zweiten Schritt fragt der Wizard ab, ob das WLAN-Netz im 2,4 GHz oder im 5 GHz Frequenzbereich betrieben werden soll. Falls Ihr WLAN Netz im 2,4 GHz und im 5 GHz Frequenzbereich arbeiten soll, wählen Sie zunächst 2,4 GHz aus. Sie können später die Konfiguration einzelner Radiomodule auf 5 GHz umstellen.

Abb. 169: **Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard**

Klicken Sie auf **Weiter**.

Im nächsten Schritt definieren Sie die SSID, die später ausgeliefert werden soll.

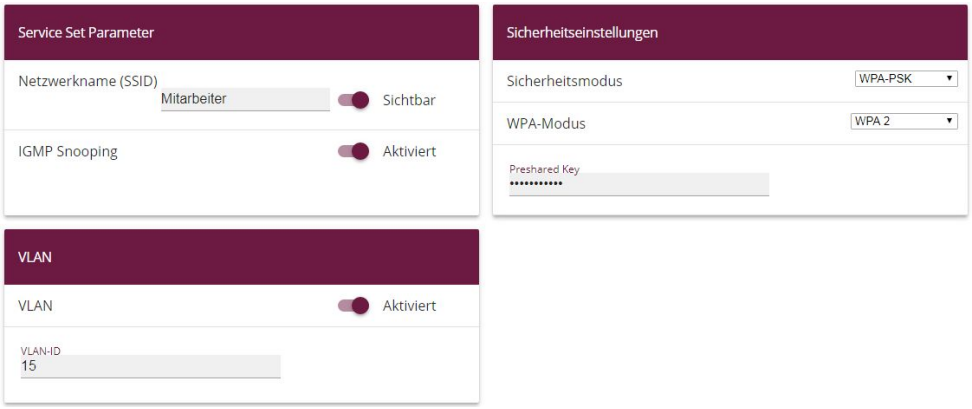


Abb. 170: **Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard**

Gehen Sie folgendermaßen vor:

(1) Klicken Sie auf **Hinzufügen**.

(2) Bei **Netzwerkname (SSID)** geben Sie `Mitarbeiter` ein.

(3) Den **Sicherheitsmodus** stellen Sie auf `WPA-PSK`.

(4) Den **WPA-Modus** stellen Sie auf `WPA2`.

(5) Geben Sie bei **Preshared Key** Ihr definiertes Passwort ein.

(6) Bei **VLAN-ID** geben SIe `15` ein.

(7) Bestätigen Sie mit **OK**.

Mit diesen Einstellungen wird jeglicher Traffic von WLAN Clients, die über diese SSID verbunden sind, zur virtuellen Schnittstelle en1-0-1 geleitet.

Nun definieren Sie die zweite SSID, die später ausgeliefert werden soll.

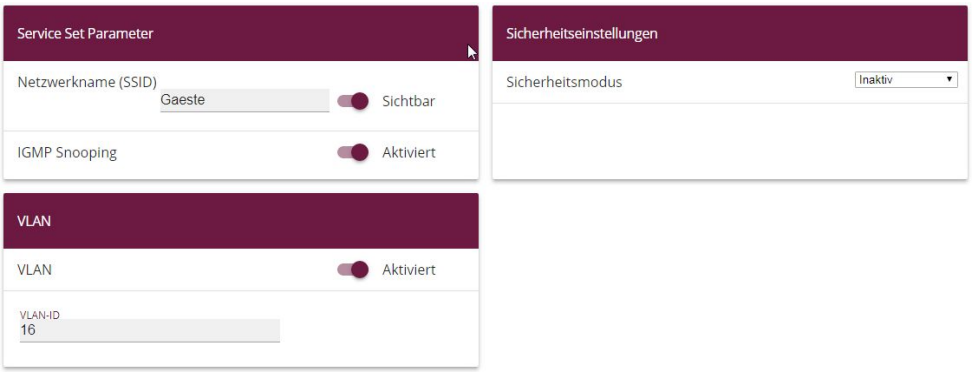


Abb. 171: **Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard**

Gehen Sie folgendermaßen vor:

(1) Klicken Sie auf **Hinzufügen**.

(2) Bei **Netzwerkname (SSID)** geben Sie *Gäste* ein.

(3) Den **Sicherheitsmodus** stellen Sie auf *Inaktiv*.

(4) Bei **VLAN-ID** geben SIe *16* ein.

(5) Bestätigen Sie mit **OK**.

Mit diesen Einstellungen wird jeglicher Traffic von WLAN Clients, die über diese SSID verbunden sind, zur virtuellen Schnittstelle en1-0-2 geleitet.

Hinweis

Bevor Sie fortfahren, stellen Sie sicher, dass alle Access Points, die der WLAN Controller verwalten soll, eingeschaltet und über einen Switch an die Schnittstelle en1-0 des Routers angeschlossen sind.

Klicken Sie auf **Weiter**.

Sie sehen jetzt eine Liste der gefundenen Access Points.

Abb. 172: **Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard**

Um die Einstellungen eines gefundenen APs zu ändern, klicken Sie im entsprechenden Eintrag auf .

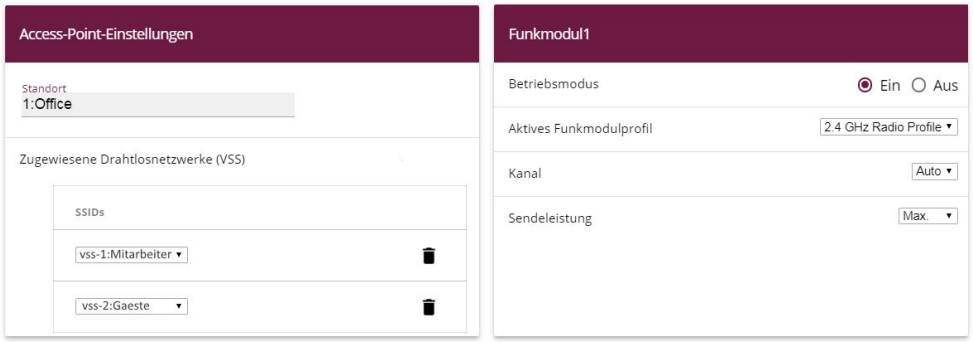


Abb. 173: **Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard**

Gehen Sie folgendermaßen vor:

(1) Tragen Sie bei **Standort** den Installationsort des Gerätes ein, z. B. `1:Office`. Dies erleichtert Ihnen später die Überwachung der Geräte.

(2) Bei **Zugewiesene Drahtlosnetzwerke (VSS)** werden Ihnen die aktuell zugewiesenen Drahtlosnetzwerke angezeigt, hier z. B. `vss-1:Mitarbeiter` und `vss-2:Gäste`.

(3) **Aktives Funkmodulprofil** zeigt das aktuell gewählte Funkmodulprofil, hier `2,4 GHz Radio Profile`. Sie können ein anderes Funkmodulprofil aus der Liste wählen, wenn mehrere Funkmodulprofile angelegt sind.

(4) Bestätigen Sie mit **OK**.

Wählen Sie nun die Access Points, welche der WLAN Controller verwalten soll. Klicken Sie dazu in der Spalte **Manage** auf die gewünschten Einträge.

Klicken Sie auf **Start**, um die Konfiguration der Access Points zu starten. Wenn die Installation abgeschlossen ist, sehen Sie eine Liste der **Managed** Access Points.

Abb. 174: **Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard**

Damit Ihre `Gäste` nur das Internet nutzen können, aber keinen Zugriff auf Ihre anderen Netzwerkkomponenten erhalten, ist es notwendig Firewall Regeln hinzuzufügen. Hier ein Beispiel einer einfachen Firewall Regel, um den `Gästen` den Zugriff auf das interne Netz zu verbieten.

Zunächst werden zwei neue Gruppen angelegt, um so die Definition der Filterregeln über-

sichtlicher zu gestalten.

Gehen Sie dazu folgendermaßen vor:

(1) Gehen Sie zu **Firewall** -> **Dienste** -> **Gruppen** -> **Neu**.

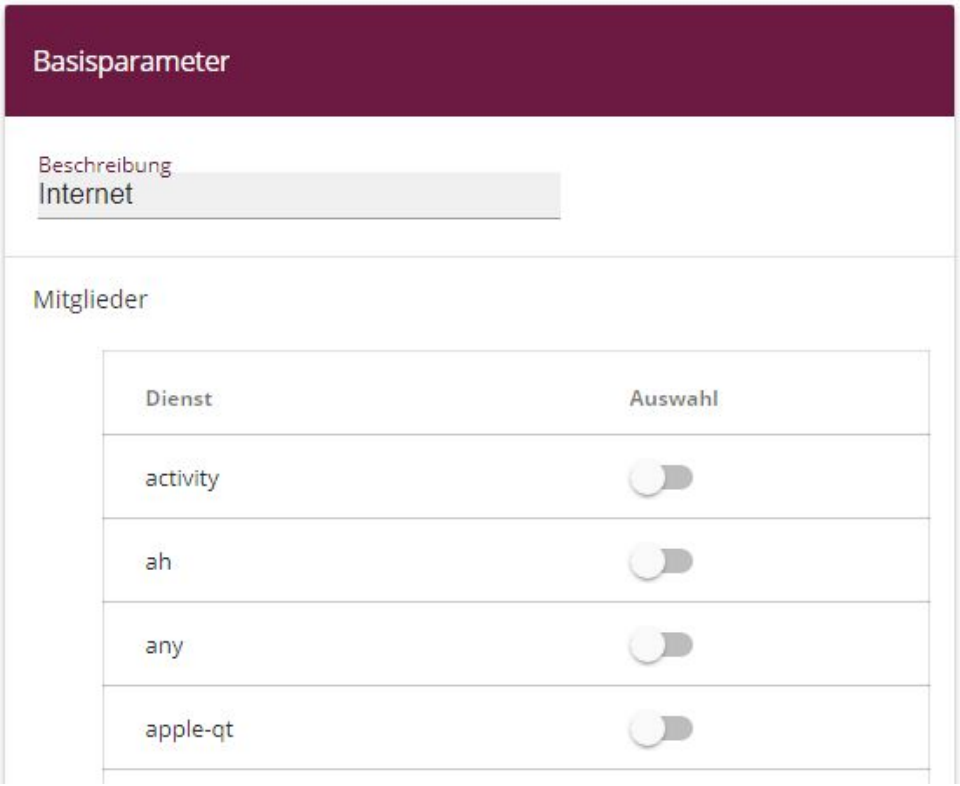


Abb. 175: **Firewall** -> **Dienste** -> **Gruppen** -> **Neu**

Gehen Sie folgendermaßen vor:

(1) Geben Sie eine **Beschreibung** der Service-Gruppe ein, z. B. `Internet`.

(2) Wählen Sie aus den zur Verfügung stehenden Service-Aliassen die Mitglieder der Gruppe aus. Aktivieren Sie dazu das Feld in der Spalte **Mitglieder**.

(3) Bestätigen Sie mit **OK**.

Gehen Sie analog für die Einstellungen der zweiten Gruppe vor, z. B. `lokale dienste`.

Die fertige Konfiguration sieht nun wie folgt aus:

Abb. 176: **Firewall** -> **Dienste** -> **Gruppen**

Im letzten Schritt werden noch die lokalen Dienste eingeschränkt. Der Zugriff auf die Dienste `http` und `http(SSL)` muss erlaubt werden, damit der Router die Anmeldeseite den HotSpot-Gästen anzeigen kann.

(1) Gehen Sie zu **Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**.

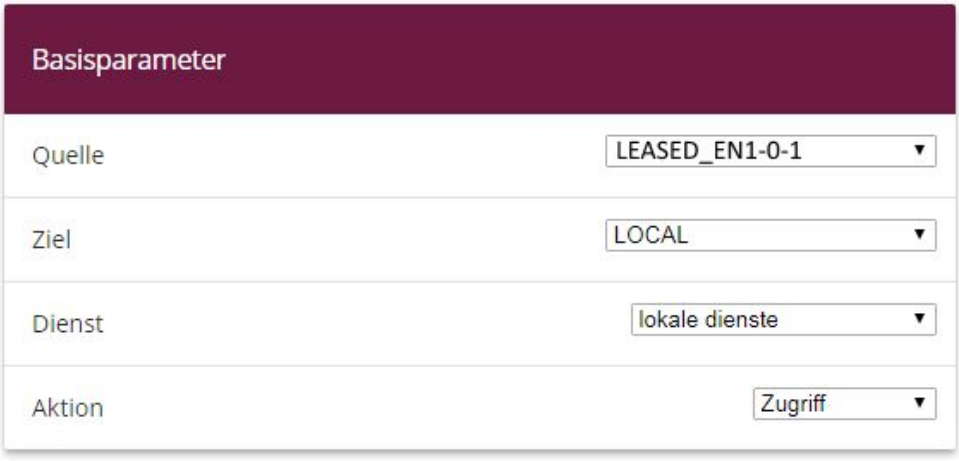


Abb. 177: **Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**

Gehen Sie folgendermaßen vor, um die Lokalen Dienste einzuschränken:

(1) Wählen Sie bei **Quelle** z. B. `LEASED_EN1-0-1` aus.

(2) Bei **Ziel** wählen Sie z. B. `LOCAL` aus.

(3) Wählen Sie den **Dienst** aus, z. B. `lokale dienste`.

(4) Wählen Sie bei **Aktion** `Zugriff` aus.

(5) Bestätigen Sie die Angaben mit **OK**.

Gehen Sie analog für die Einstellungen weiterer Dienste vor.

Die fertige Konfiguration sieht dann z. B. folgendermaßen aus:

Abb. 178: **Firewall** -> **Richtlinien** -> **Filterregeln**

Die Konfiguration ist hiermit abgeschlossen. Speichern Sie die Konfiguration mit **Konfiguration speichern** und bestätigen Sie die Auswahl mit **OK**.

Sie können nun die Konfiguration testen. Melden Sie sich dazu mit der SSID der `Mitarbeiter` beziehungsweise mit der SSID der `Gäste` an.

Hinweis

Es wird empfohlen, eine E-Mail-Benachrichtigung bei **Ausfall eines WTP** zur Überwachung des Systems zu konfigurieren.

10.4 Konfigurationsschritte im Überblick

LAN Konfiguration

Feld	Menü	Wert
IP-Adresse / Netzmaske	**LAN -> IP-Konfiguration -> Schnittstellen -> <en1-0>**	z. B. *192.168.100.254*
Schnittstellenmodus	**LAN -> IP-Konfiguration -> Schnittstellen -> <en1-0>**	*Untagged*
Basierend auf Ethernet-Schnittstelle	**LAN -> IP-Konfiguration -> Schnittstellen -> Neu**	*en1-0*
IP-Adresse / Netzmaske	**LAN -> IP-Konfiguration -> Schnittstellen -> Neu**	z. B. *192.168.15.254*
Schnittstellenmodus	**LAN -> IP-Konfiguration -> Schnittstellen -> Neu**	*Tagged (VLAN)*
VLAN-ID	**LAN -> IP-Konfiguration -> Schnittstellen -> Neu**	*15*
Basierend auf Ethernet-Schnittstelle	**LAN -> IP-Konfiguration -> Schnittstellen -> Neu**	*en1-0*
IP-Adresse / Netzmaske	**LAN -> IP-Konfiguration -> Schnittstellen -> Neu**	z. B. *192.168.16.254*
Schnittstellenmodus	**LAN -> IP-Konfiguration -> Schnittstellen -> Neu**	*Tagged (VLAN)*
VLAN-ID	**LAN -> IP-Konfiguration -> Schnittstellen -> Neu**	*16*

Hotspot Konfiguration

Feld	Menü	Wert
Authentifizierungstyp	**Systemverwaltung -> Remote Authentifizierung -> RADIUS -> Neu**	*Accounting*
Betreibermodus	**Systemverwaltung -> Remote Authentifizierung -> RADIUS -> Neu**	*bintec HotSpot Server*
Server-IP-Adresse	**Systemverwaltung -> Remote Authentifizierung -> RADIUS -> Neu**	z. B. *62.245.165.180*
RADIUS-Passwort	**Systemverwaltung -> Remote Authentifizierung -> RADIUS -> Neu**	z. B. *supersecret*
Standard-Benutzerpasswort	**Systemverwaltung -> Remote Authentifizierung -> RADIUS -> Neu**	z. B. *supersecret*

Feld	Menü	Wert
Priorität	**Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**	*0*
Authentifizierungstyp	**Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**	*Login-Authentifizierung*
Server-IP-Adresse	**Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**	z. B. *62.245.165.180*
RADIUS-Passwort	**Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**	z. B. *supersecret*
Standard-Benutzerpasswort	**Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**	z. B. *supersecret*
Priorität	**Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu**	*0*

Hotspot-Netzwerk einrichten

Feld	Menü	Wert
Schnittstelle	**Lokale Dienste** -> **Hotspot-Gateway** -> **Hotspot-Gateway** -> **Neu**	z. B. *LAN_EN1-0*
Domäne am Hotspot-Server	**Lokale Dienste** -> **Hotspot-Gateway** -> **Hotspot-Gateway** -> **Neu**	z. B. *training-fec_1.de*
Walled Garden	**Lokale Dienste** -> **Hotspot-Gateway** -> **Hotspot-Gateway** -> **Neu**	*Aktiviert*
Walled Network / Netzmaske	**Lokale Dienste** -> **Hotspot-Gateway** -> **Hotspot-Gateway** -> **Neu**	z. B. *62.146.53.196* und *255.255.255.255*
Walled Garden URL	**Lokale Dienste** -> **Hotspot-Gateway** -> **Hotspot-Gateway** -> **Neu**	*http://www.bintec-elmeg.com*
Geschäftsbedingungen	**Lokale Dienste** -> **Hotspot-Gateway** -> **Hotspot-Gateway** -> **Neu**	*http://www.bintec-elmeg.com*
Sprache für Anmeldefenster	**Lokale Dienste** -> **Hotspot-Gateway** -> **Hotspot-Gateway** -> **Neu**	z. B. *Deutsch*

DHCP Konfiguration

Feld	Menü	Wert
IP-Poolname	**Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu**	z. B. *Mitarbeiter*
IP-Adressbereich	**Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu**	z. B. *192.168.15.10* - *192.168.15.110*
Schnittstelle	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	*en1-0-1*

Feld	Menü	Wert
IP-Poolname	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	z. B. *Mitarbeiter*
Poolverwendung	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	*Lokal*
IP-Poolname	**Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfiguration** -> **Neu**	z. B. *Gäste*
IP-Adressbereich	**Lokale Dienste** -> **DHCP-Server** -> **IP-Pool-Konfigurationn** -> **Neu**	z. B. *192.168.16.10* - *192.168.16.110*
Schnittstelle	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	*en1-0-2*
IP-Poolname	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	z. B. *Gäste*
Poolverwendung	**Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Neu**	*Lokal*

WLAN Controller Wizard

Feld	Menü	Wert
Region	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard**	*Germany*
Schnittstelle	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard**	*LAN_EN1-0*
DHCP-Server	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard**	*Intern*
IP-Adressbereich	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard**	z. B. *192.168.100.10* - *192.168.100.110*
Funkmodulprofil	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard** -> **Weiter**	*2,4 GHz Radio Profile*
Netzwerkname (SSID)	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard** -> **Weiter**	z. B. *Mitarbeiter*
Sicherheitsmodus	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard** -> **Weiter**	*WPA-PSK*
WPA-Modus	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard** -> **Weiter**	*WPA2*
Preshared Key	**Wireless LAN Controller** -> **Wizard**	z. B. *supersecret*

Feld	Menü	Wert
	-> **Wireless LAN Controller Wizard** -> **Weiter**	
VLAN	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard** -> **Weiter**	*Aktiviert*
VLAN-ID	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard** -> **Weiter**	*15*
Netzwerkname (SSID)	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard** -> **Weiter** -> **Hinzufügen**	z. B. *Gäste*
Sicherheitsmodus	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard** -> **Weiter** -> **Hinzufügen**	Inaktiv
VLAN	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard** -> **Weiter** -> **Hinzufügen**	*Aktiviert*
VLAN-ID	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard** -> **Weiter** -> **Hinzufügen**	*16*
Standort	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard** -> **Weiter**	z. B. *1:Office*
Aktives Funkmodul-profil	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard** -> **Weiter**	*2,4 GHz Radio Profile*
Zugewiesene Drahtlos-netzwerke (VSS)	**Wireless LAN Controller** -> **Wizard** -> **Wireless LAN Controller Wizard** -> **Weiter**	z. B. *vss-1:Mitarbeiter* und *vss-2:Gäste*

Firewall Regeln hinzufügen

Feld	Menü	Wert
Beschreibung	**Firewall** -> **Dienste** -> **Gruppen** -> **Neu**	z. B. *Internet*
Mitglieder	**Firewall** -> **Dienste** -> **Gruppen** -> **Neu**	z. B. *http*, *http (SSL)*
Beschreibung	**Firewall** -> **Dienste** -> **Gruppen** -> **Neu**	z. B. *lokale Dienste*

Feld	Menü	Wert
Mitglieder	**Firewall** -> **Dienste** -> **Gruppen** -> **Neu**	z. B. *http*, *http (SSL)*

Lokale Dienste einschrenken

Feld	Menü	Wert
Quelle	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*LEASED_EN1-0-1*
Ziel	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*LOCAL*
Dienst	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*lokale dienste*
Aktion	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*Zugriff*
Quelle	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*LEASED_EN1-0-2*
Ziel	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*LOCAL*
Dienst	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*lokale dienste*
Aktion	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*Zugriff*
Quelle	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*LAN_EN1-0-1*
Ziel	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*LAN_EN1-0-1*
Dienst	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*any*
Aktion	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*Verweigern*
Quelle	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*LAN_EN1-0-2*
Ziel	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*LAN_EN1-0-2*
Dienst	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*any*
Aktion	**Firewall** -> **Richtlinien** -> **Filterregeln** -> **Neu**	*Verweigern*

Kapitel 11 WLAN - Cloud NetManager

11.1 Einleitung

Der Cloud NetManager ist ein System, das in der Lage ist sowohl sehr kleine als auch sehr große und auf viele Standorte verteilte Netze zu verwalten.

Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Ein registrierter Benutzer auf dem Portal des Cloud NetManager
- Ein oder mehrere **bintec** WLAN Access Points z. B. **W1001n**, **W1003n**, **W2003n**, … mit der Software Rel. 10.1.8 Patch 2 oder höher
- Den DVC (Device Verification Code) des zu verwaltenden Access Points oder ein DHCP-Server, der die Option 43 unterstützt
- Für jeden Access Point eine gültige Cloud NetManager-Lizenz
- Ein Internetzugang

11.2 Erste Schritte im Portal

11.2.1 Anlegen eines Benutzers

Öffnen Sie einen Browser, und geben Sie in die Adresszeile die URL: *https://bintec.networkcloudmanager.com* ein.

Sie müssen sich zuerst registrieren. Klicken Sie dazu auf der Anmeldeseite oben rechts auf **Registrieren**.

Geben Sie die erforderlichen Daten für die Registrierung ein.

Die Felder **Partnernummer** und **Anmeldung** sind optional.

Falls Sie für Ihr Unternehmen mehr als ein Benutzerkonto haben, beachten Sie bitte Folgendes:

- Für jeden Firmennamen kann nur ein Benutzer eingerichtet werden. Daher muss man möglicherweise die Schreibweise der Firma variieren (z. B. Firma_1; Firma_2; …).

- Falls ein weiterer Benutzer das gleiche WLAN-Netz verwalten soll, so legen Sie hier keinen weiteren Benutzer an. Weitere Benutzer für Ihren Account können Sie nach dem Login einrichten, sowohl mit vollen als auch mit eingeschränkten Benutzerrechten.
- Wenn Sie einen weiteren Benutzer einrichten möchten, der die Einstellungen des ersten bereits eingerichteten Benutzers nicht sehen soll, so können Sie das an dieser Stelle tun.

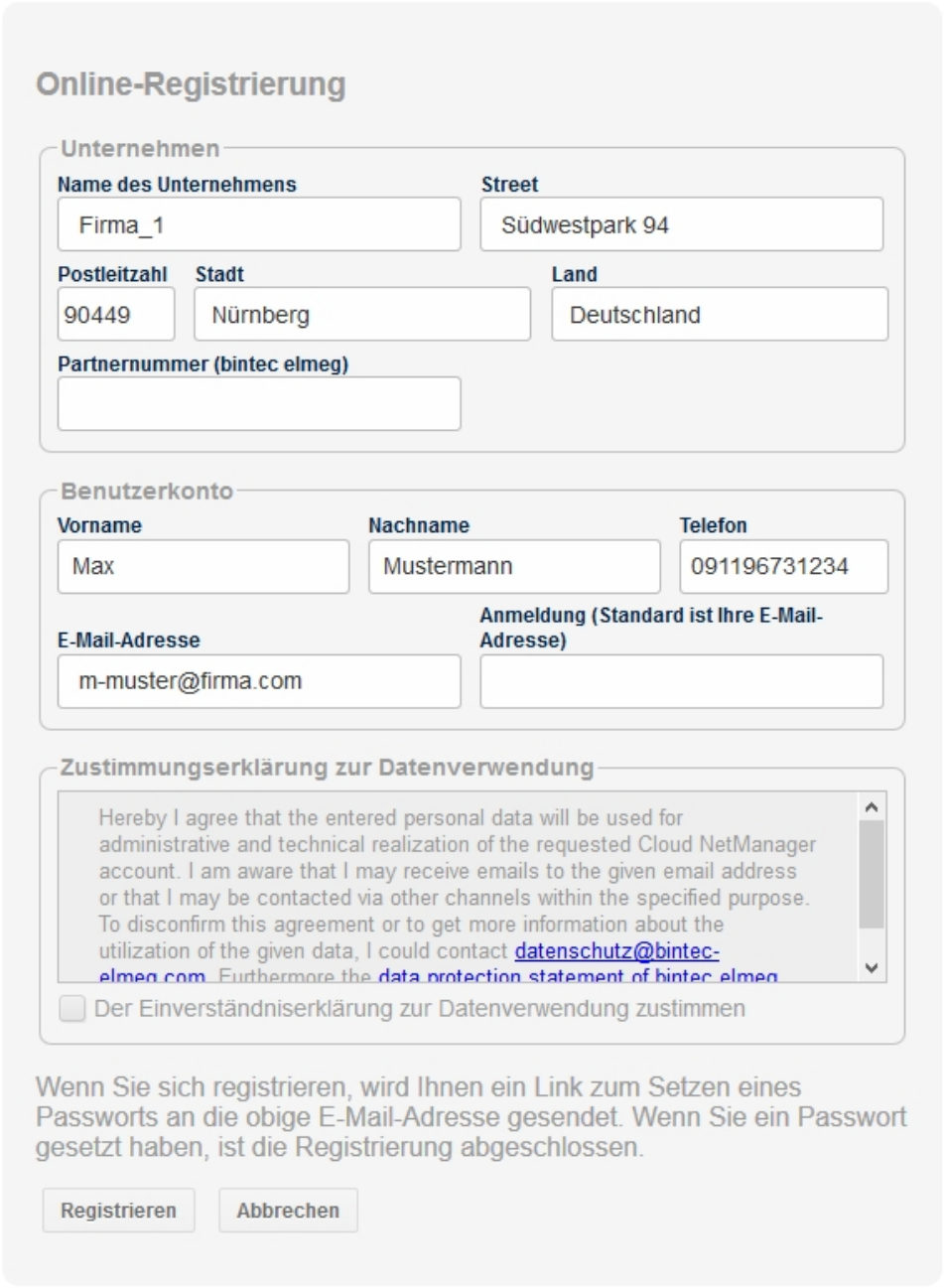


Abb. 179: Online-Registrierung

Nach dem Absenden des Registrierungsformulars erhalten Sie eine E-Mail, dies kann einige Minuten dauern.

Folgen Sie den Anweisungen und legen Sie ein **Passwort** für Ihren Benutzer fest.

11.2.2 Ändern der Zeitzone

Die Zeitzone steht beim ersten Login auf **UTC**. Bitte ändern Sie diese auf **Europe/Berlin**.

Zusätzlich haben Sie hier die Möglichkeit, die Sprache auszuwählen.

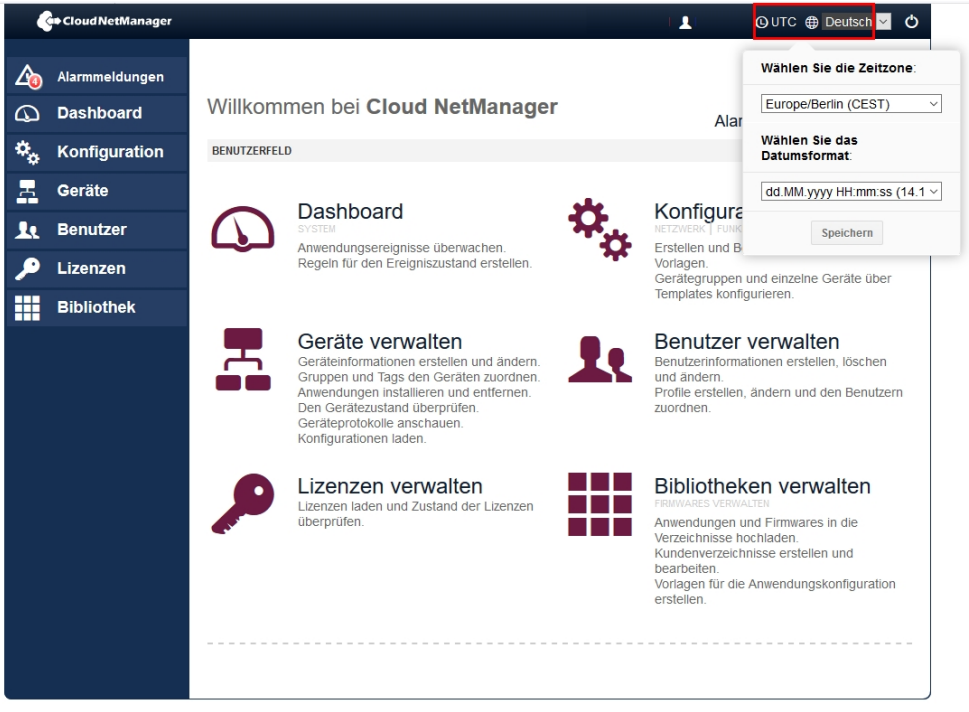


Abb. 180: Ändern der Zeitzone

11.2.3 Einspielen der Lizenzen

Gehen Sie auf der Statusseite in das Menü **Lizenzen->Lizenzen für diesen cloud Server->Neue Lizenz**.

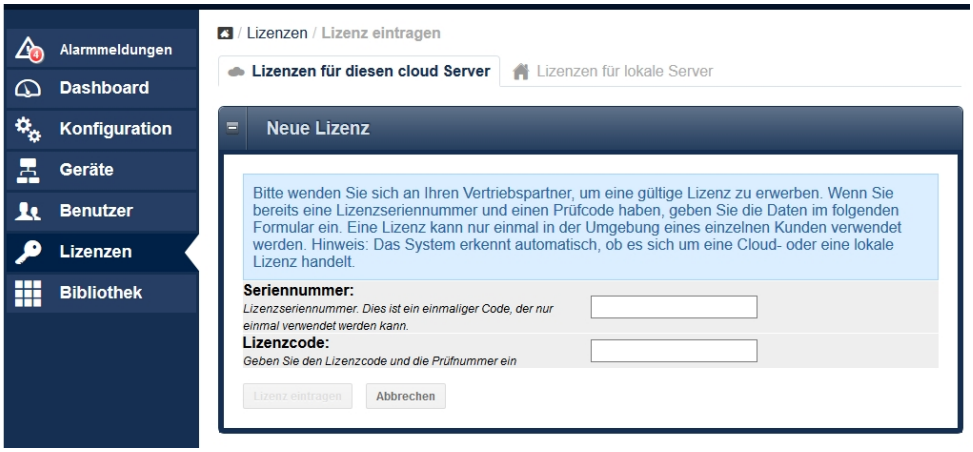


Abb. 181: Neue Lizenz

- Tragen Sie die **Seriennummer** und den **Lizenzcode** (PIN) ein.
- Klicken Sie auf **Lizenz eintragen**.

In der Übersicht **Lizenzen verwalten** wird angezeigt, welche Lizenzen unter Ihrem Account verfügbar sind.

Abb. 182: Übersicht

Bitte beachten Sie, dass hier immer nur die installierten Lizenzen angezeigt werden. Die Verfügbarkeit zeigt nicht die Restlaufzeit an, sondern die Laufzeit der gekauften Lizenz bzw. des Lizenzpaketes.

- Eine Lizenz, die auf einen Benutzer-Account registriert wurde, kann nachträglich nicht auf einen anderen Benutzer übertragen werden.
- Die Lizenzlaufzeit wird nur herunter gezählt, wenn die Lizenz für das Management eines Gerätes genutzt wird. Wenn das verwaltete Gerät entfernt wird, steht die Lizenz für andere Geräte zur Verfügung. Die Laufzeit wird nicht herunter gezählt, wenn die Lizenz nicht

in Benutzung ist.

- Wenn die Lizenz für ein verwaltetes Gerät ausläuft, holt sich das System eine weitere Lizenz aus dem Pool der registrierten Lizenzen. Wenn keine freie Lizenz mehr vorhanden ist, wird das Management für das betreffende Gerät gestoppt. Es ist keine Veränderung der Konfiguration und auch kein Monitoring mehr möglich. Das Gerät selbst funktioniert selbstverständlich weiter, auch nach einem Stromausfall.

Sie können sich die Lizenzen anzeigen lassen, die von einem verwalteten Gerät benutzt werden. Klicken Sie dazu unter **Status** auf **Gültige Lizenz**.

Abb. 183: Geräte, die der Lizenz zugeordnet sind

11.3 Anlegen der Profile

11.3.1 Anlegen der Netzwerkprofile (SSID)

Mindestens ein Netzwerkprofil (SSID) muss angelegt werden.

Gehen Sie dazu in das Menü **Konfiguration**->**Netzwerk**.

Klicken Sie auf **Neues Netzwerkprofil**.

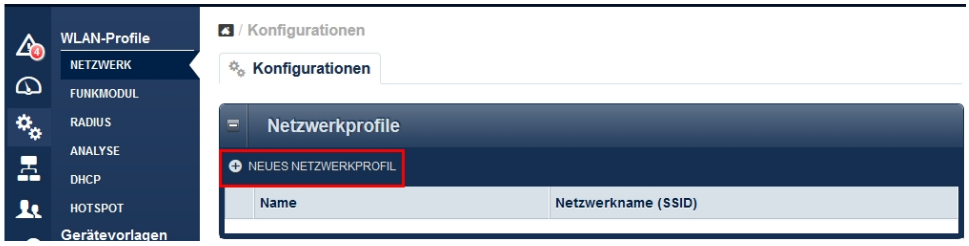


Abb. 184: Netzwerkprofile

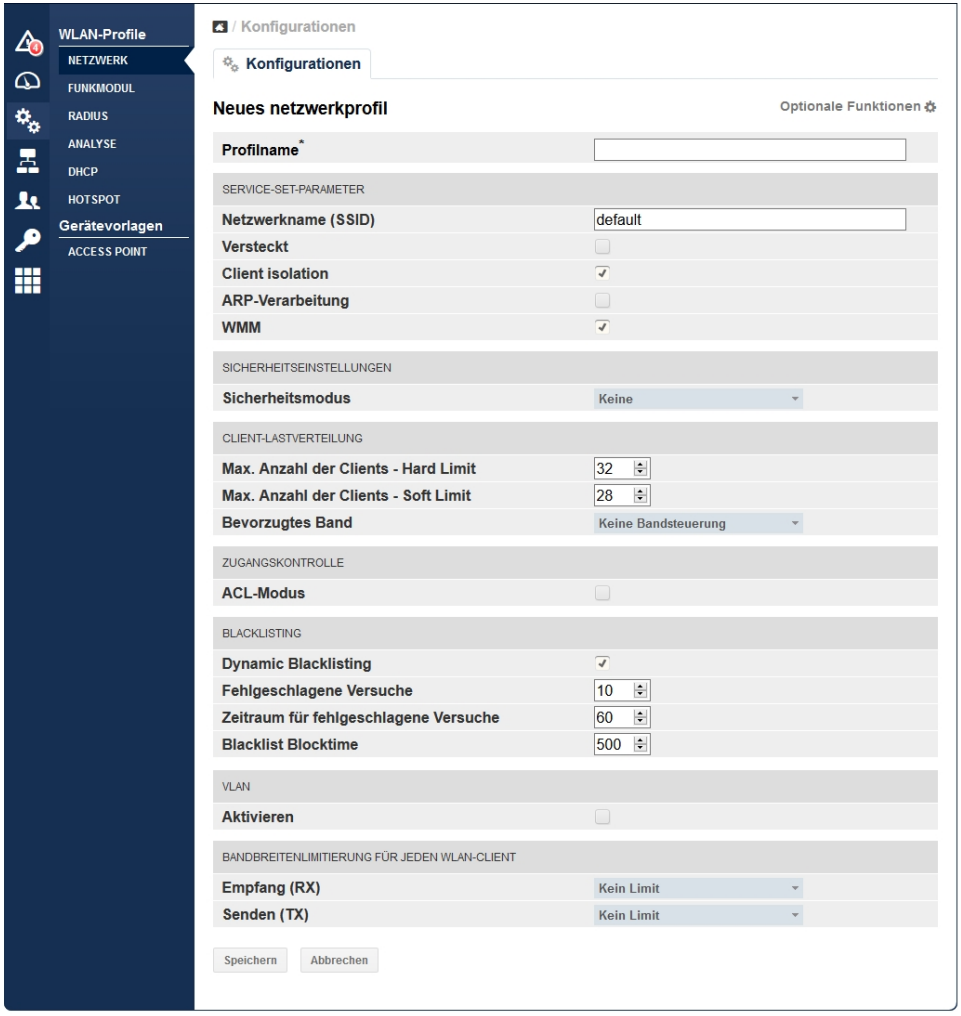


Abb. 185: Konfiguration der Netzwerkprofile

Die wesentlichen Parameter für die jeweilige SSID sind voreingestellt. Die Parameter sind

identisch zur Standardkonfiguration der bintec Access Points oder des WLAN Controllers.

- Bei **Profilname** geben Sie den Namen des WLAN-Netzwerksprofils ein.
- Der **Netzwerkname (SSID)** ist der Name des WLAN-Netzwerks, wie er von Benutzern des Access Points gesehen wird.
- Klicken Sie auf **Speichern**, um Ihre Angaben zu bestätigen.

11.3.2 Anlegen der Funkprofile

Mindestens ein Funkprofil muss angelegt werden.

Wenn Access Points mit zwei Funkmodulen verwaltet werden sollen, sollte für 2,4 GHz und für 5 GHz jeweils ein Funkprofil angelegt werden. Die Parameter sind identisch zur Standardkonfiguration der bintec Access Points oder des WLAN Controllers.

Gehen Sie in das Menü **Konfiguration**->**Funkmodul**->**Neues Funkmodul-Profil**.

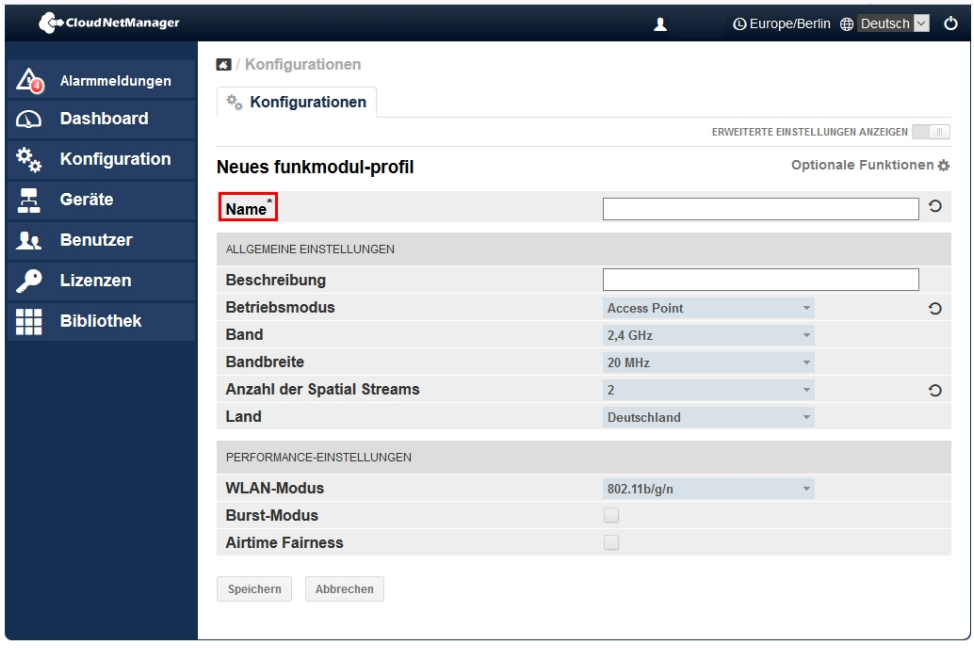


Abb. 186: Neues Funkmodulprofil

Gehen Sie folgendermaßen vor:

- Geben Sie einen **Namen** für das Funkprofil ein.
- Stellen Sie den **Betriebsmodus** auf `Access Point`.

- Für **Band** = *2,4 GHz* wählen Sie die **Bandbreite** *20 MHz* aus.
- Für **Band** = *5 GHz* wählen Sie die **Bandbreite** *20 MHz* oder *40 MHz* (empfohlen) aus.
- Den **WLAN-Modus** für 2,4 GHz Profile setzen Sie auf *802.11b/g/n*.
- Den **WLAN-Modus** für 5 GHz Profile setzen Sie auf *802.11ac/a/n*.
- Bestätigen Sie Ihre Angaben, indem Sie auf **Speichern** klicken.

11.3.3 Anlegen der Gerätevorlagen / Access-Point-Vorlage

Mindestens eine Gerätevorlage muss definiert werden.

Gehen Sie in das Menü **Konfiguration**->**Access Point**->**Neue Access-Point-Vorlage**.

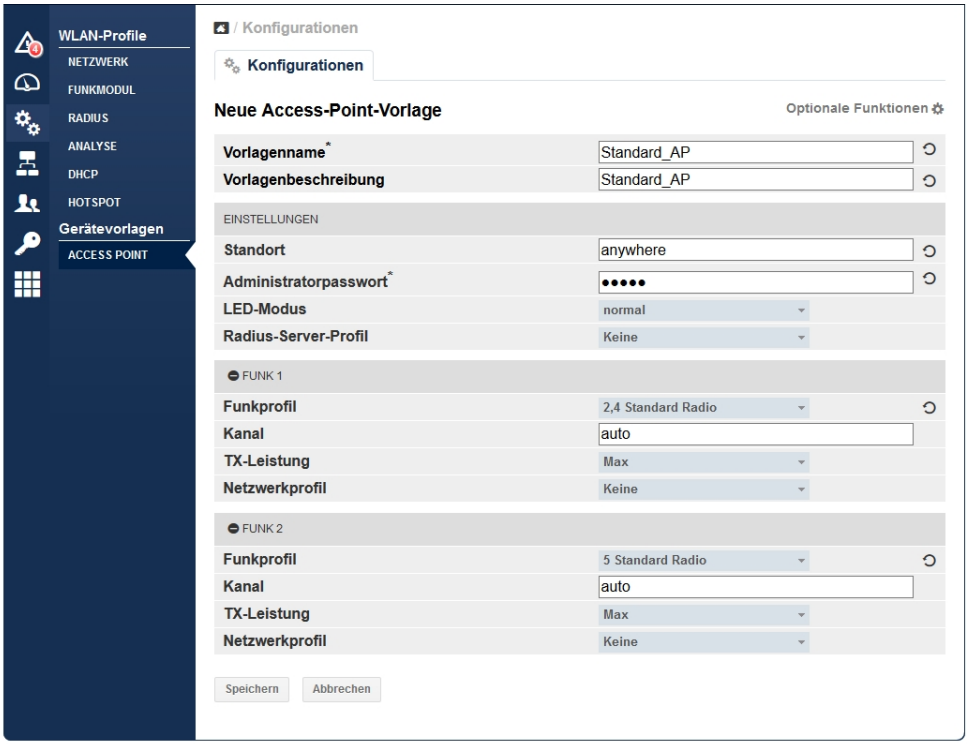


Abb. 187: Gerätevorlage

Gehen Sie folgendermaßen vor:

- Geben Sie bei **Vorlagenname** einen Namen für die Vorlage ein.
- Geben Sie das **Administratorpasswort** ein.
- Das **Administratorpasswort** ist das Passwort zum lokalen Einloggen auf einem Access

Point. Im Gegensatz zum bintec WLAN Controller kann man sich hier auf einen Access Point lokal einloggen. Allerdings sind alle WLAN-relevanten Teile der Konfiguration nicht lokal konfigurierbar.

- Falls Sie bei der SSID-Konfiguration den Sicherheitsmodus `WPA-Enterprise` gewählt haben, müssen Sie hier ein **Radius-Server-Profil** definieren.
- Wichtig ist, dass dem Funkmodul 1 ein 2,4 GHz-Funkprofil und dem Funkmodul 2 ein 5 GHz-Funkprofil zugeordnet wird.
- Bestätigen Sie Ihre Angaben, indem Sie auf **Speichern** klicken.

11.3.4 Geräte verwalten

Im Menü **Geräte** wird eine Liste aller registrierten Geräte angezeigt. Zuerst müssen Sie eine **Gruppe** anlegen.

Abb. 188: Geräte verwalten

Gehen Sie in das Menü **Geräte**->**Gruppen**->**Neue Gruppe**.

Abb. 189: Geräte verwalten / Gruppe

- Wählen Sie die zuvor definierte **Konfigurationsvorlage** aus.
- Aktivieren Sie die **Automatische Aktualisierung**. Hiermit wird jede Konfigurationsänderung sofort wirksam.

- Bestätigen Sie Ihre Angaben, indem Sie auf **Neue Gruppe** klicken.

11.4 Access Points registrieren und verwalten

Um ein neues Gerät hinzuzufügen, gehen Sie in das Menü **Geräte**->**Geräte verwalten**->**Geräte hinzufügen**.

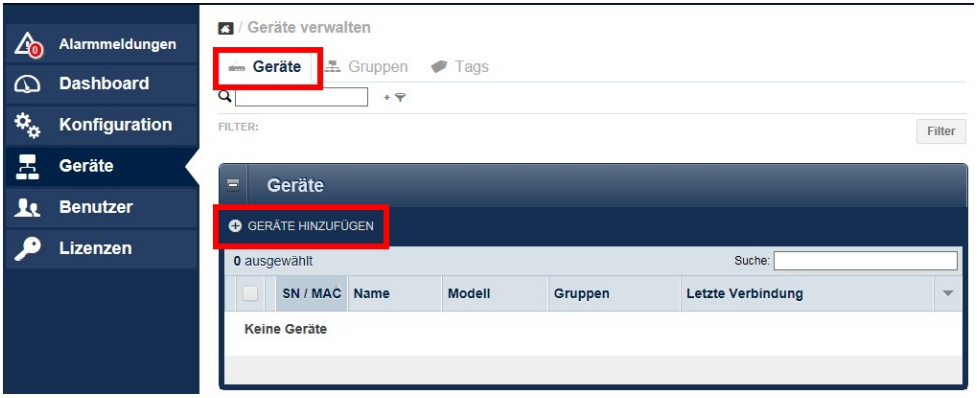


Abb. 190: Access Points registrieren und verwalten

11.4.1 Geräte manuell anmelden

Für eine manuelle Registrierung, gehen Sie in das Menü **Geräte**->**Geräte hinzufügen**->**Manuelle Anmeldung**.

Abb. 191: Manuelle Anmeldung

Gehen Sie folgendermaßen vor:

- Wenn bei **Modus** die Option **Geben Sie die Seriennummer manuell ein** aktiviert ist, benötigen Sie die **Seriennummer,** die Sie auf dem Typenschild des Gerätes finden.
- Wenn bei **Modus** die Option **Geben Sie Geräte aus der Datenquelle (.cvs) ein** aktiviert ist, benötigen Sie den **Gerätesicherheitscode (DVC),** den Sie auf dem Typenschild des Gerätes finden. Falls der DVC noch nicht auf dem Typenschild des Gerätes vorhanden ist, so wenden Sie sich bitte an unseren Support.
- Wenn Sie mehr als ein Gerät gleichzeitig registrieren möchten, können Sie eine **CSV-Datei** erstellen und einlesen.
- Klicken Sie auf **Geräte hinzufügen,** um Ihre Angaben zu bestätigen.

11.4.2 Gerät automatisch anmelden

Für die automatische Registrierung, gehen Sie in das Menü **Geräte**->**Geräte hinzufügen**->**Automatische Anmeldung**.

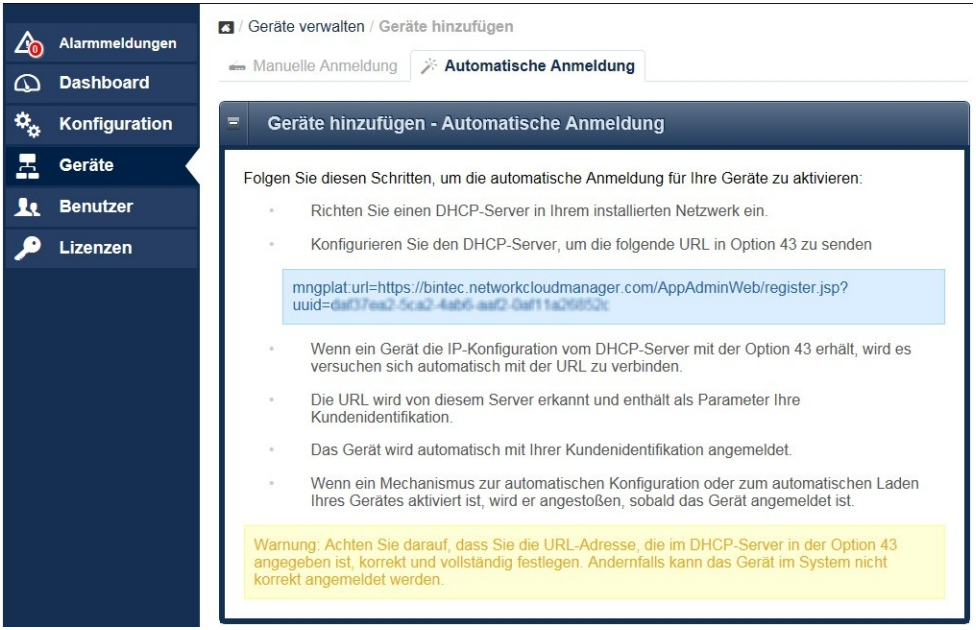


Abb. 192: Automatische Anmeldung

Mit der **DHCP-Option** *43* kann der lokale DHCP-Server des Netzes, in dem sich der Access Point befindet, dem Access Point mitteilen, mit welcher User-ID sich der Access Point beim Cloud NetManager anmelden soll. Dadurch wird eine automatische Registrierung und eine automatische Inbetriebnahme ohne Eingabe von Seriennummer und DVC (siehe *Geräte verwalten* auf Seite 276) ermöglicht.

11.5 Geräteverwaltung

Im Menü **Geräte** werden die registrierten Geräte angezeigt.

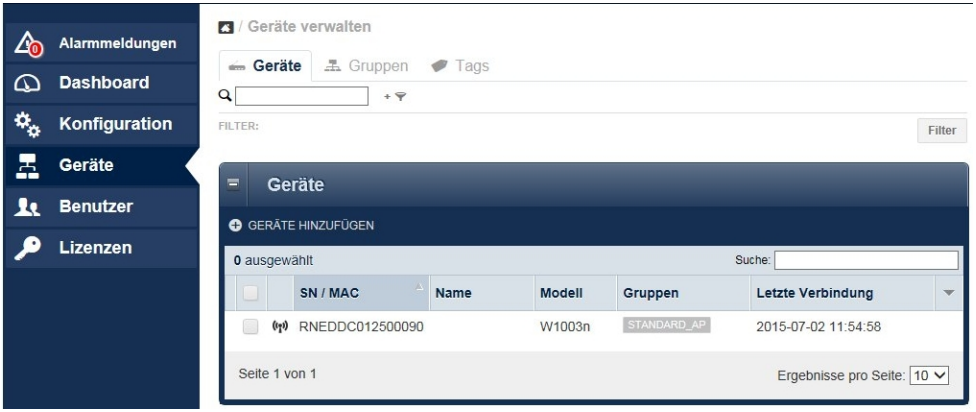


Abb. 193: Geräte anzeigen

Durch Klicken auf die Zeile eines Gerätes in der Übersicht wird die Detailansicht angezeigt.

Mit **Bearbeiten** können Sie die **Details** bearbeiten. Klicken Sie auf **Auslastung** oder **Erweitert**, um diese Optionen anzeigen zu lassen.

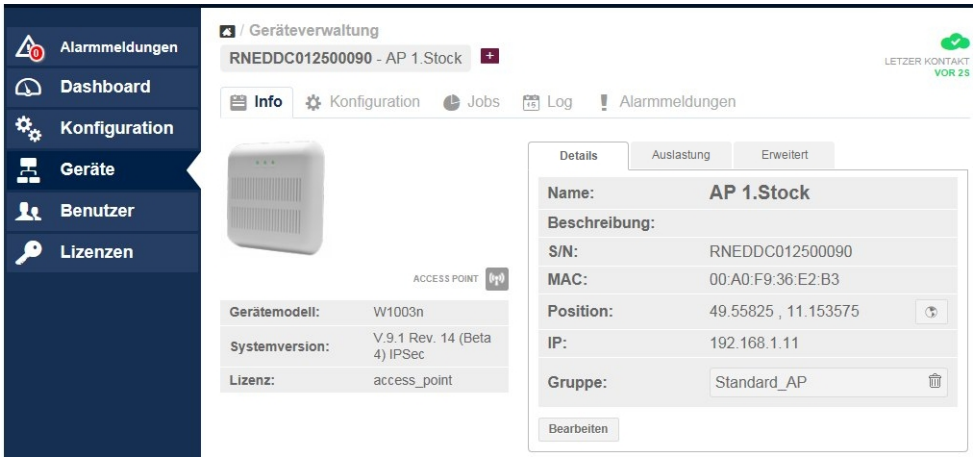


Abb. 194: Detailansicht

11.5.1 Batch-Operationen und Software-Update

In der Geräteansicht finden sich weitere Möglichkeiten zur Geräteverwaltung. Wenn Sie in der Geräteansicht mehrere Geräte markieren, gibt es zum Beispiel die Möglichkeit **Batch-Operationen** zu starten, um die **Firmware** der markierten Geräte zu aktualisieren.

Abb. 195: Bach-Operationen

Abb. 196: Operationen wählen

11.6 Anhang

11.6.1 Einrichtung eines anderen Rechenzentrums

Wenn Sie nicht unseren Cloud NetManager als SaaS (Software as a Service) verwenden möchten, sondern den Virtual Cloud NetManager in Ihrem eigenen Rechenzentrum hosten möchten, müssen Sie den Access Points eine andere Cloud NetManager-URL zuweisen. Dazu haben Sie zwei Möglichkeiten.

11.6.1.1 URL Zuweisung über die DHCP Option 43

Sie können den Access Points eine andere Cloud NetManager-URL zuweisen. Dazu müssen Sie beim dem lokalen DHCP-Server die **Option 43** (vendor specific option) konfigurieren.

Wenn Sie den DHCP-Server eines **bintec**-Router verwenden, gehen Sie folgendermaßen vor:

Gehen Sie im **GUI** (Graphical User Interface) in das Menü **Lokale Dienste**->**DHCP-Server**->**DHCP-Konfiguration**.

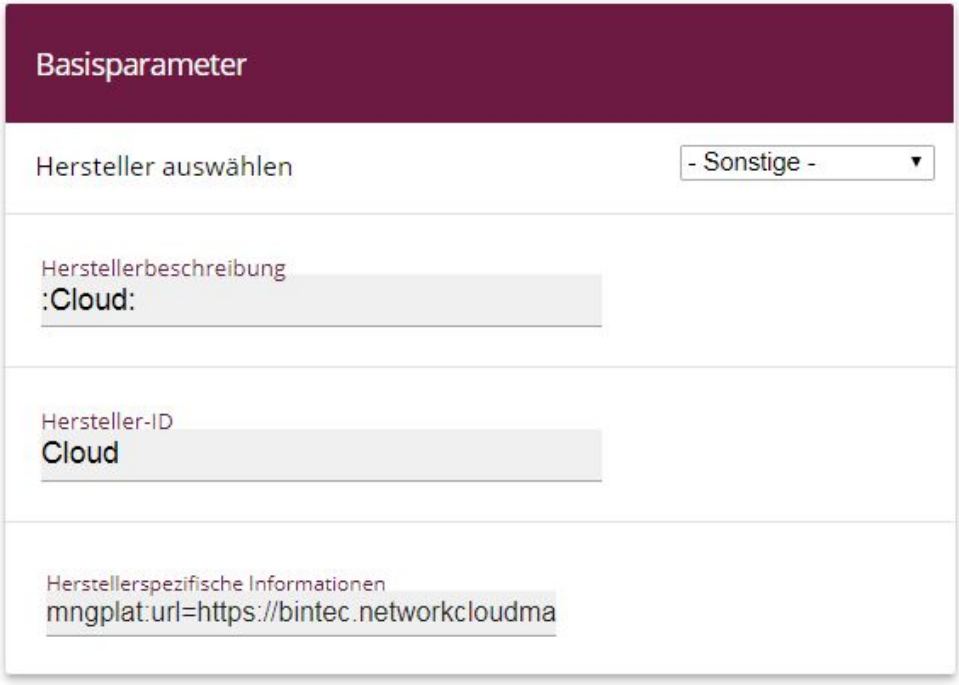


Abb. 197: **Lokale Dienste->DHCP-Server->DHCP-Konfiguration**

- Wählen Sie das Symbol , um den entsprechenden Eintrag zu bearbeiten.
- Gehen Sie zur **Erweitere Einstellungen**.
- Klicken Sie im Feld **Herstellerspezifische Informationen (DHCP-Option 43)** auf die Schaltfläche **Hersteller-String hinzufügen**.
- Bei **Hersteller auswählen** wählen Sie `-Sonstige-` aus.
- Bei **Herstellerbeschreibung** geben Sie den Namen des Herstellers, z. B. `:Cloud:` ein.
- Um das Gerät zu identifizieren, geben Sie hier die **Hersteller-ID** ein, hier z. B. `Cloud`.
- Unter **Herstellerspezifische Informationen** geben Sie die neue Cloud NetManager-URL ein. Wenn Sie gleichzeitig eine User-ID übermitteln möchten, lesen Sie zuvor den String aus dem Cloud NetManager aus (siehe *Gerät automatisch anmelden* auf Seite 278).
- Klicken Sie auf die Schaltfläche **Übernehmen**.

11.6.1.2 Direkte URL Änderung in der GUI

Über die **GUI** des Access Point können Sie eine andere Cloud NetManager-Adresse eintragen.

Optional kann auch die User-ID des betreffenden Kontos übergeben werden. In diesem Fall wird das Gerät automatisch registriert und mit der Standardkonfiguration konfiguriert.

Gehen Sie in das Menu **Systemverwaltung**->**Globale Einstellungen**->**System**.

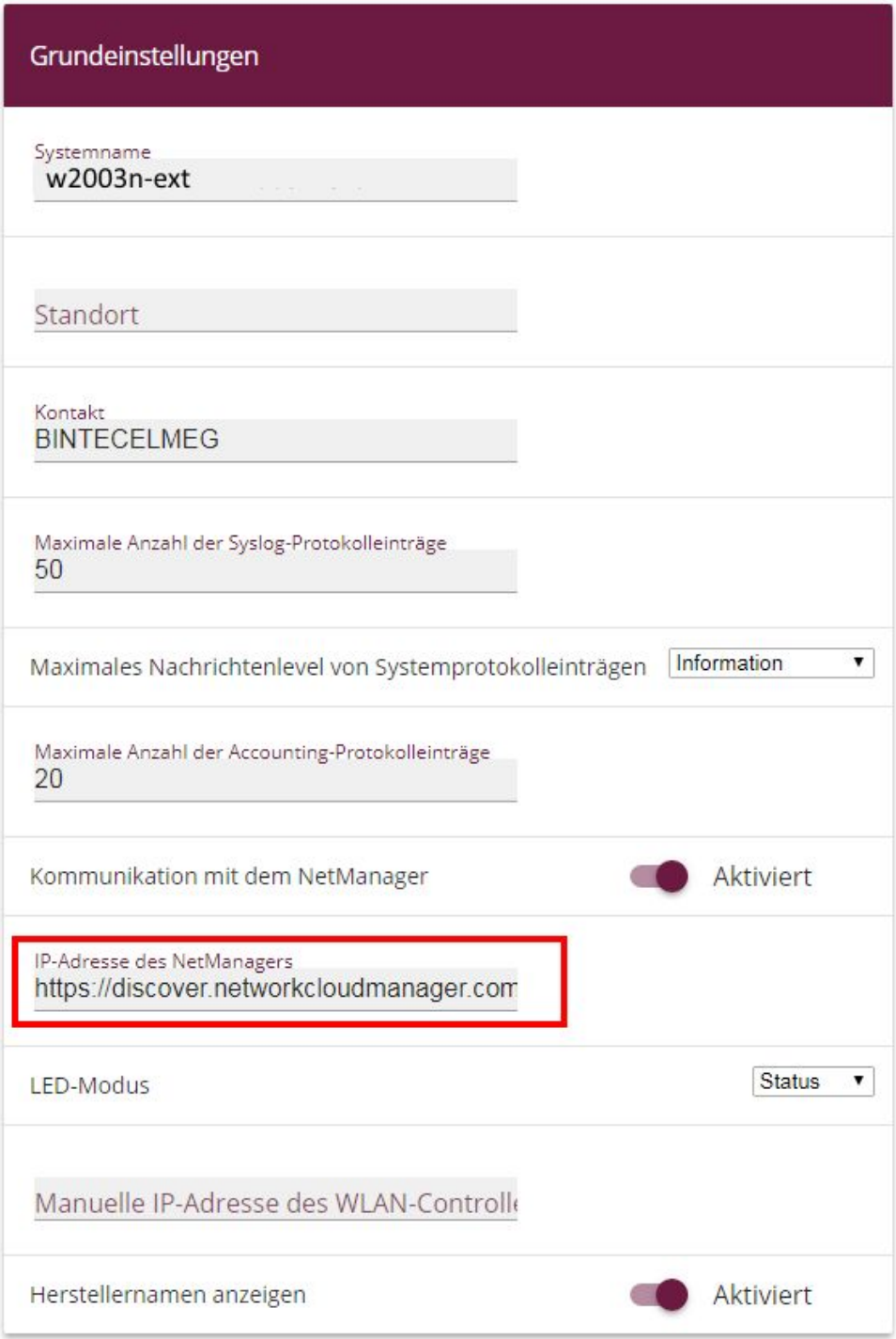

Grundeinstellungen
Systemname
w2003n-ext
Standort
Kontakt
BINTECELMEG
Maximale Anzahl der Syslog-Protokolleinträge
50
Maximales Nachrichtenlevel von Systemprotokolleinträgen
Information
Maximale Anzahl der Accounting-Protokolleinträge
20
Kommunikation mit dem NetManager
Aktiviert
IP-Adresse des NetManagers
https://discover.networkcloudmanager.com
LED-Modus
Status
Manuelle IP-Adresse des WLAN-Controlle
Herstellernamen anzeigen
Aktiviert

Abb. 198: **Systemverwaltung->Globale Einstellungen->System**

- Aktivieren Sie die Option **Kommunikation mit dem NetManager**.
- Im Feld **IP-Adresse des NetManagers** geben Sie die Cloud NetManager Adresse des Servers ein.
- Bestätigen Sie Ihre Angaben mit **OK**.

11.6.2 Automatische Konfiguration

Mit dem Cloud NetManager haben Sie die Möglichkeit eine einmal festgelegte Konfiguration automatisch auf jeden neuen Access Point, der an das lokale LAN angeschlossen wird, zu übertragen. Dieses Verfahren ist z. B. für kleine Filialen, die kein eigenes IT Personal vor Ort haben, geeignet, um schnell und einfach neue Access Points in Betrieb zu nehmen.

Um die automatische Konfiguration nutzen zu können, müssen drei Voraussetzungen erfüllt sein:

(a) Der Access Point muss sich automatisch am Cloud NetManager anmelden können. Dazu ist entweder die DHCP Option 43 mit dem User-ID String zu setzen oder die Cloud NetManager URL in der GUI des Access Point anzupassen. Die kundenspezifische URL mit User-ID können Sie unter **Geräte->Geräte hinzufügen->Automatische Anmeldung** im Cloud NetManager nachschauen.

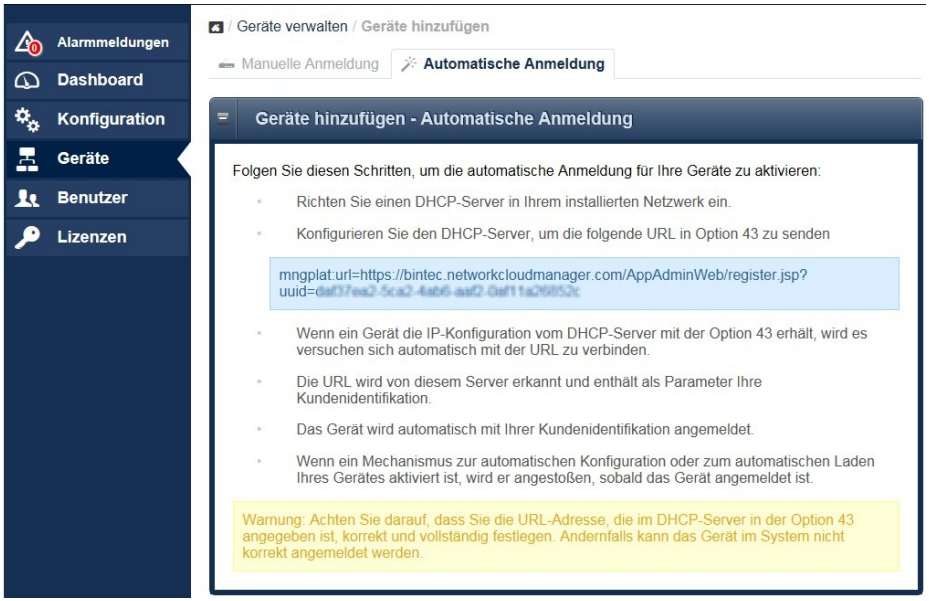


Abb. 199: **Geräte->Geräte hinzufügen->Automatische Anmeldung**

(b) Im Cloud NetManager unter **Geräte->Gruppen** muss eine **Standardgruppe** definiert

sein.

(c) Im Cloud NetManager unter **Geräte**->**Gruppen** muss bei der Standardgruppe die Option **Automatische Aktualisierung** aktiv sein.

Abb. 200: **Geräte->Gruppen**

11.7 Fehlersuche

11.7.1 Ein neues Gerät ist nicht sichtbar

Es gibt eine Reihe von Gründen, warum ein Gerät in der Geräteübersicht nicht angezeigt wird, obwohl der richtige DVC eingegeben wurde.

- Das Gerät wird lokal von einem WLAN Controller verwaltet. Bitte setzen Sie das Gerät in den Auslieferungszustand zurück und löschen Sie die DHCP-Option **WLAN Controller** im lokalen DHCP Server.
- Die lokale Firewall hat den Port 443 für ausgehende Verbindungen gesperrt.

11.7.2 Keine Kommunikation mehr mit einem verwalteten Gerät

Das Logo, das den Zustand der Kommunikation anzeigt, ist nicht mehr grün, sondern rot.

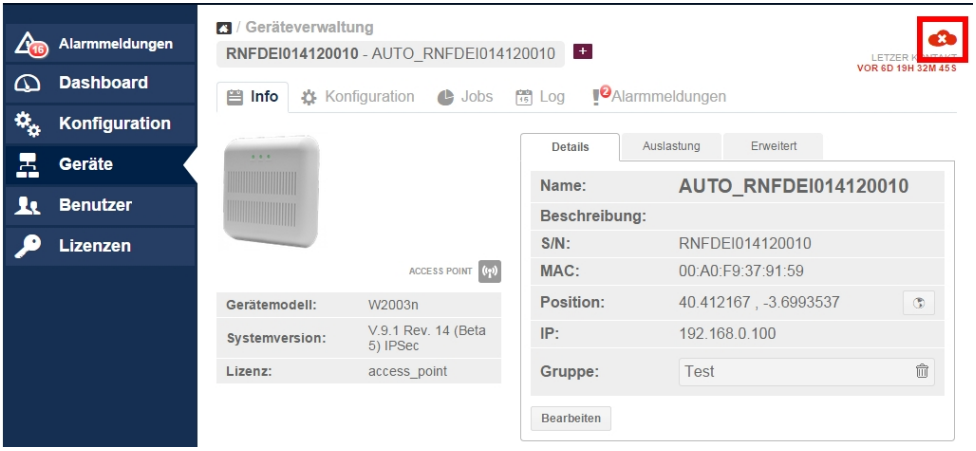


Abb. 201: Kommunikationsfehler

Zunächst sollte man sicherstellen, dass der Access Point eine Verbindung zum Internet hat. Falls die Probleme weiterbestehen, kann ein fehlerhaftes SSL-Zertifikat die Ursache sein. Dies kann verschiedene Ursachen haben, z. B. kann es auf dem Access Point gelöscht worden sein, oder das Gerät war zuvor unter einem anderen Konto angemeldet.

In diesem Fall sollte die Konfiguration des Gerätes in den Auslieferungszustand zurückgesetzt und das Sicherheitszertifikat auf dem Server für den betreffenden Access Point gelöscht werden.

Abb. 202: Kommunikationsfehler

11.7.3 Weitere Debug-Möglichkeiten

Im Menü **Geräte->Geräte verwalten** wählen Sie ein Gerät aus. Gehen Sie zu **Geräte verwalten->Konfiguration**.

Abb. 203: Kommunikationsfehler

Klicken Sie auf das kleine Logo um die Konfigurationsdatei anzeigen zu lassen.

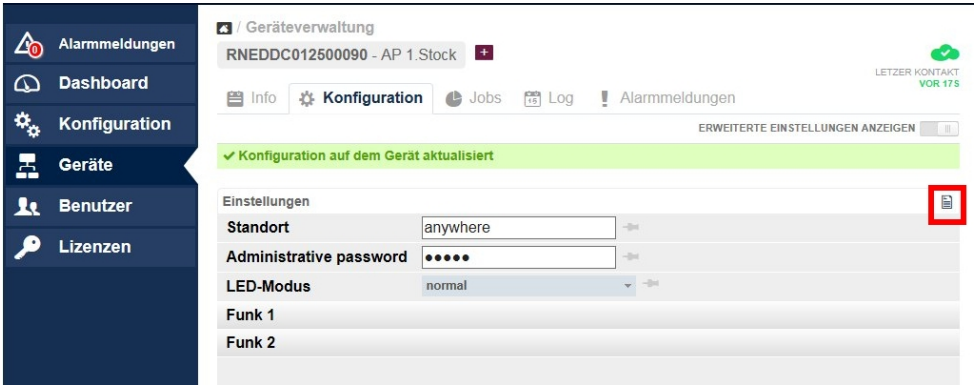


Abb. 204: Debug-Möglichkeiten

Beachten Sie, dass alle Passwörter in dieser Datei verschlüsselt angezeigt werden.

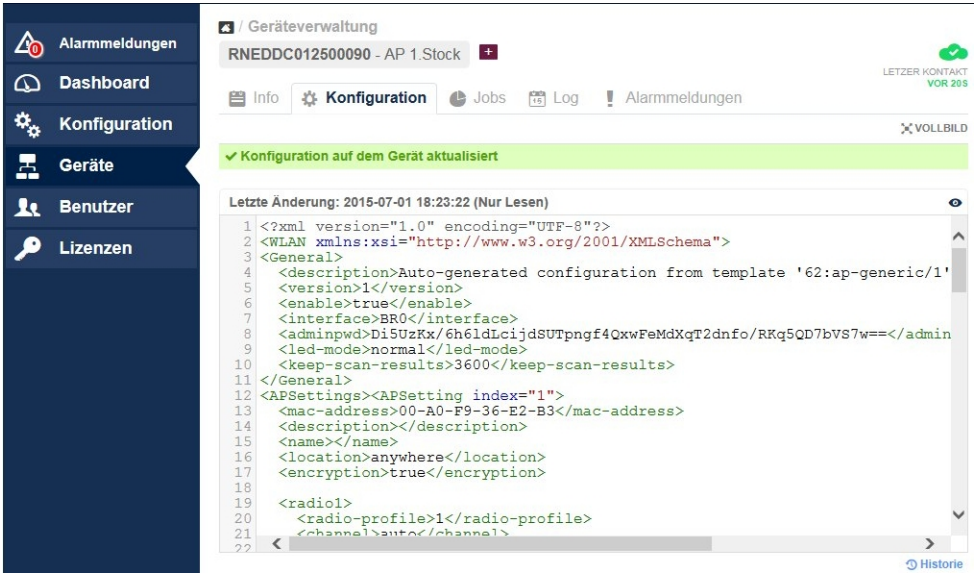


Abb. 205: Debug-Meldung

11.7.4 Debugging auf Geräteebene

Korrekte Zeitstempel

Access Points benötigen korrekte Uhrzeit, damit Performance-Werte übertragen und zugeordnet werden können. Kontrollieren Sie daher vor Beginn einer Fehlersuche, ob die Uhrzeit korrekt eingestellt ist.

Bei Verwendung eines DHCP-Servers können Sie diesen auch als Zeitserver nutzen. Wenn Sie dafür ein **bintec**-Gerät verwenden, gehen Sie in das Menü **Systemverwaltung**->**Globale Einstellungen**->**Datum und Uhrzeit** und aktivieren den Menüpunkt **System als Zeitserver**.

Wenn statische IP-Adressen verwendet werden, können Sie im selben Menü bis zu drei Zeitserver manuell eintragen.

Debugging

Falls keine Kommunikation zwischen Access Point und Cloud NetManager zustande kommt, können Sie mit Hilfe von Telnet oder SSH-Terminals die Kommunikation verfolgen. Dazu müssen Sie sich an den Access Point anmelden und den Befehl „debug tremp“ eingeben. Es wird die Kommunikation zwischen Access Point und Cloud NetManager angezeigt.

```
Welcome to W2004n version V.9.1 Rev. 14 (Beta 4) IPSec from 2015/05/27 00:00:00
systemname is w2004n, location


Login: admin
Password:

Password not changed. Call "setup" for quick configuration.

w2004n:> debug tremp
08:48:56 INFO/TREMP: -> https://discover.networkcloudmanager.com/api/task/all
08:49:01 INFO/TREMP: <- HTTP/1.1 200 OK
08:49:06 INFO/TREMP: ->
https://discover.networkcloudmanager.com/api/monitor/system/events
08:49:06 INFO/TREMP: The message has been compressed about 36%
08:49:09 INFO/TREMP: <- HTTP/1.1 200 OK
08:49:26 INFO/TREMP: -> https://discover.networkcloudmanager.com/api/task/all
08:49:29 INFO/TREMP: <- HTTP/1.1 200 OK
08:49:36 INFO/TREMP: ->
https://discover.networkcloudmanager.com/api/monitor/system/events
08:49:36 INFO/TREMP: The message has been compressed about 23%
```

Kommunikationsprobleme und Zertifikatsprobleme lassen sich auf diese Weise schnell analysieren.