



Benutzerhandbuch Workshops (Auszug)

WLAN-Workshops

Copyright© Version 08/2020 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
1.1	Einleitung	1
1.2	Konfiguration	2
1.2.1	Konfiguration der Drahtlosnetzwerke	2
1.2.2	Konfiguration der VLANs	4
1.2.3	Regeln für den Empfang an den Ports festlegen	5
1.2.4	Ports aus VLAN Management entfernen	6
1.2.5	VLAN aktivieren	8
1.2.6	Konfiguration am bintec S128p	9
1.3	Ergebnis.	11
1.4	Kontrolle.	11
1.5	Konfigurationsschritte im Überblick	12
Kapitel 2	WLAN - bintec Hotspot Solution	15
2.1	Einleitung	15
2.2	Leistungsmerkmale	17
2.2.1	Merkmale der Hotspot Solution	17
2.2.2	Merkmale des Gateways	17
2.2.3	Merkmale des Hotspot-Servers	18
2.3	Konfiguration	18
2.3.1	Konfiguration des bintec Hotspot-Gateways	18
2.3.2	Konfiguration des bintec Hotspot-Servers durch einen Fachhändler	25
2.3.3	Verwaltung von Hotspot Accounts	31
2.3.4	Betrieb an mehreren Standorten	35
2.4	Anmeldeverfahren konfigurieren	39
2.4.1	Anonym	39
2.4.2	1-Click	43

2.4.3	SMS	47
2.4.4	PayPal	52
2.4.5	Default Free Service	57
2.5	Hinweise für den sicheren Betrieb.	57
2.5.1	Mehrfaches Anmelden	57
2.5.2	Verhindern der Sichtbarkeit der Teilnehmer untereinander	57
2.5.3	Verschlüsselte / Unverschlüsselte WLAN-Verbindung	59
2.5.4	WPA-Verschlüsselung	60
2.5.5	IP/ARP Spoofing	60
2.6	Konfigurationsschritte im Überblick	60
Kapitel 3	WLAN - VoWLAN Grundlagen und Konfiguration	68
3.1	Allgemein	68
3.2	WLAN Infrastruktur	68
3.2.1	WLAN Funkausleuchtung	69
3.2.2	Handover zwischen den Access Points	70
3.2.3	Bandbreitenbedarf	70
3.2.4	Der Sicherheitsstandard und das Handover	71
3.2.5	QoS, WMM und U-APSD	72
3.2.6	WLAN Controller – Ein Muss in einem VoWLAN-Netz?	75
3.2.7	Mögliche Störquellen	75
3.3	Beispielkonfiguration	75
3.3.1	Netzwerkplan	76
3.3.2	WLAN Konfiguration mit oder ohne WLAN Controller	77
3.4	Ascom i62 Talker Konfiguration	79
3.4.1	Vorraussetzungen	79
3.4.2	Konfiguration	79
3.4.3	Testbefehle am Ascom i62.	85
3.5	Konfiguration der bintec be.IP plus	85
3.5.1	Konfiguration	85

3.5.2	Betriebsfall: WLAN-Telefon nicht erreichbar	86
3.6	Verwendung anderer WLAN-Telefone	88
3.7	Konfigurationsschritte im Überblick	88
Kapitel 4	WLAN - Management für mehrere Standorte: WLAN Controller über VPN	91
4.1	Einleitung	91
4.1.1	Voraussetzungen	92
4.1.2	Hinweise zum Test-Setup	93
4.2	Konfiguration	93
4.2.1	Voreinstellungen	93
4.2.2	Konfiguration des Routers in der Außenstelle.	94
4.2.3	Konfiguration des VPN-Konzentrators in der Zentrale	97
4.2.4	Konfiguration des WLAN-Controllers in der Zentrale.	98
4.3	Konfigurationsschritte im Überblick	109
Kapitel 5	WLAN - Wireless LAN Controller als Netzzugangsgateway	116
5.1	Einleitung	116
5.2	Konfiguration	118
5.3	Konfigurationsschritte im Überblick	147
Kapitel 6	WLAN - Netzwerk mit Gäste-WLAN	158
6.1	Einleitung	158
6.2	Konfiguration	159
6.2.1	IP-Adresse konfigurieren	159
6.2.2	Bridge-Gruppe anlegen und LAN-Schnittstelle zuweisen	160
6.2.3	Wireless LAN Controller in Betrieb nehmen	160
6.2.4	Funkmodulprofil auswählen und WLAN-Zugang zum lokalen Netz konfigurieren	161

6.2.5	Gäste-WLAN konfigurieren.	163
6.2.6	Access Points mit dem Wireless LAN Controller konfigurieren	165
6.2.7	IP-Adresse für die virtuelle Bridge-Schnittstelle konfigurieren	166
6.2.8	IP-Adressbereich für das Gästernetz einrichten	167
6.2.9	DHCP-Verwendung konfigurieren.	168
6.2.10	Firewall einrichten	170
6.3	Ergebnis.	175
6.4	Konfigurationsschritte im Überblick	175
Kapitel 7	VLAN-Einrichtung ESW4000-Switche	179
7.1	Einrichtung eines Gast-Netzwerks am Router	179
7.2	Einrichtung am Switch ESW4000	180
Kapitel 8	WLAN - WLAN-Controller-Installation mit integrierter HotSpot-Funktionalität	183
8.1	Einleitung	183
8.2	Funktion	184
8.3	Konfiguration	184
8.3.1	Basiskonfiguration	184
8.3.2	LAN-Konfiguration	185
8.3.3	HotSpot-Konfiguration	186
8.3.4	DHCP-Konfiguration	190
8.3.5	Wireless LAN Controller Wizard	193
8.4	Konfigurationsschritte im Überblick	201
Kapitel 9	WLAN - Cloud NetManager	207
9.1	Einleitung	207
9.2	Erste Schritte im Portal.	207
9.2.1	Anlegen eines Benutzers	207

9.2.2	Ändern der Zeitzone	210
9.2.3	Einspielen der Lizenzen	210
9.3	Anlegen der Profile	212
9.3.1	Anlegen der Netzwerkprofile (SSID).	212
9.3.2	Anlegen der Funkprofile	214
9.3.3	Anlegen der Gerätevorlagen / Access-Point-Vorlage	215
9.3.4	Geräte verwalten	216
9.4	Access Points registrieren und verwalten	217
9.4.1	Geräte manuell anmelden	217
9.4.2	Gerät automatisch anmelden	218
9.5	Geräteverwaltung.	219
9.5.1	Batch-Operationen und Software-Update	220
9.6	Anhang	221
9.6.1	Einrichtung eines anderen Rechenzentrums	221
9.6.2	Automatische Konfiguration	225
9.7	Fehlersuche	226
9.7.1	Ein neues Gerät ist nicht sichtbar	226
9.7.2	Keine Kommunikation mehr mit einem verwalteten Gerät	226
9.7.3	Weitere Debug-Möglichkeiten	227
9.7.4	Debugging auf Geräteebene	229
Kapitel 10	SSID - Zuweisung eines getaggten VLAN.	231
10.1	Konfiguration.	231

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.

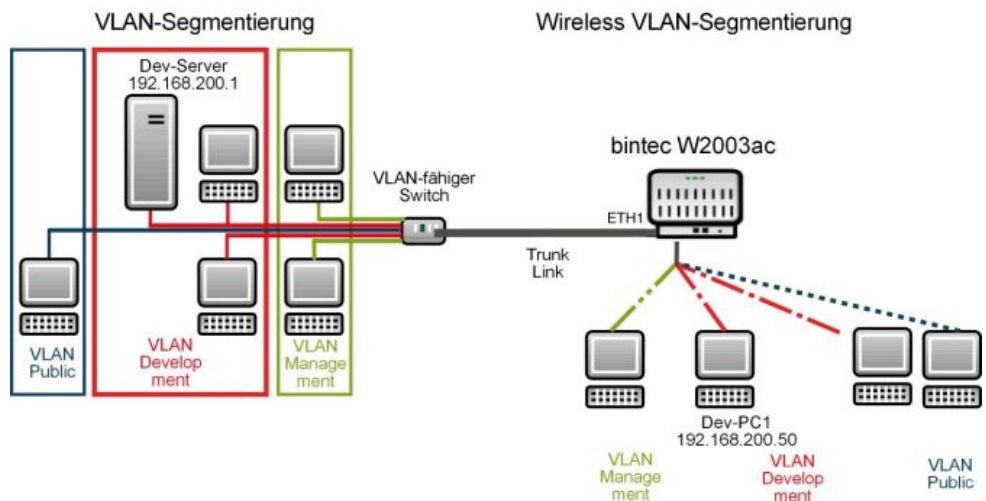


Abb. 1: VLAN-Segmentierung

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

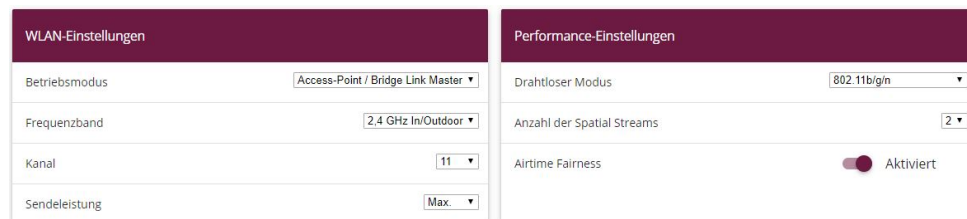
1.2.1 Konfiguration der Drahtlosnetzwerke

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.



WLAN-Einstellungen	Performance-Einstellungen
Betriebsmodus: Access-Point / Bridge Link Master	Drahtloser Modus: 802.11b/g/n
Frequenzband: 2.4 GHz In/Outdoor	Anzahl der Spatial Streams: 2
Kanal: 11	Airtime Fairness: <input checked="" type="checkbox"/> Aktiviert
Sendeleistung: Max.	

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. *Schlüssel-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)**.

VSS-	Beschreibung	Netzwerkname (SSID)	MAC-Adresse	Sicherheit	Status	Aktion
vss7-10		Management	Elmegt_6f:5e:85	WPA-PSK	aktiviert	⌵ ⌵ ⌵ ⌵

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 \wedge -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**.

VLAN konfigurieren

VLAN Identifier
2

VLAN-Name
Development

VLAN-Mitglieder

Schnittstelle	Ausgehende Regel	Löschen
vss2-1 ▼	Untagged ▼	
en1-0 ▼	Tagged ▼	

HINZUFÜGEN

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**.

Portkonfiguration			
Schnittstelle	PVID	Frames ohne Tag verwerfen	Nicht-Mitglieder verwerfen
en1-0	1 - Management ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>
en1-1	1 - Management ▼	<input type="checkbox"/>	<input checked="" type="checkbox"/>
vss2-0	1 - Management ▼	<input type="checkbox"/>	<input type="checkbox"/>
vss2-1	2 - Development ▼	<input type="checkbox"/>	<input type="checkbox"/>
vss2-2	3 - Public ▼	<input type="checkbox"/>	<input type="checkbox"/>

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> ->**  .

VLAN konfigurieren

VLAN Identifier 1

VLAN-Name
Management

VLAN-Mitglieder






Schnittstelle	Ausgehende Regel	Löschen
en1-0 ▼	Untagged ▼	
en1-1 ▼	Untagged ▼	
vss2-0 ▼	Untagged ▼	

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.




VLANs			
VLAN Identifier	VLAN-Name	VLAN-Mitglieder	
1	Management	en1-0	
		en1-1	
		vss2-0	
2	Development	vss2-1	
		en1-0	
3	Public	vss2-2	
		en1-0	

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**.

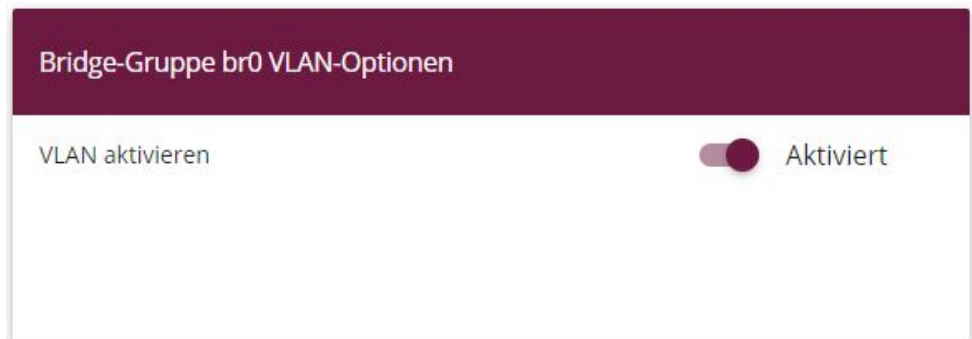


Abb. 9: LAN -> VLAN -> Verwaltung

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) Pakete verarbeitet werden. In Richtung Server soll das Tagging entfernt werden, da die Server die Pakete 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**.

VLAN Configuration

VLAN Operation Mode : 802.1Q

Enable GVRP Protocol

Management Vlan ID : 1

Apply

802.1Q Configuration Group Configuration

Port	Link Type	Untagged Vid	Tagged Vid
Port.01	Access Link	1	
Port.02	Access Link	1	
Port.03	Access Link	1	
Port.04	Access Link	1	
Port.05	Access Link	1	
Port.06	Access Link	1	
Port.07	Access Link	1	
Port.08	Access Link	1	
G1	Access Link	1	
G2	Access Link	1	

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:

VLAN Configuration

VLAN Operation Mode : 802.1Q

Enable GVRP Protocol

Management Vlan ID : 1

Apply

802.1Q Configuration Group Configuration

Port	Link Type	Untagged Vid	Tagged Vid
Port.01	Access Link	1	
Port.02	Access Link	102	
Port.03	Access Link	103	
Port.04	Access Link	1	
Port.05	Access Link	1	
Port.06	Access Link	1	
Port.07	Access Link	1	
Port.08	Trunk Link	1	1,102,103
G1	Access Link	1	
G2	Access Link	1	

Apply

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<ms> TTL=30
Antwort von 192.168.100.30: Bytes=32 Zeit<ms> TTL=30
Antwort von 192.168.100.30: Bytes=32 Zeit<ms> TTL=30
Antwort von 192.168.100.30: Bytes=32 Zeit<ms> 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<ms> TTL=63
Antwort von 192.168.200.1: Bytes=32 Zeit<ms> TTL=63
Antwort von 192.168.200.1: Bytes=32 Zeit<ms> TTL=63
Antwort von 192.168.200.1: Bytes=32 Zeit<ms> 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. Schlüssel-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. Schlüssel-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. <i>Schluessel-Alle</i>
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. <i>Development</i>
VLAN-Mitglieder	LAN -> VLAN -> VLANs -> Neu	mit Hinzufügen z. B. <i>vss2-1</i>
Ausgehende Regel	LAN -> VLAN -> VLANs -> Neu	<i>Untagged</i> für <i>vss2-1</i>
VLAN-Mitglieder	LAN -> VLAN -> VLANs -> Neu	mit Hinzufügen z. B. <i>en1-0</i>
Ausgehende Regel	LAN -> VLAN -> VLANs -> Neu	<i>Tagged</i> für <i>en1-0</i>
VLAN Identifier	LAN -> VLAN -> VLANs -> Neu	z. B. 3
VLAN-Name	LAN -> VLAN -> VLANs -> Neu	z. B. <i>Public</i>
VLAN-Mitglieder	LAN -> VLAN -> VLANs -> Neu	mit Hinzufügen z. B. <i>vss2-2</i>
Ausgehende Regel	LAN -> VLAN -> VLANs -> Neu	<i>Untagged</i> für <i>vss2-2</i>
VLAN-Mitglieder	LAN -> VLAN -> VLANs -> Neu	mit Hinzufügen z. B. <i>en1-0</i>
Ausgehende Regel	LAN -> VLAN -> VLANs -> Neu	<i>Tagged</i> für <i>en1-0</i>

Port VLAN Identifier (PVID) festlegen

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

Ports aus VLAN Management entfernen

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

VLANs aktivieren

Feld	Menü	Wert
VLAN aktivieren	LAN -> VLAN -> Verwaltung	<i>Aktiviert</i>

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 Cafés, 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.

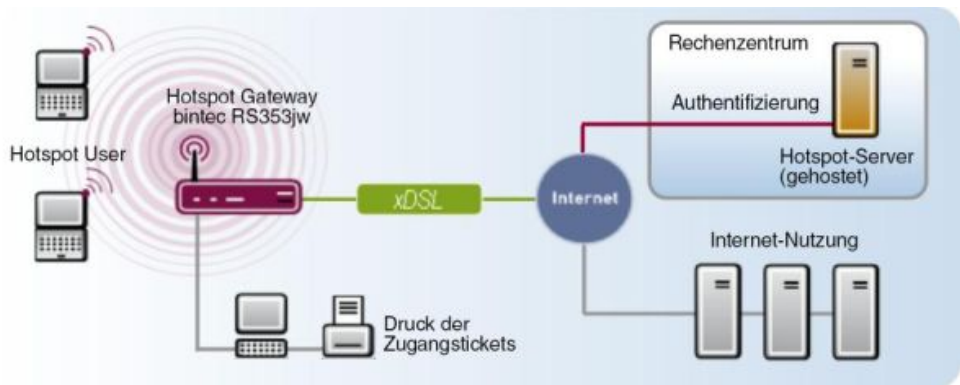


Abb. 12: Funktionsweise

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 Inaktivität 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**.

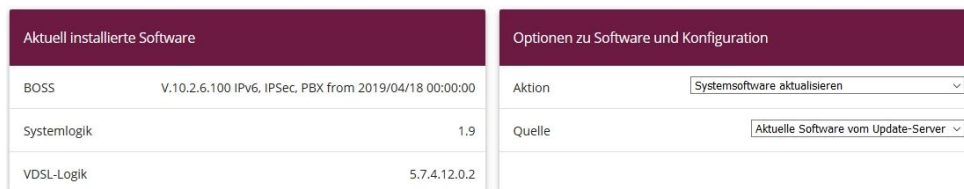


Abb. 13: **Wartung** -> **Software & Konfiguration** -> **Optionen**

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.

Basisparameter

Schnittstelle BRIDGE_BR0 -1

Domäne am Hotspot-Server

Walled Garden Deaktiviert

Aufzurufende Seite nach Login

Sprache für Anmeldefenster Deutsch

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**.

Grundeinstellungen		Manuelle Zeiteinstellung			
Zeitzone	Europe/Berlin	Datum einstellen	Tag	Monat	Jahr
Aktuelle Ortszeit	Dienstag, 18 Jun 2019, 08:49:40				
		Zeit einstellen	Stunde	Minute	
Automatische Zeiteinstellung (Zeitprotokoll)					
ISDN-Zeitserver	<input type="checkbox"/>				
Erster Zeitserver		SNTP			
Zweiter Zeitserver		SNTP			
Dritter Zeitserver		SNTP			
Zeitaktualisierungsintervall	1440	Minute(n)			
Zeitaktualisierungsrichtlinie	Normal				
System als Zeitserver	<input type="checkbox"/>				

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:

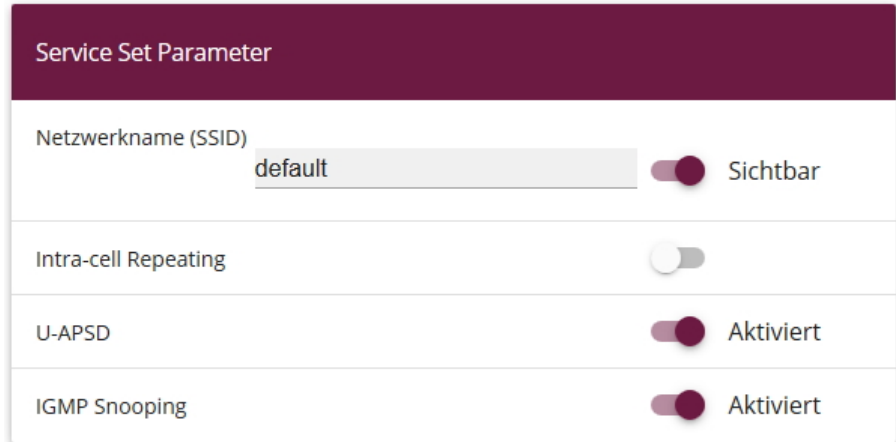
- (1) Wählen Sie im Feld **Zeitzone** *Europe/Berlin* aus. Um eine synchrone Systemzeit zu garantieren, ist eine aktuelle Systemzeit für den Betrieb notwendig.
- (2) Deaktivieren Sie **ISDN-Zeitserver**.
- (3) Deaktivieren Sie **System als Zeitserver**. Zeitanfragen eines Clients werden nicht beantwortet.
- (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)** -> 



Service Set Parameter		
Netzwerkname (SSID)	default	<input checked="" type="checkbox"/> Sichtbar
Intra-cell Repeating		<input type="checkbox"/>
U-APSD		<input checked="" type="checkbox"/> Aktiviert
IGMP Snooping		<input checked="" type="checkbox"/> Aktiviert

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)** -> 

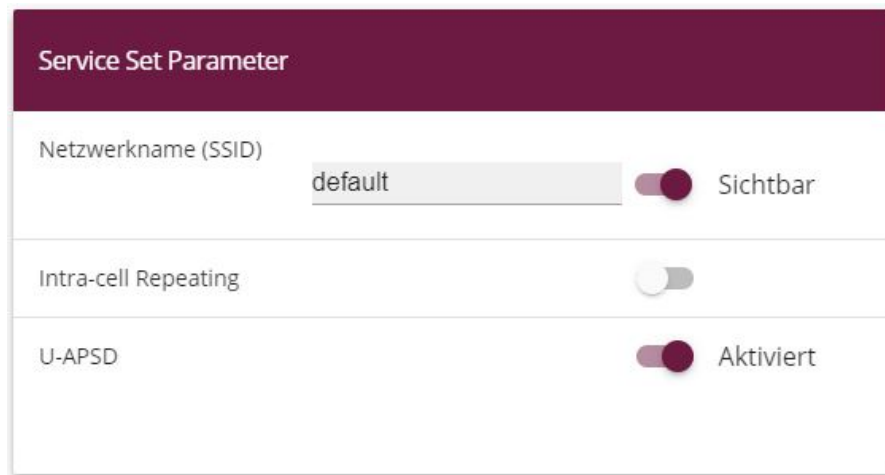



Abb. 17: **Wireless LAN -> WLAN -> Drahtlosnetzwerke (VSS) ->** 

- (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 RADIUS-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**.

Basisparameter	
Authentifizierungstyp	Accounting ▼
Betreibermodus	bintec HotSpot Server ▼
Server-IP-Adresse	62.245.165.180
RADIUS-Passwort
Standard-Benutzerpasswort
Priorität	2 ▼
Eintrag aktiv	<input checked="" type="checkbox"/> Aktiviert
Gruppenbeschreibung	Standardgruppe 0 ▼

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

Erweiterte Einstellungen

Server-Optionen

Richtlinie	Nicht verbindlich ▾
UDP-Port	1813
Server Timeout	3000 Millisekunden
Erreichbarkeitsprüfung	<input checked="" type="checkbox"/> Aktiviert
Wiederholungen	3

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.



The image shows a login interface with a light blue background. At the top left, the word "Login" is written in a white sans-serif font. Below this, there are two input fields: the first is labeled "Benutzername:" and the second is labeled "Passwort:". Both fields are empty and have a white background with a thin grey border. At the bottom left of the form, there is a yellow button with the word "Login" written in black text.

Abb. 20: Login

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

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

Mandant bearbeiten	
Allgemein	
Kennung	Roadshow
Straße	Südwestpark 94
PLZ	90449
Ort	Nürnberg
Land	DE
Ansprechpartner	
Vorname	
Nachname	
Telefon	
Telefax	
E-Mail	
Sprache	Englisch
Zugangskennungen	
Domäne	
Zusatztext	
Zusatztext Englisch	
Rechnungsabschnitt	<input type="checkbox"/> anzeigen
Passwörter	<input checked="" type="radio"/> nur Ziffern <input type="radio"/> nur Zeichen <input type="radio"/> alphanumerisch <input type="radio"/> sichere Passwörter
Passwort-Länge	9 <input type="text"/>
General-Passwort für Voucher	-----
Logo (maximal 5 MB, nur jpeg oder png)	<input type="button" value="Durchsuchen..."/> Keine Datei ausgewählt.
AGB	<input type="button" value="Aktuelle Datei"/> <input type="checkbox"/> Löschen <input type="button" value="Durchsuchen..."/> Keine Datei ausgewählt. <input type="button" value="Aktuelle Datei"/> <input type="checkbox"/> Löschen

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**.

Neuer Benutzer		» Benutzer Übersicht <
Zugangskennungen		
* Benutzername	<input type="text" value="Hotel_Rezeption"/>	
Passwort	<input type="password"/>	
Passwort wiederholen	<input type="password"/>	
Berechtigungsgruppe	(wird automatisch generiert, falls nicht angegeben)	
	Mitarbeiter	▼
Standort	Alle	▼
Benutzerdaten		
Vorname	<input type="text"/>	
* Nachname	<input type="text" value="Rezeption"/>	
Telefon	<input type="text"/>	
Telefax	<input type="text"/>	
* E-Mail	<input type="text" value="test@test.de"/>	
Sprache	<input type="radio"/> Englisch <input checked="" type="radio"/> Deutsch <input type="radio"/> Spanisch <input type="radio"/> Französisch <input type="radio"/> Italienisch <input type="radio"/> Portugiesisch <input type="radio"/> Niederländisch	
	<input type="button" value="speichern"/>	<input type="button" value="abbrechen"/>
	* wird benötigt	
		» Benutzer Übersicht <

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 angegebene 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 gestellte 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)**.

Neuer Account (einfach) > Account - Suche < > Neuer Account (erweitert) < > Hilfe <

* Benutzername Gast_25

* Tarif 2h Ticket ▼

* Nachname Lüdenscheid

Zugangsdaten

herunterladen

speichern abbrechen

* wird benötigt

> Account - Suche < > Neuer Account (erweitert) < > Hilfe <

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)**.

Neuer Account (erweitert) > Account - Suche < > Neuer Account (einfach) < > Hilfe <

Zugangskennungen

*** Benutzername**
Passwort
Passwort wiederholen

(wird automatisch generiert, falls nicht angegeben)

*** Tarif**
gueltig ab
gültig bis
*** Standort**

Bintec-Elmeg-Support / Nr. 1
 Roadshow
 SE-Test
 Support NCR
 WBT

Gruppe

verfügbar

Famillienticket
Test-dauer
test1

Gruppenmitglied

SSID

Vorlage diesen Account als Vorlage verwenden

Personendaten

Anrede
Vorname
*** Nachname**
Zimmer
Zusatz
E-Mail
Telefon

Zugangsdaten

auf Englisch
 herunterladen
 per SMS senden

* wird benötigt

> Account - Suche < > Neuer Account (einfach) < > Hilfe <

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 **Account** 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<** .

Account - Suche > Neuer Account (erweitert) < > Neuer Account (einfach) < > Hilfe <

Account Status

Benutzername

Nachname

Tarif

Gruppe

Online

Benutzername	Standort	Name	Tarif	Betrag	Restzeit	Restvolumen	Online	
✓ 10min-1	SE-Test	10min-1	10MB/10Min	bezahlt	00:10:00	10 MB	Nein	
✓ se-team	SE-Test	SE-Team	unbegrenzt	0,00 €	---:--:--	--	Nein	

> Neuer Account (erweitert) < > Neuer Account (einfach) < > 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.

Standort Übersicht					> Upload Manager <	> Hilfe <
Standort	Ort	Lizenz	gültig bis	Host		
✓ Bintec-Elmeg-Support / Nr. 1	Nürnberg	DEMO20420150107	2020-01-07			Übersicht
✓ Roadshow	Nürnberg	DEMO57020141107	2020-11-07			Übersicht
✓ SE-Test	DEU	DEMO57220151209	2020-12-09			Übersicht
✓ Support NCR	DEU	DEMO20520141021	2020-10-21			Übersicht
✓ WBT	Nürnberg	Es ist keine Lizenznummer hinterlegt.				Übersicht

Abb. 27: Standort -> Übersicht

Upload Manager

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

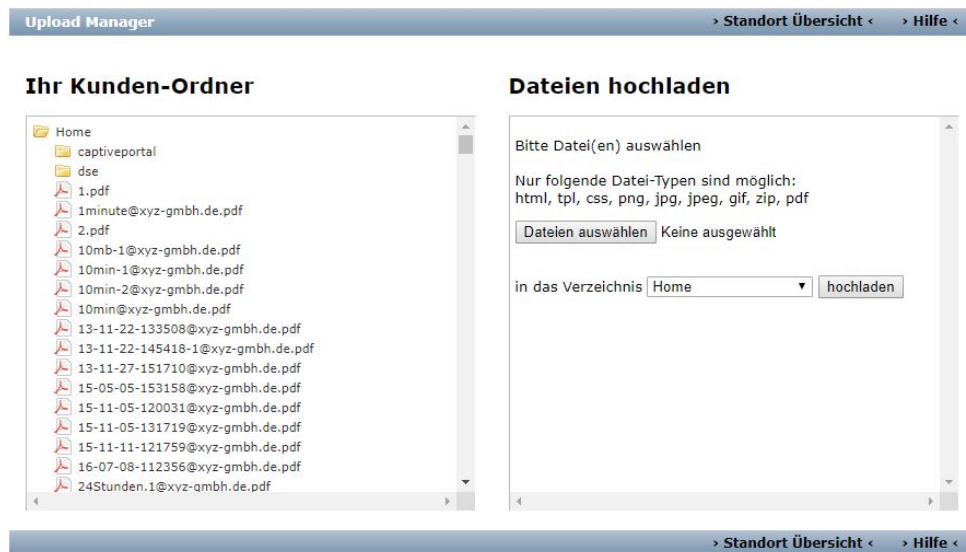


Abb. 28: Upload Manager

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.

Standort bearbeiten > Host Übersicht < > Upload Manager < > Hilfe <

Allgemein

Kennung Support NCR

Straße

PLZ

Ort DEU

Land Deutschland

Bemerkung

Ansprechpartner

Vorname [blurred]

Nachname [blurred]

Telefon

Telefax

E-Mail [blurred]

Walled Garden (http://Hotspot-Station-Management.com/1/100/)

Anmeldemethode Default Free Service ▾

Tarif 24-Stunden ▾

Tickets müssen manuell freigeschaltet werden.

Passwort Automatisch generieren und anzeigen ▾

Lizenz

Lizenznummer DEMO20520110629

gültig bis 2011-06-29

Abb. 29: Standort bearbeiten

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

(1) Gehen Sie zu **Host Übersicht**.

Host Übersicht > Neuer Host < > Standort Übersicht <

Host	NAS-Identifizier
nureintest	nureintest

> Neuer Host < > Standort Übersicht <

Abb. 30: Host Übersicht

Hier wird der **NAS-Identifizier** 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-Identifizier definiert und im Gateway eingetragen ist.

Sollte kein **NAS-Identifizier** 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* auswählen, ist der Account für alle Standorte gültig.

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

Neuer Gutschein > Gutschein - Suche <

* **Anzahl** 100

Benutzername

- Fortlaufend (370:1, 370:2)
- Numerisch (4798811)
- Alphanumerisch klein (a7z89vk)
- Alphanumerisch (A7z89vK)

Präfix Benutzername

Passwort

Passwort wiederholen

(wird automatisch generiert, falls nicht angegeben)

* **Tarif** 2h Ticket ▼

gueltig ab ----- ▼ ----- ▼ ----- ▼

gültig bis 23 ▼ Juni ▼ 2020 ▼

Beschreibung

* **Standort**

verfügbar

- Bintec-Elmeg-Support ▲
- Roadshow
- SE-Test
- Support NCR
- WBT ▼

>> <<

ausgewählt

- Alle ▲

speichern abbrechen

* wird benötigt

> Gutschein - Suche <

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) Wählen 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 Authentifizierungsmethode 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.

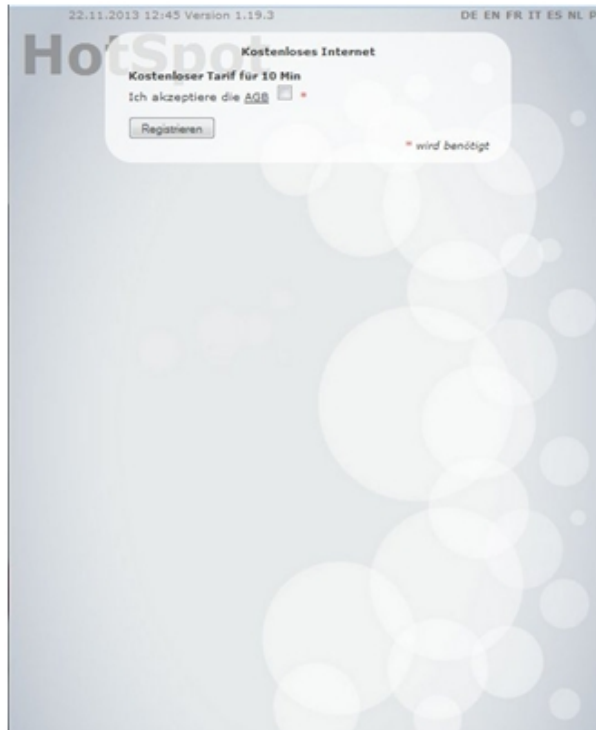


Abb. 32: Anonyme Anmeldung

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>**.

Walled Garden (https://hotspot.bintec-elmeg.com/3/572/)	
Anmeldemethode	Anonym ▼
Tarif	5 Tage ▼
Neuregistrierung verhindern	<input type="text"/> Minuten ▼
Gültigkeitsdauer Account	365 Tage ab erstem Login ▼
Router-Typ	bintec > 9.1.4 ▼
Anmeldeseite des Routers	<input type="text" value="http://192.168.1.254/auth"/>
Tickets	<input type="checkbox"/> müssen manuell freigeschaltet werden.
Passwort	Automatisch generieren und anzeigen ▼
Layout	Standard grau ▼
Token-basierte Anmeldung	nur nach Akzeptieren der AGBs ▼

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

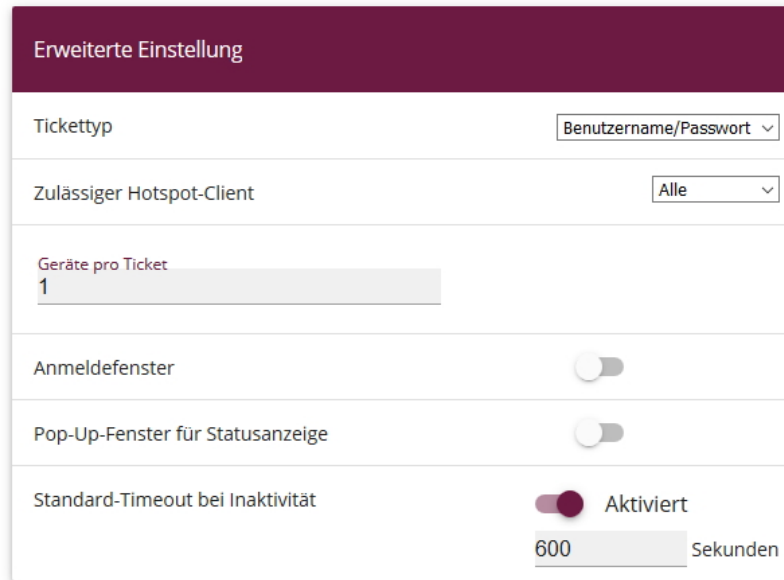
Starten Sie eine Web-Verbindung zum bintec-Gateway (z. B. **bintec RS353xx**).

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

Basisparameter

Schnittstelle	BRIDGE_BR0 -1
Domäne am Hotspot-Server	
Walled Garden	<input checked="" type="checkbox"/> Aktiviert
Walled Network / Netzmaske	<input type="checkbox"/> Deaktiviert
Walled Garden URL	https://hotspot.bintec-elmeg.com/3/205
Geschäftsbedingungen	http://www.bintec-elmeg.com
Zusätzliche, frei zugängliche Domännennamen	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Domänenname / IP-Adresse</div> <p>HINZUFÜGEN</p>
Aufzurufende Seite nach Login	
Sprache für Anmeldefenster	Deutsch ▼

Erweiterte Einstellungen



Erweiterte Einstellung	
Tickettyp	Benutzername/Passwort ▾
Zulässiger Hotspot-Client	Alle ▾
Geräte pro Ticket	1
Anmeldefenster	<input type="checkbox"/>
Pop-Up-Fenster für Statusanzeige	<input type="checkbox"/>
Standard-Timeout bei Inaktivität	<input checked="" type="checkbox"/> Aktiviert 600 Sekunden

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 Anmelde-seite 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.

27.11.2013 14:51 Version 1.19.3
DE EN FR IT ES NL PT

HotSpot

Anmelden

Benutzername *

Passwort *

Ich akzeptiere die AGB *

Anmelden * wird benötigt

Kostenloses Internet

Kostenloser Tarif für 10 Min
Bitte registrieren Sie sich mit Ihrer eMail Adresse.

E-Mail *

Ich akzeptiere die AGB *

Registrieren * wird benötigt

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>**.

Walled Garden (https://hotspot.bintec-elmeg.com/3/572/)	
Anmeldemethode	1-Click ▼
Tarif	5 Tage ▼
Neuregistrierung verhindern	<input type="text"/> Minuten ▼
Gültigkeitsdauer Account	365 Tage ab erstem Login ▼
Router-Typ	bintec > 9.1.4 ▼
Anmeldeseite des Routers	<input type="text" value="http://192.168.1.254/auth"/>
Autologin	<input type="checkbox"/>
Tickets	<input type="checkbox"/> müssen manuell freigeschaltet werden.
Passwort	Automatisch generieren und anzeigen ▼
Layout	Standard grau ▼
Token-basierte Anmeldung	nur nach Akzeptieren der AGBs ▼

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	<input checked="" type="checkbox"/> Aktiviert
Walled Network / Netzmaske	<input type="checkbox"/> Deaktiviert
Walled Garden URL	https://hotspot.bintec-elmeg.com/3/205
Geschäftsbedingungen	http://www.bintec-elmeg.com
Zusätzliche, frei zugängliche Domännennamen	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Domänenname / IP-Adresse</div> <p>HINZUFÜGEN</p>
Aufzurufende Seite nach Login	
Sprache für Anmeldefenster	Deutsch ▼

Erweiterte Einstellungen

Erweiterte Einstellung	
Tickettyp	Benutzername/Passwort ▾
Zulässiger Hotspot-Client	Alle ▾
Geräte pro Ticket	1
Anmeldefenster	<input type="checkbox"/>
Pop-Up-Fenster für Statusanzeige	<input type="checkbox"/>
Standard-Timeout bei Inaktivität	<input checked="" type="checkbox"/> Aktiviert 600 Sekunden

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.

22.11.2013 13:32 Version 1.19.3
DE EN FR IT ES NL PT

HotSpot

Anmelden

Benutzername *

Passwort *

Ich akzeptiere die [AGB](#) *

* wird benötigt

Kostenloses Internet - Zugangsdaten per SMS

Kostenloser Tarif für 10 Min
Wenn Sie hier Ihre Handynummer eingeben, werden Ihnen Ihre Zugangsdaten per SMS zugesandt.

Telefon

Ich akzeptiere die [AGB](#) *

* wird benötigt

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>** .

SMS Zugangsdaten (optional)	
SMS Anbieter	lox24 ▾
Account ID	<input type="text"/>
Passwort	<input type="password"/>
API/Service-ID Economy	<input type="text"/>
API/Service-ID Pro	<input type="text"/>
API/Service-ID Direct	<input type="text"/>
Versandroute Deutschland	Economy ▾
Versandroute weltweit	Economy ▾
	<input type="button" value="speichern"/> <input type="button" value="abbrechen"/>

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>.

Walled Garden (https://hotspot.bintec-elmeg.com/3/572/)	
Anmeldemethode	SMS ▼
Tarif	5 Tage ▼
SMS-Vorschau	DE EN FR IT ES NL PT
Neuregistrierung verhindern	<input type="text"/> Minuten ▼
Gültigkeitsdauer Account	365 Tage ab erstem Login ▼
Router-Typ	bintec > 9.1.4 ▼
Anmeldeseite des Routers	<input type="text" value="http://192.168.1.254/auth"/>
Tickets	<input type="checkbox"/> müssen manuell freigeschaltet werden.
Passwort	Automatisch generieren und anzeigen ▼
Layout	Standard grau ▼
Token-basierte Anmeldung	nur nach Akzeptieren der AGBs ▼

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	<input checked="" type="checkbox"/> Aktiviert
Walled Network / Netzmaske	<input type="checkbox"/> Deaktiviert
Walled Garden URL	https://hotspot.bintec-elmeg.com/3/205
Geschäftsbedingungen	http://www.bintec-elmeg.com
Zusätzliche, frei zugängliche Domännennamen	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Domänenname / IP-Adresse</div> <p>HINZUFÜGEN</p>
Aufzurufende Seite nach Login	
Sprache für Anmeldefenster	Deutsch ▼

Erweiterte Einstellungen

Erweiterte Einstellung	
Tickettyp	Benutzername/Passwort ▾
Zulässiger Hotspot-Client	Alle ▾
Geräte pro Ticket	1
Anmeldefenster	<input type="checkbox"/>
Pop-Up-Fenster für Statusanzeige	<input type="checkbox"/>
Standard-Timeout bei Inaktivität	<input checked="" type="checkbox"/> Aktiviert 600 Sekunden

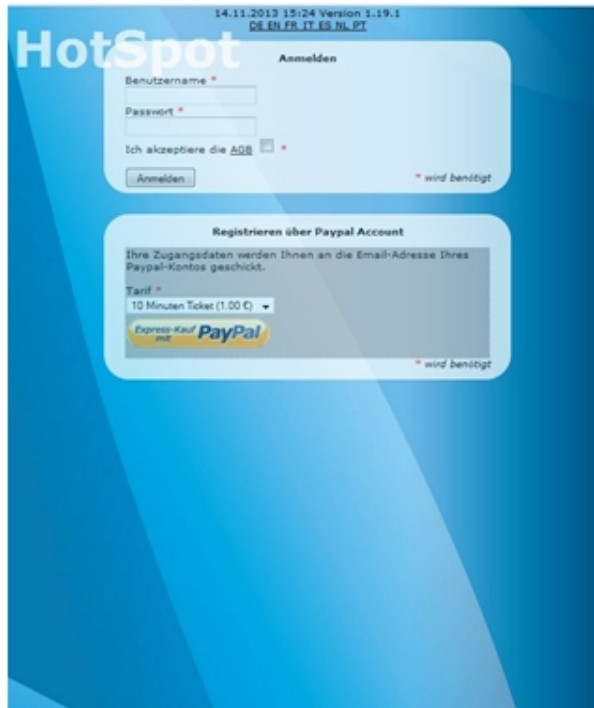
Abb. 44: Lokale Dienste -> Hotspot-Gateway -> Hotspot-Gateway -> BRIDGE_BR0-1 ✎

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 Anmelde-seite 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.



The screenshot shows a web interface for a HotSpot. At the top, it displays the date and time '14.11.2013 15:24' and the version 'Version 3.19.1'. Below this are language selection links: 'DE EN FR IT ES NL PT'. The main heading is 'HotSpot'. The 'Anmelden' (Login) section contains fields for 'Benutzername' (Username) and 'Passwort' (Password), a checkbox for 'Ich akzeptiere die AOB' (I accept the terms of use), and an 'Anmelden' button. A note '* wird benötigt' (required) is present. The 'Registrieren über Paypal Account' (Register via PayPal account) section includes a message: 'Ihre Zugangsdaten werden Ihnen an die Email-Adresse Ihres Paypal-Kontos geschickt.' (Your login data will be sent to the email address of your PayPal account). It features a 'Tarif' (Rate) dropdown menu currently set to '10 Minuten Ticket (1.00 €)' and a prominent 'Express-Kauf PayPal' button. A note '* wird benötigt' is also present here.

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>**.

PayPal Anmeldeinformationen (optional)	
API-Benutzername	<input type="text"/>
API-Passwort	<input type="password"/>
API-Passwort wiederholen	<input type="password"/>
Signatur	<input type="text"/>

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>.

Walled Garden (https://hotspot.bintec-elmeg.com/3/572/)	
Anmeldemethode	<input type="text" value="Paid Service"/>
Tarif	<input type="text" value="Alle"/>
Neuregistrierung verhindern	<input type="text"/> <input type="text" value="Minuten"/>
Gültigkeitsdauer Account	<input type="text" value="365"/> <input type="text" value="Tage ab erstem Login"/>
Router-Typ	<input type="text" value="bintec > 9.1.4"/>
Anmeldeseite des Routers	<input type="text" value="http://192.168.1.254/auth"/>
Tickets	<input type="checkbox"/> müssen manuell freigeschaltet werden.
Passwort	<input type="text" value="Automatisch generieren und anzeigen"/>
Layout	<input type="text" value="Standard grau"/>
Token-basierte Anmeldung	<input type="text" value="nur nach Akzeptieren der AGBs"/>


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** .

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 Domännennamen

Domänenname / IP-Adresse	
www.paypal.com	
api.paypal.com	
api-aa-3t.paypal.com	
notify.paypal.com	
www.paypalobjects.com	

HINZUFÜGEN

Aufzurufende Seite nach Login

Sprache für Anmeldefenster Deutsch ▼

Erweiterte Einstellungen

Erweiterte Einstellung

Tickettyp	Benutzername/Passwort ▾
Zulässiger Hotspot-Client	Alle ▾
Geräte pro Ticket	<input style="width: 100%;" type="text" value="1"/>
Anmeldefenster	<input type="checkbox"/>
Pop-Up-Fenster für Statusanzeige	<input type="checkbox"/>
Standard-Timeout bei Inaktivität	<input checked="" type="checkbox"/> Aktiviert <input style="width: 50px;" type="text" value="600"/> Sekunden

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 Anmelde-seite 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 Menü **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. Kabelgebundenes LAN wird nicht verwendet. Der Internetzugang erfolgt über ein lokales Netzwerk oder über ADSL.

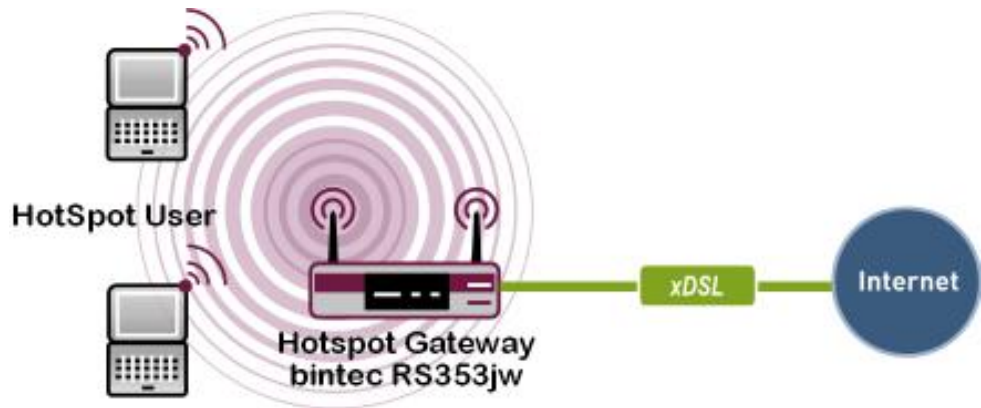



Abb. 50: Hotspot mit einem WLAN Access Point

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.

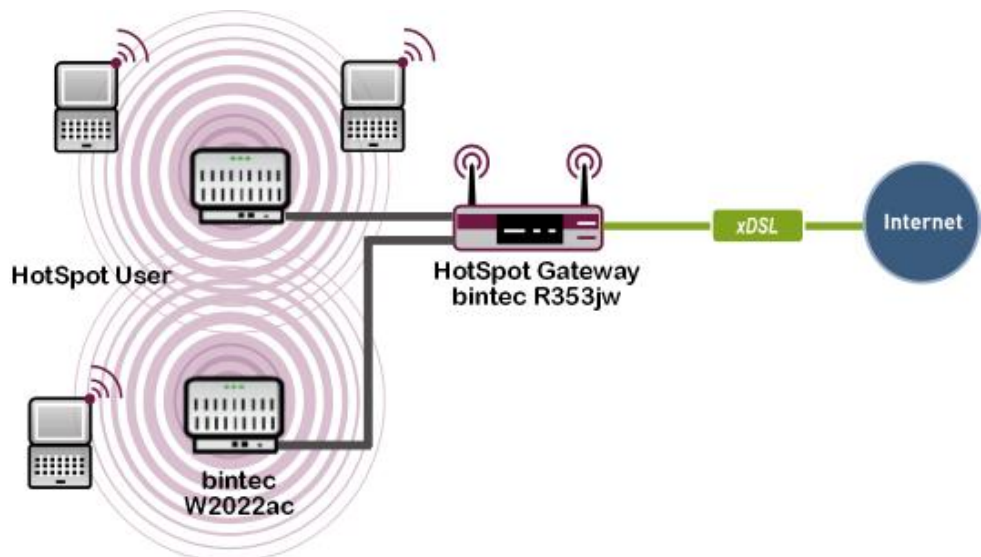



Abb. 51: Hotspot mit mehreren WLAN Access Points

Um die Sichtbarkeit zwischen den einzelnen Hotspot-Benutzern zu verhindern, muss an allen WLAN-Arbeitsplätzen im Menü **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.

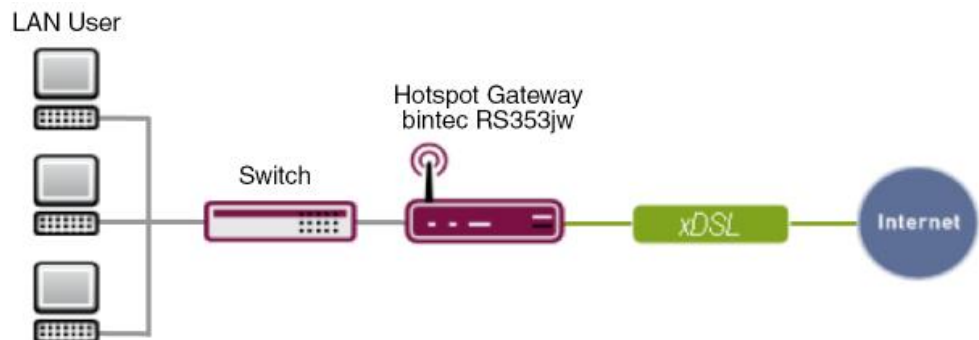


Abb. 52: Hotspot mit Ethernet-LAN-Client

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.
- Anmeldeinformationen 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	<i>Accounting</i>
Betreibermodus	Systemverwaltung -> Remote Authentifizierung -> RADIUS-> Neu	<i>bintec HotSpot Server</i>
Server-IP-Adresse	Systemverwaltung -> Remote Authentifizierung -> RADIUS-> Neu	z. B. <i>62.245.165.180</i>
RADIUS-Passwort	Systemverwaltung -> Remote Authentifizierung -> RADIUS-> Neu	<i>funkwerk-ec</i>
Priorität	Systemverwaltung -> Remote Authentifizierung -> RADIUS-> Neu	<i>2</i>
Richtlinie	Systemverwaltung -> Remote Authentifizierung -> RADIUS-> Neu->Erweiterte Einstellungen	<i>Nicht verbindlich</i>
Server Timeout	Systemverwaltung -> Remote Authentifizierung -> RADIUS-> Neu->Erweiterte Einstellungen	<i>3000</i>
Wiederholungen	Systemverwaltung -> Remote Authentifizierung -> RADIUS-> Neu->Erweiterte Einstellungen	<i>3</i>

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	<i>gesamt</i>
Preis	Tarif -> Neuer Tarif	z. B. <i>1,00</i> Euro
Standort	Tarif -> Neuer Tarif	<i>Alle</i>

Account erzeugen (einfach)

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

Account erzeugen (erweitert)

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

Account verwalten

Feld	Menü	Wert
Betrag	Account -> Übersicht	<i>Betrag</i> anklicken






Upload Manager verwenden

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

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. http://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>	xxxxxxxxxxxxxxxxxxxx
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. <i>http://hotspot.bintec-elmeg.com/3/205</i>
Geschäftsbedingungen	Lokale Dienste -> Hotspot-Gateway -> Hotspot-Gateway -> BRIDGE_BR0-1 -> 	z. B. <i>http://www.bintec-elmeg.com</i>
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>	xxxxxxxxxxxxxxxxxxxx
API-Passwort	Mandant -> <Mandant bearbeiten>	z. B. <i>supersecret</i>
API-Passwort wiederholen	Mandant -> <Mandant bearbeiten>	z. B. <i>supersecret</i>
Signatur	Mandant -> <Mandant bearbeiten>	xxxxxxxxxxxxxxxxxxxx
Anmeldemethode	Standort -> <Standort bearbeiten>	<i>Paid Service</i>
Tarif	Standort -> <Standort bearbeiten>	z. B. <i>Alle</i>
Anmeldeseite des Routers	Standort -> <Standort bearbeiten>	z. B. <i>http://192.168.1.254/auth</i>
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. <i>http://hotspot.bintec-elmeg.com/3/205</i>
Geschäftsbedingungen	Lokale Dienste -> Hotspot-Gateway -> Hotspot-Gateway ->	z. B. <i>http://www.bintec-</i>

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

Kapitel 3 WLAN - VoWLAN Grundlagen und Konfiguration

3.1 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 merkbare 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.

3.2 WLAN Infrastruktur

3.2.1 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.

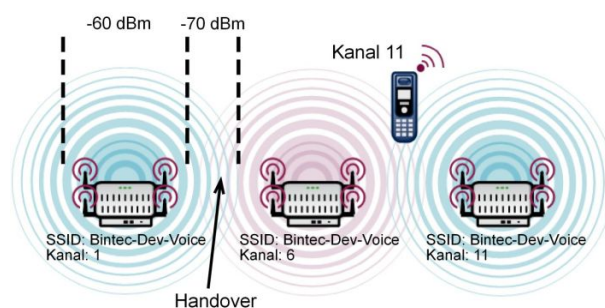


Abb. 53: Darstellung der Mindestanforderungen an die WLAN-Ausleuchtung für VoWLAN

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.

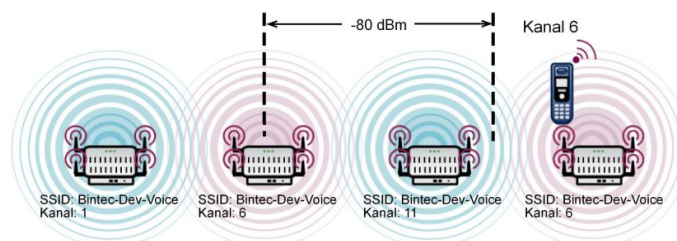


Abb. 54: Mindestabstand zweier WLAN Access Points auf dem gleichen Sendekanal

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.

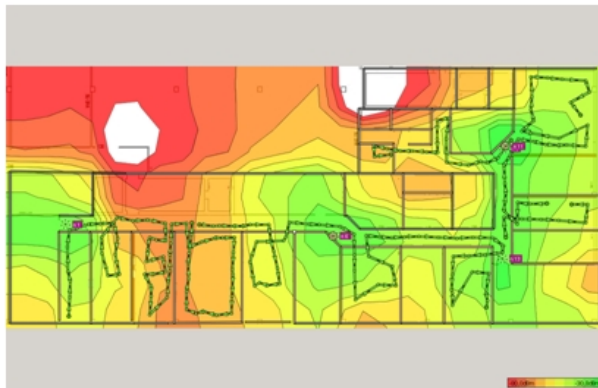


Abb. 55: Typisches Ergebnis eines Site Survey

3.2.2 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.

3.2.3 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 Bruttoreate	Minimale Bruttoreate
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.

3.2.4 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.

3.2.5 QoS, WMM und U-APSD

Damit die Endgeräte eine lange Gesprächszeit und hohe Standby-Zeiten mit einer Akkulaudung 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.

3.2.5.1 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 benutzen 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.

3.2.5.2 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 funktionierendem 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.

3.2.6 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.

3.2.7 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 funkeln.“ 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.

3.3 Beispielkonfiguration

3.3.1 Netzwerkplan

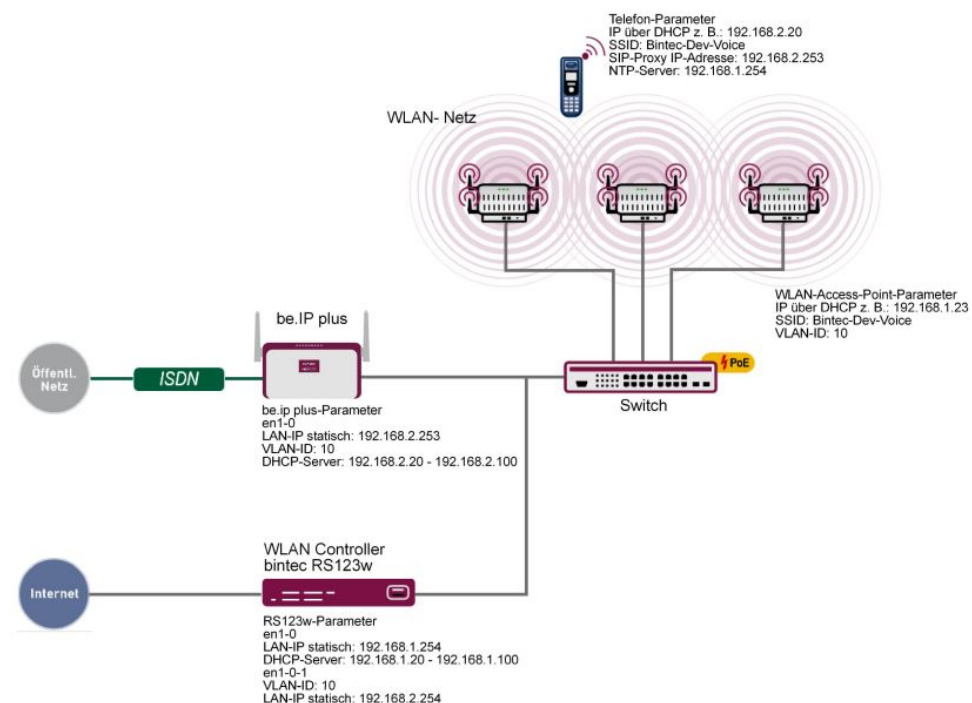


Abb. 56: Beispielszenario

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 hybrid 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.

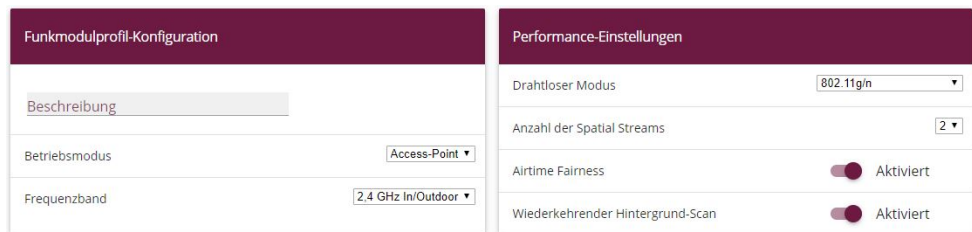
3.3.2 WLAN Konfiguration mit oder ohne WLAN Controller

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**.



Funkmodulprofil-Konfiguration	Performance-Einstellungen
Beschreibung	Drahtloser Modus: 802.11g/n
Betriebsmodus: Access-Point	Anzahl der Spatial Streams: 2
Frequenzband: 2,4 GHz In/Outdoor	Airtime Fairness: Aktiviert
	Wiederkehrender Hintergrund-Scan: Aktiviert

Abb. 57: **Wireless LAN Controller -> Slave-AP-Konfiguration -> Funkmodulprofile -> Neu**

Gehen Sie folgendermaßen vor:

- (1) Bei **Betriebsmodus** legen Sie fest, in welchem Modus das Funkmodulprofil 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**.

The screenshot shows the configuration interface for a new Wireless LAN network (VSS). It is organized into six main sections:

- Service Set Parameter:**
 - Netzwerkname (SSID): Sichtbar
 - Intra-cell Repeating:
 - U-APSD: Aktiviert
 - IGMP Snooping:
- Sicherheitseinstellungen:**
 - Sicherheitsmodus:
 - WPA-Modus:
 - WPA2 Cipher: AES TKIP AES und TKIP
 - Preshared Key:
- Client-Lastverteilung:**
 - Max. Anzahl Clients - Hard Limit:
 - Max. Anzahl Clients - Soft Limit:
 - Auswahl des Client-Bands:
- MAC-Filter:**
 - Zugriffskontrolle:
 - Dynamische Black List:
- VLAN:**
 - VLAN: Aktiviert
 - VLAN-ID:
- Bandbreitenbeschränkung für jeden WLAN-Client:**
 - Rx Shaping:
 - Tx Shaping:

Abb. 58: **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**.

3.4 Ascom i62 Talker Konfiguration

3.4.1 Voraussetzungen

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

3.4.2 Konfiguration

3.4.2.1 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*.

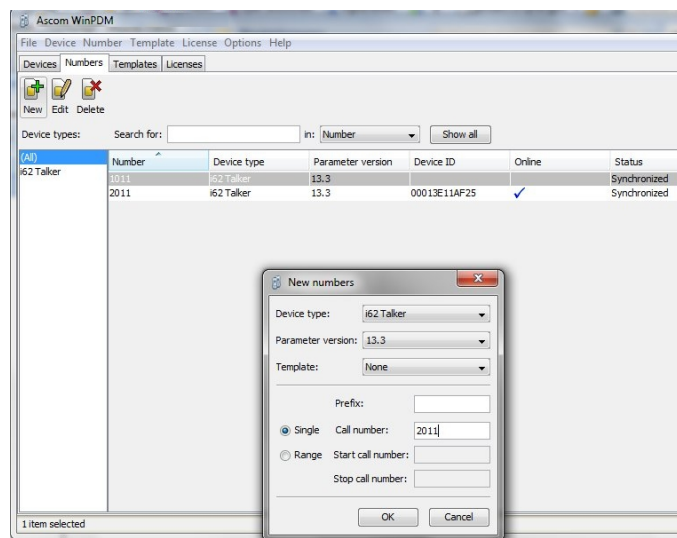


Abb. 59: Numbers -> New

Netzwerk definieren

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

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

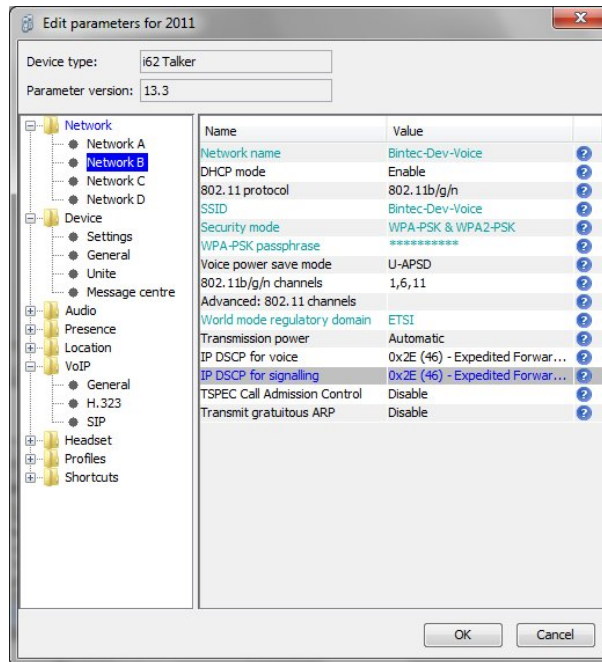


Abb. 60: **Network** -> **Network B**

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**.

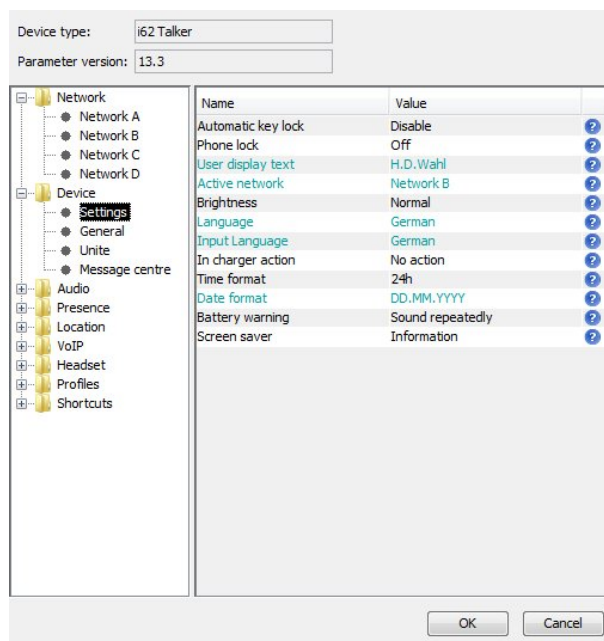


Abb. 61: Device -> Settings

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**.

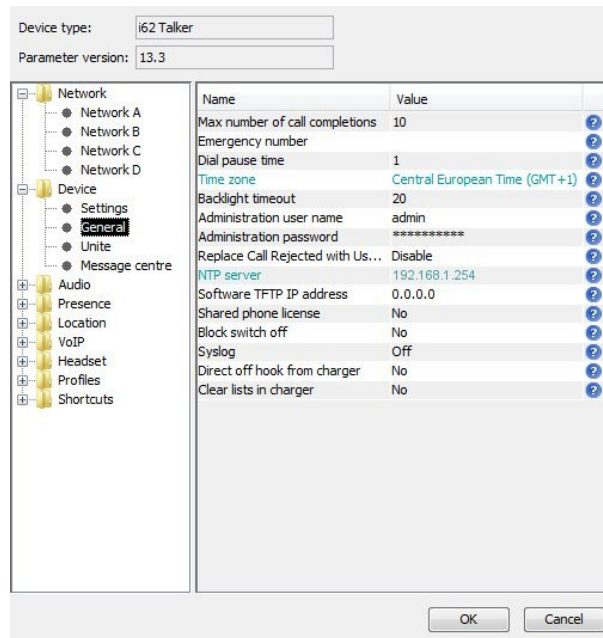


Abb. 62: Device -> General

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**.

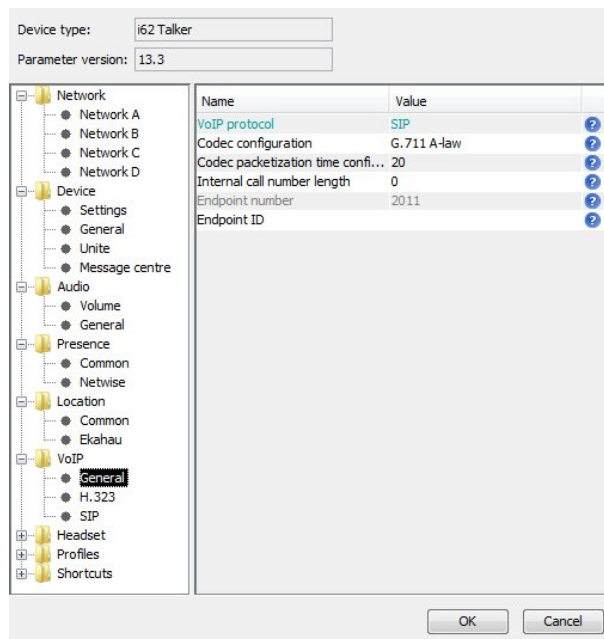


Abb. 63: VoIP -> General

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 Geräteparametersatzes festgelegt.

SIP-Konfiguration

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

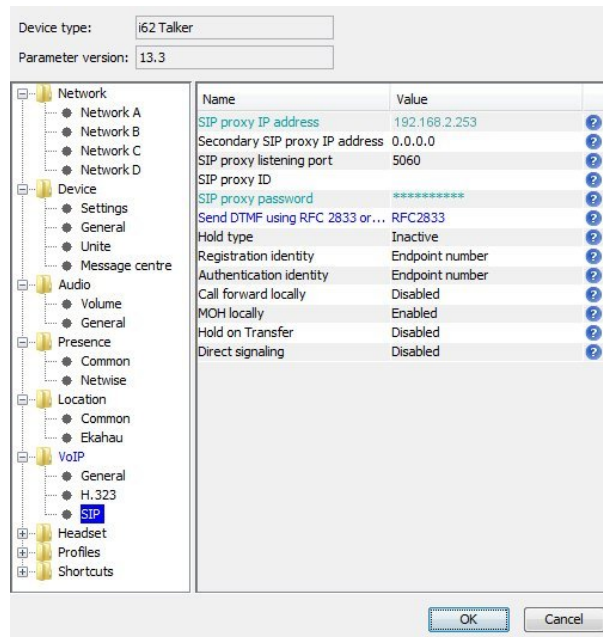


Abb. 64: VoIP -> SIP

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)

3.4.3 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

3.5 Konfiguration der bintec be.IP plus

3.5.1 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**.

The screenshot shows the configuration page for a new LAN interface. It is divided into two main sections:

- Basisparameter:**
 - Basierend auf Ethernet-Schnittstelle:** A dropdown menu showing 'en1-4'.
 - Schnittstellenmodus:** Radio buttons for 'Untagged' and 'Tagged (VLAN)', with 'Tagged (VLAN)' selected.
 - VLAN-ID:** A text input field containing '10'.
 - MAC-Adresse:** A text input field containing '00:a0:f9' and a toggle switch for 'Voreingestellte verwenden' which is turned on.
- Grundlegende IPv4-Parameter:**
 - Sicherheitsrichtlinie:** Radio buttons for 'Nicht Vertrauenswürdig' and 'Vertrauenswürdig', with 'Vertrauenswürdig' selected.
 - Adressmodus:** Radio buttons for 'Statisch' and 'DHCP', with 'Statisch' selected.
 - IP-Adresse / Netzmaske:** A section with two input fields for 'IP-Adresse' and 'Netzmaske', and a 'HINZUFÜGEN' button below them.

Abb. 65: 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**.

3.5.2 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 **Anrufwefterschaltung (AWS)** *Bei Besetzt/Bei Nichtmelden* in der **bi.IP plus** für die betreffende Nebenstelle einzurichten.

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

> **Neu.**

Grundeinstellungen

Interne Rufnummer

Art der Anrufweiserschaltung

Zielrufnummer (Bei Besetzt)
Geben Sie die Zielnummer ohne Amtskennziffer ein.
Zielrufnummer (Bei Besetzt)

Zielrufnummer (Bei Nichtmelden)
Geben Sie die Zielnummer ohne Amtskennziffer ein.
Zielrufnummer (Bei Nichtmelden)

Abb. 66: **Anrufkontrolle -> Ausgehende Dienste -> Anrufweiserschaltung (AWS) -> Neu**

Gehen Sie folgendermaßen vor:

- (1) Wählen Sie eine **Interne Rufnummer** aus, für die kommende Anrufe weitergeschaltet werden sollen.
- (2) Bei **Art der Anrufweiserschaltung** 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**.

3.6 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**

3.7 Konfigurationsschritte im Überblick

Funkmodulprofile konfigurieren

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

Funkmodulprofile konfigurieren

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

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. <i>supersecret</i>
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. <i>Bintec-Dev-Voice</i>
Security mode	Network -> Network B	WPA-PSK & WPA2-PSK
WPA-PSK passphrase	Network -> Network B	z. B. <i>supersecret</i>
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. <i>bintec elmeg</i>

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

Anrufweberschaltung konfigurieren

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

Kapitel 4 WLAN - Management für mehrere Standorte: WLAN Controller über VPN

4.1 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.

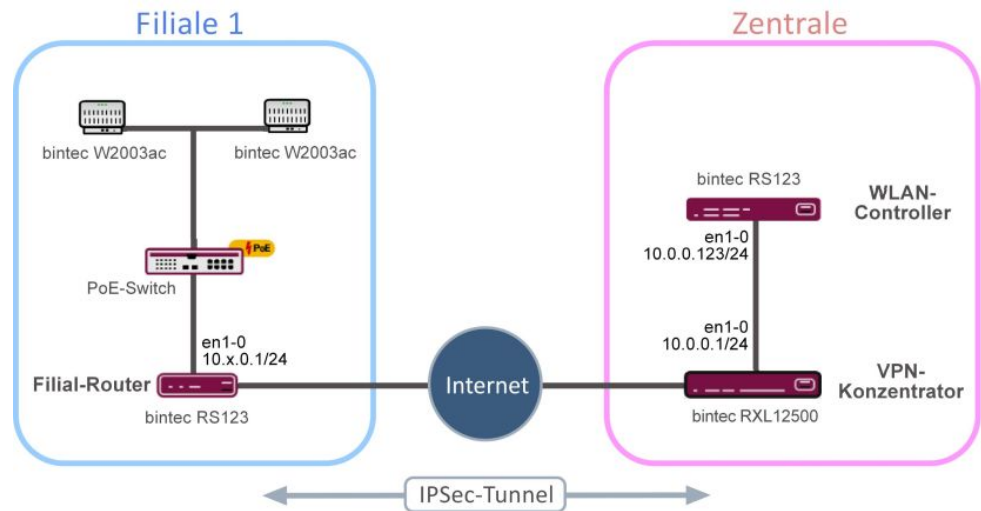


Abb. 67: Beispielszenario

4.1.1 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.

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).

4.1.2 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	

4.2 Konfiguration

4.2.1 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.

4.2.2 Konfiguration des Routers in der Außenstelle

4.2.2.1 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>** .



The screenshot shows two panels of the router configuration interface. The left panel, titled "Basisparameter", has "Schnittstellenmodus" set to "Untagged" (selected) and "Tagged (VLAN)". The "MAC-Adresse" is "00:09:4f:6f:5e:80" and the "Voreingestellte verwenden" checkbox is checked. The right panel, titled "Grundlegende IPv4-Parameter", has "Sicherheitsrichtlinie" set to "Vertrauenswürdig" (selected) and "Nicht Vertrauenswürdig". The "Adressmodus" is "Statisch" (selected) and "DHCP". The "IP-Adresse / Netzmaske" section shows "IP-Adresse" as "10.1.0.1" and "Netzmaske" as "255.255.255.0". A "HINZUFÜGEN" button is at the bottom.

Abb. 68: **LAN -> IP-Konfiguration -> Schnittstellen -> <en1-0>** 

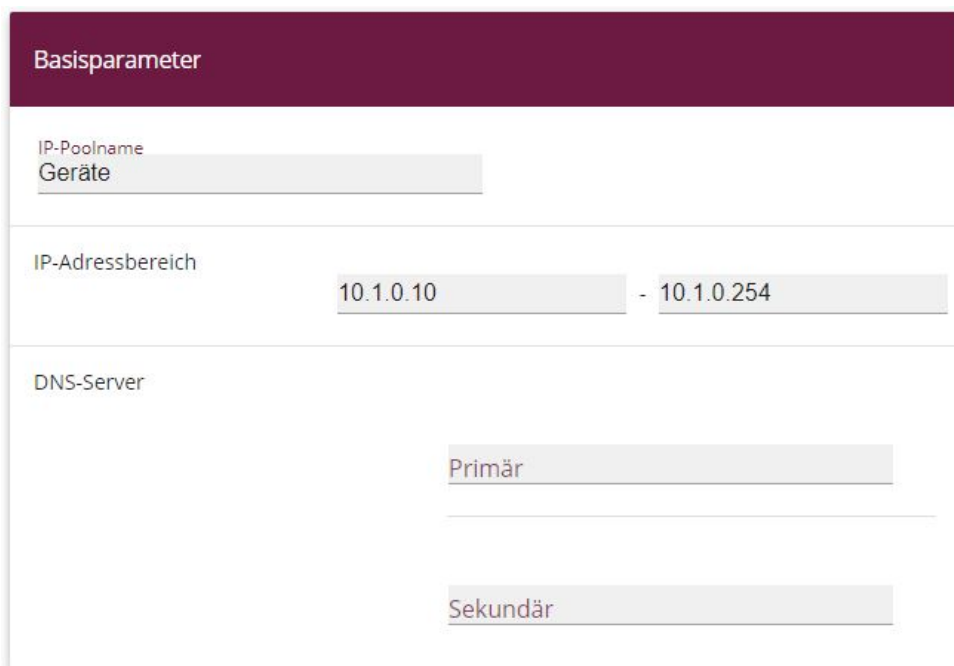
Gehen Sie folgendermaßen vor:

- (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**.

4.2.2.2 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 angebundene Mitarbeitergeräte, anlegen.

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



The screenshot shows a web-based configuration interface for a DHCP pool. The title bar is dark red and contains the text 'Basisparameter'. Below this, there are three main sections, each with a label on the left and a corresponding input field on the right:

- IP-Poolname**: The input field contains the text 'Geräte'.
- IP-Adressbereich**: The input field contains the range '10.1.0.10 - 10.1.0.254'.
- DNS-Server**: There are two input fields. The top one is labeled 'Primär' and is empty. The bottom one is labeled 'Sekundär' and is also empty.

Abb. 69: **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.

Basisparameter

Schnittstelle	en1-0
IP-Poolname	Geräte
Pool-Verwendung	Lokal
<input type="text" value="Beschreibung"/>	

Erweiterte Einstellungen:

Erweiterte Einstellung

Gateway	Router als Gateway verwenden
Lease Time	120 Minuten
DHCP-Optionen	
Option	Wert
DNS-Server	10.1.0.1
CAPIWAP Controller	10.0.0.123
HINZUFÜGEN	
Herstellerspezifische Informationen (DHCP-Option 43)	
Hersteller-ID	Herstellerspezifische Informationen
HERSTELLER-STRING HINZUFÜGEN	HERSTELLERGRUPPE HINZUFÜGEN

Abb. 71: 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-Gateway 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-Domänennamen*, *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**.

4.2.3 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>** .

The image shows two side-by-side configuration panels. The left panel, titled 'Basisparameter', has a dark header. Below it, 'Schnittstellenmodus' has two radio buttons: 'Untagged' (selected) and 'Tagged (VLAN)'. Below that, 'MAC-Adresse' is shown as '00:09:4f:6f:5e:80' with a toggle switch for 'Voreingestellte verwenden' which is turned on. The right panel, titled 'Grundlegende IPv4-Parameter', also has a dark header. It shows 'Sicherheitsrichtlinie' with radio buttons for 'Nicht Vertrauenswürdig' and 'Vertrauenswürdig' (selected). Below that, 'Adressmodus' has radio buttons for 'Statisch' (selected) and 'DHCP'. The 'IP-Adresse / Netzmaske' section contains two input fields: 'IP-Adresse' with '10.0.0.1' and 'Netzmaske' with '255.255.255.0'. A trash icon is to the right of the netmask field. At the bottom of this section is a 'HINZUFÜGEN' button.

Abb. 72: 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**.

4.2.4 Konfiguration des WLAN-Controllers in der Zentrale

4.2.4.1 IP-Konfiguration

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

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

This screenshot is identical to the one in Abb. 72, but the 'IP-Adresse' field in the 'Grundlegende IPv4-Parameter' section now contains the value '10.0.0.123' instead of '10.0.0.1'. All other settings remain the same.

Abb. 73: 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**.

4.2.4.2 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. 74: **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:

Routen							
Ziel-IP-Adresse	Netzmaske	Gateway	Schnittstelle	Metrik	Routentyp	Erweiterte Route	
0.0.0.0	0.0.0.0	10.0.0.1	LAN_EN1-0	1	Standardroute über Schnittstelle	<input type="checkbox"/>	
10.0.0.0	255.255.255.0	10.0.0.151	LAN_EN1-0	0	Netzwerkroute via Schnittstelle	<input type="checkbox"/>	

Abb. 75: **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**.

4.2.4.3 WLAN-Controller konfigurieren

Nun kann der eigentliche WLAN-Controller aktiviert werden.

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

Grundeinstellungen	
Status	<input checked="" type="checkbox"/> Aktiviert
Region	Germany ▼
Schnittstelle	LAN_EN1-0 ▼
DHCP-Server	DHCP-Server mit aktivierter CAPWAP Option (138): <input checked="" type="radio"/> Extern oder statisch <input type="radio"/> Intern
Slave-AP-Standort	<input type="radio"/> Lokal (LAN) <input checked="" type="radio"/> Entfernt (WAN)
Slave-AP-LED-Modus	Status ▼

Abb. 76: **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).

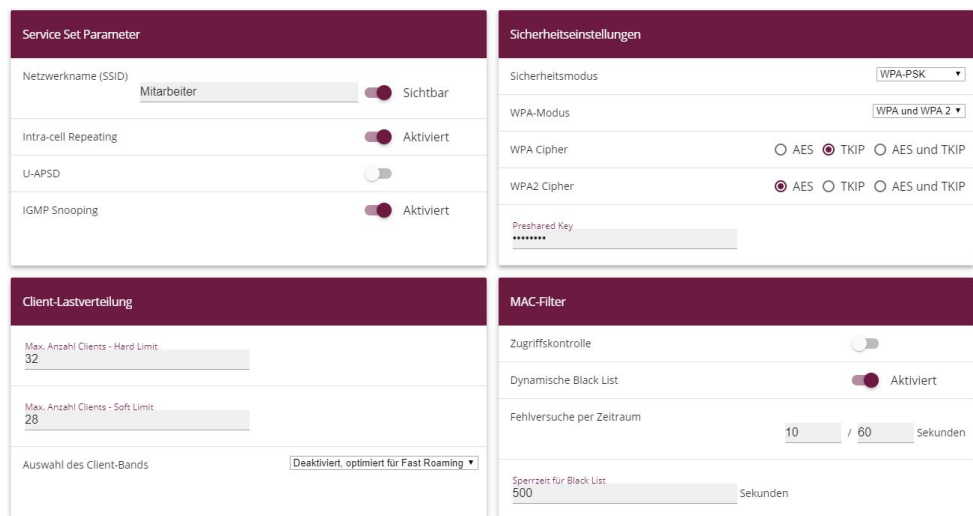
- (5) Bestätigen Sie mit **OK**.
Die Einstellungen sind jetzt aktiv und der WLAN Controller wird gestartet.

4.2.4.4 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.



The screenshot displays the configuration interface for a Wireless LAN Controller, divided into four main sections:

- Service Set Parameter:**
 - Netzwerkname (SSID): Mitarbeiter (Visible:)
 - Intra-cell Repeating: Aktiviert
 - U-APSD:
 - IGMP Snooping: Aktiviert
- Sicherheitseinstellungen:**
 - Sicherheitsmodus: WPA-PSK
 - WPA-Modus: WPA und WPA 2
 - WPA Cipher: AES TKIP AES und TKIP
 - WPA2 Cipher: AES TKIP AES und TKIP
 - Preshared Key: [Redacted]
- Client-Lastverteilung:**
 - Max. Anzahl Clients - Hard Limit: 32
 - Max. Anzahl Clients - Soft Limit: 28
 - Auswahl des Client-Bands: Deaktiviert, optimiert für Fast Roaming
- MAC-Filter:**
 - Zugriffskontrolle:
 - Dynamische Black List: Aktiviert
 - Fehlversuche per Zeitraum: 10 / 60 Sekunden
 - Sperrzeit für Black List: 500 Sekunden


Abb. 77: **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**.

4.2.4.5 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.





Funkmodulprofil-Konfiguration		Performance-Einstellungen	
Beschreibung 2.4 GHz Radio Profile		Drahtloser Modus	802.11g/n
Betriebsmodus	Access-Point	Anzahl der Spatial Streams	3
Frequenzband	2.4 GHz In/Outdoor	Airtime Fairness	<input checked="" type="checkbox"/> Aktiviert
		Wiederkehrender Hintergrund-Scan	<input checked="" type="checkbox"/> Aktiviert

Erweiterte Einstellungen

Erweiterte Einstellung

Kanalplan Benutzerdefiniert ▾

Benutzerdefinierter Kanalplan

Kanal	
1 ▾	
5 ▾	
9 ▾	
13 ▾	

HINZUFÜGEN

Beacon Period ms

DTIM Period

RTS Threshold

Short Guard Interval Aktiviert

Max. Übertragungsrate Auto ▾

Short Retry Limit

Long Retry Limit

Fragmentation Threshold Bytes

Abb. 79: 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.

4.2.4.6 Access Points konfigurieren

Jetzt werden die Access Points aktiviert und eingerichtet.

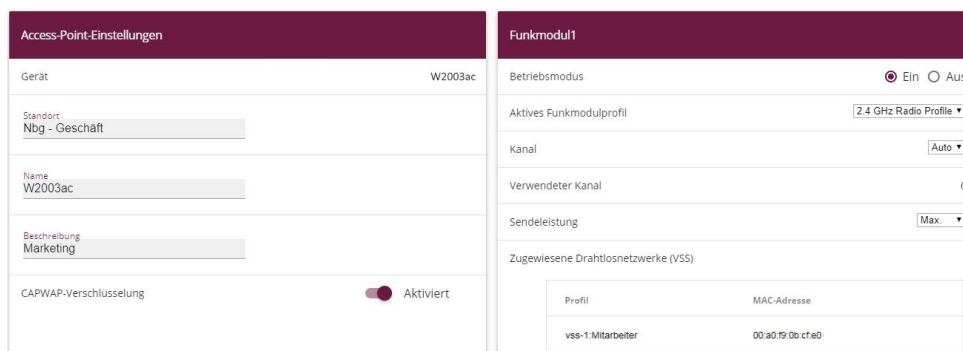
- (1) Gehen Sie zu **Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points**.

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 CAP-WAP-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-Profil 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** .



Profil	MAC-Adresse
vss-1.Mitarbeiter	00:a0:f9:00:cf:e0

Abb. 80: **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 Funkmodulprofils 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:

Slave Access Points								
Standort	Name	IP-Adresse	LAN-MAC-Adresse	Kanal	Kanalsuche	Status	Aktion	
Nbg - Geschäft	W2003ac	10.1.0.14	00:01:cd:0f:4a:88	13 HT20 (automatisch)	↻	Managed	^ v	🗑️ ✎
Nbg - Büro	W2003ac	10.1.0.13	00:01:cd:0e:58:1a	9 HT20 (automatisch)	↻	Managed	^ v	🗑️ ✎
Nbg - Lager	W2003ac	10.1.0.12	00:01:cd:0e:b3:d0	5 HT20 (automatisch)	↻	Managed	^ v	🗑️ ✎
Nbg - Ausstellungsraum	W2003ac	10.1.0.10	00:01:cd:0e:8e:fa	1 HT20 (automatisch)	↻	Managed	^ v	🗑️ ✎

Abb. 81: Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points

4.2.4.7 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**.

Basisparameter	E-Mail-Parameter
Benachrichtigungsdienst <input checked="" type="checkbox"/> Aktiviert	E-Mail-Adresse des Senders wlc@it.company.tld
Maximale E-Mails pro Minute <input type="text" value="6"/>	SMTP-Server smtp.mail.com
	SMTP-Port <input type="text" value="25"/> <input checked="" type="checkbox"/> SSL
	SMTP-Authentifizierung <input checked="" type="radio"/> Keiner <input type="radio"/> ESMTP <input type="radio"/> SMTP after POP

Abb. 82: Externe Berichterstellung -> Benachrichtigungsdienst -> Benachrichtigungseinstellungen

Gehen Sie folgendermaßen vor:

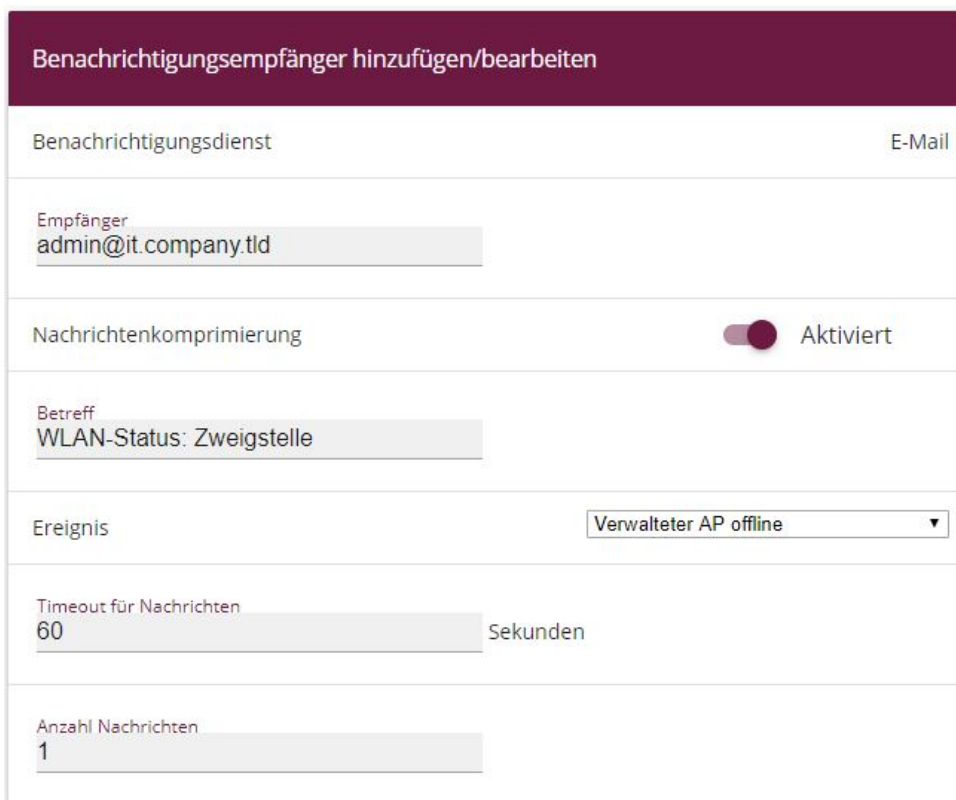
- (1) Der **Benachrichtigungsdienst** muss aktiviert sein.
- (2) Über den Wert bei **Maximale E-Mails pro Minute** können Sie die Anzahl der ausgehenden Mails pro Minute begrenzen, z. B. 6.
- (3) Tragen Sie eine Adresse ein, die in das Absenderfeld der E-Mail eingetragen wird, z.

B. *wlc@it.company.tld*.

- (4) Geben Sie die IP-Adresse oder den DNS-Namen des **SMTP-Servers** 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**.



The screenshot shows a configuration interface for adding or editing a notification recipient. The title is 'Benachrichtigungsempfänger hinzufügen/bearbeiten'. The configuration is for an 'E-Mail' notification service. The recipient is 'admin@it.company.tld'. The 'Nachrichtenkomprimierung' (Message compression) is turned on ('Aktiviert'). The subject line is 'WLAN-Status: Zweigstelle'. The event is set to 'Verwalteter AP offline'. The message timeout is 60 seconds. The number of messages is 1.

Abb. 83: **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**.

4.3 Konfigurationsschritte im Überblick

Konfiguration des Routers in der Außenstelle - IP-Konfiguration





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

Konfiguration des Routers in der Außenstelle - DHCP-Pool




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

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 -> Allgemein	LAN_EN1-0
DHCP-Server	Wireless LAN Controller -> Controller-Konfiguration -> Allgemein	Extern oder statisch
Slave-AP-Standort	Wireless LAN Controller -> Controller-Konfiguration -> Allgemein	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 -> Funkmodulprofile -> 2.4 GHz Radio Profile 	2
Drahtloser Modus	Wireless LAN Controller -> Slave-AP-Konfiguration -> Funkmodulprofile -> 2.4 GHz Radio Profile 	802.11 g / n
Max. Übertragungsrate	Wireless LAN Controller -> Slave-AP-Konfiguration -> Funkmodulprofile -> 2.4 GHz Radio Profile 	Auto
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 	Benutzerdefiniert
Benutzerdefinierter Kanalplan	Wireless LAN Controller -> Slave-AP-Konfiguration -> Funkmodulprofile -> 2.4 GHz Radio Profile  ->Erweiterte Einstellungen	1, 5, 9, 13
Beacon Period	Wireless LAN Controller -> Slave-AP-Konfiguration -> Funkmodulprofile -> 2.4 GHz Radio Profile  ->Erweiterte Einstellungen	100 ms
DTIM Period	Wireless LAN Controller -> Slave-AP-Konfiguration -> Funkmodulprofile -> 2.4 GHz Radio Profile  ->Erweiterte Einstellungen	2
RTS Threshold	Wireless LAN Controller -> Slave-AP-Konfiguration -> Funkmodulprofile -> 2.4 GHz Radio  Profile->Erweiterte Einstellungen	2347
Short Guard Interval	Wireless LAN Controller -> Slave-AP-Konfiguration -> Funkmodulprofile -> 2.4 GHz Radio  Profile->Erweiterte Einstellungen	Aktiviert
Short Retry Limit	Wireless LAN Controller -> Slave-AP-Konfiguration -> Funkmodulprofile -> 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. <i>Nbg - Geschäft</i>
CAPWAP-Verschlüsselung	Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points	<i>Aktiviert</i>
Betriebsmodus	Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points	<i>Ein</i>
Aktives Funkmodulprofil	Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points	z. B. <i>2.4 GHz Radio Profile</i>
Kanal	Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points	<i>Auto</i>
Verwendeter Kanal	Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points	z. B. <i>13</i>
Sendeleistung	Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points	<i>Max.</i>
Zugewiesene Drahtlosnetzwerke (VSS)	Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points	z. B. <i>vss-1: Mitarbeiter</i>

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. <i>wlc@itcompany.tld</i>
SMTP-Server	Externe Berichterstellung -> Benachrichtigungsdienst -> Benachrichtigungseinstellungen	z. B. <i>smtp.mail.com</i>
SMTP- Authentifizierung	Externe Berichterstellung -> Benachrichtigungsdienst -> Benachrichtigungseinstellungen	z. B. <i>Keine</i>

E-Mail-Benachrichtigung einrichten - Empfänger

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

Kapitel 5 WLAN - Wireless LAN Controller als Netzzugangsgateway

5.1 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.

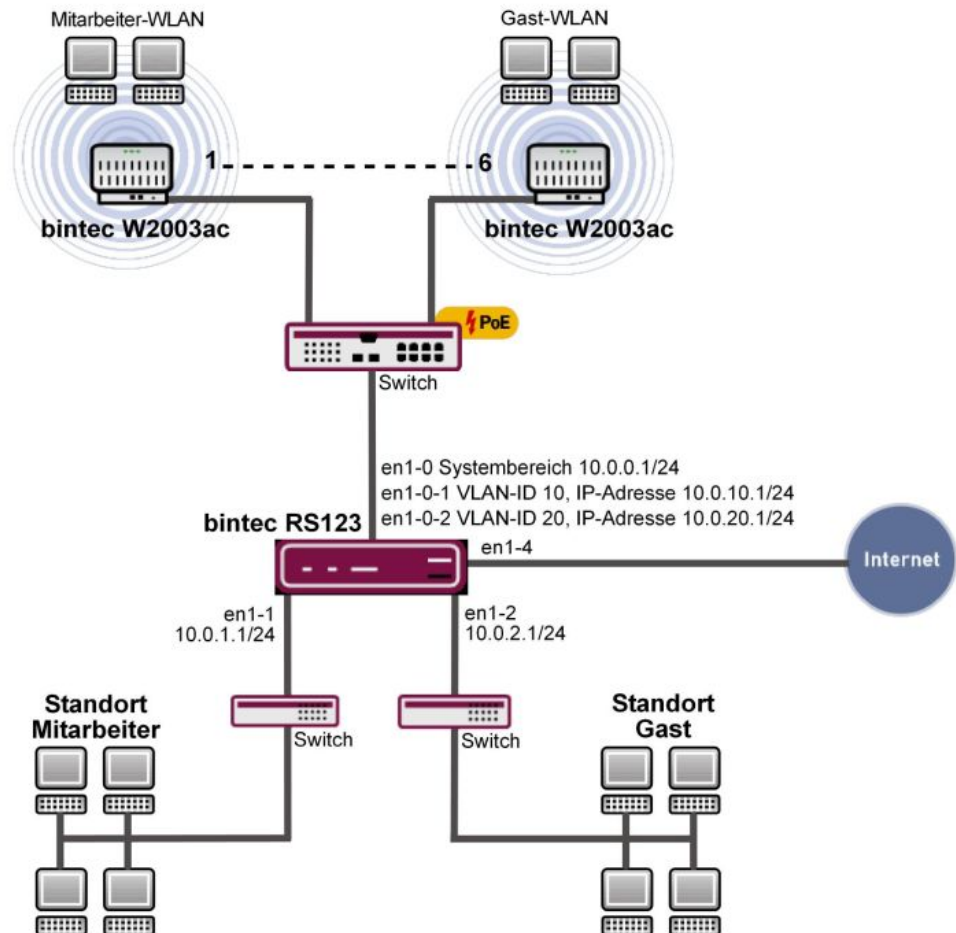


Abb. 84: Beispielszenario

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 Switches 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

5.2 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**.

Switch-Konfiguration				
Automatisches Aktualisierungsintervall <input type="text" value="60"/> Sekunden <input type="button" value="ÜBERNEHMEN"/>				
Switch-Port	Ethernet-Schnittstellenauswahl	Konfigurierte Geschwindigkeit / Konfigurierter Modus	Aktuelle Geschwindigkeit / Aktueller Modus	Flusskontrolle
1	<input type="text" value="en1-0"/>	<input type="text" value="Vollständige automatische Aushandlung"/>	100 Mbit/s / Full Duplex	<input type="text" value="Deaktiviert"/>
2	<input type="text" value="en1-1"/>	<input type="text" value="Vollständige automatische Aushandlung"/>	Inaktiv	<input type="text" value="Deaktiviert"/>
3	<input type="text" value="en1-2"/>	<input type="text" value="Vollständige automatische Aushandlung"/>	Inaktiv	<input type="text" value="Deaktiviert"/>
4	<input type="text" value="en1-3"/>	<input type="text" value="Vollständige automatische Aushandlung"/>	Inaktiv	<input type="text" value="Deaktiviert"/>
5	<input type="text" value="en1-4"/>	<input type="text" value="Vollständige automatische Aushandlung"/>	Inaktiv	<input type="text" value="Deaktiviert"/>

Abb. 85: **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.

The screenshot shows a four-step configuration assistant for an Internet connection. Step 1: 'Wählen Sie den physischen Ethernet-Port aus, der mit dem externen Gateway/Kabelmodem verbunden ist:' with a dropdown menu showing 'ETH5'. Step 2: 'Wählen Sie aus der Liste Ihren Internetdiensteanbieter (ISP) aus:' with a dropdown menu showing '-- Benutzerdefiniert --'. Step 3: 'Werden IP-Parameter dynamisch abgerufen?' with a toggle switch turned off. Step 4: 'Geben Sie die IP-Einstellungen Ihres Internetzugangs ein:' with input fields for 'Lokale IP-Adresse' (1.2.3.4), 'Gateway-IP-Adresse' (1.2.3.1), 'Netzmaske' (255.255.255.0), 'DNS-Server 1' (1.2.3.1), and 'DNS-Server 2' (0.0.0.0).

Abb. 86: **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 Firewallrichtung relevant.



Hinweis

Diese Schnittstelle darf nicht mit der ebenfalls vorhandenen (zugrundeliegenden) *eth0a*-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. 87: **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**.

The screenshot shows two side-by-side configuration panels. The left panel, titled 'Basisparameter', has a dropdown menu for 'Basierend auf Ethernet-Schnittstelle' set to 'en1-0'. Below it, 'Schnittstellenmodus' has radio buttons for 'Untagged' and 'Tagged (VLAN)', with 'Tagged (VLAN)' selected. The 'VLAN-ID' field contains the number '10'. The 'MAC-Adresse' field contains '00:a0:f9' and has a toggle switch for 'Voreingestellte verwenden' which is turned on. The right panel, titled 'Grundlegende IPv4-Parameter', has radio buttons for 'Sicherheitsrichtlinie' set to 'Vertrauenswürdig'. The 'Adressmodus' has radio buttons for 'Statisch' and 'DHCP', with 'Statisch' selected. Below, the 'IP-Adresse / Netzmaske' section has two input fields: 'IP-Adresse' with '10.0.10.1' and 'Netzmaske' with '255.255.255.0'. A trash icon is to the right of the netmask field. At the bottom of this section is a 'HINZUFÜGEN' button.

Abb. 88: **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:

Ethernet-/VLAN-Ports						
Schnittstelle	IPv4-Adresse/Netzmaske	IPv6-Adresse/Länge	Status	Aktion		
en1-0	10.0.0.1/255.255.255.0	-	✓	^	v	
en1-4	1.2.3.4/255.255.255.0	-	✓	^	v	
en1-1	10.0.1.1/255.255.255.0	-	✗	^	v	
en1-2	10.0.2.1/255.255.255.0	-	✓	^	v	
en1-3	Nicht konfiguriert/Nicht konfiguriert	-	✗	^	v	
ethoa35-5	Nicht konfiguriert/Nicht konfiguriert	-	✗	^	v	
en1-0-1(VLAN-ID10)	10.0.10.1/255.255.255.0	-	✓	^	v	
en1-0-2(VLAN-ID20)	10.0.20.1/255.255.255.0	-	✓	^	v	

Abb. 89: LAN -> IP-Konfiguration -> Schnittstellen

Systemzugangs- und Firewall einrichtung

Im Menü **Zugriff** wird der administrative 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**.

Zugriff						
Schnittstelle	Telnet	SSH	HTTP	HTTPS	Ping	SNMP
en1-0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
en1-4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
en1-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
en1-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
en1-3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
en1-0-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
en1-0-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
br0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Abb. 90: 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	<input type="checkbox"/>
ah	<input type="checkbox"/>
any	<input type="checkbox"/>
clients_1	<input type="checkbox"/>
clients_2	<input type="checkbox"/>
daytime	<input type="checkbox"/>
dhcp	<input checked="" type="checkbox"/>
discard	<input type="checkbox"/>
dns	<input checked="" type="checkbox"/>
echo-req	<input checked="" type="checkbox"/>
echo-req-ipv6	<input type="checkbox"/>
esp	<input type="checkbox"/>

Abb. 91: 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**.

The screenshot shows a configuration window titled 'Basisparameter'. It contains the following fields and controls:

- Beschreibung:** A text input field containing 'Broadcast'.
- IPv4:** A toggle switch that is turned on, labeled 'Aktiviert'.
- Adresstyp:** Two radio buttons: 'Adresse/Subnetz' (selected) and 'Adressbereich'.
- Adresse/Subnetz:** Two text input fields. The first contains '255.255.255.255' and the second contains '255.255.255.255', separated by a slash.
- IPv6:** A toggle switch that is turned off, labeled 'Deaktiviert'.

Abb. 92: 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:

Adressliste				
Beschreibung	Adresse/Subnetz/Adressbereich	Adresse/Präfix		
ANY	0.0.0.0/0	::/0		
Broadcast	255.255.255.255/32			
Mitarbeiter-LAN-GW	10.0.1.1/32			
Gast-LAN-GW	10.0.2.1/32			
Mitarbeiter-WLAN-GW	10.0.10.1/32			
Gast-WLAN-GW	10.0.20.1/32			

Abb. 93: Firewall -> Adressen -> Adressliste

Jetzt müssen Sie noch die Schnittstellen für die einzelnen Benutzergruppen definieren.

- (1) Gehen Sie zu **Firewall -> Schnittstellen -> IPv4-Gruppen -> Neu**.

Basisparameter

Beschreibung
Mitarbeiter

Mitglieder

Schnittstelle	Auswahl
LOCAL	<input type="checkbox"/>
LAN_EN1-0	<input type="checkbox"/>
LAN_EN1-5	<input type="checkbox"/>
LAN_EN1-1	<input checked="" type="checkbox"/>
LAN_EN1-2	<input type="checkbox"/>
LAN_EN1-3	<input type="checkbox"/>
LAN_EN1-4	<input type="checkbox"/>
LEASED_EN1-0-1	<input checked="" type="checkbox"/>
LEASED_EN1-0-2	<input type="checkbox"/>

Abb. 94: 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:







IPv4-Gruppen			
Beschreibung	Mitglieder		
Mitarbeiter	LAN_EN1-1, LEASED_EN1-0-1		
Gast	LAN_EN1-2, LEASED_EN1-0-2		
Benutzer	LAN_EN1-1, LAN_EN1-2, LEASED_EN1-0-1, LEASED_EN1-0-2		

Abb. 95: 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**.

Basisparameter	
Quelle	LAN_EN1-0 ▾
Ziel	ANY ▾
Dienst	any ▾
Aktion	Zugriff ▾

Abb. 96: 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**.



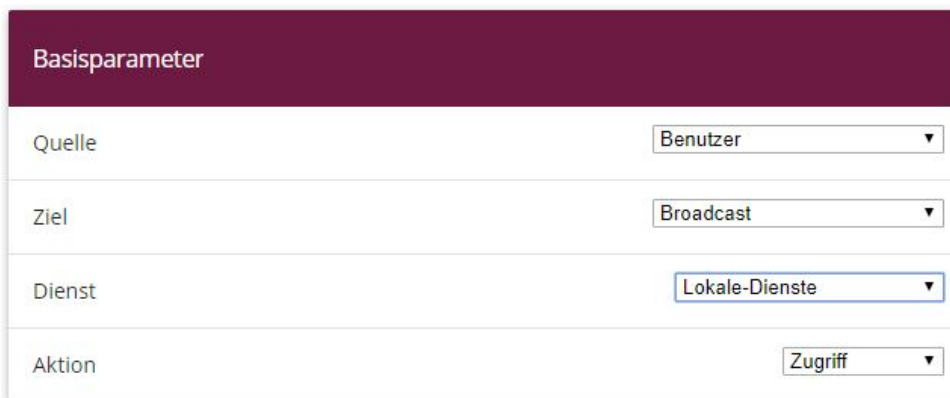
Hinweis

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**.



Basisparameter	
Quelle	Benutzer
Ziel	Broadcast
Dienst	Lokale-Dienste
Aktion	Zugriff

Abb. 97: **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:

Filterregeln						
Abfolge	Quelle	Ziel	Dienst	Aktion	Richtlinie aktiv	
1	LAN_EN1-0	ANY	any	Zugriff	<input checked="" type="checkbox"/> Aktiviert	↑↓ ⋮ 🗑️ ✎
2	Mitarbeiter	Benutzer	any	Zugriff	<input checked="" type="checkbox"/> Aktiviert	↑↓ ⋮ 🗑️ ✎
3	Gast	Gast	any	Zugriff	<input checked="" type="checkbox"/> Aktiviert	↑↓ ⋮ 🗑️ ✎
4	Benutzer	LAN_EN1-4	any	Zugriff	<input checked="" type="checkbox"/> Aktiviert	↑↓ ⋮ 🗑️ ✎
5	Benutzer	Broadcast	Lokale-Dienste	Zugriff	<input checked="" type="checkbox"/> Aktiviert	↑↓ ⋮ 🗑️ ✎
6	LAN_EN1-1	Mitarbeiter-LAN-GW	Lokale-Dienste	Zugriff	<input checked="" type="checkbox"/> Aktiviert	↑↓ ⋮ 🗑️ ✎
7	LAN_EN1-2	Gast-LAN-GW	Lokale-Dienste	Zugriff	<input checked="" type="checkbox"/> Aktiviert	↑↓ ⋮ 🗑️ ✎
8	LEASED_EN1-0-1	Mitarbeiter-WLAN-GW	Lokale-Dienste	Zugriff	<input checked="" type="checkbox"/> Aktiviert	↑↓ ⋮ 🗑️ ✎
9	LEASED_EN1-0-2	Gast-WLAN-GW	Lokale-Dienste	Zugriff	<input checked="" type="checkbox"/> Aktiviert	↑↓ ⋮ 🗑️ ✎

Abb. 98: 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**.

Globale Firewall-Optionen		Sitzungstimer	
Status der IPv4-Firewall	<input checked="" type="checkbox"/> Aktiviert	UDP-Inaktivität	180 Sekunden
Protokollierte Aktionen	Alle	TCP-Inaktivität	3600 Sekunden
Vollständige IPv4-Filterung	<input checked="" type="checkbox"/> Aktivieren	PPTP-Inaktivität	86400 Sekunden
STUN Handler	<input type="checkbox"/>	Andere Inaktivität	30 Sekunden

Abb. 99: 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**.

Basisparameter	
IP-Poolname	Slave-APs
IP-Adressbereich	10.0.0.10 - 10.0.0.29
DNS-Server	<div style="margin-bottom: 10px;">Primär</div> <div>Sekundär</div>

Abb. 100: 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.

Basisparameter

Schnittstelle	en1-0 ▼
IP-Poolname	Slave-APs ▼
Pool-Verwendung	Lokal ▼
Beschreibung	

Erweiterte Einstellungen:

Erweiterte Einstellung

Gateway Router als Gateway verwenden ▾

Lease Time Minuten

Option	Wert	
DNS-Server ▾	<input type="text" value="10.0.0.1"/>	✖
CAPWAP Controller ▾	<input type="text" value="10.0.0.1"/>	✖

HINZUFÜGEN

Herstellerspezifische Informationen (DHCP-Option 43)

Hersteller-ID	Herstellerspezifische Informationen
<input type="text"/>	<input type="text"/>

HERSTELLER-STRING HINZUFÜGEN HERSTELLERGRUPPE HINZUFÜGEN

Abb. 102: **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:

IP Pools:			
IP-Poolname	IP-Adressbereich	Primärer DNS-Server	Sekundärer DNS-Server
Slave-APs	10.0.0.10 - 10.0.0.29	0.0.0.0	0.0.0.0
Mitarbeiter-WLAN	10.0.10.10 - 10.0.10.254	0.0.0.0	0.0.0.0
Mitarbeiter-Ethernet	10.0.1.10 - 10.0.1.254	0.0.0.0	0.0.0.0
Gast-WLAN	10.0.20.10 - 10.0.20.254	0.0.0.0	0.0.0.0
Gast-Ethernet	10.0.2.10 - 10.0.2.254	0.0.0.0	0.0.0.0

Abb. 103: 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**.

Grundeinstellungen

Status Aktiviert

Region Germany

Schnittstelle en1-0

DHCP-Server DHCP-Server mit aktivierter CAPWAP Option (138):
 Extern oder statisch
 Intern

IP-Adressbereich 10.0.0.10 - 10.0.0.29

Slave-AP-Standort Lokal (LAN)
 Entfernt (WAN)

Slave-AP-LED-Modus Status

Abb. 104: 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.

Service Set Parameter

Netzwerkname (SSID)
Mitarbeiter Sichtbar

Intra-cell Repeating Aktiviert

U-APSD

IGMP Snooping Aktiviert

Sicherheitseinstellungen

Sicherheitsmodus

WPA-Modus

WPA Cipher AES TKIP AES und TKIP

WPA2 Cipher AES TKIP AES und TKIP

Preshared Key

Client-Lastverteilung

Max. Anzahl Clients - Hard Limit
32

Max. Anzahl Clients - Soft Limit
24

Auswahl des Client-Bands

MAC-Filter

Zugriffskontrolle

Dynamische Black List Aktiviert

Fehlversuche per Zeitraum
10 / 60 Sekunden

Sperrzeit für Black List
500 Sekunden

VLAN

VLAN Aktiviert

VLAN-ID
10

Bandbreitenbeschränkung für jeden WLAN-Client

Rx Shaping

Tx Shaping

Abb. 105: 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**.

The screenshot shows the configuration interface for a new WLAN network. It is organized into several sections:

- Service Set Parameter:**
 - Netzwerkname (SSID): Sichtbar
 - Intra-cell Repeating: Aktiviert
 - U-APSD: Aktiviert
 - IGMP Snooping:
- Sicherheitseinstellungen:**
 - Sicherheitsmodus:
 - WPA-Modus:
 - WPA Cipher: AES TKIP AES und TKIP
 - WPA2 Cipher: AES TKIP AES und TKIP
 - Preshared Key:
- Client-Lastverteilung:**
 - Max. Anzahl Clients - Hard Limit:
 - Max. Anzahl Clients - Soft Limit:
 - Auswahl des Client-Bands:
- MAC-Filter:**
 - Zugriffskontrolle:
 - Dynamische Black List: Aktiviert
 - Fehlversuche per Zeitraum: / Sekunden
 - Sperrzeit für Black List: Sekunden
- VLAN:**
 - VLAN: Aktiviert
 - VLAN-ID:
- Bandbreitenbeschränkung für jeden WLAN-Client:**
 - Rx Shaping:
 - Tx Shaping:


Abb. 106: **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.

Funkmodulprofil-Konfiguration	Performance-Einstellungen
Beschreibung 2.4 GHz Radio Profile	Drahtloser Modus 802.11b/g/n
Betriebsmodus Access-Point	Anzahl der Spatial Streams 3
Frequenzband 2.4 GHz In/Outdoor	Airtime Fairness <input checked="" type="checkbox"/> Aktiviert
	Wiederkehrender Hintergrund-Scan <input checked="" type="checkbox"/> Aktiviert

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**.

Erweiterte Einstellungen

Erweiterte Einstellung

Kanalplan Benutzerdefiniert ▾

Benutzerdefinierter Kanalplan

Kanal	
1 ▾	
5 ▾	
9 ▾	
13 ▾	

HINZUFÜGEN

Beacon Period 100 ms

DTIM Period 2

RTS Threshold 2347

Short Guard Interval Aktiviert

Max. Übertragungsrate Auto ▾

Short Retry Limit 7

Long Retry Limit 4

Fragmentation Threshold 2346 Bytes

Abb. 108: 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**.



Standort	Name	IP-Adresse	LAN-MAC-Adresse	Kanal	Kanalsuche	Status	Aktion
1:	bintec W2003ac	10.0.0.11	00:01:cd:0e:ee:bc			 Managed	  

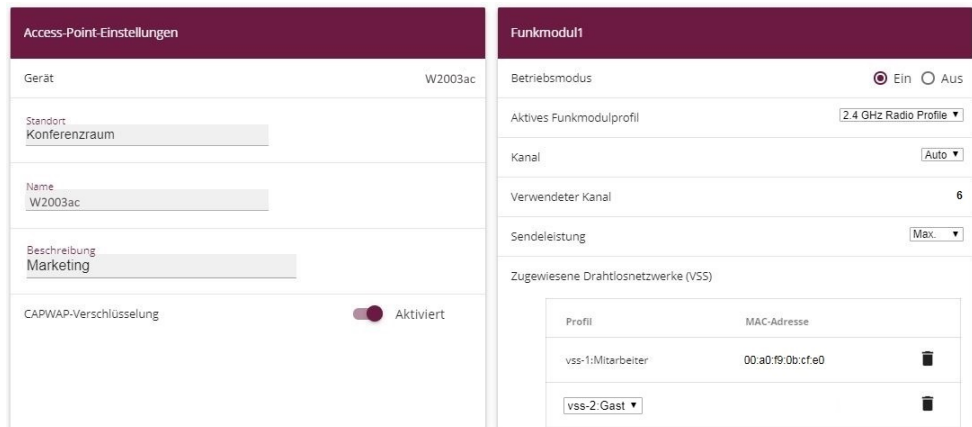
Abb. 109: **Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points**

**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** .



The screenshot shows two configuration panels. The left panel, 'Access-Point-Einstellungen', has a device ID of 'W2003ac'. Fields include 'Standort' (Konferenzraum), 'Name' (W2003ac), 'Beschreibung' (Marketing), and 'CAPWAP-Verschlüsselung' (Aktiviert). The right panel, 'Funkmodul1', shows 'Betriebsmodus' (Ein), 'Aktives Funkmodulprofil' (2.4 GHz Radio Profile), 'Kanal' (Auto), 'Verwendeter Kanal' (6), and 'Sendeleistung' (Max.). Below, a table lists 'Zugewiesene Drahtlosnetzwerke (VSS)' with columns for 'Profil' and 'MAC-Adresse'.



Profil	MAC-Adresse	
vss-1:Mitarbeiter	00:a0:f9:0b:cfe0	
vss-2:Gast		

Abb. 110: **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 **Zugewiesene Drahtlosnetzwerke (VSS)** werden die beiden konfigurierten Drahtlosnetzwerke *Mitarbeiter* und *Gast* dem Funkmodul zugewiesen.
- (8) Bestätigen Sie mit **OK**.

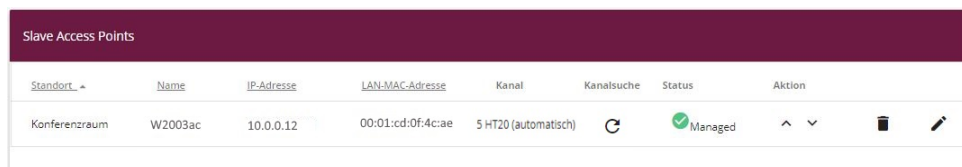
Konfigurieren Sie analog dazu alle gefundenen Access-Points.



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:



Standort	Name	IP-Adresse	LAN-MAC-Adresse	Kanal	Kanalsuche	Status	Aktion
Konferenzraum	W2003ac	10.0.0.12	00:01:cd:0f:4c:ae	5 HT20 (automatisch)		Managed	

Abb. 111: **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 -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 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) Feuerstutztüren 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.

5.3 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 -> Administrativer Zugriff -> Zugriff	Ping

Field	Menu	Value
	ver Zugriff -> Zugriff	

Passwort ändern

Field	Menu	Value
Systemadministrator-Passwort	Systemverwaltung -> Globale Einstellungen -> Passwörter	z. B. <i>test12345</i>
Systemadministrator-Passwort bestätigen	Systemverwaltung -> Globale Einstellungen -> Passwörter	z. B. <i>test12345</i>

Firewall einrichten

Field	Menu	Value
Beschreibung	Firewall -> Dienste -> Gruppen -> Neu	<i>Lokale-Dienste</i>
Mitglieder	Firewall -> Dienste -> Gruppen -> Neu	z. B. <i>echo, dns, dhcp, ntp</i>

Adressen definieren

Field	Menu	Value
Beschreibung	Firewall -> Adressen -> Adressliste -> Neu	<i>Broadcast</i>
Adresse/Subnetz	Firewall -> Adressen -> Adressliste -> Neu	<i>255.255.255.255 / 255.255.255.255</i>
Beschreibung	Firewall -> Adressen -> Adressliste -> Neu	z. B. <i>Mitarbeiter-LAN-GW</i>
Adresse/Subnetz	Firewall -> Adressen -> Adressliste -> Neu	<i>10.0.1.1 / 255.255.255.255</i>
Beschreibung	Firewall -> Adressen -> Adressliste -> Neu	<i>Gast-LAN-GW</i>
Adresse/Subnetz	Firewall -> Adressen -> Adressliste -> Neu	<i>10.0.2.1 / 255.255.255.255</i>
Beschreibung	Firewall -> Adressen -> Adressliste -> Neu	<i>Mitarbeiter-WLAN-GW</i>
Adresse/Subnetz	Firewall -> Adressen -> Adressliste -> Neu	<i>10.0.10.1 / 255.255.255.255</i>
Beschreibung	Firewall -> Adressen -> Adressliste -> Neu	<i>Gast-WLAN-GW</i>
Adresse/Subnetz	Firewall -> Adressen -> Adressliste -> Neu	<i>10.0.20.1 / 255.255.255.255</i>

Gruppen definieren

Field	Menu	Value
Beschreibung	Firewall -> Schnittstellen -> IPv4-Gruppen -> Neu	Mitarbeiter
Mitglieder	Firewall -> Schnittstellen -> IPv4-Gruppen -> Neu	LAN_EN1-1, LEA-SED_EN1-0-1
Beschreibung	Firewall -> Schnittstellen -> IPv4-Gruppen -> Neu	Gast
Mitglieder	Firewall -> Schnittstellen -> IPv4-Gruppen -> Neu	LAN_EN1-2, LEA-SED_EN1-0-2
Beschreibung	Firewall -> Schnittstellen -> IPv4-Gruppen -> Neu	Benutzer
Mitglieder	Firewall -> Schnittstellen -> IPv4-Gruppen -> Neu	LAN_EN1-1, LAN_EN1-2, LEA-SED_EN1-0-1, LEA-SED_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	<i>any</i>
Aktion	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Zugriff</i>
Quelle	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Benutzer</i>
Ziel	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>LAN_EN1-4</i>
Dienst	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>any</i>
Aktion	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Zugriff</i>

Richtlinien erstellen (auf den Router gebundene IP-Adressen)

Field	Menu	Value
Quelle	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Benutzer</i>
Ziel	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Broadcast</i>
Dienst	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Lokale-Dienste</i>
Aktion	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Zugriff</i>
Quelle	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>LAN_EN1-1</i>
Ziel	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Mitarbeiter-LAN-GW</i>
Dienst	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Lokale-Dienste</i>
Aktion	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Zugriff</i>
Quelle	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>LAN_EN1-2</i>
Ziel	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Gast-LAN-GW</i>
Dienst	Firewall -> Richtlinien ->	<i>Lokale-Dienste</i>

Field	Menu	Value
	IPv4-Filterregeln -> Neu	
Aktion	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Zugriff</i>
Quelle	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>LEASED_EN1-0-1</i>
Ziel	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Mitarbeiter-WLAN-GW</i>
Dienst	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Lokale-Dienste</i>
Aktion	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Zugriff</i>
Quelle	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>LEASED_EN1-0-2</i>
Ziel	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Gast-WLAN-GW</i>
Dienst	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Lokale-Dienste</i>
Aktion	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Zugriff</i>

DHCP-Konfiguration

Field	Menu	Value
IP-Poolname	Lokale Dienste -> DHCP-Server -> IP-Pool-Konfiguration -> Neu	<i>z. B. Slave-APs</i>
IP-Adressbereich	Lokale Dienste -> DHCP-Server -> IP-Pool-Konfiguration -> Neu	<i>10.0.0.10 - 10.0.0.29</i>
Schnittstelle	Lokale Dienste -> DHCP-Server -> DHCP-Konfiguration -> Neu	<i>en1-0</i>
IP-Poolname	Lokale Dienste -> DHCP-Server -> DHCP-Konfiguration -> Neu	<i>z. B. Slave-APs</i>
Pool-Verwendung	Lokale Dienste -> DHCP-Server -> DHCP-Konfiguration -> Neu	<i>Lokal</i>
Gateway	Lokale Dienste -> DHCP-Server -> DHCP-Konfiguration -> Neu	<i>Router als Gateway verwenden</i>
DHCP-Optionen	Lokale Dienste -> DHCP-Server -> DHCP-Konfiguration -> Neu	<i>DNS-Server/ 10.0.0.1 und CAPWAP Controller/</i>

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	<i>Ein</i>
Aktives Funkmodulprofil	Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points	<i>2.4 GHz Radio Profile</i>
Kanal	Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points	<i>Auto</i>
Zugewiesene Drahtlosnetzwerke (VSS)	Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points	<i>vss-1: Mitarbeiter / vss-2: Gast</i>
Standort	Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points	<i>z. B. Küche</i>
Standort	Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points	<i>z. B. Terrasse</i>
Standort	Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points	<i>z. B. Flur zum Treppenhaus</i>
Standort	Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points	<i>z. B. Flurknick</i>
Standort	Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points	<i>z. B. Flurende</i>

Neue Kanalfestlegung

Field	Menu	Value
Neue Kanalfestlegung	Wireless LAN Controller -> Slave-AP-Konfiguration -> Slave Access Points	START

Kapitel 6 WLAN - Netzwerk mit Gäste-WLAN

6.1 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.

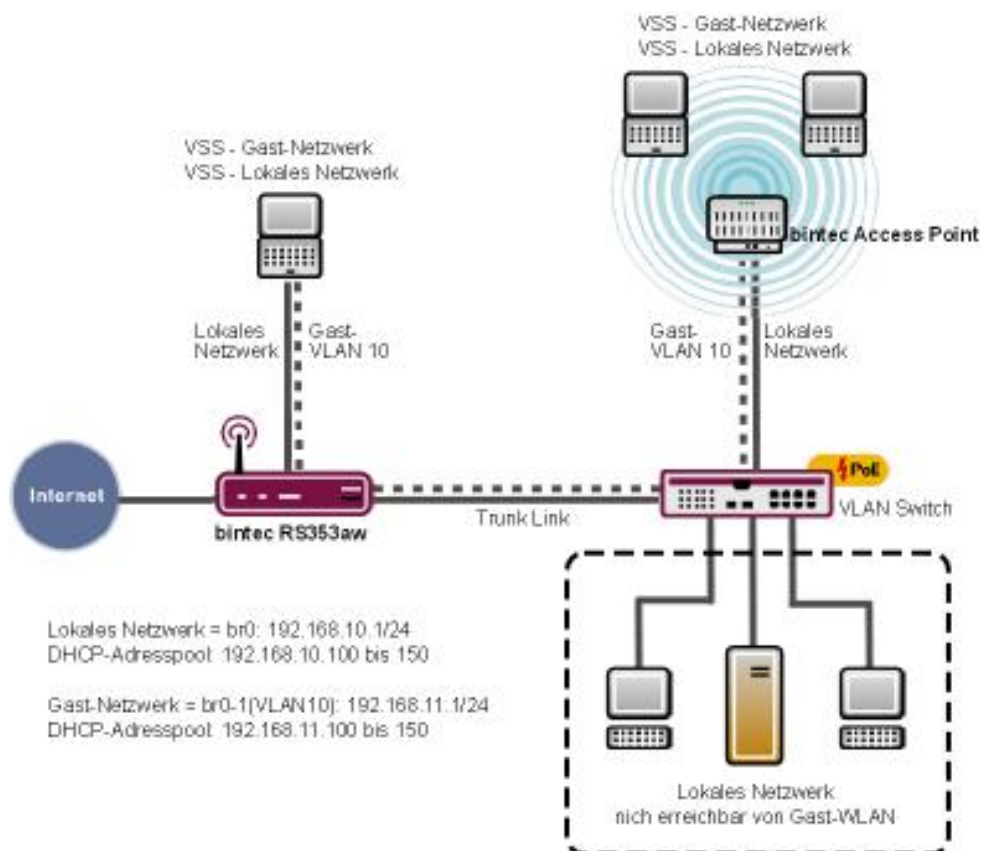


Abb. 112: Beispielszenario WLAN mit Gäste-WLAN



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
- Switch, die 802.1q VLAN unterstützen

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

6.2 Konfiguration

6.2.1 IP-Adresse konfigurieren

Konfigurieren Sie eine IP-Adresse auf der LAN-Schnittstelle.

Gehen Sie zu **LAN->IP-Konfiguration->Schnittstellen-><en1-0>->** 

The screenshot shows two panels of the configuration interface:

- Basisparameter:**
 - Schnittstellenmodus: Untagged Tagged (VLAN)
 - MAC-Adresse: Voreingestellte verwenden
- Grundlegende IPv4-Parameter:**
 - Sicherheitsrichtlinie: Nicht Vertrauenswürdig Vertrauenswürdig
 - Adressmodus: Statisch DHCP
 - IP-Adresse / Netzmaske:

IP-Adresse	Netzmaske
<input type="text" value="192.168.10.1"/>	<input type="text" value="255.255.255.0"/>
 - HINZUFÜGEN

Abb. 113: **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**.

6.2.2 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**.

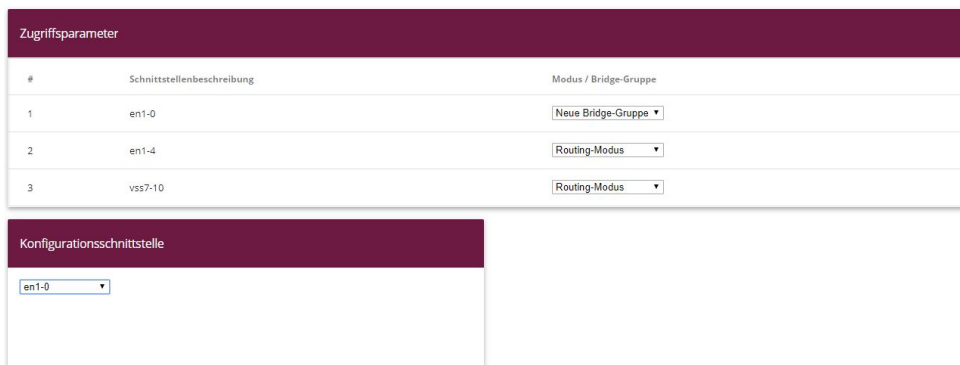



Abb. 114: **Systemverwaltung ->Schnittstellenmodus / Bridge-Gruppen->Schnittstellen**

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.

6.2.3 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**.

Grundeinstellungen	
Region	Germany ▼
Schnittstelle	BRIDGE_BR0 ▼
DHCP-Server	DHCP-Server mit aktivierter CAPWAP Option (138): <input type="radio"/> Extern oder statisch <input checked="" type="radio"/> Intern
IP-Adressbereich	192.168.10.100 - 192.168.10.150

Abb. 115: **Wireless LAN Controller->Wizard**

Gehen Sie folgendermaßen vor:

- (1) Wählen Sie das Land, in welchem der Wireless 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**.

6.2.4 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. 116: **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

VSS-Beschreibung	Netzwerkname (SSID)	Sicherheit
vss-1	default	WPA-PSK

HINZUFÜGEN

Abb. 117: **Wireless LAN Controller->Wizard**

Konfigurieren Sie den WLAN-Zugang zu Ihrem lokalen Netz. Klicken Sie dazu bei vss-1 auf das -Symbol.

Schritt 3

Service Set Parameter		Sicherheitseinstellungen	
Netzwerkname (SSID)	Lokales Netzwerk <input checked="" type="checkbox"/> Sichtbar	Sicherheitsmodus	WPA-PSK
IGMP Snooping	<input checked="" type="checkbox"/> Aktiviert	WPA-Modus	WPA 2
		Preshared Key	*****

Abb. 118: **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.

6.2.5 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 Switches 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 Switches müssen Sie selbst entsprechend konfigurieren.

Klicken Sie im **Wireless LAN Controller->Wizard** auf **Hinzufügen**.

Schritt 3

The screenshot shows three configuration panels for a Wireless LAN Controller:

- Service Set Parameter:**
 - Netzwerkname (SSID): Gaeste-Netzwerk (Visible)
 - IGMP Snooping: Aktiviert
- Sicherheitseinstellungen:**
 - Sicherheitsmodus: WPA-PSK
 - WPA-Modus: WPA 2
 - Preshared Key: [Redacted]
- VLAN:**
 - VLAN: Aktiviert
 - VLAN-ID: 10

Abb. 119: Wireless LAN Controller->Wizard->Hinzufügen

Gehen Sie folgendermaßen vor:

- (1) Geben Sie einen **Netzwerknamen (SSID)** für das Gästernetz 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**.



Hinweis

Wenn Sie verhindern wollen, dass im Gästernetz angemeldete Clients untereinander Daten austauschen können, deaktivieren Sie die Option **Intra-cell Repeating**. Wie Sie diese Art der Kommunikation auch in komplexeren Installationen unterbinden können, ist in einem Artikel der bintec-elmeg-Wissensdatenbank beschrieben: [Verbindungen zwischen WLAN-Clients verhindern](#).

Sie sehen das lokale Netz zusammen mit dem Gästernetz, das Sie soeben konfiguriert haben.

Drahtlosnetzwerke (VSS)		
VSS-Beschreibung	Netzwerkname (SSID)	Sicherheit
vss-1	Lokales Netzwerk	WPA-PSK
vss-2	Gaeste-Netzwerk	WPA-PSK

Abb. 120: Wireless LAN Controller->Wizard, mit konfiguriertem Gästernetz

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

Wireless LAN Controller Wizard

Manage
[Alle auswählen/](#)
[Alle deaktivieren](#)

	Standort	Gerät	IP-Adresse	LAN-MAC-Adresse	Drahtlosnetzwerk	Funkmodulprofil	Kanal	Status
<input type="checkbox"/>	1:	be.iP plus	192.168.0.251	Elmeqt_6f5e:7c	vss-1:Lokales Netzwerk vss-2:Gaeeste-Netzwerk	2.4 GHz Radio Profile	0	Gefunden
<input type="checkbox"/>	2:	W2003ac	192.168.0.100	BintecCo_48:69:c1	vss-1:Lokales Netzwerk vss-2:Gaeeste-Netzwerk	2.4 GHz Radio Profile 5 GHz Radio Profile	0	Gefunden

Fertig! Um nun die automatische Installation zu starten, wählen Sie die gewünschten managed Access Points aus und klicken Sie START. Die Funkkanäle werden automatisch ausgewählt. Dieses kann bis zu 10 Minuten dauern.

Abb. 121: Wireless LAN Controller->Wizard

6.2.6 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.

Slave Access Points

Standort	Gerät	IP-Adresse	LAN-MAC-Adresse	Drahtlosnetzwerk-Profil	Funkmodulprofil	Kanal	Status
1:	be.iP plus	192.168.0.251	Elmeqt_6f5e:7c	vss-1:Lokales Netzwerk vss-2:Gaeeste-Netzwerk	2.4 GHz Radio Profile	6	Managed
2:	W2003ac	192.168.0.100	BintecCo_48:69:c1	vss-1:Lokales Netzwerk vss-2:Gaeeste-Netzwerk	2.4 GHz Radio Profile 5 GHz Radio Profile	11 36	Managed

Die WLAN-Controller Installation ist abgeschlossen.

Bitte speichern Sie die Konfiguration mit der Schaltfläche „Konfiguration speichern“.

Abb. 122: Wireless LAN Controller->Wizard

6.2.7 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.**

The screenshot shows two configuration panels side-by-side. The left panel, titled 'Basisparameter', has a dropdown menu for 'Basierend auf Ethernet-Schnittstelle' set to 'br0'. Below it, 'Schnittstellenmodus' has radio buttons for 'Untagged' and 'Tagged (VLAN)', with 'Tagged (VLAN)' selected. The 'VLAN-ID' field contains the number '10'. The 'MAC-Adresse' field contains '00:a0:f9' and there is a toggle switch for 'Voreingestellte verwenden' which is turned off. The right panel, titled 'Grundlegende IPv4-Parameter', has a 'Sicherheitsrichtlinie' section with radio buttons for 'Nicht Vertrauenswürdig' (selected) and 'Vertrauenswürdig'. Below that, 'Adressmodus' has radio buttons for 'Statisch' (selected) and 'DHCP'. The 'IP-Adresse / Netzmaske' section contains two input fields: 'IP-Adresse' with '192.168.11.1' and 'Netzmaske' with '255.255.255.0'. A trash icon is next to the netmask field. At the bottom of this panel is a 'HINZUFÜGEN' button.

Abb. 123: 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.












Ethernet-/VLAN-Ports				
Schnittstelle	IPv4-Adresse/Netzmaske	IPv6-Adresse/Länge	Status	Aktion
en1-4	192.168.4.251/255.255.255.0	-	✖	^ v  
efm35-60	Nicht konfiguriert/Nicht konfiguriert	-	✖	^ v  
ethoa35-5	Nicht konfiguriert/Nicht konfiguriert	-	✖	^ v  
br0(VLAN-ID1)	192.168.10.1/255.255.255.0	-	✔	^ v  
br0-1(VLAN-ID10)	192.168.11.1/255.255.255.0	-	✔	  

Abb. 124: LAN->IP-Konfiguration->Schnittstellen->Neu

6.2.8 IP-Adressbereich für das Gästernetz einrichten

Konfigurieren Sie einen IP-Adressbereich für die IP-Adressvergabe an WLAN-Clients im Gästernetz. Dieser IP-Adressbereich 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**.

Basisparameter

IP-Poolname
Gast-Adress-Pool

IP-Adressbereich
192.168.11.100 - 192.168.11.150

DNS-Server

Primär

Sekundär

Abb. 125: 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.

IP-Poolname	IP-Adressbereich	Primärer DNS-Server	Sekundärer DNS-Server	
Gast-Adress-Pool	192.168.11.100 - 192.168.11.150	0.0.0.0	0.0.0.0	🗑️ ✎
	192.168.10.100 - 192.168.10.150	0.0.0.0	0.0.0.0	🗑️ ✎

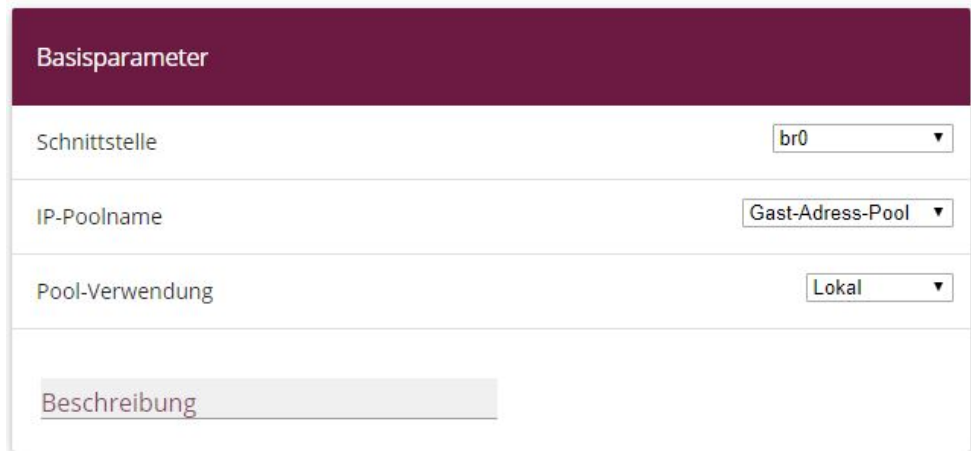
Abb. 126: Lokale Dienste->DHCP-Server->IP-Pool-Konfiguration

6.2.9 DHCP-Verwendung konfigurieren

Konfigurieren Sie die Verwendung von DHCP für WLAN-Clients im Gästernetz.

Gehen Sie in folgendes Menü:

Gehen Sie zu **Lokale Dienste->DHCP-Server->DHCP-Konfiguration->Neu.**



The screenshot shows a form titled 'Basisparameter' with the following fields:

- Schnittstelle:** A dropdown menu with 'br0' selected.
- IP-Poolname:** A dropdown menu with 'Gast-Adress-Pool' selected.
- Pool-Verwendung:** A dropdown menu with 'Lokal' selected.
- Beschreibung:** A text input field that is currently empty.

Abb. 127: **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.



The screenshot shows a table titled 'DHCP-Server:' with the following columns: Schnittstelle, IP-Poolname, Gateway, LeaseTime, and Status. There are two rows of data:

Schnittstelle	IP-Poolname	Gateway	LeaseTime	Status	
br0-1	Gast-Adress-Pool	Router als Gateway verwenden	120Min.	<input checked="" type="checkbox"/> Aktiviert	 
br0		Router als Gateway verwenden	120Min.	<input checked="" type="checkbox"/> Aktiviert	 

Abb. 128: **Lokale Dienste->DHCP-Server->DHCP-Konfiguration**

6.2.10 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.

Basisparameter	
Beschreibung	Vertrauenswürdige Schnittstellen
Mitglieder	
Schnittstelle	Vertrauenswürdige
LAN_EN1-4	<input type="checkbox"/>
WAN_ETHOA35-5	<input type="checkbox"/>
efm35-60	<input type="checkbox"/>
BRIDGE_BR0	<input checked="" type="checkbox"/>
BRIDGE_BR0-1	<input type="checkbox"/>

Abb. 129: **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**.

Basisparameter

Beschreibung

Mitglieder

Dienst	Auswahl
activity	<input type="checkbox"/>
ah	<input type="checkbox"/>
any	<input type="checkbox"/>
dhcpc	<input checked="" type="checkbox"/>
discard	<input type="checkbox"/>
dns	<input checked="" type="checkbox"/>
echo-req	<input checked="" type="checkbox"/>
echo-req-ipv6	<input type="checkbox"/>
esp	<input type="checkbox"/>

Abb. 130: 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. *dhcpc*, *dns* und *echo-req*.
- (3) Bestätigen Sie Ihre Eingaben mit **OK**.

Die konfigurierte Service-Gruppe wird angezeigt.



Gruppen			
Beschreibung	Mitglieder		
Gast-Lokal Zugriff	echo-req, dns, dhcp		

Abb. 131: 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**.

Basisparameter	
Quelle	BRIDGE_BR0-1 ▼
Ziel	LOCAL ▼
Dienst	Gast-Lokal-Zugriff ▼
Aktion	Zugriff ▼

Abb. 132: 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.

Filterregeln						
Abfolge	Quelle	Ziel	WAN_INTERNET	Dienst	Aktion	Richtlinie aktiv
1	BRIDGE_BR0-1	LOCAL		Gast-Lokal Zugriff	Zugriff	<input checked="" type="checkbox"/> Aktiviert
2	BRIDGE_BR0-1	WAN_INTERNET		any	Zugriff	<input checked="" type="checkbox"/> Aktiviert

Standardfilterregeln						
Abfolge	Quelle	Ziel	Dienst	Aktion	Richtlinie aktiv	
n+1	Vertrauenswürdige Schnittstellen	Beliebig	Beliebig	Zugriff	<input checked="" type="checkbox"/> Aktiviert	
n+2	Nicht vertrauenswürdige Schnittstellen	Beliebig	Beliebig	Verweigern	<input checked="" type="checkbox"/> Aktiviert	

Abb. 133: 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**.

Globale Firewall-Optionen	Sitzungstimer
Status der IPv4-Firewall <input checked="" type="checkbox"/> Aktiviert	UDP-Inaktivität: 180 Sekunden
Protokollierte Aktionen: Alle	TCP-Inaktivität: 3600 Sekunden
Vollständige IPv4-Filterung <input checked="" type="checkbox"/> Aktivieren	PPTP-Inaktivität: 86400 Sekunden
STUN Handler <input type="checkbox"/>	Andere Inaktivität: 30 Sekunden

Abb. 134: Firewall->Richtlinien->Optionen

Gehen Sie folgendermaßen vor:



- (1) Aktivieren Sie den **Status der IPv4-Firewall**.
- (2) Bestätigen Sie Ihre Eingaben mit **OK**.

6.3 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.

6.4 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	<i>br0</i>
Schnittstellenmodus	LAN ->IP-Konfiguration-> Schnittstellen-> Neu	<i>Tagged (VLAN)</i>
VLAN-ID	LAN-> IP-Konfiguration-> Schnittstellen ->Neu	<i>10</i>
Sicherheitsrichtlinie	LAN ->IP-Konfiguration-> Schnittstellen ->Neu	<i>Nicht Vertrauenswürdig</i>
Adressmodus	LAN ->IP-Konfiguration-> Schnittstellen ->Neu	<i>Statisch</i>
IP-Adresse / Netzmaske	LAN-> IP-Konfiguration-> Schnittstellen ->Neu	<i>192.168.11.1 / 255.255.255.0</i>

IP-Adressbereich für das Gästernetz einrichten

Feld	Menü	Wert
IP-Poolname	Lokale Dienste ->DHCP-Server ->IP-Pool-Konfiguration ->Neu	<i>Gast-Adress-Pool</i>
IP-Adressbereich	Lokale Dienste ->DHCP-Server-> IP-Pool-Konfiguration -> Neu	<i>z. B. 192.168.11.100 - 192.168.11.150</i>

DHCP-Verwendung konfigurieren

Feld	Menü	Wert
Schnittstelle	Lokale Dienste ->DHCP-Server ->DHCP-Konfiguration-> Neu	<i>br0-1</i>
IP-Poolname	Lokale Dienste ->DHCP-Server-> DHCP-Konfiguration ->Neu	<i>Gast-Adress-Pool</i>
Pool-Verwendung	Lokale Dienste-> DHCP-Server ->DHCP-Konfiguration ->Neu	<i>Lokal</i>

Firewall einrichten

Feld	Menü	Wert
BRIDGE_BR0	Firewall ->Richtlinien-> IPv4-Filterregeln ->Standardfilterregeln-> 	Vertrauenswürdig <i>Aktiviert</i>
Beschreibung	Firewall ->Dienste ->Gruppen ->Neu	<i>z. B. Gast-Lokal-Zugriff</i>
Mitglieder	Firewall ->Dienste ->Gruppen ->Neu	<i>z. B. dhcp, dns und echo-req</i>

Feld	Menü	Wert
Quelle	Firewall ->Richtlinien ->IPv4-Filterregeln -> Neu	<i>BRIDGE_BR0-1</i>
Ziel	Firewall ->Richtlinien ->IPv4-Filterregeln ->Neu	<i>LOCAL</i>
Dienst	Firewall ->Richtlinien ->IPv4-Filterregeln ->Neu	<i>Gast-Lokal-Zugriff</i>
Aktion	Firewall ->Richtlinien ->IPv4-Filterregeln ->Neu	<i>Zugriff</i>
Quelle	Firewall ->Richtlinien ->IPv4-Filterregeln ->Neu	<i>BRIDGE_BR0-1</i>
Ziel	Firewall ->Richtlinien ->IPv4-Filterregeln ->Neu	<i>WAN_INTERNET</i>
Dienst	Firewall ->Richtlinien ->IPv4-Filterregeln ->Neu	z. B. <i>any</i>
Aktion	Firewall ->Richtlinien ->IPv4-Filterregeln ->Neu	<i>Zugriff</i>
Status der IPv4-Firewall	Firewall ->Richtlinien ->Optionen	<i>Aktiviert</i>

Kapitel 7 VLAN-Einrichtung ESW4000-Switche

Die Ports der **ESW4000**-Switch-Serie sind im Auslieferungszustand 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.

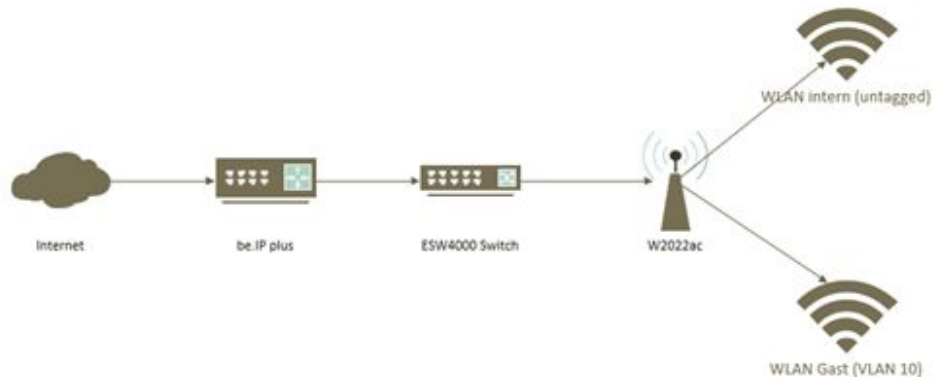


Abb. 135: Aufbaubauspiel

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

7.1 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 158 oder auf unserer Homepage unter: <https://www.bintec-elmeg.com/mc/workshops/anwendungs-workshops/>

7.2 Einrichtung am Switch ESW4000

Öffnen Sie einen Webbrowser und geben Sie die Standard-IP-Adresse `192.168.2.10` in das Adressfeld ein.



The image shows the login page of the ESW4000 switch. At the top, there is a dark blue header with a hummingbird logo and the text "esw 4000". Below the header, there are two input fields: "Username" and "Password", both containing the text "admin". A "Login" button is positioned below the password field.

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**.

VLAN > Static

Action:

VLAN ID (1-4094) -

Status Enabled

Remote VLAN Enabled

- (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.

VLAN > Static

Action:

Interface Port Trunk

Mode

PVID

Acceptable Frame Type

Ingress Filtering Enabled

Static VLAN Membership List Total: 2

VLAN	Membership Type			
	Tagged	Untagged	Forbidden	None
1	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
10	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- (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.

VLAN > Static

Action: Edit Member by Interface

Interface: Port 8 Trunk

Mode: Hybrid

PVID: 1

Acceptable Frame Type: All

Ingress Filtering: Enabled

Static VLAN Membership List Total 2

VLAN	Membership Type			
	Tagged	Untagged	Forbidden	None
1	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
10	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Apply Revert

- (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.

Action: Edit Member by VLAN

VLAN: 10

Interface: Port Trunk

Static VLAN Port Member List Total 12

Port	Mode	PVID (1-4094)	Acceptable Frame Type	Ingress Filtering	Membership Type			
					Tagged	Untagged	Forbidden	None
1	Hybrid	1	All	<input checked="" type="checkbox"/> Enabled	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2	Hybrid	1	All	<input checked="" type="checkbox"/> Enabled	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
3	Hybrid	1	All	<input checked="" type="checkbox"/> Enabled	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
4	Hybrid	1	All	<input checked="" type="checkbox"/> Enabled	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
5	Hybrid	1	All	<input checked="" type="checkbox"/> Enabled	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
6	Hybrid	1	All	<input checked="" type="checkbox"/> Enabled	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
7	Hybrid	1	All	<input checked="" type="checkbox"/> Enabled	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
8	Hybrid	1	All	<input checked="" type="checkbox"/> Enabled	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
9	Hybrid	1	All	<input checked="" type="checkbox"/> Enabled	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

In der Übersicht **Statische VLAN-Port-Mitgliederliste** sind alle vorhandenen VLAN-Mitglieder aufgelistet.

Hier können Sie die **Eingangsfiltrierung** aktivieren/deaktivieren, sowie die **Art der Mitgliedschaft** festlegen.

Kapitel 8 WLAN - WLAN-Controller-Installation mit integrierter HotSpot-Funktionalität

8.1 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.

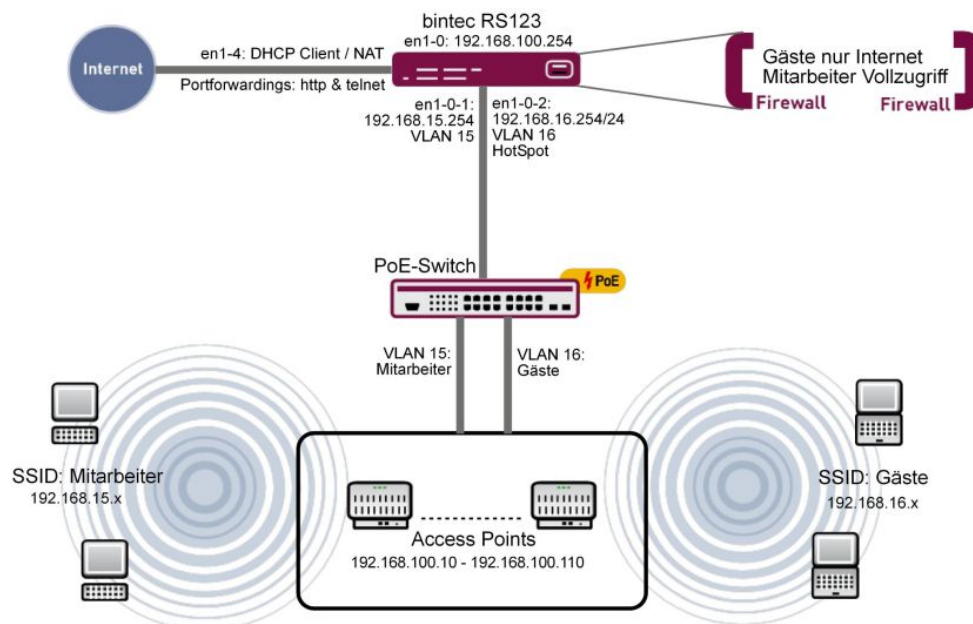


Abb. 141: Beispielszenario

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

8.2 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.

8.3 Konfiguration

8.3.1 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.

8.3.2 LAN-Konfiguration

Ändern Sie zuerst in Menü **IP-Konfiguration** die IP-Adresse.


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



Abb. 142: **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. 143: **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.

Ethernet-/VLAN-Ports					
Schnittstelle	IPv4-Adresse/Netzmaske	IPv6-Adresse/Länge	Status	Aktion	
en1-0	192.168.100.254/255.255.255.0	-	✓	^	∨
en1-4	Nicht konfiguriert/Nicht konfiguriert	-	✗	^	∨
en1-0-1(VLAN-ID15)	192.168.15.254/255.255.255.0	-	✓	^	∨
en1-0-2(VLAN-ID16)	192.168.16.254/255.255.255.0	-	✓	^	∨

Abb. 144: LAN -> IP-Konfiguration -> Schnittstellen

8.3.3 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**.

Basisparameter

Authentifizierungstyp	Accounting ▼
Betreibermodus	bintec HotSpot Server ▼
Server-IP-Adresse	62.245.165.180
RADIUS-Passwort	••••••
Standard-Benutzerpasswort	••••••
Priorität	0 ▼
Eintrag aktiv	<input checked="" type="checkbox"/> Aktiviert
Gruppenbeschreibung	Standardgruppe 0 ▼

Abb. 145: **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:

RADIUS-Parameter						
Authentifizierungstyp	Server-IP-Adresse	Richtlinie	Priorität	Aktiviert	Status	
Accounting	62.245.165.180	Verbindlich	0	<input checked="" type="checkbox"/>	✓	 
Login-Authentifizierung	62.245.165.180	Nicht verbindlich	0	<input checked="" type="checkbox"/>	✓	 

Abb. 146: **Systemverwaltung -> Remote Authentifizierung -> RADIUS**

Im nächsten Schritt wird ein Hotspot-Netzwerk eingerichtet.

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

Basisparameter

Schnittstelle LAN_EN1-0 ▾

Domäne am Hotspot-Server

Walled Garden Aktiviert

Walled Network / Netzmaske Aktiviert
 /

Walled Garden URL

Geschäftsbedingungen

Zusätzliche, frei zugängliche Domänennamen

HINZUFÜGEN

Sprache für Anmeldefenster English ▾

Abb. 147: Lokale Dienste -> Hotspot-Gateway -> Hotspot-Gateway -> Neu

Gehen Sie folgendermaßen vor:

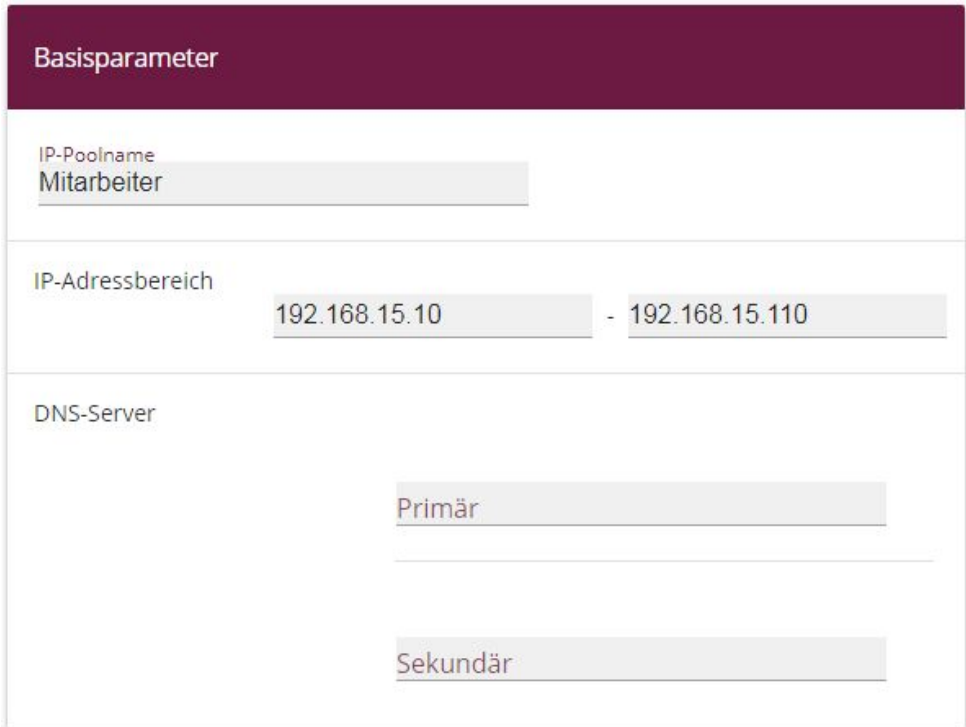
- (1) Wählen Sie die **Schnittstelle** `LAN_EN1-0` aus. Diese korrespondiert später mit der **SSID** `Gäste`.

- (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**.

8.3.4 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.



The screenshot shows a configuration window titled "Basisparameter" (Basic Parameters) for a DHCP server. It contains three main sections:

- IP-Poolname:** A text input field containing the value "Mitarbeiter".
- IP-Adressbereich:** Two text input fields separated by a hyphen. The first field contains "192.168.15.10" and the second field contains "192.168.15.110".
- DNS-Server:** Two text input fields. The top field is labeled "Primär" (Primary) and the bottom field is labeled "Sekundär" (Secondary). Both fields are currently empty.

Abb. 148: **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.

The screenshot shows a configuration window titled 'Basisparameter'. It contains three dropdown menus: 'Schnittstelle' with the value 'en1-0-1', 'IP-Poolname' with the value 'Mitarbeiter', and 'Pool-Verwendung' with the value 'Lokal'. Below these is a text input field labeled 'description'.

Abb. 149: **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:

DHCP-Server:					
Schnittstelle	IP-Poolname	Gateway	Lease Time	Status	
en1-0-2	Gaeste	Router als Gateway verwenden	120Min.	<input checked="" type="checkbox"/> Aktiviert	
en1-0-1	Mitarbeiter	Router als Gateway verwenden	120Min.	<input checked="" type="checkbox"/> Aktiviert	

Abb. 150: Lokale Dienste -> DHCP-Server -> DHCP-Konfiguration

8.3.5 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**.

Grundeinstellungen

Region Germany ▼

Schnittstelle LAN_EN1-0 ▼

DHCP-Server DHCP-Server mit aktivierter CAPWAP Option (138):
 Extern oder statisch
 Intern

IP-Adressbereich 192.168.100.10 - 192.168.100.110

Wenn Sie Ihre Access Points bereits mit dem WLAN Controller verbunden haben, müssen Sie die Access Points nun zurücksetzen.

Die ausgewählte Schnittstelle ist keine Bridge-Schnittstelle. Das integrierte WLAN-Modul kann nicht vom Wireless LAN Controller verwaltet werden.

Abb. 151: 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.



Wählen Sie das Funkmodulprofil aus

Zwei unabhängige Funkmodulprofile verwenden

Funkmodulprofil 2.4 GHz Radio Profile ▾

Abb. 152: **Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard**

Klicken Sie auf **Weiter**.

Im nächsten Schritt definieren Sie die SSID, die später ausgeliefert werden soll.

The screenshot shows the configuration interface for a wireless LAN controller. It is divided into three main sections:

- Service Set Parameter:**
 - Netzwerkname (SSID): Mitarbeiter (Visible)
 - IGMP Snooping: Aktiviert
- VLAN:**
 - VLAN: Aktiviert
 - VLAN-ID: 15
- Sicherheitseinstellungen:**
 - Sicherheitsmodus: WPA-PSK
 - WPA-Modus: WPA 2
 - Preshared Key: [Redacted]

Abb. 153: 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.

The screenshot shows the configuration interface for a second wireless LAN controller. It is divided into three main sections:

- Service Set Parameter:**
 - Netzwerkname (SSID): Gaeste (Visible)
 - IGMP Snooping: Aktiviert
- VLAN:**
 - VLAN: Aktiviert
 - VLAN-ID: 16
- Sicherheitseinstellungen:**
 - Sicherheitsmodus: Inaktiv

Abb. 154: 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.

Wireless LAN Controller Wizard

Manage
[Alle auswählen/](#)
[Alle deaktivieren](#)

	Standort	Gerät	IP-Adresse	LAN-MAC-Adresse	Drahtlosnetzwerk	Funkmodulprofil	Kanal	Status	
<input checked="" type="checkbox"/>	1:	bintec W1002n	192.168.100.11	00:01:cd:0e:97:c4	vss-1:Mitarbeiter vss-2:Gaeste	2.4 GHz Radio Profile	0	Gefunden	

Fertig! Um nun die automatische Installation zu starten, wählen Sie die gewünschten managed Access Points aus und klicken Sie START. Die Funkkanäle werden automatisch ausgewählt. Dieses kann bis zu 10 Minuten dauern.

Abb. 155: **Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard**

Um die Einstellungen eines gefundenen APs zu ändern, klicken Sie im entsprechenden Eintrag auf .

Abb. 156: **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.

Wireless LAN Controller Wizard							
Standort	Gerät	IP-Adresse	LAN-MAC-Adresse	Drahtlosnetzwerk-Profil	Funkmodulprofil	Kanal	Status
1:Office	bintec W1002n	192.168.100.11	00:01:cd:0e:97:c4	vss-1:Mitarbeiter vss-2:Gaeste	2.4 GHz Radio Profile	11	Managed

Abb. 157: **Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard**

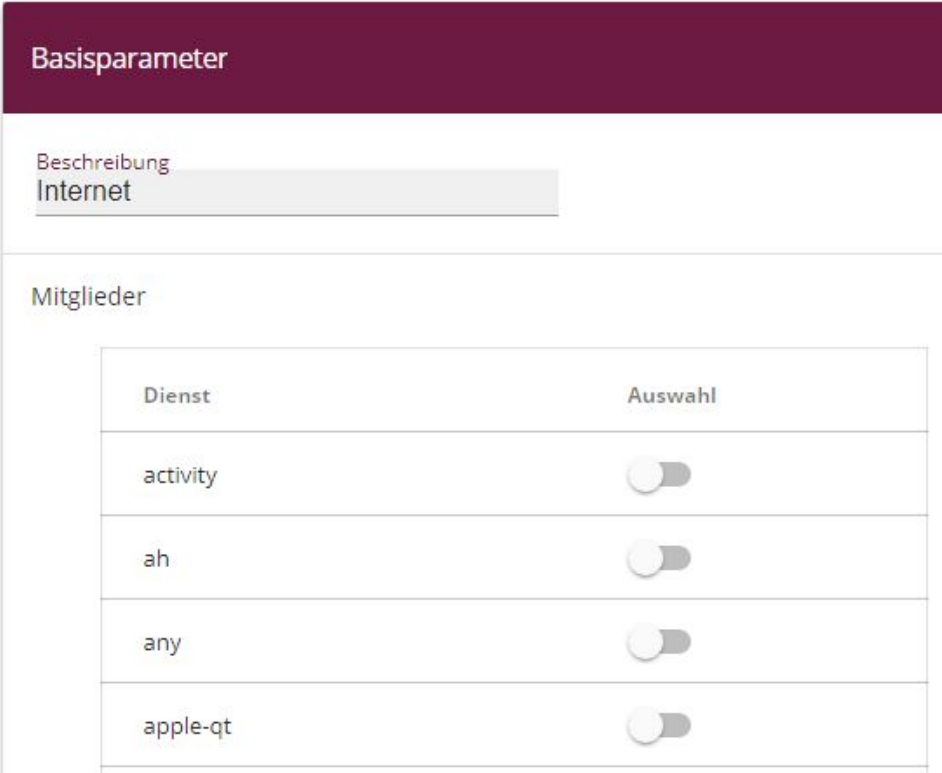
Damit Ihre *Gäste* nur das Internet nutzen können, aber keinen Zugriff auf Ihre anderen Netzwerkkomponenten erhalten, ist es notwendig Firewall Regeln hinzuzufügen. Hier ein Beispiel einer einfachen Firewall Regel, um den *Gästen* den Zugriff auf das interne Netz zu verbieten.

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**.



The screenshot shows a configuration window titled "Basisparameter". Under "Beschreibung", the text "Internet" is entered. Below this is a section titled "Mitglieder" containing a table with two columns: "Dienst" and "Auswahl".

Dienst	Auswahl
activity	<input type="checkbox"/>
ah	<input type="checkbox"/>
any	<input type="checkbox"/>
apple-qt	<input type="checkbox"/>

Abb. 158: **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:

Gruppen		
Beschreibung	Mitglieder	
Internet	http, http (SSL), echo-req, ftp, ssh, dns, pop3, pop3 (SSL), imap, imap (SSL), snmp, imap3, ip-sec, sip	 
lokale dienste	echo-req, dns, dhcp, http, http (SSL), ntp	 

Abb. 159: 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**.

Basisparameter	
Quelle	LEASED_EN1-0-1 ▼
Ziel	LOCAL ▼
Dienst	lokale dienste ▼
Aktion	Zugriff ▼

Abb. 160: 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:

Filterregeln							
Abfolge	Quelle	Ziel	Dienst	Aktion	Richtlinie aktiv	LEASED_EN1-0-1	LEASED_EN1-0-2
1	LEASED_EN1-0-1	LOCAL	lokale dienste	Zugriff	<input checked="" type="checkbox"/> Aktiviert	Verweigern	↓ ≡ 🗑️
2	LEASED_EN1-0-2	LOCAL	lokale dienste	Zugriff	<input checked="" type="checkbox"/> Aktiviert		↑ ≡ 🗑️

Abb. 161: 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.

8.4 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. <i>Mitarbeiter</i>
Poolverwendung	Lokale Dienste -> DHCP-Server -> DHCP-Konfiguration -> Neu	<i>Lokal</i>
IP-Poolname	Lokale Dienste -> DHCP-Server -> IP-Pool-Konfiguration -> Neu	z. B. <i>Gäste</i>
IP-Adressbereich	Lokale Dienste -> DHCP-Server -> IP-Pool-Konfiguration -> Neu	z. B. <i>192.168.16.10 - 192.168.16.110</i>
Schnittstelle	Lokale Dienste -> DHCP-Server -> DHCP-Konfiguration -> Neu	<i>en1-0-2</i>
IP-Poolname	Lokale Dienste -> DHCP-Server -> DHCP-Konfiguration -> Neu	z. B. <i>Gäste</i>
Poolverwendung	Lokale Dienste -> DHCP-Server -> DHCP-Konfiguration -> Neu	<i>Lokal</i>

WLAN Controller Wizard

Feld	Menü	Wert
Region	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard	<i>Germany</i>
Schnittstelle	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard	<i>LAN_EN1-0</i>
DHCP-Server	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard	<i>Intern</i>
IP-Adressbereich	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard	z. B. <i>192.168.100.10 - 192.168.100.110</i>
Funkmodulprofil	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard -> Weiter	<i>2,4 GHz Radio Profile</i>
Netzwerkname (SSID)	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard -> Weiter	z. B. <i>Mitarbeiter</i>
Sicherheitsmodus	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard -> Weiter	<i>WPA-PSK</i>
WPA-Modus	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard -> Weiter	<i>WPA2</i>
Preshared Key	Wireless LAN Controller -> Wizard	z. B. <i>supersecret</i>

Feld	Menü	Wert
	-> Wireless LAN Controller Wizard -> Weiter	
VLAN	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard -> Weiter	<i>Aktiviert</i>
VLAN-ID	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard -> Weiter	<i>15</i>
Netzwerkname (SSID)	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard -> Weiter -> Hinzufügen	<i>z. B. Gäste</i>
Sicherheitsmodus	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard -> Weiter -> Hinzufügen	<i>Inaktiv</i>
VLAN	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard -> Weiter -> Hinzufügen	<i>Aktiviert</i>
VLAN-ID	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard -> Weiter -> Hinzufügen	<i>16</i>
Standort	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard -> Weiter ✎	<i>z. B. 1:Office</i>
Aktives Funkmodulprofil	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard -> Weiter ✎	<i>2,4 GHz Radio Profile</i>
Zugewiesene Drahtlosnetzwerke (VSS)	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard -> Weiter ✎	<i>z. B. vss-1:Mitarbeiter und vss-2:Gäste</i>

Firewall Regeln hinzufügen

Feld	Menü	Wert
Beschreibung	Firewall -> Dienste -> Gruppen -> Neu	<i>z. B. Internet</i>
Mitglieder	Firewall -> Dienste -> Gruppen -> Neu	<i>z. B. http, http (SSL)</i>
Beschreibung	Firewall -> Dienste -> Gruppen -> Neu	<i>z. B. lokale Dienste</i>

Feld	Menü	Wert
Mitglieder	Firewall -> Dienste -> Gruppen -> Neu	z. B. <i>http, http (SSL)</i>

Lokale Dienste einschränken

Feld	Menü	Wert
Quelle	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>LEASED_EN1-0-1</i>
Ziel	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>LOCAL</i>
Dienst	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>lokale dienste</i>
Aktion	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>Zugriff</i>
Quelle	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>LEASED_EN1-0-2</i>
Ziel	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>LOCAL</i>
Dienst	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>lokale dienste</i>
Aktion	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>Zugriff</i>
Quelle	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>LAN_EN1-0-1</i>
Ziel	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>LAN_EN1-0-1</i>
Dienst	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>any</i>
Aktion	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>Verweigern</i>
Quelle	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>LAN_EN1-0-2</i>
Ziel	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>LAN_EN1-0-2</i>
Dienst	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>any</i>
Aktion	Firewall -> Richtlinien -> Filterregeln -> Neu	<i>Verweigern</i>

Kapitel 9 WLAN - Cloud NetManager

9.1 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

9.2 Erste Schritte im Portal

9.2.1 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.

Online-Registrierung

Unternehmen

Name des Unternehmens	<input type="text" value="Firma_1"/>	Street	<input type="text" value="Südwestpark 94"/>
Postleitzahl	<input type="text" value="90449"/>	Stadt	<input type="text" value="Nürnberg"/>
		Land	<input type="text" value="Deutschland"/>
Partnernummer (bintec elmeg)	<input type="text"/>		

Benutzerkonto

Vorname	<input type="text" value="Max"/>	Nachname	<input type="text" value="Mustermann"/>	Telefon	<input type="text" value="091196731234"/>
E-Mail-Adresse	<input type="text" value="m-muster@firma.com"/>		Anmeldung (Standard ist Ihre E-Mail-Adresse)	<input type="text"/>	

Zustimmungserklärung zur Datenverwendung

Hereby I agree that the entered personal data will be used for administrative and technical realization of the requested Cloud NetManager account. I am aware that I may receive emails to the given email address or that I may be contacted via other channels within the specified purpose. To disconfirm this agreement or to get more information about the utilization of the given data, I could contact datenschutz@bintec-elmeg.com. Furthermore, the data protection statement of bintec elmeg

Der Einverständniserklärung zur Datenverwendung zustimmen

Wenn Sie sich registrieren, wird Ihnen ein Link zum Setzen eines Passworts an die obige E-Mail-Adresse gesendet. Wenn Sie ein Passwort gesetzt haben, ist die Registrierung abgeschlossen.

Abb. 162: 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.

9.2.2 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.

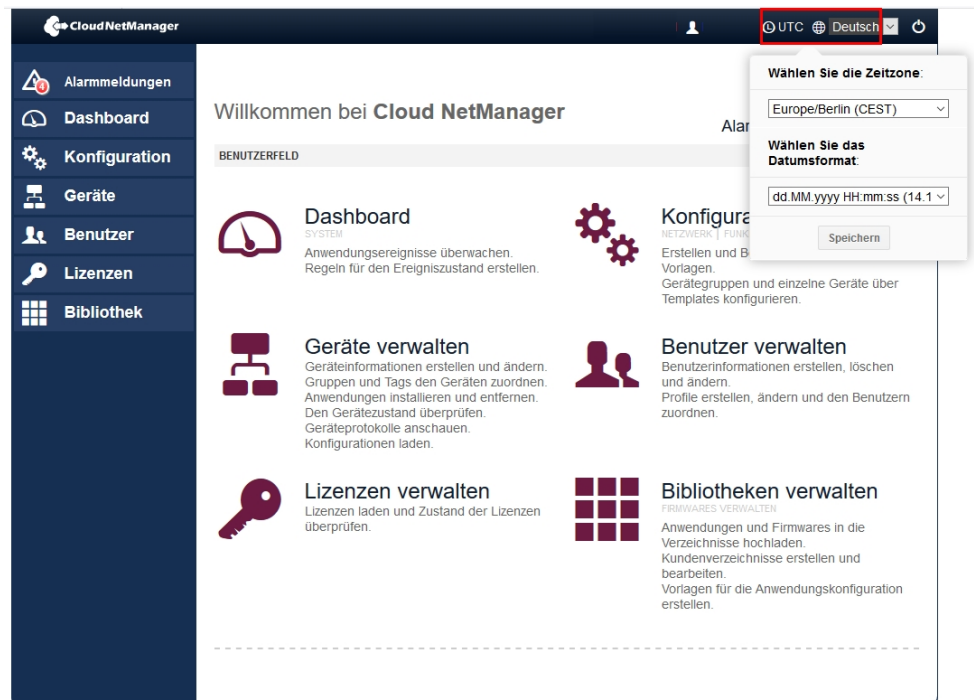


Abb. 163: Ändern der Zeitzone

9.2.3 Einspielen der Lizenzen

Gehen Sie auf der Statusseite in das Menü **Lizenzen->Lizenzen für diesen cloud Server->Neue Lizenz**.



Abb. 164: 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.

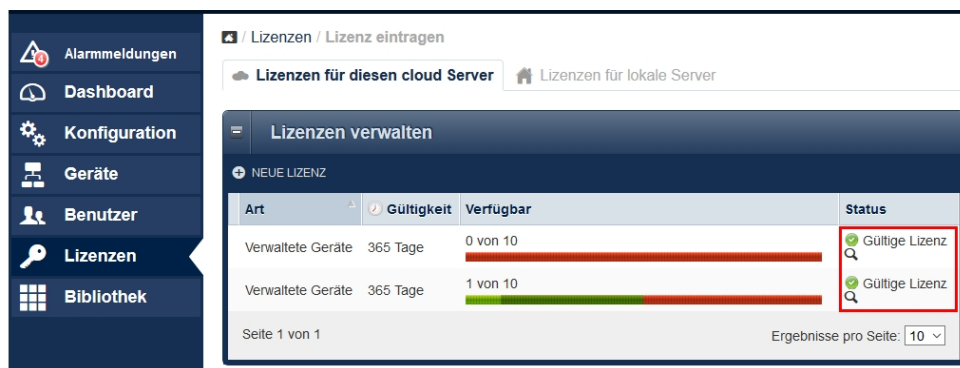


Abb. 165: Übersicht

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**.

Datum der Zuordnung	Ablaufdatum	Tage	Seriennr.	Name
2016-07-11 15:22:07	2017-07-11 15:22:07	0 Tage		
2016-08-26 07:42:45	2015-02-10 07:38:07	0 Tage	RNGDAG013120007	bei SE
2017-02-21 10:12:02	2016-02-03 12:36:41	0 Tage	RNEDDB012480097	W1003n
2017-03-07 20:43:59	2018-03-07 20:43:59	0 Tage	RN08AAC16070002	W2003ac
2018-05-04 15:04:06	2017-08-08 19:56:13	0 Tage	RN08AAC16070002	W2003ac
2019-03-12 08:25:29	2019-10-17 10:22:29	154 Tage	RN08AAD16040087	W2003ac-ext
2019-03-12 08:26:46	2020-03-11 08:26:46	300 Tage	RN08AAC16040003	W2003ax
2019-03-12 08:36:20	2020-03-11 08:36:20	300 Tage	RNEDDC012500136	W1003n
2019-03-12 08:44:39	2020-03-11 08:44:39	300 Tage	RN08BCC16200090	W2003ac-17

Seite 1 von 1 Ergebnisse pro Seite: 10

Abb. 166: Geräte, die der Lizenz zugeordnet sind

9.3 Anlegen der Profile

9.3.1 Anlegen der Netzwerkprofile (SSID)

Mindestens ein Netzwerkprofil (SSID) muss angelegt werden.

Gehen Sie dazu in das Menü **Konfiguration->Netzwerk**.

Klicken Sie auf **Neues Netzwerkprofil**.

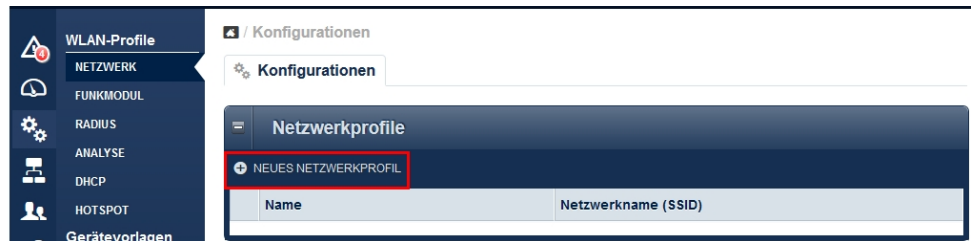


Abb. 167: Netzwerkprofile

Neues Netzwerkprofil Optionale Funktionen ✨

Profilname*

SERVICE-SET-PARAMETER

Netzwerkname (SSID)

Versteckt

Client isolation

ARP-Verarbeitung

WMM

SICHERHEITSEINSTELLUNGEN

Sicherheitsmodus

CLIENT-LASTVERTEILUNG

Max. Anzahl der Clients - Hard Limit

Max. Anzahl der Clients - Soft Limit

Bevorzugtes Band

ZUGANGSKONTROLLE

ACL-Modus

BLACKLISTING

Dynamic Blacklisting

Fehlgeschlagene Versuche

Zeitraum für fehlgeschlagene Versuche

Blacklist Blocktime

VLAN

Aktivieren

BANDBREITENLIMITIERUNG FÜR JEDEN WLAN-CLIENT

Empfang (RX)

Senden (TX)

Abb. 168: 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.

9.3.2 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**.

The screenshot shows the 'Neues Funkmodul-profil' configuration page in the CloudNetManager interface. The 'Name' field is highlighted with a red box. The page includes a sidebar with navigation options like 'Alarmlmeldungen', 'Dashboard', 'Konfiguration', 'Geräte', 'Benutzer', 'Lizenzen', and 'Bibliothek'. The main content area shows configuration fields for 'Beschreibung', 'Betriebsmodus', 'Band', 'Bandbreite', 'Anzahl der Spatial Streams', 'Land', 'WLAN-Modus', 'Burst-Modus', and 'Airtime Fairness'.

ALLGEMEINE EINSTELLUNGEN	
Beschreibung	<input type="text"/>
Betriebsmodus	Access Point
Band	2,4 GHz
Bandbreite	20 MHz
Anzahl der Spatial Streams	2
Land	Deutschland

PERFORMANCE-EINSTELLUNGEN	
WLAN-Modus	802.11b/g/n
Burst-Modus	<input type="checkbox"/>
Airtime Fairness	<input type="checkbox"/>

Buttons: Speichern, Abbrechen

Abb. 169: 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.

9.3.3 Anlegen der Gerätevorlagen / Access-Point-Vorlage

Mindestens eine Gerätevorlage muss definiert werden.

Gehen Sie in das Menü **Konfiguration->Access Point->Neue Access-Point-Vorlage**.

Konfigurationen

Neue Access-Point-Vorlage Optionale Funktionen ✨

Vorlagenname* ↻

Vorlagenbeschreibung ↻

EINSTELLUNGEN

Standort ↻

Administratorpasswort* ↻

LED-Modus ▼

Radius-Server-Profil ▼

FUNK 1

Funkprofil ↻

Kanal

TX-Leistung ▼

Netzwerkprofil ▼

FUNK 2

Funkprofil ↻

Kanal

TX-Leistung ▼

Netzwerkprofil ▼

Abb. 170: 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.

9.3.4 Geräte verwalten

Im Menü **Geräte** wird eine Liste aller registrierten Geräte angezeigt. Zuerst müssen Sie eine **Gruppe** anlegen.



Abb. 171: Geräte verwalten

Gehen Sie in das Menü **Geräte->Gruppen->Neue Gruppe**.



Abb. 172: 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.

9.4 Access Points registrieren und verwalten

Um ein neues Gerät hinzuzufügen, gehen Sie in das Menü **Geräte->Geräte verwalten->Geräte hinzufügen**.

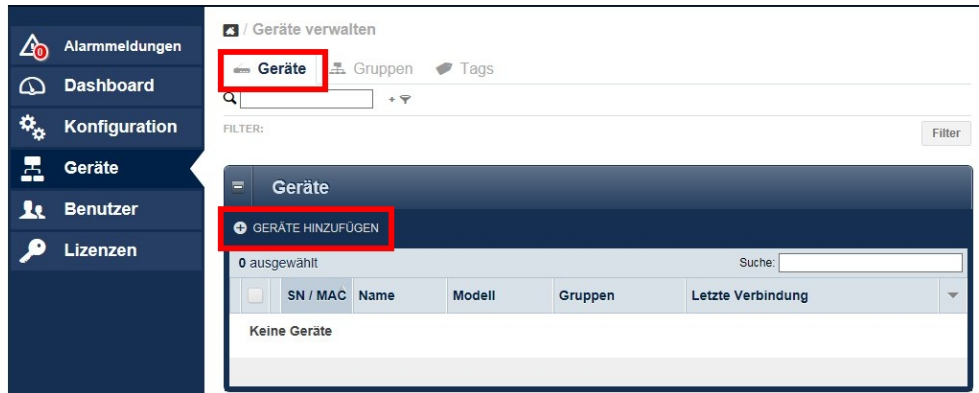


Abb. 173: Access Points registrieren und verwalten

9.4.1 Geräte manuell anmelden

Für eine manuelle Registrierung, gehen Sie in das Menü **Geräte->Geräte hinzufügen->Manuelle Anmeldung**.

Abb. 174: 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 (.csv) 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.

9.4.2 Gerät automatisch anmelden

Für die automatische Registrierung, gehen Sie in das Menü **Geräte->Geräte hinzufügen->Automatische Anmeldung**.

Geräte verwalten / Geräte hinzufügen

Manuelle Anmeldung Automatische Anmeldung

Geräte hinzufügen - Automatische Anmeldung

Folgen Sie diesen Schritten, um die automatische Anmeldung für Ihre Geräte zu aktivieren:

- Richten Sie einen DHCP-Server in Ihrem installierten Netzwerk ein.
- Konfigurieren Sie den DHCP-Server, um die folgende URL in Option 43 zu senden


```
mngplat url=https://bintec.networkcloudmanager.com/AppAdminWeb/register.jsp?
      uuid=da1037ea2-5ca2-4ab6-aad2-0af11a26852c
```
- Wenn ein Gerät die IP-Konfiguration vom DHCP-Server mit der Option 43 erhält, wird es versuchen sich automatisch mit der URL zu verbinden.
- Die URL wird von diesem Server erkannt und enthält als Parameter Ihre Kundenidentifikation.
- Das Gerät wird automatisch mit Ihrer Kundenidentifikation angemeldet.
- Wenn ein Mechanismus zur automatischen Konfiguration oder zum automatischen Laden Ihres Gerätes aktiviert ist, wird er angestoßen, sobald das Gerät angemeldet ist.

Warnung: Achten Sie darauf, dass Sie die URL-Adresse, die im DHCP-Server in der Option 43 angegeben ist, korrekt und vollständig festlegen. Andernfalls kann das Gerät im System nicht korrekt angemeldet werden.

Abb. 175: 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 216) ermöglicht.

9.5 Geräteverwaltung

Im Menü **Geräte** werden die registrierten Geräte angezeigt.

Abb. 176: 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. 177: Detailansicht

9.5.1 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. 178: Batch-Operationen



Abb. 179: Operationen wählen

9.6 Anhang

9.6.1 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.

9.6.1.1 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**.

The screenshot shows a web-based configuration interface for DHCP. The title bar is dark red and contains the text 'Basisparameter'. Below this, there are four main sections:

- Hersteller auswählen:** A dropdown menu currently showing '- Sonstige -'.
- Herstellerbeschreibung:** A text input field containing ':Cloud:'.
- Hersteller-ID:** A text input field containing 'Cloud'.
- Herstellerspezifische Informationen:** A text input field containing 'mngplat.url=https://bintec.networkcloudma'.

Abb. 180: 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 218).
- Klicken Sie auf die Schaltfläche **Übernehmen**.

9.6.1.2 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-Controll

Herstellernamen anzeigen Aktiviert

Abb. 181: **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**.

9.6.2 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:

- 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.

The screenshot displays the 'Geräte hinzufügen - Automatische Anmeldung' configuration page in the Cloud NetManager interface. The left sidebar contains navigation links: Alarmmeldungen, Dashboard, Konfiguration, Geräte, Benutzer, and Lizenzen. The main content area is titled 'Geräte hinzufügen - Automatische Anmeldung' and includes the following instructions:

- Folgen Sie diesen Schritten, um die automatische Anmeldung für Ihre Geräte zu aktivieren:
- Richten Sie einen DHCP-Server in Ihrem installierten Netzwerk ein.
- Konfigurieren Sie den DHCP-Server, um die folgende URL in Option 43 zu senden:

The URL provided is: `mngplat url=https://bintec.networkcloudmanager.com/AppAdminWeb/register.jsp?uid=6ad37ea2-5ca2-4ab6-aaf2-0af11a26853c`

- Wenn ein Gerät die IP-Konfiguration vom DHCP-Server mit der Option 43 erhält, wird es versuchen sich automatisch mit der URL zu verbinden.
- Die URL wird von diesem Server erkannt und enthält als Parameter Ihre Kundenidentifikation.
- Das Gerät wird automatisch mit Ihrer Kundenidentifikation angemeldet.
- Wenn ein Mechanismus zur automatischen Konfiguration oder zum automatischen Laden Ihres Gerätes aktiviert ist, wird er angestoßen, sobald das Gerät angemeldet ist.

A warning box at the bottom states: **Warnung:** Achten Sie darauf, dass Sie die URL-Adresse, die im DHCP-Server in der Option 43 angegeben ist, korrekt und vollständig festlegen. Andernfalls kann das Gerät im System nicht korrekt angemeldet werden.

Abb. 182: **Geräte->Geräte hinzufügen->Automatische Anmeldung**

- 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. 183: Geräte->Gruppen

9.7 Fehlersuche

9.7.1 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.

9.7.2 Keine Kommunikation mehr mit einem verwalteten Gerät

Das Logo, das den Zustand der Kommunikation anzeigt, ist nicht mehr grün, sondern rot.

Geräteverwaltung
RNFDEI014120010 - AUTO_RNFDEI014120010

Info Konfiguration Jobs Log Alarmmeldungen

Gerätemodell: W2003n
Systemversion: V.9.1 Rev. 14 (Beta 5) IPSec
Lizenz: access_point

ACCESS POINT

Details Auslastung Erweitert

Name: AUTO_RNFDEI014120010
Beschreibung:
S/N: RNFDEI014120010
MAC: 00:A0:F9:37:91:59
Position: 40.412167, -3.6993537
IP: 192.168.0.100
Gruppe: Test

Bearbeiten

Abb. 184: 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.

Geräteverwaltung
RNEDDC012500090 - AP 1.Stock

Info Konfiguration Jobs Log Alarmmeldungen

Gerätemodell: W1003n
Systemversion: V.9.1 Rev. 14 (Beta 4) IPSec
Lizenz: access_point

ACCESS POINT

Details Auslastung Erweitert

Zertifikat: Vorhanden
Sicherheitsdaten entfernen

Erweiterte Operationen:

Letzer Kontakt: 2015-07-02 12:01:29
Lizenz-Gültigkeit: Gültige Lizenz (Verbleibende Tage: 365)

Abb. 185: Kommunikationsfehler

9.7.3 Weitere Debug-Möglichkeiten

Im Menü **Geräte->Geräte verwalten** wählen Sie ein Gerät aus. Gehen Sie zu **Geräte verwalten->Konfiguration**.

Geräte verwalten

Geräte Gruppen Tags Konfigurationsvorlagen

FILTER: Filter

Geräte

GERÄTE HINZUFÜGEN GERÄTE LÖSCHEN **GERÄTE VERWALTEN** BATCH-OPERATIONEN

1 ausgewählt Suche:

	SN / MAC	Name	Modell	Gruppen	Letzte Verbindung
<input checked="" type="checkbox"/>	RNEDDC012500136	HD_Wahl@office	W1003n	HD_WAHL	15.04.2015 11:32:42

Seite 1 von 1 Ergebnisse pro Seite: 10

Abb. 186: Kommunikationsfehler

Klicken Sie auf das kleine Logo um die Konfigurationsdatei anzeigen zu lassen.

Geräteverwaltung

RNEDDC012500090 - AP 1.Stock

Info Konfiguration Jobs Log Alarmmeldungen

LETZTER KONTAKT VOR 175

ERWEITERTE EINSTELLUNGEN ANZEIGEN

✓ Konfiguration auf dem Gerät aktualisiert

Einstellungen

Standort anywhere

Administrative password

LED-Modus normal

Funk 1

Funk 2

Abb. 187: Debug-Möglichkeiten

Beachten Sie, dass alle Passwörter in dieser Datei verschlüsselt angezeigt werden.

Geräteverwaltung
RNEDDC012500090 - AP 1.Stock

Info Konfiguration Jobs Log Alarmmeldungen

LETZER KONTAKT VOR 20S

VOLLBILD

✓ Konfiguration auf dem Gerät aktualisiert

Letzte Änderung: 2015-07-01 18:23:22 (Nur Lesen)

```

1 <?xml version="1.0" encoding="UTF-8"?>
2 <WLAN xmlns:xsi="http://www.w3.org/2001/XMLSchema">
3 <General>
4   <description>Auto-generated configuration from template '62:ap-generic/1'
5   <version>1</version>
6   <enable>true</enable>
7   <interface>BR0</interface>
8   <adminpwd>Di5UzKx/6h6ldLcijdSUTpngf4QxwFeMdXqT2dnfo/RKq5QD7bvS7w==</admin
9   <led-mode>normal</led-mode>
10  <keep-scan-results>3600</keep-scan-results>
11 </General>
12 <APSettings><APSetting index="1">
13   <mac-address>00-A0-F9-36-E2-B3</mac-address>
14   <description></description>
15   <name></name>
16   <location>anywhere</location>
17   <encryption>true</encryption>
18
19   <radio1>
20     <radio-profile>1</radio-profile>
21     <channel>auto</channel>
22

```

Historie

Abb. 188: Debug-Meldung

9.7.4 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.

Kapitel 10 SSID - Zuweisung eines getaggten VLAN

Ein Virtual Local Area Network (VLAN) ist ein logisches Teilnetz innerhalb eines physischen Netzwerks, es trennt physische Netze in Teilnetze auf, indem es dafür sorgt, dass VLAN-fähige Switches Datenpakete nicht in ein anderes VLAN weiterleiten (obwohl die Teilnetze an gemeinsamen Switches angeschlossen sein können). Mit einer eindeutigen VLAN-ID wird das virtuelle LAN gekennzeichnet. Im Folgenden wird beschrieben, wie Sie einer SSID ein VLAN zuweisen.



Hinweis

Hinweis: Die angeschlossenen Router und Switches benötigen eine entsprechende Konfiguration, um dem virtuellen Netz mit der **VLAN-ID 10** einen eigenen IP-Adressbereich zuordnen zu können.

Für die Konfiguration wird ein **bintec W2022ac** mit der Firmware-Version 2.2.1.1 verwendet.


10.1 Konfiguration

Im ersten Schritt werden die Regeln für den Empfang von VLANs an den Ports festgelegt.

Gehen Sie dazu in das Menü **LAN->VLAN/Bridge-Gruppen->Portkonfiguration**.


Portkonfiguration				
Port	VLAN-ID	Beschreibung	Bridge-Gruppe	Non-Member-Frames
eth0	Keiner		br0	Verwerfen
eth1	Keiner		br0	Verwerfen

Abb. 189: LAN->VLAN/Bridge-Gruppen->Portkonfiguration

Wählen Sie das Symbol , um vorhandenen Eintrag zu bearbeiten.

Port einstellen

Mitgliedschaft in VLAN/Bridge-Gruppe

VLAN-ID	Beschreibung	Bridge-Gruppe	
Keiner	default	br0	
10	Gast	Neu	

HINZUFÜGEN

Abb. 190: LAN->VLAN/Bridge-Gruppen->Portkonfiguration-> 

Gehen Sie folgendermaßen vor:

- (1) Für die bessere Übersicht, geben Sie im Feld **Beschreibung** einen Namen für das Ethernet ein. Hier z. B. *default*.
- (2) Klicken Sie auf **Hinzufügen**.
- (3) Bei **VLAN-ID** geben Sie z. B. *10* ein.
- (4) Geben Sie eine **Beschreibung** ein, z. B. *Gast*.
- (5) Bei **Bridge-Gruppe** wählen Sie *Neu* aus. Eine neue Bridge-Gruppe wird hinzugefügt.
- (6) Klicken Sie auf **OK**.

Im Menü **LAN->IP-Konfiguration->Schnittstellen** ist die neue Bridge-Gruppe aufgelistet. Hier sind keine weiteren Einstellungen nötig.







Schnittstelle	IPv4-Adresse/Netzmaske	Status	Aktion		
br0	192.168.0.10/255.255.255.0 (DHCP)		^ v		
br1	Nicht konfiguriert/Nicht konfiguriert		^ v		

Abb. 191: LAN->IP-Konfiguration->Schnittstellen

Im nächsten Schritt wird dem **Drahtlosnetzwerk (SSID)** die **Bridge-Gruppe** *br1* mit der **VLAN-ID** *10* zugeordnet.

Gehen Sie dazu in das Menü **Wireless LAN->WLAN1->Drahtlosnetzwerk (VSS)->Neu**.

The screenshot displays the configuration interface for a new wireless LAN network. It is divided into four main sections:

- Service Set Parameter:**
 - Beschreibung: Gast
 - Netzwerkname (SSID): Gast (with a toggle for 'Sichtbar' which is turned on)
 - Intra-cell Repeating: (with a toggle for 'Aktiviert' which is turned on)
 - WMM: (with a toggle for 'Aktiviert' which is turned off)
- Einstellungen der Bridge-Gruppe:**
 - Bridge-Gruppe: A dropdown menu with options 'br0', 'br1', and 'Keine'. 'br1' is selected.
- Sicherheitseinstellungen:**
 - Sicherheitsmodus: WPA-PSK
 - WPA-Modus: WPA 2 und WPA 3
 - Pre-shared Key: A field containing several asterisks.
- Client-Lastverteilung:**
 - Max. Anzahl Clients - Hard Limit: 32
 - Max. Anzahl Clients - Soft Limit: 28
 - Auswahl des Client-Bands: Deaktiviert, optimiert für Fast Roaming

Abb. 192: **Wireless LAN->WLAN1->Drahtlosnetzwerk (VSS)->Neu**

Gehen Sie folgendermaßen vor:

- (1) Sie können hier eine **Beschreibung** eingeben.
- (2) Geben Sie den **Netzwerknamen (SSID)** ein, z. B. *Gast*.
- (3) Im Bereich **Einstellungen der Bridge-Gruppe** wählen Sie die **Bridge-Gruppe** *br1* aus.
- (4) Für den **Sicherheitsmodus** *WPA - PSK* ist ein WPA-Passwort notwendig. Ändern Sie unbedingt den Standard **Pre-shared Key**!
- (5) Belassen Sie die restlichen Einstellungen und bestätigen Sie Ihre Angaben mit **OK**.

Im Menü **LAN->VLAN/Bridge-Gruppen->Portkonfiguration** sind die zugeordneten Bridge-Gruppen sichtbar.




Portkonfiguration					
Port	VLAN-ID	Beschreibung	Bridge-Gruppe	Non-Member-Frames	
eth0	Keiner	default	br0	Verwerfen	
eth0	10	Gast	br1		
eth1	Keiner		br0	Verwerfen	

Abb. 193: LAN->VLAN/Bridge-Gruppen->Portkonfiguration

Damit ist die Konfiguration am **bintec W2022ac** abgeschlossen.