



Manual Workshops (Excerpt)

WLAN Workshops

Copyright© Version 08/2020 bintec elmeg GmbH

Legal Notice

Warranty

This publication is subject to change.

bintec elmeg GmbH offers no warranty whatsoever for information contained in this manual. bintec elmeg GmbH is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

Copyright © bintec elmeg GmbH.

All rights to the data included, in particular the right to copy and propagate, are reserved by bintec elmeg GmbH.

Table of Contents

Chapter 1	WLAN - VLAN with Multi SSID WLAN	1
1.1	Introduction	1
1.2	Configuration	1
1.2.1	Configuring the wireless networks.	2
1.2.2	Configuring VLANs	4
1.2.3	Defining rules for receiving at the ports	5
1.2.4	Removing ports from VLAN management	6
1.2.5	Enable VLAN	7
1.2.6	Configuration on bintec S128p	8
1.3	Result	10
1.4	Checking the connection.	10
1.5	Overview of configuration steps	10
Chapter 2	WLAN - bintec Hotspot Solution	14
2.1	Introduction	14
2.2	Performance features	16
2.2.1	Hotspot solution features	16
2.2.2	Gateway features	16
2.2.3	Hotspot server features	16
2.3	Configuration	17
2.3.1	Configuration of the bintec Hotspot gateway	17
2.3.2	Configuration of the bintec Hotspot server by the dealer	24
2.3.3	Administration of Hotspot accounts	30
2.3.4	Operation at several locations	34
2.4	Configuring login methods	38
2.4.1	Anonymous login	38
2.4.2	1-Click	42

2.4.3	SMS	46
2.4.4	PayPal	51
2.4.5	Default Free Service	56
2.5	Instructions for safe operation	56
2.5.1	Multiple login	56
2.5.2	Preventing mutual visibility of extensions	56
2.5.3	Encrypted/unencrypted WLAN connection	58
2.5.4	WPA Encryption	59
2.5.5	IP/ARP Spoofing	59
2.6	Overview of configuration steps.	59
Chapter 3	WLAN - VoWLAN Basics and Configuration	66
3.1	General	66
3.2	WLAN infrastructure	66
3.2.1	WLAN radio illumination	66
3.2.2	Handover between the access points	68
3.2.3	Bandwidth requirement	68
3.2.4	The safety standard and the handover	69
3.2.5	QoS, WMM and U-APSD	69
3.2.6	WLAN controllers – A must in a VoWLAN network?	72
3.2.7	Potential sources of interference	73
3.3	Example configuration	73
3.3.1	Network plan	74
3.3.2	WLAN configuration with or without WLAN controller	75
3.4	Ascom i62 Talker configuration	76
3.4.1	Requirements	77
3.4.2	Configuration	77
3.4.3	Test commands on the Ascom i62	82
3.5	Configuring the elmeg hybrid 300	82
3.5.1	Configuration	82

3.5.2	Operational scenario: WLAN telephone cannot be accessed	83
3.6	Use other WLAN telephones	84
3.7	Overview of Configuration Steps	85
Chapter 4	WLAN Management for Multiple Locations: WLAN controller via VPN	88
4.1	Introduction	88
4.1.1	Requirements	89
4.1.2	About the test setup.	89
4.2	Configuration.	90
4.2.1	Presettings	90
4.2.2	Configure the router in the field office	90
4.2.3	Configure the VPN concentrator at head office	94
4.2.4	Configure the WLAN controller at head office.	95
4.3	Overview of Configuration Steps	106
Chapter 5	WLAN - Wireless LAN Controller as Network Access Gateway	113
5.1	Introduction	113
5.2	Configuration	115
5.3	Overview of Configuration Steps	143
Chapter 6	WLAN network with guest WLAN	154
6.1	Introduction	154
6.2	Configuration.	155
6.2.1	Configuring the IP address	155
6.2.2	Create bridge groups and assign LAN interface.	156
6.2.3	Put Wireless LAN Controller into operation	156
6.2.4	Choose radio profile and configure WLAN access to the local network.	157

6.2.5	Configure guest WLAN	159
6.2.6	Configure Access Points with the Wireless LAN Controller	160
6.2.7	Configure the IP address for the virtual Bridge Interface	161
6.2.8	Configure the IP Address Range for the guest network	162
6.2.9	Configure DHCP use	163
6.2.10	Set up firewall	164
6.3	Result	169
6.4	Overview of Configuration Steps	169
Chapter 7	WLAN - WLAN controller installation with integrated HotSpot functionality	173
7.1	Introduction	173
7.2	Function	174
7.3	Configuration	174
7.3.1	Basic configuration	174
7.3.2	LAN configuration	174
7.3.3	HotSpot configuration	176
7.3.4	DHCP configuration	180
7.3.5	Wireless LAN controller wizard	183
7.4	Overview of configuration steps	192
Chapter 8	WLAN - Cloud NetManager	198
8.1	Introduction	198
8.2	First steps in the portal	198
8.2.1	Creating a user	198
8.2.2	Changing the time zone	201
8.2.3	Importing the licences	201
8.3	Creation of profiles	203
8.3.1	Creation of network profiles (SSID)	203

8.3.2	Creation of radio profiles	205
8.3.3	Creation of device templates / access point template	206
8.3.4	Administer devices	207
8.4	Register and administer access points.	208
8.4.1	Manually register devices	208
8.4.2	Automatically register device	209
8.5	Device administration	210
8.5.1	Batch operations and software update.	211
8.6	Appendix	211
8.6.1	Establishing another data centre	212
8.6.2	Automatic configuration	215
8.7	Error search	216
8.7.1	A new device is not visible	216
8.7.2	No more communication with an administered device	216
8.7.3	Further debug options	217
8.7.4	Debugging at device level	219

Chapter 1 WLAN - VLAN with Multi SSID WLAN

1.1 Introduction

The following chapters describe how to configure a VLAN (Virtual LAN). You connect your WLAN clients wirelessly to the corporate network via a **W2003ac**. **W2003ac** serves as the access point for the wireless networks *Management*, *Development* and *Public*. The Ethernet interface to which your hard-wired LAN is connected is operated in bridge mode and is connected over a VLAN-capable switch to the hard-wired network. The network is segmented virtually in the VLANs *Management*, *Development* and *Public*.

Configuration is performed with the **GUI** (Graphical User Interface).

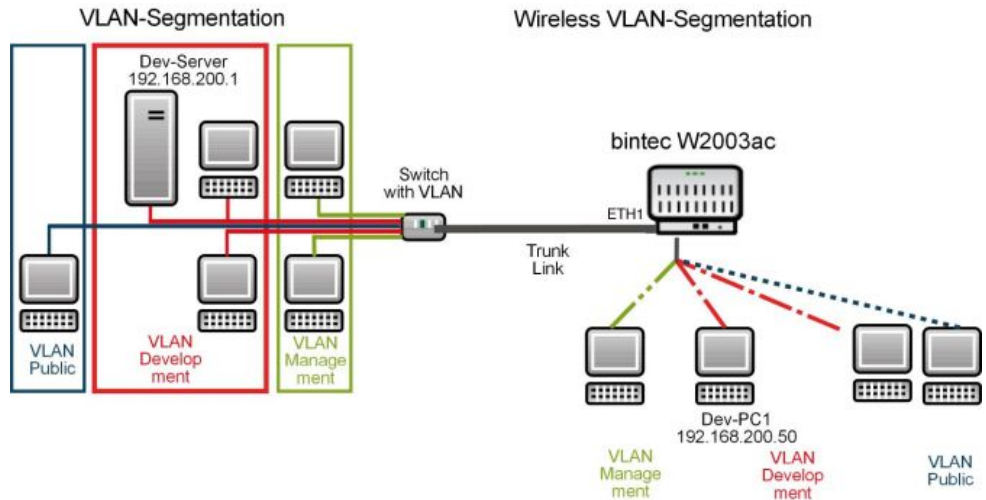


Fig. 1: VLAN segmenting

Requirements

The following are required for the configuration:

- A boot image of version 10.1.9 or later.
- A VLAN-capable switch.


1.2 Configuration

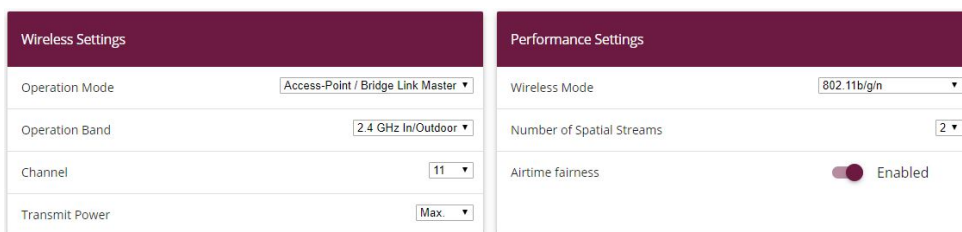
1.2.1 Configuring the wireless networks

You must set up wireless networks on the access points so that the clients can connect to the network over their access point.

Proceed as follows to create wireless networks:

- (1) Go to **Wireless LAN -> WLAN-> Radio Settings**.

Configure the wireless module by editing the default entry. To do this, click the  icon next to the existing entry.



The image shows two configuration panels side-by-side. The left panel is titled 'Wireless Settings' and contains four rows of settings: 'Operation Mode' set to 'Access-Point / Bridge Link Master', 'Operation Band' set to '2.4 GHz In/Outdoor', 'Channel' set to '11', and 'Transmit Power' set to 'Max'. The right panel is titled 'Performance Settings' and contains three rows: 'Wireless Mode' set to '802.11b/g/n', 'Number of Spatial Streams' set to '2', and 'Airtime fairness' which is a toggle switch currently turned 'Enabled'.

Fig. 2: **Wireless LAN -> WLAN-> Radio Settings** -> 

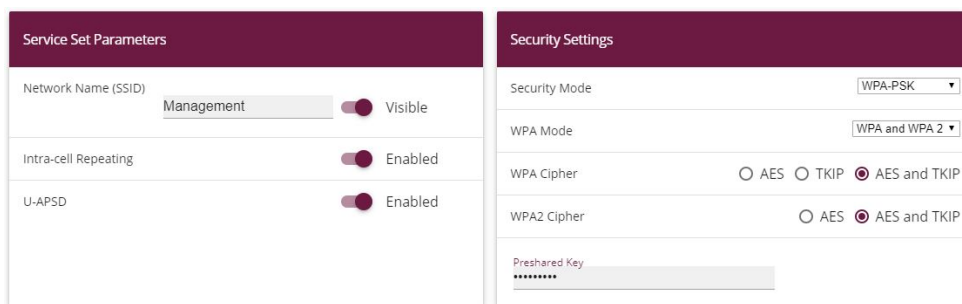
Proceed as follows:

- (1) Set **Operation Mode** to *Access-Point /Bridge Link Master*.
- (2) Set the **Channel** to *11* for example.
- (3) Confirm with **OK**.

Then create the wireless network entries.

- (1) Go to **Wireless LAN -> WLAN->Wireless Networks (VSS)->**.

Configure the WLAN connection by editing the default entry.



The image shows two configuration panels side-by-side. The left panel is titled 'Service Set Parameters' and contains three rows: 'Network Name (SSID)' with the value 'Management' and a 'Visible' toggle switch turned on; 'Intra-cell Repeating' with a toggle switch turned on; and 'U-APSD' with a toggle switch turned on. The right panel is titled 'Security Settings' and contains four rows: 'Security Mode' set to 'WPA-PSK', 'WPA Mode' set to 'WPA and WPA 2', 'WPA Cipher' with radio buttons for 'AES', 'TKIP', and 'AES and TKIP' (where 'AES and TKIP' is selected), 'WPA2 Cipher' with radio buttons for 'AES' and 'AES and TKIP' (where 'AES and TKIP' is selected), and 'Preshared Key' with a masked input field containing several asterisks.

Fig. 3: **Wireless LAN -> WLAN1->Wireless Networks (VSS)->**

Proceed as follows:

- (1) Under **Network Name (SSID)** enter *Management* for example.
- (2) Under **Network Name (SSID)** the **Visible** option remains enabled.
- (3) Set the **Security Mode** to *WPA-PSK*.
- (4) Under **Preshared Key** enter *Key-Admin*, for example.
- (5) Confirm with **OK**.



Note

You should use special characters, numbers and upper and lower case letters in your key to increase security.

You must then enable the wireless network you have just configured. To do this, go to the overview in the **Wireless LAN -> WLAN->Wireless Networks (VSS)**.

Wireless Networks (VSS)						
VSS						
Description	Network Name (SSID)	MAC Address	Security	Status	Action	
vss7-10	Management	Elmeqt_6f5e:85	WPA-PSK	✔	^	▼

Fig. 4: **Wireless LAN -> WLAN->Wireless Networks (VSS)**

Proceed as follows:

- (1) In the currently only list entry click the icon in the **Action** column. Refer to the **Status** column: After a short delay, the icon will be displayed here.

Configure the corresponding new entries for the wireless networks *Development* and *Public*.



Note

Make sure that you assign different **Preshared Keys** to the various wireless networks.

Next configure the wireless adapter of the clients in your network to connect to their corresponding wireless network (VSS).

1.2.2 Configuring VLANs

VLAN *Management* is pre-configured by default on your device. Now create the VLANs *Development* and *Public*.

Go to the following menu to create a VLAN:

- (1) Go to **LAN -> VLAN -> VLANs -> New**.

Configure VLAN

VLAN Identifier
2

VLAN Name
Development

VLAN Members

Interface	Egress Rule	Delete
vss2-1 ▼	Untagged ▼	
en1-0 ▼	Tagged ▼	

ADD

Fig. 5: **LAN -> VLAN -> VLANs -> New**

Proceed as follows:

- (1) Under **VLAN Identifier** enter a value between 1 and 4094, in this example 2.
- (2) Under **VLAN Name** enter *Development* for example.
- (3) Under **VLAN Members** click **Add** and select the corresponding WLAN interface, e.g. *vss2-1*. In addition, select the **Egress Rule** *Untagged*.

- (4) Under **VLAN Members** click **Add** and select the corresponding LAN interface, e.g. *en1-0*. In addition, select the **Egress Rule** *Tagged*.
- (5) Click **OK**.

Repeat these steps to create the *Public* VLAN.

- (1) Under **VLAN Identifier** enter a value between 1 and 4094, in this example *3*.
- (2) Under **VLAN Name** enter *Public* for example.
- (3) Under **VLAN Members** click **Add** and select the corresponding WLAN interface, e.g. *vss2-2*. In addition, select the **Egress Rule** *Untagged*.
- (4) Under **VLAN Members** click **Add** and select the corresponding LAN interface, e.g. *en1-0*. In addition, select the **Egress Rule** *Tagged*.
- (5) Click **OK**.

1.2.3 Defining rules for receiving at the ports

In the **Port Configuration** menu, you can define the rules for receiving frames at the VLAN ports.

Proceed to the following menu to define the Port VLAN Identifier (PVID):

- (1) Go to **LAN -> VLAN -> Port Configuration**.

Port Configuration			
Interface	PVID	Drop untagged frames	Drop non-members
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"/>

Fig. 6: **LAN -> VLAN -> Port Configuration**

Proceed as follows:

- (1) In addition to the **Interface** *vss2-1*, select the **Port VLAN Identifier (PVID)**, in this example *Development*.
- (2) In addition to the **Interface** *vss2-2*, select the **Port VLAN Identifier (PVID)**, in this example *Public*.
- (3) Leave the option disabled for the interfaces *en1-0* and *en1-1* under **Drop untagged frames**. Enable the option for the interfaces *en1-0* and *en1-1* under **Drop non-**

members.

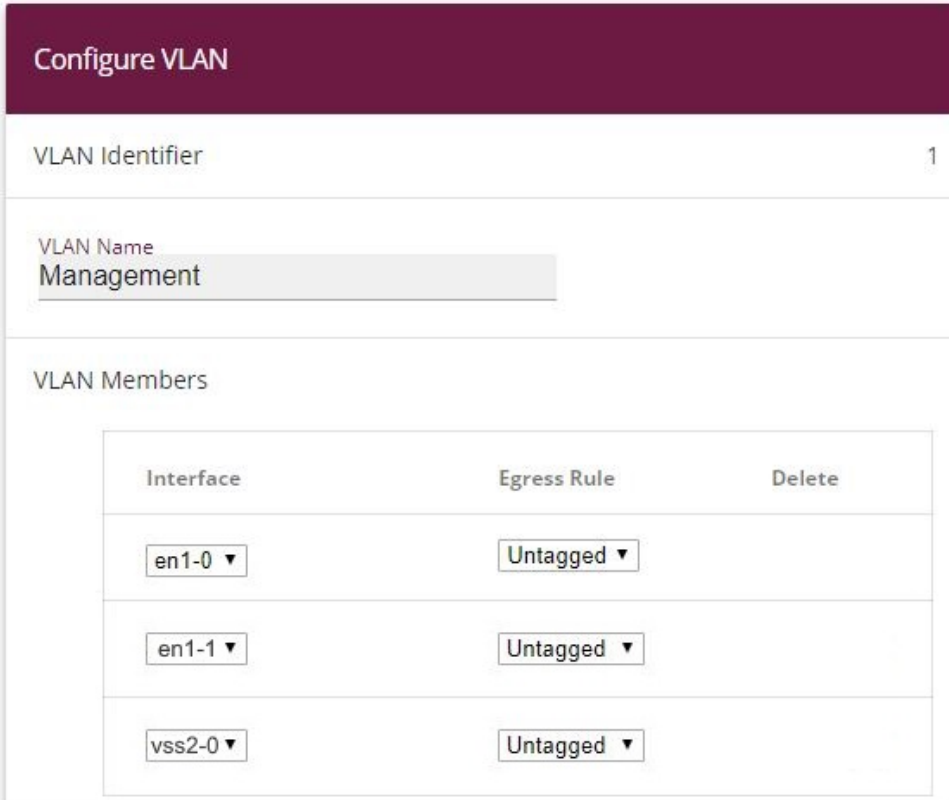
(4) Click **OK**.

1.2.4 Removing ports from VLAN management

The ports that you have assigned to the *Development* and *Public* VLANs will be removed from VLAN *Management*.

To do this, go to the following menu:


(1) Go to **LAN -> VLAN -> VLANs -> <Management>** -> .




Interface	Egress Rule	Delete
en1-0 ▼	Untagged ▼	
en1-1 ▼	Untagged ▼	
vss2-0 ▼	Untagged ▼	

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

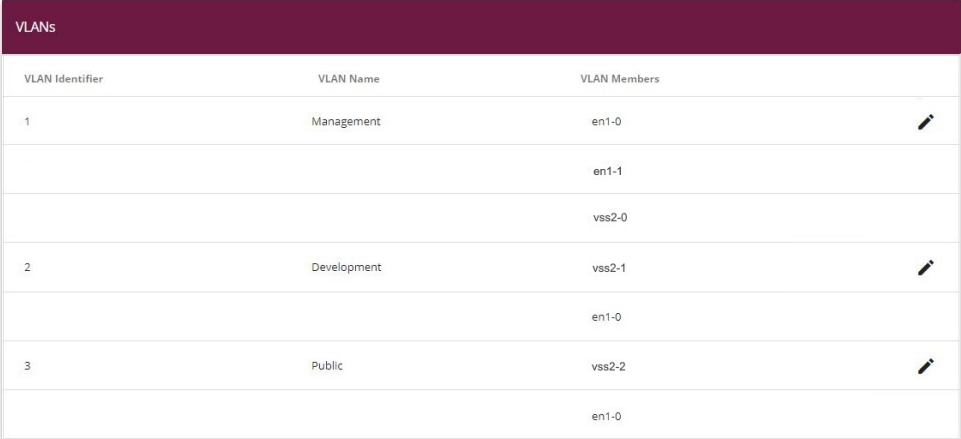
Proceed as follows:

(1) Click the  icon for **Interface** *vss2-1*.

(2) Click the  icon for **Interface** *vss2-2*.

- (3) Leave the **Interfaces** *en1-0*, *en1-1* and *vss2-0* *Untagged* under **Egress Rule**.
- (4) Click **OK**.

You have now set up all the necessary VLANs. You can check these in the list in the **LAN -> VLAN -> VLANs** menu.



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

Fig. 8: VLAN overview

1.2.5 Enable VLAN

Finally, you must enable the VLAN function for the bridge group *br0*.

For this, go to the following menu:

- (1) Go to **LAN -> VLAN -> Administration**.

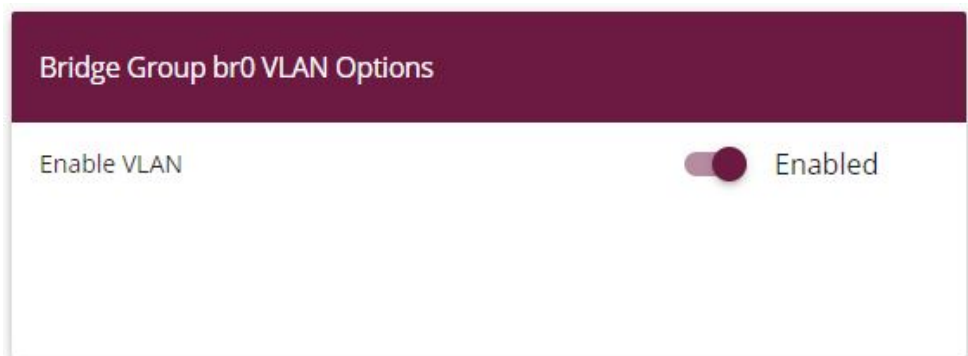


Fig. 9: LAN -> VLAN -> Administration

Proceed as follows:

- (1) Select **Enable VLAN**.
- (2) Click **OK**.

1.2.6 Configuration on bintec S128p

The switch must be configured in the same way as the access point. Only tagged (VLAN) packets must be processed in the access point direction. Tagging must be removed in the client direction, otherwise the clients cannot process the packets.

- (1) Launch the browser and log in to the switch.
- (2) Go to **Protocol -> VLAN**.
- (3) Under **VLAN Operation Mode** select *802.1Q*.
- (4) Click **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	

Apply

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	

Fig. 10: Protocol -> VLAN -> VLAN Configuration

A total of 3 VLANs are required. In each case the **Port** (Port.01, Port.02, Port.03) and **Untagged Vid** (1, 102, 103) must be set correctly.

Proceed as follows to configure the ports:

- (1) Under **Port** select *Port.01*.
- (2) Set **Link Type** to *Access Link*.

- (3) Under **Untagged Vid** enter *1*.
- (4) Press **Apply** to confirm your entries.
- (5) Proceed in the same way to configure *Port.02 (Untagged Vid 102)* and *Port.03 (Untagged Vid 103)*.
- (6) Press **Apply** to confirm your entries.
- (7) Under **Port** select *Port.08*.
- (8) Set **Link Type** to *Trunk Link*.
- (9) Under **Tagged Vid** enter *1,102,103*.
- (10) Press **Apply** to confirm your entries.

The complete configuration looks like this:

The screenshot shows the 'VLAN Configuration' interface. On the left is a navigation menu with categories: System, Port, Protocol (VLAN, RSTP, SNMP, QoS, IGMP, X-Ring), Security, Power over Ethernet, Factory Default, and System Reboot. The 'VLAN' option under 'Protocol' is selected.

The main configuration area is titled 'VLAN Configuration'. It includes a 'VLAN Operation Mode' dropdown set to '802.1Q', an 'Enable GVRP Protocol' checkbox, and a 'Management Vlan ID' field set to '1'. An 'Apply' button is below these fields.

Below this is the '802.1Q Configuration' section, which has a 'Group Configuration' sub-section. It contains a table with columns: Port, Link Type, Untagged Vid, and Tagged Vid. The table shows configurations for Port.01 through G2.

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	

An 'Apply' button is located below the table.

Fig. 11: Protocol -> VLAN -> VLAN Configuration

Checking the connection

To check the configuration, call up the command prompt on a PC and send a ping to the head office network:

e.g. ping 192.168.100.30

You should then receive the following message:

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

Ping wird ausgeführt für 192.168.100.30 mit 32 Bytes Daten:

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

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

1.3 Result

You have set up different wireless networks for the WLAN clients in your network. The entire network has been segmented into various VLANs.

1.4 Checking the connection

To check the configuration, call up the command prompt, for example on PC Dev-PC1 (192.168.200.50), and send a ping to the Dev-Server (192.168.200.1):

e.g. `ping 192.168.200.1`

You should then receive the following messages:



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

Antwort von 192.168.200.1: Bytes=32 Zeit<lt;ms TTL=63
Antwort von 192.168.200.1: Bytes=32 Zeit<lt;ms TTL=63
Antwort von 192.168.200.1: Bytes=32 Zeit<lt;ms TTL=63
Antwort von 192.168.200.1: Bytes=32 Zeit<lt;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 Overview of configuration steps

Enabling the access point

Field	Menu	Value
Operation Mode	Wireless LAN -> WLAN -> Radio Settings-> 	Access-Point / Bridge Link Master
Channel	Wireless LAN -> WLAN -> Radio Settings-> 	e.g. 11

Setting up wireless networks

Field	Menu	Value
Network Name	Wireless LAN -> WLAN ->Wireless Networks (VSS) ->Neu	<i>Management</i> ; Visible remains enabled
Security Mode	Wireless LAN -> WLAN ->Wireless Networks (VSS) ->Neu	<i>WPA-PSK</i>
Preshared Key	Wireless LAN -> WLAN ->Wireless Networks (VSS) ->Neu	<i>Key-Admin</i>
Action	Wireless LAN -> WLAN ->Wireless Networks (VSS) -><Management>	^
Network Name	Wireless LAN -> WLAN ->Wireless Networks (VSS) ->Neu	<i>Development</i> ; Visible remains enabled
Security Mode	Wireless LAN -> WLAN ->Wireless Networks (VSS) ->Neu	<i>WPA-PSK</i>
Preshared Key	Wireless LAN -> WLAN ->Wireless Networks (VSS) ->Neu	<i>Key-Devs</i>
Action	Wireless LAN -> WLAN ->Wireless Networks (VSS) -><Development>	^
Network Name	Wireless LAN -> WLAN ->Wireless Networks (VSS) ->Neu	<i>Public</i> ; Visible remains enabled
Security Mode	Wireless LAN -> WLAN ->Wireless Networks (VSS) ->Neu	<i>WPA-PSK</i>
Preshared Key	Wireless LAN -> WLAN ->Wireless Networks (VSS) ->Neu	<i>Key-All</i>
Action	Wireless LAN -> WLAN ->Wireless Networks (VSS) -> <Public>	^

Configuring VLANs

Field	Menu	Value
VLAN Identifier	LAN -> VLAN -> VLANs -> New	e.g. 2
VLAN Name	LAN -> VLAN -> VLANs -> New	e.g. <i>Development</i>
VLAN Members	LAN -> VLAN -> VLANs -> New	with Add e.g. <i>vss2-1</i>
Egress Rule	LAN -> VLAN -> VLANs -> New	<i>Untagged</i> for <i>vss2-1</i>
VLAN Members	LAN -> VLAN -> VLANs -> New	with Add e.g. <i>en1-0</i>
Egress Rule	LAN -> VLAN -> VLANs -> New	<i>Tagged</i> for <i>en1-0</i>
VLAN Identifier	LAN -> VLAN -> VLANs -> New	e.g. 3
VLAN Name	LAN -> VLAN -> VLANs -> New	e.g. <i>Public</i>
VLAN Members	LAN -> VLAN -> VLANs -> New	with Add e.g. <i>vss2-2</i>
Egress Rule	LAN -> VLAN -> VLANs -> New	<i>Untagged</i> for <i>vss2-2</i>
VLAN Members	LAN -> VLAN -> VLANs -> New	with Add e.g. <i>en1-0</i>
Egress Rule	LAN -> VLAN -> VLANs -> New	<i>Tagged</i> for <i>en1-0</i>

Defining the Port VLAN Identifier (PVID)

Field	Menu	Value
Port VLAN Identifier (PVID)	LAN -> VLAN -> Port Configuration	for Interface <i>vss2-1</i> e.g. <i>Development</i> ; for Interface <i>vss2-2</i> e.g. <i>Public</i>
Drop non-members	LAN -> VLAN -> Port Configuration	Select interfaces <i>en1-0</i> and <i>en1-1</i>

Removing ports from VLAN management

Field	Menu	Value
VLAN Members	LAN -> VLAN -> VLANs ->	 for Interface <i>vss2-1</i>

Field	Menu	Value
	<Management>	and <i>vss2-2</i>

Enabling VLANs

Field	Menu	Value
Enable VLAN	LAN -> VLAN -> Administration	<i>Enabled</i>

Chapter 2 WLAN - bintec Hotspot Solution

2.1 Introduction

The **bintec Hotspot Solution** allows provision of public Internet accesses. The solution is adapted to setup of smaller and larger Hotspot solutions for cafes, hotels, companies, communal residences, campgrounds, etc.

The **bintec Hotspot Solution** consists of a **bintec RS353xx**, a **bintec RXL12x00** or a **be.IP** device installed onsite, which functions as a gateway, and of a Hotspot server, centrally located at a computing centre. The operator account is administered on the server via a PC with internet access (e.g., a hotel reception PC); this includes functions such as registration entry, generating tickets, statistical analysis, etc.

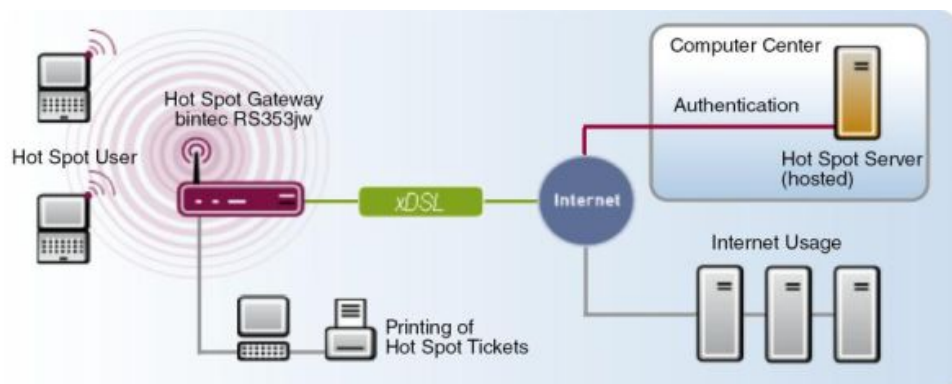


Fig. 12: Method of operation

Login sequence at the Hotspot server

- When a new user connects with the Hotspot, he/she is automatically assigned an IP address via DHCP.
- As soon as he attempts to access any Internet site with a browser, the user is redirected to the start/login page.
- After the user has entered the registration data (user/password), these are sent to the central RADIUS server (Hotspot server) as RADIUS registration.
- Following successful registration, the gateway opens Internet access.
- For each user, the gateway sends regular additional information to the RADIUS server for accounting purposes.

- When the ticket expires, the user is automatically logged off and again redirected to the start/login page.

Requirements

To operate a Hotspot, the customer requires:

- a be.IP- , RS- (e.g. **bintec RS353xx**) or RXL-series router (e.g. **bintec RXL12100**)
- **bintec Hotspot hosting** (article number 5510000198 or 5510000197)
- Access data
- Documentation
- Software licensing

Please note that you must first activate the licence.

- Go to www.bintec-elmeg.com then **Service & Support->Product Licencing -> Hot-Spot Licencing** .

- Enter the required data (please note the relevant explanations on the license sheet), and follow the instructions of the online licensing.

- You then receive the Hotspot server's login data.



Note

Activation may require 2 - 3 business days.

Access data for gateway configuration

RADIUS Server IP	62.245.165.180
RADIUS Server Password	funkwerk-ec
Domain	Individually set for customers by customer/dealer
Walled Network	Individually set for customers by customer/dealer
Walled Server URL	The URL set by the Hotspot-Server is to be entered here.
Terms & Conditions URL	During uploading the terms and conditions, the Hotspot server provides an URL for them. This URL is to be entered here.

Access data for configuration of the Hotspot server

Admin URL	https://hotspot.bintec-elmeg.com/
Username	Individually set by bintec elmeg
Password	Individually set by bintec elmeg

2.2 Performance features

2.2.1 Hotspot solution features

- Can be a free service, or as a time- or volume-based ticket system
- Free advertising websites accessible without registration (Walled Garden Pages)
- Applicable to WLAN as well as to wire connection LAN users
- The system is franchise-capable, i.e., a cafe- or restaurant chain can offer the system at various localities, and administer it centrally. Here, an issued ticket can be further used at other locations.

2.2.2 Gateway features

- Simple user login via Internet browser
- Redirection to a login page on initial access
- Login via RADIUS authentication
- Multiple logins for the same user are configurable
- Time credits remain if the user logs out, or the connection is interrupted
- Automatic logout of Hotspot users in case of inactivity or if users forget to log out.
- The user must actively confirm the general terms and conditions at login. You'll find model general terms & conditions in the download area at www.bintec-elmeg.com

2.2.3 Hotspot server features

- Several localities can be created for each customer (franchise support)
- Several rates can be created for each customer (e.g., daily ticket, hourly ticket, volume ticket)
- Every customer has a personal administrative area for ticket creation and management

2.3 Configuration

Requirements

The following are required for the configuration:

- an be.IP-, RS- (e.g. **bintec RS353xx**) or RXL-series router (e.g. **RXL12100**)
- Internet access, either via LAN, DSL or other connections
- Activated account on the central **bintec Hotspot server**

2.3.1 Configuration of the bintec Hotspot gateway

You configure your device using the **GUI** (Graphical User Interface).

Update of the gateway

Your device contains the version of the system software available at the time of production. More recent versions may have since been released. You can easily perform an update with the **GUI** using the **Software & Configuration** menu.

- (1) Go to **Maintenance-> Software & Configuration -> Options**.

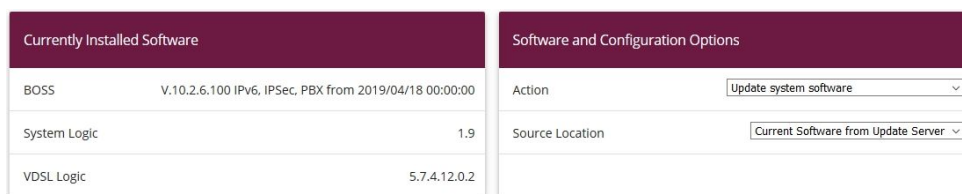


Fig. 13: **Maintenance -> Software & Configuration -> Options**

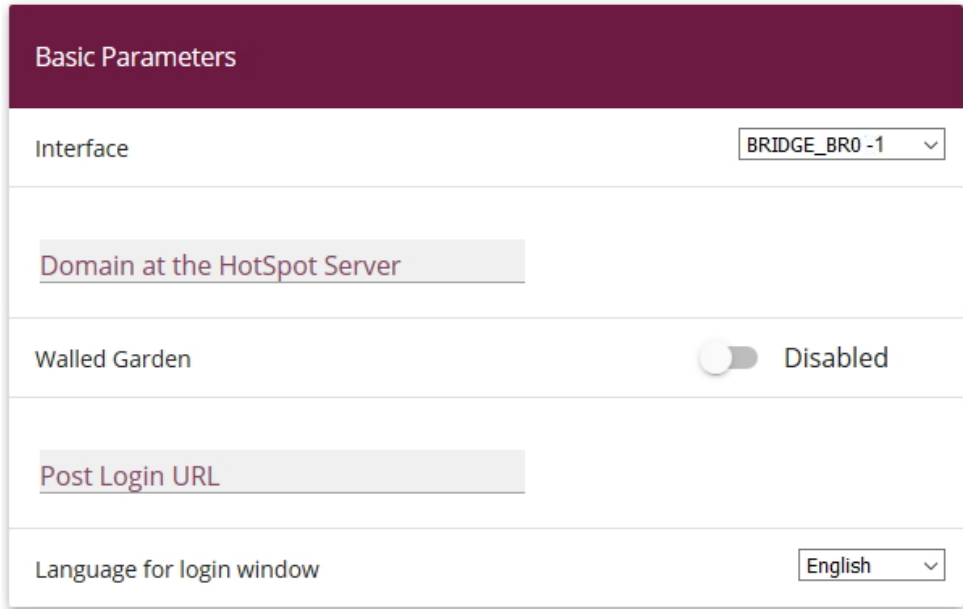
Proceed as follows:

- (1) Under **Action** select *Update system software*.
- (2) As **Source**, select *Current Software from Update Server*.
- (3) Click **Start** to complete the update.

Configure language (reseller / partner)

You can select the language for the start/login page of a reseller / partner in the **Local Services -> HotSpot Gateway-> HotSpot Gateway-> New** menu.

The language can be changed on the start/login page at any time.



Basic Parameters

Interface BRIDGE_BR0 -1

Domain at the HotSpot Server

Walled Garden Disabled

Post Login URL

Language for login window English

Fig. 14: **Local Services -> HotSpot Gateway -> HotSpot Gateway -> New**

Set time zone

You need the system time for tasks such as correct time-stamps for system messages, or accounting. For this, go to the following menu:

- (1) Go to **System Management -> Global Settings -> Date and Time**.

Basic Settings	
Time Zone	Europe/Berlin
Current Local Time	Wednesday, 2019 May 29, 13:57:31

Manual Time Settings			
Set Date	Day	Month	Year
	<input type="text"/>	<input type="text"/>	<input type="text"/>
Set Time	Hour	Minute	
	<input type="text"/>	<input type="text"/>	

Automatic Time Settings (Time Protocol)	
First Timeserver	<input type="text"/> SNTP
Second Timeserver	<input type="text"/> SNTP
Third Timeserver	<input type="text"/> SNTP
Time Update Interval	1440 Minute(s)
Time Update Policy	Endless
Internal Time Server	<input type="checkbox"/>

Fig. 15: System Management -> Global Settings -> Date and Time



Note

If a method for automatically deriving the time is defined on the device, the values obtained in this way automatically have higher priority. A manually entered system time is therefore overwritten.

Proceed as follows to configure the time zone settings:

- (1) In the **Time Zone** field, select *Europe/Berlin*. To guarantee a synchronous system time, a current system time is required for operation.
- (2) Disable **ISDN Timeserver**.
- (3) Deactivate **Internal Time Server**. Time requests from a client are not answered.
- (4) Confirm with **OK**.

Disabling of local communication

If a Wireless LAN Controller manages several access points or if you use a stand-alone access point, you can prevent communication of hotspot users registered at the same access point among each other.

If you operate a Wireless LAN Controller, proceed as follows:

- (1) Go to **Wireless LAN Controller -> Slave AP configuration -> Wireless Networks (VSS) -> **

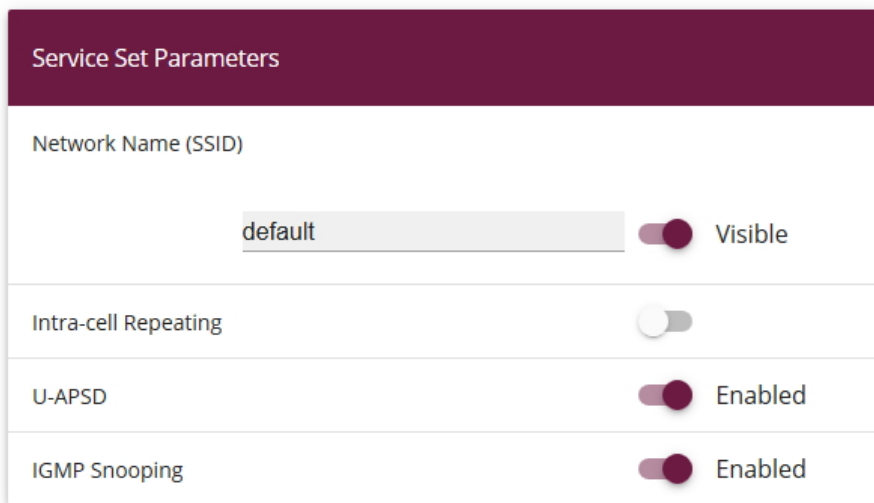




Fig. 16: **Wireless LAN Controller -> Slave AP configuration -> Wireless Networks (VSS) -> **

- (2) Disable **Intra-cell Repeating**.
- (3) Confirm with **OK**.

If you operate a stand-alone-device in access point mode (**Wireless LAN -> WLAN -> Radio Settings ->  -> Operation Mode = Access Point**), you can set up and edit the desired wireless networks in the **Wireless LAN -> WLAN -> Wireless Networks (VSS) -> New** menu.

In the following procedure, local communication between individual hotspot users registered at a stand-alone access point is prevented.

Proceed as follows:

- (1) Go to **Wireless LAN -> WLAN -> Wireless Networks (VSS) -> **.

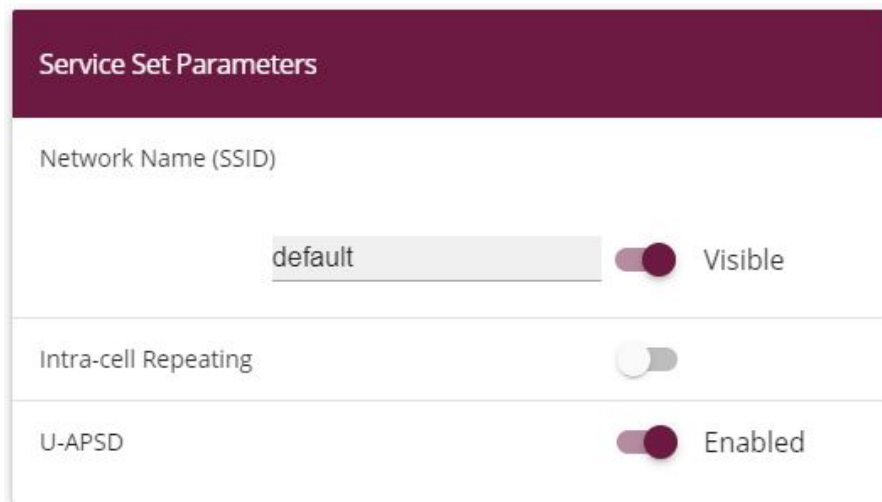



Fig. 17: **Wireless LAN** -> **WLAN** -> **Wireless Networks (VSS)** -> 

- (2) Disable **Intra-cell Repeating**.
- (3) Confirm with **OK**.

Configure RADIUS Server access

Two entries must be created for access to the RADIUS server. The RADIUS server is a component of the central bintec Hotspot server. Use the IP address `62.245.165.180` and the password `funkwerk-ec` for RADIUS server login.

In the **System Management** -> **Remote Authentication** -> **RADIUS** menu, a list of all registered RADIUS servers is displayed.

To configure the first entry, go to the following menu:

- (1) Go to **System Management** -> **Remote Authentication** -> **RADIUS** -> **New**.

Basic Parameters

Authentication Type	Accounting ▼
Vendor Mode	bintec HotSpot Server ▼
Server IP Address	62.245.165.180
RADIUS Secret	••••••
Default User Password	••••••
Priority	2 ▼
Entry active	<input checked="" type="checkbox"/> Enabled
Group Description	Default Group 0 ▼

Fig. 18: **System Management -> Remote Authentication -> RADIUS -> New**

Advanced Settings

Server Options

Policy	Non-authoritative ▾
UDP Port	1813
Server Timeout	3000 <small>Milliseconds</small>
Alive Check	<input checked="" type="checkbox"/> Enabled
Retries	3

Fig. 19: System Management -> Remote Authentication -> RADIUS -> New->Advanced Settings

Proceed as follows:

- (1) In **Authentication Type**, select *Accounting*.
- (2) As the **Vendor Mode** choose *bintec HotSpot Server*.
- (3) Enter the **Server IP Address** *62.245.165.180* of the RADIUS server.
- (4) Enter the **RADIUS Secret** *funkwerk-ec*.
- (5) Set **Priority** to *2*. The server with the highest priority will be used first.
- (6) Click **Advanced Settings**.
- (7) Select the **Policy** type *Non-authoritative*.
- (8) Set **Server Timeout** to *3000*.
- (9) Set **Retries** to *3*.
- (10) Confirm with **OK**.

To configure the second entry, go again to the menu:

- (1) Go to **System Management -> Remote Authentication -> RADIUS -> New**.

Proceed as follows:

- (1) In **Authentication Type**, select *Login Authentication*.
- (2) Enter the **Server IP Address** *62.245.165.180* of the RADIUS server.
- (3) Enter the **RADIUS Secret** *funkwerk-ec*.
- (4) Set **Priority** to *1*.
- (5) Click **Advanced Settings**.
- (6) Select the **Policy** type *Non-authoritative*.
- (7) Confirm with **OK**.

2.3.2 Configuration of the bintec Hotspot server by the dealer

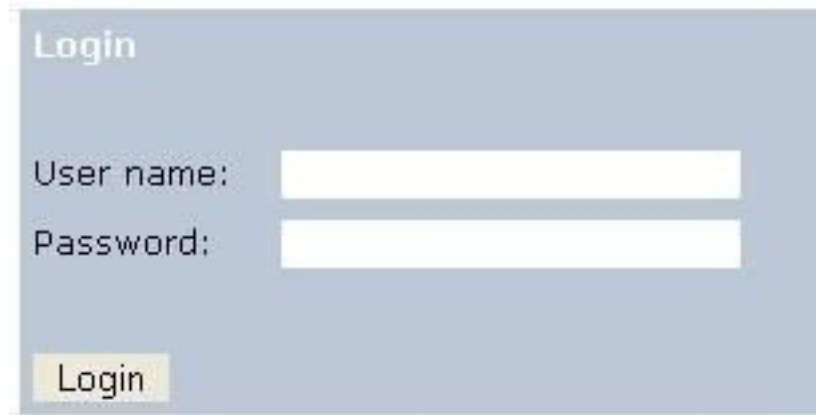
Dealers/service providers wishing to set up bintec Hotspot service receive the access data for an administrator access when ordering. This access allows the service provider to perform all relevant configurations and presets for his customers.

The dealer must determine these settings and configurations:

- Complete client profile
- Create users
- Create the desired rates
- Edit locality

Complete client profile

- (1) Launch an Internet browser and open the page at <https://hotspot.bintec-elmeg.com>.
- (2) Enter your user name in the **User name** field of the input window.
- (3) Enter your password in the **Password** field of the input window and click on the **Login** button.



The image shows a login form 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: "User name:" followed by a white rectangular box, and "Password:" followed by another white rectangular box. At the bottom left of the form, there is a yellow rectangular button with the word "Login" written in black text.

Fig. 20: Login

Proceed as follows to edit the client profile:

- (1) Go to **Client** -> **Overview**.

Edit client	
General	
Identifier	Roadshow
Street	Südwestpark 94
Zip code	90449
City	Nürnberg
Country	DE
Contact person	
First name	
Last name	
Telephone	
Fax	
E-Mail	
Language	English
Access Identifier	
Domain	
Additional text	<input type="text"/>
Additional text English	<input type="text"/>
Bill part	<input type="checkbox"/> Show
Passwords	<input checked="" type="radio"/> Only figures <input type="radio"/> Only chars <input type="radio"/> alphanumeric <input type="radio"/> Safe passwords
Password length	9 <input type="text"/>
General Voucher Password	-----
Logo (maximum 5MB, only jpeg or png)	<input type="button" value="Browse..."/> No file selected.
Terms and conditions	<input type="button" value="Browse..."/> No file selected. <input type="checkbox"/> Delete

Fig. 21: Client-> Edit Client

Proceed as follows:

- (1) Under **Logo** select the file with **Browse...** via the file browser. Under **Logo**, you can upload your company logo in PNG format. Your logo will appear on each printout. (The Logo of the users starting page, you can configure via edit template.)

- (2) Under **Terms and conditions**, you can upload your company-specific terms and conditions for the Hotspot. However, this is only necessary if you use the Default Free Service; usually, you'll save the general terms and conditions on your own webspace (refer to **Location->Overview->Upload Manager**).
- (3) Confirm your entries with **Save**.



Note

Under **Passwords** we recommend you to select the parameter *Only figures*. Thus, entering the password on Tablet PCs or with different keyboard layouts is made easier.

Create users

A list of all users is displayed in **Users -> Overview**. The dealer can create users. Proceed as follows:

- (1) Go to **User-> New assistant**.

New assistant > User overview <

Access Identifier

*User name: Hotel_Reception

Password: []

Password repeat: []

(Will generate automatically if no one is insert)

Authorisation group: Assistant

Location: All

Assistant data

First name: []

*Last name: Reception

Telephone: []

Fax: []

*E-Mail: test@test.de

Language: English
 German
 Spanish
 French
 Italian
 Portuguese
 Dutch

Submit cancel

* is required

> User overview <

Fig. 22: User -> New assistant

Die fields **User name**, **Last name** and **E-Mail** are required fields.

Proceed as follows:

- (1) Under **User name** enter *Hotel_Reception* for example.
- (2) Under **Authorisation group** select *Assisant*. The assistant can only manage accounts, e.g., as needed for a hotel reception. The administrator can manage localities, users, charges and accounts, but cannot create new clients.
- (3) Select a **Location**, in case several localities exist.
- (4) Under **Last name** enter the surname of the user, e.g. *Reception*.
- (5) Enter the **E-Mail** address of the user, e.g. *test@test.de*. The access data are automatically sent to the indicated e-mail address.
- (6) Confirm your entries with **Submit**.

Create rates

A list of all created rates is displayed in **Tariff** -> **Overview**. You can edit existing rates or create new ones.

- (1) Go to **Tariff** -> **New tariff** to create a new rate.

Fig. 23: **Tariff** -> **New tariff**

The **Identifier** field is a mandatory field.

Proceed as follows to create a new charge:

- (1) Under **Identifier** enter a identifier for the rate, *10 Minute Ticket* for example.
- (2) Enter the **Runtime**, e.g. *10* minutes.
- (3) Select the **Time unit (runtime)** *Total*.



Note

Note that the available time begins to run when the user logged in for the first time. Inactivity or logging out does not stop time from decreasing. *Total* means the overall available runtime while the *daily* setting provides the available runtime every day.

The price is a symbolic parameter displayed on the pint-out.

- (4) Under **Price** if applicable, enter a price in Euro, *1.00* for example.

- (5) Enter an end date for the runtime of a time or volume rate.
- (6) Under **Location** select *All*.
- (7) Confirm your entries with **Submit**.



Tip

If you wish to enter a permanent flatrate, under **Runtime** enter *1440* minutes and under **Time unit (runtime)** select *daily*.

Edit locations

In the menus for the desired login method, you can edit a location in the **Location-> Overview-> <Edit Location>** submenu. There, the upload manager allows you to upload your terms and conditions into the provided **Home** directory.

If you intend to create additional locations, you can purchase a corresponding license, enter your data and then activate the new location at www.bintec-elmeg.com under **Hotspot Licensing**.

2.3.3 Administration of Hotspot accounts

You can manage Hotspot accounts on-site via the <https://hotspot.bintec-elmeg.com/> user interface. You've already received the login data per e-mail.

Creation of an account

You can generate a new ticket for a Hotspot user. Here, you can choose between simple entry and advanced entry. For simple entry, go to the following menu:

- (1) Go to **Account -> New Account (easy)**.

Fig. 24: **Account -> New Account (easy)**

The fields **User name**, **Tariff** and **Last name** are required fields.

Proceed as follows:

- (1) Under **User name** enter *Guest_25* for example.
- (2) Select the **Tariff**, e.g. *2h Ticket*. The rate selection can be expanded by your administrator.
- (3) Under **Last name** enter *Lüdenscheid* for example.
- (4) Confirm your entries with **Submit**.

Click **>Help<** for additional information.

For advanced entry, go to the following menu:

- (1) Go to **Account -> New Account (extended)**.

New Account (extended) > Account - Search < > New Account (easy) < > help <

Access Identifier

* User name
 Password
 Password repeat
 (Will generate automatically if no one is insert)

* Tariff
 Valid from
 Valid until
 * Location
 Bintec-Elmeg-Support / Nr. 1
 Roadshow
 SE-Test
 Support NCR
 WBT

Groups

available

member

SSID

Template use this account as template

Personal data

Title

First name
 * Last name
 Room
 Addition
 E-Mail
 Telephone

data sheet
 in English
 download
 send per SMS

* is required

> Account - Search < > New Account (easy) < > help <

Fig. 25: Account -> New Account (extended)

Die fields **User name**, **Last name**, **Tariff** and **Location** are required fields.

Proceed as follows:

- (1) Under **User name** enter *Guest_26* for example.
- (2) Select the **Tariff**, e.g. *2h Ticket*. The tariff selection can be extended by your administrator.
- (3) Select the **Location**, e.g. *SE-Test*.

- (4) Under **Groups**, you can merge several tickets to a group and disable internet access for this group during a certain period.
Under **Account->Groups**, the existing groups are displayed. You can disable internet access for a group. To do so, click on the displayed number in the **actions** column of the desired group and then click on **New action**. In the **New group action** window, you can set the period for which to block internet access. This is useful, for example, to block internet access for students of a class during a test.
- (5) The **SSID** field is optional, and is printed on the ticket.
- (6) Under **First name** enter *Hans-Hubert* for example.
- (7) Under **Last name** enter *Lüdenscheid* for example.
- (8) Under **Room** enter *214* for example.
- (9) Confirm your entries with **Submit**.

Click **>Help<** for additional information.

Manage account

Under **Account**, you can enable a new ticket for a Hotspot user, delete accounts and read off the remaining time. In addition, you can print the access data for your customer or generate a PDF file.

- (1) Go to **Account -> Overview** to activate a new ticket.
To enable a newly-created user, you must first click on **Amount**. The display then switches to *Paid*.
Click **>Help<** for additional information.

The screenshot shows the 'Account - Search' interface. At the top, there are navigation links: '> New Account (extended) <', '> New Account (easy) <', and '> help <'. Below this is a search form with the following fields:

- Account State:** active (dropdown)
- User name:** (text input)
- Last name:** (text input)
- Tariff:** All (dropdown)
- Groups:** (dropdown)
- Online:** All (dropdown)
- search:** (button)

Below the search form is a table with the following columns: User name, Location, Name, Tariff, Amount, Time left, Capacity remains, and Online. The table contains two rows of data:

User name	Location	Name	Tariff	Amount	Time left	Capacity remains	Online
✓ 10min-1	SE-Test	10min-1	10MB/10Min	Payed	00:10:00	10 MB	No
✓ se-team	SE-Test	SE-Team	unbegrenzt	0,00 €	--:--:--	--	No

At the bottom of the table, there are navigation links: '> New Account (extended) <', '> New Account (easy) <', and '> help <'.

Fig. 26: **Account -> Overview**

2.3.4 Operation at several locations

The **bintec Hotspot Solution** allows operation of a Hotspot across locations. The Hotspot user tickets can be managed in a centralised or decentralised manner. It is possible to generate tickets which are only valid for a specific location, as it is possible to generate tickets that are valid for all locations.

As is generally known, the Hotspot server is centrally located and identical for all bintec customers (clients). Detection of which client is communicating with the Hotspot RADIUS server occurs over the so-called domain. At licence activation, this domain is issued over the licence portal (www.bintec-elmeg.com **Service & Support->Product Licencing -> HotSpot Licencing**) and entered at configuration of the **bintec RS353xx**. In the case of a solution with several locations, this domain is identical for all locations.

In order to nevertheless allow differentiation of locations, the *RadiusNasId* parameter is introduced.

Configuring the bintec Hotspot server

After you log in with your access data at <https://hotspot.bintec-elmeg.com>, all configured locations are displayed in the **Location -> Overview** menu.

Location overview					> Upload Manager <	> help <
Location	City	License	Valid until	Host		
✓ Bintec-Elmeg-Support / Nr. 1	Nürnberg	DEMO20420150107	2020-01-07			Overview
✓ Roadshow	Nürnberg	DEMO57020141107	2020-11-07			Overview
✓ SE-Test	DEU	DEMO57220151209	2020-12-09			Overview
✓ Support NCR	DEU	DEMO20520141021	2020-10-21			Overview
✓ WBT	Nürnberg	There is no license number registered.				Overview

Fig. 27: Location -> Overview

Upload Manager

Click **Upload Manager** in the **Location** menu to upload your company-specific terms and conditions, for example.

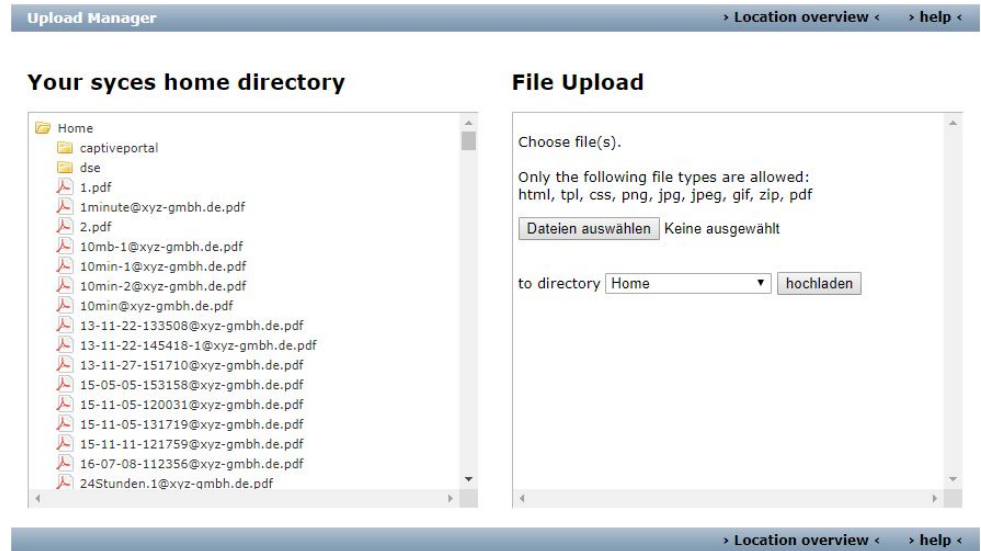


Fig. 28: Upload Manager

Click **>Help<** for information on how to use the upload manager.

Edit location

In **Location overview** select a *Location*. A detailed view of locations is now displayed. Here, you can edit **Location**.

Location edit		> Show host <	> Upload Manager <	> help <
General				
Identifier	Support NCR			
Street				
Zip code				
City	DEU			
Country	Germany			
Remark				
Contact person				
First name	Support			
Last name	Team			
Telephone				
Fax				
E-Mail	support@bintec-elmerg.com			
Walled Garden https://hotspot.bintec-elmerg.com/10.99.1/				
Registration type	Default Free service ▼			
Tariff	24-Stunden ▼			
Tickets	<input type="checkbox"/> have to be unlocked manual.			
Password	Auto generate and display ▼			
License				
License number	DEMO20520110629			
Valid until	2011-06-29			

Fig. 29: Location edit

In the **Location edit** menu, you also have the option of switching to **Show host**.

- (1) Go to **Show host**.

Show host		> New host <	> Location overview <
Host	NAS-Identifier		
nureintest	nureintest		

Fig. 30: Show host

Here, the **NAS Identifier** is displayed, which is required for **bintec RS353xx** configuration of the parameter **Host for multiple locations** under **Local Services->Hotspot Gateway->Options**.

**Note**

Note that you can only use a tariff for a special location, if a NAS identifier is set here and entered in the gateway too.

If no NAS identifier is displayed, you can set it under **New host**.

If you now create an **Account** or a **Voucher**, under **Location** you can select a location or *All*.

If you select *All* the account is valid for all locations.

(1) Go to **Voucher** -> **New voucher** to create a voucher.

New voucher > Voucher - Search <

* **Quantity**

User name

- Consecutively (370:1, 370:2)
- Numeric (4798811)
- Alphanumeric small (a7z89vk)
- Alphanumeric (A7z89vK)

Prefix to Username

Password

Password repeat

(Will generate automatically if no one is insert)

* **Tariff**

Valid from

Valid until

Description

* **Location**

available

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

>> <<

selected

- All

* is required

> Voucher - Search <

Fig. 31: New voucher

Fill in the mandatory fields **Quantity**, **Tariff** and **Location**.

Proceed as follows:

- (1) Enter *100* for **Quantity**, for example.
- (2) Select a **Tariff**, e. g. *2h Ticket*. The rate selection can be extended by your administrator.
- (3) Under **Location** select *All*.
- (4) Confirm your entries with **Submit**.

2.4 Configuring login methods

The hotspot server provides the login page for the hotspot.

Features

- There are 3 designs available (standard blue, standard grey, custom).
- The design of the login page is optimised for PC, tablet PC and smartphones. The display adjusts automatically, depending on the device.
- The language is selected automatically and is the same as the language of the browser.
- Any guest who has logged in before is automatically logged in again (Cookie-based).

Authentication processes

The following authentication methods are available for hotspot login:

- Anonymous
- 1-Click
- SMS
- PayPal

Below, you will learn how to configure a particular authentication method for hotspot login.

2.4.1 Anonymous login

With this authentication method a user can log into a hotspot free of charge simply by accepting the General Terms and Conditions.

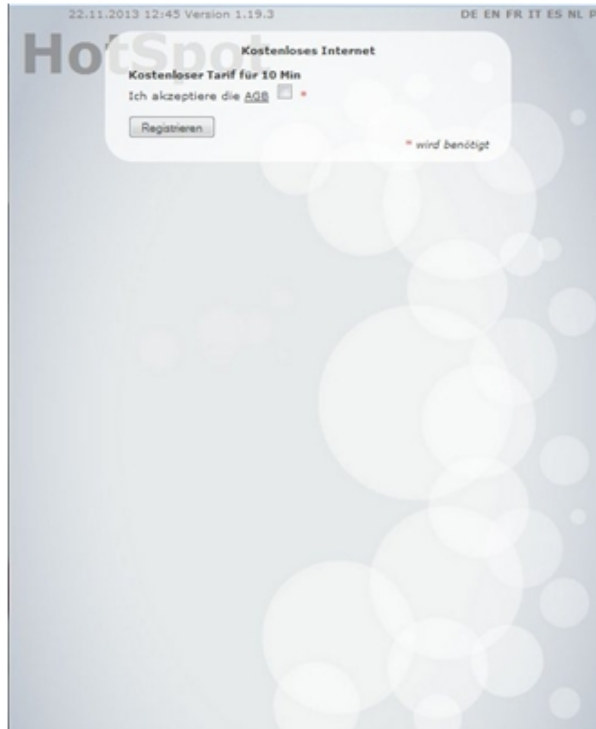


Fig. 32: Anonymous login

Configuring the bintec hotspot server

First, configure the authentication method on the hotspot server.

- (1) Start a Web browser, open the <https://hotspot.bintec-elmeg.com> page and enter your login data.
- (2) Go to **Location** -> **<Edit location>**.

Walled Garden (https://hotspot.bintec-elmeg.com/3/572/)	
Registration type	Anonymous login ▾
Tariff	5 Tage ▾
Prevent second registration for	<input type="text"/> Minutes ▾
Account validity	365 Days from first login ▾
Router Type	bintec > 9.1.4 ▾
URL of login page	<input type="text" value="http://192.168.1.254/auth"/>
Tickets	<input type="checkbox"/> have to be unlocked manuel.
Password	Auto generate and display ▾
Layout	Default gray ▾
Token Based Access	Accept Terms and Conditions first ▾

Fig. 33: Location -> <Edit location>

To create a new location, proceed as follows:

- (1) For the **Registration type**, select *Anonymous login*.
- (2) Select a **Tariff**, e. g. *5 Days*.
- (3) The **URL of login page** is the local IP address for the hotspot gateway, here e. g. *http://192.168.1.254/auth*.



Note

Note that the IP address appendix */auth* is essential for operation here.

- (4) Press **Submit** to confirm your entries.

Configuring the bintec gateway

Establish a web connection to the bintec gateway (e. g. **bintec RS353xx**).

- (1) Go to **Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1**



Basic Parameters

Interface	BRIDGE_BR0 -1
<input type="text" value="Domain at the HotSpot Server"/>	
Walled Garden	<input checked="" type="checkbox"/> Enabled
Walled Network / Netmask	<input type="checkbox"/> Disabled
Walled Garden URL	<input type="text" value="https://hotspot.bintec-elmeg.com/3/205"/>
Terms & Conditions	<input type="text" value="https://www.bintec-elmeg.com"/>
Additional freely accessible Domain Names	
<input type="text" value="Domain Name / IP Address"/>	
ADD	
<input type="text" value="Post Login URL"/>	
Language for login window	English ▼

Advanced Settings

Fig. 35: **Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1** ✎

Proceed as follows in order to configure Hotspot-Gateway:

- (1) Enable the **Walled Garden** function so that you can define a charge-free area on websites (intranet).
- (2) Enter the login page provided by the hotspot server as the **Walled Garden URL**, here e. g. <https://hotspot.bintec-elmeg.com/3/205/>.
- (3) In the **Terms & Conditions** input field enter the address of the General Terms and Conditions on the intranet server, or public server, e.g., <http://www.bintec-elmeg.com>. The page must lie within the address range of the walled garden network.
- (4) Disable the **Login Frameset** function. When the function is disabled, only the website with information, adverts and/or links to freely accessible websites is displayed.
- (5) Confirm with **OK**.

2.4.2 1-Click

With this authentication method a user can log into a hotspot free of charge by entering his email address.

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

Fig. 36: 1-Click login

Users have to enter their email address and accept the General Terms and Conditions. Then, they are logged in automatically as guests. They receive an email containing credentials so that they can log in with a second device if required.

Configuring the bintec hotspot server

First, configure the authentication method at the hotspot server.

- (1) Go to the **Location ->Overview-> <Edit location>** menu.

Walled Garden (<https://hotspot.bintec-elmeg.com/3/572/>)

Registration type	1-Click ▼
Tariff	5 Tage ▼
Prevent second registration for	<input type="text"/> Minutes ▼
Account validity	365 Days from first login ▼
Router Type	bintec > 9.1.4 ▼
URL of login page	<input type="text" value="http://192.168.1.254/auth"/>
Autologin	<input type="checkbox"/>
Tickets	<input type="checkbox"/> have to be unlocked manual.
Password	Auto generate and display ▼
Layout	Default gray ▼
Token Based Access	Accept Terms and Conditions first ▼

Fig. 37: Location ->Overview-> <Edit location>

To edit a location, proceed as follows:

- (1) The page provided by the hotspot server is displayed as a **Walled Garden** URL.
- (2) Here you select the *1-Click* login method under **Type**.
- (3) Select a **Tariff**, e. g. *5 Days*.
- (4) The **URL of login page** is the local IP address for the hotspot gateway, here e. g. *http://192.168.1.254/auth*.
- (5) Press **Submit** to confirm your entries.

Configuring the bintec hotspot gateway

Open a Web browser and establish a web connection to the bintec gateway (e. g. **bintec RS353xx**).

- (1) Go to **Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1**




Basic Parameters

Interface	BRIDGE_BR0 -1
<input type="text" value="Domain at the HotSpot Server"/>	
Walled Garden	<input checked="" type="checkbox"/> Enabled
Walled Network / Netmask	<input type="checkbox"/> Disabled
Walled Garden URL	<input type="text" value="https://hotspot.bintec-elmeg.com/3/205"/>
Terms & Conditions	<input type="text" value="https://www.bintec-elmeg.com"/>
Additional freely accessible Domain Names	
<input type="text" value="Domain Name / IP Address"/>	
ADD	
<input type="text" value="Post Login URL"/>	
Language for login window	English ▼

Advanced Settings

Advanced Parameter	
Ticket Type	Username/Password ▾
Allowed HotSpot Client	All ▾
Devices per ticket	1
Login Frameset	<input type="checkbox"/>
Pop-Up window for status indication	<input type="checkbox"/>
Default Idle Timeout	<input checked="" type="checkbox"/> Enabled 600 Seconds

Fig. 39: Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 

Proceed as follows in order to configure Hotspot-Gateway:

- (1) Enable the **Walled Garden** function so that you can define a charge-free area on websites (intranet).
- (2) Enter the login page provided by the hotspot server as the **Walled Garden URL**, here e. g. `https://hotspot.bintec-elmeg.com/3/205/`.
- (3) In the **Terms & Conditions** input field enter the address of the General Terms and Conditions on the intranet server, or public server, e.g., `http://www.bintec-elmeg.com`. The page must lie within the address range of the walled garden network.
- (4) Disable the **Login Frameset** function. When the function is disabled, only the website with information, adverts and/or links to freely accessible websites is displayed.
- (5) Confirm with **OK**.

2.4.3 SMS

With this authentication method users can register at a hotspot free of charge by entering their mobile phone number. They will be sent an SMS containing credentials that they needs to enter on the login page. Additionally, they have to accept the terms and conditions.

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

Fig. 40: SMS login

The service uses an SMS service provider to send access codes, www.lox24.de for example. **LOX24** requires an account to be created on www.lox24.de or www.lox24.eu. **LOX24** offers different tariffs, **Economy** for example. For starters, a test account can be created on **LOX24**.

Configuring the bintec hotspot server

- (1) Start a Web browser, open the <https://hotspot.bintec-elmeg.com> page and enter your login data.
- (2) Go to the **Client** -> **<Edit Client>** menu.

SMS Credentials (optional)	
SMS Provider	lox24 ▼
Account-ID	<input type="text"/>
Password	<input type="password"/>
API/Service-ID Economy	<input type="text"/>
API/Service-ID Pro	<input type="text"/>
API/Service-ID Direct	<input type="text"/>
Route Germany	Economy ▼
Route world wide	Economy ▼
	<input type="button" value="Submit"/> <input type="button" value="cancel"/>

Fig. 41: Client -> <Edit Client>

Proceed as follows:

- (1) Under **SMS Credentials** select **SMS Provider** *lox24*.



Note

Note that **smstrade** is also available, but it can not be used for new installations.

- (2) For the **Route Germany**, select the tariff, e. g. *Economy*.
- (3) Press **Submit** to confirm your entries.

Now select the **Login Method**.

- (1) Go to **Location** -> <Edit Location>.

Walled Garden (https://hotspot.bintec-elmeg.com/3/572/)	
Registration type	SMS ▼
Tariff	5 Days ▼
Preview SMS	DE EN FR IT ES NL PT
Prevent second registration for	<input type="text"/> Minutes ▼
Account validity	365 Days from first login ▼
Router Type	bintec > 9.1.4 ▼
URL of login page	<input type="text" value="http://192.168.1.254/auth"/>
Tickets	<input type="checkbox"/> have to be unlocked manuel.
Password	Auto generate and display ▼
Layout	Default gray ▼
Token Based Access	Accept Terms and Conditions first ▼

Fig. 42: Location -> <Edit Location>

Proceed as follows to edit the location:

- (1) The page provided by the hotspot server is displayed as a **Walled Garden** URL.
- (2) Here you select the *SMS* login method under **Registration type**.
- (3) Select a **Tariff**, e. g. *5 Days*.
- (4) The **URL of login page** is the local IP address for the hotspot gateway, here e. g. *http://192.168.1.254/auth*.
- (5) Press **Submit** to confirm your entries.

Configuring the bintec hotspot gateway

Establish a web connection to the bintec gateway (e. g. **bintec RS353xx**).

- (1) Go to **Local Services** -> **Hotspot Gateway** -> **Hotspot Gateway** -> **BRIDGE_BR0-1**



Basic Parameters

Interface	BRIDGE_BR0 -1
<input type="text" value="Domain at the HotSpot Server"/>	
Walled Garden	<input checked="" type="checkbox"/> Enabled
Walled Network / Netmask	<input type="checkbox"/> Disabled
Walled Garden URL	<input type="text" value="https://hotspot.bintec-elmeg.com/3/205"/>
Terms & Conditions	<input type="text" value="https://www.bintec-elmeg.com"/>
Additional freely accessible Domain Names	
<input type="text" value="Domain Name / IP Address"/>	
ADD	
<input type="text" value="Post Login URL"/>	
Language for login window	English ▼

Advanced Settings

Advanced Parameter	
Ticket Type	Username/Password ▾
Allowed HotSpot Client	All ▾
Devices per ticket	1
Login Frameset	<input type="checkbox"/>
Pop-Up window for status indication	<input type="checkbox"/>
Default Idle Timeout	<input checked="" type="checkbox"/> Enabled 600 Seconds

Fig. 44: Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 

Proceed as follows in order to configure Hotspot-Gateway:

- (1) Enable the **Walled Garden**, function so that you can define a charge-free area on websites (intranet).
- (2) Enter the login page provided by the hotspot server as the **Walled Garden URL**, here e. g. <https://hotspot.bintec-elmeg.com/3/205/>.
- (3) In the **Terms & Conditions** input field enter the address of the General Terms and Conditions on the intranet server, or public server, e.g., <http://www.bintec-elmeg.com>. The page must lie within the address range of the walled garden network.
- (4) Disable the **Login Frameset** function. When the function is disabled, only the website with information, adverts and/or links to freely accessible websites is displayed.
- (5) Confirm with **OK**.

2.4.4 PayPal

With the PayPal authentication method a fee-paying hotspot service is available.

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' in large white letters. The page is divided into two main sections:

- Anmelden (Login):** This section contains a form with fields for 'Benutzername' (username) and 'Passwort' (password). Below these fields is a checkbox labeled 'Ich akzeptiere die AOB' (I accept the terms of service) and a small icon. A 'Anmelden' button is located at the bottom left of this section. A red asterisk and the text '* wird benötigt' (required) are positioned at the bottom right.
- Registrieren über Paypal Account (Register via PayPal account):** This section includes a text box stating: '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). Below this is a 'Tarif' (tariff) dropdown menu currently set to '10 Minuten Ticket (1.00 €)'. At the bottom of this section is a prominent 'Express-Kauf PayPal' button with the PayPal logo. A red asterisk and the text '* wird benötigt' are at the bottom right.

Fig. 45: PayPal login

Users select a **Tariff**, e. g. *10 Minute Ticket (1.00 €)* and clicks on the **PayPal Express Buy** button. Then, the PayPal payment page is displayed. When users have made the payment they are automatically logged in. An email containing credentials is also sent to the email address registered at PayPal so that users can log in with a different device if desired.

A PayPal business account is required to use this service. It is free to register this type of account. PayPal charges a fee on the sums of money collected. Please refer to the PayPal website for details.

Configuring the bintec hotspot server

- (1) Start a Web browser, open the <https://hotspot.bintec-elmeg.com> page and enter your login data.
- (2) Go to **Client** -> **<Edit Client>**.

PayPal Credentials (optional)	
API Username	<input type="text"/>
API Password	<input type="password"/>
API Password repeat	<input type="password"/>
Signature	<input type="text"/>

Fig. 46: Client -> <Edit Client>

Enter the API login data (**API Username**, **API Password** and the **Signature**). You can access this data via your PayPal dealer account (Mein_Profil/mehr/Verkäufer_Händler/API-Zugriff).

Now select the **Registration type**.

- (1) Go to the hotspot server page at **Location** -> <Edit Location>.

Walled Garden (https://hotspot.bintec-elmeg.com/3/572/)	
Registration type	Paid service ▼
Tariff	All ▼
Prevent second registration for	<input type="text"/> Minutes ▼
Account validity	365 Days from first login ▼
Router Type	bintec > 9.1.4 ▼
URL of login page	<input type="text" value="http://192.168.1.254/auth"/>
Tickets	<input type="checkbox"/> have to be unlocked manuel.
Password	Auto generate and display ▼
Layout	Default gray ▼
Token Based Access	Accept Terms and Conditions first ▼

Fig. 47: Location -> <Edit Location>

To create a new location, proceed as follows:

- (1) The page provided by the hotspot server is displayed as a **Walled Garden** URL.
- (2) Here you select the *Paid service* **Registration type**.
- (3) The **URL of login page** is the local IP address for the hotspot gateway, here e. g. *http://192.168.1.254/auth*.
- (4) Press **Submit** to confirm your entries.

Configuring the bintec hotspot gateway

To configure the hotspot gateway, establish a web connection to the bintec gateway (e. g. **bintec RS353xx**).

- (1) Go to **Local Services** -> **Hotspot Gateway** -> **Hotspot Gateway** -> **BRIDGE_BR0-1**



Basic Parameters

Interface BRIDGE_BR0 -1

Domain at the HotSpot Server

Walled Garden Enabled

Walled Network / Netmask Disabled

Walled Garden URL
<https://hotspot.bintec-elmeg.com/3/205>

Terms & Conditions
<https://www.bintec-elmeg.com>

Additional freely accessible Domain Names

Domain Name / IP Address	
www.paypal.com	
api.paypal.com	
api-aa-3t.paypal.com	
notify.paypal.com	
www.paypalobjects.com	

ADD

Post Login URL

Language for login window English ▼

Advanced Settings

Advanced Parameter

Ticket Type	Username/Password ▾
Allowed HotSpot Client	All ▾
Devices per ticket	<input type="text" value="1"/>
Login Frameset	<input type="checkbox"/>
Pop-Up window for status indication	<input type="checkbox"/>
Default Idle Timeout	<input checked="" type="checkbox"/> Enabled <input type="text" value="600"/> Seconds

Fig. 49: Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1

Proceed as follows in order to configure Hotspot-Gateway:

- (1) Enable the **Walled Garden**, function so that you can define a charge-free area on websites (intranet).
- (2) Enter the login page provided by the hotspot server as the **Walled Garden URL**, here e. g. `https://hotspot.bintec-elmeg.com/3/205/`.
- (3) In the **Terms & Conditions** input field enter the address of the General Terms and Conditions on the intranet server, or public server, e.g., `http://www.bintec-elmeg.com`. The page must lie within the address range of the walled garden network.
- (4) Disable the **Login Frameset** function. When the function is disabled, only the website with information, adverts and/or links to freely accessible websites is displayed.
- (5) Confirm with **OK**.



Tip

Depending on the time of day it can take quite a while for the login page and the PayPal payment pages to load because of the high traffic density on the PayPal.com website. This also affects the PayPal logo on the login page because this is always loaded by PayPal.com.

With some browsers you can only avoid a security warning if you have called the **router login page** via https, for which an SSL certificate is required.

2.4.5 Default Free Service

Default Free Service is required so that previous installations will continue to work without changes. For new installations, **Default Free Service** is no longer available.

2.5 Instructions for safe operation

2.5.1 Multiple login

If configured, users can be logged in with multiple devices using a single coupon (user name, password). (Refer to **Devices per ticket** in the **Local Services->Hotspot Gateway->Hotspot Gateway->New->Advanced Settings** gateway menu.)

This is useful if they want to use a smartphone and a tablet at the same time, for example, or if there are multiple devices within a family.

2.5.2 Preventing mutual visibility of extensions

In a LAN or WLAN, all extensions at the IP level are connected to each other. This must naturally be prevented in a Hotspot system.

Hotspot with a single WLAN access point

Here, only one **bintec RS353xw** is employed as HotSpot gateway. All users are exclusively logged in over WLAN. Wired LAN is not used. Internet access is provided via a local network or ADSL.

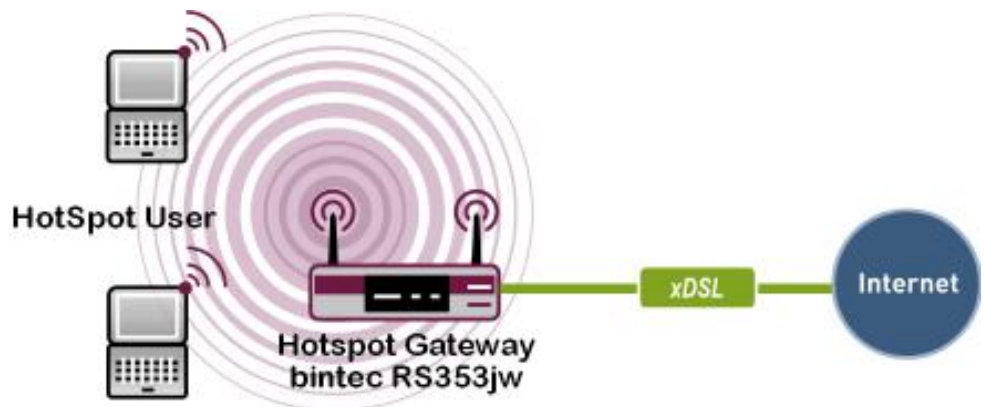



Fig. 50: Hotspot with a single WLAN access point

To prevent internal communication between Hotspot users (WLAN clients), in the menu **Wireless LAN -> WLAN -> Radio Settings ->** , the parameter **Intra-cell Repeating** must be disabled.

Hotspot with multiple WLAN access points

Here, several WLAN access points connected over LAN with the **bintec RS353xw** gateway are employed. Internet access is provided via a local network or ADSL.

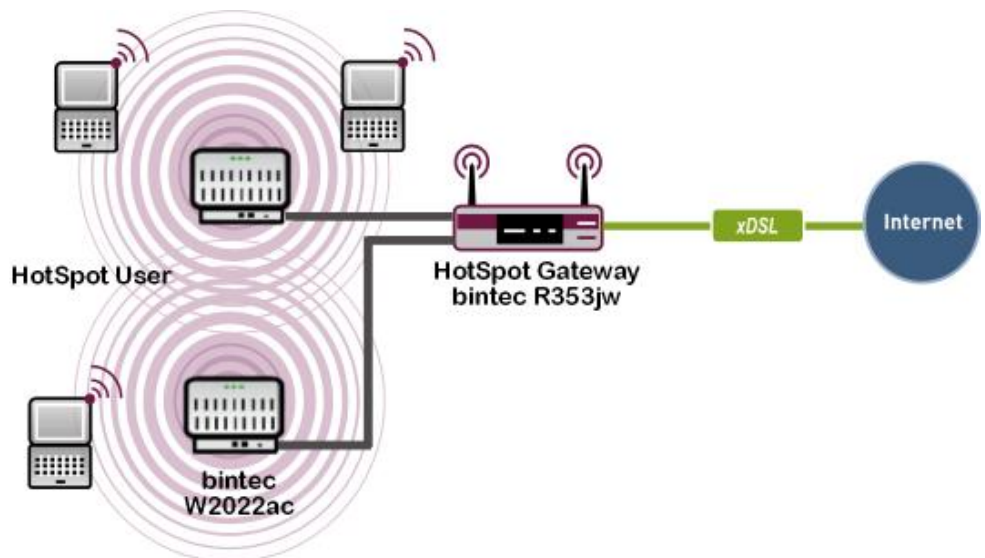


Fig. 51: Hotspot with multiple WLAN access points

To prevent visibility between Hotspot users (WLAN clients) for all WLAN workstations in the

menu **Wireless LAN** -> **WLAN** -> **Radio Settings** -> ✎, the parameter **Intra-cell Repeating** must be disabled. Further, a specific VLAN must be created for each WLAN access point to prevent internal communication between extensions logged into the various access points.

Hot Spot with Ethernet LAN clients

Here, several Hotspot users are connected to the Hotspot gateway over a LAN. Internet access is provided via a local network or ADSL.

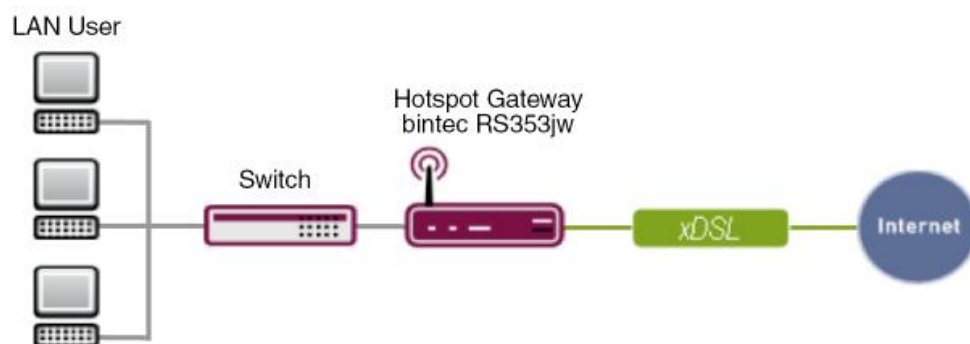


Fig. 52: Hotspot with Ethernet LAN client

A Hotspot user's PC is connected to a VLAN-capable switch. Here, each physical port of the switch has its own VLAN.

2.5.3 Encrypted/unencrypted WLAN connection

To facilitate user login to the Hotspot, most Hotspots operate without encryption.

This has the following disadvantages:

- All WLAN traffic may be intercepted by third parties with the requisite technical skill and equipment.
 - Coupon/login data for subscriber login to the Hotspot.
 - All visited websites, unless encrypted with SSL, https websites, for example. Bank websites are generally not affected, as these are SSL encrypted.
 - Non-SSL-encrypted emails.
 - Login data for non-SSL-encrypted email accounts.

**Note**

It is important to indicate this in the General Terms and Conditions.

2.5.4 WPA Encryption

To avoid the above disadvantages, the WLAN interface may for example be encrypted with WPA PSK. However, this does not yield much added security as this key must be known to all.

2.5.5 IP/ARP Spoofing

If the parameter **Allowed Peers** is set on *DHCP Clients* at gateway configuration, there occurs also a verification of the source *MAC+IP* for incoming packets. With IPv4A, a "spoofed" MAC+IP leads to an address conflict. This scenario is thus not intercepted.

2.6 Overview of configuration steps

Update of the gateway

Field	Menu	Value
Action	Maintenance -> Software & Configuration -> Options	Update system software
Source	Maintenance -> Software & Configuration -> Options	Current Software from Update Server



Configure language

Field	Menu	Value
Language for login window	Local Services -> Hotspot Gateway -> Hotspot Gateway -> New	e.g. English

Set time zone

Field	Menu	Value
Time Zone	System Management -> Global Settings -> Date and Time	Europe/Berlin
ISDN Timeserver	System Management -> Global Settings -> Date and Time	Disabled
Internal Time Server	System Management -> Global Settings -> Date and Time	Disabled

Disabling of local communication

Field	Menu	Value
Intra-cell Repeating	Wireless LAN Controller->Slave AP configuration -> Wireless Networks (VSS) -> 	Disabled
Intra-cell Repeating	Wireless LAN -> WLAN -> Wireless Networks (VSS) -> 	Disabled

Configure RADIUS Server access 1

Field	Menu	Value
Authentication Type	System Management -> Remote Authentication -> RADIUS -> New	<i>Accounting</i>
Vendor Mode	System Management -> Remote Authentication -> RADIUS -> New	<i>bintec HotSpot Server</i>
Server IP Address	System Management -> Remote Authentication -> RADIUS -> New	e.g. <i>62.245.165.180</i>
RADIUS Secret	System Management -> Remote Authentication -> RADIUS -> New	<i>funkwerk-ec</i>
Priority	System Management -> Remote Authentication -> RADIUS -> New	<i>2</i>
Policy	System Management -> Remote Authentication -> RADIUS -> New->Advanced Settings	<i>Non-authoritative</i>
Server Timeout	System Management -> Remote Authentication -> RADIUS -> New->Advanced Settings	<i>3000</i>
Retries	System Management -> Remote Authentication -> RADIUS -> New->Advanced Settings	<i>3</i>

Configure RADIUS Server access 2

Field	Menu	Value
Authentication Type	System Management -> Remote Authentication -> RADIUS -> New	<i>Login Authentication</i>
Server IP Address	System Management -> Remote Authentication -> RADIUS -> New	e.g. <i>62.245.165.180</i>
RADIUS Secret	System Management -> Remote Authentication -> RADIUS -> New	<i>funkwerk-ec</i>

Field	Menu	Value
Priority	System Management -> Remote Authentication -> RADIUS -> New	1
Policy	System Management -> Remote Authentication -> RADIUS -> New->Advanced Settings	Non-authoritative
Server Timeout	System Management -> Remote Authentication -> RADIUS -> New->Advanced Settings	3000
Retries	System Management -> Remote Authentication -> RADIUS -> New->Advanced Settings	3

Complete client profile

Field	Menu	Value
Logo	Client -> Edit Client	Browse...
Terms and conditions	Client -> Edit Client	Browse...

Create additional users

Field	Menu	Value
User name	User -> New assistant	e.g. <i>Hotel_Reception</i>
Authorisation group	User -> New assistant	<i>Assistant</i>
Location	User -> New assistant	<i>All</i>
Last name	User -> New assistant	e.g. <i>Reception</i>
E-Mail	User -> New assistant	e.g. <i>test@test.de</i>

Create rates

Field	Menu	Value
Identifier	Tariff -> New tariff	e.g. <i>10 Minutes Ticket</i>
Runtime	Tariff -> New tariff	<i>10 Minutes</i>
Time unit (capacity)	Tariff -> New tariff	<i>Total</i>
Price	Tariff -> New tariff	e.g. <i>1.00 euro</i>
Location	Tariff -> New tariff	<i>All</i>

Creation of an account (easy)

Field	Menu	Value
User name	Account -> New Account (easy)	e.g. <i>Guest_25</i>

Field	Menu	Value
Tariff	Account -> New Account (easy)	e.g. 2h Ticket
Last name	Account -> New Account (easy)	e.g. Lüdenscheid

Creating of an account (extended)

Field	Menu	Value
User name	Account -> New Account (extended)	e.g. Guest_26
Tariff	Account -> New Account (extended)	e.g. 2h Ticket
Location	Account -> New Account (extended)	e.g. SE-Test
First name	Account -> New Account (extended)	e.g. Hans-Hubert
Last name	Account -> New Account (extended)	e.g. Lüdenscheid
Room	Account -> New Account (extended)	e.g. 214

Manage account

Field	Menu	Value
Amount	Account -> Overview	Click Amount

Using the upload manager






Field	Menu	Value
Location	Location -> Overview	Location
Upload Manager	LocationUpload Manager	File Upload/Call help

Creating a voucher

Field	Menu	Value
Quantity	Voucher -> New Voucher	e.g. 100
Tariff	Voucher -> New Voucher	e.g. 2h Ticket
Location	Voucher -> New Voucher	All





Configuring login methods

Anonymous





Field	Menu	Value
Registration type	Location -> <Edit Location>	<i>Anonymous login</i>
Tariff	Location -> <Edit Location>	e.g. 5 Days
URL of login page	Location -> <Edit Location>	<i>ht-tp://192.168.1.254/auth</i>
Walled Garden	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 -> 	<i>Enabled</i>
Walled Garden URL	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 -> 	e.g. <i>ht-tps://www.hotspot.bintec-elmeg.com/3/205/</i>
Terms & Conditions	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 -> 	e.g. <i>ht-tp://www.hotspot.bintec-elmeg.com</i>
Login Frameset	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 ->  ->Advanced Settings	<i>Disabled</i>
Pop-Up window for status indication	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 ->  ->Advanced Settings	<i>Disabled</i>


1-Click

Field	Menu	Value
Walled Garden	Location -> Overview-> <Edit Location>	URL is displayed
Type	Location -> Overview-> <Edit Location>	<i>1-Click</i>
Tariff	Location -> Overview-> <Edit Location>	e.g. 5 Days
URL of login page	Location -> Overview-> <Edit Location>	e.g. <i>ht-tp://192.168.1.254/auth</i>
Walled Garden	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 -> 	<i>Enabled</i>

Field	Menu	Value
Walled Garden URL	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 -> 	e.g. <i>https://hotspot.bintec-elmeg.com/3/205</i>
Terms & Conditions	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 -> 	e.g. <i>https://www.bintec-elmeg.com</i>
Login Frameset	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 ->  ->Advanced Settings	<i>Disabled</i>
Pop-Up window for status indication	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 ->  ->Advanced Settings	<i>Disabled</i>

SMS

Field	Menu	Value
SMS Provider	Client -> <Edit Client>->	lox24
Account ID	Client -> <Edit Client>->	xxxxxxxxxxxxxxxxxxxx
Route Germany	Client -> <Edit Client>->	e.g. <i>Economy</i>
Registration type	Location -> <Edit Location>	<i>SMS</i>
Tariff	Location -> <Edit Location>	e.g. <i>5 Days</i>
URL of login page	Location -> <Edit Location>	e.g. <i>https://192.168.1.254/auth</i>
Walled Garden	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 -> 	<i>Enabled</i>
Walled Garden URL	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 -> 	e.g. <i>https://hotspot.bintec-elmeg.com/3/205</i>
Terms & Conditions	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 -> 	e.g. <i>https://www.bintec-elmeg.com</i>
Login Frameset	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 ->  ->Advanced	<i>Disabled</i>

Field	Menu	Value
	Settings	
Pop-Up window for status indication	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 -> ->Advanced Settings	<i>Disabled</i>

PayPal

Field	Menu	Value
API Username	Client-> <Edit Client>	xxxxxxxxxxxxxxxxxxxx
API Passwort	Client-> <Edit Client>	e.g. <i>supersecret</i>
API Passwort repeat	Client-> <Edit Client>	e.g. <i>supersecret</i>
Signature	Client-> <Edit Client>	xxxxxxxxxxxxxxxxxxxx
Registration type	Location -> <Edit Location>	<i>Paid service</i>
Tariff	Location -> <Edit Location>	e.g. <i>All</i>
URL of login page	Location -> <Edit Location>	e.g. <i>http://192.168.1.254/auth</i>
Walled Garden	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 -> 	<i>Enabled</i>
Walled Garden URL	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 -> 	e.g. <i>https://hotspot.bintec-elmeg.com/3/205</i>
Terms & Conditions	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 -> 	e.g. <i>http://www.bintec-elmeg.com</i>
Login Frameset	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 -> ->Advanced Settings	<i>Disabled</i>
Pop-Up window for status indication	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 -> ->Advanced Settings	<i>Disabled</i>

Chapter 3 WLAN - VoWLAN Basics and Configuration

3.1 General

When using a cordless phone, the user expects the best possible voice quality and excellent reliability.

The DECT (Digital Enhanced Cordless Telecommunications) standard has a high level of acceptance and fulfils those requirements. In contrast to WLAN, DECT uses its own reserved frequency range. Because DECT works in the 1.9 GHz range, the high frequency propagation characteristic is better than with WLAN, and this results in a greater coverage. So, with VoWLAN, more access points are also required than with DECT. WLAN was originally developed for data transmission by terminals whose location does not change. With VoWLAN, however, the wifi telephone's location is constantly changing. So VoWLAN must be capable of handing the connection over from one access point to the next access point (handover/roaming). This must be possible with no noticeable interruption to the connection (seamless handover). This feature is particularly important for installations in large enterprises in which multiple access points are being used.

The chapters that follow will show how this type of VoWLAN network has to be configured and set up so that the main quality features demanded of cordless telephony can be provided. We shall use the **bintec be.IP** oder **be.IP plus**, **bintec W2003ac-ext** WLAN access point, a **bintec RS123w** as WLAN controller, and the bintec-certified **Ascom i62**.

3.2 WLAN infrastructure

3.2.1 WLAN radio illumination

When faced with a WLAN infrastructure for data transmission, the design of the WLAN network for VoWLAN must be more closely meshed. In doing the planning, the WLAN supply to nearby areas also needs to be considered so that, for example, phone calls can be made in the coffee area. For the roaming to function perfectly and to achieve good voice quality, a supply with at least -70 dBm within a cell must be assured. The radio cells should also overlap by 6-10 dBm. The VoWLAN telephones and the access points should be set to maximum transmit power (20 dBm/100 mW).

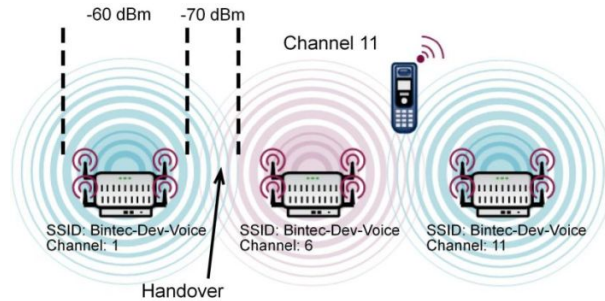


Fig. 53: List of minimum requirements for the WLAN radio frequency site survey for VoWLAN

With larger buildings, the three available non-overlapping radio channels, (e. g. 1, 6, 11) will need to be assigned more than once. For there to be no restrictions on performance it should be ensured that, within a radio cell on the same channel, there are no access points working that deliver a signal that is stronger than -80 dBm.

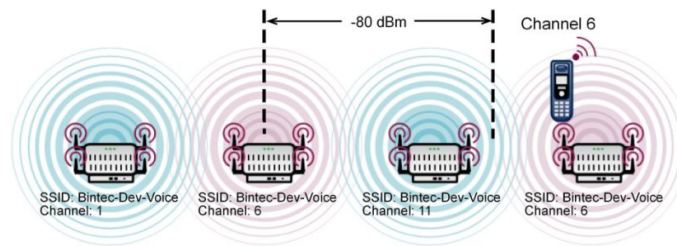


Fig. 54: Minimum space between two WLAN access points on the same transmit channel

When installing a VoWLAN it is essential to do an **Ekahau site survey** (www.ekahau.de) to plan the building's illumination and to identify the locations for the access points. A **site survey** uses PC-based planning software to inspect the building and calculate comprehensive illumination. It also identifies the best locations for the WLAN access points.

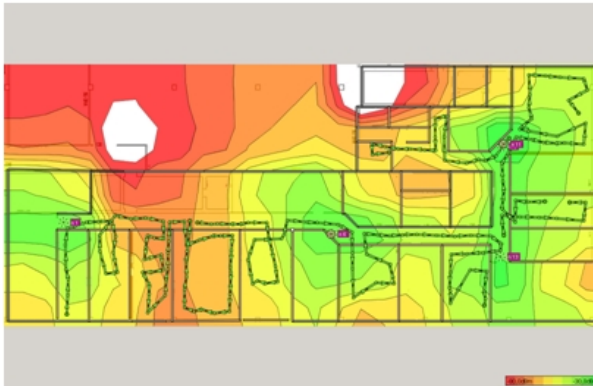


Fig. 55: Typical result of a site survey

3.2.2 Handover between the access points

For the handover between the access points to function correctly, all the access points need to use the same SSID. It is preferable that a separate SSID is used for the voice communication.

In the case of networks with 802.11g and 802.11n (20 MHz), the radio channels must have a channel spacing of 5 channels. So, e. g., only channels 1, 6 and 11 can be assigned without an overlap.

With some VoWLAN telephones (e. g. Ascom), a channel plan (e. g. channel 1, 6, 11) can be entered to optimise the handover between the access points. This means that, when the WLAN signal is weak, the telephone only searches for a new access point on the channels in the channel plan. This method enables a rather quicker handover. It is just important that, when doing the configuration, the telephone's channel plan is the same as the channels used in the WLAN network.

3.2.3 Bandwidth requirement

The maximum achievable gross data rate of a WLAN connection initially depends on the 802.11 operating mode used. But it should be noted that, when the distance between the access point and the terminal is on the large side, this gross rate can easily drop to the minimum gross rate. However, the actual net rate is only around 40-50 % of the gross rate.

802.11 operating mode	Maximum gross rate	Minimum gross rate
802.11b	11 Mbit/s	1 Mbit/s
802.11g	54 Mbit/s	6 Mbit/s
802.11n (1stream/20 MHz)	72.2 Mbit/s	7.2 Mbit/s

A voice channel requires around 100 kbit/s, but when doing the capacity planning it should be assumed that there are sufficient reserves in the basic channel to also be able to transmit each RTP packet immediately.

802.11g and 802.11n are mutually 100 % compatible, so a WLAN network can run in mixed mode with no problems. With 802.11b (11 Mbit/s), however, there is the peculiarity that a device with 802.11b (11 Mbit/s) pulls an entire network onto this low bit rate. 802.11b devices are still uncommon, so we strongly recommend that an operating mode that does not permit 802.11b is used. Therefore we recommend that "802.11g/n" is set up as the 802.11 operating mode in order to not permit 802.11b devices.

3.2.4 The safety standard and the handover

WLAN was originally developed for data transmission by terminals whose location does not change. With VoWLAN, however, the WLAN telephone's location is constantly changing. So a VoWLAN installation must be capable of handing the connection over from one access point to the next access point without any noticeable interruption to the connection (seamless handover). This feature is particularly important for installations in large enterprises in which multiple access points are being used. In particular, simple, cheap access points from the consumer sector, and older terminals too, often have problems here.

The WLAN security method selected also has a crucial impact on handover performance. When handing over from one access point to another access point with a better WLAN signal, once the connection has been established the WLAN security must be restored before the next voice data packet can be transmitted. We recommend WPA2-PSK, as this achieves a high level of security with, at the same time, excellent handover times (<40 ms).

We advise against using 802.1x or WPA2-Enterprise in wireless VoWLAN networks, because the restoring of security after a handover to a new access point takes far longer than with WPA2-PSK. This may then result in audible interruptions and interfering sounds.

3.2.5 QoS, WMM and U-APSD

For the terminals to achieve a long talk time and high standby times with one battery charge, both the terminals and the access points need to support relevant power saving mechanisms. U-APSD (Unscheduled Automatic Power Save Delivery) ensures that the terminal only transmits when necessary. During the terminal's sleep phase, the access point ensures that data packets which are to be sent to the telephone are temporarily stored and that the telephone is also woken up on time. Whether U-APSD functions correctly depends on the QoS class that is signalled, because U-APSD always has a reference to the QoS class. When doing the configuration, therefore, the manufacturer's recommendations should be complied with.

The voice data is transmitted as RTP (real-time transport protocol) data. To achieve the

transmitting of the RTP voice data packets between the IP PABX and the VoWLAN telephone with low latency times, the voice data needs to be given priority over the normal data.

This chapter describes how the prioritising of the voice data works in the LAN and the WLAN, and what relationship there is with the U-APSD power saving mechanism.

3.2.5.1 WMM priority classes and COS (Layer 2) mapping

The 802.11e standard defines four WMM access categories (AC's) for handling the data traffic in compliance with the QoS requirements.

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

802.11e also specifies a mapping between the LAN's Layer 2 (802.1d) Class of Service and the WLAN's WMM access categories.

Mapping table based on 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)
	5	AC_VI (video)
	6	AC_VO (voice)
Highest	7	AC_VO (voice)

The access points (**bintec W2003ac-ext**, **bintec W11003n**) have implemented the mapping in compliance with the 802.11e standard. The access points' WLAN driver does the mapping between the LAN's Layer 2 priority and the WLAN's WMM class, in both directions.

In the many IP networks (no VLAN or VLAN without Layer 2 priority), the QoS requirements for the data transmission are signalled using Layer 3 priority (TOS/DSCP). Therefore the WLAN access points need to support Layer 3 <- -> Layer 2 mapping.

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

The mapping above only includes the top three bits in the TOS/DSCP field, so it is relatively fuzzy and leads to problems with VoWLAN devices.

But most VoWLAN devices use as Class of Service Expedited Forwarding (EF) with DSCP value (0x2E / 101110 / 46) in compliance with RFC 4594. The mapping table above would map this class in the WMM Class 'AC_VI'. But this is incorrect, because the VoWLAN telephone uses "WMM AC 'AC_VO" for the opposite direction.

To avoid this problem, bintec access points map data tagged with "EF" in the following way:

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

Note: When doing the installation, the user only needs to be aware that the VoWLAN telephone and the IP PABX use as Class of Service Expedited Forwarding (EF) with DSCP value (0x2E / 101110 / 46). In the case of the **bintec be.IP plus** this value is preset.

3.2.5.2 U-APSD (Unscheduled Automatic Power Save Delivery)

U-APSD is a part of 802.11e and helps considerably in increasing the battery life of VoWLAN terminals. U-APSD must be supported both by the VoWLAN terminal and by the WLAN access point. U-APSD always only works for the WMM access category concerned, so it is important that the requirements listed in the chapter above are met.

The basic procedure works as follows:

- The VoWLAN terminal logs in with Class of Service Expedited Forwarding (EF) and U-APSD at the WLAN access point.
- The VoWLAN terminal then switches to power-save mode.
- If the WLAN access point is sent data packets for the VoWLAN terminal concerned with the Class of Service Expedited Forwarding (EF), the access point temporarily stores this data for a short time and waits until the VoWLAN terminal is woken up again. Only then is the data sent.
- The procedure works so rapidly that, even in the call status, the terminal still has enough time for the power-save mode.

Apart from the longer battery life, U-APSD has another positive effect. With longer phone calls, VoWLAN terminals with functioning U-APSD are far cooler than devices that do not support U-APSD.

U-APSD is supported by the access points (**bintec W2003ac-ext**, **bintec WI1003n**) upwards of relay 10.1.609.

3.2.6 WLAN controllers – A must in a VoWLAN network?

To optimise the handover, some manufacturers' solutions manage the WLAN data centrally in the WLAN controller. These solutions then use so-called thin APs, i. e. access points with no intelligence of their own. The disadvantage of these solutions is that all the data traffic is centrally decoupled so that a load is put on the networks. Since the introduction of 802.11n technology, the data volume has risen substantially, so solutions using thin APs have become even less significant in comparison with intelligent, fat APs. Since the introduction of the WPA2-PSK security standard and fast roaming in compliance with 802.11r, the handover problem in the case of WLAN solutions with fat APs has been resolved, too.

The **bintec WLAN Controller** solution works with intelligent access points (fat APs) that manage the basic data locally. This scenario has considerable performance benefits in comparison with thin client solutions. The **bintec WLAN Controller** is not obligatory for a VoWLAN installation, but it makes installation far easier and it simplifies system monitoring.

3.2.7 Potential sources of interference

The 2.4 GHz band is used by all sorts of wireless services as well as WLAN. Most of these services are limited to small transmission power and only have limited coverage. For instance, most Bluetooth devices that we often find in office environments only have a transmission power of 1 mW, so they are not really a problem for VoWLAN. For VoWLAN operations to be free of interference it is also important, of course, that there are as few third-party access points (neighbours) in the vicinity as possible. While these third-party access points do not actually interfere, they reduce the net bandwidth. This can be improved by, e. g., changing the channel plan so that your transmission bypasses the neighbouring access point. Particularly if a VoWLAN network is planned for a large number of subscribers, it may also be useful to install a second WLAN network with 5 GHz in order to bring the data applications to the free 5 GHz network.

In our experience, it is unusual for there to be unidentified sources of interference in VoWLAN applications if the basic rules described here are adhered to when doing the installation. Any broadband sources of interference or neighbouring access points that might lead to problems at a later stage are also identified by a site survey of the building, and counter measures can be taken in advance.

3.3 Example configuration

3.3.1 Network plan

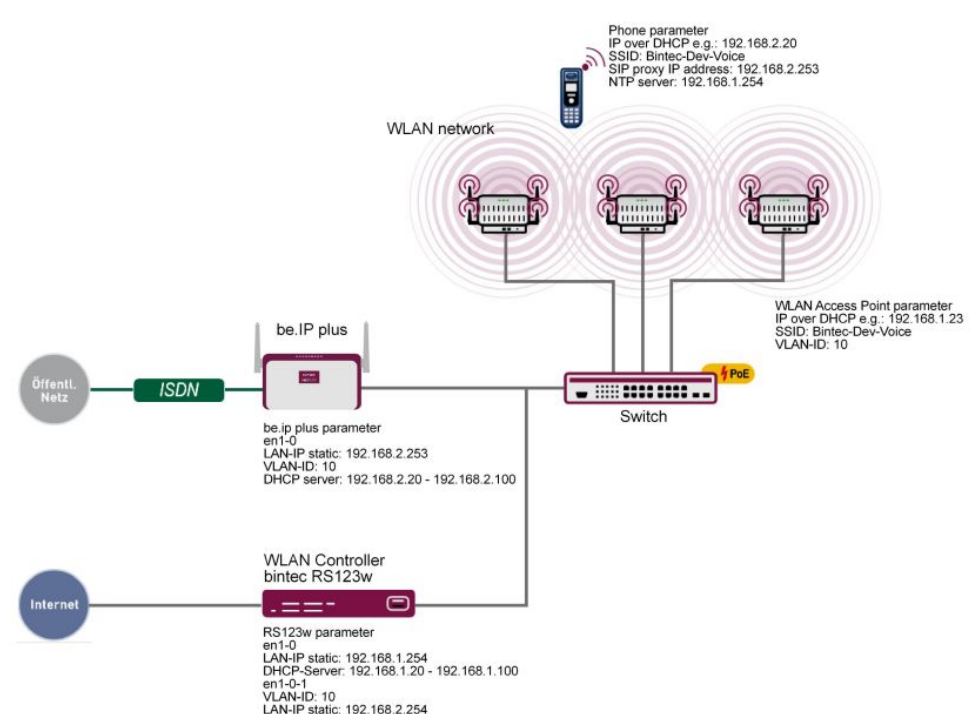


Fig. 56: Example scenario

The example configuration above shows a small application scenario, comprising an **bintec be.IP plus**, a **bintec RS123w** as the WLAN controller, three **bintec W2003ac-ext** access points and an **Ascom i62** VoWLAN telephone.

The LAN consists of two networks. Firstly the 192.168.1.0/24 network - this network is used for communications between the WLAN controller (**bintec RS123w**) and the access points.

The second network, 192.168.2.0/24, is tagged here with the **VLAN ID 10** and is used to transport the voice data. The **SSID Bintec-Dev-Voice** is assigned to the **VLAN-ID 10**, which means that only the voice data is sent between the VoWLAN telephone and the hybrid via the WLAN route.

bintec RS123w works as the WLAN controller and also provides the NTP time server (192.168.1.254) for the VoWLAN telephones.

3.3.2 WLAN configuration with or without WLAN controller

A VoWLAN network can be configured and operated via a WLAN controller or manually. As the handling work involved in a larger installation is far less when a WLAN controller is used, and is also more convenient in terms of monitoring, we recommend that a WLAN controller is deployed in installations with more than three access points.

The GUI (Graphical User Interface) is used to do the configuration.

To access the configuration interface enter the IP address **bintec RS123w** in your Web browser.

Go to **Wireless LAN Controller -> Slave AP Configuration -> Radio Profiles -> New**.

The screenshot displays two side-by-side configuration panels. The left panel, titled 'Radio Profile Definition', contains three rows: 'Description' with a text input field, 'Operation Mode' with a dropdown menu set to 'Access Point', and 'Operation Band' with a dropdown menu set to '2.4 GHz In/Outdoor'. The right panel, titled 'Performance Settings', contains four rows: 'Wireless Mode' with a dropdown menu set to '802.11g/n', 'Number of Spatial Streams' with a dropdown menu set to '2', 'Airtime fairness' with a toggle switch set to 'Enabled', and 'Cyclic Background Scanning' with a toggle switch set to 'Enabled'.

Fig. 57: **Wireless LAN Controller -> Slave AP Configuration -> Radio Profiles -> New**

Proceed as follows:

- (1) For **Operation Mode**, specify the mode in which the wireless module profile is to be run, here *Access Point*.
- (2) Select the **Operation Band** of the wireless module profile *2.4 GHz In/Outdoor*.
- (3) For **Number of Spatial Streams**, select how many traffic flows are to be used in parallel, e. g. *2* (default value): Two traffic flows will be used.
- (4) For **Wireless Mode**, select the wireless technology that the access point is to use, here *802.11 g/n*.
- (5) Click **Advanced Settings**.
- (6) Select the **Max. Transmission Rate**. With *Auto* (default value), the transmission speed is determined automatically.
- (7) Confirm with **OK**.

Then create the wireless network entries.

Go to **Wireless LAN Controller -> Slave AP Configuration -> Wireless Networks (VSS)-> New**.

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

- Service Set Parameters:**
 - Network Name (SSID): Bintec-Dev-Voice (Visible)
 - Intra-cell Repeating: Disabled
 - U-APSD: Enabled
 - IGMP Snooping: Disabled
- Client load balancing:**
 - Max. number of clients - hard limit: 32
 - Max. number of clients - soft limit: 28
 - Client Band select: Disabled - optimized for fast roaming
- VLAN:**
 - VLAN: Enabled
 - VLAN ID: 10
- Security Settings:**
 - Security Mode: WPA-PSK
 - WPA Mode: WPA 2
 - WPA2 Cipher: AES and TKIP (selected)
 - Preshared Key: *****
- MAC-Filter:**
 - Access Control: Disabled
 - Dynamic blacklisting: Disabled
- Bandwidth limitation for each WLAN client:**
 - Rx Shaping: No limit
 - Tx Shaping: No limit

Fig. 58: Wireless LAN Controller -> Slave AP Configuration -> Wireless Networks (VSS) -> New

Proceed as follows:

- (1) Enter the **Network Name (SSID)** for the wireless network, e. g. *Bintec-Dev-Voice*.
- (2) Disable **Intra-cell Repeating**. Communication between the WLAN clients within a radio cell is permitted.
- (3) Under **Security Mode**, select *WPA-PSK*.
- (4) For **WPA Mode**, select the encryption that is to be applied, here *WPA2*.
- (5) For **WPA2 Cipher**, select the encryption with which you wish to apply WPA, here *TKPI* and *AES*.
- (6) For **Preshared Key** enter the WPA password, e. g., *supersecret*. If the key has not been changed, your device will not be protected against unauthorised access!
- (7) Disable **ACL Mode**. All clients are permitted for this wireless network.
- (8) For **VLAN ID**, select the numerical value that identifies the VLAN, here *10*.
- (9) Confirm with **OK**.

3.4 Ascom i62 Talker configuration

3.4.1 Requirements

The following devices and software are required to configure the **Ascom i62**:

- **Ascom i62** Talker (EH1-AAAA/1A)
- Ascom Desktop Programmer (DP1-AAAA)
- Ascom WinPDM Version 3.8.1 or later
- Software version 2.1.20 or later
- Parameter version 13.3 or later

3.4.2 Configuration

3.4.2.1 Create a new telephone

- (1) Open the Ascom WinPDM program.
- (2) To create a new subscriber, go to **Numbers -> New**.
- (3) In the **Call number** field, enter the SIP number, e. g. *2011*.

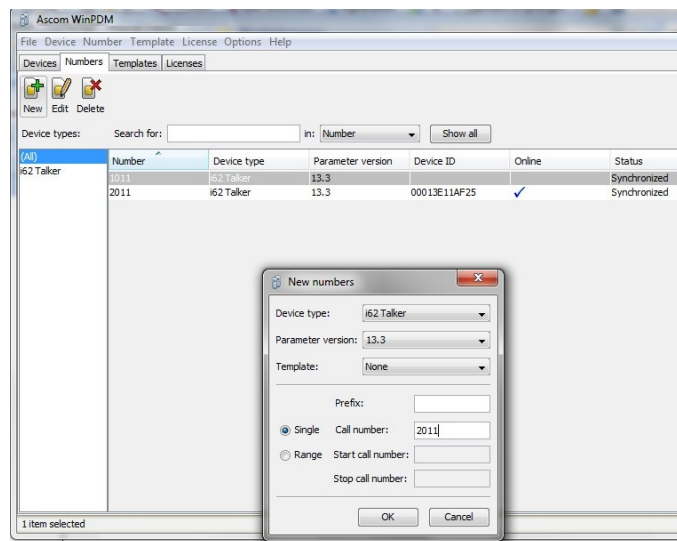


Fig. 59: **Numbers -> New**

Define a network

With the **Ascom i62**, four WLAN networks (networks A to D) can be defined.

Go to **Network** -> **Network B**.

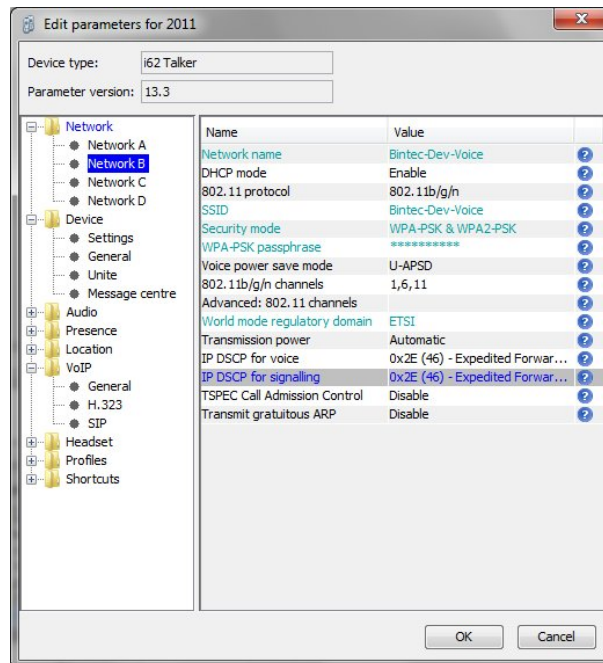


Fig. 60: **Network** -> **Network B**

For it to operate, the following entries are required:

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

Device settings

Go to **Device** -> **Settings**.

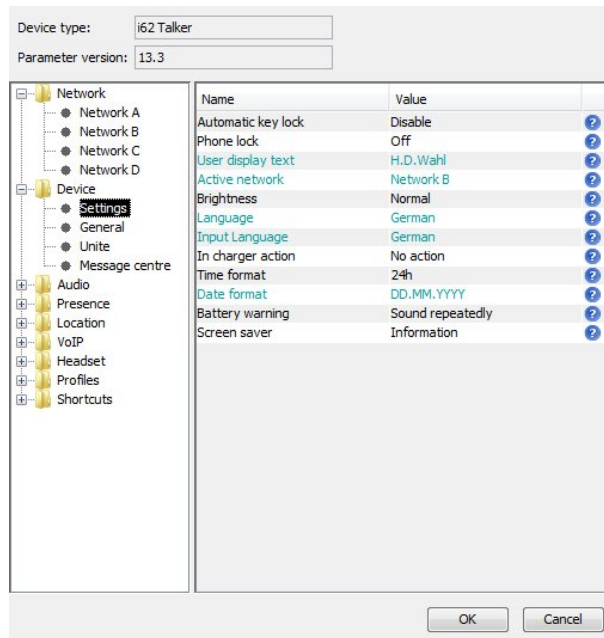


Fig. 61: **Device -> Settings**

For it to operate, the following entries are required:

Name	Value
User display text	e. g. bintec elmeg
Active Network	Network B

General device settings

Go to **Device -> General**.

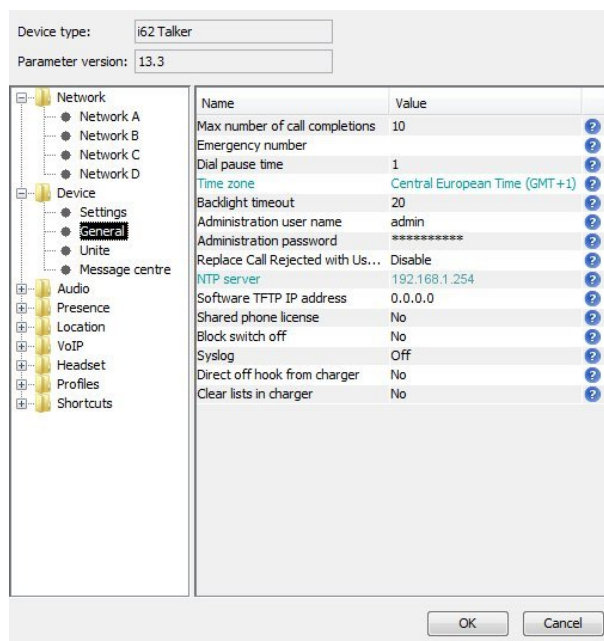


Fig. 62: Device -> General

For it to operate, the following entries are required:

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

General VoIP settings

Go to **VoIP -> General**.

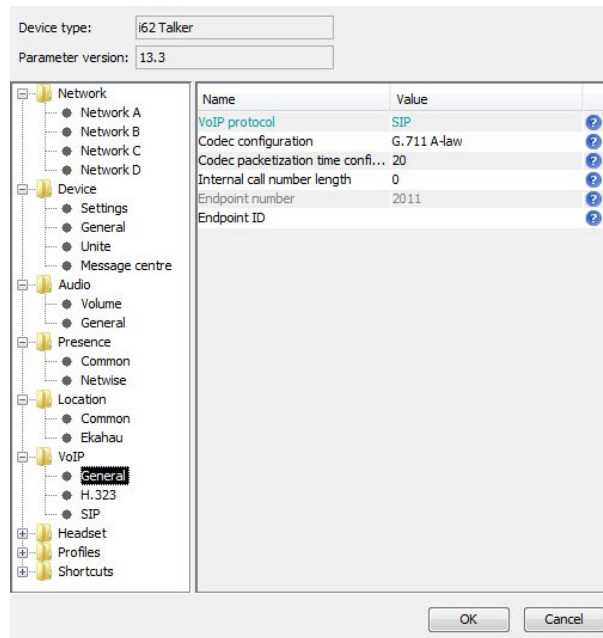


Fig. 63: VoIP -> General

For it to operate, the following entries are required:

Name	Value
VoIP protocol	SIP
Endpoint number	Displays the number of the device and cannot be modified here. The number is specified when the device's parameter set is generated.

SIP configuration

Go to **VoIP -> SIP**.

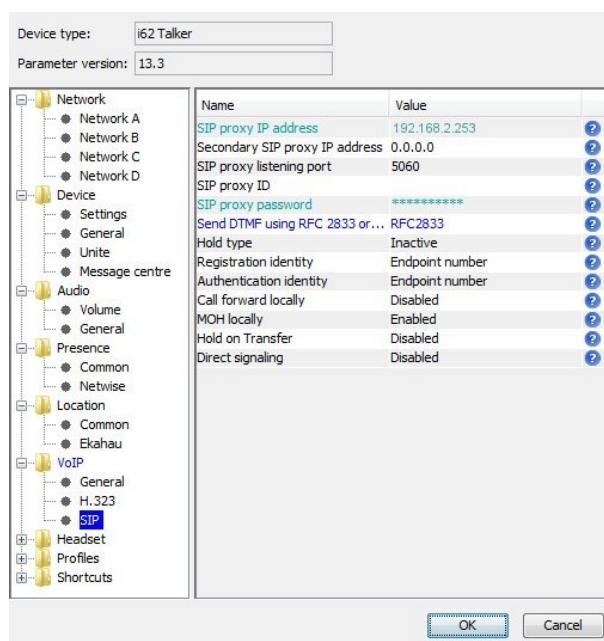


Fig. 64: VoIP -> SIP

For it to operate, the following entries are required:

Name	Value
SIP proxy IP address	192.168.2.253
SIP proxy password	e. g. supersecret
Authentication identity	Endpoint number (the number is used as the SIP username)

3.4.3 Test commands on the Ascom i62

The **Ascom i62** has certain test commands which are useful when installing it and troubleshooting:

*#76# Switches the RSSID display on/off

*#77# Switches the site survey tools on

3.5 Configuring the elmeg hybrid 300

3.5.1 Configuration

A SIP subscriber must be set up for the VoWLAN telephone. The DSCP value being set to 0x2E / 101110 / 46, which is vital, is taken into account as the default setting, so that no further change is required here.

In our example, the network interface of the **elmeg hybird 300** must be tagged with **VLAN ID 10**.

To access the configuration interface enter the IP address of the **elmeg hybird 300** in your Web browser.

Go to **LAN -> IP Configuration -> Interfaces -> New**.

Basic Parameters	Basic IPv4 Parameters
Based on Ethernet Interface: en1-4	Security Policy: <input type="radio"/> Untrusted <input checked="" type="radio"/> Trusted
Interface Mode: <input type="radio"/> Untagged <input checked="" type="radio"/> Tagged (VLAN)	Address Mode: <input checked="" type="radio"/> Static <input type="radio"/> DHCP
VLAN ID: 10	IP Address / Netmask: [IP Address] [Netmask] [ADD]
MAC Address: 00:a0:f9 <input checked="" type="checkbox"/> Use built-in	

Fig. 65: LAN -> IP Configuration -> Interfaces -> New

Proceed as follows:

- (1) For **Based on Ethernet Interface**, select the virtual interface, e. g. *en1-4*.
- (2) For **Interface Mode**, select *Tagged (VLAN)*.
- (3) For **VLAN ID**, enter *10*.
- (4) Confirm with **OK**.

3.5.2 Operational scenario: WLAN telephone cannot be accessed

A call to the WLAN telephone may fail if, for example, the subscriber is situated outside the range of an access point, the telephone is switched off, or if the battery is dead. To ensure calls are not lost, it is a good idea to set up **call forwarding on busy / on no reply** in the **elmeg hybird 300** for the extensions concerned.

Go to **Call Routing -> Outgoing Services -> Call Forwarding -> New**.

Basic Settings

Internal Number

Type of Call Forwarding

Target Number (On busy)
Enter Target Number without Line Access Digit.
Target Number (On busy)

Target Number (On no reply)
Enter Target Number without Line Access Digit.
Target Number (On no reply)

Fig. 66: Call routing -> Outgoing Services -> Call Forwarding -> New

Proceed as follows:

- (1) Select an **Internal Number** for which incoming calls are to be forwarded.
- (2) For **Type of Call Forwarding**, select *On busy / On no reply*.
- (3) Enter a **Target Number** to which incoming calls should be forwarded on busy or on no replay.
- (4) Confirm with **OK**.

3.6 Use other WLAN telephones

Other devices from other suppliers can, of course, be used apart from the **Ascom i62** VoWLAN terminals which we certify and recommend. Smartphones such as an **Apple iPhone** can also be used. Unfortunately, with these there are small differences in the performance, for example certain devices do not have U-APSD implemented or the roaming performance leaves something to be desired.

We have achieved good results with the devices listed here:

- **Apple iPhone 4** with bintec SIP APP (no U-APSD)
- **Nokia 6710**

3.7 Overview of Configuration Steps

Configure radio profiles

Action	Menu	Value
Operation Mode	Wireless LAN Controller -> Slave AP Configuration -> Radio Profiles -> New	Access Point
Operation Band	Wireless LAN Controller -> Slave AP Configuration -> Radio Profiles -> New	2.4 GHz In/Outdoor
Number of Spatial Streams	Wireless LAN Controller -> Slave AP Configuration -> Radio Profiles -> New	2
Wireless Mode	Wireless LAN Controller -> Slave AP Configuration -> Radio Profiles -> New	802.11 g/n
Max. Transmission Rate	Wireless LAN Controller -> Slave AP Configuration -> Radio Profiles -> New	Auto

Configure radio profiles

Action	Menu	Value
Network Name (SSID)	Wireless LAN Controller -> Slave AP Configuration -> Wireless Networks (VSS) -> New	e. g. <i>Bintec-Dev-Voice</i>
Intra-cell Repeating	Wireless LAN Controller -> Slave AP Configuration -> Wireless Networks (VSS) -> New	Disabled
Security mode	Wireless LAN Controller -> Slave AP Configuration -> Wireless Networks (VSS) -> New	WPA-PSK
WPA Mode	Wireless LAN Controller -> Slave AP Configuration -> Wireless Networks (VSS) -> New	WPA2

Action	Menu	Value
WPA2 Cipher	Wireless LAN Controller -> Slave AP Configuration -> Wireless Networks (VSS) -> New	AES and TKIP enabled
Preshared key	Wireless LAN Controller -> Slave AP Configuration -> Wireless Networks (VSS) -> New	e. g. <i>supersecret</i>
ACL Mode	Wireless LAN Controller -> Slave AP Configuration -> Wireless Networks (VSS) -> New	Disabled
VLAN ID	Wireless LAN Controller -> Slave AP Configuration -> Wireless Networks (VSS) -> New	10

Configure Ascom i62

Field	Menu	Value
Call number	Numbers -> New	e. g. 2011
DHCP mode	Network -> Network B	Enable
SSID	Network -> Network B	e. g. <i>Bintec-Dev-Voice</i>
Security mode	Network -> Network B	WPA-PSK & WPA2-PSK
WPA-PSK passphrase	Network -> Network B	e. g. <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	e. g. <i>bintec elmeg</i>
Active network	Device -> Settings	Network B
Time zone	Device -> General	Central European Time (GMT+1)
NTP server	Device -> General	e. g. 192.168.1.254
VoIP protocol	VoIP -> General	SIP
SIP proxy IP address	VoIP -> SIP	e. g. 192.168.2.253
SIP proxy password	VoIP -> SIP	e. g. <i>supersecret</i>

Field	Menu	Value
Authentication identity	VoIP -> SIP	<i>Endpoint number</i>

Configure interface

Field	Menu	Value
Based on Ethernet Interface	LAN -> IP Configuration -> Interfaces -> New	e.g. <i>en1-4</i>
Interface Mode	LAN -> IP Configuration -> Interfaces -> New	<i>Tagged (VLAN)</i>
VLAN ID	LAN -> IP Configuration -> Interfaces -> New	<i>10</i>

Configure call forwarding

Field	Menu	Value
Internal Number	Call routing -> Outgoing Services -> Call Forwarding -> New	Internal number
Type of call forwarding	Call routing -> Outgoing Services -> Call Forwarding -> New	<i>On busy/On no reply</i>
Target Number (On Busy)	Call routing -> Outgoing Services -> Call Forwarding -> New	Target number
Target Number (On no reply)	Call routing -> Outgoing Services -> Call Forwarding -> New	Target number

Chapter 4 WLAN Management for Multiple Locations: WLAN controller via VPN

4.1 Introduction

We shall now describe how to configure a bintec router from the **RS** series as the central WLAN controller for a WLAN infrastructure spread over more than one location (**bintec W2003ac** access points). A bintec router from the **RS** series is used, here, at the location concerned as a gateway for the Internet access.

The **GUI** (Graphical User Interface) is used for configuring.

Workshop task profile:

- A company has multiple locations that are to have WLAN installed. The plan is that all the employees will then be able to access the WLAN, and that it will be possible to manage it centrally.
- The employee's devices are to be automatically integrated into the company network by DHCP.
- The employees are to be able to use the WLAN to access both the Internet and the company's intranet. Access to the company intranet at head office and the field offices will be via the Internet using a VPN secured by IPSec.

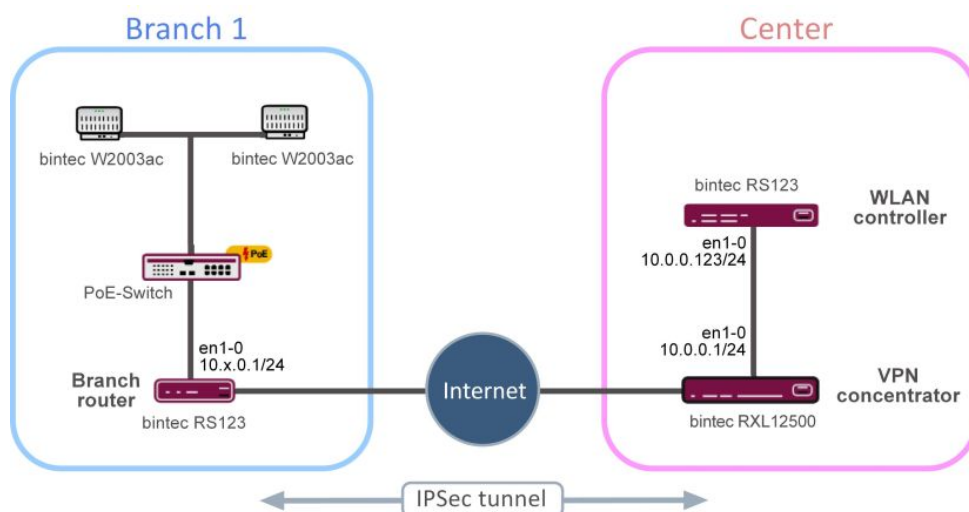


Fig. 67: Example scenario

4.1.1 Requirements

At company head office:

- Two bintec routers from the **RS** or **RXL** series, bintec be.IP or be.IP plus whose firmware version is at least **10.1.9**.

As examples, the workshop will use a **bintec RS123** as the WLAN controller and a **bintec RXL12500** as a VPN concentrator.

At the branch office:

- A bintec router with firmware which is at least version **10.1.9**. Routers from the **RS**, **TR** or the various **R** series (old **R2xx** series, old **Rxx00** series and new **RS** series) are used for Internet access in the branch office.

A **bintec RS123** is used as a branch router in the example.

- One or more bintec access points from the **bintec W2003ac** or **bintec WI1003n** with at least firmware version **10.1.9**. The minimum number of access points required depends on the size and building structure of the company location and can be accurately determined by a prior WLAN radio frequency site survey.

In this workshop, four **bintec W2003ac** access points are used in the example branch office.

- Internet access
- A PoE switch for the access points (optional).

4.1.2 About the test setup

Here you will find an overview of the interface assignment in the individual routers.

Router	Interface	Description	IP address / address range
Routers in the xth branch office	en1-0	LAN connection in the branch office	10.x.0.1/24
	en1-0	DHCP server for access points and WLAN devices in the branch office	10.x.0.10 to 10.x.0.254
VPN concentrator at head office	en1-0	LAN connection at head office	10.0.0.1/24
WLAN controller at	en1-0	IP address of the	10.0.0.123/24

Router	Interface	Description	IP address / address range
head office		WLAN controller which must be accessible in the entire VPN	
	en1-0	Default route on the VPN concentrator	10.0.0.1
	en1-0	WLAN controller for all access points in all the branch offices	

4.2 Configuration

4.2.1 Presettings

A functioning VPN needs to be set up in advance between the VPN concentrator at head office (in the workshop **bintec RXL12500**) and one or more branch routers (in the workshop **bintec RS123**). To install a VPN, please refer to the IP workshop »RIPv2 Routing Protocol over IPsec Connection«. In the settings for this workshop you need to replace the IP address ranges in the LAN segments concerned with the values from the table above. Please leave the other settings unchanged.

Using RIPv2 offers these benefits:

- All the routers listed above for use in the branch office can be used.
- The devices used are relative simple to set up.
- The configuration can easily be extended to other locations while live.

4.2.2 Configure the router in the field office

4.2.2.1 IP configuration

As a supplement to the IP workshop »RIPv2 Routing Protocol over IPsec Connection«, the first branch office router's IP interface is configured as follows.

- (1) Go the menu **LAN -> IP Configuration -> Interfaces -> <en1-0>** .

The screenshot displays two configuration panels for interface `en1-0`. The left panel, titled "Basic Parameters", shows "Interface Mode" set to "Untagged" (selected) and "Tagged (VLAN)" (unselected). The "MAC Address" is set to "00:09:4f:6f:5e:80" with the "Use built-in" option selected. The right panel, titled "Basic IPv4 Parameters", shows "Security Policy" set to "Trusted" (selected) and "Untrusted" (unselected). The "Address Mode" is set to "Static" (selected) and "DHCP" (unselected). Under "IP Address / Netmask", the "IP Address" field contains "10.1.0.1" and the "Netmask" field contains "255.255.255.0". An "ADD" button is visible at the bottom of the right panel.

Fig. 68: LAN -> IP Configuration-> Interfaces -> <en1-0> 

Proceed as follows:

- (1) In **Address Mode**, select *Static*.
- (2) In this field, enter the **IP Address / Netmask** e. g. *10.1.0.1* of the first branch office router. The IP addresses for the second, third, etc. branches are, as a result, *10.2.0.1*, *10.3.0.1*, etc. As the **Netmask** you select *255.255.255.0* in this case.
- (3) Leave the **Interface Mode** set to *Untagged*.
- (4) For **MAC Address**, leave *Use built-in* selected.
- (5) Confirm with **OK**.

4.2.2.2 Configure DHCP pool

You then need to create a DHCP pool on the interface concerned for all the devices in the LAN, such as the slave access points and the employee devices that will later be connected via the WLAN.

- (1) To do this, go to the menu **Local Services -> DHCP Server -> IP Pool Configuration -> New**.

The screenshot shows a configuration window titled "Basic Parameters" for a DHCP IP Pool. It contains the following fields:

- IP Pool Name:** A text input field containing the value "Devices".
- IP Address Range:** Two text input fields containing "10.1.0.10" and "10.1.0.254", separated by a hyphen.
- DNS Server:** Two text input fields. The top field contains "Primary" and the bottom field contains "Secondary".

Fig. 69: **Local Services -> DHCP Server -> IP Pool Configuration -> New**

Proceed as follows:

- (1) For the **IP Pool Name**, you can use *Devices*, for example.
- (2) For the **IP Address Range** for the first branch router, use e. g. *10.1.0.10* to *10.1.0.254*. This means that, in this case, another eight addresses are free below 10.1.0.10 for other statically configured devices.
- (3) Press **OK** to confirm your entries.

In the **Local Services -> DHCP Server -> DHCP Configuration -> New** menu, you can perform additional configuration.

The screenshot shows the 'Basic Parameters' configuration page. It features a dark purple header with the title 'Basic Parameters'. Below the header, there are three rows of configuration options, each with a label on the left and a dropdown menu on the right. The first row is 'Interface' with 'en1-0' selected. The second row is 'IP Pool Name' with 'Devices' selected. The third row is 'Pool Usage' with 'Local' selected. Below these rows is a text input field labeled 'Description'.

Advanced Settings:

The screenshot shows the 'Advanced Settings' configuration page. It features a dark purple header with the title 'Advanced Parameter'. Below the header, there are several sections. The first section is 'Gateway' with a dropdown menu set to 'Use router as gateway'. The second section is 'Lease Time' with a text input field containing '120' and the unit 'Minutes'. The third section is 'DHCP Options', which contains a table with two rows. The first row has 'DNS Server' as the option and '10.1.0.1' as the value. The second row has 'CAPWAP Controller' as the option and '10.0.0.123' as the value. Below the table is an 'ADD' button. The fourth section is 'Vendor Specific Information (DHCP Option 43)', which contains a text input field for 'Vendor ID' and another for 'Vendor Specific Information'. At the bottom of this section are two buttons: 'ADD VENDOR STRING' and 'ADD VENDOR GROUP'.

Fig. 71: Local Services -> DHCP Server -> DHCP Configuration -> New

Proceed as follows:

- (1) Select the **Interface** *en1-0*.
- (2) Select a valid **IP Pool Name**, here e. g. *Devices*.
- (3) The **Pool Usage** is set to *Local*.
- (4) Click **Advanced Settings**.
- (5) The setting *User Router as Gateway* is retained under **Gateway**. This means that all the DHCP-capable devices in the network can access the default gateway under the current IP address of interface *en1-0*.
- (6) The **Lease Time** is set to *120* minutes.
- (7) For **DHCP Options**, click **Add**.

- (8) First specify the DNS server's IP address. To do this, under **Option** select *DNS Server* and, under **Value**, enter the IP address of interface *en1-0* e. g. *10.1.0.1*.
- (9) Click **Add**.
- (10) Under **Option**, select *CAPWAP Controller* and, under **Value**, enter the IP address of the WLAN controller at head office, thus, in our case *10.0.0.123*.
- (11) Press **OK** to confirm your entries.



Note

It is not essential that you set up any other DHCP options for the slave access points and WLAN devices. However, configuring the *DNS domain name, time server*, etc. can be useful and depends on the infrastructure present.



Note

We do not recommend that you set up, on the branch router instead of the local DHCP server, a so-called **DHCP relay** to a DHCP server located at head office. Because that would mean that, at head office, you could no longer easily see from the slave access points' IP address range and from the employees' devices which branch the device concerned was located in. Moreover, if you were using **DHCP relay** and the Internet access or the VPN failed, the employees' devices might no longer be able to log into the relevant location's local network because they would no longer be getting an IP address via DHCP.

This completes the configuration of the branch router. Save the configuration with **Save configuration** and confirm the selection with **OK**.

4.2.3 Configure the VPN concentrator at head office

As a supplement to the IP workshop »RIPv2 Routing Protocol over IPsec Connection«, the IP interface of the VPN concentrator at head office is set up as follows.

- (1) Go to menu **LAN -> IP Configuration -> Interfaces -> <en1-0>** .

The image shows two side-by-side configuration panels. The left panel, titled 'Basic Parameters', has 'Interface Mode' with radio buttons for 'Untagged' (selected) and 'Tagged (VLAN)'. Below it, 'MAC Address' is '00:09:4f:6f:5e:80' with a 'Use built-in' toggle. The right panel, titled 'Basic IPv4 Parameters', has 'Security Policy' with radio buttons for 'Untrusted' and 'Trusted' (selected). 'Address Mode' has radio buttons for 'Static' (selected) and 'DHCP'. Below, 'IP Address / Netmask' shows 'IP Address' as '10.0.0.1' and 'Netmask' as '255.255.255.0' with a trash icon and an 'ADD' button.

Fig. 72: LAN -> IP Configuration-> Interfaces -> <en1-0> ✎

Proceed as follows:

- (1) For the **Address Mode**, select *Static*.
- (2) In this field, enter the **IP Address** e. g. *10.0.0.1* and the **Netmask** *255.255.255.0*.
- (3) Leave the **Interface Mode** set to *Untagged*.
- (4) Confirm with **OK**.

4.2.4 Configure the WLAN controller at head office

4.2.4.1 IP configuration

First of all you set the WLAN controller's IP parameters.

- (1) Go to **LAN -> IP Configuration -> Interfaces -> <en1-0>** ✎.

The image shows two side-by-side configuration panels. The left panel, titled 'Basic Parameters', has 'Interface Mode' with radio buttons for 'Untagged' (selected) and 'Tagged (VLAN)'. Below it, 'MAC Address' is '00:09:4f:6f:5e:80' with a 'Use built-in' toggle. The right panel, titled 'Basic IPv4 Parameters', has 'Security Policy' with radio buttons for 'Untrusted' and 'Trusted' (selected). 'Address Mode' has radio buttons for 'Static' (selected) and 'DHCP'. Below, 'IP Address / Netmask' shows 'IP Address' as '10.0.0.123' and 'Netmask' as '255.255.255.0' with a trash icon and an 'ADD' button.

Fig. 73: LAN -> IP Configuration-> Interfaces -> <en1-0> ✎

Proceed as follows:

- (1) For the **Address Mode**, select *Static*.
- (2) In this field, enter the **IP Address** e. g. *10.0.0.123* and the **Netmask** *255.255.255.0*.

- (3) Leave the **Interface Mode** set to *Untagged*.
- (4) Confirm with **OK**.

4.2.4.2 Set up the default route

The default route via interface *en1-0* to the VPN concentrator's IP address is then set up on the WLAN controller.

- (1) Go to **Network -> Routes -> IPv4 Route Configuration -> New**.

Basic Parameters		Route Parameters	
Route Type	Default Route via Interface	Local IP Address	10.0.0.1
Interface	LAN_EN1-0	Metric	1
Route Class	<input checked="" type="radio"/> Standard <input type="radio"/> Extended		

Fig. 74: **Network -> Routes -> IPv4 Route Configuration -> New**

Proceed as follows:

- (1) Set the **Route Type** to *Default Route via Interface*.
- (2) As the **Interface**, select *LAN_EN1-0*.
- (3) Under **Local IP Address**, select the IP address of the host to which your device will pass the IP packets, in this case the VPN concentrator's LAN ID address *10.0.0.1*.
- (4) Set the **Metric** of the route to e. g. *1* to select the route's priority. The lower the value, the higher the priority of the route.
- (5) Select **OK** to confirm your entries.

The IP routes overview then looks like this:

Routes							Extended Route		
Destination IP Address	Netmask	Gateway	Interface	Metric	Route Type				
0.0.0.0	0.0.0.0	10.0.0.1	LAN_EN1-0	1	Default Route via Interface	<input type="checkbox"/>			
10.0.0.0	255.255.255.0	10.0.0.151	LAN_EN1-0	0	Network Route via Interface	<input type="checkbox"/>			

Fig. 75: **Network -> Routes -> IPv4 Route Configuration**

This completes the configuration of the VPN concentrator. Save the configuration with **Save configuration** and confirm the selection with **OK**.

4.2.4.3 Configure WLAN controller

The WLAN controller itself can be activated now.

- (1) Go to **Wireless LAN Controller -> Controller Configuration -> General**.

The screenshot shows the 'Basic Settings' section of the Wireless LAN Controller configuration. The 'Status' is set to 'Enabled'. The 'Region' is set to 'Germany'. The 'Interface' is set to 'LAN_EN1-0'. The 'DHCP Server' is set to 'External or static'. The 'Slave AP location' is set to 'Remote (WAN)'. The 'Slave AP LED mode' is set to 'Status'.

Basic Settings	
Status	<input checked="" type="checkbox"/> Enabled
Region	Germany ▼
Interface	LAN_EN1-0 ▼
DHCP Server	DHCP Server with enabled CAPWAP option (138): <input checked="" type="radio"/> External or static <input type="radio"/> Internal
Slave AP location	<input type="radio"/> Local (LAN) <input checked="" type="radio"/> Remote (WAN)
Slave AP LED mode	Status ▼

Fig. 76: **Wireless LAN Controller -> Controller- Configuration-> General**

Proceed as follows:

- (1) The **Region** must be set up to match the location of the access points, e. g. *Germany*. The result of this setting is that the access points' WLAN wireless module will only run inside the legally permitted framework of the country concerned.
- (2) As the WLAN controller's **Interface**, select *LAN_EN1-0*.
- (3) The **DHCP Server** setting must be left at *External or static* because the DHCP server has already been set up on the branch office routers.
- (4) The **Slave AP location** must be changed to *Remote (WAN)*. The result of this is that managed slave access points continue to run autonomously if the network falls over (so that, at least, the local WLAN at the location affected goes on working) and are only reinitialized after reconnecting to the WLAN controller. Likewise, this switch is also used to adapt slave access points' and WLAN controllers' mutual waiting times to typical WAN characteristics (e. g. short network interruptions due to forced DSL separation).
- (5) Confirm with **OK**.

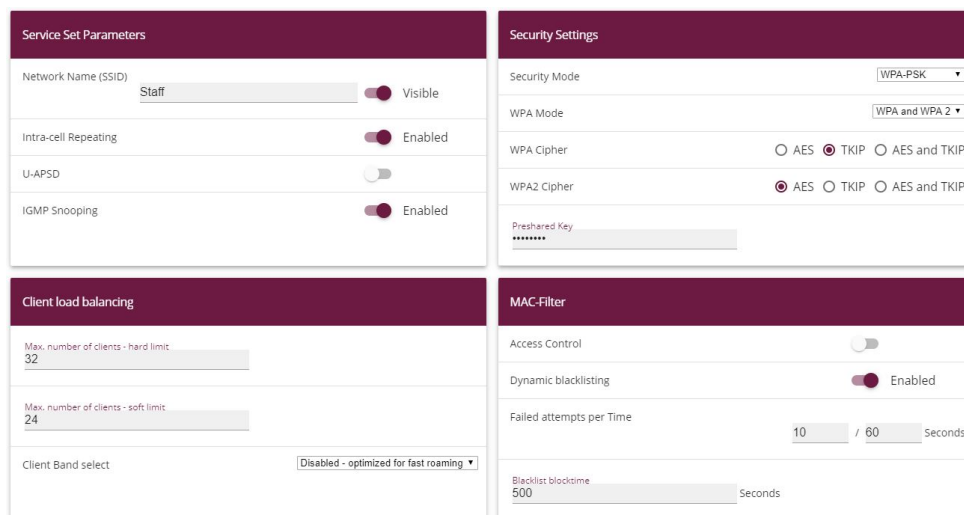
The settings are now enabled and the WLAN controller is started.

4.2.4.4 Configure wireless network profile

Next, the default existing profile for a wireless network is modified as follows.

- (1) Go to **Wireless LAN Controller -> Slave AP Configuration->Wireless Networks (VSS)**.

To do this, for the existing entry **<vss-1>** click the  symbol.



The screenshot displays the configuration interface for a wireless network profile, divided into four main sections:

- Service Set Parameters:**
 - Network Name (SSID): Visible
 - Intra-cell Repeating: Enabled
 - U-APSD: Disabled
 - IGMP Snooping: Enabled
- Security Settings:**
 - Security Mode: (dropdown)
 - WPA Mode: (dropdown)
 - WPA Cipher: AES TKIP AES and TKIP
 - WPA2 Cipher: AES TKIP AES and TKIP
 - Preshared Key:
- Client load balancing:**
 - Max. number of clients - hard limit:
 - Max. number of clients - soft limit:
 - Client Band select: (dropdown)
- MAC-Filter:**
 - Access Control: Disabled
 - Dynamic blacklisting: Enabled
 - Failed attempts per Time: / Seconds
 - Blacklist blocktime: Seconds


Fig. 77: **Wireless LAN Controller -> Slave AP Configuration->Wireless Networks (VSS)-> <vss-1>** 

Proceed as follows:

- (1) The **Network Name (SSID)** is change to e. g. *Staff*.
- (2) The default settings are left for **Intra-cell Repeating** and **Max. Clients**.
- (3) As the **Security Mode**, select *WPA-PSK*.
- (4) You can then leave the **WPA Mode** set to *WPA and WPA 2* .
- (5) For **WPA Cipher**, *TKIP* is enabled and, for **WPA2 Cipher**, *AES* is enabled.
- (6) The **Preshared Key** is the WLAN access password for all the employees. Enter an ASCII string with 8 - 63 characters.
- (7) Confirm with **OK**.

4.2.4.5 Configure Radio Profiles

In the next step, the **Radio Profiles** are edited. You configure the **Radio Profiles** by editing the default entry.

- (1) Go to **Wireless LAN Controller -> Slave AP configuration -> Radio Profiles**.
- (2) Where you have the existing entry **<2.4 GHz Radio Profile>**, click the  symbol.





Radio Profile Definition	Performance Settings
Description 2.4 GHz Radio Profile	Wireless Mode 802.11g/n
Operation Mode Access Point	Number of Spatial Streams 3
Operation Band 2.4 GHz In/Outdoor	Airtime fairness Enabled
	Cyclic Background Scanning Enabled

Advanced Settings

Advanced Parameter

Channel Plan User defined ▾

User Defined Channel Plan

Channel	
1 ▾	
5 ▾	
9 ▾	
13 ▾	

ADD

Beacon Period ms

DTIM Period

RTS Threshold

Short Guard Interval Enabled

Max. Transmission Rate Auto ▾

Short Retry Limit

Long Retry Limit

Fragmentation Threshold Bytes

Fig. 79: Wireless LAN Controller -> Slave AP configuration-> Radio Profiles-> <2.4 GHz Radio Profile> 

Proceed as follows:

- (1) The wireless module profile's **frequency range** is left at *2.4 GHz In/Outdoor*.
- (2) Change the **Wireless Mode** to *802.11g/n*.



Note

The result of changing the wireless mode is that older WLAN devices which are only based on the 802.11b transmission standard will no longer be able to use the WLAN. The main advantage of doing this, however, is to prevent any automatic reduction in bandwidth once a 802.11b is connected.

- (3) Enable the option **Burst Mode** to increase the transmission speed.
- (4) Click **Advanced Settings**.
- (5) Select the **Channel Plan** you require. *User-defined* enables you to select the channels you require yourself.
- (6) Under **User-defined**, select as the permitted channels *1, 5, 9 and 13*. This channel plan is the recommended ideal channel plan for every country where channels 1 to 13 are allowed and it does not have any (significant) frequency overlaps with 802.11g/n. This means that the access points have more choices for using a channel with minimal interference, which improves the performance and reliability of the entire WLAN.
- (7) Enable the **Short Guard Interval** function in order to reduce the guard interval (= time between transmitting two data symbols) from 800 ns to 400 ns.
- (8) The other settings remain unchanged and you save and leave the configuration menu with **OK**.

All the necessary profiles have now been set up in the WLAN controller.

4.2.4.6 Configure access points

Now the access points are enabled and set up.

- (1) Go to **Wireless LAN Controller -> Slave AP configuration-> Slave Access Points**.

In this overview, all the existing access points should be marked as *Found*. If this is not the case, we recommend that you take another look at the DHCP server settings on the branch office router. You should check, particularly, whether the CAPWAP option has been set up correctly. The VPN network connection from head office to the branch office may also be the cause of the fault. If these can be ruled out as the cause of the fault, an accidentally activated DHCP server on a device in the branch office may be causing the problem. This server must be deactivated and all the access points in the branch office disconnected from

the mains in order to get a fresh network configuration from the DHCP server. Another alternative is to wait for the so-called DHCP Lease Time to expire.

Now the wireless and VSS profiles that were set up previously can be set up on the access points that have been found. We shall now describe how to modify an access point for the location »Nbg - Shop«.

- (1) Go to **Wireless LAN Controller -> Slave AP Configuration-> Slave Access Points**



The screenshot shows two configuration panels. The left panel, titled 'Access Point Settings', includes fields for Device (W2003ac), Location (Nbg - Shop), Name (W2003ac), Description (Marketing), and CAPWAP Encryption (Enabled). The right panel, titled 'Radio Module1', includes Operation Mode (On), Active Radio Profile (2.4 GHz Radio Profile), Channel (Auto), Used Channel (6), Transmit Power (Max), and Assigned Wireless Network (VSS) with a table showing Profile (vss-1:Staff) and MAC Address (00:a0:f9:0b:cfe0).

Fig. 80: **Wireless LAN Controller -> Slave-AP Configuration -> Slave Access Points**

Proceed as follows:

- (1) A name that is as unambiguous as possible should be given as the **Location**, e. g. *Nbg - Shop*.
- (2) It is essential that the wireless module's **Operation Mode** is left as *On*. This means that the wireless module profile being used determines the operating mode.
- (3) Next the *2.4 GHz Radio Profile* that was configured previously is selected to be the **Active Radio Profile**.
- (4) The **Channel** is left as *Auto* so that it is determined dynamically using the wireless profile's channel plan and the WLAN environment.
- (5) Lastly, under **Assigned Wireless Networks (VSS)** and using the **Add** button, the wireless network *Staff* that has been configured is assigned to the wireless module.
- (6) The other settings are applied as they are. Confirm with **OK**.



Note

If an access point has two wireless modules, two configuration masks appear for **Wireless Module 1** and **Wireless Module 2**. They are set in the same way as in the previous example.

The other access points in the overview list are configured in exactly the same way as the first one was. Just one unique location name must be given to each access point, otherwise there is no longer any way to distinguish between the access points, e. g. when doing the WLAN network monitoring (in the menu **Wireless LAN Controller ->Monitoring**).

Once the access points have all been set up, they are given the status *Managed* in the overview under **Wireless LAN Controller ->Slave AP configuration-> Slave Access Points**, so they are now live. The WLAN controller is also blocking them against any sort of external configuration access.

Choose whether the selected Access Point is to be managed by the WLAN Controller by clicking the \wedge button or the \vee button in the **Action** column.

You can disconnect the Access Point from the WLAN Controller and therefore remove it from your WLAN infrastructure by click on the \vee button. The Access Point then receives the *Discovered* status, but is no longer *Managed*.

However, the WLAN channels shown in the menu (**Wireless LAN Controller ->Slave AP configuration -> Slave Access Points**) may not be ideal, e. g. in terms of one channel being assigned more than once. While being taken up and running, the access points were only able to tune into the general WLAN environment, not to each other. There are two ways of correcting this retrospectively: Either by using the **START** button to trigger the **New channel setting** action for all the managed access points at every location, or by triggering the channel search specifically for one affected access point by clicking the Refresh symbol in the **Channel search** column.

When the channel setting is complete, adjacent access points at any location ought to transmit on different channels.

The list of configured access points now looks like this:

Slave Access Points							
Location	Name	IP Address	LAN MAC Address	Channel	Search Channel	Status	Action
Nbg - Shop	W2003ac	10.1.0.14	00:01:cd:0f:4a:88	13 HT20 (auto)		Managed	\wedge \vee
Nbg - Back office	W2003ac	10.1.0.13	00:01:cd:0e:58:1a	9 HT20 (auto)		Managed	\wedge \vee
Nbg - Warehouse	W2003ac	10.1.0.12	00:01:cd:0e:b3:d0	5 HT20 (auto)		Managed	\wedge \vee
Nbg - Show room	W2003ac	10.1.0.10	00:01:cd:0e:8e:fa	1 HT20 (auto)		Managed	\wedge \vee

Fig. 81: **Wireless LAN Controller -> Slave-AP configuration -> Slave Access Points**

4.2.4.7 Set up an email alarm

An email alarm is then set up for the slave access points. This is to immediately and automatically notify the system administrators responsible about (WLAN) network problems at individual locations, including (indirect) faults due to Internet access and VPNs going down. When there are network problems, the access points become invisible to the WLAN controller and they are declared *offline* after a particular period of time, even if they are continuing to perform their service locally.

To be able to use the email alarm, you need to first set up an email server, and then a recipient for the alarm message.

- (1) Go to **External Reporting -> Alert Service -> Alert Settings**.

Fig. 82: **External Reporting -> Alert Service -> Alert Settings**

Proceed as follows:

- (1) The **Alert Service** must be enabled.
- (2) Enter an address that will be put in the email's sender field, e. g. *wlc@it.company.tld*.
- (3) You can use the value for **Maximum E-mails per Minute** to delimit the number of outgoing mails per minute, e. g. *6*.
- (4) Enter the IP address of the **SMTP Server** that is to be used to send the mails, e. g. *smtp.mail.com*.
- (5) You may wish to select an authentication method for the SMTP server.
- (6) Confirm with **OK**.

Finally, an email alarm is set up for the slave access points.

- (1) Go to **External Reporting -> Alert Service -> Alert Recipient -> New**.

Add / Edit Alert Recipient

Alert Service E-mail

Recipient

Message Compression Enabled

Subject

Event

Message Timeout
 Seconds

Number of Messages

Fig. 83: **External Reporting -> Alert Service -> Alert Recipient -> New**

Proceed as follows:

- (1) The email contact address of the system administrators responsible for this WLAN is entered as the **Recipient**, e. g. *admin@it.company.tld*.
- (2) Some information which should be kept as short as possible should be entered as the **E-Mail Subject**, e. g. *WLAN status: branches*.



Note





The content of an alarm email includes other information such as the reason for the alarm, the time of the event, and the device affected.

- (3) *Managed AP offline* must be entered as the **Event**.
- (4) Leave the remaining settings unchanged and confirm them with **OK**.

This completes the configuration of the WLAN controller-. Save the configuration with **Save configuration** and confirm the selection with **OK**.

4.3 Overview of Configuration Steps





Configure the router in the field office - IP configuration

Field	Menu	Value
Address mode	LAN -> IP Configuration-> Interfaces -> <en1-0> 	Static
IP Address / Netmask	LAN -> IP Configuration-> Interfaces -> <en1-0> 	IP address: e. g. 10.0.0.123 Net mask: e. g. 255.255.255.0
Interface Mode	LAN -> IP Configuration-> Interfaces -> <en1-0> 	Untagged:
MAC Address	LAN -> IP Configuration-> Interfaces -> <en1-0> 	Use Built-In





Configure the router in the field office - DHCP pool

Field	Menu	Value
IP pool name	Local Services -> DHCP Server -> IP Pool Configuration -> New	e. g. Devices
IP Address Range	Local Services -> DHCP Server -> IP Pool Configuration -> New	e. g. 10.1.0.10 - 10.1.0.254
Interface	Local Services -> DHCP Server -> DHCP Configuration -> New	en1-0
IP pool name	Local Services -> DHCP Server -> DHCP Configuration -> New	e. g. Devices
Pool Usage	Local Services -> DHCP Server -> DHCP Configuration -> New	Local
Gateway	Local Services -> DHCP Server -> DHCP Configuration -> New	Use Router as Gateway
Lease Time	Local Services -> DHCP Server -> DHCP Configuration -> New	e. g. 120
DHCP Options	Local Services -> DHCP Server -> DHCP Configuration -> New-> Add	DNS Server: e. g. 10.1.0.1 CAPWAP Controller: e. g. 10.0.0.123

Configure the VPN concentrator at head office

Field	Menu	Value
Address mode	LAN -> IP Configuration-> Interfaces -> <en1-0> 	Static
IP Address / Netmask	LAN -> IP Configuration-> Interfaces -> <en1-0> 	IP Address: e. g. 10.0.0.1 Netmask: e. g. 255.255.255.0
Interface Mode	LAN -> IP Configuration-> Interfaces -> <en1-0> 	Untagged:
MAC address	LAN -> IP Configuration-> Interfaces -> <en1-0> 	Use Built-In

Configure the WLAN controller at head office - IP configuration

Field	Menu	Value
Address mode	LAN -> IP Configuration-> Interfaces -> <en1-0> 	Static
IP Address / Netmask	LAN -> IP Configuration-> Interfaces -> <en1-0> 	IP Address: e. g. 10.0.0.123 Netmask: e. g. 255.255.255.0
Interface Mode	LAN -> IP Configuration-> Interfaces -> <en1-0> 	Untagged:
MAC address	LAN -> IP Configuration-> Interfaces -> <en1-0> 	Use Built-In

Configure the WLAN controller at head office - default route

Field	Menu	Value
Route Type	Network -> Routes-> IPv4 Route Configuration -> New	Default Route via Interface
Interface	Network -> Routes-> IPv4 Route Configuration -> New	LAN_EN1-0
Gateway	Network -> Routes-> IPv4 Route Configuration -> New	e. g. 10.0.0.1
Metric	Network -> Routes-> IPv4 Route	e. g. 1

Field	Menu	Value
	Configuration -> New	

Configure the WLAN controller at head office - WLAN controller







Field	Menu	Value
Region	Wireless LAN Controller -> Controller Configuration -> General	e. g. <i>Germany</i>
Interface	Wireless LAN Controller -> Controller Configuration-> General	<i>LAN_EN1-0</i>
DHCP Server	Wireless LAN Controller -> Controller Configuration-> General	<i>External or static</i>
Slave AP location	Wireless LAN Controller -> Controller Configuration-> General	<i>Remote (WAN)</i>











Configure the WLAN controller at head office - wireless network profile

Field	Menu	Value
Network Name (SSID)	Wireless LAN Controller ->Slave AP Configuration ->Wireless Networks (VSS)	e. g. <i>Staff</i> (visible)
Intra-cell Repeating	Wireless LAN Controller ->Slave AP Configuration ->Wireless Networks (VSS)	<i>Enabled</i>
ARP Processing	Wireless LAN Controller ->Slave AP Configuration ->Wireless Networks (VSS)	<i>Disabled</i>
WMM	Wireless LAN Controller ->Slave AP Configuration ->Wireless Networks (VSS)	<i>Enabled</i>
Max. Clients	Wireless LAN Controller ->Slave AP Configuration ->Wireless Networks (VSS)	e. g. <i>32</i>
Security mode	Wireless LAN Controller ->Slave AP Configuration ->Wireless Networks (VSS)	<i>WPA-PSK</i>
WPA Mode	Wireless LAN Controller ->Slave AP Configuration ->Wireless Networks (VSS)	<i>WPA and WPA 2</i>
WPA Cipher	Wireless LAN Controller ->Slave AP Configuration ->Wireless Networks (VSS)	<i>TKIP</i>



Field	Menu	Value
WPA2 Cipher	Wireless LAN Controller ->Slave AP Configuration ->Wireless Networks (VSS)	<i>AES</i>
Preshared key	Wireless LAN Controller ->Slave AP Configuration ->Wireless Networks (VSS)	String with 8 - 63 characters
ACL Mode	Wireless LAN Controller ->Slave AP Configuration ->Wireless Networks (VSS)	<i>Disabled</i>
Allowed Addresses	Wireless LAN Controller ->Slave AP Configuration ->Wireless Networks (VSS)	<i>None</i>
VLAN	Wireless LAN Controller ->Slave AP Configuration ->Wireless Networks (VSS)	<i>Disabled</i>







Configure the WLAN controller at head office - Radio Profiles

Field	Menu	Value
Description	Wireless LAN Controller -> Slave AP Configuration-> Radio Profiles-> 2.4 GHz Radio Profile> 	e. g. <i>2.4 GHz Radio Profile</i>
Operation Mode	Wireless LAN Controller -> Slave AP Configuration-> Radio Profiles-> 2.4 GHz Radio Profile> 	<i>Access Point</i>
Operation Band	Wireless LAN Controller -> Slave AP Configuration-> Radio Profiles-> 2.4 GHz Radio Profile> 	<i>2.4 GHz In / Outdoor</i>
Number of Spatial Streams	Wireless LAN Controller -> Slave AP Configuration-> Radio Profiles-> 2.4 GHz Radio Profile> 	<i>2</i>
Wireless Mode	Wireless LAN Controller -> Slave AP Configuration-> Radio Profiles-> 2.4 GHz Radio Profile> 	<i>802.11 g/n</i>
Max. Transmission Rate	Wireless LAN Controller -> Slave AP Configuration-> Radio Profiles-> 2.4 GHz Radio Profile> 	<i>Auto</i>
Burst Mode	Wireless LAN Controller -> Slave AP Configuration-> Radio Profiles-	<i>Enabled</i>

Field	Menu	Value
	> 2.4 GHz Radio Profile> 	
Channel plan	Wireless LAN Controller -> Slave AP Configuration-> Radio Profiles-> 2.4 GHz Radio Profile> 	<i>User-defined</i>
User-defined Channel Plan	Wireless LAN Controller -> Slave AP Configuration-> Radio Profiles-> 2.4 GHz Radio Profile> 	1, 5, 9, 13
Beacon Period	Wireless LAN Controller -> Slave AP Configuration-> Radio Profiles-> 2.4 GHz Radio Profile> 	100 ms
DTIM Period	Wireless LAN Controller -> Slave AP Configuration-> Radio Profiles-> 2.4 GHz Radio Profile> 	2
RTS Threshold	Wireless LAN Controller -> Slave AP Configuration -> Radio Profiles-> 2.4 GHz Radio  Profiles	2347
Short Guard Interval	Wireless LAN Controller -> Slave AP Configuration -> Radio Profiles-> 2.4 GHz Radio  Profiles	<i>Enabled</i>
Short Retry Limit	Wireless LAN Controller -> Slave AP Configuration -> Radio Profiles-> 2.4 GHz Radio  Profiles	7
Long Retry Limit	Wireless LAN Controller -> Slave AP Configuration -> Radio Profiles-> 2.4 GHz Radio  Profiles	4
Fragmentation Threshold	Wireless LAN Controller -> Slave AP Configuration -> Radio Profiles-> 2.4 GHz Radio  Profiles	2346 bytes

Configure the WLAN controller at head office - access points

Field	Menu	Value
Location	Wireless LAN Controller -> Slave AP Configuration-> Slave Access Points 	e. g. <i>Nbg - Shop</i>
CAPWAP Encryption	Wireless LAN Controller -> Slave AP Configuration-> Slave Access Points 	<i>Enabled</i>

Field	Menu	Value
Operation Mode	Wireless LAN Controller -> Slave AP Configuration-> Slave Access Points 	On
Active Radio Profile	Wireless LAN Controller -> Slave AP Configuration-> Slave Access Points 	e. g. 2.4 GHz Radio Profile
Channel	Wireless LAN Controller -> Slave AP Configuration-> Slave Access Points 	Auto
Used Channel	Wireless LAN Controller -> Slave AP Configuration-> Slave Access Points 	e. g. 13
Transmit Power	Wireless LAN Controller -> Slave AP Configuration-> Slave Access Points 	Max.
Assigned wireless networks (VSS)	Wireless LAN Controller -> Slave AP Configuration-> Slave Access Points 	e. g. Staff

Set up an email alarm - server

Field	Menu	Value
Alert Service	External Reporting -> Alert Service -> Alert Settings	Enable
Maximum E-mails per Minute	External Reporting -> Alert Service -> Alert Settings	e. g. 6
Sender E-Mail Address	External Reporting -> Alert Service -> Alert Settings	e. g. wlc@itcompany.tld
SMTP Server	External Reporting -> Alert Service -> Alert Settings	e. g. smtp.mail.com
SMTP Authentication	External Reporting -> Alert Service -> Alert Settings	e. g. None

Set up an email alarm - email recipient

Field	Menu	Value
Recipient	External Reporting -> Alert Service -> Alert Recipient -> New	e. g. admin@itcompany.tld
Message Compression	External Reporting -> Alert Service -> Alert Recipient -> New	Enabled

Field	Menu	Value
Subject	External Reporting -> Alert Service -> Alert Recipient -> New	e. g. <i>WLAN status: branches</i>
Event	External Reporting -> Alert Service -> Alert Recipient -> New	<i>Managed AP offline</i>
Message Timeout	External Reporting -> Alert Service -> Alert Recipient -> New	e. g. <i>60</i>
Number of Messages	External Reporting -> Alert Service -> Alert Recipient -> New	e. g. <i>1</i>

Chapter 5 WLAN - Wireless LAN Controller as Network Access Gateway

5.1 Introduction

We shall now describe how to configure a bintec router in the Rxx02 series as a WLAN controller for the local WLAN infrastructure (**bintec W2003ac** access points) and as the central access gateway in the WAN (Internet) with automatic network setup and firewall for devices in the WLAN and Ethernet LAN.

The **GUI** (Graphical User Interface) is used for configuring.

A company location should be equipped with Ethernet LAN and WLAN used separate by employees and guests:

- The computers and other devices of the two user groups should be automatically integrated into the network by DHCP and be able to access the Internet.
- Guests should not be able to access the employee intranet.
- However, employees ought to be able to access the guests' intranet, for example to be able to securely and quickly share selected documents with an external project partner on the premises within the company.
- Access to the network infrastructure should also be limited to system administrators.

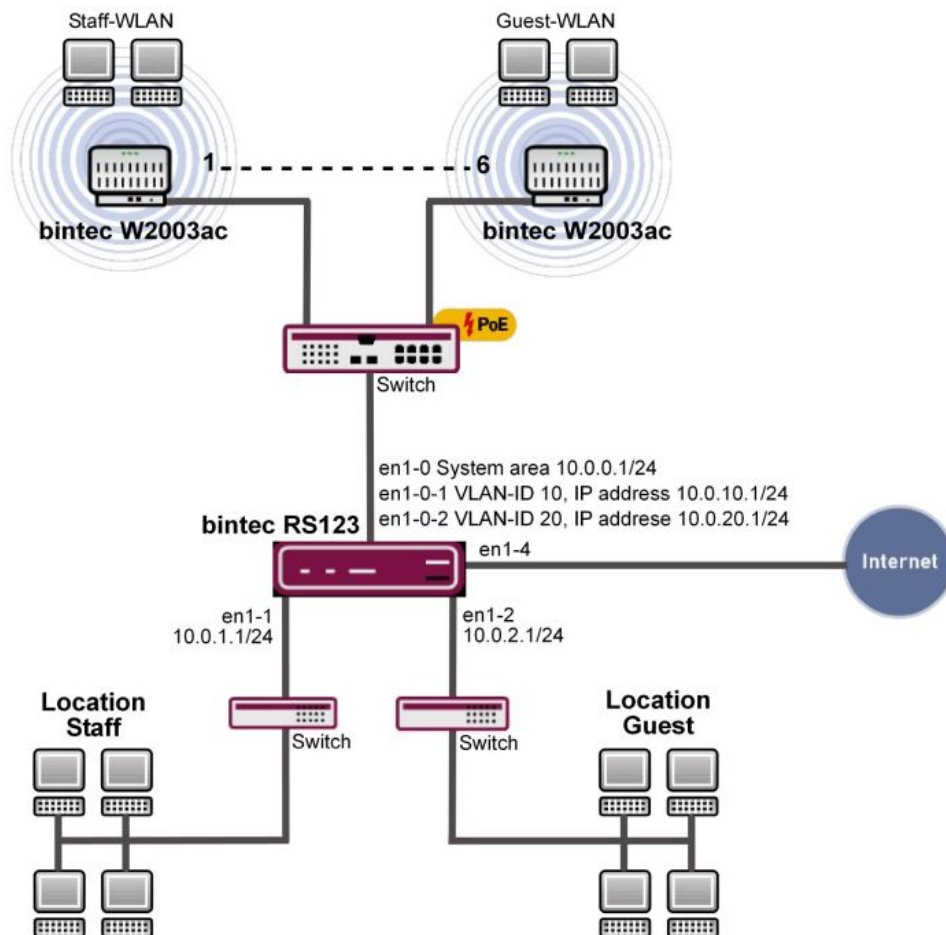


Fig. 84: Example scenario

Requirements

The following are required for the configuration:

- A Bintec router from the RS series, the RXL series, the **be.IP** or **be.IP plus**.
- Access points from the **bintec W2003ac** series or bintec Wlx0xxn series (e. g. **bintec WI1003n**). The minimum number of necessary access points depends on the size and building structure of the company location and can be accurately determined by a prior WLAN radio frequency site survey (see the WLAN Controller introduction for more on this). In our example, we use 5 **bintec W2003ac**'s and one **bintec WI1003n**.
- A boot image with at least version 10.1.9 for the Bintec router

- A boot image with at least version 10.1.9 for the access points
- Internet access at the company location.
- At least one PoE switch for the access points and other switches for the LAN.

About the test setup

Overview of interface configuration on the Bintect router:

en1-0	System area	IP address 10.0.0.1/24: DHCP server for access points and the WLAN controller interface
en1-0-1	Staff WLAN	Virtual interface via en1-0 with VLAN ID 10, IP address 10.0.10.1/24: DHCP server and gateway for the employee WLAN
en1-0-2	Guest WLAN	Virtual interface via en1-0 with VLAN ID 20, IP address 10.0.20.1/24: DHCP server and gateway for the employee WLAN
en1-1	Staff Ethernet LAN	IP address 10.0.1.1/24: DHCP server and gateway for the employee Ethernet WLAN
en1-2	Guest Ethernet LAN	IP address 10.0.2.1/24: DHCP server and gateway for the guest Ethernet WLAN
en1-4	WAN	Uplink to the Internet

5.2 Configuration

Port Configuration

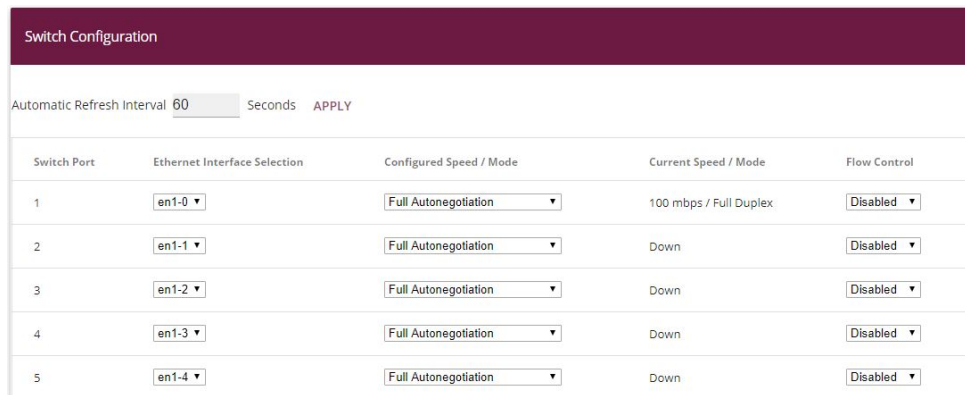


Note

The computer from which the router is being configured should be connected to Ethernet port 1 throughout the configuration process. Otherwise, one will be repeatedly locked out of the router during the configuration process.

First of all, the Ethernet ports are configured as separate interfaces, and a separate interface is assigned to each port, in ascending order, beginning with en1-0.

- (1) Go to **Physical Interfaces** -> **Ethernet Ports** -> **Port Configuration**.



Switch Configuration

Automatic Refresh Interval Seconds

Switch Port	Ethernet Interface Selection	Configured Speed / Mode	Current Speed / Mode	Flow Control
1	en1-0 ▼	Full Autonegotiation ▼	100 mbps / Full Duplex	Disabled ▼
2	en1-1 ▼	Full Autonegotiation ▼	Down	Disabled ▼
3	en1-2 ▼	Full Autonegotiation ▼	Down	Disabled ▼
4	en1-3 ▼	Full Autonegotiation ▼	Down	Disabled ▼
5	en1-4 ▼	Full Autonegotiation ▼	Down	Disabled ▼

Fig. 85: Physical Interfaces -> Ethernet Ports -> Port Configuration

Proceed as follows to assign the ports to the interfaces:

- (1) Under **Ethernet Interface Selection** select *en1-0* to *en1-4* for the **Switch Ports 1** and **5** from the dropdown menu.
- (2) Confirm with **OK**.

The WAN and Internet access is then set up. The **GUI** has a **wizard** to configure the Internet access. To do this, go to the following menu:

- (1) Go to **Assistants -> Internet Access-> Internet Connections -> New**.
- (2) For **Connection Type**, select the appropriate connection type for your Internet access, in our example *External gateway/cable modem*.
- (3) Click on **Next** to configure a new Internet connection.

The screenshot shows a four-step configuration wizard for Internet Access. Step 1: 'Select the physical Ethernet port the external gateway / cable modem is connected to:' with a dropdown menu showing 'ETH5'. Step 2: 'Select your Internet Service Provider (ISP) from the list:' with a dropdown menu showing '--User-defined--'. Step 3: 'Are the IP parameters obtained dynamically?' with a toggle switch turned off. Step 4: 'Enter the IP settings of your Internet access:' with input fields for Local IP Address (1.2.3.4), Gateway IP Address (1.2.3.1), Netmask (255.255.255.0), DNS Server 1 (1.2.3.1), and DNS Server 2 (0.0.0.0).

Fig. 86: Assistants -> Internet Access -> Internet Connections -> New -> Next

We shall now describe the setup for an external gateway:

- (1) Under **Physical Ethernet Port** select the physical Ethernet port to which the xDSL modem or the Internet uplink is connected, in this case *ETH5*.
- (2) For **Internet Service Provider**, select *--User-defined--*.
- (3) Deselect the **IP parameters obtained dynamically** option.
- (4) Under **Local IP Address**, enter your Internet access data, e. g. *1.2.3.4*.
- (5) For **Gateway IP Address** enter the gateway's IP address, e. g. *1.2.3.1*.
- (6) Enter the relevant **Netmask**, e. g. *255.255.255.0*.
- (7) For **DNS Server 1** enter the name server's IP address, e. g. *1.2.3.1*.
- (8) Press **OK** to confirm your entries.


Variant:

- (1) If the uplink is a provider's xDSL access, you can, instead, select *Internal modem* as the **Connection Type** in the first step of the Internet access wizard.
- (2) In this case, the internal **Network Interface**, instead of being called *en1-4*, is usually called *WAN_Providername* and, when the configuration has been completed in the menu **Network -> Routes -> IP Routes**, appears as the interface for the default gateway (in the simplest case, this is the only entry with the target IP address and netmask the same *0.0.0.0*).
- (3) The **interface** name is relevant for subsequent configuration steps when setting up the firewall.

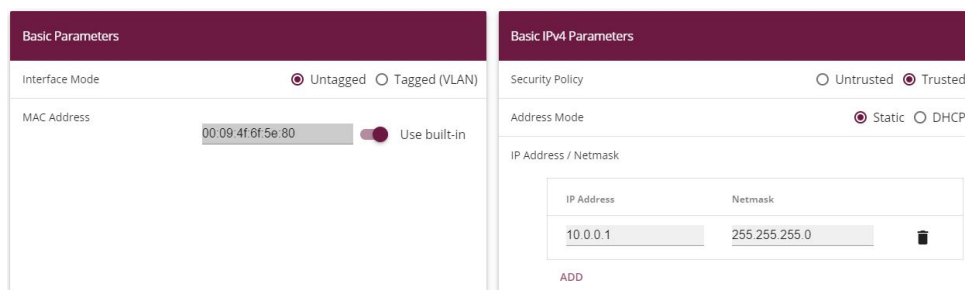
**Note**

This interface is not to be confused with the (underlying) *eth0a* interface which is also present.

The LAN interfaces are then configured.

You configure the Ethernet interface by editing the default entry. To do this, click the  icon next to the existing **<en1-0>** entry.

- (1) Go to **LAN -> IP Configuration -> Interfaces ->** .



The screenshot shows two panels for configuring an interface. The left panel, titled 'Basic Parameters', has 'Interface Mode' set to 'Untagged' (selected) and 'Tagged (VLAN)'. The 'MAC Address' is '00:09:4f:6f:5e:80' and the 'Use built-in' toggle is turned on. The right panel, titled 'Basic IPv4 Parameters', has 'Security Policy' set to 'Trusted' (selected) and 'Untrusted'. The 'Address Mode' is 'Static' (selected) and 'DHCP'. Under 'IP Address / Netmask', the 'IP Address' is '10.0.0.1' and the 'Netmask' is '255.255.255.0'. There is an 'ADD' button at the bottom.

Fig. 87: **LAN -> IP Configuration -> Interfaces ->** .

Proceed as follows to configure the Ethernet interface:

- (1) Enter the static **IP Address** *10.0.0.1* and the **Netmask** *255.255.255.0*.
- (2) Confirm with **OK**.

**Note**

After you have confirmed the configuration with **OK**, you have locked yourself (just the once) out of the router. Log back onto the newly set up **IP Address** *10.0.0.1* for *en1-0* (your own computer's network configuration may have to be changed before doing this).

- (1) The static **IP Address** *10.0.1.1* with **Netmask** *255.255.255.0* is then set up on the Ethernet interface *en1-1*.
- (2) Confirm with **OK**.
- (3) Finally, the Ethernet interface *en1-2* is set up with the static **IP Address** *10.0.2.1* and with the **Netmask** *255.255.255.0*. The Ethernet interface *en1-3* remains unused.
- (4) Confirm with **OK**.

In the next step, two virtual interfaces based on `en1-0` are added.

- (1) Go to **LAN -> IP Configuration -> Interfaces -> New**.

The screenshot displays two panels for configuring a new virtual interface. The left panel, titled "Basic Parameters", shows the interface is based on "en1-0", set to "Tagged (VLAN)" mode with "VLAN ID 10" and "MAC Address 00:a0:f9". The right panel, titled "Basic IPv4 Parameters", shows the "Security Policy" set to "Trusted" and "Address Mode" set to "Static". Under "IP Address / Netmask", a table lists "10.0.10.1" for the IP Address and "255.255.255.0" for the Netmask, with an "ADD" button below.

Fig. 88: **LAN -> IP Configuration -> Interfaces -> New**

Proceed as follows to configure the first virtual interface:

- (1) For **Based on Ethernet Interface**, select the interface `en1-0`.
- (2) Assign **VLAN ID 10** to the interface.
- (3) For **IP Address / Netmask**, click **Add**.
- (4) The first virtual interface is given the static **IP Address 10.0.10.1** and the **Netmask 255.255.255.0**.
- (5) Confirm with **OK**.

You configure the second virtual interface as follows:

- (1) For **Based on Ethernet Interface**, select the interface `en1-0`.
- (2) Assign **VLAN ID 20** to the interface.
- (3) For **IP Address / Netmask**, click **Add**.
- (4) The second virtual interface is given the static **IP Address 10.0.20.1** and the **Netmask 255.255.255.0**.
- (5) Confirm with **OK**.

Results:

Ethernet/VLAN Ports						
Interface	IPv4 Address/Netmask	IPv6 Address/Length	Status	Action		
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	Not configured/Not configured	-	✗	^ v		
ethoa35-5	Not configured/Not configured	-	✗	^ 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		

Fig. 89: LAN -> IP Configuration -> Interfaces

System access and firewall setup

Administrative access to the device is configured in the **Access** menu. Firstly, all of the router's configuration services are restricted to the administrative Ethernet interface *en1-0*.

- (1) Go to **System Management -> Administrative Access -> Access** .

Access						
Interface	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"/>

Fig. 90: System Management -> Administrative Access -> Access

Proceed as follows:

- (1) For the **Interface** *en1-0*, select the router's configuration services *Telnet*, *SSH*, *HTTP*, *HTTPS*, *Ping* and *SNMP*.
- (2) On all the other interfaces, only *Ping* should be allowed. We do not recommend that you also block Ping, because this makes it unnecessarily difficult to search for errors

in the LAN (with no additional security).

- (3) Click **OK**.

Setting the **Passwords** is another basic system setting. Make sure you change the passwords to prevent unauthorised access to the device

- (1) Go to **System Administration** -> **Global Settings** -> **Passwords**.
- (2) Enter the password for the user name *admin*.
- (3) Confirm the password by entering it again.
- (4) Click **OK**.

The **Firewall** for the LAN is then set up. Define a group that contains all the services that the router itself is to offer in the LAN.

- (1) Go to **Firewall** -> **Services** -> **Groups** -> **New**.

Basic Parameters

Description
Local-Services

Members

Service	Selection
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"/>

Fig. 91: Firewall -> Services -> Groups -> New

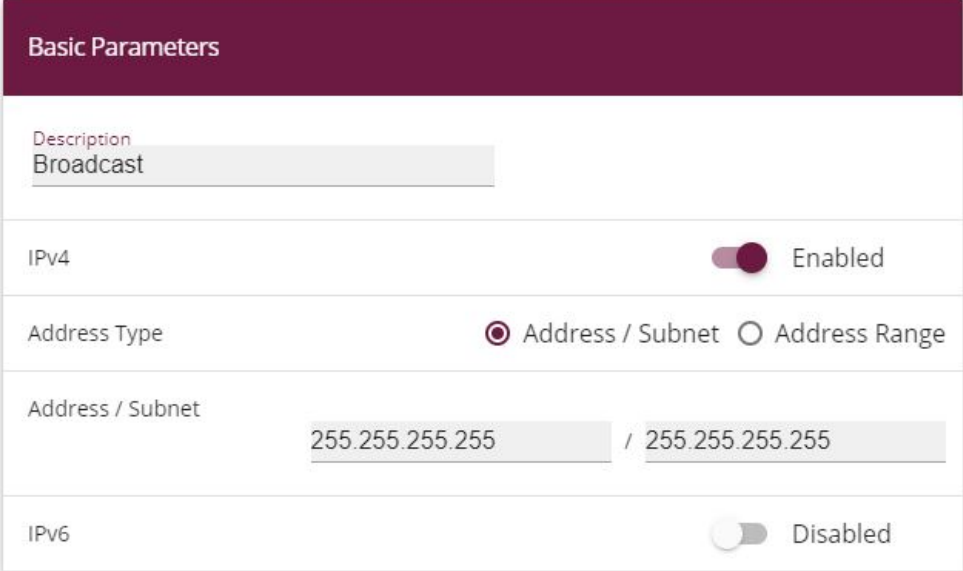
Proceed as follows:

- (1) For **Description**, enter *Local-Services* for the group.

- (2) Select the **Members** of the group, e. g. *echo*, *dns*, *dhcp*, *ntp*. To do this, activate the field in the **Members** column.
- (3) Confirm with **OK**.

In the next step, you define the firewall's address lists. By default, *ANY* is the only entry.

- (1) Go to **Firewall -> Addresses -> Address List -> New**.



Basic Parameters

Description
Broadcast

IPv4 Enabled

Address Type Address / Subnet Address Range

Address / Subnet
255.255.255.255 / 255.255.255.255

IPv6 Disabled

Fig. 92: **Firewall -> Addresses -> Address List -> New**

Proceed as follows:

- (1) Under **Description**, enter *Broadcast*.
- (2) For the **Address / Subnet**, enter *255.255.255.255* and *255.255.255.255*.
- (3) Confirm with **OK**.

Define other LAN IP address lists.

- (1) For *Employee LAN GW* (en1-1) the **IP Address** *10.0.1.1* with the **Netmask** *255.255.255.255*.
- (2) Confirm with **OK**.
- (3) For *Guest LAN GW* (en1-2) the **IP Address** *10.0.2.1* with the **Netmask** *255.255.255.255*.
- (4) Confirm with **OK**.
- (5) For *Employee WLAN GW* (en1-0-1) the **IP Address** *10.0.10.1* with the **Netmask** *255.255.255.255*.

- (6) Confirm with **OK**.
- (7) For *Guest WLAN GW* (en1-0-2) the **IP Address** `10.0.20.1` with the **Netmask** `255.255.255.255`.
- (8) Confirm with **OK**.



Note

The IP addresses in the firewall need to match the interfaces concerned for IP configuration (and be modified if the configuration is changed). The mask must always be 255.255.255.255 and has nothing to do with the netmask of the networks concerned. The mask restricts the range of the relevant address list to precisely the one IP address that was entered.

The list of configured addresses now looks like this:

Address List					
Description	Address/Subnet/Address Range	Address / Prefix			
ANY	0.0.0.0/0	:::0			
Broadcast	255.255.255.255/32				
Staff-LAN-GW	10.0.1.1/32				
Guest-LAN-GW	10.0.2.1/32				
Staff-WLAN-GW	10.0.10.1/32				
Guest-WLAN-GW	10.0.20.1/32				

Fig. 93: Firewall -> Addresses -> Address List

Now you still need to define the interfaces for the individual user groups.

- (1) Go to **Firewall -> Interfaces-> IPv4 Groups -> New**.

Basic Parameters

Description
Staff

Members

Interface	Selection
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"/>

Fig. 94: Firewall -> Interfaces -> IPv4 Groups -> New

Proceed as follows to set up the *Employees* group:

- (1) Enter *Staff* as the **Description** for the group.
- (2) From the interfaces that have been configured, select *LAN_EN1-1* and *LEASED_EN1-0-1* as **Members** of the group.
- (3) Confirm with **OK**.

Define another group *Guest* as follows:

- (1) Enter *Guest* as the **Description** for the group.

- (2) Select `LAN_EN1-2` and `LEASED_EN1-0-2` as **Members** of the group.
- (3) Confirm with **OK**.

Set up the interfaces group `Users` (staff and guests).

- (1) Enter `User` as the **Description** for the group.
- (2) As **Members** of the group, select `LAN_EN1-1`, `LAN_EN1-2`, `LEASED_EN1-0-1` and `LEASED_EN1-0-2`.
- (3) Confirm with **OK**.

The list of configured groups now looks like this:







IPv4 Groups			
Description	Members		
Staff	LAN_EN1-1, LEASED_EN1-0-1		
Guests	LAN_EN1-2, LEASED_EN1-0-2		
Users	LAN_EN1-1, LAN_EN1-2, LEASED_EN1-0-1, LEASED_EN1-0-2		

Fig. 95: Firewall -> Interfaces -> IPv4 Groups

Now the actual firewall rules can be created based on these definitions. Firstly, the rule for the administrators area in `en1-0` must be defined (otherwise one will be locked out totally and immediately).

- (1) Go to **Firewall -> Policies -> IPv4 Filter Rules -> New**.

Basic Parameters	
Source	LAN_EN1-0 ▾
Destination	ANY ▾
Service	any ▾
Action	Access ▾

Fig. 96: Firewall -> Policies -> IPv4 Filter Rules -> New

Proceed as follows:

- (1) Select the packet's **Source**, in this case `LAN_EN1-0`.

- (2) Set the **Destination** to *ANY*. Neither the destination interface or the destination address will be checked.
- (3) For **Services**, select *any* (all the services).
- (4) Select the **Action** that is to be applied, in this case *Access*. The packets are forwarded on the basis of the entries.
- (5) Confirm with **OK**.
- (6) As the next rule, the **Source group** *Staff* is to be granted access to the **Destination group** *Users* via **Services** *any* .
- (7) Confirm with **OK**.
- (8) After that, a rule is created which is used to permit access from the **Source group** *Guest* to the **Destination group** *Guest* via **Services** *any*.
- (9) Confirm with **OK**.
- (10) Another rule should give all the *Users* access to the Internet: As the **Source**, select *Users*, as the **Destination**, select *LAN_EN1-4* , and as the **Service**, select *any*.
- (11) Confirm with **OK**.

**Note**

If an Internet access via an internal xDSL modem has been set up, instead of *LAN_EN1-4*, you need to select the relevant WAN interface (*WAN_Providername*) as the **Destination**.

Up to this point, the only access rules to have been defined are those for network areas connected via the router, and nobody outside the system area at the interface *en1-0* is permitted to access IP addresses defined locally in the router.

To be able to use the basic services such as *dns*, *dhcp* etc., you need to explicitly allow **access** to the IP address of the interface concerned which is linked to the router.

- (1) Go to **Firewall -> Policies -> IPv4 Filter Rules -> New**.

Basic Parameters	
Source	Users ▼
Destination	Broadcast ▼
Service	Local-Services ▼
Action	Access ▼

Fig. 97: Firewall -> Policies -> IPv4 Filter Rules -> New

Proceed as follows:

- (1) As the **Source** of the packet, select the *Users* group.
- (2) As the **Destination**, select the *Broadcast* address that was defined previously.
- (3) For **Service**, select the service group that the users are to be permitted to access, in this case *Local-Services*.
- (4) Select the **Action** that is to be applied, in this case *Access*. The packets are forwarded on the basis of the entries.
- (5) Confirm with **OK**.
- (6) In the next rule you select the **Source** *LAN_EN1-1*. As the **Destination**, select the *Staff LAN GW* that was defined previously, as the **Service** select *Local Services* and, for the **Action**, select *Access*.
- (7) Confirm with **OK**.
- (8) In the next rule you select the **Source** *LAN_EN1-2*. As the **Destination**, select the *Guests LAN GW* address that was defined previously, as the **Service** select *Local-Services* and, for the **Action**, select *Access*.
- (9) Confirm with **OK**.
- (10) In the next rule, as the **Source** you select *LEASED_EN1-0-1*, as the **Destination** you select the *Staff WLAN GW* address which was defined previously, as the **Service** you select *Local services* and as the **Action** you select *Access*.
- (11) Confirm with **OK**.
- (12) In the final rule, as the **Source** you select *LEASED_EN1-0-2*. As the **Destination**, select the *Guests WLAN GW* address that was defined previously, as the **Service** select *Local Services* and, for the **Action**, select *Access*.
- (13) Confirm with **OK**.

The list of configured filter rules now looks like this:

Order	Source	Destination	Service	Action	Policy active				
1	LAN_EN1-4	ANY	any	Access	<input checked="" type="checkbox"/> Enabled	↑↓	≡+	🗑️	✎
2	Staff	Users	any	Access	<input checked="" type="checkbox"/> Enabled	↑↓	≡+	🗑️	✎
3	Guests	Guests	any	Access	<input checked="" type="checkbox"/> Enabled	↑↓	≡+	🗑️	✎
4	Users	LAN_EN1-4	any	Access	<input checked="" type="checkbox"/> Enabled	↑↓	≡+	🗑️	✎
5	Users	Broadcast	Local-Services	Access	<input checked="" type="checkbox"/> Enabled	↑↓	≡+	🗑️	✎
6	LAN_EN1-1	Staff-LAN-GW	Local-Services	Access	<input checked="" type="checkbox"/> Enabled	↑↓	≡+	🗑️	✎
7	LAN_EN1-2	Guest-LAN-GW	Local-Services	Access	<input checked="" type="checkbox"/> Enabled	↑↓	≡+	🗑️	✎
8	LEASED_EN1-0-1	Staff-WLAN-GW	Local-Services	Access	<input checked="" type="checkbox"/> Enabled	↑↓	≡+	🗑️	✎
9	LEASED_EN1-0-2	Guest-WLAN-GW	Local-Services	Access	<input checked="" type="checkbox"/> Enabled	↑↓	≡+	🗑️	✎

Fig. 98: Firewall -> Policies -> IPv4 Filter Rules

The firewall automatically rejects any other data which does not fit with the above rules. So there is no need to create any explicit exclusion rules to reject the other data traffic. This also means that, with the current firewall configuration, any IP data traffic on the router and to the LAN that is initiated by the WAN/Internet (*en1-4* in our example) is suppressed. If access from outside is required, separate firewall rules need to be defined for this purpose with the WAN interface (in this case *LAN_EN1-4*) as the source.

To finish, check whether the firewall is enabled. To do this, go to the following menu:

- (1) Go to **Firewall -> Policies -> Options** .

Global Firewall Options	Session Timer
IPv4 Firewall Status <input checked="" type="checkbox"/> Enabled	UDP Inactivity <input type="text" value="180"/> Seconds
Logged Actions <input type="text" value="All"/>	TCP Inactivity <input type="text" value="3600"/> Seconds
IPv4 Full Filtering <input checked="" type="checkbox"/> Enable	PPTP Inactivity <input type="text" value="86400"/> Seconds
STUN Handler <input type="checkbox"/>	Other Inactivity <input type="text" value="30"/> Seconds

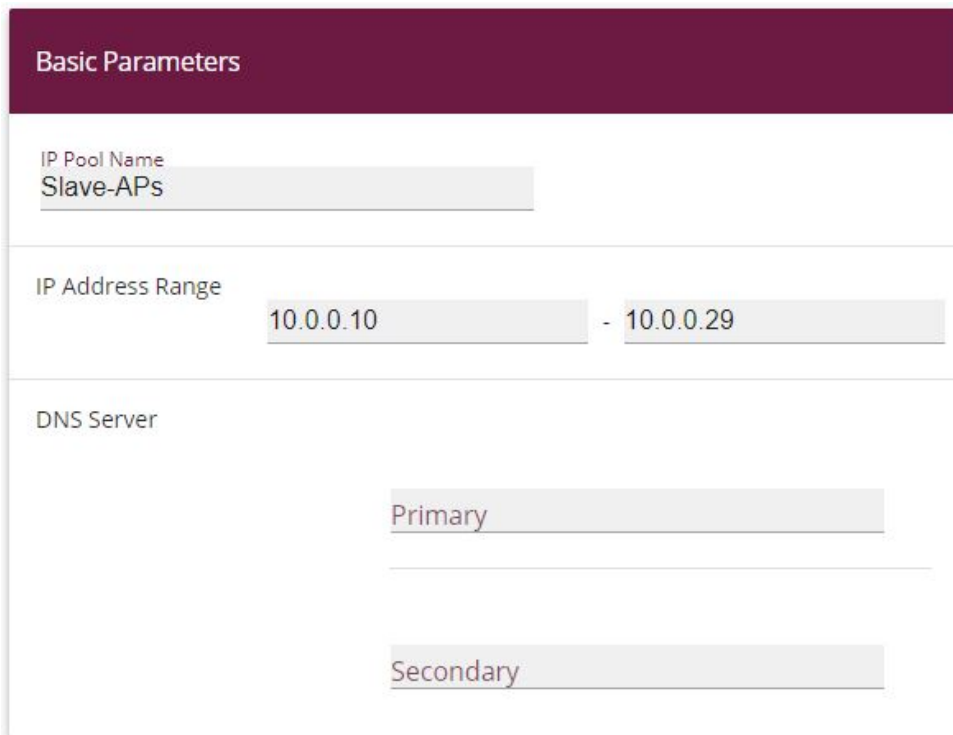
Fig. 99: Firewall ->Policies->Options

The **IPv4 Firewall Status** option must be set to *Activated*.

DHCP server configuration

After that, 5 DHCP servers, in all, now need to be configured to match the relevant interface's network.

- (1) Go to **Local Services -> DHCP Server -> IP Pool Configuration -> New**.



The screenshot shows a web-based configuration form titled "Basic Parameters" for a new DHCP IP pool. The form has three main sections:

- IP Pool Name:** A text input field containing "Slave-APs".
- IP Address Range:** Two text input fields separated by a hyphen. The first field contains "10.0.0.10" and the second field contains "10.0.0.29".
- DNS Server:** Two text input fields. The top field is labeled "Primary" and is currently empty. The bottom field is labeled "Secondary" and is also empty.

Fig. 100: **Local Services -> DHCP Server -> IP Pool Configuration -> New**

Proceed as follows to set up the IP address pool for the slave APs:

- (1) Enter a unique **IP Pool Name**, e. g. *Slave APs*.
- (2) Enter an **IP Address Range**. In our example, we shall take the IP address range from *10.0.0.10* to *10.0.0.29*. The size of the IP address range depends on the maximum number of access points required (6 plus reserve in our example). So the remaining addresses can be used for other infrastructure in the same network.
- (3) Press **OK** to confirm your entries

In the **Local Services -> DHCP Server -> DHCP Configuration -> New** menu, you can perform additional configuration.

Basic Parameters

Interface	en1-0
IP Pool Name	Slave-APs
Pool Usage	Local
Description	

Advanced Settings:

Advanced Parameter

Gateway	Use router as gateway									
Lease Time	120 Minutes									
DHCP Options	<table><thead><tr><th>Option</th><th>Value</th><th></th></tr></thead><tbody><tr><td>DNS Server</td><td>10.0.0.1</td><td>🗑</td></tr><tr><td>CAPWAP Controller</td><td>10.0.0.1</td><td>🗑</td></tr></tbody></table>	Option	Value		DNS Server	10.0.0.1	🗑	CAPWAP Controller	10.0.0.1	🗑
Option	Value									
DNS Server	10.0.0.1	🗑								
CAPWAP Controller	10.0.0.1	🗑								
Vendor Specific Information (DHCP Option 43)	<table><thead><tr><th>Vendor ID</th><th>Vendor Specific Information</th></tr></thead><tbody><tr><td></td><td></td></tr></tbody></table>	Vendor ID	Vendor Specific Information							
Vendor ID	Vendor Specific Information									

ADD VENDOR STRING ADD VENDOR GROUP

Fig. 102: Local Services -> DHCP Server -> DHCP Configuration -> New

Proceed as follows:

- (1) Under **Interface**, select the logical interface *en1-0*.
- (2) Select a valid **IP-Pool**, here e. g. *Slave-APs*.
- (3) Click **Advanced Settings**.
- (4) Under **Gateway** leave the setting *Use Router as Gateway*. The current IP address of the interface *en1-0* is propagated as the default gateway to the DHCP devices.

- (5) For **DHCP Options**, click **Add**.
- (6) Select the option *DNS Server* and enter the IP address of the interface *en1-0*, in this case *10.0.0.1*.
- (7) Click **Add** again.
- (8) Select the option *CAPWAP Controller* and enter the IP address of the interface *en1-0*, in this case *10.0.0.1*.
- (9) Press **OK** to confirm your entries.

No other DHCP options are required for the slave access points to operate correctly.

In the next step, you define the **DHCP Pool** *Staff WLAN* .

Go to **Local Services -> DHCP Server -> IP Pool Configuration -> New**.

- (1) For **IP Pool Name**, enter e. g. *Staff-WLAN*.
- (2) Enter an **IP Address Range**. In our example, the IP address range from *10.0.20.10* to *10.0.20.254*.
- (3) Press **OK** to confirm your entries.
- (4) Go to **Local Services -> DHCP Server -> DHCP Configuration -> New**.
- (5) Under **Interface**, select the interface *en1-0-1*.
- (6) For **IP Pool Name**, enter e. g. *Staff-WLAN*.
- (7) Click **Advanced Settings**.
- (8) Under **Gateway** leave the setting *Use Router as Gateway*.
- (9) For **DHCP Options**, click **Add**.
- (10) Select the option *DNS Server* and enter the IP address of the interface *en1-0*, in this case *10.0.10.1*.
- (1) Press **OK** to confirm your entries.

Proceed as follows to set up another IP address pool for the *Guest WLAN*:

Go to **Local Services -> DHCP Server -> IP Pool Configuration -> New**.

- (1) For **IP Pool Name**, enter e. g. *Guest-WLAN*.
- (2) Enter an **IP address range**. In our example, the IP address range from *10.0.20.10* to *10.0.20.254*.
- (3) Press **OK** to confirm your entries.
- (4) Go to **Local Services -> DHCP Server -> DHCP Configuration -> New**.
- (5) Under **Interface**, select the interface *en1-0-2*.
- (6) Select a valid **IP-Pool**, here e. g. *Guest-WLAN* .
- (7) Click **Advanced Settings**.

- (8) Under **Gateway** leave the setting *Use Router as Gateway*.
- (9) For **DHCP Options**, click **Add**.
- (10) Select the option *DNS Server* and enter the IP address of the interface, in this case *10.0.20.1*.
- (11) Press **OK** to confirm your entries.

Do the same thing to configure the **DHCP Pool** for *Staff Ethernet*.

Go to **Local Services -> DHCP Server -> IP Pool Configuration -> New**.

- (1) For **IP Pool Name**, enter e. g. *Staff-Ethernet*.
- (2) Enter an **IP Address Range**. In our example, the IP address range from *10.0.1.10* to *10.0.1.254*.
- (3) Press **OK** to confirm your entries.
- (4) Go to **Local Services -> DHCP Server -> DHCP Configuration -> New**.
- (5) Under **Interface**, select the interface *en1-1*.
- (6) Select a valid **IP-Pool**, here e. g. *Staff-Ethernet*.
- (7) Click **Advanced Settings**.
- (8) Under **Gateway** leave the setting *Use Router as Gateway*.
- (9) For **DHCP Options**, click **Add**.
- (10) Select the option *DNS Server* and enter the IP address of the interface, in this case *10.0.1.1*.
- (11) Press **OK** to confirm your entries.

Then configure the **DHCP Pool** for *Guest Ethernet*.

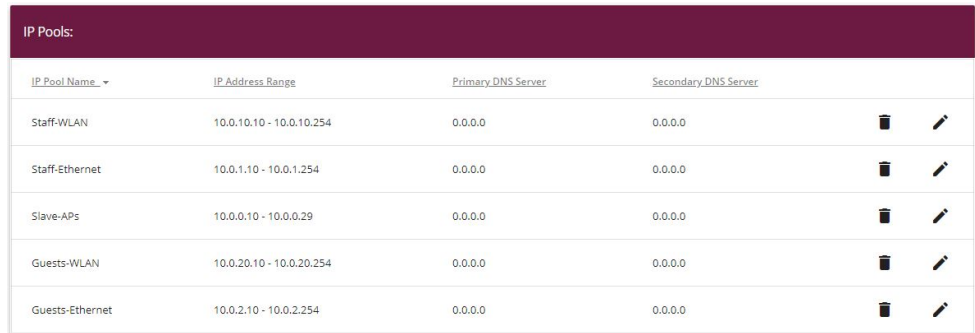
Go to **Local Services -> DHCP Server -> IP Pool Configuration -> New**.

- (1) For **IP Pool Name**, enter e. g. *Guest-Ethernet*.
- (2) Enter an **IP address range**. In our example, the IP address range from *10.0.2.10* to *10.0.2.254*.
- (3) Press **OK** to confirm your entries.
- (4) Goto **Local Services -> DHCP Server -> DHCP Configuration -> New**.
- (5) Under **Interface**, select the interface *en1-2*.
- (6) Select a valid **IP-Pool**, here e. g. *Guest-Ethernet*.
- (7) Click **Advanced Settings**.
- (8) Under **Gateway** leave the setting *Use Router as Gateway*.
- (9) For **DHCP Options**, click **Add**.
- (10) Select the option *DNS Server* and enter the IP address of the interface, in this case

10.0.2.1.

(11) Press **OK** to confirm your entries.

The list of configured DHCP pools now looks like this:

A screenshot of a web interface showing a table of IP Pools. The table has a dark red header with the text 'IP Pools:'. Below the header, the table has four columns: 'IP Pool Name', 'IP Address Range', 'Primary DNS Server', and 'Secondary DNS Server'. There are also two icons (trash and edit) on the right side of each row. The table contains six rows of data.

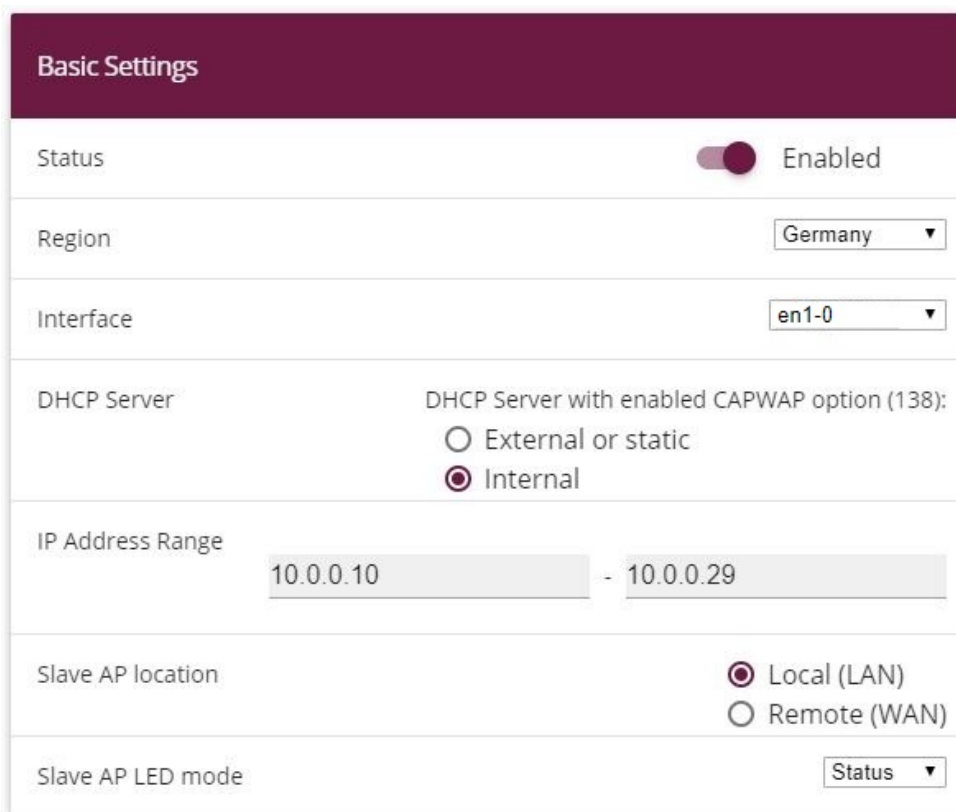
IP Pool Name	IP Address Range	Primary DNS Server	Secondary DNS Server		
Staff-WLAN	10.0.10.10 - 10.0.10.254	0.0.0.0	0.0.0.0	🗑️	✎
Staff-Ethernet	10.0.1.10 - 10.0.1.254	0.0.0.0	0.0.0.0	🗑️	✎
Slave-APs	10.0.0.10 - 10.0.0.29	0.0.0.0	0.0.0.0	🗑️	✎
Guests-WLAN	10.0.20.10 - 10.0.20.254	0.0.0.0	0.0.0.0	🗑️	✎
Guests-Ethernet	10.0.2.10 - 10.0.2.254	0.0.0.0	0.0.0.0	🗑️	✎

Fig. 103: Local Services -> DHCP Server -> IP Pool Configuration

WLAN Controller setup

Now the **Wireless LAN Controller** on interface `en1-0` can be enabled.

(1) Go to **Wireless LAN Controller -> Controller Configuration -> General**.



Basic Settings

Status Enabled

Region

Interface

DHCP Server External or static
 Internal

DHCP Server with enabled CAPWAP option (138):

IP Address Range -

Slave AP location Local (LAN)
 Remote (WAN)

Slave AP LED mode

Fig. 104: **Wireless LAN Controller -> Controller Configuration -> General**

Proceed as follows:


- (1) The **Region** must be set up to match the location of the access points, *Germany* in our example. This means that the access points' WLAN wireless modules will only run inside the legally permitted framework of the country concerned.
- (2) As the WLAN controller's **Interface**, select *en1-0*.
- (3) When the interface has been selected, the **DHCP Server** settings automatically change to *Internal*.
- (4) **IP Address Range** displays the address range that was configured in the DHCP Pools menu on interface *en1-0*, in this case *10.0.0.10 - 10.0.0.29*.
- (5) Leave the **Slave AP location** set to *Local (LAN)*.
- (6) Confirm with **OK**.

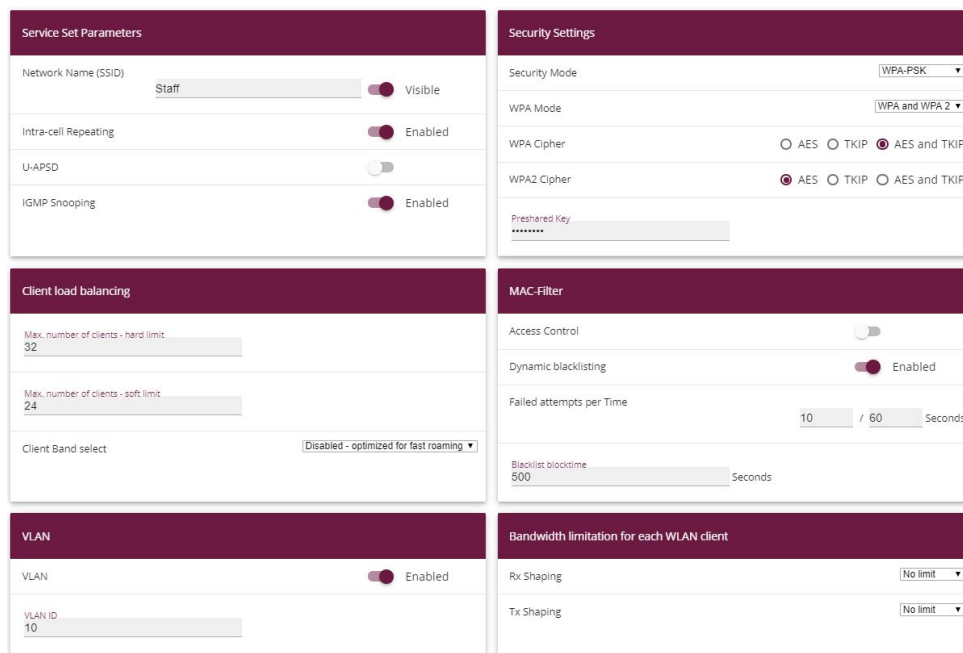
The settings are now enabled and the WLAN controller is started.

The **Wireless Networks (VSS)** are now edited.

Go to the following menu to set up your WLAN network:

- (1) Go to **Wireless LAN Controller -> Slave AP Configuration->Wireless Networks (VSS)**.

Configure the WLAN connection by editing the default entry. To do this, for the existing entry <vss-1> click the  symbol.



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

- Service Set Parameters:** Network Name (SSID) is 'Staff' with a 'Visible' toggle. Intra-cell Repeating is 'Enabled'. U-APSD is disabled. IGMP Snooping is 'Enabled'.
- Security Settings:** Security Mode is 'WPA-PSK'. WPA Mode is 'WPA and WPA 2'. WPA Cipher is 'AES and TKIP'. WPA2 Cipher is 'AES'. A 'Preshaed Key' field contains 8 asterisks.
- Client load balancing:** Max. number of clients - hard limit is '32'. Max. number of clients - soft limit is '24'. Client Band select is 'Disabled - optimized for fast roaming'.
- MAC-Filter:** Access Control is disabled. Dynamic blacklisting is 'Enabled'. Failed attempts per Time is '10 / 60' seconds. Blacklist blocktime is '500' seconds.
- VLAN:** The 'VLAN' toggle is 'Enabled'. The 'VLAN ID' is '10'.
- Bandwidth limitation for each WLAN client:** Both 'Rx Shaping' and 'Tx Shaping' are set to 'No limit'.

Fig. 105: **Wireless LAN Controller -> Slave AP Configuration->Wireless Networks (VSS)-> <vss-1>** 

Proceed as follows:

- (1) Under **Network Name (SSID)** enter e. g. *Staff*. The **Visible** option remains enabled.
- (2) Set the **Security Mode** to *WPA-PSK*.
- (3) Leave the **WPA Mode** set to *WPA and WPA 2*.
- (4) The **WPA Cipher** is set to *TKIP*.
- (5) Set the **WPA2 Cipher** to *AES*.
- (6) The **Preshaed Key** is the WLAN access password for all the employees. Enter an ASCII string with 8 - 63 characters.
- (7) Enable the **VLAN** option.
- (8) Enter the **VLAN-ID** *10*.

The result of this is that all the data that from the WLAN devices connected later to the SSID *Employees* is marked by the slave access points in the Ethernet with the **VLAN-ID 10**. This means that the employee data traffic between router and access points is a standalone network area at the Ethernet level (layer 2), too.

(9) Confirm with **OK**.

Select the **New** button to configure a wireless network for the guest access.

(1) Go to **Wireless LAN Controller -> Slave AP Configuration->Wireless Networks (VSS)-> New**.

The screenshot displays the configuration interface for a new wireless network, organized into several sections:

- Service Set Parameters:**
 - Network Name (SSID): Visible
 - Intra-cell Repeating: Enabled
 - U-APSD: Enabled
 - IGMP Snooping:
- Security Settings:**
 - Security Mode: ▼
 - WPA Mode: ▼
 - WPA Cipher: AES TKIP AES and TKIP
 - WPA2 Cipher: AES TKIP AES and TKIP
 - Preshared Key:
- Client load balancing:**
 - Max. number of clients - hard limit:
 - Max. number of clients - soft limit:
 - Client Band select: ▼
- MAC-Filter:**
 - Access Control:
 - Dynamic blacklisting: Enabled
 - Failed attempts per Time: / Seconds
 - Blacklist blocktime: Seconds
- VLAN:**
 - VLAN: Enabled
 - VLAN ID:
- Bandwidth limitation for each WLAN client:**
 - Rx Shaping: ▼
 - Tx Shaping: ▼


Fig. 106: Wireless LAN Controller -> Slave AP Configuration->Wireless Networks (VSS)-> New

Proceed as follows:

- (1) Under **Network Name (SSID)** enter *Guest* for example. The **Visible** option remains enabled.
- (2) Set the **Security Mode** to *WPA-PSK*.
- (3) Leave the **WPA Mode** set to *WPA and WPA 2*.
- (4) The **WPA Cipher** is set to *TKIP*.
- (5) Set the **WPA2 Cipher** to *AES*.
- (6) The **Preshared Key** is the WLAN access password for all the guests. Enter an ASCII string with 8 - 63 characters.

- (7) Enable the **VLAN** option.
- (8) Enter the **VLAN-ID 20**.
- (9) Confirm with **OK**.

In the next step, the **Radio Profiles** are edited. You configure the **Radio Profiles** by editing the default entry.

- (1) Go to **Wireless LAN Controller -> Slave AP Configuration-> Radio Profiles** .
- (2) Where you have the existing entry **<2.4 GHz Radio Profile>** , click the  symbol.





Radio Profile Definition	Performance Settings
Description 2.4 GHz Radio Profile	Wireless Mode 802.11b/g/n
Operation Mode Access Point	Number of Spatial Streams 3
Operation Band 2.4 GHz In/Outdoor	Airtime fairness Enabled
	Cyclic Background Scanning Enabled

Advanced Settings

Advanced Parameter

Channel Plan User defined ▾

User Defined Channel Plan

Channel	
1 ▾	
5 ▾	
9 ▾	
13 ▾	

ADD

Beacon Period ms

DTIM Period

RTS Threshold

Short Guard Interval Enabled

Max. Transmission Rate Auto ▾

Short Retry Limit

Long Retry Limit

Fragmentation Threshold Bytes

Fig. 108: Wireless LAN Controller -> Slave AP Configuration-> Radio Profiles-> <2.4

GHz Radio Profile 

Proceed as follows:

- (1) The wireless module profile's **frequency range** is left at *2.4 GHz In/Outdoor*.
- (2) For **Wireless Mode**, select *802.11 g/n*. The result of changing the **Wireless Mode** is that old WLAN devices which have become relatively rare and which only talk 802.11b will no longer be able to use the WLAN. The great advantage of only allowing 802.11g/n is that the data throughput for all the connected WLAN devices is no longer automatically and drastically reduced as soon as a WLAN device attempts to get into the WLAN network in 802.11b mode.
- (3) Enable the option **Burst Mode** to increase the transmission speed.
- (4) Click **Advanced Settings**.
- (5) Select the **Channel Plan** you require. *User-defined* enables you to select the channels you require yourself.
- (6) Under **User Defined Channel Plan**, select the permitted channels, *1, 5, 9 and 13* . This channel plan is the recommended ideal channel plan for every country where channels 1 to 13 are allowed and it does not have any (significant) frequency overlaps with 802.11g/n. This means that the access points have more choices for using a channel with minimal interference, which improves the performance and reliability of the entire WLAN.
- (7) Enable the **Short Guard Interval** function in order to reduce the guard interval (= time between transmitting two data symbols) from 800 ns to 400 ns.
- (8) Leave the remaining settings unchanged and confirm them with **OK**.

All the necessary profiles have now been set up in the WLAN controller.

Now the access points are enabled and set up. The **Slave Access Points** menu displays a list of all the APs found using the **Wizard** (here e.g. a **bintec W2003ac**).

- (1) Go to **Wireless LAN Controller** -> **Slave AP Configuration**-> **Slave Access Points** .






Slave Access Points							
Location	Name	IP Address	LAN MAC Address	Channel	Search Channel	Status	Action
1:	bintec W2003ac	10.0.0.11	00:01:cd:0e:ee:bc			 Managed	  

Fig. 109: **Wireless LAN Controller** -> **Slave-AP Configuration**-> **Slave Access Points**

**Note**

If no access points are displayed, we recommend that you re-check the DHCP server settings for the **DHCP pool** *slave APs*, whether it is connected to the correct interface (*en1-0* in this case) and whether the CAPWAP option has been set correctly (*10.0.0.1* in this case). Also check whether another DHCP server is enabled on a different device in the system area. Switch all the access points off and back on so that they get the network configuration settings from the DHCP server again.

Finally, the **Radio Profiles** that were configured previously and the **wireless networks** are set up for each access point.

- (1) Go to **Wireless LAN Controller -> Slave AP Configuration-> Slave Access Points**



The screenshot displays two configuration panels for a Slave Access Point. The left panel, titled 'Access Point Settings', shows fields for Device (W2003ac), Location (Meeting Room), Name (W2003ac), Description (Marketing), and CAPWAP Encryption (Enabled). The right panel, titled 'Radio Module1', shows Operation Mode (On), Active Radio Profile (2.4 GHz Radio Profile), Channel (Auto), Used Channel (6), Transmit Power (Max), and Assigned Wireless Network (VSS). The VSS table lists two networks: vss-1:Staff with MAC address 00:a0:f9:0b:cf:e0 and vss-2:Guest.

Profile	MAC Address	
vss-1:Staff	00:a0:f9:0b:cf:e0	
vss-2:Guest		

Fig. 110: **Wireless LAN Controller -> Slave-AP Configuration-> Slave Access Points**

Proceed as follows:

- (1) For **Location** enter e. g. *Meeting Room*.
- (2) For **Description** enter e. g. *Marketing*.
- (3) Leave the **CAPWAP Encryption** set to *Enabled*.
- (4) Leave the **Operation Mode** set to *On*. This results in all the settings being used in the selected radio profiles.
- (5) As the **Active Radio Profile**, select the wireless module profile that was configured previously, in this case *2.4 GHz Radio Profile*.
- (6) Leave the **Channel** set to *Auto* (this means it is determined dynamically using the wireless profile's channel plan and the WLAN environment).
- (7) For **Assigned Wireless Networks (VSS)**, the two configured wireless networks *Staff* and *Guest* are assigned to the wireless module.

(8) Confirm with **OK**.

Configure all the access points that have been found in the same way.



Note

Every access point must be given a unique location name. Otherwise there will be no way of distinguishing between the access points once they are running.

The list of configured access points (here e. g. a **bintec W2003ac**) now looks like this:

Slave Access Points							
Location	Name	IP Address	LAN MAC Address	Channel	Search Channel	Status	Action
Meeting Room	W2003ac	10.0.0.12	00:01:cd:0f:4c:ae	5 HT20 (auto)		Managed	

Fig. 111: **Wireless LAN Controller -> Slave-AP Configuration-> Slave Access Points**

Once all the access points have been set up, there is a short initialization phase and they are given the status *Managed*, so they are now up and running. The WLAN controller is also blocking them against any sort of external configuration access.

Choose whether the selected Access Point is to be managed by the WLAN Controller by clicking the button or the button in the **Action** column.

You can disconnect the Access Point from the WLAN Controller and therefore remove it from your WLAN infrastructure by click on the button. The Access Point then receives the *Discovered* status, but is no longer *Managed*.

The WLAN channels currently being used which are displayed on the overview page are not yet optimal because during the initial startup, the access points were only able to tune in to the general WLAN environment.

Under **New Channel Setting**, click the **START** button to be able to optimally tune the assigned channels to one another.

When the channel setting is complete, adjacent access points ought to have different channels.

This concludes the configuring of the WLAN controller and of the router as an access gateway. Save the configuration with **Save configuration** and confirm the selection with **OK**.

**Note**

In some cases it may occur that individual adjacent access points still have the same channel even after the channels have been newly set. This always occurs if adjacent access points cannot identify one another sufficiently, or at all, with the WLAN. If the access points are correctly spaced out, one frequent reason for this is strong local interference from third party access points, or a difficult building structure such as fire doors made of steel (usually closed) between two adjacent building areas. In such cases we recommend that, for each access point in the pairs affected, you manually set a fixed channel (which fits with the channel plan) for the wireless modules and you re-run the search for new channels. The result of this is that the other access points which were configured using the automatic channel selection are assigned channels which suit the environment of the access points that have been fixed manually.

5.3 Overview of Configuration Steps

Assign interfaces

Field	Menu	Value
Switch port 1 to 5	Physical Interfaces -> Ethernet Ports -> Port Configuration	en1-0 to en1-4

Set up Internet access

Field	Menu	Value
Connector Type	Assistants -> Internet Access -> Internet Connections -> New	External gateway/ cable modem
Physical Ethernet Port	Assistants -> Internet Access -> Internet Connections -> Next	ETH5
Internet Service Provider	Assistants -> Internet Access -> Internet Connections -> Next	- User-Specified -
IP parameters obtained dynamically	Assistants -> Internet Access -> Internet Connections -> Next	Disabled
Local IP Address	Assistants -> Internet Access -> Internet Connections -> Next	e. g. 1.2.3.4
Gateway IP address	Assistants -> Internet Access -> Internet Connections -> Next	e. g. 1.2.3.1
Netmask	Assistants -> Internet Access -> Internet Connections -> Next	255.255.255.0
DNS Server 1	Assistants -> Internet Access -> In-	e. g. 1.2.3.1

Field	Menu	Value
	ternet Connections -> Next	

Configure interfaces

Field	Menu	Value
IP Address / Netmask	LAN -> IP Configuration-> Interfaces -> <en1-0> 	<i>10.0.0.1 and 255.255.255.0</i>
IP Address / Netmask	LAN -> IP Configuration-> Interfaces -> <en1-1> 	<i>10.0.1.1 and 255.255.255.0</i>
IP Address / Netmask	LAN -> IP Configuration-> Interfaces -><en1-2> 	<i>10.0.2.1 and 255.255.255.0</i>
Based on Ethernet Interface	LAN -> IP Configuration-> Interfaces -> New	<i>en1-0</i>
Address mode	LAN -> IP Configuration-> Interfaces -> New	<i>Static</i>
IP Address / Netmask	LAN -> IP Configuration-> Interfaces -> New	<i>10.0.10.1 and 255.255.255.0</i>
Interface Mode	LAN -> IP Configuration-> Interfaces -> New	<i>Tagged (VLAN)</i>
VLAN ID	LAN -> IP Configuration-> Interfaces -> New	<i>10</i>
Based on Ethernet Interface	LAN -> IP Configuration-> Interfaces -> New	<i>en1-0</i>
Address mode	LAN -> IP Configuration-> Interfaces -> New	<i>Static</i>
IP Address / Netmask	LAN -> IP Configuration-> Interfaces -> New	<i>10.0.20.1 and 255.255.255.0</i>
Interface Mode	LAN -> IP Configuration-> Interfaces -> New	<i>Tagged (VLAN)</i>
VLAN ID	LAN -> IP Configuration-> Interfaces -> New	<i>20</i>

Set up access

Field	Menu	Value
en1-0	System Management -> Administrative Access -> Access	<i>Telnet, SSH, HTTP, HTTPS, Ping, SNMP</i>
en1-1 to en1-4	System Management -> Administrative Access -> Access	<i>Ping</i>

Change password

Field	Menu	Value
System Admin Password	System Management -> Global Settings -> Passwords	e. g. <i>test12345</i>
Confirm Admin Password	System Management -> Global Settings -> Passwords	e. g. <i>test12345</i>

Set up firewall

Field	Menu	Value
Description	Firewall -> Services -> Groups -> New	<i>Local services</i>
Members	Firewall -> Services -> Groups -> New	e. g. <i>echo, dns, dhcp, ntp</i>

Define addresses

Field	Menu	Value
Description	Firewall -> Addresses -> Address List -> New	<i>Broadcast</i>
Address / Subnet	Firewall -> Addresses -> Address List -> New	<i>255.255.255.255 / 255.255.255.255</i>
Description	Firewall -> Addresses -> Address List -> New	e. g. <i>Employee LAN GW</i>
Address / Subnet	Firewall -> Addresses -> Address List -> New	<i>10.0.1.1 / 255.255.255.255</i>
Description	Firewall -> Addresses -> Address List -> New	<i>Guest LAN GW</i>
Address / Subnet	Firewall -> Addresses -> Address List -> New	<i>10.0.2.1 / 255.255.255.255</i>
Description	Firewall -> Addresses -> Address List -> New	<i>Employee WLAN GW</i>
Address / Subnet	Firewall -> Addresses -> Address List -> New	<i>10.0.10.1 / 255.255.255.255</i>
Description	Firewall -> Addresses -> Address List -> New	<i>Guest WLAN GW</i>
Address / Subnet	Firewall -> Addresses -> Address List -> New	<i>10.0.20.1 / 255.255.255.255</i>

Define groups

Field	Menu	Value
Description	Firewall -> Interfaces -> IPv4 Groups -> New	Employees
Members	Firewall -> Interfaces -> IPv4 Groups -> New	LAN_EN1-1, LEASED_EN1-0-1
Description	Firewall -> Interfaces -> IPv4 Groups -> New	Guest
Members	Firewall -> Interfaces -> IPv4 Groups -> New	LAN_EN1-2, LEASED_EN1-0-2
Description	Firewall -> Interfaces -> IPv4 Groups -> New	Users
Members	Firewall -> Interfaces -> IPv4 Groups -> New	LAN_EN1-1, LAN_EN1-2, LEASED_EN1-0-1, LEASED_EN1-0-2

Create policies (network areas connected by the router)

Field	Menu	Value
Source	Firewall -> Policies -> IPv4 Filter Rules -> New	LAN_EN1-0
Destination	Firewall -> Policies -> IPv4 Filter Rules -> New	ANY
Service	Firewall -> Policies -> IPv4 Filter Rules -> New	any
Action	Firewall -> Policies -> IPv4 Filter Rules -> New	Access
Source	Firewall -> Policies -> IPv4 Filter Rules -> New	Employees
Destination	Firewall -> Policies -> IPv4 Filter Rules -> New	Users
Service	Firewall -> Policies -> IPv4 Filter Rules -> New	any
Action	Firewall -> Policies -> IPv4 Filter Rules -> New	Access
Source	Firewall -> Policies -> IPv4 Filter Rules -> New	Guest
Destination	Firewall -> Policies -> IPv4 Filter Rules -> New	Guest

Field	Menu	Value
Service	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>any</i>
Action	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>Access</i>
Source	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>Users</i>
Destination	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>LAN_EN1-4</i>
Service	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>any</i>
Action	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>Access</i>

Create policies (IP addresses connected on the router)

Field	Menu	Value
Source	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>Users</i>
Destination	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>Broadcast</i>
Service	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>Local services</i>
Action	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>Access</i>
Source	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>LAN_EN1-1</i>
Destination	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>Employee LAN GW</i>
Service	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>Local services</i>
Action	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>Access</i>
Source	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>LAN_EN1-2</i>
Destination	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>Guest LAN GW</i>
Service	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>Local services</i>

Field	Menu	Value
Action	Firewall -> Policies -> IPv4 Filter Rules -> New	Access
Source	Firewall -> Policies -> IPv4 Filter Rules -> New	LEASED_EN1-0-1
Destination	Firewall -> Policies -> IPv4 Filter Rules -> New	Employee WLAN GW
Service	Firewall -> Policies -> IPv4 Filter Rules -> New	Local services
Action	Firewall -> Policies -> IPv4 Filter Rules -> New	Access
Source	Firewall -> Policies -> IPv4 Filter Rules -> New	LEASED_EN1-0-2
Destination	Firewall -> Policies -> IPv4 Filter Rules -> New	Guest WLAN GW
Service	Firewall -> Policies -> IPv4 Filter Rules -> New	Local services
Action	Firewall -> Policies -> IPv4 Filter Rules -> New	Access

DHCP configuration

Field	Menu	Value
IP Pool Name	Local Services -> DHCP Server -> IP Pool Configuration -> New	e. g. Slave APs
IP Address Range	Local Services -> DHCP Server -> IP Pool Configuration -> New	10.0.0.10 - 10.0.0.29
Interface	Local Services -> DHCP Server -> DHCP Configuration -> New	en1-0
IP Pool Name	Local Services -> DHCP Server -> DHCP Configuration -> New	e. g. Slave APs
Pool Usage	Local Services -> DHCP Server -> DHCP Configuration -> New	Local
Gateway	Local Services -> DHCP Server -> DHCP Configuration -> New	Use Router as Gateway
DHCP Options	Local Services -> DHCP Server -> DHCP Configuration -> New	DNS Server / 10.0.0.1 and CAPWAP Controller / 10.0.0.1


Field	Menu	Value
IP Pool Name	Local Services -> DHCP Server -> IP Pool Configuration -> New	e. g. <i>Staff-WLAN</i>
IP Address Range	Local Services -> DHCP Server -> IP Pool Configuration -> New	<i>10.0.10.10 - 10.0.10.254</i>
Interface	Local Services -> DHCP Server -> DHCP Configuration -> New	<i>en1-0-1</i>
IP Pool Name	Local Services -> DHCP Server -> DHCP Configuration -> New	e. g. <i>Staff-WLAN</i>
Pool Usage	Local Services -> DHCP Server -> DHCP Configuration -> New	<i>Local</i>
Gateway	Local Services -> DHCP Server -> DHCP Configuration -> New	<i>Use Router as Gateway</i>
DHCP Options	Local Services -> DHCP Server -> DHCP Configuration -> New	<i>DNS Server / 10.0.10.1</i>
IP Pool Name	Local Services -> DHCP Server -> IP Pool Configuration -> New	e. g. <i>Guest-WLAN</i>
IP Address Range	Local Services -> DHCP Server -> IP Pool Configuration -> New	<i>10.0.20.10 - 10.0.20.254</i>
Interface	Local Services -> DHCP Server -> DHCP Configuration -> New	<i>en1-0-2</i>
IP Pool Name	Local Services -> DHCP Server -> DHCP Configuration -> New	e. g. <i>Guest-WLAN</i>
Pool Usage	Local Services -> DHCP Server -> DHCP Configuration -> New	<i>Local</i>
Gateway	Local Services -> DHCP Server -> DHCP Configuration -> New	<i>Use Router as Gateway</i>
DHCP Options	Local Services -> DHCP Server -> DHCP Configuration -> New	<i>DNS Server / 10.0.20.1</i>
IP Pool Name	Local Services -> DHCP Server -> IP Pool Configuration -> New	e. g. <i>Staff-Ethernet</i>
IP Address Range	Local Services -> DHCP Server -> IP Pool Configuration -> New	<i>10.0.1.10 - 10.0.1.254</i>
Interface	Local Services -> DHCP Server -> DHCP Configuration -> New	<i>en1-1</i>
IP Pool Name	Local Services -> DHCP Server -> DHCP Configuration -> New	e. g. <i>Staff-Ethernet</i>
Pool Usage	Local Services -> DHCP Server ->	<i>Local</i>

Field	Menu	Value
	DHCP Configuration -> New	
Gateway	Local Services -> DHCP Server -> DHCP Configuration -> New	Use Router as Gateway
DHCP Options	Local Services -> DHCP Server -> DHCP Configuration -> New	DNS Server/ 10.0.1.1
IP Pool Name	Local Services -> DHCP Server -> IP Pool Configuration -> New	e. g. Guest-Ethernet
IP Address Range	Local Services -> DHCP Server -> IP Pool Configuration -> New	10.0.2.10 - 10.0.2.254
Interface	Local Services -> DHCP Server -> DHCP Configuration -> New	en1-2
IP Pool Name	Local Services -> DHCP Server -> DHCP Configuration -> New	e. g. Guest-Ethernet
Pool Usage	Local Services -> DHCP Server -> DHCP Configuration -> New	Local
Gateway	Local Services -> DHCP Server -> DHCP Configuration -> New	Use Router as Gateway
DHCP Options	Local Services -> DHCP Server -> DHCP Configuration -> New	DNS Server/ 10.0.2.1

Configure WLAN controller







Field	Menu	Value
Region	Wireless LAN Controller -> Controller Configuration -> General	Germany
Interface	Wireless LAN Controller -> Controller Configuration -> General	LAN_EN1-0
DHCP Server	Wireless LAN Controller -> Controller Configuration -> General	Internal
IP Address Range	Wireless LAN Controller -> Controller Configuration -> General	10.0.0.10 - 10.0.0.29
Slave AP location	Wireless LAN Controller -> Controller Configuration -> General	Local (LAN)

Edit wireless networks

Field	Menu	Value
Network Name (SSID)	Wireless LAN Controller -> Slave AP Configuration->Wireless Networks (VSS)-> <vss-1> 	e. g. Employees

Field	Menu	Value
Security mode	Wireless LAN Controller -> Slave AP Configuration->Wireless Networks (VSS)-> <vss-1> 	WPA-PSK
WPA Mode	Wireless LAN Controller -> Slave AP Configuration->Wireless Networks (VSS)-> <vss-1> 	WPA and WPA 2
WPA Cipher	Wireless LAN Controller -> Slave AP Configuration->Wireless Networks (VSS)-> <vss-1> 	TKIP
WPA2 Cipher	Wireless LAN Controller -> Slave AP Configuration->Wireless Networks (VSS)-> <vss-1> 	AES
Preshared key	Wireless LAN Controller -> Slave AP Configuration->Wireless Networks (VSS)-> <vss-1> 	Enter password
VLAN	Wireless LAN Controller -> Slave AP Configuration->Wireless Networks (VSS)-> <vss-1> 	Enabled
VLAN ID	Wireless LAN Controller -> Slave AP Configuration->Wireless Networks (VSS)-> <vss-1> 	10
Network Name (SSID)	Wireless LAN -> WLAN1 ->Wireless Networks (VSS)-> New	e. g. Guest
Security mode	Wireless LAN -> WLAN1 ->Wireless Networks (VSS)-> New	WPA-PSK
WPA Mode	Wireless LAN -> WLAN1 ->Wireless Networks (VSS)-> New	WPA and WPA 2
WPA Cipher	Wireless LAN -> WLAN1 ->Wireless Networks (VSS)-> New	TKIP
WPA2 Cipher	Wireless LAN -> WLAN1 ->Wireless Networks (VSS)-> New	AES
Preshared key	Wireless LAN -> WLAN1 ->Wireless Networks (VSS)-> New	Enter password
VLAN	Wireless LAN -> WLAN1 ->Wireless Networks (VSS)-> New	Enabled
VLAN ID	Wireless LAN -> WLAN1 ->Wireless Networks (VSS)-> New	20

Edit radio profiles

Field	Menu	Value
Operation Band	Wireless LAN Controller -> Slave AP Configuration-> Radio Profiles-> <2.4 GHz Radio Profile> 	2.4 GHz In/Outdoor
Wireless Mode	Wireless LAN Controller -> Slave AP Configuration-> Radio Profiles-> <2.4 GHz Radio Profile> 	802.11g/n
Burst Mode	Wireless LAN Controller -> Slave AP Configuration-> Radio Profiles-> <2.4 GHz Radio Profile> 	Enabled
Channel plan	Wireless LAN Controller -> Slave AP Configuration -> Radio Profiles-> <2.4 GHz Radio Profile>  -> Advanced Settings	User-defined
User-defined Channel Plan	Wireless LAN Controller -> Slave AP Configuration -> Radio Profiles-> <2.4 GHz Radio Profile>  -> Advanced Settings	1, 5, 9, 13
Short Guard Interval	Wireless LAN Controller -> Slave AP Configuration -> Radio Profiles-> <2.4 GHz Radio Profile>  -> Advanced Settings	Enabled

Set up slave access points

Field	Menu	Value
Location	Wireless LAN Controller -> Slave-AP Configuration-> Slave Access Points	e. g. Meeting Room
Description	Wireless LAN Controller -> Slave-AP Configuration-> Slave Access Points	e. g. Marketing
CAPWAP Encryption	Wireless LAN Controller -> Slave-AP Configuration-> Slave Access Points	Enabled
Operation Mode	Wireless LAN Controller -> Slave-AP Configuration-> Slave Access Points	On
Active wireless module	Wireless LAN Controller -> Slave-	2.4 GHz Radio Pro-

Field	Menu	Value
profile	AP Configuration-> Slave Access Points	<i>file</i>
Channel	Wireless LAN Controller -> Slave-AP Configuration-> Slave Access Points	<i>Auto</i>
Assigned wireless networks (VSS)	Wireless LAN Controller -> Slave-AP Configuration-> Slave Access Points	<i>vss-1: Employee/ vss-2: Guest</i>
Location	Wireless LAN Controller -> Slave-AP Configuration-> Slave Access Points	<i>e. g. Kitchen</i>
Location	Wireless LAN Controller -> Slave-AP Configuration-> Slave Access Points	<i>e. g. Terrace</i>
Location	Wireless LAN Controller -> Slave-AP Configuration-> Slave Access Points	<i>e. g. Bottom of stairs</i>
Location	Wireless LAN Controller -> Slave-AP Configuration-> Slave Access Points	<i>e. g. Bend in stairs</i>
Location	Wireless LAN Controller -> Slave-AP Configuration-> Slave Access Points	<i>e. g. End of hall</i>

New channel setting

Field	Menu	Value
New channel setting	Wireless LAN Controller -> Slave-AP Configuration-> Slave Access Points	START

Chapter 6 WLAN network with guest WLAN

6.1 Introduction

The following section describes how to configure a WLAN access to the local network and a guest WLAN. To integrate additional Access Points, use the Wireless LAN Controller. For the separation of both networks on Layer 2 level, a VLAN is configured for the guest network. The users of the guest WLAN have unrestricted access to the internet, but no access to the local network.

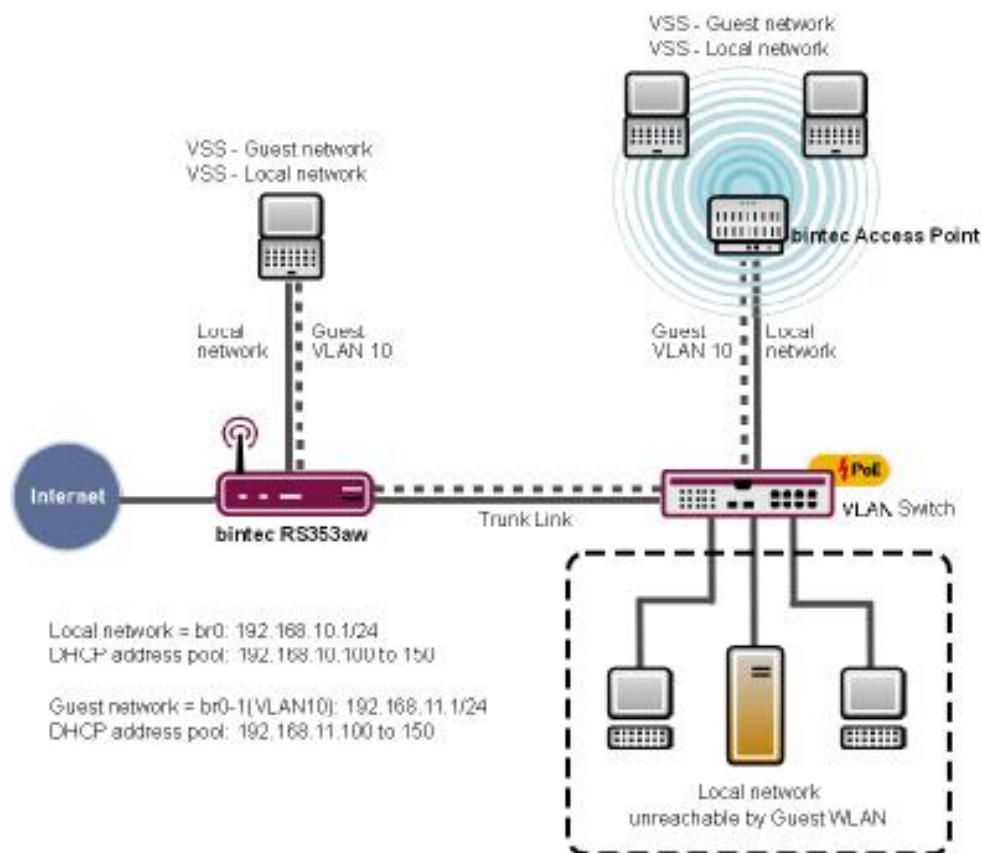


Fig. 112: Example WLAN scenario with guest WLAN



Note

The Trunk Link (see illustration) leads to **RS353aw** with one of the four ETH Ports (ETH1 to ETH4), which are assigned 1-0 by default.

Requirements

The following prerequisites for configuration must be met:

- An RS-series device, a be.IP or be.IP plus
- A boot image of version 10.1.9 patch 3 or above
- Switches, which support 802.1q VLAN

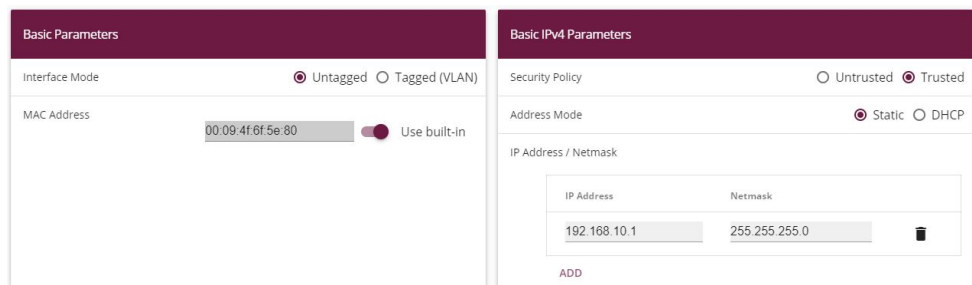
The **GUI** (Graphical User Interface) is used for configuring.

6.2 Configuration

6.2.1 Configuring the IP address

Configure an IP address from the LAN interface.

- (1) Go to **LAN->IP Configuration->Interfaces-><en1-0>->** 



The screenshot shows two configuration panels for the interface en1-0:

- Basic Parameters:**
 - Interface Mode: Untagged Tagged (VLAN)
 - MAC Address: 00:09:4f:6f:5e:80 Use built-in
- Basic IPv4 Parameters:**
 - Security Policy: Untrusted Trusted
 - Address Mode: Static DHCP
 - IP Address / Netmask:


IP Address	Netmask	
192.168.10.1	255.255.255.0	
 - ADD button

Fig. 113: **LAN->IP Configuration->Interfaces-><en1-0>->** 

Proceed as follows to configure the IP address:

- (1) Set the **Security Policy** to *Trusted*.
- (2) Leave the **Address Mode** on *Static*.
- (3) Click **Add**. Enter the IP address, e.g. *192.168.10.1*. Leave **Netmask** *255.255.255.0*.

(4) Press **OK** to confirm your entries.

6.2.2 Create bridge groups and assign LAN interface

Create a new bridge group and assign the LAN interface to these.

Go to **System Management->Interface Mode / Bridge Groups->Interfaces**.

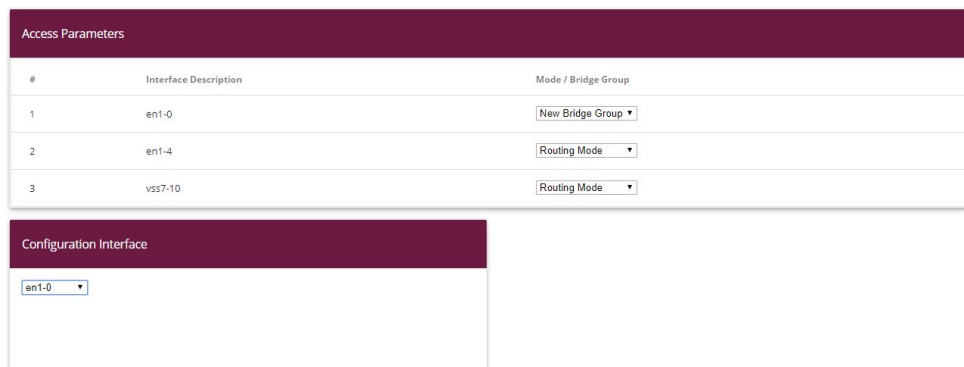



Fig. 114: **System Management->Interface Mode / Bridge Groups->Interfaces**

Proceed as follows to assign the LAN interface to a new bridge group and to transfer the IP address of the LAN interface to the bridge group.

- (1) Choose the line *en1-0* under **Mode / Bridge Group** *New Bridge Group*.
- (2) Set to **Configuration Interface** *en1-0*.

As soon as you have pressed **OK**, the bridge group *br0* is created automatically and the interface *en1-0* is added to this bridge group. The bridge group *br0* automatically receives the IP configuration for the *en1-0* interface. You can check the IP configuration of the bridge group *br0* in the **LAN -> IP Configuration -> <br0>** ->  menu.

6.2.3 Put Wireless LAN Controller into operation

The IP Address Range, which you will configure below, must match the IP address of the LAN facility.

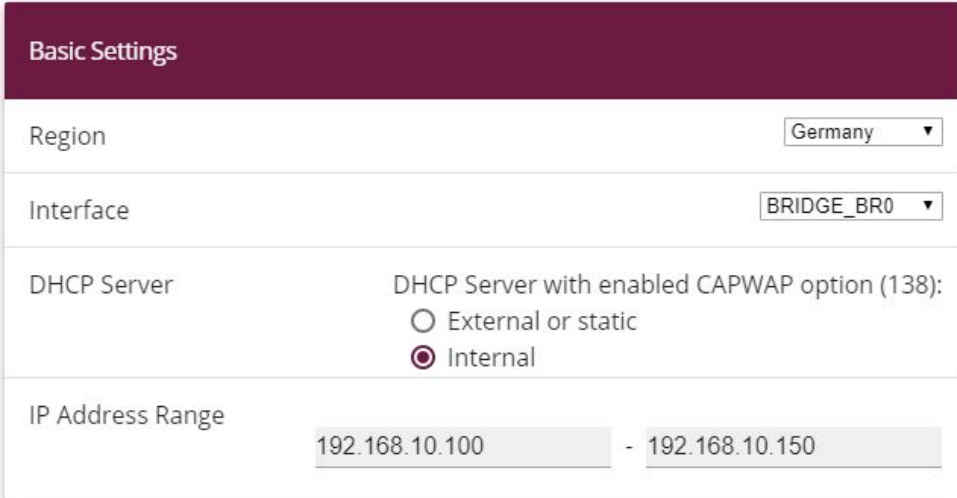


Note

If, in the menu **Local Services->DHCP Server->DHCP Configuration** of the interface *en1-0*, there was already an IP pool assigned, then this entry must be deleted.

Go to the following menu to configure an IP Address Range:

Go to **Wireless LAN Controller->Wizard->Step 1**.



The screenshot shows a configuration window titled "Basic Settings". It contains the following fields and options:

- Region:** A dropdown menu set to "Germany".
- Interface:** A dropdown menu set to "BRIDGE_BR0".
- DHCP Server:** A section titled "DHCP Server with enabled CAPWAP option (138):" containing two radio buttons: "External or static" (unselected) and "Internal" (selected).
- IP Address Range:** Two input fields containing "192.168.10.100" and "192.168.10.150", separated by a hyphen.

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

Proceed as follows:

- (1) Select the country in which the wireless LAN controller is to be operated. Leave, under **Region**, the entry *Germany*.
- (2) Select the **Interface** to be used for the wireless controller, here *BRIDGE_BR0*.
- (3) Select **DHCP Server** *Internal*.
- (4) Enter the first and last value of the IP Address Range, e.g. *192.168.10.100 - 192.168.10.150*.
- (5) Click on **Next**.

6.2.4 Choose radio profile and configure WLAN access to the local network.

Determine which radio profile is to be used. **Use two independent radio profiles** should be activated, when access point with two 2.4/5 Ghz-capable radio profiles are installed.

Step 2

Fig. 116: **Wireless LAN Controller->Wizard**

Proceed as follows:

- (1) Activate this option **Use two independent radio profiles** when APs with two radio profiles are used in your network.
Radio profile for module 1 (for all Access Points) = 2.4 GHz Radio Profile
and Radio profile for module 2 (only for APs with 2 radio modules) = 5 GHz Radio Profile is automatically chosen and shown.

- (2) Click **Next**.

Step 3

VSS Description	Network Name (SSID)	Security
vss-1	default	WPA-PSK

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

Configure the WLAN access to your local network. At vss-1, click the icon .

Step 3

Fig. 118: **Wireless LAN Controller->Wizard-><vss-1>**

- (3) Enter a **Network Name (SSID)** for the profile, e.g. *Local-Network*.
- (4) Enter, under **Preshared Key**, a password, e.g. *supersecret*, leave the presetting of the remaining parameters and click on **OK**.
 You see the local network which you have configured.

6.2.5 Configure guest WLAN

You have configured a WLAN access to your local network and are now configuring a guest network. For the separation of both networks on Layer 2 level, configure a VLAN for the guest network, in the following example with VLAN ID 10. All data packets in the guest WLAN are VLAN 10 tagged, data packets in the local WLAN are untagged.



Note

Please note that the switches in your 802.1q VLAN network must be supporting, so that the Layer 2 separation of both network works.

The Wireless LAN Controller configures your bintec-elmeg Access Points, you must configure your switches according yourself.

Click, in **Wireless LAN Controller->Wizard Add.**

Step 3

Service Set Parameters	
Network Name (SSID)	Guest-Network <input type="checkbox"/> Visible
IGMP Snooping	<input checked="" type="checkbox"/> Enabled

Security Settings	
Security Mode	WPA-PSK
WPA Mode	WPA 2
Preshared Key	*****

VLAN	
VLAN	<input checked="" type="checkbox"/> Enabled
VLAN ID	10

Fig. 119: **Wireless LAN Controller->Wizard->Add**

Proceed as follows:

- (1) Enter a **Network Name (SSID)** for the guest network, e.g. *Guest-Network*.
- (2) Set **Security Mode** *WPA PSK*.
- (3) Set **WPA Mode** *WPA 2*.
- (4) Enter a **Preshared Key**, e.g. *supersecret*.
- (5) Click **VLAN** on *Enabled*.
- (6) Enter a **VLAN ID**, e.g. *10*.
- (7) Confirm with **OK**.

You see the local network together with the guest network which you have just configured.





Wireless Networks (VSS)			
VSS Description	Network Name (SSID)	Security	
vss-1	Local-Network	WPA-PSK	 
vss-2	Guest-Network	WPA-PSK	 

Fig. 120: **Wireless LAN Controller->Wizard** with configured guest network
Click **Next**.

All found Access Points are shown.

Set **Manage** in the column of those Access Points which you wish to have automatically configured and managed by the Wireless LAN Controller.

Step 4

Wireless LAN Controller Wizard								
Manage								
<input type="checkbox"/> Select all / <input type="checkbox"/> Deselect all	Location	Device	IP Address	LAN MAC Address	Wireless Network	Radio Profile	Channel	Status
<input checked="" type="checkbox"/>	1:	be.IP plus	192.168.0.251	Elmeqt_6f5e7c	vss-1:Local-Network vss-2:Guest-Network	2.4 GHz Radio Profile	0	Discovered 
<input checked="" type="checkbox"/>	2:	W2003ac	192.168.0.100	BintecCo_48:69:c1	vss-1:Local-Network vss-2:Guest-Network	2.4 GHz Radio Profile 5 GHz Radio Profile	0 0	Gefunden 

 Ready to apply the automatic installation! Select the access points that are to be managed with the Wireless LAN Controller and click START if you want to start the automatic installation now! The radio channels will be selected automatically. This may take up to 10 minutes.

Fig. 121: **Wireless LAN Controller->Wizard**

6.2.6 Configure Access Points with the Wireless LAN Controller

Let the chosen Access Points from the Wireless LAN Controller be automatically configured.

(1) Click **Start**.

The configuration process is carried out step by step and can, according to the number of the installed points, take a while.

(2) After the configuration is finished, check if all of the chosen access points are in **Status Managed**. All *Managed* Access Points have received a configuration from the WLAN controller and are managed by these.

Slave Access Points							
Location	Device	IP Address	LAN MAC Address	Wireless Network Profile	Radio Profile	Channel	Status
1:	be.IP plus	192.168.0.251	Elmegt_6f5e7c	vss-1:Local-Network vss-2:Guest-Network	2.4 GHz Radio Profile	6	Managed
2:	W2003ac	192.168.0.100	BintecCo_48f69c1	vss-1:Local-Network vss-2:Guest-Network	2.4 GHz Radio Profile 5 GHz Radio Profile	0 0	Managed

WLAN-Controller Installation completed.

Please save the configuration by pressing the "Save Configuration" Button.

Fig. 122: Wireless LAN Controller->Wizard

6.2.7 Configure the IP address for the virtual Bridge Interface

Configure a virtual bridge interface with VLAN ID 10, so that the WLAN clients can access the local service, e.g. DHCP, DNS and Echo. Configure an IP address for this interface.

Go to the following menu:

Go to **LAN->IP Configuration->Interfaces->New**.

Basic Parameters

Based on Ethernet Interface br0

Interface Mode Untagged Tagged (VLAN)

VLAN ID 10

MAC Address 00:a0:f9 Use built-in

Basic IPv4 Parameters

Security Policy Untrusted Trusted

Address Mode Static DHCP

IP Address / Netmask

IP Address	Netmask	
192.168.11.1	255.255.255.0	🗑️

ADD

Fig. 123: LAN->IP Configuration->Interfaces->New

Proceed as follows:

- (1) Set *br0* under **Based on Ethernet Interface**.
- (2) Leave, under **Interface Mode**, the *Tagged (VLAN)* entry.
- (3) Enter the **VLAN ID** value *10*.
- (4) Under **Security Policy** select *Untrusted*.
- (5) Leave the **Address Mode** *Static*.
- (6) Click **Add**. Enter the IP address, e.g. *192.168.11.1*. Leave the **Netmask** *255.255.255.0*.

(7) Press **OK** to confirm your entries.

The result of your configuration is shown in the list in the last line.

Ethernet/VLAN Ports				
Interface	IPv4 Address/Netmask	IPv6 Address/Length	Status	Action
en1-4	192.168.4.251/255.255.255.0	-	✘	^ v ✎ 🔍
efm35-60	Not configured/Not configured	-	✘	^ v ✎ 🔍
ethoa35-5	Not configured/Not configured	-	✘	^ v ✎ 🔍
br0(VLAN ID1)	192.168.0.251/255.255.255.0	-	✔	^ v ✎ 🔍
br0-1(VLAN ID10)	192.168.10.1/255.255.255.0	-	✔	🗑️ ✎ 🔍
br0-2(VLAN ID10)	192.168.11.1/255.255.255.0	-	✔	🗑️ ✎ 🔍

Fig. 124: LAN->IP Configuration->Interfaces->New

6.2.8 Configure the IP Address Range for the guest network

Configure an IP Address Range for the IP Address Assignment to WLAN Clients in the guest network. This IP Address Range must match the just-configured IP address of the virtual Bridge Interface.

Go to the following menu to configure an IP Address Range:

Go to **Local Services->DHCP Server->IP Pool Configuration->New**.

Basic Parameters

IP Pool Name

IP Address Range
 -

DNS Server

Fig. 125: Local Services->DHCP Server->IP Pool Configuration->New

Proceed as follows:

- (1) Enter, under **IP Pool Name**, a description, e.g. *Guest-Address-Pool*.
- (2) Enter, under **IP Address Range**, the first and last value of the IP Address Range, e.g. *192.168.11.100 - 192.168.11.150*.
- (3) Press **OK** to confirm your entries.

You see the new IP Address Range in the list.

IP Pools:				
IP Pool Name	IP Address Range	Primary DNS Server	Secondary DNS Server	
Guest-Address-Pool	192.168.11.100 - 192.168.11.150	0.0.0.0	0.0.0.0	<input type="checkbox"/> <input type="checkbox"/>
	192.168.10.100 - 192.168.10.150	0.0.0.0	0.0.0.0	<input type="checkbox"/> <input type="checkbox"/>

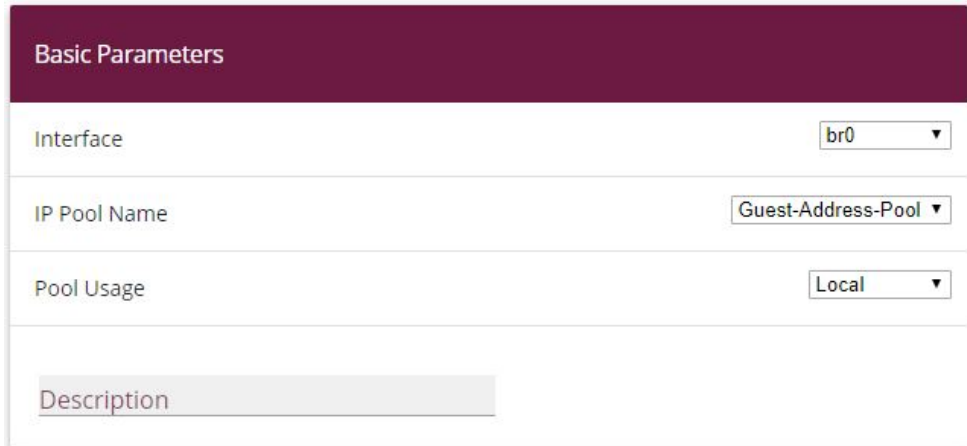
Fig. 126: Local Services->DHCP Server->IP Pool Configuration

6.2.9 Configure DHCP use

Configure the use of DHCP for WLAN Clients in guest networks.

Go to the following menu:

Go to **Local Services->DHCP Server->DHCP Configuration->New**.



The screenshot shows a web form titled "Basic Parameters" for creating a new DHCP configuration. It contains the following fields:

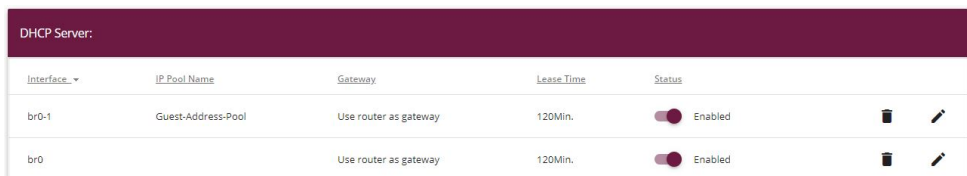
- Interface:** A dropdown menu with "br0" selected.
- IP Pool Name:** A dropdown menu with "Guest-Address-Pool" selected.
- Pool Usage:** A dropdown menu with "Local" selected.
- Description:** A text input field that is currently empty.

Fig. 127: **Local Services->DHCP Server->DHCP Configuration->New**

Proceed as follows:

- (1) Select a **Interface** e.g. *br0-1*.
- (2) Choose, under **IP Pool Name**, an IP address pool, e.g. *Guest-Address-Pool*.
- (3) Choose, under **Pool Usage**, for which the DNCP requests of the DHCP pool should be used, e.g. *Local*.
- (4) Press **OK** to confirm your entries.

You see the new DHCP configuration in the list.



The screenshot shows a table titled "DHCP Server:" with the following columns: Interface, IP Pool Name, Gateway, Lease Time, and Status. There are two rows of configuration data.

Interface	IP Pool Name	Gateway	Lease Time	Status
br0-1	Guest-Address-Pool	Use router as gateway	120Min.	Enabled
br0		Use router as gateway	120Min.	Enabled


Fig. 128: **Local Services->DHCP Server->DHCP Configuration**

6.2.10 Set up firewall

The following firewall configuration is a simple example, to guarantee the basic function of the firewall. If you require further safety adjustments, then adapt this example to your requirements.

Define bridge interface as trustworthy

Define the interface *br0* (the interface for your local network) as a trustworthy interface.

Go to **Firewall->Policies->IPv4 Filter Rules**. In the **Default Filter Rules** in the Trusted Interfaces area, click the  icon.

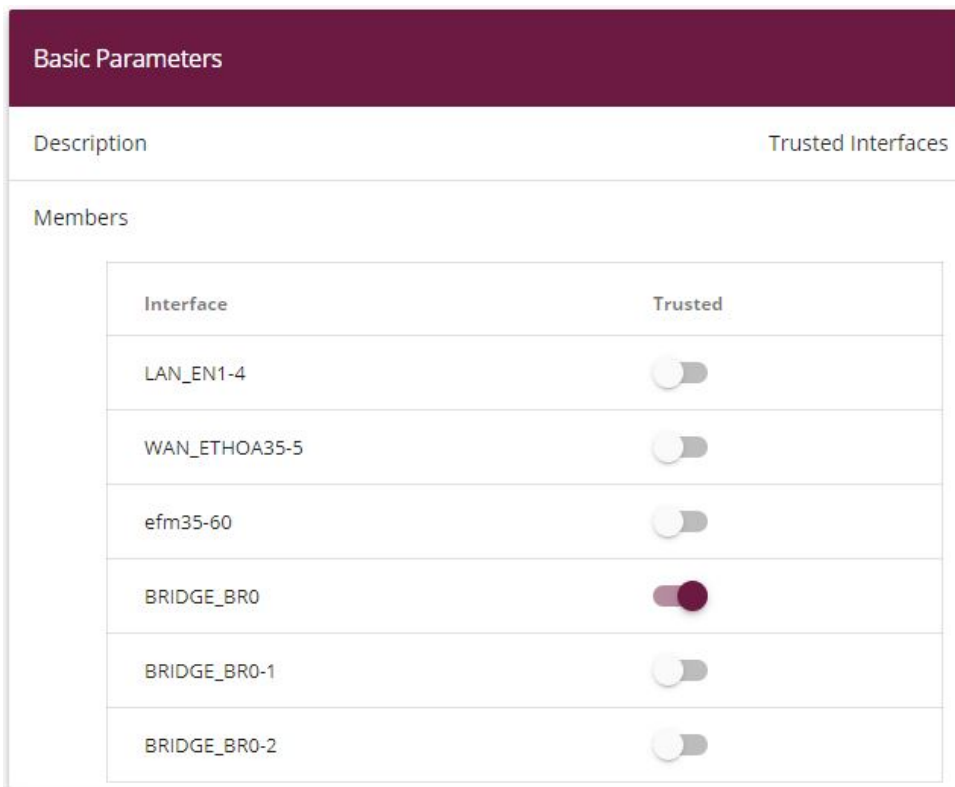


Fig. 129: **Firewall->Policies->IPv4 Filter Rules->Default Filter Rules** 

Proceed as follows:

- (1) Highlight the interface *BRIDGE_BR0* as a trustworthy interface.
- (2) Make sure that no further interface is highlighted.
- (3) Press **OK** to confirm your entries.

Create service group

Create a service group with the services which the clients in the guest WLAN wish to use.

Go to **Firewall->Services->Groups->New**.

Basic Parameters

Description
Guest-Local Access

Members

Service	Selection
activity	<input type="checkbox"/>
ah	<input type="checkbox"/>
any	<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"/>

Fig. 130: **Firewall->Services->Groups->New**

Proceed as follows:

- (1) Enter a **Description**, e.g. *Guest-Local-Access*.
- (2) Choose the desired **Members**, e.g. *dhcp*, *dns* and *echo*.
- (3) Press **OK** to confirm your entries.

The configured service group is displayed.



Groups			
Description	Members		
Guest-Local Access	echo-req, dns, dhcp		

Fig. 131: Firewall->Services->Groups

Creating Ipv4 filter rules

Create a rule, so that your guests can use the services of the DHCP, DNS and Echo, that you have combined in a Service Group.

Go to **Firewall->Policies->IPv4 Filter Rules->New**.

Basic Parameters

Source	BRIDGE_BR0-1 ▼
Destination	LOCAL ▼
Service	Guest-Local-Access ▼
Action	Access ▼

Fig. 132: Firewall->Policies->IPv4 Filter Rules->New

Proceed as follows:

- (1) Set **Source** *BRIDGE_BR0-1*.
- (2) Set **Destination** *LOCAL*.
- (3) Set *Guest-Local-Access* as a **Service** or service group.
- (4) Set **Action** *Access*.
- (5) Press **OK** to confirm your entries.

Create a filter rule for the access of your guests to the internet.

Go to **Firewall->Policies->IPv4 Filter Rules->New**.

Proceed as follows:

- (1) Set **Source** `BRIDGE_BR0-1`.
- (2) Set **Destination** `WAN_INTERNET`.
- (3) Select a **Service**, e.g. `any`.
- (4) Set **Action** `Access`.
- (5) Press **OK** to confirm your entries.

Both filter rules are shown.

Filter Rules						
Order	Source	Destination	Service	Action	Policy active	
1	BRIDGE_BR0-1	LOCAL	Guest-Local Access	Access	<input checked="" type="checkbox"/> Enabled	↑ ↓ ⋮ 🗑️ ✎
2	BRIDGE_BR0-1	WAN_INTERNET	any	Access	<input checked="" type="checkbox"/> Enabled	↑ ↓ ⋮ 🗑️ ✎

Default Filter Rules						
Order	Source	Destination	Service	Action	Policy active	
n+1	Trusted Interfaces	✎ ANY	ANY	Access	<input type="checkbox"/> Enabled	
n+2	Untrusted Interfaces	ANY	ANY	Deny	<input type="checkbox"/> Enabled	

Fig. 133: Firewall->Policies->IPv4 Filter Rules

Add further rules to this if needed.

Switch on firewall

When you have finished the firewall configuration, you must switch on the firewall.

Go to **Firewall->Policies->options**.

Global Firewall Options	
IPv4 Firewall Status	<input checked="" type="checkbox"/> Enabled
Logged Actions	All ▾
IPv4 Full Filtering	<input checked="" type="checkbox"/> Enable
STUN Handler	<input type="checkbox"/>

Session Timer	
UDP Inactivity	180 Seconds
TCP Inactivity	3600 Seconds
PPTP Inactivity	86400 Seconds
Other Inactivity	30 Seconds

Fig. 134: Firewall->Policies->Options

Proceed as follows:




- (1) Activate the **IPv4 Firewall Status**.
- (2) Press **OK** to confirm your entries.

6.3 Result

You have configured a WLAN access to the local network and a guest WLAN. Your guests can access the internet, but not the local network.

6.4 Overview of Configuration Steps

Configuring the IP address

Field	Menu	Value
Security Policy	LAN-> IP Configuration-> Interfaces -><en1-0-> 	<i>Trusted</i>
Address Mode	LAN ->IP Configuration-> Interfaces-><en1-0-> 	<i>Static</i>
IP Address / Netmask	LAN ->IP Configuration ->Interfaces -><en1-0-> 	<i>192.168.10.1 / 255.255.255.0</i>

Create bridge groups and assign LAN interface

Field	Menu	Value
Interface Description	System Management ->Interface Mode / Bridge Groups ->Interfaces	<i>en1-0</i>
Mode / Bridge Group	System Management ->Interface Mode / Bridge Groups ->Interfaces	<i>New Bridge Group</i>
Configuration Interface	System Management ->Interface Mode / Bridge Groups ->Interfaces	<i>en1-0</i>

Put Wireless LAN Controller into operation

Field	Menu	Value
Region	Wireless LAN Controller-> Wizard	<i>Germany</i>
Interface	Wireless LAN Controller ->Wizard	<i>BRIDGE_BRO</i>
DHCP Server	Wireless LAN Controller ->Wizard	<i>Internal</i>
IP Address Range	Wireless LAN Controller ->Wizard	<i>e. g. 192.168.10.100 / 192.168.10.150</i>

Choose radio profile and configure WLAN access to the local network.

Field	Menu	Value
Use two independent radio profiles	Wireless LAN Controller-> Wizard ->Next	Enabled
Radio profile for module 1 (for all Access Points)	Wireless LAN Controller-> Wizard ->Next	2.4 GHz Radio Profile
Radio profile for module 2 (only for APs with two radio modules)	Wireless LAN Controller-> Wizard ->Next	5 GHz Radio Profile
Network Name (SSID)	Wireless LAN Controller-> Wizard ->Next -><vss-1>> 	Local Network
Preshared Key	Wireless LAN Controller ->Wizard ->Next -><vss-1>> 	e. g. supersecret

Configure guest WLAN

Field	Menu	Value
Network Name (SSID)	Wireless LAN Controller ->Wizard ->Next ->Add	e.g. Guest-Network
Security Mode	Wireless LAN Controller-> Wizard ->Next-> Add	WPA PSK
WPA Mode	Wireless LAN Controller-> Wizard ->Next ->Add	WPA2
Preshared Key	Wireless LAN Controller-> Wizard ->Next-> Add	e.g. Super-Secret-1
VLAN	Wireless LAN Controller-> Wizard ->Next-> Add	Enabled
VLAN ID	Wireless LAN Controller ->Wizard ->Next-> Add	e. g. 10
Manage	Wireless LAN Controller ->Wizard ->Next	Enabled

Configure Access Points with the Wireless LAN Controller

Field	Menu	Value
Wireless LAN Controller Wizard	Wireless LAN Controller-> Wizard ->Next-> Next ->Next	START

Configure the IP address for the virtual Bridge Interface

Field	Menu	Value
Based on Ethernet In-	LAN ->IP Configuration ->Inter-	br0

Field	Menu	Value
terface	faces-> New	
Interface Mode	LAN-> IP Configuration-> Inter- faces-> New	<i>Tagged (VLAN)</i>
VLAN ID	LAN ->IP Configuration ->Inter- faces-> New	<i>10</i>
Security Policy	LAN-> IP Configuration ->Inter- faces ->New	<i>Untrusted</i>
Address Mode	LAN-> IP Configuration ->Inter- faces-> New	<i>Static</i>
IP Address / Netmask	LAN ->IP Configuration ->Inter- faces-> New	<i>192.168.11.1 / 255.255.255.0</i>


Configure the IP Address Range for the guest network

Field	Menu	Value
IP Pool Name	Local Services ->DHCP Server-> IP Pool Configuration-> New	<i>Guest-Address-Pool</i>
IP Address Range	Local Services ->DHCP Server ->IP Pool Configuration ->New	<i>e. g. 192.168.11.100 / 192.168.11.150</i>

Configure DHCP use

Field	Menu	Value
Interface	Local Services-> DHCP Server-> DHCP Configuration ->New	<i>br0-1</i>
IP Pool Name	Local Services-> DHCP Server-> DHCP Configuration-> New	<i>Guest-Address-Pool</i>
Pool Usage	Local Services ->DHCP Server-> DHCP Configuration ->New	<i>Local</i>

Set up firewall

Field	Menu	Value
BRIDGE_BR0	Firewall-> Policies ->IPv4 Filter Rules ->Default Filter Rules 	Trusted <i>Enabled</i>
Description	Firewall-> Services-> Groups-> New	<i>e.g. Guest-Lo- cl-Access</i>
Members	Firewall-> Services-> Groups-> New	<i>e.g. dhcp, dns and echo</i>
Source	Firewall ->Policies-> IPv4 Filter Rules-> New	<i>BRIDGE_BR0-1</i>

Field	Menu	Value
Destination	Firewall-> Policies ->IPv4 Filter Rules ->New	<i>LOCAL</i>
Service	Firewall-> Policies ->IPv4 Filter Rules ->New	<i>Guest-Local-Access</i>
Action	Firewall-> Policies ->IPv4 Filter Rules ->New	<i>Access</i>
Source	Firewall ->Policies-> IPv4 Filter Rules-> New	<i>BRIDGE_BR0-1</i>
Destination	Firewall-> Policies ->IPv4 Filter Rules ->New	<i>WAN_INTERNET</i>
Service	Firewall-> Policies ->IPv4 Filter Rules ->New	e.g. <i>any</i>
Action	Firewall-> Policies ->IPv4 Filter Rules ->New	<i>Access</i>
Status of the IPv4 Firewall	Firewall-> Policies-> Options	<i>Enabled</i>

Chapter 7 WLAN - WLAN controller installation with integrated HotSpot functionality

7.1 Introduction

A WLAN network is to be created with a wireless LAN controller and the **bintec HotSpot Solution**. The WLAN network is to provide two SSIDs. One SSID for employees, who are to be given full access to the internal network and the Internet. The second SSID is for guests who are only to have Internet access after logging in via the bintec HotSpot solution.

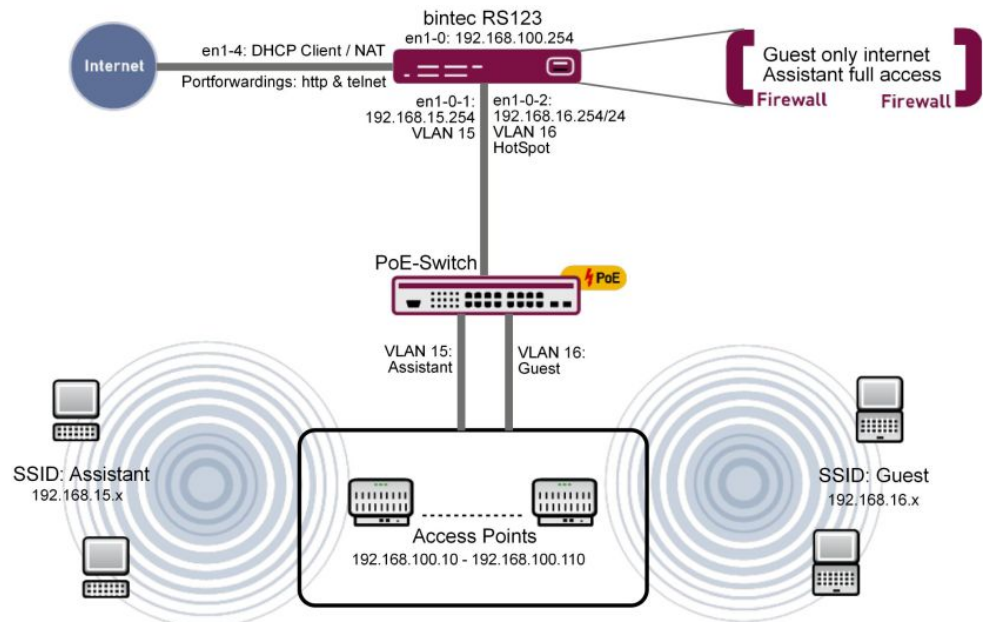


Fig. 135: Example scenario

Requirements

- An RS series router (e. g. **bintec RS123**) or an RXL series device (e. g. **bintec RXL12500**)
- A **bintec W2003ac**
- Software licenses for the bintec router
- WLAN controller licence

- 6 access points
- bintec Hotspot hosting 2yrs 1 location

7.2 Function

The bintec router (e. g. **bintec RS123**) serves, at the same time, as a gateway, firewall, WLAN controller and HotSpot gateway. The access points provide SSIDs which are each tagged with a separate VLAN. The router uses the tagging to separate the two traffic flows and provides them internally to two virtual ports.

The router provides three DHCP pools. One for the access points (192.168.100.10 to 192.168.100.110), this is automatically created by the wireless LAN controller wizard. When doing so, the wireless LAN controller wizard automatically includes the configuring of the DHCP option 138. That is the WLAN controller address which the access points require to communicate with the WLAN controller. The other two DHCP pools are created manually and are used, respectively, for the SSIDs *employees* and SSIDs *guests*.



Note

In small WLAN installations of up to 6 access points, a **bintec W2003ac** can also be used as a WLAN controller. This cannot be done here because the device also has to take on the HotSpot gateway functionality at the same time. However, to do this, router functions are required which are deactivated in the **bintec W2003ac** if it is working as a WLAN controller.

7.3 Configuration

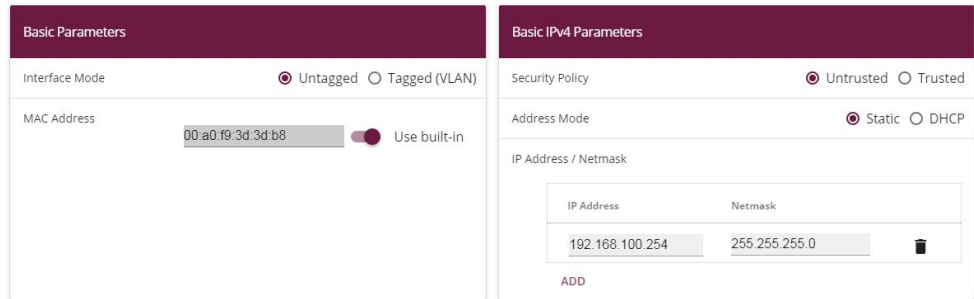
7.3.1 Basic configuration

Before you start configuring based on the description below, you need to set up an Internet access using the assistants. If you have acquired a WLAN controller license, you need to enter it in the menu **System Management -> Global Settings -> System Licenses**. You also need to specify an NTP time server and set up the time zone. This is vital if the HotSpot is to work reliably. Do not, initially, set up a DHCP pool for the router, since the DHCP pool for the WLAN access points is set up automatically when setting up the WLAN controller.

7.3.2 LAN configuration

First of all, change the IP address in the **IP Configuration** menu.

- (1) Go to **LAN -> IP Configuration -> Interfaces -> <en1-0>** .



The screenshot shows two configuration panels for the interface `en1-0`.

- Basic Parameters:**
 - Interface Mode: Untagged Tagged (VLAN)
 - MAC Address: `00:a0:f9:3d:b8` Use built-in
- Basic IPv4 Parameters:**
 - Security Policy: Untrusted Trusted
 - Address Mode: Static DHCP
 - IP Address / Netmask:
 - IP Address: `192.168.100.254`
 - Netmask: `255.255.255.0`

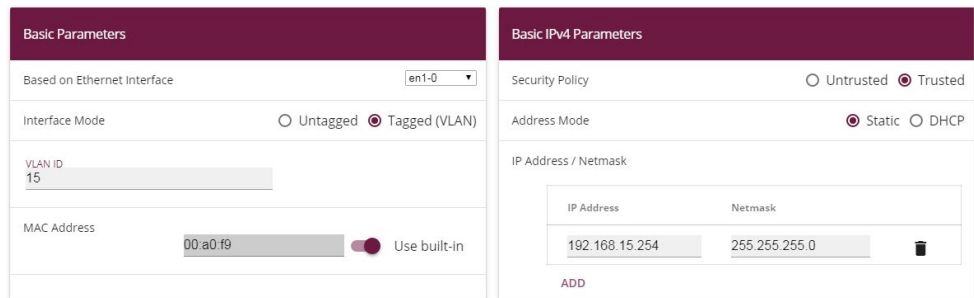
Fig. 136: **LAN -> IP Configuration -> Interfaces -> <en1-0>** .

Proceed as follows:

- (1) Set the **Interface Mode** to *Untagged*.
- (2) Enter the **IP Address / Netmask** `192.168.100.254`.
- (3) Confirm with **OK**.

Now add the virtual interface.

- (1) Go to **LAN -> IP Configuration -> Interfaces -> New**.



The screenshot shows two configuration panels for a new virtual interface.

- Basic Parameters:**
 - Based on Ethernet Interface: `en1-0`
 - Interface Mode: Untagged Tagged (VLAN)
 - VLAN ID: `15`
 - MAC Address: `00:a0:f9` Use built-in
- Basic IPv4 Parameters:**
 - Security Policy: Untrusted Trusted
 - Address Mode: Static DHCP
 - IP Address / Netmask:
 - IP Address: `192.168.15.254`
 - Netmask: `255.255.255.0`

Fig. 137: **LAN -> IP Configuration -> Interfaces -> New**

Proceed as follows:

- (1) For **Based on Ethernet Interface**, select `en1-0`.
- (2) For **Interface Mode**, select *Tagged (VLAN)*.
- (3) Assign a **VLAN ID** to the interface, e. g. `15`.
- (4) Use **Add** to enter the **IP Address / Netmask** `192.168.15.254`.
- (5) Confirm with **OK**.

You have added a virtual interface `en1-0-1` with the **VLAN ID** `15`.

- (1) Go to **LAN -> IP Configuration -> Interfaces -> New** to create another interface.
- (2) For **Based on Ethernet Interface**, select `en1-0`.
- (3) For **Interface Mode**, select `Tagged (VLAN)`.
- (4) Assign a **VLAN ID** to the interface, e. g. `16`.
- (5) Use **Add** to enter the **IP Address / Netmask** `192.168.16.254`.
- (6) Confirm with **OK**.

You have added a virtual interface `en1-0-2` with the **VLAN ID** `16`.

After this configuration, the **Interfaces** menu looks like this.

Ethernet/VLAN Ports					
Interface	IPv4 Address/Netmask	IPv6 Address/Length	Status	Action	
en1-0	192.168.100.254/255.255.255.0	-	✓	^ v	
en1-4	Not configured/Not configured	-	✗	^ v	
efm35-60	Not configured/Not configured	-	✗	^ v	
en1-0-1(VLAN ID15)	192.168.15.254/255.255.255.0	-	✓	^ v	
en1-0-2(VLAN ID16)	192.168.16.254/255.255.255.0	-	✓	^ v	

Fig. 138: LAN -> IP Configuration -> Interfaces

7.3.3 HotSpot configuration

To prepare for the configuration, you need to get your license authorised via the licensing portal on the bintec elmeg website <http://www.bintec-elmeg.com>. You will then quickly be sent your personal access data.

First you need to enter a RADIUS server.

RADIUS (Remote Authentication Dial In User Service) is a service that enables authentication and configuration information to be exchanged between your device and a RADIUS server.

- (1) Go to **System Management -> Remote Authentication -> RADIUS ->New**.

The screenshot displays a configuration form for a RADIUS server. The form is titled "Basic Parameters" and contains the following fields:

- Authentication Type:** A dropdown menu set to "Accounting".
- Vendor Mode:** A dropdown menu set to "bintec HotSpot Server".
- Server IP Address:** A text input field containing "62.245.165.180".
- RADIUS Secret:** A text input field with masked characters (dots).
- Default User Password:** A text input field with masked characters (dots).
- Priority:** A dropdown menu set to "0".
- Entry active:** A toggle switch that is turned on, labeled "Enabled".
- Group Description:** A dropdown menu set to "Default Group 0".

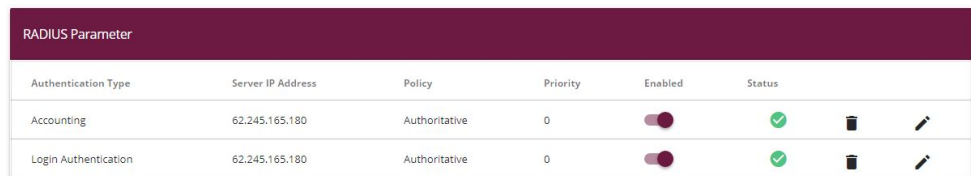
Fig. 139: **System Management -> Remote Authentication -> RADIUS -> New**

Proceed as follows to set up a RADIUS server:

- (1) Select the **Authentication Type** *Accounting*. The RADIUS server is used for recording statistical call data.
- (2) As **Vendor Mode**, select *bintec HotSpot Server*.
- (3) For **Server IP Address**, enter the address of the central bintec HotSpot server, here e. g. *62.245.165.180*.
- (4) You will find the **RADIUS Secret** in your access data.
- (5) The **Default User Password** is the same as the **RADIUS Secret**.
- (6) Set the **Priority** to *0* (top priority).
- (7) Confirm with **OK**.
- (1) Go to **System Management -> Remote Authentication -> RADIUS ->New** to set up the second RADIUS server.

- (2) Select the **Authentication Type** *Login Authentication*.
- (3) For **Server IP Address**, enter the address of the central bintec HotSpot server, here e. g. *62.245.165.180*.
- (4) You will find the **RADIUS Secret** in your access data.
- (5) The **Default User Password** is the same as the **RADIUS Secret**.
- (6) Set the **Priority** to *0* (top priority).
- (7) In the **Advanced Settings** menu, choose *Non-authoritative* for **Policy**.
- (8) Confirm with **OK**.

The complete configuration looks like this:







RADIUS Parameter						
Authentication Type	Server IP Address	Policy	Priority	Enabled	Status	
Accounting	62.245.165.180	Authoritative	0	<input checked="" type="checkbox"/>	✓	 
Login Authentication	62.245.165.180	Authoritative	0	<input checked="" type="checkbox"/>	✓	 

Fig. 140: System Management -> Remote Authentication -> RADIUS

In the next step, a HotSpot network will be set up.

- (1) Go to **Local Services** -> **Hotspot Gateway** -> **Hotspot Gateway** -> **New**.

Basic Parameters

Interface LAN_EN1-0

Domain at the HotSpot Server
trainingfec_1.de

Walled Garden Enabled

Walled Network / Netmask Enabled
62.146.53.196 / 255.255.255.255

Walled Garden URL
http://www.bintec-elmeg.com

Terms & Conditions
http://www.bintec-elmeg.com

Additional freely accessible Domain Names

Domain Name / IP Address

ADD

Post Login URL

Language for login window English

Fig. 141: Local Services -> Hotspot Gateway -> Hotspot Gateway -> New

Proceed as follows:

- (1) Select the **Interface** `LAN_EN1-0`. This will later correspond with the **SSID** `Guests`.
- (2) Under **Domain at the HotSpot Server**, specify the domain that you were sent with

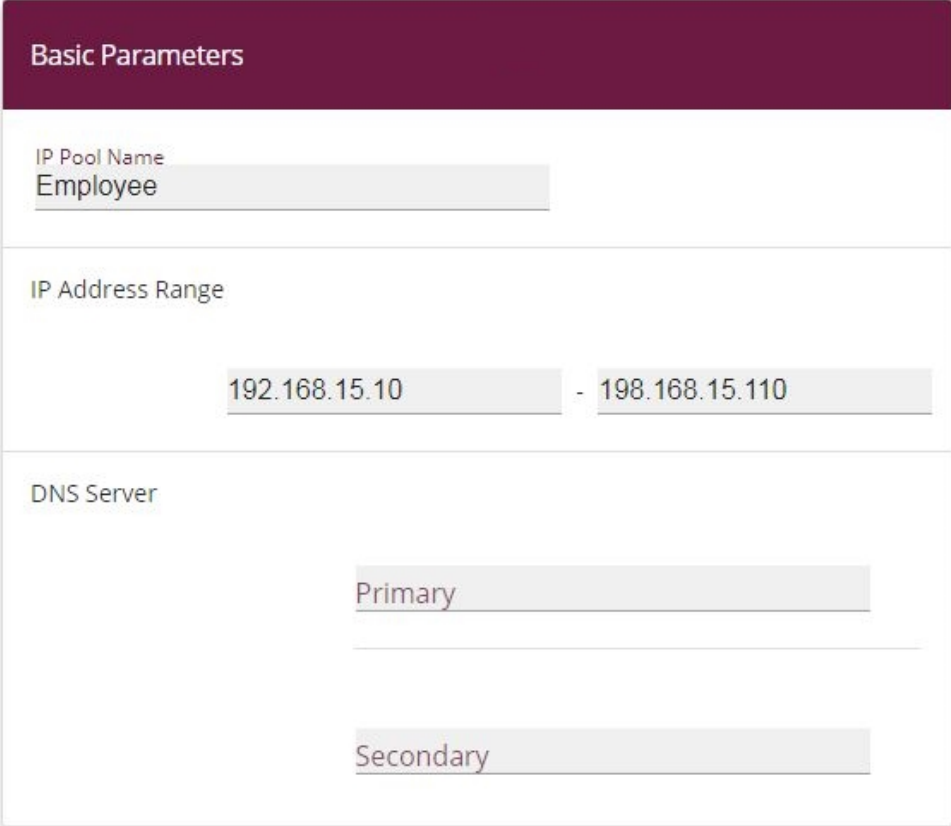
the access data, e. g. *trainingfec_1.de*.

- (3) Enable the **Walled Garden** option.
- (4) For **Walled Network / Netmask**, specify the IP address which your HotSpot guests are permitted to reach without login in, e. g. *62.146.53.196* and *255.255.255.255*.
- (5) Under **Walled Garden URL** specify the URL that your HotSpot guests are to be able to see without logging in, e. g. *http://www.bintec-elmeg.com*. The Walled Garden URL must be accessible under the Walled Network address.
- (6) Under **Terms & Conditions**, enter the URL at which you created your General Terms and Conditions website, e. g. *http://www.bintec-elmeg.com*. The URL must be accessible under the Walled Network address.
- (7) Confirm with **OK**.

7.3.4 DHCP configuration

Now the two DHCP pools are created for the virtual interfaces en1-0-1 (VLAN ID 15) and en1-0-2 (VLAN ID 16).

- (1) Go to **Local Services -> DHCP Server -> IP Pool Configuration -> New** to configure the IP pool.



The screenshot displays the 'Basic Parameters' section of a DHCP server configuration interface. It features three main input fields: 'IP Pool Name' with the value 'Employee', 'IP Address Range' with the value '192.168.15.10 - 198.168.15.110', and 'DNS Server' with two sub-fields, 'Primary' and 'Secondary', both currently empty.

Fig. 142: **Local Services -> DHCP Server -> IP Pool Configuration -> New**

Proceed as follows:

- (1) For **IP Pool Name**, enter any description to name the IP pool in a unique way, e. g. *Employee*.
- (2) For **IP Address Range**, enter the first (first field) and the last (second field) IP address in the IP address pool, e. g. *192.168.15.10 - 192.168.15.110*.
- (3) Confirm with **OK**.

In the **Local Services -> DHCP Server -> DHCP Configuration -> New** menu, you can perform additional configuration.

The screenshot shows a web form titled "Basic Parameters" for configuring a new DHCP pool. It contains three dropdown menus and one text input field:

- Interface:** en1-0-1
- IP Pool Name:** Employee
- Pool Usage:** Local
- description:** (empty text input field)

Fig. 143: **Local Services -> DHCP Server -> DHCP Configuration -> New**

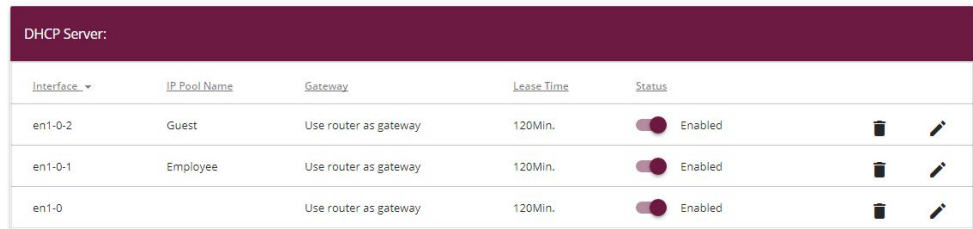
Proceed as follows:

- (1) Select the **Interface** *en1-0-1*.
- (2) Select a valid **IP-Pool Name**, here e. g. *Employee*.
- (3) For **Pool Usage**, select *Local*. The DHCP pool is only used for DHCP requests in the same subnet.
- (4) Confirm with **OK**.

Now create another DHCP pool for the second virtual interface en1-0-2 (VLAN ID 16).

- (1) Go to **Local Services -> DHCP Server -> IP Pool Configuration -> New**.
- (2) For **IP Pool Name**, enter e. g. *Guest*.
- (3) For **IP Address Range**, enter the IP address of the IP address pool, e. g. *192.168.16.10 - 192.168.16.110*.
- (4) Confirm with **OK**.
- (5) Go to **Local Services -> DHCP Server -> DHCP Configuration -> New**.
- (6) Select the **Interface** *en1-0-2*.
- (7) Select a valid **IP Pool Name**, here e. g. *Guest*.
- (8) For **Pool Usage**, select *Local*.
- (9) Confirm with **OK**.

The complete configuration looks like this:



The screenshot shows the DHCP Server configuration page. At the top, there is a dark red header with the text "DHCP Server:". Below this is a table with the following columns: "Interface" (with a dropdown arrow), "IP Pool Name", "Gateway", "Lease Time", and "Status". The "Status" column contains a toggle switch and the text "Enabled". To the right of each row are two icons: a trash can and a pencil.

Interface	IP Pool Name	Gateway	Lease Time	Status		
en1-0-2	Guest	Use router as gateway	120Min.	Enabled		
en1-0-1	Employee	Use router as gateway	120Min.	Enabled		
en1-0		Use router as gateway	120Min.	Enabled		

Fig. 144: Local Services -> DHCP Server -> DHCP Configuration

7.3.5 Wireless LAN controller wizard

By using the **wireless LAN controller**, you can set up and manage a WLAN infrastructure with multiple access points (APs). The WLAN controller has a Wizard which assists you in the configuration of your access points.

- (1) Go to **Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard**.

Basic Settings


Region Germany ▼

Interface LAN_EN1-4 ▼

DHCP Server DHCP Server with enabled CAPWAP option (138):
 External or static
 Internal

IP Address Range

192.168.100.10 - 192.168.100.110

 If you have already connected your Access Point to the WLAN Controller you have to Reset the Access Points now.


 The selected interface is not a bridge interface. The integrated WLAN module cannot be managed by the Wireless LAN Controller.

Fig. 145: **Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard**

Proceed as follows:

- (1) For **Region**, select *Germany*.
- (2) Select the **Interface** *LAN_EN1-0*.
- (3) For **DHCP Server**, select *Internal*.
- (4) Enter the **IP Address Range**, here *192.168.100.10 - 192.168.100.110*.
Now another DHCP pool is automatically created for the interface EN1-0. In doing this, it is taken into account that the IP address of the WLAN controller is sent as CAPWAP Option 138 for each DHCP request. The access points are told the address of the WLAN controller in this way.
- (5) Select **Next**.

In the second step, the wizard queries whether the WLAN network is to be run in the 2.4 or 5 GHz frequency range. If you WLAN network is to work in the 2.4 and the 5 GHz frequency range, select 2.4 GHz initially. Later on you can change the configuration of individual radio modules to 5 GHz.

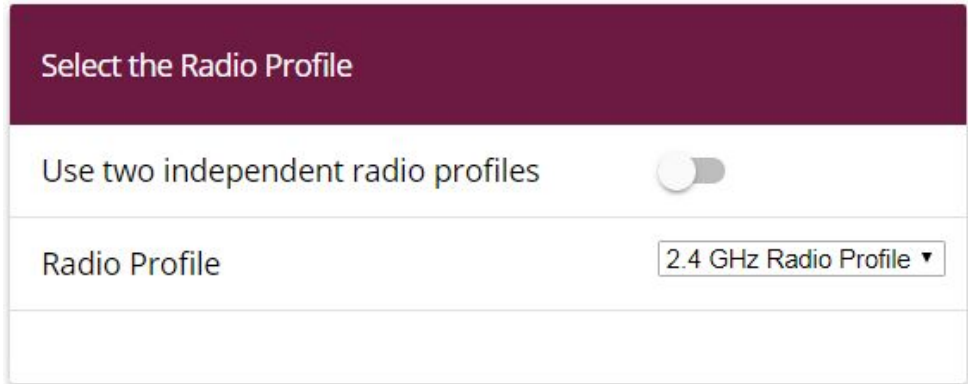


Fig. 146: **Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard**

Click **Next**.

In the next step you define the SSID which is to be supplied later.

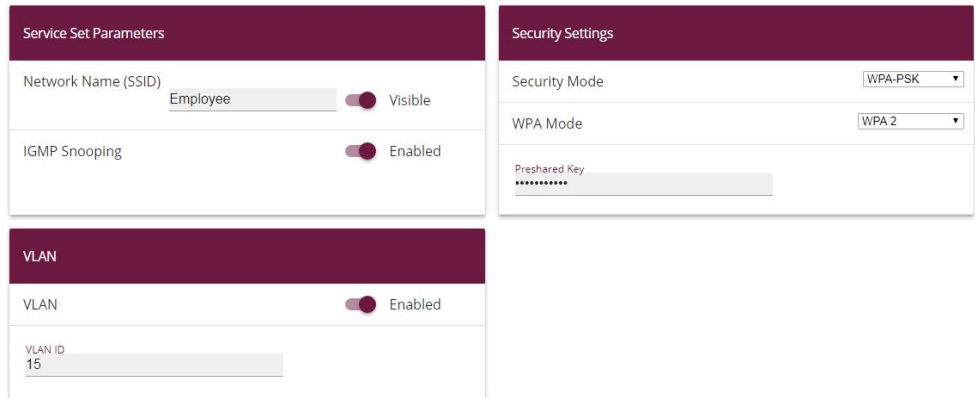


Fig. 147: **Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard**

Proceed as follows:

- (1) Click **Add**.
- (2) For **Network Name (SSID)**, enter *Employee*.
- (3) Set the **Security Mode** to *WPA-PSK*.

- (4) Set the **WPA Mode** set to *WPA 2*.
- (5) For Preshared Key, enter your defined password.
- (6) For **VLAN ID**, enter *15*.
- (7) Confirm with **OK**.

With these settings, all the traffic from WLAN clients which are connected via this SSID are routed to virtual interface en1-0-1.

Now define the second SSIDs which are to be supplied later.

The screenshot displays three configuration panels for a wireless LAN controller. The first panel, 'Service Set Parameters', includes a text input for 'Network Name (SSID)' containing 'Guest', a 'Visible' toggle switch that is turned on, and an 'IGMP Snooping' toggle switch that is also turned on. The second panel, 'VLAN', features a 'VLAN' toggle switch that is turned on and a 'VLAN ID' text input containing '16'. The third panel, 'Security Settings', shows a 'Security Mode' dropdown menu currently set to 'Inactive'.

Fig. 148: **Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard**

Proceed as follows:

- (1) Click **Add**.
- (2) For **Network Name (SSID)**, enter *Guest*.
- (3) Set **Security Mode** to *Inactive*.
- (4) For **VLAN ID**, enter *16*.
- (5) Confirm with **OK**.

With these settings, all the traffic from WLAN clients which are connected via this SSID are routed to virtual interface en1-0-2.

Note: Before you continue, ensure that all the access points that the WLAN controller is going to manage are switched on and connected via a switch to the router's en1-0 interface.

Click **Next**.

You now see a list of all the access points detected.

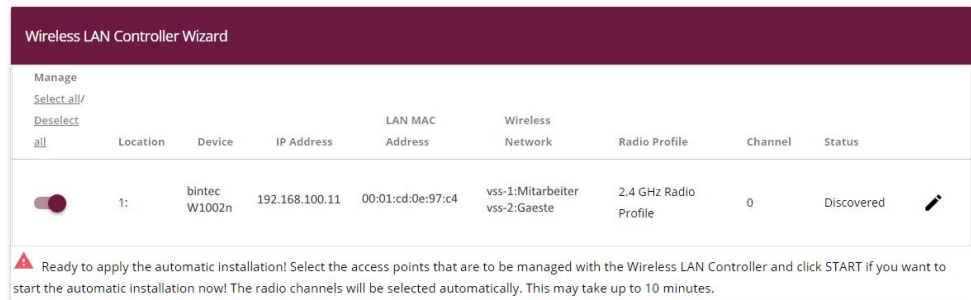



Fig. 149: Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard

If you wish to change the settings of a detected AP, click on  in the corresponding entry.

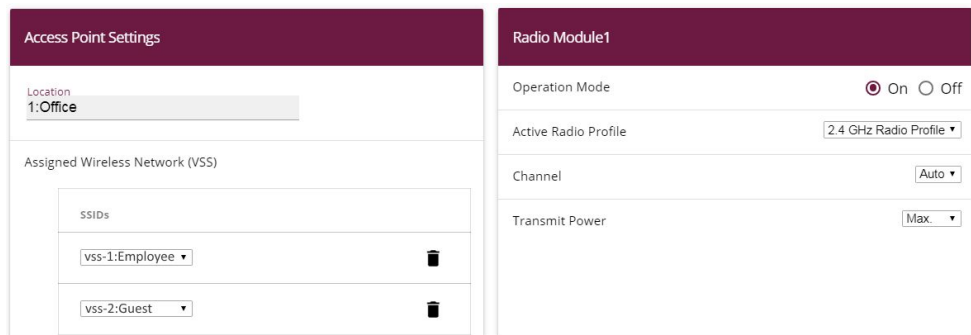


Fig. 150: Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard

Proceed as follows:

- (1) For **Location**, enter the installation location for the device, e. g. *1:Office*. This will make it easier for you to monitor the devices later on.
- (2) For **Assigned Wireless Network (VSS)** you are shown the wireless networks that are currently assigned, here e. g. *vss-1:Employee* and *vss-2:Guest*.
- (3) **Active Radio Profile** displays the wireless module profile that is currently selected, here *2.4 GHz Radio Profile*. You can select another wireless module profile from the list if more than one wireless module profile are being set up.
- (4) Confirm with **OK**.

Now select the access points that your WLAN controller is to manage. To do this, click the entries you want in the **Manage** column.

Click **Start** to begin configuring the access points. When the installation is complete, you will see a list of the **Managed** access points.


Wireless LAN Controller Wizard							
Location	Device	IP Address	LAN MAC Address	Wireless Network Profile	Radio Profile	Channel	Status
1:Office	bintec W1002n	192.168.100.11	00:01:cd:0e:97:c4	vss-1:Employee vss-2:Guest	2.4 GHz Radio Profile	11	 Managed

Fig. 151: **Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard**

To ensure your *Guests* can use the Internet but are not given access to your other network components, firewall rules need to be added. Here is an example of a simple firewall rule intended to prevent the *Guests* from accessing the internal network.

First of all, two new groups are created to ensure that defining the filter rules is easier to understand.

Proceed as follows:

- (1) Go to **Firewall -> Services -> Groups -> New**.

Basic Parameters

Description
Internet

Members

Service	Selection
activity	<input type="checkbox"/>
ah	<input type="checkbox"/>
any	<input type="checkbox"/>
apple-qt	<input type="checkbox"/>
auth	<input type="checkbox"/>

Fig. 152: **Firewall -> Services -> Groups -> New**

Proceed as follows:

- (1) Enter a **Description** of the service group, e. g. *Internet*.
- (2) Select the members of the group from the available service aliases. To do this, activate the field in the **Members** column.
- (3) Confirm with **OK**.

Proceed in the same way for the settings for the second group, e. g. *local services*.

The complete configuration now looks like this:

Groups		
Description	Members	
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	 

Fig. 153: Firewall -> Services -> Groups

In the last step, the local services are further restricted. Access to the *http* and *http (SSL)* services must be permitted so that the router can show the login page to the Hot-Spot guests.

- (1) Go to **Firewall -> Policies -> Filter Rules ->New**.

Basic Parameters	
Source	LEASED_EN1-0-1 ▼
Destination	LOCAL ▼
Service	local services ▼
Action	Access ▼

Fig. 154: Firewall -> Policies -> Filter Rules -> New

Proceed as follows to restrict the local services.

- (1) For **Source**, select e. g. *LEASED_EN1-0-1*.
- (2) For **Destination** select e. g. *LOCAL*.
- (3) Select the **Service**, e. g. *local services*.
- (4) For **Action**, select *Access*.
- (5) Confirm your entries with **OK**.

Proceed in the same way in making the settings for other services.

The complete configuration then looks like this, e. g.:

Order	Source	Destination	Service	Action	Policy active	Deny
1	LEASED_EN1-0-1	LOCAL	local services	Access	<input checked="" type="checkbox"/> Enabled	⌵ ⌵ ⌵ ⌵
2	LEASED_EN1-0-2	LOCAL	local services	Access	<input checked="" type="checkbox"/> Enabled	⌵ ⌵ ⌵ ⌵

Fig. 155: Firewall -> Policies -> Filter Rules

This concludes the configuration. Save the configuration with **Save configuration** and confirm the selection with **OK**.

You can now test the configuration. To do this, log in with the SSID of the *employees*, or with the SSID of the *guests*.





Note

For **WTP failure**, we recommend that you configure an email notification to monitor the system.

7.4 Overview of configuration steps

LAN configuration

Field	Menu	Value
IP Address / Netmask	LAN -> IP Configuration -> Interfaces -> <en1-0> 	e. g. <i>192.168.100.254</i>
Interface Mode	LAN -> IP Configuration -> Interfaces -> <en1-0> 	<i>Untagged:</i>
Based on Ethernet Interface	LAN -> IP Configuration -> Interfaces -> New	en1-0
IP Address / Netmask	LAN -> IP Configuration -> Interfaces -> New	e. g. <i>192.168.15.254</i>
Interface Mode	LAN -> IP Configuration -> Interfaces -> New	<i>Tagged (VLAN)</i>
VLAN ID	LAN -> IP Configuration -> Interfaces -> New	<i>15</i>
Based on Ethernet Interface	LAN -> IP Configuration -> Interfaces -> New	en1-0
IP Address / Netmask	LAN -> IP Configuration -> Interfaces -> New	e. g. <i>192.168.16.254</i>
Interface Mode	LAN -> IP Configuration -> Interfaces -> New	<i>Tagged (VLAN)</i>
VLAN ID	LAN -> IP Configuration -> Interfaces -> New	<i>16</i>

Hotspot configuration

Field	Menu	Value
Authentication Type	System Management -> Remote Authentication -> RADIUS -> New	<i>Accounting</i>
Vendor Mode	System Management -> Remote Authentication -> RADIUS -> New	<i>bintec HotSpot Server</i>
Server IP Address	System Management -> Remote Authentication -> RADIUS -> New	e. g. <i>62.245.165.180</i>
RADIUS Secret	System Management -> Remote Authentication -> RADIUS -> New	e. g. <i>supersecret</i>
Default User Password	System Management -> Remote Authentication -> RADIUS -> New	e. g. <i>supersecret</i>

Field	Menu	Value
Priority	System Management -> Remote Authentication -> RADIUS -> New	0
Authentication Type	System Management -> Remote Authentication -> RADIUS -> New	Login Authentica-tion
Server IP Address	System Management -> Remote Authentication -> RADIUS -> New	e. g. 62.245.165.180
RADIUS Secret	System Management -> Remote Authentication -> RADIUS -> New	e. g. <i>supersecret</i>
Default User Password	System Management -> Remote Authentication -> RADIUS -> New	e. g. <i>supersecret</i>
Priority	System Management -> Remote Authentication -> RADIUS -> New	0

Set up Hotspot network

Field	Menu	Value
Interface	Local Services -> Hotspot Gateway -> Hotspot Gateway -> New	e. g. LAN_EN1-0
Domain at the HotSpot Server	Local Services -> Hotspot Gateway -> Hotspot Gateway -> New	e. g. <i>training-fec_1.de</i>
Walled Garden	Local Services -> Hotspot Gateway -> Hotspot Gateway -> New	<i>Enabled</i>
Walled Network / Net-mask	Local Services -> Hotspot Gateway -> Hotspot Gateway -> New	e. g. 62.146.53.196 and 255.255.255.255
Walled Garden URL	Local Services -> Hotspot Gateway -> Hotspot Gateway -> New	<i>ht-tp://www.bintec-elmeg.com</i>
Terms & Conditions	Local Services -> Hotspot Gateway -> Hotspot Gateway -> New	<i>ht-tp://www.bintec-elmeg.com</i>
Language for login window	Local Services -> Hotspot Gateway -> Hotspot Gateway -> New	e. g. <i>German</i>

DHCP configuration

Field	Menu	Value
IP Pool Name	Local Services -> DHCP Server -> IP Pool Configuration -> New	e. g. <i>Assistant</i>
IP Address Range	Local Services -> DHCP Server -> IP Pool Configuration -> New	e. g. 192.168.15.10 - 192.168.15.110

Field	Menu	Value
Interface	Local Services -> DHCP Server -> DHCP Configuration -> New	<i>en1-0-1</i>
IP Pool Name	Local Services -> DHCP Server -> DHCP Configuration -> New	e. g. <i>Assistant</i>
Pool Usage	Local Services -> DHCP Server -> DHCP Configuration -> New	<i>Local</i>
IP Pool Name	Local Services -> DHCP Server -> IP Pool Configuration -> New	e. g. <i>Guests</i>
IP Address Range	Local Services -> DHCP Server -> IP Pool Configuration -> New	e. g. <i>192.168.16.10 - 192.168.16.110</i>
Interface	Local Services -> DHCP Server -> DHCP Configuration -> New	<i>en1-0-2</i>
IP Pool Name	Local Services -> DHCP Server -> DHCP Configuration -> New	e. g. <i>Guests</i>
Pool Usage	Local Services -> DHCP Server -> DHCP Configuration -> New	<i>Local</i>

WLAN Controller Wizard

Field	Menu	Value
Region	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard.	<i>Germany</i>
Interface	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard.	<i>LAN_EN1-0</i>
DHCP Server	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard.	<i>Internal</i>
IP Address Range	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard.	e. g. <i>192.168.100.10 - 192.168.100.110</i>
Radio profile	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard ->Next	<i>2.4 GHz Radio Profile</i>
Network Name (SSID)	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard ->Next	e. g. <i>Employees</i>
Security Mode	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard ->Next	<i>WPA-PSK</i>
WPA Mode	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard	<i>WPA2</i>

Field	Menu	Value
	->Next	
Preshared key	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard ->Next	e. g. <i>supersecret</i>
VLAN	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard ->Next	<i>Enabled</i>
VLAN ID	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard ->Next	15
Network Name (SSID)	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard -> Next-> Add	e. g. <i>Guests</i>
Security Mode	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard -> Next-> Add	Inactive
VLAN	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard -> Next-> Add	<i>Enabled</i>
VLAN ID	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard -> Next-> Add	16
Location	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard ->Next 	e. g. <i>1:Office</i>
Active Radio Profile	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard ->Next 	<i>2.4 GHz Radio Profile</i>
Assigned Wireless Networks (VSS)	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard -> Next 	e. g. <i>vss-1:Employees</i> and <i>vss-2:Guests</i>

Add firewall rules

Field	Menu	Value
Description	Firewall -> Services -> Groups -> New	e. g. <i>Internet</i>
Members	Firewall -> Services -> Groups -> New	e. g. <i>http, http (SSL)</i>

Field	Menu	Value
Description	Firewall -> Services -> Groups -> New	e. g. <i>Local Services</i>
Members	Firewall -> Services -> Groups -> New	e. g. <i>http, http (SSL)</i>

Restrict local services

Field	Menu	Value
Source	Firewall -> Policies -> Filter Rules -> New	<i>LEASED_EN1-0-1</i>
Destination	Firewall -> Policies -> Filter Rules -> New	<i>LOCAL</i>
Service	Firewall -> Policies -> Filter Rules -> New	<i>local services</i>
Action	Firewall -> Policies -> Filter Rules -> New	<i>Access</i>
Source	Firewall -> Policies -> Filter Rules -> New	<i>LEASED_EN1-0-2</i>
Destination	Firewall -> Policies -> Filter Rules -> New	<i>LOCAL</i>
Service	Firewall -> Policies -> Filter Rules -> New	<i>local services</i>
Action	Firewall -> Policies -> Filter Rules -> New	<i>Access</i>
Source	Firewall -> Policies -> Filter Rules -> New	<i>LAN_EN1-0-1</i>
Destination	Firewall -> Policies -> Filter Rules -> New	<i>LAN_EN1-0-1</i>
Service	Firewall -> Policies -> Filter Rules -> New	<i>any</i>
Action	Firewall -> Policies -> Filter Rules -> New	<i>Deny</i>
Source	Firewall -> Policies -> Filter Rules -> New	<i>LAN_EN1-0-2</i>
Destination	Firewall -> Policies -> Filter Rules -> New	<i>LAN_EN1-0-2</i>
Service	Firewall -> Policies -> Filter Rules -> New	<i>any</i>

Field	Menu	Value
Action	Firewall -> Policies -> Filter Rules -> New	<i>Deny</i>

Chapter 8 WLAN - Cloud NetManager

8.1 Introduction

The Cloud NetManager is a system that is able to administer both small as well as very large networks that are distributed over many locations.

Requirements

The following prerequisites for configuration must be met:

- registers users on the Cloud NetManager portal
- one or several bintec WLAN Access Points e.g., **W1001n**, **W1003n**, **W2003n**, ... with SW Rel. 10.1.8.Patch 2 or higher
- DVC (Device Verification Code) of the access points to be administered or a DHCP server that supports option 43
- a valid Cloud NetManager licence for each access point
- Internet access

8.2 First steps in the portal

8.2.1 Creating a user

Open a browser and enter the URL into the address line: <https://bintec.networkcloudmanager.com>.

First, you must register. To do so, on the registration page click on **Register** on the top right.

Enter the required data for the registration.

The **Partner number** and **Login** fields are optional.

If you have more than one user account for your company, please observe the following:

- Only one user can be created per company name. Therefore, the form of the company must vary (e.g., Company_1; Company_2; ...).
- If another user is to administer the same WLAN network, do not create any other users.

You can set up other users for your account after the login with both full as well as restricted user rights.

- If you would like to set up an additional user who is not to see the settings of the first user already set up, you can do so at this point.

Online registration

Company

Company name	<input type="text" value="Company_1"/>	Street	<input type="text" value="Suedwestpark 94"/>
Zip code	<input type="text" value="90449"/>	City	<input type="text" value="Nuremberg"/>
		Country	<input type="text" value="Germany"/>
Partner number (bintec elmeg)			
<input type="text"/>			

User account

First name	<input type="text" value="John"/>	Last name	<input type="text" value="Smith"/>	Phone	<input type="text" value="091196731234"/>
Email address			Login (the default is your email address)		
<input type="text" value="j-smith@company.com"/>			<input type="text"/>		

Declaration of consent relating to data usage

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](#).

Accept declaration of consent relating to data usage

When you register, you will be sent a link for setting a password to the above email account. Once you have done this, you will have completed your registration.

Fig. 156: Online registration

Once the registration form has been submitted, you will receive an email after a few minutes.

Follow the instructions and create a **Password** for your user.

8.2.2 Changing the time zone

The time zone when logging in for the first time is set to **UTC**. Please change this to **Europe/Berlin**.

Furthermore, you have the option of selecting a language.

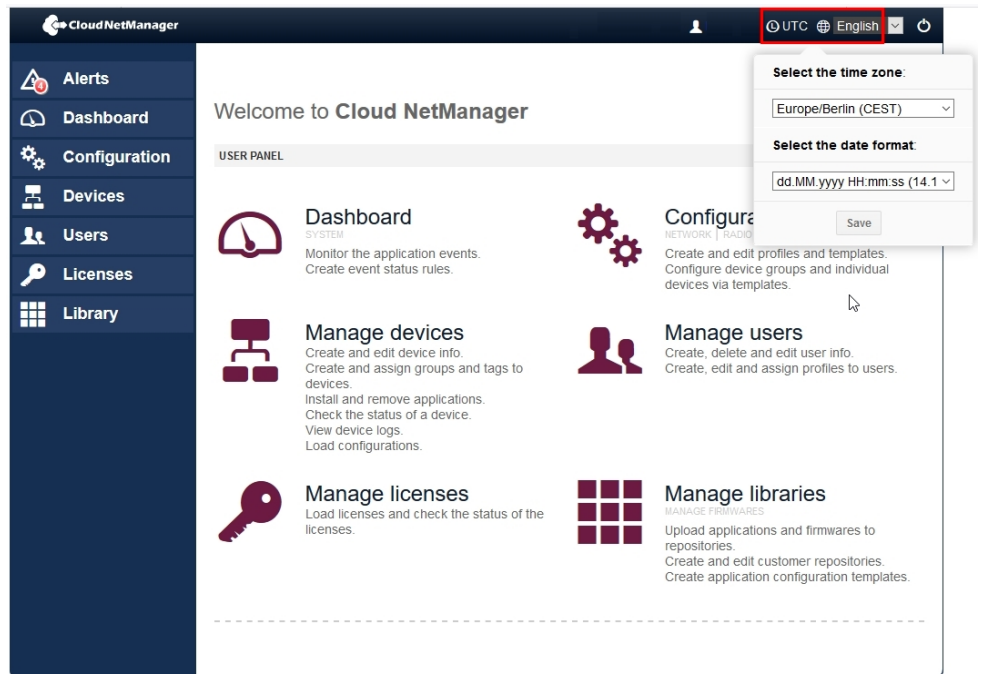


Fig. 157: Changing the time zone

8.2.3 Importing the licences

On the status page go to the **Licences->Licences for this cloud server->New Licence** menu.

The screenshot shows the 'Licenses / Register license' page. The left sidebar contains navigation options: Alerts, Dashboard, Configuration, Devices, Users, and Licenses. The main content area has a breadcrumb 'Licenses / Register license' and two tabs: 'Licenses for this cloud server' (selected) and 'Licenses for local servers'. Below the tabs is a 'New license' form with a blue informational box stating: 'Please contact to your sales representative in order to obtain a valid license. If you already have a serial number and a license validation code, just enter the data in the following form. A license can be used only once on a single customer environment. NOTE: System will automatically detect if your new license is a cloud or a local license.' The form includes two input fields: 'Serial number:' with a sub-note 'Serial number of the license. This is a unique code and it can be used once.' and 'License code:' with a sub-note 'Enter the license code with the validation number'. At the bottom are 'Register license' and 'Cancel' buttons.

Fig. 158: New licence

- Enter the **Serial number** and the **Licence code** (PIN).
- Press **Register Licence**.

The **Manage Licences** overview shows which licences are still available in your account.

The screenshot shows the 'Licenses / Register license' page with the 'Manage licenses' tab selected. The left sidebar is the same as in Fig. 158. The main content area shows a table with the following data:

Type	Validity	Available	Status
Managed devices	365 days	1 of 10	Valid license

The 'Valid license' status is highlighted with a red box. Below the table, it shows 'Page 1 of 1' and 'Results by page: 10'.

Fig. 159: Overview

Please note that only the installed licences will be displayed. The availability does not indicate the remaining time but the runtime of the purchased licence or licences packet.

- A licence which was registered on a user account cannot be subsequently transmitted to another user.
- The licence runtime is only counted down here if the licence for the management of a device was used. If the used device is removed, the licence will be available for other devices. The runtime is not counted down if the licence is not being used.
- If the licence for an administered device expires, the system will obtain another licence from the pool of registered licences. If no free licences are available, the device in ques-

tion will no longer be managed. The configuration cannot be changed and monitoring is no longer possible. The device itself will continue to work even in the event of a power failure.

You can display the licences which are to be used by an administered device. To do so, under **Status** click on **Valid Licence**.

Assign date	Serial Num.	Name
2015-02-25 16:37:16	RNEDDH014430001	AUTO_RNEDDH014430001
2015-05-13 23:02:21	757/00120	DISCV_757/00120
2015-05-26 09:55:50	777/000329	DISCV_777/000329
2015-06-11 14:56:26	757/00120	DISCV_757/00120
2015-06-15 11:10:33	RNFDEI014280016	
2015-06-16 12:04:45	RNFDEI014110186	Nils W2003n
2015-06-16 14:03:04	757/00120	DISCV_757/00120
2015-06-16 15:52:01	757/00120	DISCV_757/00120
2015-06-16 15:54:18	757/00120	DISCV_757/00120

Fig. 160: Devices that are associated with the licence

8.3 Creation of profiles

8.3.1 Creation of network profiles (SSID)

At least one network profile (SSID) must be created.

To do so, go to the **Configuration->Network** menu.

Click on **New Network Profile**.

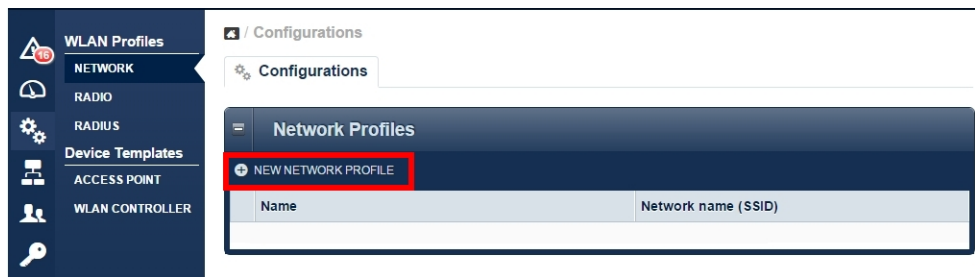


Fig. 161: Network profiles

New network profile Additional features

Profile name

SERVICE SET PARAMETERS

Network name (SSID)

Hidden

Client isolation

ARP processing

WMM

SECURITY SETTINGS

Security mode

CLIENT LOAD BALANCING

Maximum number of clients - Hard limit

Maximum number of clients - Soft limit

Client band select

ACCESS CONTROL

ACL Mode

BLACKLISTING

Dynamic blacklisting

Failed attempts

Failed attempts time window

Blacklist duration

VLAN

Enable

BANDWIDTH LIMITATION FOR EACH WLAN CLIENT

Rx shaping

TX shaping

Fig. 162: Configuring network profiles

The important parameters for the respective SSID are predefined. The parameters are identical to the default configuration of the bintec access points or the WLAN Controllers.

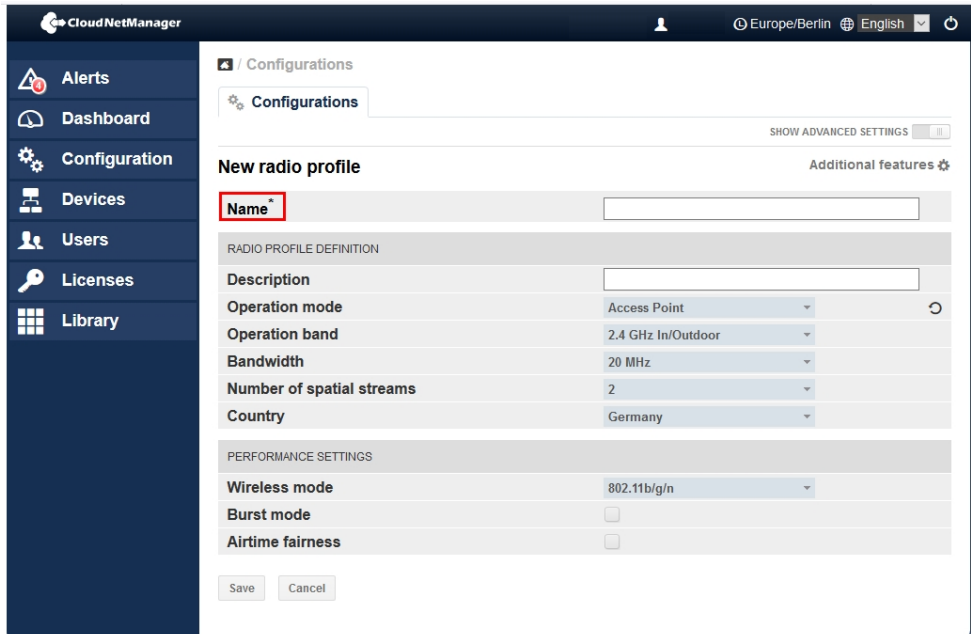
- In **Profile name** enter the name of the WLAN network profile..
- The **Network Name (SSID)** is the name of the WLAN network that is viewed by the users of the access points.
- Click on **Save** to confirm your details.

8.3.2 Creation of radio profiles

At least one radio profile must be created.

If access points with two radio modules are to be administered, a radio profile must be created for 2.4 GHz and 5 GHz. The parameters are identical to the default configuration of the bintec access points or the WLAN Controllers.

Go to the **Configuration->Radio ->New radio profile** menu.



The screenshot displays the CloudNetManager web interface. On the left is a dark blue navigation sidebar with menu items: Alerts, Dashboard, Configuration, Devices, Users, Licenses, and Library. The main content area is titled 'Configurations' and shows a 'New radio profile' form. The form has a 'Name' field with a red box around it. Below this is a 'RADIO PROFILE DEFINITION' section with fields for Description, Operation mode (set to 'Access Point'), Operation band (set to '2.4 GHz In/Outdoor'), Bandwidth (set to '20 MHz'), Number of spatial streams (set to '2'), and Country (set to 'Germany'). A 'PERFORMANCE SETTINGS' section follows, with 'Wireless mode' set to '802.11b/g/n', and 'Burst mode' and 'Airtime fairness' checkboxes. 'Save' and 'Cancel' buttons are at the bottom.

Fig. 163: New radio profile

Proceed as follows:

- Enter a **Name** for the radio profile.
- Set **Operation mode** to *Access Point*.

- Select the 20 MHz **Bandwidth** for **Operation band** = 2.4 GHz.
- Select the 20 MHz or 40 MHz **Bandwidth** for **Operation band** = 5 GHz.
- Set the **Wireless mode** for 2.4 GHz profile to 802.11b/g/n.
- Set the **Wireless mode** for 5 GHz profile to 802.11ac/a/n.
- Confirm your details by clicking on **Save**.

8.3.3 Creation of device templates / access point template

At least one device template must be defined.

Go to the **Configuration->Access Point->New Access point template** menu.

The screenshot displays the 'New access point template' configuration page in the NetManager interface. The left sidebar contains navigation options: WLAN Profiles, NETWORK, RADIO, RADIUS, ANALYTICS, DHCP, HOTSPOT, Device templates, and ACCESS POINT. The main content area is titled 'Configurations' and shows the 'New access point template' form. The form includes the following fields and settings:

- Template name***: Standard_AP
- Template description**: Standard_AP
- SETTINGS** section:
 - Location**: anywhere
 - Administration password***: [masked]
 - LED mode**: normal
 - Radius Server Profile**: None
- RADIO MODULE 1** section:
 - Radio profile**: 2.4 Standard Radio
 - Channel**: auto
 - TX Power**: Max
 - Network profile**: None
- RADIO MODULE 2** section:
 - Radio profile**: 5 Standard Radio
 - Channel**: auto
 - TX Power**: Max
 - Network profile**: None

At the bottom of the form, there are 'Save' and 'Cancel' buttons.

Fig. 164: Device template

Proceed as follows:

- For **Template name** please enter a template name.
- Enter the **Administration password**.
- The **Administration password** is the password to locally login to an access point. In

comparison to bintec WLAN Controller, here it is possible to log into one access point locally. However, all WLAN parts relevant for configuration cannot not be locally configured.

- If, in the case of SSID configuration, you select the security mode *WPA Enterprise*, you must define a **Radius Server Profile**.
- It is important for a 2.4 GHz to be associated with radio module 1 and a 5 GHz radio profile to be associated with radio module 2.
- Confirm your details by clicking on **Save**.

8.3.4 Administer devices

In the **Devices** menu, a list of all registered device is displayed. First, you must create a **Group**.

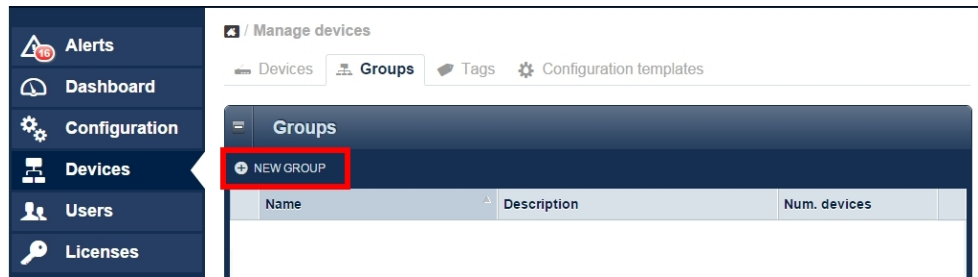


Fig. 165: Administer devices

Go to the **Devices->Groups->New Group** menu.



Fig. 166: Administer devices/group

- Select the previously defined **Configuration template**.
- Activate the **Automatic update**. In doing so, the configuration change becomes effective immediately. Furthermore, newly registered access points are automatically put into operation with this default group immediately.

- Confirm your details by clicking on **New group**.

8.4 Register and administer access points

To add a new device, go to the **Devices->Managed Devices->Add Devices** menu.

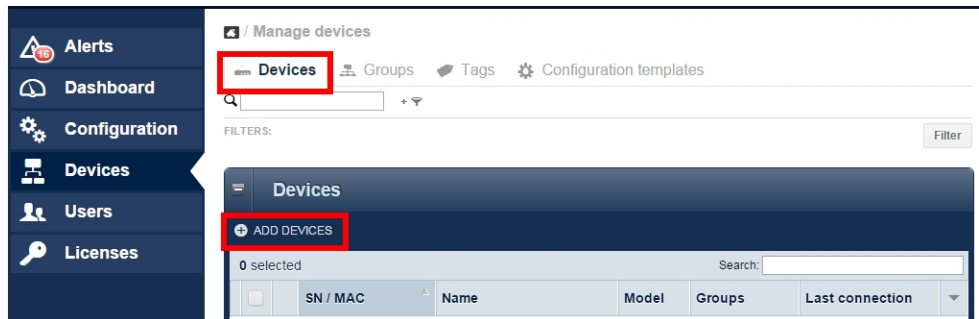


Fig. 167: Register and administer access points

8.4.1 Manually register devices

For manual registration, go to the **Devices->Add Devices->Manual registration** menu.

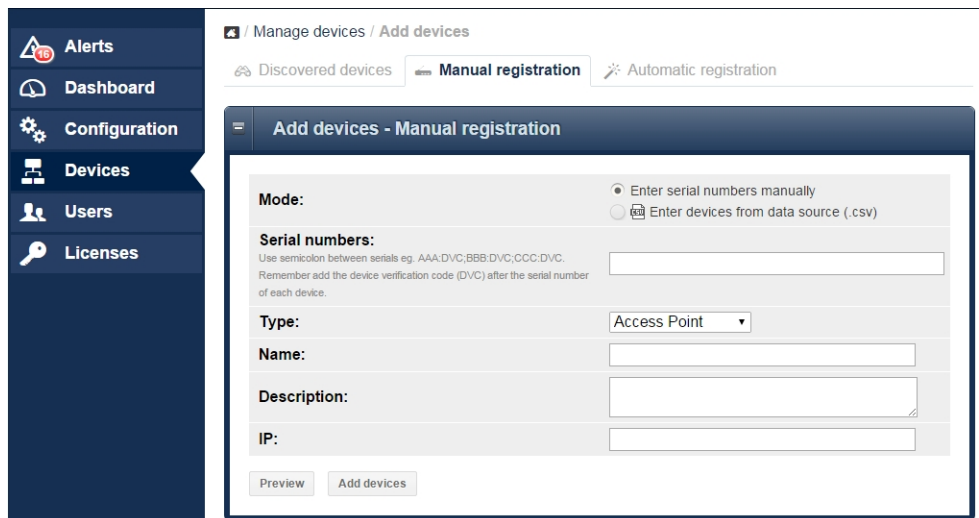


Fig. 168: Manual registration

Proceed as follows:

8.5 Device administration

In the **Devices** menu, registered devices are displayed.

Fig. 170: Display devices

By clicking on the line of the device in the overview, a detailed view is displayed.

Using **Edit** you can edit the **Details**. Click on **Health** or **Advanced** to display these options.

Fig. 171: Detailed view

8.5.1 Batch operations and software update

Further device administration options are available in the device view. If you mark several devices in the device view, there is, for example, the option of starting **Batch Operations** to update the **Firmware** of the marked devices.

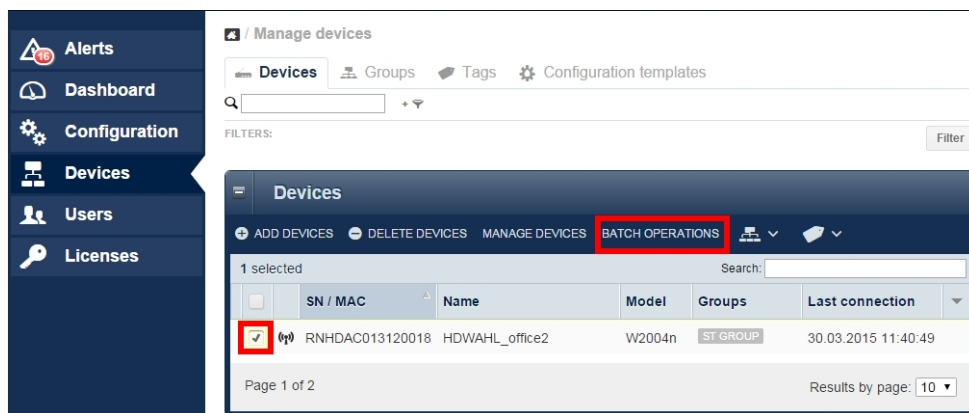


Fig. 172: Batch operations

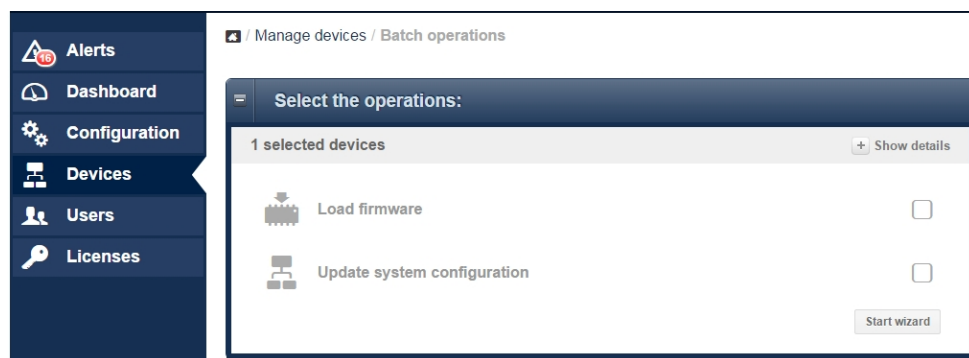


Fig. 173: Select operations

8.6 Appendix

8.6.1 Establishing another data centre

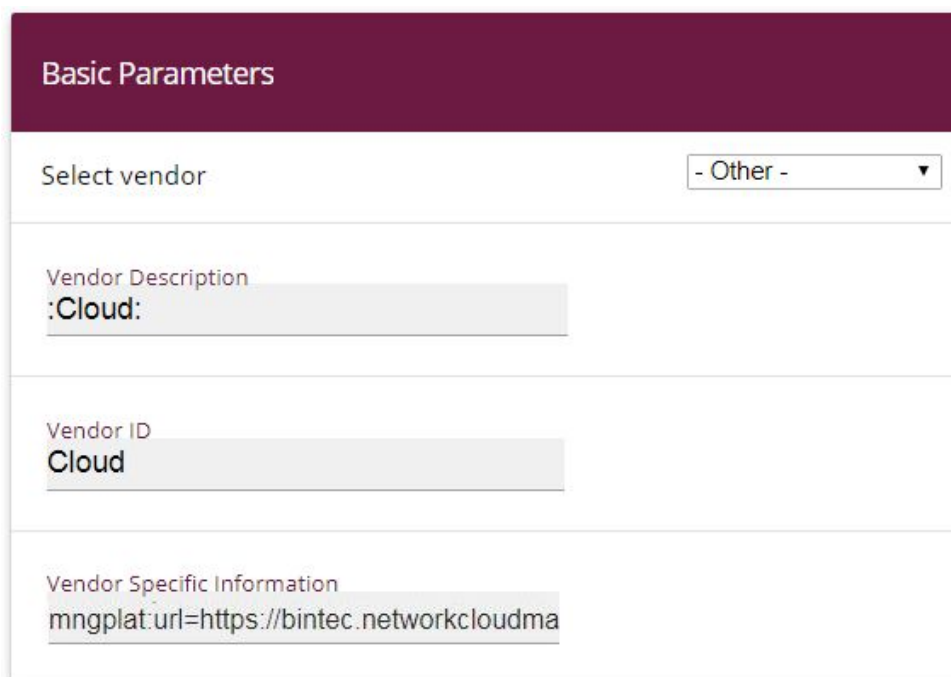
If you do not want to use our Cloud NetManager as an SAAS (Software as a Service), but want to host the virtual Cloud NetManager in your own data centre, you must assign the access points to another Cloud NetManager URL. You have two options.

8.6.1.1 URL allocation via DHCP Option 43

You can assign the access points to another Cloud NetManager URL. You must configure **Option 43** (vendor specific option) on the local DHCP server.

If you are using the DHCP server of a **bintec** router, proceed as follows:

Enter **GUI** (Graphical User Interface) in the **Local Services->DHCP Server->DHCP Configuration** menu.




The screenshot displays the 'Basic Parameters' section of a DHCP configuration interface. It features a dark purple header with the text 'Basic Parameters'. Below the header, there are three main sections:

- Select vendor:** A dropdown menu currently showing '- Other -'.
- Vendor Description:** A text input field containing ':Cloud:'.
- Vendor ID:** A text input field containing 'Cloud'.

Below these fields is a section titled 'Vendor Specific Information' with a text input field containing 'mngplat.url=https://bintec.networkcloudma'.

Fig. 174: Local Services -> DHCP Server -> DHCP Configuration

- Choose the  icon to edit an existing entry.
- Go to **Advanced Settings**.
- In the **Vendor Specific Information (DHCP Option 43)** field, click on the **Add Vendor**

String button.

- Under **Select vendor**, choose *-Other-*.
- Under **Vendor Description**, enter the name of the manufacturer, e.g. *:Cloud:*.
- To identify the device, enter the **Vendor ID**, e.g. *Cloud*.
- Under **Vendor Specific Information**, enter the new Cloud NetManager URL. If you want to submit a user ID, please read the string from the Cloud NetManager (see [Automatically register device](#) on page 209).
- Click **Apply**.

8.6.1.2 Direct URL change in the GUI

Using the **GUI** of the Access Point, you can enter other Cloud NetManager addresses.

Optionally, the user ID of the account in question can be transferred. In this case, the device is automatically registered and configured with the default configurations.

In the **System Management** menu, go to **Global Settings** -> **System**.

Basic Settings

System Name
w2003n-ext

Location

Contact
BINTECELMEG

Maximum Number of Syslog Entries
50

Maximum Message Level of Syslog Entries Information ▼

Maximum Number of Accounting Log Entries
20

NetManager communication Enabled

NetManager address
https://discover.networkcloudmanager.com

LED mode Status ▼

Manual WLAN Controller IP Address

Show Manufacturer Names Enabled

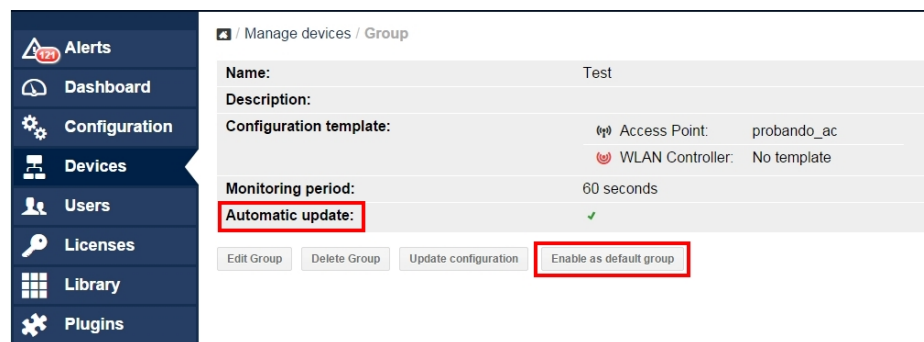


Fig. 177: Devices->Groups

8.7 Error search

8.7.1 A new device is not visible

There are a number of reasons why a device is not displayed in the device overview although the correct DVC was entered.

- The device is locally administered by a WLAN Controller. Please reset the device to the ex works state and delete the **WLAN Controller** DHCP option in the local DHCP server.
- The local firewall blocked port 443 for outgoing connections.

8.7.2 No more communication with an administered device

The logo that displays the communication state is no longer green but red.

The screenshot shows the 'Device management' page for an access point named 'RNFDEI014120010 - AUTO_RNFDEI014120010'. The left sidebar contains navigation options: Alerts, Dashboard, Configuration, Devices, Users, and Licenses. The main content area has tabs for 'Info', 'Configuration', 'Jobs', 'Log', and 'Alerts'. The 'Info' tab is active, displaying a device icon and the following details:

Device Model:	W2003n
System version:	V.9.1 Rev. 14 (Beta 5) IPsec
License:	access_point

On the right, there are tabs for 'Details', 'Health', and 'Advanced'. The 'Details' tab is active, showing the following information:

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

An 'Edit' button is located at the bottom of the details panel. In the top right corner, a red box highlights an 'Alerts' icon with a red exclamation mark and the text 'LAST CONTACT 6D 15H 41M 45S AGO'.

Fig. 178: Communication error

First, it must be ensured that the access point has an Internet connection. If the problem persists, the cause may be an incorrect SSL certificate. This can have different causes, e.g., it may have been deleted on the access point or the device may have been registered to another account.

In this case, the device configuration must be reset to the ex works state and the security certificate on the server must be deleted from the access point in question.

The screenshot shows the same 'Device management' page, but now the 'Advanced' tab is active. The 'Certificate' section shows 'Present' and a red box highlights the 'Remove security data' button. Below this, the 'Advanced operations' section contains icons for refresh, search, and delete. At the bottom, the 'Last contact' is '31.07.2015 18:28:44' and the 'License validity' is 'Valid license (Remaining days: 229)'.

Fig. 179: Communication error

8.7.3 Further debug options

In the **Devices->Manage devices** menu, select a device. Go to **Manage devices->Configuration**.

Alerts
Dashboard
Configuration
Devices
Users
Licenses

/ Manage devices

Devices Groups Tags Configuration templates

FILTERS: Filter

Devices

ADD DEVICES DELETE DEVICES **MANAGE DEVICES** BATCH OPERATIONS

2 selected Search:

	SN / MAC	Name	Model	Groups	Last connection
<input checked="" type="checkbox"/>	RNHDAC013120018	HDWAHL_office2	W2004n	ST GROUP	30.03.2015 11:40:49

Page 1 of 1 Results by page: 10

Fig. 180: Communication error

Click on the small logo to display the configuration file.

Alerts
Dashboard
Configuration
Devices
Users
Licenses

/ Device management

Test

Info Configuration Jobs Log Alerts

SHOW ADVANCED SETTINGS

✓ Configuration updated on device

Settings

Location anywhere

Administrative password

LED mode normal

Radius Server Profile

Radio module 1

Fig. 181: Debug options

Make sure that all passwords in this file are encrypted.

The screenshot shows the Cloud NetManager interface. On the left is a dark blue sidebar with navigation options: Alerts, Dashboard, Configuration, Devices, Users, and Licenses. The main area is titled 'Device management' and has a 'Test' button. Below the title are tabs for 'Info', 'Configuration', 'Jobs', 'Log', and 'Alerts'. A green notification bar at the top of the main area says 'Configuration updated on device'. Below this, a message indicates the last change was on 18.06.2015 at 12:05:27. The XML configuration content is displayed in a code editor with line numbers 1 through 27. The XML includes settings for a WLAN interface, such as description, version, enable status, interface name, admin password, LED mode, scan results, AP settings, MAC address, name, location, encryption, radius profile, and radio profile details.

Fig. 182: Debug message

8.7.4 Debugging at device level

Correct timestamps

Access points need a correct time setting in order to transmit and allocate performance values. Therefore, check the time setting before starting error diagnostics.

A DHCP server can be used as time server too. If you use a **bintec** device for this, go to the **System Management->Global Settings->Time and Date** menu and activate the **Internal Time Server** item.

Using static IP addresses you can enter manually up to three time servers in the same menu.

Debugging

If there is no communication between the access point and Cloud NetManager, you can track communications using Telnet or the SSH terminal. You must log into the access point and enter the command "debug trempl". No communication between the access point and Cloud NetManager is displayed.

```
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%
```

In this way, communication problems and certification problems can be analysed quickly.