



Manual Workshops (Excerpt)

WLAN Workshops

Copyright© Version 01/2020 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	Introduction
1.2	Configuration
1.2.1	Configuring the wireless networks
1.2.2	Configuring VLANs
1.2.3	Defining rules for receiving at the ports
1.2.4	Removing ports from VLAN management
1.2.5	Enable VLAN
1.2.6	Configuration on bintec S128p
1.3	Result
1.4	Checking the connection
1.5	Overview of configuration steps
Chapter 2	WLAN - bintec Hotspot Solution
2.1	Introduction
2.2	Performance features
2.2.1	Hotspot solution features
2.2.2	Gateway features
2.2.3	Hotspot server features
2.3	Configuration
2.3.1	Configuration of the bintec Hotspot gateway
2.3.2	Configuration of the bintec Hotspot server by the dealer
2.3.3	Administration of Hotspot accounts
2.3.4	Operation at several locations
2.4	Configuring login methods
2.4.1	Anonymous login
2.4.2	1-Click

2.4.3	SMS
2.4.4	PayPal
2.4.5	Default Free Service
2.5	Instructions for safe operation
2.5.1	Multiple login
2.5.2	Preventing mutual visibility of extensions
2.5.3	Encrypted/unencrypted WLAN connection
2.5.4	WPA Encryption
2.5.5	IP/ARP Spoofing
2.6	Overview of configuration steps
Chapter 3	WLAN - 802.1x authentication using a Microsoft Server 2008
3.1	Introduction
3.2	Server configuration.
3.2.1	Configuration of active directory certificate services
3.2.2	Reservation of access point IP addresses at DHCP server (Windows Server 2008) 76
3.2.3	Installation of network policy and access services (NPS/RADIUS server). 78
3.2.4	Configuration of network policy and access services (NPS/RADIUS server) 80
3.3	RADIUS configuration of the access point
3.4	WLAN configuration of the access point
3.5	Connection of a Windows 7 WLAN client.
3.5.1	Importing the certification from the certification authority (CA certificate) $.$ 88
3.5.2	Configuration of the Windows 7 WLAN client
3.6	Overview of Configuration Steps
Chapter 4	WLAN - Bintec WLAN Controller Introduction 101
4.1	Functional overview

4.2	Project planning
4.2.1	Determining customer requirements
4.2.2	Recommended hardware installation on site
4.3	System requirements
4.3.1	WLAN Controller hardware
4.3.2	Access Point hardware
4.3.3	WLAN Controller software licences
4.4	Network configuration
4.4.1	WLAN Controller device network settings
4.4.2	DHCP server
4.5	WLAN rollout with the WLAN controller wizard
4.5.1	Wizard Step 1
4.5.2	Wizard Step 2
4.5.3	Wizard Step 3
4.5.4	Wizard Step 4
4.5.5	Start WLAN rollout to access points
4.6	Appendix
4.6.1	E-mail alert in case of access point failure
4.6.2	Configuration of a DHCP server on another Bintec router
4.6.3	Configuration of a DHCP server on Windows Server 2003/2008 114
4.6.4	Configuration of a DHCP server under Linux
4.6.5	Operation of APs with static IP address settings
4.7	Overview of configuration steps
Chapter 5	WLAN - VoWLAN Basics and Configuration 125
5.1	General
5.2	WLAN infrastructure
5.2.1	WLAN radio illumination
5.2.2	Handover between the access points
5.2.3	Bandwidth requirement

5.2.4	The safety standard and the handover
5.2.5	QoS, WMM and U-APSD
5.2.6	WLAN controllers – A must in a VoWLAN network?
5.2.7	Potential sources of interference
5.3	Example configuration
5.3.1	Network plan
5.3.2	WLAN configuration with or without WLAN controller
5.4	Ascom i62 Talker configuration
5.4.1	Requirements
5.4.2	Configuration
5.4.3	Test commands on the Ascom i62
5.5	Configuring the elmeg hybird 300
5.5.1	Configuration
5.5.2	Operational scenario: WLAN telephone cannot be accessed 142
5.6	Use other WLAN telephones
5.7	Overview of Configuration Steps
5.7	
Chapter 6	WLAN Management for Multiple Locations: WLAN controller via
-	
-	WLAN Management for Multiple Locations: WLAN controller via
Chapter 6	WLAN Management for Multiple Locations: WLAN controller via VPN
Chapter 6 6.1	WLAN Management for Multiple Locations: WLAN controller via VPN 147 Introduction 147
Chapter 6 6.1 6.1.1	WLAN Management for Multiple Locations: WLAN controller via VPN
Chapter 6 6.1 6.1.1 6.1.2	WLAN Management for Multiple Locations: WLAN controller via VPN 147 Introduction 147 Requirements 148 About the test setup. 148
Chapter 6 6.1 6.1.1 6.1.2 6.2	WLAN Management for Multiple Locations: WLAN controller via VPN
Chapter 6 6.1 6.1.1 6.1.2 6.2 6.2.1	WLAN Management for Multiple Locations: WLAN controller via VPN 147 Introduction 147 Requirements 148 About the test setup. 148 Configuration. 149 Presettings 149
Chapter 6 6.1 6.1.1 6.1.2 6.2 6.2.1 6.2.2	WLAN Management for Multiple Locations: WLAN controller via VPN 147 Introduction 147 Requirements 148 About the test setup. 148 Configuration. 149 Presettings 149 Configure the router in the field office 149

Chapter 7 WLAN - Wireless LAN Controller as Network Access Gateway

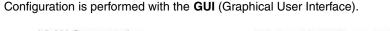
7.1	Introduction
7.2	Configuration
7.3	Overview of Configuration Steps
Chapter 8	WLAN network with guest WLAN
8.1	Introduction
8.2	Configuration
8.2.1	Configuring the IP address
8.2.2	Create bridge groups and assign LAN interface
8.2.3	Put Wireless LAN Controller into operation
8.2.4	Choose radio profile and configure WLAN access to the local network 216
8.2.5	Configure guest WLAN
8.2.6	Configure Access Points with the Wireless LAN Controller
8.2.7	Configure the IP address for the virtual Bridge Interface
8.2.8	Configure the IP Address Range for the guest network
8.2.9	Configure DHCP use
8.2.10	Set up firewall
8.3	Result
8.4	Overview of Configuration Steps
Chapter 9	WLAN - WLAN controller installation with integrated HotSpot functionality
9.1	Introduction
9.2	Function
9.3	Configuration
9.3.1	Basic configuration
9.3.2	LAN configuration

9.3.3	HotSpot configuration
9.3.4	DHCP configuration
9.3.5	Wireless LAN controller wizard
9.4	Overview of configuration steps
Chapter 10	WLAN - Cloud NetManager
10.1	Introduction
10.2	First steps in the portal
10.2.1	Creating a user
10.2.2	Changing the time zone
10.2.3	Importing the licences
10.3	Creation of profiles
10.3.1	Creation of network profiles (SSID)
10.3.2	Creation of radio profiles
10.3.3	Creation of device templates / access point template
10.3.4	Administer devices
10.4	Register and administer access points
10.4.1	Manually register devices
10.4.2	Automatically register device
10.5	Device administration
10.5.1	Batch operations and software update
10.6	Appendix
10.6.1	Establishing another data centre
10.6.2	Automatic configuration
10.7	Error search
10.7.1	A new device is not visible
10.7.2	No more communication with an administered device
10.7.3	Further debug options
10.7.4	Debugging at device level

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*.



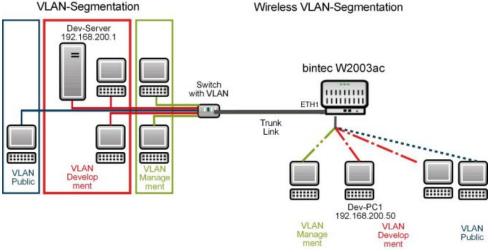


Fig. 1: VLAN segmenting

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 \checkmark icon next to the existing entry.

Wireless Settings		Performance Settings	
Operation Mode	Access-Point / Bridge Link Master 🔻	Wireless Mode	802.11b/g/n 🔻
Operation Band	2.4 GHz In/Outdoor •	Number of Spatial Streams	2 •
Channel	11 •	Airtime fairness	Enabled
Transmit Power	Max. •		

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.

Service Set Paramete	rs		Security Settings	
Network Name (SSID)	Management	Visible	Security Mode	WPA-PSK •
	Management	Visible	WPA Mode	WPA and WPA 2
Intra-cell Repeating		Enabled	WPA Cipher	○ AES ○ TKIP
U-APSD		Enabled	WPA2 Cipher	O AES AES and TKI
			Preshared Key	

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).

VSS						
Description	Network Name (SSID)	MAC Address	Security	Status	Action	
vss7-10	Management	Elmegt_6f:5e:85	WPA-PSK		~ ~	/

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

Proceed as follows:

(1) In the currently only list entry click the \mathbf{A} 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.

Confi	igure VLAN		
VLAN 2	ldentifier		
VLAN Deve	Name Plopment		
VLAN	Members		
	Interface vss2-1 v	Egress Rule Untagged ▼	Delete
	en1-0 ▼	Tagged •	T
	ADD		

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

- (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):

nterface	PVID	Drop untagged frames	Drop non-members
n1-0	1 - Management 🔻		
en1-1	1 - Management V		
ss2-0	1 - Management V		
ss2-1	2 - Development T		
rss2-2	3 - Public 🔻		

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

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

- (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> -> ...

Conf	igure VLAN		
VLAN	I Identifier		1
	Name agement		
VLAN	l Members		
	Interface	Egress Rule	Delete
	en1-0 v	Untagged v	
	en1-1 ▼	Untagged v	
	vss2-0▼	Untagged V	

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

- (1) Click the \blacksquare icon for Interface vss2-1.
- (2) Click the \blacksquare 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.

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



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.

Bridge Group br0 VLAN Options		
Enable VLAN	Enabled	

Fig. 9: LAN -> VLAN -> Administration

- (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**.

em				
		VLAN Operation Mode : 802.1Q		
ocol		Enable GVRP Protocol		
AN		Management Vlan ID : 1		
ГР			F	
MP			Apply	
S AP				
ling				
rity		802.10 0	onfiguration Group Config	ouration
er over Ethernet		Port Link 1	Type Untagged Vid Tag	
ory Default		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		
ory Denaute				gea via
em Reboot		Port.01 💌 Acces		ged vid
Control Management of the Control of Control			ss Link 1	gea via
Control Management of the Control of Control				gea via
Control Management of the Control of Control	Port		ss Link 1	Tagged Vid
Control Management of the Control of Control	Port Port.01	Port.01 🗾 Acces	ss Link 1 Apply	
Control Management of the Control of Control		Port.01 SAcces	Apply Untagged Vid	
Control Management of the Control of Control	Port.01	Port.01 🗾 Acces	Apply Untagged Vid	
Control Management of the Control of Control	Port.01 Port.02	Port.01 🗾 Acces Link Type Access Link Access Link	Apply Untagged Vid 1 1	
Control Management of the Control of Control	Port.01 Port.02 Port.03	Port.01 🗾 Acces Link Type Access Link Access Link Access Link	Apply Untagged Vid 1 1 1	
Control Management of the Control of Control	Port.01 Port.02 Port.03 Port.04	Port.01 T Acces Link Type Access Link Access Link Access Link Access Link	Apply Untagged Vid 1 1 1 1 1	
Control Management of the Control of Control	Port.01 Port.02 Port.03 Port.04 Port.05	Port.01 🗾 Acces Link Type Access Link Access Link Access Link Access Link Access Link	Apply Untagged Vid 1 1 1 1 1 1 1 1 1 1	
Control Management of the Control of Control	Port.01 Port.02 Port.03 Port.04 Port.05 Port.06	Port.01 🗾 Acces Link Type Access Link Access Link Access Link Access Link Access Link Access Link	Apply Untagged Vid	
Control Management of the Control of Control	Port.01 Port.02 Port.03 Port.04 Port.05 Port.06 Port.07	Port.01 🗾 Acces Link Type Access Link Access Link Access Link Access Link Access Link Access Link Access Link Access Link	Ss Link 1 Apply Untagged Vid 1 1 1 1 1 1 1 1 1 1 1 1 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 was 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:

		VL	AN Configura	tion
System		and the second	ann ann anna - ann ann an Arlanda Chaile an Arlanda	
Port		VLAN O	peration Mode : 802.1Q	•
Protocol		[Enal	ble GVRP Protocol	
VLAN			ement Vlan ID : 1	
RSTP		manage		
SNMP			Apply	
QoS				
IGMP				
X-Ring		902 10	Configuration Group Con	nfiguration
Security		002.10	configuration droup con	Ingulation
Power over Ethernet		Port Link	Type Untagged Vid T	agod Vid
Factory Default		The second se		
Factory Default System Reboot		Port.01 💌 Acce		-33
And a second sec		The second se	ess Link 🔟 📔	
And the second se		The second se		
The second s	Port	The second se	ess Link 🔟 📔	Tagged Vid
Manufacture of the second s	Port Port.01	Port.01 🔟 Acce	Apply	
And a second sec		Port.01 💌 Acce	Apply Untagged Vid	
And a second sec	Port.01	Port.01 V Acce	Apply Untagged Vid	
And the second se	Port.01 Port.02	Port.01 1 Acce Link Type Access Link Access Link	Apply Untagged Vid 1 102	
	Port.01 Port.02 Port.03	Port.01 1 Acces Link Type Access Link Access Link Access Link	Apply Untagged Vid 1 102 103	
	Port.01 Port.02 Port.03 Port.04	Port.01 1 Acce Link Type Access Link Access Link Access Link Access Link	Link ▼ 1 Apply Untagged Vid 1 102 103 1	
And a second sec	Port.01 Port.02 Port.03 Port.04 Port.05	Port.01 1 Acces Link Type Access Link Access Link Access Link Access Link Access Link	Link ▼ 1 Apply Untagged Vid 1 102 103 1 1 1	
The second s	Port.01 Port.02 Port.03 Port.04 Port.05 Port.06	Port.01 1 Acces Link Type Access Link Access Link Access Link Access Link Access Link Access Link	Link ▼ 1 Apply Untagged Vid 1 102 103 1 1 1 1 1	
The second se	Port.01 Port.02 Port.03 Port.04 Port.05 Port.06 Port.07	Port.01 1 Acces Link Type Access Link Access Link Access Link Access Link Access Link Access Link Access Link	Link ▼ 1 Apply Untagged Vid 1 102 103 1 1 1 1 1 1 1	Tagged Vid

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<1ms TTL=30 Antwort von 192.168.100.30: Bytes=32 Zeit<1ms TTL=30 Antwort von 192.168.100.30: Bytes=32 Zeit<1ms TTL=30 Antwort von 192.168.100.30: Bytes=32 Zeit<1ms TTL=30
<pre>Ping-Statistik für 192.168.100.30: Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust), C:\></pre>

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<1ms TTL=63
Ping-Statistik für 192.168.200.1:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = Oms, Maximum = Oms, Mittelwert = Oms
```

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

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

Configuring VLANs

Defining the Port VLAN Identifier (PVID)

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

Removing ports from VLAN management

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

Field	Menu	Value
	<management></management>	and vss2-2
Enabling VLANs		
Field	Menu	Value
Enable VLAN	LAN -> VLAN -> Adminis tration	S- Enabled

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.

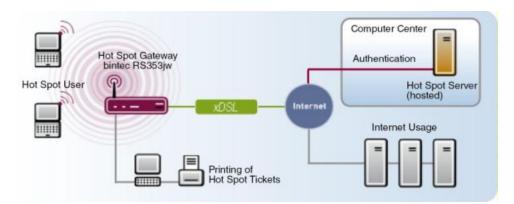


Fig. 12: Method of operation

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.

Currently Install	ed Software	Software and Configurat	ion Options
BOSS	V.10.2.6.100 IPv6, IPSec, PBX from 2019/04/18 00:00:00	Action	Update system software ~
System Logic	1.9	Source Location	Current Software from Update Server $ \lor $
VDSL Logic	5.7.4.12.0.2		

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 V
Domain at the HotSpot Server	
Walled Garden	Disabled
Post Login URL	
Language for login window	English V

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				Manual Time Settings			
Time Zone	Europ	oe/Berlin	~	Set Date	Day	Month	Year
Current Local Time	Wednesday, 20	19 May 29, 1	3:57:31	Set Time		Hour	Minute
Automatic Time Settings (Time Protocol)						
First Timeserver	<u></u>	SNTP	~				
Second Timeserver							
	5	SNTP	~				
Third Timeserver	5	SNTP	~				
Time Update Interval	1440	M	linute(s)				
Time Update Policy		Endles	ss v				
Internal Time Server	0	Ð					

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:

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

Service Set Parameters	
Network Name (SSID)	
default	Visible
Intra-cell Repeating	
U-APSD	Enabled
IGMP Snooping	Enabled

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) -> ...

Service Set Pa	rameters		
Network Name	(SSID)		
	default	-	Visible
Intra-cell Repea	ting		
U-APSD		-	Enabled

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	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		Milliseconds
Alive Check		•• E	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.

- (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.

Login		
User name: Password:		
Login		

Fig. 20: Login

Proceed as follows to edit the client profile:

(1) Go to Client -> Overview.

General	
Identifier Street Zip code City Country	Roadshow Südwestpark 94 90449 Nürnberg DE
Contact person	
First name Last name Telephone Fax E-Mail Language	English
Access Identifier	Ligion
Domain Additional text Additional text English	
Bill part	Show
Passwords	 Only figures Only chars O alphanumeric Safe passwords
Password length	9 🗸
General Voucher Password Logo (maximum 5MB, only jpeg or png)	
Logo (maximum sind, only jpeg of phg)	
Terms and conditions	Current File Delete Browse No file selected. Current File Delete

Fig. 21: Client-> Edit Client

Proceed as follows:

 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 overvie
Access Identifier	
*User name Password Password repeat	Hotel_Reception
Authorisation group	(Will generate automatically if no one is insert) Assistant All
Assistant data	
First name *Last name Telephone Fax	Reception
*E-Mail	test@test.de
Language	 English German Spanish Frensh Italian Portuguese Dutch Submit cancel * is required
	> User overvie

Fig. 22: User -> New assistant

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

- (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.

New tariff	> Tariff overview <
*Identifier	10 Minutes Ticket
Runtime Time unit (runtime) Capacity (<= 2000) Time unit (capacity)	IMPORTANT: Changes on time/volume restrictions will affect existing accounts. Reactivated accounts may have to be reactivated again. 10 Minutes ~ Total ~ MB Total ~
Price Valid until Location	1,00 € > > All > Submit cancel * is required
	> Tariff overview <

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.

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**-> **Over-view**-> **<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 **Hot-spot 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).

New Account (easy)	Account - Search <	> New Account (extended) <	> help <
*User name	Guest_25		
*Tariff	2h Ticket 🔻		
*Last name	Lüdenscheid		
data sheet	download		
	Submit cancel		
	* is required		
	> Account - Search <	> New Account (extended) <	→ help <

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 (exten	nded)
Access Identifier	
*User name	Guest_26
Password	
Password repeat	
	(Will generate automatically if no one is insert)
*Tariff	2h Ticket 🔹
Valid from	25 V Jun V 2019 V
Valid until	24 🔻 Jun 🔻 2020 🔻
*Location	Bintec-Elmeg-Support / Nr. 1
	Roadshow
	Support NCR
	WBT
Groups	available member
	Familienticket
	Test-dauer >>
	test1
0.070	
SSID	
Template	use this account as template
Personal data	
Title	Mr. 🔻
First name	Hans-Hubert
*Last name	Lüdenscheid
Room	214
Addition	
E-Mail	
Telephone	
data sheet	🗆 in English
	🗹 download
	send per SMS
	Submit cancel
	* 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 use-

ful, 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.

A	ccount - Sear	ch			> Ne	w Account (e	extended) < > New /	Account (ea	asy) < → he	lp <
				Account State User name Last name	active	¥				
				Tariff Groups Online	All All search	7	JC.			
	User name	Location	Name	Tariff	Amount	Time left	Capacity remains	Online		
-	<u>10min-1</u>	SE-Test	10min-1	10MB/10Min	Payed	00:10:00	10 MB	No	🤓 🖾 🖀 (
4	<u>se-team</u>	SE-Test	SE-Team	unbegrenzt	<u>0.00 €</u>	::		No	🤓 🖾 😫 (0
					> Ne	w Account (e	extended) < > New /	Account (ea	asy) < → he	lp «

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 *RadiusNasld* 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.

	ocation overview			> Upload Manager <	> help ·
1	Bintec-Elmeg-Support / Nr. 1	Nürnberg	DEM020420150107	2020-01-07	<u>Overview</u>
1	Roadshow	Nürnberg	DEM057020141107	2020-11-07	<u>Overview</u>
1	SE-Test	DEU	DEM057220151209	2020-12-09	<u>Overview</u>
1	Support NCR	DEU	DEM020520141021	2020-10-21	<u>Overview</u>
1	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.

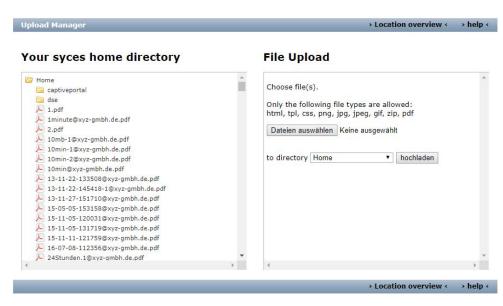


Fig. 28: Upload Manager

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 Street Zip code	Support NCR
City Country Remark	DEU Germany
Contact person	
First name Last name Telephone Fax E-Mail	Saland Tanada eduard:tanadir@imilec.etmes_com
Walled Garden	Report Bhilton altrong com//1//3892/1
Registration type Tariff	Default Free service ▼ 24-Stunden ▼
Tickets Password	☐ have to be unlocked manuel. Auto generate and display ▼
License	
License number Valid until	DEMO20520110629 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
	NAS-Identifier		
<u>nureintest</u>	nureintest		
		> New host <	> Location overview <

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.

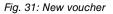
If no NAS identifier is displayed, you can set it under **New host**.

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	> V	oucher - Search «
*Quantity	100	
User name	O Consecutively (370:1, 370:2)	
	O Numeric (4798811)	
	• Alphanumeric small (a7z89vk)	
	Alphanumeric (A7z89vK)	
Prefix to Username		
Password		
Password repeat		
	(Will generate automatically if no one is ins	ert)
Tariff	2h Ticket	
Valid from	T T	
Valid until	23 V Jun V 2020 V	
Description		
*Location	available selected	
Location	Bintec-Elmeg-Support A	
	Roadshow	
	Support NCR	
	WBT SE-Test	2
	Submit cancel	
	* is required	
		/oucher - Search <



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>.

Registration type	Anonymous login 🔹
Tariff	5 Tage 🔹
Prevent second registration for	Minutes V
Account validity	365 Days from first login 🔻
Router Type	bintec > 9.1.4 T
URL of login page	http://192.168.1.254/auth
Tickets	have to be unlocked manuel.
Password	Auto generate and display <
Layout	Default gray ▼
Token Based Access	Accept Terms and Conditions first V

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
 .

Interface		BRIDGE_BR0 -
Domain at the HotSpot Server		
Walled Garden		Enabled
Walled Network / Netmask	Disab	led
Walled Garden URL		
https://hotspot.bintec-elmeg.com/3/205		
	L	
https://hotspot.bintec-elmeg.com/3/205		
https://hotspot.bintec-elmeg.com/3/205 Terms & Conditions https://www.bintec-elmeg.com		
https://hotspot.bintec-elmeg.com/3/205 Terms & Conditions https://www.bintec-elmeg.com Additional freely accessible Domain Names		

Advanced Settings

Advanced Parameter	
Ticket Type	Username/Password ~
Allowed HotSpot Client	All ~
Devices per ticket 1	
Login Frameset	
Pop-Up window for status indication	
Default Idle Timeout	Enabled
	600 Seconds

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
Hot Spot Anmelden Eenutzername " Passwort " Ich akzeptiere die AGB • • Anmelden • wird benötigt
Kostenloses Internet Kostenloser Tarif für 10 Hin Bitte registrieren Sie sich mit Ihrer eMail Adresse.
E-Mail * Ich skzeptiere die ASE
Registieren "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.

Registration type	1-Click	
Tariff	5 Tage	T
Prevent second registration for		Minutes T
Account validity	365	Days from first login 🔻
Router Type	bintec	> 9.1.4 ▼
URL of login page	http://19	92.168.1.254/auth
Autologin		
Tickets	🗆 hav	e to be unlocked manuel.
Password	Auto generate and display 🔻	
Layout	Default gray T	
Token Based Access	Accept Terms and Conditions first V	

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
 .

Interface		BRIDGE_BR0 -
Domain at the HotSpot Server		
Walled Garden		Enabled
Walled Network / Netmask	Disab	led
Walled Garden URL		
https://hotspot.bintec-elmeg.com/3/205		
	L	
https://hotspot.bintec-elmeg.com/3/205		
https://hotspot.bintec-elmeg.com/3/205 Terms & Conditions https://www.bintec-elmeg.com		
https://hotspot.bintec-elmeg.com/3/205 Terms & Conditions https://www.bintec-elmeg.com Additional freely accessible Domain Names		

Advanced Settings

Advanced Parameter	
Ticket Type	Username/Password ~
Allowed HotSpot Client	All ~
Devices per ticket 1	
Login Frameset	
Pop-Up window for status indication	
Default Idle Timeout	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.



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 on *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 Provider	lox24
Account-ID	
Password	
API/Service-ID Economy	
API/Service-ID Pro	
API/Service-ID Direct	
Route Germany	Economy *
Route world wide	Economy V
Route world wide	

Fig. 41: Client -> <Edit Client>

Proceed as follows:

(1) Under SMS Credentials select SMS Provider 10x24.

- 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>.

legistration type	SMS	T		
	5 Days	•		
iff				
eview SMS	DE EN FR IT ES NL PT			
event second registration for		Minutes T		
count validity	365	Days from first login ▼		
uter Type	bintec > 9.1.4 ▼			
L of login page	http://192.168.1.254/auth			
kets	🗌 have	e to be unlocked manuel.		
sword	Auto generate and display 🔻			
out	Default gray ▼			
ken Based Access	Accept	Accept Terms and Conditions first V		

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
Domain at the HotSpot Server	
Walled Garden	Enabled
Walled Network / Netmask	Disabled
Walled Garden URL https://hotspot.bintec-elmeg.com/3/205	L.
Terms & Conditions https://www.bintec-elmeg.com	
Additional freely accessible Domain Names	
Domain Name / IP Address	
ADD	
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	
Pop-Up window for status indication	
Default Idle Timeout	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.



Fig. 45: PayPal login

Users select a **Tariff**, e. g. 10 Minute Ticket $(1.00 \in)$ 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 (optiona	al)	
API Username		ians-statier want jaget statiat de
API Password	۲	
API Password repeat	۲	
Signature		HAT AND STREET AND MINING STREET STATE

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>.

Registration type	Paid service	
Tariff	All 🔻	
Prevent second registration for		Minutes T
Account validity	365	Days from first login ▼
Router Type	bintec > 9.1.4 ▼	
URL of login page	http://192.168.1.254/auth	
Tickets	🗌 har	ve to be unlocked manuel.
Password	Auto generate and display ▼	
Layout	Default gray ▼	
Token Based Access	Accept Terms and Conditions first V	

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 P	arameters	
Interfac	e	BRIDGE_BR0 -1
Domai	in at the HotSpot Server	
Walled (Garden	Enabled
Walled I	Network / Netmask	Disabled
	Sarden URL hotspot.bintec-elmeg.com/3/205	
	Conditions www.bintec-elmeg.com	
Addition	nal freely accessible Domain Names	
	Domain Name / IP Address	
	www.paypal.com	I I
	api.paypal.com	Ť.
	api-aa-3t.paypal.com	i
	notify paypal.com	•
	www.paypalobjects.com	Ť
	ADD	
Post Lo	ogin URL	
Languag	ge for login window	English

Advanced Settings

Advanced Parameter	
Ticket Type	Username/Password $\!$
Allowed HotSpot Client	All ~
Devices per ticket 1	
Login Frameset	
Pop-Up window for status indication	
Default Idle Timeout	Enabled
	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.

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.

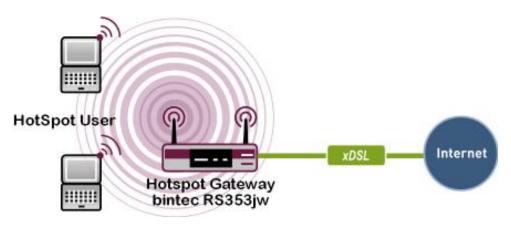


Fig. 50: Hotspot with a single WLAN access point

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.

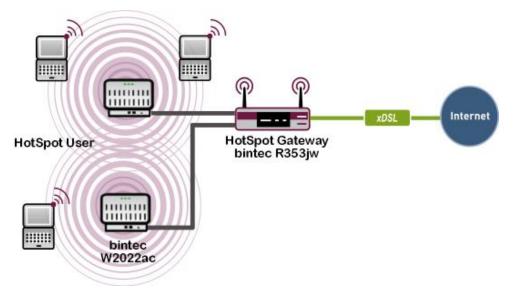


Fig. 51: Hotspot with multiple WLAN access points

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.

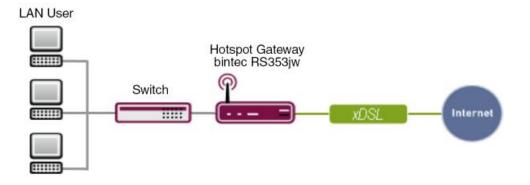


Fig. 52: Hotspot with Ethernet LAN client

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 & Config- uration -> Options	Update system software
Source	Maintenance -> Software & Config- uration -> 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 Set- tings -> Date and Time	Europe/Berlin
ISDN Timeserver	System Management -> Global Set- tings -> Date and Time	Disabled
Internal Time Server	System Management -> Global Set- tings -> 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	Accounting
Vendor Mode	System Management -> Remote Authentication -> RADIUS -> New	bintec HotSpot Server
Server IP Address	System Management -> Remote Authentication -> RADIUS -> New	e.g. 62.245.165.180
RADIUS Secret	System Management -> Remote Authentication -> RADIUS -> New	funkwerk-ec
Priority	System Management -> Remote Authentication -> RADIUS -> New	2
Policy	System Management -> Remote Authentication -> RADIUS -> New->Advanced Settings	<i>Non-authoritative</i>
Server Timeout	System Management -> Remote Authentication -> RADIUS -> New->Advanced Settings	3000
Retries	System Management -> Remote Authentication -> RADIUS -> New->Advanced Settings	3

Configure RADIUS Server access 2

Field	Menu	Value
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	funkwerk-ec

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. Hotel_Reception
Authorisation group	User -> New assistant	Assistant
Location	User -> New assistant	All
Last name	User -> New assistant	e.g. Reception
E-Mail	User -> New assistant	e.g. test@test.de

Create rates

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

Creation of an account (easy)

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

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=""></edit>	Anonymuous login
Tariff	Location -> <edit location=""></edit>	e.g. 5 Days
URL of login page	Location -> <edit location=""></edit>	ht- tp://192.168.1.254 /auth
Walled Garden	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 ->	Enabled
Walled Garden URL	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 ->	e.g. ht- tps://www.hotspot. bintec-el- meg.com/3/205/
Terms & Conditions	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 ->	e.g. ht- tp://www.hotspot.b intec-elmeg.com
Login Frameset	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 -> ->Advanced Settings	Disabled
Pop-Up window for status indication	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 -> Settings	Disabled

1-Click

Field	Menu	Value
Walled Garden	Location -> Overview-> <edit loca-<br="">tion></edit>	URL is displayed
Туре	Location -> Overview-> <edit loca-<br="">tion></edit>	1-Click
Tariff	Location -> Overview-> <edit loca-<br="">tion></edit>	e.g. 5 Days
URL of login page	Location -> Overview-> <edit loca-<br="">tion></edit>	e.g .ht- tp://192.168.1.254 /auth
Walled Garden	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 ->	Enabled

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

SMS

51415		
Field	Menu	Value
SMS Provider	Client -> <edit client="">-></edit>	lox24
Account ID	Client -> <edit client="">-></edit>	*****
Route Germany	Client -> <edit client="">-></edit>	e.g. Economy
Registration type	Location -> <edit location=""></edit>	SMS
Tariff	Location -> <edit location=""></edit>	e.g. 5 Days
URL of login page	Location -> <edit location=""></edit>	e.g .ht- tp://192.168.1.254 /auth
Walled Garden	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 ->	Enabled
Walled Garden URL	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 ->	<pre>e.g. ht- tps://hotspot.bint ec-elmeg.com/3/205</pre>
Terms & Conditions	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 ->	e.g. ht- tp://www.bintec-el meg.com
Login Frameset	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 -> ->Advanced	Disabled

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

PayPal

Field	Menu	Value
API Username	Client-> <edit client=""></edit>	****
API Passwort	Client-> <edit client=""></edit>	e.g. supersecret
API Passwort repeat	Client-> <edit client=""></edit>	e.g. supersecret
Signature	Client-> <edit client=""></edit>	*****
Registration type	Location -> <edit location=""></edit>	Paid service
Tariff	Location -> <edit location=""></edit>	e.g. All
URL of login page	Location -> <edit location=""></edit>	e.g .ht- tp://192.168.1.254 /auth
Walled Garden	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 ->	Enabled
Walled Garden URL	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 ->	<pre>e.g. ht- tps://hotspot.bint ec-elmeg.com/3/205</pre>
Terms & Conditions	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 ->	e.g . ht- tp://www.bintec-el meg.com
Login Frameset	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 -> ->Advanced Settings	Disabled
Pop-Up window for status indication	Local Services -> Hotspot Gateway -> Hotspot Gateway -> BRIDGE_BR0-1 -> ->Advanced Settings	Disabled

Chapter 3 WLAN - 802.1x authentication using a Microsoft Server 2008

3.1 Introduction

The following describes connection of WLAN clients to a Windows Server 2008 using the 802.1x (EAP-PEAP) protocol.

WLAN authentication is performed by a RADIUS server. Here, authentication data (user name/password/certificates) are administered on the central Windows server. For this, a Windows 2008 Server is used; it features the following server roles:

- Active directory domain services (ADS)
- Active directory certificate services (CA)
- Network guidelines and access services (NPS)

The workshop demonstrates configuration of the server as certification authority (CA) and setup of the RADIUS server (Network Policy Server [NPS]). Next, configuration of an access point is described. Standard tools are used for connection of a WLAN client under Windows 7.

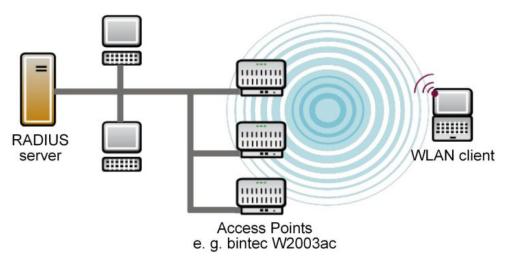


Fig. 53: Example scenario

Prerequisites

- A Microsoft Windows Server 2008 (e.g. Windows Server 2008 R2 Standard)
- · Active Directory configuration is required
- A DHCP server in the network is required (e.g. Windows DHCP-Server)
- One or more bintec access points (e.g. bintec W2003ac)
- One or more WLAN clients (e.g. Windows 7 WLAN supplicant)

3.2 Server configuration

3.2.1 Configuration of active directory certificate services

Authentication of WLAN clients at the RADIUS server occurs via secure transport connection. For this, the certificate from a certification authority (CA certificate) is necessary. The Server Manager is used to add the **Server role**.

(1) Go to "Add roles" assistant -> Server roles.

The Active Directory Certificate Services of the Windows Server are used in this workshop.

Assistent "Rollen hinzufügen"		×
Serverrollen aus	wählen	
Vorbemerkungen Serverrollen AD-Zertifikatdienste Rollendienste Installationstyp Zertifizierungsstellentyp Privater Schlüssel Kryptografie Zertifizierungsstelle Gültigkeitsdauer Zertifikatdatenbank Bestätigung Status Ergebnisse	Wählen Sie für die Installation auf dem Server eine oder mehrere Roll Rollen: Active Directory-Domänendienste (installiert) Active Directory-Parchteverwaltungsdienste Active Directory-Rechteverwaltungsdienste Active Directory-Verbunddienste Active Directory-Verbunddienste Active Directory-Verbunddienste Active Directory-Verbunddienste Active Directory-Verbunddienste Active Directory-Verbunddienste Dateidienste DHCP-Server DhS-Server (installiert) Druck- und Dokumentdienste Raxserver Hyper-V Netzwerkrichtlinien- und Zugriffsdienste Remotedesktopdienste Webserver (IIS) (installiert) Windows Server Update Services (WSUS) Windows-Bereitstellungsdienste Weitere Informationen zu Serverrollen	Beschreibung: Active Directory-Zertifikatdienste wird zum Erstellen von Zertifizierungsstellen und dazugehörigen Rollendiensten verwendet, die Ihnen das Ausstellen und Verwälten von Zertifikaten ermöglichen, die in einer Vielzahl von Anwendungen verwendet werden.
	< Zurück Weiter	> Installieren Abbrechen

Access to the certificate occurs via a web interface.

For this, **Role service** *Certification authority web registration* is installed in addition to the certification authority itself.

Rollendienste hinzufügen		×
Rollendienste au	swählen	
Rollendienste Webserver (IIS) Rollendienste Bestätigung Status Ergebnisse	Wählen Sie die zu installierenden Rollendienste für "Active Direr Rollendienste: Zertifizierungsstelle (installiert) Ertifizierungsstellen-Webregistrierung Webdienst für Zertifikatregistrierungsrichtlinie Webdienst für Zertifikatregistrierungsrichtlinie Webdienst für Zertifikatregistrierungsrichtlinie Webdienst für Zertifikatregistrierungsrichtlinie Keitere Informationen zu Rollendiensten Zurück.	ctory-Zertifikatdienste" aus: Beschreibung: Die Zertifizierungsstellen- Webregistrierung stellt eine einfache Webschnittstelle bereit, die Benutzern das Ausführen von Aufgaben ermöglicht, z. B. Anfordern und Ermeuern von Zertifikaten, Aburfen von Zertifikatsperrlisten (CRLs) und Registrieren für Smartcardzertifikate. Weiter > Instellieren

In the next steps of the assistant for creating server roles *Active Directory Certi-ficate Services* the **Installation Type** of the certification authority is selected.

Select the *Company* option.

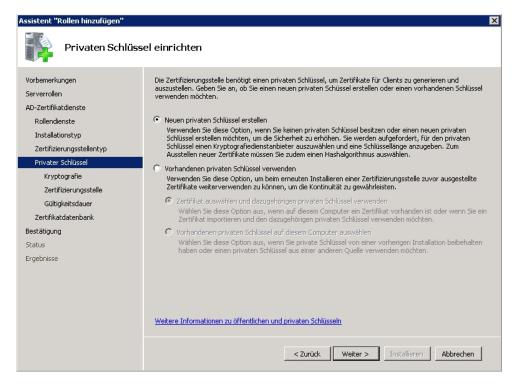
Assistent "Rollen hinzufügen"		×
Setuptyp angebe	n	
Vorbemerkungen Serverrollen AD-Zertifikatdienste Rollendienste Installationstyp Zertifizierungsstellentyp Privater Schlüssel Kryptografie Zertifizierungsstelle Gültigkeitsdauer Zertifikatdatenbank Bestätigung Status Ergebnisse	 Zertifizierungsstellen können Daten in Active Directory verwenden, um die Ausstellung und Verwaltung von Zertifikaten zu vereinfachen. Geben Sie an, ob Sie eine Unternehmenszertifizierungsstelle oder eine eigenständige Zertifizierungsstelle einrichten möchten. Unternehmen Wählen Sie diese Option aus, wenn diese Zertifizierungsstelle Mitglied einer Domäne ist und den Verzeichnisdienst zum Ausstellen und Verwalten von Zertifikaten verwenden kann. Eigenständig Wählen Sie diese Option aus, wenn diese Zertifizierungsstelle Mitglied einer Domäne ist und den Verzeichnisdienst zum Ausstellen und Verwalten von Zertifikaten verwenden kann. Eigenständig Wählen Sie diese Option aus, wenn diese Zertifizierungsstelle keine Verzeichnisdienstdaten zum Ausstellen oder Verwalten von Zertifikaten verwendet. Eine eigenständige Zertifizierungsstelle kann Mitglied einer Domäne sein. 	
	Weitere Informationen zu den Unterschieden zwischen Unternehmenssetup und eigenständigem Setup	
	< Zurück Weiter > Installieren Abbrechen	

In the Certification Authority Type menu, select the *Root Certification Author-ity* option.

Assistent "Rollen hinzufügen"	X
Zertifizierungsst	ellentyp angeben
Vorbemerkungen Serverrollen AD-Zertifikatdienste Rollendienste Installationstyp Zertifizierungsstellentyp Privater Schlüssel Kryptografie Zertifizierungsstelle Gültigkeitsdauer Zertifikatdatenbank Bestätigung Status Ergebnisse	 Sie können eine Kombination aus Stammzertifizierungsstellen und untergeordneten Zertifizierungsstellen konfigurieren, um eine hierarchische Public Key-Infrastruktur (PKI) zu erstellen. Eine Stammzertifizierungsstelle ist eine Zertifizierungsstelle empfängt Zertifikate von einer anderen Zertifizierungsstelle. Geben Sie an, ob Sie eine Stammzertifizierungsstelle oder eine untergeordnete Zertifizierungsstelle in einer Public Key-Infrastruktur (PKI) zu erstellen. Eine Stammzertifizierungsstelle oder eine untergeordnete Zertifizierungsstelle einrichten möchten. C Stammzertifizierungsstelle wenn Sie die erste oder einzige Zertifizierungsstelle in einer Public Key-Infrastruktur installieren. C Untergeordnete Zertifizierungsstelle Wählen Sie diese Option aus, wenn Sie die erste oder einzige Zertifizierungsstelle in einer Public Key-Infrastruktur installieren. C Untergeordnete Zertifizierungsstelle Wählen Sie diese Option aus, wenn die Zertifizierungsstelle das Zertifizierungsstelle in einer Public Key-Infrastruktur installieren.
Ligennisse	Weitere Informationen zur Public Key-Infrastruktur < Zurück

In our example, at initial installation of the certification authority, a new **Private Key** is also generated.

Select the Create New Private key option.



In the Encryption menu, select hash algorithm *SHA1* and a Key Character Length of 2048 bits.

Assistent "Rollen hinzufügen"	X
Kryptografie für	ZS konfigurieren
Vorbemerkungen Serverrollen AD-Zertifikatdienste Rollendienste Installationstyp Zertifizierungsstellentyp Privater Schlüssel	Zum Erstellen eines neuen privaten Schlüssells müssen Sie zunächst einen Kryptografiedienstanbieter, einen Hashalgorithmus und eine Schlüssellange auswählen, die für den beabsichtigten Zweck der von Ihnen ausgestellten Zertifikate geeignet sind. Ein höherer Wert für die Schlüssellange verstarkt die Sicherheit, erhöht aber auch den Zeitaufwand zum Abschließen von Signaturvorgängen. Wählen Sie einen Kryptografiedienstanbieter (CSP) aus: Schlüsselzeichenlänge: RSA#Microsoft Software Key Storage Provider Schlüsselzeichenlänge: Wählen Sie den Hashalgorithmus zum Signieren von Zertifikaten aus, die von dieser Zertifizierungsstelle
Frivater Schlussei Kryptografie Zertifizierungsstelle Gültigkeitsdauer Zertifikatdatenbank Bestätigung Status Ergebnisse	SHA384 SHA512 SHA1 Administratorinteraktion bei jedem Zertifizierungsstellenzugriff auf den privaten Schlüssel zulassen
	Weitere Informationen zu kryptografischen Optionen für eine Zertifizierungsstelle
	< Zurück Weiter > Installieren Abbrechen

In the next step, the designation of the certification authority certificate is specified in the **Certification Authority** menu, along with the distinguished name (DN).

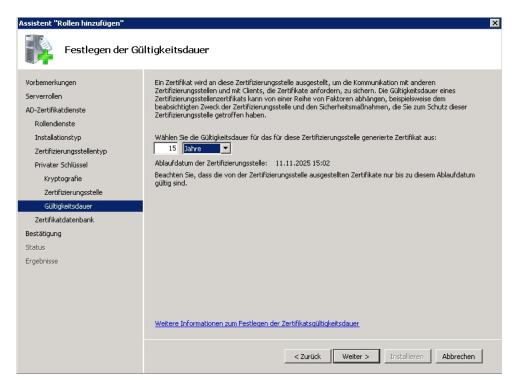
Under Common Name of this Certification Authority enter ${\it WorkshopWLANCA},$ for example.

As Suffix of the defined name enter *DC=wlan*, *DC=funkwerk-ec*, *DC=com*, for example.

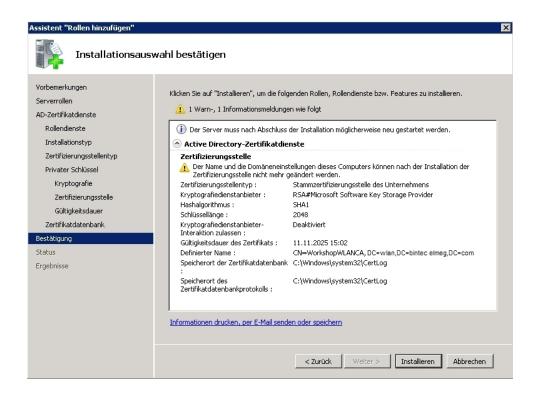
Assistent "Rollen hinzufügen"		x
Name der Zertifiz	zierungsstelle konfigurieren	
Vorbemerkungen Serverrollen AD-Zertifikatdienste Rollendienste Installationstyp Zertifizierungsstellentyp Privater Schlüssel Kryptografie Zertifizierungsstelle Gültigkeitsdauer Zertifikatdatenbank Bestätigung Status Ergebnisse	Geben Sie einen allgemeinen Namen zur Identifizierung der Zertifizierungsstelle an. Dieser Name wird allen von der Zertifizierungsstelle ausgestellten Zertifizierungstelle. Allgemeiner Name dieser Zertifizierungsstelle: WorkshopWLANCA Suffix des definierten Namens: DC=wlan,DC=bintec eimeg,DC=com Vorschau des definierten Namens: CN=WorkshopWLANCA,DC=wlan,DC=bintec eimeg,DC=com WorkshopWLANCA,DC=wlan,DC=bintec eimeg,DC=com	
	< Zurück Weiter > Instellieren Abbrechen	

Also select the **Period of Validity** for the certification authority certificate.

In our example, the period of validity is set to 15 years.



At conclusion of the installation of the server role **Active Directory Certificate Services** a summary is displayed, along with the result of the installation.



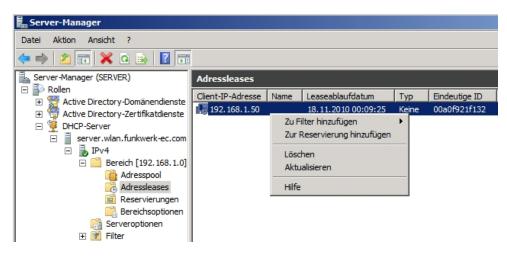
Assistent "Rollen hinzufügen"		×
Installationser	gebnisse	
Vorbemerkungen	Die folgenden Rollen, Rollendienste bzw. Features wurden erfolgreich installiert:	
Serverrollen		-
AD-Zertifikatdienste	 Active Directory-Zertifikatdienste Installation war erfolgreich 	
Rollendienste	Die folgenden Rollendienste wurden installiert: Zertifizierungsstelle	
Installationstyp		
Zertifizierungsstellentyp		
Privater Schlüssel		
Kryptografie		
Zertifizierungsstelle		
Gültigkeitsdauer		
Zertifikatdatenbank		
Bestätigung		
Status		
Ergebnisse		
	Installationsbericht drucken, per E-Mail senden oder speichern	
	< Zurück Weiter > Schließen Abbrechen]

3.2.2 Reservation of access point IP addresses at DHCP server (Windows Server 2008)

The **bintec** access points employed (e.g. **bintec W1002n**) are integrated into the network with the DHCP client mechanism. In this workshop, the Windows Server operates as a DH-CP server, notably administering IP addresses of access points. To insure that the access points always remain accessible at the same IP address and always use the same IP address for RADIUS authentication, their IP addresses are reserved at the DHCP server.

Previously allocated IP addresses are listed in the **Address Leases** menu of the Windows 2008 Server manager. Using the context menu, the addresses of access points can be added as **Reservations**.

(1) Go to Server Manager -> DHCP Server -> Address leases.



WLAN access points without active **Address Leases** (no IP address assigned) can be created via the **New Reservation** context menu. For this, the Ethernet MAC address of the respective access point must be saved.

(1) Go to Server Manager -> DHCP Server -> Reservations.

Server-Manager (SERVER) Reservierungen Server-Manager (SERVER) Reservierungen	
	<u>I</u>
 	
□ ■ server.wlan.funkwerk-ec.com □ ■ IPv4 Reservierungsname: WLANAccessPointZimmer1	
Bereich [192.168.1.0] IP-Adresse: 192.168.1.254	
Adressleases MAC-Adresse: 00:a0:f9:a0:b0:21	
Bereichsoptionen Beschreibung:	
E Filter	
🗆 🐻 IPv6	
G DHCP Serveroptionen ODHCP	
Provide the second secon	
Features	
🗆 🖬 Diagnose Hinzufügen Schließer	
	-

To specify the information for a reserved client, proceed as follows;

- (1) Under Reservation number enter WLANAccessPointRoom1, for example.
- (2) Enter the IP Address, e.g. 192.168.1.254.
- (3) As MAC Address, enter e.g. 00:a0:f9:a0:b0:21

3.2.3 Installation of network policy and access services (NPS/RADIUS server)

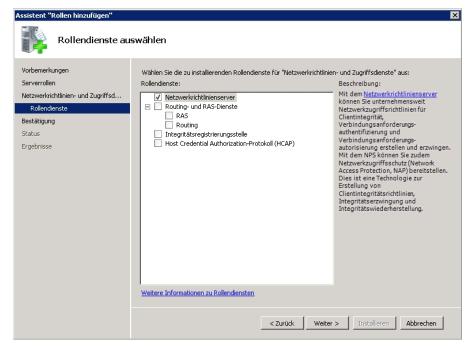
With installation of the *Network Policy and access services (NPS)* the RADIUS server of Windows 2008 Server is installed. For this, use the **Add Roles** function of the server manager. Proceed as follows:

- (1) Go to "Add Roles" assistant ->Server Roles.
- (2) Select the option Network policy and access services.

Assistent "Rollen hinzufügen" Serverrollen aus	wählen	×
Vorbemerkungen Serverrollen Netzwerkrichtlinien- und Zugriffsd Rollendienste Bestätigung Status Ergebnisse	Wählen Sie für die Installation auf dem Server eine oder mehrer Rollen: Active Directory-Domänendienste (installiert) Active Directory-Rechteverwaltungsdienste Active Directory-Zertifikatdienste (installiert) Active Directory-Zertifikatdienste (installiert) Active Directory-Zertifikatdienste (installiert) Active Directory-Zertifikatdienste (installiert) Directory-Zertifikatdienste (installiert) Direck-Server Diruck- und Dokumentdienste Paxserver Hyper-V Vekzwerkrichtlinien- und Zugriffsdienste Webserver (IIS) (installiert) Windows-Bereitstellungsdienste Windows-Bereitstellungsdienste Windows-Bereitstellungsdienste	re Rollen aus. Beschreibung: <u>Netzwerkrichtlinien- und</u> <u>Zuariffsdienste</u> stellen Netzwerkrichtlinienserver (Network Policy Server, NPS), Routing und RAS, Integritätsregistrierungsstelle (HRA) und HCAP (Host Credential Authorization-Protokoll) bereit, um die Integrität und Sicherheit des Netzwerks zu schützen.

(3) Go to Role Services.

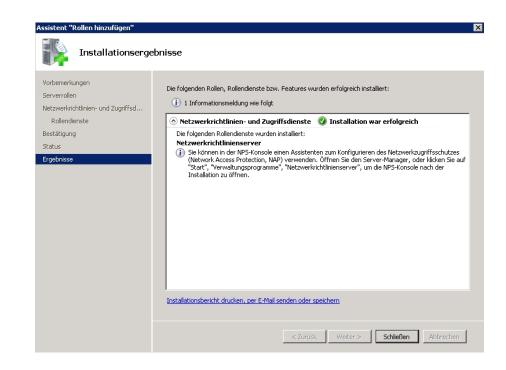
Enable the option Network Policy Server.



(4) Click Install. The roles are installed.

Vorbemerkungen Serverrollen Netzwerkrichtlinien- und Zugriffsd Rollendienste Bestätigung Status Ergebnisse	n hinzufügen" stallationsauswahl b	E
Informationen drucken, per E-Mail senden oder speichern	sn- und Zugriffsd	

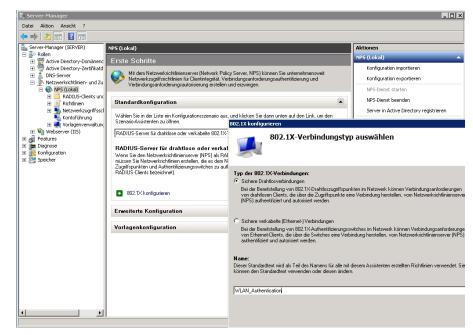
(5) Under **Results** you can check whether the roles are successfully installed.



3.2.4 Configuration of network policy and access services (NPS/RADIUS server)

The RADIUS server for the 802.1x WLAN authentication is configured in the **Network Policy Servers (NPS)** menu.

 Go to Server Manager -> Network Policies and Access Services (NPS) -> NPS (local).



- (2) Select a configuration scenario.
- (3) Click on the Configure 802.1X link to open the scenario assistant.
- (4) In the first step, select Type of 802.1x Connections Secure Wireless Connections and assign a Name e. g. WLAN_Authentication.
- (5) In the second step of the assistant, all access points are configured as RADIUS client. At login of a WLAN client, the access points send authentication requests to the RADI-US server (network policies and access services, NPS). When creating the RADIUS clients (access points), their IP address and a password are assigned to protect the RADIUS authentication.

Geben Sie 802.1X-Switches oder Drahtloszugriffspunkte (RADIUS-Clients) an. CADIUS-Clients sind Netzwerkzugriffsserver, z.B. Authentifizierungsswitches und Drahtloszugriffs ADIUS-Clients sind keine Clientcomputer. Glicken Sie auf "Hinzufügen", um einen RADIUS-Client anzugeben. CADIUS-Clients: WLAN_AccessPoint_Zimmer_1 WLAN_AccessPoint_Zimmer_2 WLAN_AccessPoint_Zimmer_3 enschaften von WLAN_AccessPoint_Zimmer_1 Einstellungen Vorhandene Vorlage auswählen: WLAN_AccessPoint_Zimmer_1 Adresse Anzeigename: WLAN_AccessPoint_Zimmer_1 Adresse (IP oder DNS): [192.168.1.254 Uberprüfen Gemeinsamer geheimer Schlüssel auswählen: Kaine		802.1X-Switches angeben	
ADIUS-Clients sind Netzwerkzugriffsserver, z.B. Authentifizierungsswitches und Drahtloszugriffs ADIUS-Clients sind keine Clientcomputer. Bicken Sie auf "Hinzufügen", um einen RADIUS-Client anzugeben. ADIUS-Clients: ALAN_AccessPoint_Zimmer_1 MLAN_AccessPoint_Zimmer_3 enschaften von WLAN_AccessPoint_Zimmer_1 Enthe Einstellungen Vorhendene Vorlage auswählen: WLAN_AccessPoint_Zimmer_1 Adresse Anzeigename: WLAN_AccessPoint_Zimmer_1 Adresse (IP oder DNS): 192:168:1.254 Uberprüfen Gemeinsamer geheime Schlüssel Vorlage für gemeinsame geheime Schlüssel auswählen: Keine Klicken Sie zum manuellen Eingeben eines gemeinsamen geheimen Schlüssels auf "Manuell", zum automatischen Erzeugen auf "Generieren". Konfigurieren Sie den RADIUS-Client mit demselben Schlüssel. Dabei ist auf Groß-/Kleinschreibung zu achten. Bestötigen:		-	
ADIUS-Clients sind keine Clientcomputer. Gicken Sie auf "Hinzufügen", um einen RADIUS-Client anzugeben. ADIUS-Clients: MLAN_AccessPoint_Zimmer_1 MLAN_AccessPoint_Zimmer_2 MLAN_AccessPoint_Zimmer_3 enschaften von WLAN_AccessPoint_Zimmer_1 Enth Einstellungen Vorhandene Vorlage auswählen: WLAN_AccessPoint_Zimmer_1 Adresse Anzeigename: WLAN_AccessPoint_Zimmer_1 Adresse (IP oder DNS): 132.1681.254 Uberprüfen Gemeinsamer geheimer Schlüssel Vorlage für gemeinsame geheime Schlüssel auswählen: Klicken Sie zum manuellen Eingeben eines gemeinsamen geheimen Schlüssel auf "Manuell" _ zum automatischen Erzeugen auf "Generieren". Konfigurieren Sie den RADIUS-Client mit demselben Schlüssel. • Manuell _ Generieren Gemeinsamer geheimer Schlüssel: • Manuell _ Generieren Generieren Bestätigen:		Geben Sie 802.1X-Switches oder Drahtloszugriftspunkte (RADIUS-Client	ts) an.
ADIUS-Clients: MLAN_AccessPoint_Zimmer_1 MLAN_AccessPoint_Zimmer_3 Bearb enschaften von WLAN_AccessPoint_Zimmer_1 Einstellungen Vorhandene Vorlage auswählen: WLAN_AccessPoint_Zimmer_1 Adresse Anzeigename: WLAN_AccessPoint_Zimmer_1 Adresse (IP oder DNS): 192.168.1.254 Uberprüfen Gemeinsamer geheimer Schlüssel Vorlage für gemeinsame geheime Schlüssel auswählen: Keine Klicken Sie zum manuellen Eingeben eines gemeinsamen geheimen Schlüssels auf "Manuell", zum automatischen Erzeugen auf "Generieren". Konfigurieren Sie den RADIUS-Client mit demselben Schlüssel. Dabei ist auf Groß-/Kleinschreibung zu achten. Manuell Generieren Gemeinsamer geheimer Schlüssel: Bestätigen:			oszugriffspu
MIAN_AccessPoint_Zimmer_1 Hinzul MIAN_AccessPoint_Zimmer_3 Bearb enschaften von WLAN_AccessPoint_Zimmer_1 X Einstellungen Image: Comparison of the second secon	Klicken Sie aut	f "Hinzufügen", um einen RADIUS-Client anzugeben.	
WLAN_AccessPoint_Zimmer_2 WLAN_AccessPoint_Zimmer_3 enschaften von WLAN_AccessPoint_Zimmer_1 Entit Einstellungen Vorhandene Vorlage auswählen: Vorhandene Vorlage auswählen: WLAN_AccessPoint_Zimmer_1 Adresse (IP oder DNS): 192.168.1.254 Uberprüfen Gemeinsamer geheimer Schlüssel Vorlage für gemeinsame geheime Schlüssel auswählen: Keine Klicken Sie zum manuellen Eingeben eines gemeinsamen geheimen Schlüssels auf "Manuell", zum automatischen Erzeugen auf "Generieren". Konfigurieren Sie den RADIUS-Client mit demselben Schlüssel. Dabei ist auf Groß-/Kleinschreibung zu achten. Manuell Generieren Generieren Generieren Generieren Bestätigen:	RADIUS-Clier	nts:	
WLAN_AccessPoint_Zimmer_3 Beath enschaften von WLAN_AccessPoint_Zimmer_1 Intri Einstellungen Intri Vorhandene Vorlage auswählen: Intri Mane und Adresse Anzeigename: WLAN_AccessPoint_Zimmer_1 Intri Adresse (IP oder DNS): Ip2.168.1.254 Uberprüfen Gemeinsamer geheimer Schlüssel Vorlage für gemeinsame geheime Schlüssel auswählen: Intri Keine Intri Klicken Sie zum manuellen Eingeben eines gemeinsamen geheimen Schlüssels auf "Manuell", zum automatischen Erzeugen auf "Generieren". Konfigurieren Sie den RADIUS-Client mit demselben Schlüssel. Dabei ist auf Groß-/Kleinschreibung zu achten. Manuell Generieren Gemeinsamer geheimer Schlüssel: Intri Manuell Generieren Bestätigen: Intri			Hinzufüge
Entri Einstellungen			Bearbeite
Einstellungen	genschaften [.]	von WLAN_AccessPoint_Zimmer_1	
Vorhandene Vorlage auswählen: Image: Name und Adresse Anzeigename: MLAN_AccessPoint_Zimmer_1 Adresse (IP oder DNS): 192.168.1.254 Uberprüfen Gemeinsamer geheimer Schlüssel Vorlage für gemeinsame geheime Schlüssel auswählen: Keine Klicken Sie zum manuellen Eingeben eines gemeinsamen geheimen Schlüssels auf "Manuell", zum automatischen Erzeugen auf "Generieren". Konfigurieren Sie den RADIUS-Client mit demselben Schlüssel. Dabei ist auf Groß-/Kleinschreibung zu achten. Imanuell Generieren Gemeinsamer geheimer Schlüssel: Estätigen:	Finstellungen		Entrerne
Name und Adresse Anzeigename: WLAN_AccessPoint_Zimmer_1 Adresse (IP oder DNS): 192.168.1.254 Uberprüfen Gemeinsamer geheimer Schlüssel Vorlage für gemeinsame geheime Schlüssel auswählen: Keine Klicken Sie zum manuellen Eingeben eines gemeinsamen geheimen Schlüssels auf "Manuell", zum automatischen Erzeugen auf "Generieren". Konfigurieren Sie den RADIUS-Client mit demselben Schlüssel. Dabei ist auf Groß-/Kleinschreibung zu achten. Manuell Generieren Gemeinsamer geheimer Schlüssel: Bestätigen:		· · · · · · · · · · · · · · · · · · ·	
Anzeigename: WLAN_AccessPoint_Zimmer_1 Adresse (IP oder DNS): 192.168.1.254 Uberprüfen Gemeinsamer geheimer Schlüssel Vorlage für gemeinsame geheime Schlüssel auswählen: Keine Klicken Sie zum manuellen Eingeben eines gemeinsamen geheimen Schlüssels auf "Manuell", zum automatischen Erzeugen auf "Generieren". Konfigurieren Sie den RADIUS-Client mit demselben Schlüssel. Dabei ist auf Groß-/Kleinschreibung zu achten. Manuell Generieren Gemeinsamer geheimer Schlüssel: ••••••••••••••••••••••••••••••••••••	Vorhande	ne Vorlage auswählen:	
Anzeigename: WLAN_AccessPoint_Zimmer_1 Adresse (IP oder DNS): 192.168.1.254 Uberprüfen Gemeinsamer geheimer Schlüssel Vorlage für gemeinsame geheime Schlüssel auswählen: Keine Klicken Sie zum manuellen Eingeben eines gemeinsamen geheimen Schlüssels auf "Manuell", zum automatischen Erzeugen auf "Generieren". Konfigurieren Sie den RADIUS-Client mit demselben Schlüssel. Dabei ist auf Groß-/Kleinschreibung zu achten. Manuell Generieren Gemeinsamer geheimer Schlüssel: ••••••••••••••••••••••••••••••••••••			
Anzeigename: WLAN_AccessPoint_Zimmer_1 Adresse (IP oder DNS): 192.168.1.254 Uberprüfen Gemeinsamer geheimer Schlüssel Vorlage für gemeinsame geheime Schlüssel auswählen: Keine Klicken Sie zum manuellen Eingeben eines gemeinsamen geheimen Schlüssels auf "Manuell", zum automatischen Erzeugen auf "Generieren". Konfigurieren Sie den RADIUS-Client mit demselben Schlüssel. Dabei ist auf Groß-/Kleinschreibung zu achten. Manuell Generieren Gemeinsamer geheimer Schlüssel: ••••••••••••••••••••••••••••••••••••	⊢ Name und A	dresse	
Adresse (IP oder DNS): 192.168.1.254 Uberprüfen Gemeinsamer geheimer Schlüssel Uberprüfen Vorlage für gemeinsame geheime Schlüssel auswählen: Image: Comparison of the second			
192.168.1.254 Uberprüfen Gemeinsamer geheimer Schlüssel Vorlage für gemeinsame geheime Schlüssel auswählen: Keine Image: Comparison of the second sec	WLAN_Acc	cessPoint Zimmer 1	
192.168.1.254 Uberprüfen Gemeinsamer geheimer Schlüssel Vorlage für gemeinsame geheime Schlüssel auswählen: Keine Image: Comparison of the second sec			
Vorlage für gemeinsame geheime Schlüssel auswählen: Keine Klicken Sie zum manuellen Eingeben eines gemeinsamen geheimen Schlüssels auf "Manuell", zum automatischen Erzeugen auf "Generieren". Konfigurieren Sie den RADIUS-Client mit demselben Schlüssel. Dabei ist auf Groß-/Kleinschreibung zu achten. Manuell Generieren Gemeinsamer geheimer Schlüssel: • Bestätigen:	Adresse (IP		
Vorlage für gemeinsame geheime Schlüssel auswählen: Keine Klicken Sie zum manuellen Eingeben eines gemeinsamen geheimen Schlüssels auf "Manuell", zum automatischen Erzeugen auf "Generieren". Konfigurieren Sie den RADIUS-Client mit demselben Schlüssel. Dabei ist auf Groß-/Kleinschreibung zu achten. Manuell Generieren Gemeinsamer geheimer Schlüssel: • Bestätigen:		oder DNS):	
Keine Abbra Klicken Sie zum manuellen Eingeben eines gemeinsamen geheimen Schlüssels auf "Manuell", zum automatischen Erzeugen auf "Generieren". Konfigurieren Sie den RADIUS-Client mit demselben Schlüssel. Dabei ist auf Groß-/Kleinschreibung zu achten. • Manuell • Generieren Generieren Generieren Bestätigen:	192.168.1.2	oder DNS): 254 Überprüfen	
Klicken Sie zum manuellen Eingeben eines gemeinsamen geheimen Schlüssels auf "Manuell", zum automatischen Erzeugen auf "Generieren". Konfigurieren Sie den RADIUS-Client mit demselben Schlüssel. Dabei ist auf Groß-/Kleinschreibung zu achten. Manuell G Generieren Gemeinsamer geheimer Schlüssel: Bestätigen:	Gemeinsame	oder DNS): 254 Überprüfen	
 "Manuell", zum automatischen Erzeugen auf "Generieren". Konfigurieren Sie den RADIUS-Client mit demselben Schlüssel. Dabei ist auf Groß-/Kleinschreibung zu achten. Manuell Generieren Gemeinsamer geheimer Schlüssel: Bestätigen: 	Gemeinsame Vorlage für g	oder DNS): 254 Überprüfen er geheimer Schlüssel gemeinsame geheime Schlüssel auswählen:	
Gemeinsamer geheimer Schlüssel:	Gemeinsame Vorlage für g	oder DNS): 254 Überprüfen er geheimer Schlüssel gemeinsame geheime Schlüssel auswählen:	Abbreche
Gemeinsamer geheimer Schlüssel:	Gemeinsame Vorlage für g Keine Klicken Sie z "Manuell", z RADIUS-Clie	oder DNS): 254 er geheimer Schlüssel gemeinsame geheime Schlüssel auswählen: zum manuellen Eingeben eines gemeinsamen geheimen Schlüssels auf rum automatischen Erzeugen auf "Generieren". Konfigurieren Sie den	Abbreche
Bestätigen:	192.168.1.2 Gemeinsame Vorlage für g Keine Klicken Sie : "Manuell", z RADIUS-Clie achten.	oder DNS): 254 er geheimer Schlüssel gemeinsame geheime Schlüssel auswählen: zum manuellen Eingeben eines gemeinsamen geheimen Schlüssels auf zum automatischen Erzeugen auf "Generieren". Konfigurieren Sie den ent mit demselben Schlüssel. Dabei ist auf Groß-/Kleinschreibung zu	Abbreche
	192.168.1.2 Gemeinsame Vorlage für g Keine Klicken Sie : "Manuell", z RADIUS-Clie achten. Imanuell	oder DNS): 254 Uberprüfen er geheimer Schlüssel gemeinsame geheime Schlüssel auswählen: zum manuellen Eingeben eines gemeinsamen geheimen Schlüssels auf zum automatischen Erzeugen auf "Generieren". Konfigurieren Sie den ent mit demselben Schlüssel. Dabei ist auf Groß-/Kleinschreibung zu Generieren	Abbreche
••••••	192.168.1.2 Gemeinsame Vorlage für g Keine Klicken Sie a "Manuell", z RADIUS-Clie achten. © Manuell Gemeinsame	oder DNS): 254 Uberprüfen er geheimer Schlüssel gemeinsame geheime Schlüssel auswählen: zum manuellen Eingeben eines gemeinsamen geheimen Schlüssels auf zum automatischen Erzeugen auf "Generieren". Konfigurieren Sie den ent mit demselben Schlüssel. Dabei ist auf Groß-/Kleinschreibung zu Generieren er geheimer Schlüssel:	Abbreche
	192.168.1.2 Gemeinsame Vorlage für g Keine Klicken Sie : "Manuell", z RADIUS-Clia achten. © Manuell Gemeinsame ••••••••••••••••••••••••••••••••••••	oder DNS): 254 Uberprüfen er geheimer Schlüssel gemeinsame geheime Schlüssel auswählen: zum manuellen Eingeben eines gemeinsamen geheimen Schlüssels auf zum automatischen Erzeugen auf "Generieren". Konfigurieren Sie den ent mit demselben Schlüssel. Dabei ist auf Groß-/Kleinschreibung zu Generieren er geheimer Schlüssel:	Abbreche
	192.168.1.2 Gemeinsame Vorlage für g Keine Klicken Sie : "Manuell", z RADIUS-Clie achten. © Manuell Gemeinsame Bestätigen:	oder DNS): 254 Uberprüfen er geheimer Schlüssel gemeinsame geheime Schlüssel auswählen: zum manuellen Eingeben eines gemeinsamen geheimen Schlüssels auf zum automatischen Erzeugen auf "Generieren". Konfigurieren Sie den ent mit demselben Schlüssel. Dabei ist auf Groß-/Kleinschreibung zu Generieren er geheimer Schlüssel:	Abbrech

(6) Next, the **EAP type** (Extensible Authentication Protocol) is selected for authentication of the WLAN client. In this workshop *EAP-PEAP* is used. In the EAP-PEAP option configuration dialog box, the server certificate for identification to the WLAN client must be selected.

802.1X konfigu	rieren	X
	Authentifizierungsmethode konfigurieren	
Wählen Sie der	n EAP-Typ für diese Richtlinie aus.	
Typ (basierer	nd auf der Zugriffsmethode und der Netzwerkkonfiguration):	
Microsoft: Ges	chütztes EAP (PEAP)	igurieren
	Eigenschaften für geschütztes EAP bearbeiten	
	Wählen Sie das Zertifikat aus, das der Server verwenden soll, um sei gegenüber einem Client zu bestätigen. Ein für geschütztes EAP in der Verbindungsanforderungsrichtlinie konfiguriertes Zertifikat setzt diese	r
	Zertifikat ausgestellt für: Server.wlan.bintec-elmeg.com	•
	Anzeigename:	
	Aussteller: WorkshopWLANCA	
	Ablaufdatum: 11.11.2011 22:44:15	
	Schnelle Wiederherstellung der Verbindung aktivieren	
	Clients ohne Kryptografiebindung trennen	
	EAP-Typen	
	Gesichertes Kennwort (EAP-MSCHAP v2)	Nach oben
		Nach unten

(7) In the next step, WLAN access can be restricted to individual user groups. In this workshop, we're allowing access to members of the **WLAN**user group.

)2.1X konfigu	rieren			
	Benutzergruppen angeber Benutzern, die Mitglied der ausgewählten basierend auf der Netzwerkrichtlinieneinst verweigert.	Gruppe oder Gruppe		
	Hinzufügen von Benutzergruppen auf "Hinzuf für alle Benutzer.	ügen". Wurden keine	Gruppen ausg	gewählt, gilt
Gruppen				Hinzufügen
WLANWLAI	L_users		[Entfernen

(8) Before closing, the assistant displays a summary and the configuration of the Network Policy Server (NPS) is created.

802.1X konfiguri	eren 🔉
	Abschließen neuer sicherer verkabelter und drahtloser IEEE 802.1X-Verbindungen und RADIUS-Clients
Folgende Richtlin	ien wurden erstellt und folgende RADIUS-Clients konfiguriert.
• Klicken Sie zum	n Anzeigen der Konfigurationsdetails im Standardbrowser auf "Konfigurationsdetails". Nändern der Konfiguration auf "Zurück". Speichern der Konfiguration und zum Schließen des Assistenten auf "Fertig stellen".
WLAN_AccessPi WLAN_AccessPi Verbindungsar	ont_Zimmer_1 (192.168.1.254) oint_Zimmer_2 (192.168.1.253) oint_Zimmer_3 (192.168.1.252) o forderungsrichtlinie:
WLAN_Authentic	
WLAN_Authentic	
Konfigurationsdet	<u>ails</u>
	Zurück Weiter Fertig stellen Abbrechen

3.3 RADIUS configuration of the access point

When a WLAN client logs in, the access point routes the authentication request to the RA-DIUS server (Windows 2008 NPS) as a RADIUS request. The RADIUS server is configured at the **bintec** access point using the GUIGUIGUI.

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

Basic Parameters	
Authentication Type	WLAN (802.1x)
Server IP Address 192.168.1.10	
RADIUS Secret	
Default User Password	
Priority	0 •
Entry active	Enabled
Group Description	Default Group 0

Fig. 54: System Management -> Remote Authentication -> RADIUS -> New

To configure the RADIUS server, proceed as follows:

- (1) To control access to WLAN network, you must set **Authentication Type** to the value *WLAN (802.1x)*.
- (2) Enter the IP Address of the Windows 2008 server, e.g. 192.168.1.10.
- (3) Communication with the RADIUS server is protected by a **RADIUS password**. Here, please use the password saved in the RADIUS server.
- (4) Press OK to confirm your entries.

3.4 WLAN configuration of the access point

You can adapt settings of the WLAN wireless module to requirements. In our example, we're using the 2.4 GHz band with automatic channel selection.

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

Wireless Settings		Performance Settings	
Operation Mode	Access-Point / Bridge Link Master 🔻	Wireless Mode	802.11b/g/n •
Operation Band	2.4 GHz In/Outdoor V	Number of Spatial Streams	2 •
Channel	Auto 🔻	Airtime fairness	
Transmit Power	Max. •		

Fig. 55: Wireless LAN -> WLAN -> Radio Settings->

To configure the access point, proceed as follows:

- (1) For Operating Mode, select Access-Point / Bridge Link Master.
- (2) For Frequency Band select 2.4 GHz In/Outdoor.
- (3) Set Channel to Auto.
- (4) Leave the remaining settings unchanged and confirm with OK.

With configuration of a wireless network (VSS), authentication requests of a WLAN client are routed to the configured RADIUS server.

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

Service Set Parameters			Security Settings		
Network Name (SSID)	workshop	Visible	Security Mode		WPA Enterprise *
			Warning: No Radius Server cor	figured for 802.1x	
Intra-cell Repeating		Enabled	WPA Mode		WPA and WPA 2 🔻
U-APSD		Enabled	WPA Cipher	O AES O TKIP	AES and TKIP
			WPA2 Cipher	O AES	AES and TKIP
			EAP Preauthentification	-	Enabled

Fig. 56: Wireless LAN -> WLAN -> Wireless networks (VSS) ->New

To configure wireless networks, proceed as follows:

- (1) In Network name (SSID) enter workshop, for example.
- (2) For Safety Mode, the WPA Enterprise safety mode must be selected.
- (3) For WPA Mode select WPA and WPA 2.
- (4) For WPA Cipher select AES and TKIP encryption.
- (5) For WPA2 Cipher select AES and TKIP encryption.
- (6) Leave the remaining settings unchanged and confirm with OK.

3.5 Connection of a Windows 7 WLAN client

3.5.1 Importing the certification from the certification authority (CA certificate)

With the selected authentication method $802.1x \neq EAP-PEAP$ a secure transport connection for transmission of login information is established. To insure that this tunnel is set up to the right remote terminal, the WLAN client identifies the server using the issued certificate. Hence, the certificate from the certification authority must be installed on every WLAN client.

In this workshop the web interface of the certificate server is used for installation of the certification authority certificate (CA certificate). For this, the notebook to be connected is first linked per Ethernet with the Window Server network. The web interface of the certificate server is accessible over the following URL: "http://SERVER_IP_Adresse/certsrv/" (e.g. http://192.168.1.10/certsrv/).

Microsoft-Active Directory-Zertifikatdienste - Windows Internet Explorer				
	<mark>ب</mark> م			
🖕 Favoriten 🖉 Microsoft-Active Directory-Zertifikatdienste 🛛 🏠 🔻 🖾 👻 🖃 🖶 Seite 👻 Sicherheit 👻 Extr	ras 🔻 🔞 🔻			
	tseite			
Willkommen				
Auf diese Website können Sie ein Zertifikat für den Webbrowser, E-Mail-Client oder andere Programm anfordern. Mit einem Zertifikat können Sie Ihre Identität gegenüber anderen Leuten, mit denen Sie über Web kommunizieren, bestätigen, E-Mail-Nachrichten signieren oder verschlüsseln und weitere Sicherheitsaufgaben, abhängig vom angeforderten Zertifikattyp, durchführen.				
Sie können diese Website auch zum Download eines Zertifizierungsstellenzertifikats, einer Zertifikatket oder einer Sperrliste verwenden, oder Sie können den Status einer ausstehenden Anforderung anzeige				
Weitere Informationen zu Active Directory-Zertifikatdienste erhalten Sie unter <u>Active Directory-Zertifikatdienstedokumentation</u> .				
Wählen Sie eine Aufgabe: Ein Zertifikat anfordern Status ausstehender Zertifikate anzeigen Download eines Zertifizierungsstellenzertifikats, einer Zertifikatkette oder einer Sperrliste				
🕒 😜 Internet Geschützter Modus: Aktiv 🍕 🔻 🎕 10)0% •			

With the **Download a certification authority certificate** option, the root certificate can be transferred onto the notebook (WLAN client).

Microsoft-Active Directory-Zertifikatdienste - Windows Internet Explorer	- - X
💽 💮 🗢 🖻 http://192.168.1.10/certsrv/certcarc.asp 🔹 🔄 🔄 🗞 🖸 Bing	+ م
🖕 Favoriten 🖉 Microsoft-Active Directory-Zertifikatdienste 🛛 🖄 🔻 🖾 👻 🚍 🖶 👻 Seite 🔻 Sicherh	eit 🔻 Extras 👻 🕢 🔻
Microsoft-Active Directory-Zertifikatdienste WorkshopWLANCA	<u>Startseite</u>
Download eines Zertifizierungsstellenzertifikats, einer Zertifikatkette oder einer Zertifika	tsperrliste
Installieren Sie diese Zertifizierungsstellen-Zertifikatkette, damit von dieser Zertifizierungsstelle Zertifikaten vertraut werden kann.	ausgestellten
Wählen Sie das Zertifikat und die Codierungsmethode für den Download eines Zertifizierungsstellenzertifikats, einer Zertifikatkette oder einer Sperrliste aus.	
Zertifizierungsstellenzertifikat:	
Aktuelles [WorkshopWLANCA]	E
Codierungsmethode:	
 ● DER ● Base 64 	
Download des Zertifizierungsstellenzertifikats	
Download der Zertifizierungsstellen-Zertifikatkette	
Download der aktuellen Basissperrliste	
Download der aktuellen Deltasperrliste	
Internet Geschützter Modus: Aktiv	▼ € 100% ▼

The certificate is then installed.

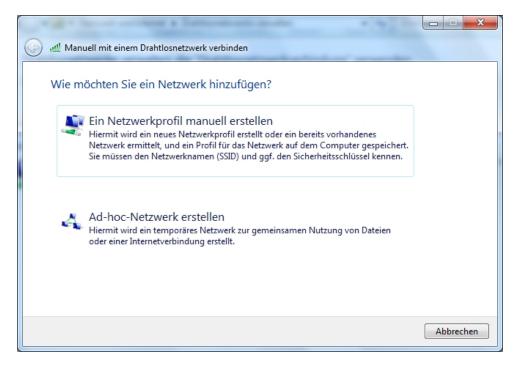
Zertifikat	x			
Allgemein Details Zertifizierungspfad				
Zertifikatsinformationen				
Dieses Zertifizierungsstellen-Stammzertifikat ist nicht vertrauenswürdig. Installieren Sie das Zertifikat in den Speicher vertrauenswürdiger Stammzertifizierungsstellen, um die Vertrauensstellung zu aktivieren.				
Ausgestellt für: WorkshopWLANCA	-			
Ausgestellt von: WorkshopWLANCA				
Gültig ab 11. 11. 2010 bis 11. 11. 2025				
Zertifikat installieren Ausstellererklärung Weitere Informationen über Zertifikate				
	ж			

Manually select the location where you wish to save the certificate.

Zertifikats	peicher
Zertifi	katspeicher sind Systembereiche, in denen Zertifikate gespeichert werden.
	ows kann automatisch einen Zertifikatspeicher auswählen, oder Sie können einen nerort für die Zertifikate angeben.
0	Zertifikatspeicher automatisch auswählen (auf dem Zertifikattyp basierend)
۲	Alle Zertifikate in folgendem Speicher speichern
	Zertifikatspeicher:
	Vertrauenswürdige Stammzertifizierungsstellen Durchsuchen
Weitere In	formationen über <u>Zertifikatspeicher</u>

3.5.2 Configuration of the Windows 7 WLAN client

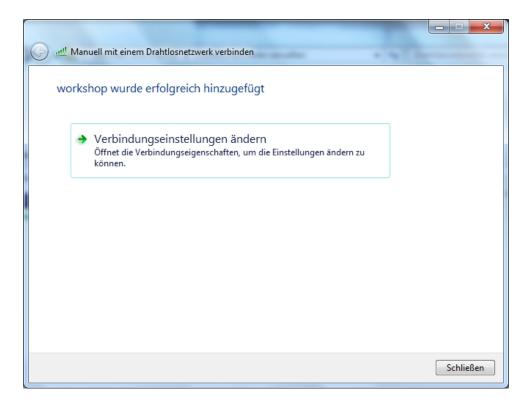
WLAN configuration is illustrated with the example of a Windows 7 client. Here, a new wireless connection is added using the **Manage wireless networks** dialog box.



The **Network Name**, along with **Safety Type** and **Encryption Type** are manually saved in the assistant.

	at a latticestonic second		
🚱 📲 Manuell mit einem Dra	htlosnetzwerk verbinden		
Geben Sie Informatio	onen für das Drahtlosnetzwerk	cein, das Sie hinzufüg	gen möchten.
Netzwerkname:	workshop		
Sicherheitstyp:	WPA2-Enterprise	•	
Verschlüsselungstyp:	AES	•	
Sicherheitsschlüssel:		Zeichen ausblende	n
🔽 Diese Verbindung a	utomatisch starten		
	enn das Netzwerk keine Kennung ausser		
Warnung: Bei Ausw	ahl dieser Option ist der Datenschutz die	eses Computers ggf. gefähr	rdet.
		Weiter	Abbrechen

After the new connection has been added using the assistant, the connection settings must be further adjusted.



In the process, the previously-installed certificate from the certification authority is selected as a trustworthy certificate in the safety method settings *Protected EAP (PEAP)*. This configuration step defines the Windows 2008 RADIUS server as a trustworthy remote terminal.

Eigenschaften für Drahtlosnetzwerk workshop	Eigenschaften für geschütztes EAP
Verbindung Sicherheit Sicherheitstyp: WPA2-Enterprise Verschlüsselungstyp: AES	Beim Herstellen der Verbindung:
Wählen Sie eine Methode für die Netzwerkauthentifizierung aus: Microsoft: Geschütztes EAP (PEAP) Für diese Verbindung eigene Anmeldeinformationen für jede Anmeldung speichern Erweiterte Einstellungen	Vertrauenswürdige Stammzertifizierungsstellen: GlobalSign Root CA GTE CyberTrust Global Root Microsoft Root Authority Microsoft Root Certificate Authority Thawte Timestamping CA UTN-USERFirst-Object V WorkshopWLANCA Keine Benutzeraufforderung zur Autorisierung neuer Server oder vertrauenswürdiger Zertifizierungsstellen Authentifizierungsmethode auswählen: Gesichertes Kennwort (EAP-MSCHAP v2) Konfigurieren
OK Abbrechen	Schnelle Wiederherstellung der Verbindung aktivieren Netzwerkzugriffsschutz erzwingen Verbindung trennen, wenn Server kein Kryptografiebindungs-TLV vorweist Identitätsdatenschutz aktivieren OK Abbrechen

Using the generated certificate, a secure connection is established between the WLAN client and the Windows 2008 server when setting up the WLAN connection. This connection serves for transmission of the Windows login data (user- or computer authentication) to the Microsoft Network Policy Server (RADIUS server).

Status von Drahtlosnetzwerkver	
Allgemein	
Verbindung	
IPv4-Konnektivität:	Internet
IPv6-Konnektivität:	Kein Netzwerkzugriff
Medienstatus:	Aktiviert
Kennung (SSID):	workshop
Dauer:	01:24:59
Übertragungsrate:	130,0 MBit/s
Signalqualität:	-atl
Details Drahtloseiger	nschaften
Aktivität	
Gesendet	Empfangen
Bytes: 18.775	14.021
🛞 Eigenschaften 🛛 🛞 Deakt	tivieren Diagnose
	Schließen

3.6 Overview of Configuration Steps

Configuration of	Configuration of active directory certificate services		
Field	Menu	Va	

Field	Menu	Value
Active directory certific- ate services	"Add Roles" assistant -> Server Roles.	Enable
Certification authority web registration	"Add Roles" assistant -> Role Ser- vices.	Enable
Company	"Add roles" assistant -> Installa- tion type.	Enable
Root certification author- ity	"Add Roles" assistant -> Certifica- tion Authority Type.	Enable
Generate new private key	"Add Roles" assistant -> Private Key.	Enable
Key character length	"Add Roles" assistant -> Encryp- tion.	2048
Hash algorithm	"Add Roles" assistant -> Encryp- tion.	SHA1
Common name of certi- fication authority	"Add Roles" assistant -> Certifica- tion Authority.	e.g. WorkshopWLANCA.
Suffix of the defined name	"Add Roles" assistant -> Certifica- tion Authority.	e.g. DC=wlan,DC=funkwer k,DC=com
Validity period	"Add Roles" assistant -> Validity Period.	15 years

Reservation of access point IP addresses at DHCP server

Field	Menu	Value
Address leases	Server Manager -> DHCP Server -> Address Leases.	Add to reservation
Reservation name	Server Manager -> DHCP Server -> Address Leases.	E.g. WLANAccess- PointRoom1
IP address	Server Manager -> DHCP Server -> Address Leases.	e.g. 192.168.1.254
MAC address	Server Manager -> DHCP Server -> Address Leases.	E.g . 00:a0:f9:a0:b2:21

Installation of network policies and access services

Field		Menu	Value
Network po cess servic		"Add Roles" assistant -> Server Roles.	Enable
Network po	olicy server	"Add Roles" assistant -> Role Ser- vices.	Enable

Configuration of network policies and access services

Field	Menu	Value
Configure 802.1X	Server Manager -> Network policies and access services (NPS) -> NPS (local).	Starting
Secure wireless connec- tions	Server Manager -> Network policies and access services (NPS) -> NPS (local).	Enable
Name	Server Manager -> Network policies and access services (NPS) -> NPS (local).	E.g. WLAN_Authenticatio n
Display name	configure 802.1X -> specify 802.1X Switches	E.g. WLAN_AccessPoint_R oom_1
Address (IP or DNS)	configure 802.1X -> specify 802.1X Switches	e.g. 192.168.1.254
Common secret key	configure 802.1X -> specify 802.1X Switches	e.g. supersecret
Туре	configure 802.1X -> Configure au- thentication method	<i>Microsoft: protec- ted EAP (PEAP)</i>
Certificate issued for:	configure 802.1X -> Configure au- thentication method	Serv- er.wlan.bintec-elm eg.com
WLAN\WLAN_users	configure 802.1X -> Specify user groups	Add

Radius configuration of access point

Field	Menu	Value
Authentication Type	System Management->Remote Au- thentication->RADIUS-> New	WLAN (802.1x)
Server IP Address	System Management->Remote Au- thentication->RADIUS-> New	e.g . 192.168.1.10

Field	Menu	Value
RADIUS Password	System Management->Remote Au- thentication->RADIUS-> New	e.g. supersecret

WLAN configuration of the access point

Field	Menu	Value
Operation Mode	Wireless LAN -> WLAN -> Radio Settings->	Access-Point / Bridge Link Master
Operation Band	Wireless LAN -> WLAN -> Radio Settings->	2.4GHz In/Outdoor
Channel	Wireless LAN -> WLAN -> Radio Settings->	Auto
Network Name (SSID)	Wireless LAN -> WLAN -> Wireless networks (VSS) ->New	e.g. workshop
Security mode	Wireless LAN -> WLAN -> Wireless networks (VSS) ->New	WPA Enterprise
WPA Mode	Wireless LAN -> WLAN -> Wireless networks (VSS) ->New	WPA and WPA 2
WPA Cipher	Wireless LAN -> WLAN -> Wireless networks (VSS) ->New	AES and TKIP
WPA2 Cipher	Wireless LAN -> WLAN -> Wireless networks (VSS) ->New	AES and TKIP

Connection of a Windows 7 WLAN client

Field	Menu	Value
Certification authority certificate download	Explorer 192.168.1.10	Enable
Certification authority certificate	Explorer 192.168.1.10	Current (WorkshopWLANCA)
Certificate	Explorer 192.168.1.10	Install certificate
Certificate memory	Explorer 192.168.1.10	Save all certificates in the following memory

Configuration of the Windows 7 WLAN client

Field	Menu	Value
Wireless connection	Manage wireless network connec- tion	Add
Network Name	Manage wireless network connec-	e.g. workshop

Field	Menu	Value
	tion	
Safety type	Manage wireless network connec- tion	WPA2 Enterprise
Encryption type	Manage wireless network connec- tion	AES
Modify connection set- tings	Manage wireless network connec- tion	Enable
Select authentication method	Manage wireless network connec- tion	Secure password (EAP-MSCHAP v2)

Chapter 4 WLAN - Bintec WLAN Controller Introduction

4.1 Functional overview

The **bintec WLAN Controller** offers the following advantages for an easier management of your WLAN infrastructure:

- · Wizard-guided quick installation in five steps
- · Automatic recognition and installation of new devices
- · VLAN and Multi SSID support
- Integrated 802.11abgn support
- Optimised roaming characteristics for VoWLAN
- · Centralised management of all Access Points:
 - · Easy modification of settings for all APs
 - · Any modification, e.g. of the SSIDs, immediately applies to all APs
- · Access Points installed at public locations no longer are a security risk:
 - Network keys and passwords are not saved on the AP and hence cannot fall into unauthorised hands through AP theft
 - · Any direct AP (configuration) access is blocked by the WLAN controller
- Automated frequency management:
 - Integrated channel plan, for non-overlapping frequency assignment
 - · Interference reduction through intelligent frequency assignment
 - Consideration of foreign access points (neighbor APs)
- Monitoring:
 - Access point operation
 - Client activity
 - · Recognition and display of undesired access points (neighbor access points)
- E-mail Alert in case of failure of a managed access points
- · Scheduler based actions (e.g. overnight shutdown of the WLAN)
- Configuration Management: The configuration is centrally saved and automatically reassigned to APs, e.g. after loss of power.
- Centralised firmware updates

4.2 Project planning

4.2.1 Determining customer requirements

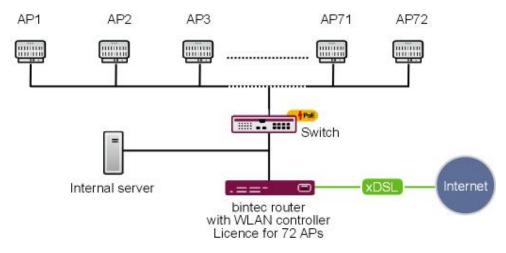
It all starts with the customers - and determining what their needs really are. In most cases customers want a WLAN network in the 2.4 GHz frequency range, allowing employees and visitors wireless connection to the company network and the Internet throughout offices and meeting rooms. Next the question arises of whether a radio frequency site survey by a specialist needs to be performed. Because of the considerable expense involved, the radio frequency site survey is frequently skipped; instead the APs are positioned at customer discretion and in consideration of the facility's spatial arrangement.

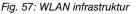
However in case of complex buildings or if the customer requires a high-performance network with continuous coverage and VoWLAN-readiness, a radio frequency site survey is indispensable.

4.2.2 Recommended hardware installation on site

Next an electrician comes into play to install the access points in corridors and offices. If doing without a radio frequency site survey, APs should be mounted at a distance of 15-20 meters to each other: this rule usually results in a functional setup.

All APs should be connected to a PoE-capable switch over an Ethernet cable. Power supply via the Ethernet cable (PoE) avoids installation of a 230 V socket and considerably simplifies setup.





The electrician should document the locations and MAC addresses of the devices so that names or locations can later be assigned to the devices during configuration.

4.3 System requirements

4.3.1 WLAN Controller hardware

The following devices with firmware versions 10.1.21 or higher can be used as WLAN controllers (supported devices with firmware versions lower than 10.1.21 need to be updated before installation):

- bintec Access Points (W1001n, W1003n, W2003ac/ext, W2022 ac/ext., WI1003n, W01003ac, W02003ac)
- bintec Medium Router (RS123 series, RS353 series)
- bintec be.IP , be.IP plus
- bintec RXL12100: central router, high-performance multiplex VPN gateway
- bintec RXL12500: central router, high-performance central site VPN gateway

For small installations up to 6 access points no dedicated WLAN controller hardware is needed and one of the access points (running as master access point) can take on the function of the WLAN controller. If a WLAN network with more than 6 access points is desired, at mimimum a R1202 is necessary as WLAN controller hardware.

4.3.2 Access Point hardware

The WLAN controller can manage the Access Points with software version 10.1.21.

4.3.3 WLAN Controller software licences

For testing purposes, the WLAN controller is already activated in the firmware of every supported device; however, only a single access point can be managed. For business operation a WLAN controller licence must be installed on the controller.

The WLAN controller licenses can be found on our homepage at *ht-tps://www.bintec-elmeg.com/service-support/produkt-lizenzierung/*

4.4 Network configuration

4.4.1 WLAN Controller device network settings

Before connecting the WLAN controller device to the network of the (still unconfigured) access points it needs to have its IP address and network settings (different from factory defaults) configured according to the setup of your local network. Otherwise the next steps will fail.

4.4.2 DHCP server

4.4.2.1 Internal DHCP server

If there is no active DHCP server in your network, and if the WLAN controller device will also act as DHCP server (internal DHCP server) you can directly proceed with *WLAN rol-lout with the WLAN controller wizard* on page 105 and start the WLAN rollout. The WLAN controller wizard includes the setup of all necessary DHCP server settings.

4.4.2.2 External DHCP server

For the access points to be manageable by the WLAN controller they must know the IP address of the WLAN controller. So in addition to the required basic network settings such as device IP address, default gateway and nameserver, the DHCP server needs to provide the access point with the IP address of the WLAN controller. This is done via option 138 of the DHCP protocol. This option (also named CAPWAP Access Controller) must, therefore, be enabled on the DHCP server, and the IP address of the WLAN controller (which you configured in chapter 4.1) must be specified. In case:

• Another Bintec router is operating as DHCP server:

The required configuration steps are described in the appendix.

• A Microsoft Server 2003 or Server 2008 is operating as DHCP server:

The required configuration steps are described in the appendix.

• A Linux server is operating as DHCP server:

The required configuration steps are described in the appendix.

• The router of a third-party provider is operating as DHCP server:

Please perform the configuration of DHCP option 138 according to the respective documentation.

4.4.2.3 No DHCP server - APs with static IP address settings

Occasionally, it may be necessary to operate a WLAN-controller-managed network with static IP address and network settings. Thus each access point requires the manual configuration of IP and network settings. The necessary configuration steps for all access points is described in *Appendix* on page 110.

4.5 WLAN rollout with the WLAN controller wizard

The WLAN controller wizard guides you through configuration and rollout of your WLAN network in five steps.

4.5.1 Wizard Step 1

Region		Germany
Interface		LAN_EN1-0
DHCP Server	DHCP Server O Externa	r with enabled CAPWAP option (138 Il or static
	Internal	
IP Address Rang	•	

Fig. 58: Wireless LAN Controller->Wizard->Wireless LAN Controller Wizard

Here you define certain basic characteristics of the WLAN controller:

- (1) **Region**: The region where your WLAN network is located. This setting adapts your WLAN network to the WLAN regulations of your region (e.g. permitted frequencies).
- (2) Interface: Defines over which interface the controller communicates with the APs (the

IP of this interface is the WLAN Controller IP address configured in option 138 of the DHCP server).

- (3) DHCP Server: Defines whether the Internal or an External DHCP server is used for the access points. When using the internal DHCP server, all DHCP server settings including option 138 are made automatically. You'll find information on configuring an external DHCP server in Appendix on page 110.
- (4) IP Address Range: Defines the IP address range available to the internal DHCP server.
- (5) Click on Next.

- Note

Before proceeding, please make sure that any existing external DHCP server is operative and that DHCP option 138 is enabled. If an external or internal DHCP server was already enabled at the time of AP installation, but DHCP option 138 was only subsequently enabled, the WLAN controller may fail to display the APs within your network. This can happen because the APs have already been assigned an IP address, but have not yet received the WLAN controller IP address. This can be remedied by waiting for the expiration of the DHCP lease time or by resetting the APs.

4.5.2 Wizard Step 2

Select the Radio Profile	
Use two independent radio profiles	Enabled
Radio Profile for Radio 1	2.4 GHz Radio Profile
(used for all Access Points)	
Radio Profile for Radio 2	5 GHz Radio Profile
(only for dual radio APs)	

Fig. 59: Wireless LAN Controller->Wizard->Wireless LAN Controller Wizard

Here, you define the radio profile with which the WLAN network will operate. A 2.4 GHz and a 5 GHz radio profile are available by default. Additional radio profiles can be created outside of the wizard via the **Wireless LAN Controller**->**Slave AP configuration**->**Radio Profile** menu.

Click on Next.

4.5.3 Wizard Step 3

/SS Description	Network Name (SSID)	Security	
vss-1	Assistant	WPA-PSK	

Fig. 60: Wireless LAN Controller->Wizard->Wireless LAN Controller Wizard

Here, you define which SSID/VSS shall be present in the network. One VSS is already available per default; this can be customised via the ricon. With **Add** you can can create up to seven additional VSS.

In this example, we create an additional VSS for visitor access:

Service Set Parameters		Security Settings
Network Name (SSID) Guests	/isible	Security Mode WPA-PSK •
		WPA Mode WPA and WPA 2 •
IGMP Snooping	nabled	Preshared Key
VLAN		
VLAN 🛑 E	nabled	
VLAN ID 2		

Fig. 61: Wireless LAN Controller->Wizard->Wireless LAN Controller Wizard

- (1) A Network Name (SSID) is assigned for the new VSS.
- (2) Select the Security Mode WPA-PSK.
- (3) As we do not want access to the company intranet from the guest network, a VLAN is defined for this VSS (in this example VLAN ID 2): All data from the "Guest" network will be tagged with that VLAN ID on the Ethernet (LAN).
- (4) Click on OK.



Note

VLAN ID 0 and 1 are reserved (for management VLAN) and cannot be used for any VSS.

VLAN tagging gives you the possibility to separate guest data from other data, and you can setup your network switches and/or Internet access routers in a way 'so that, e.g., all data from VLAN ID 2 and thus all guests are allowed to access the Internet but not the company intranet (please see the manual of your switch and/or router for how to configure VLAN separation there).

We now leave the VSS configuration with **OK** and return back to the VSS overview page. Before proceeding to wizard step 4 make sure that all access points that are supposed to be managed are connected to your LAN and are powered on.

4.5.4 Wizard Step 4

Manage								
Select all/								
Deselect all	Location	Device	IP Address	LAN MAC Address	Wireless Network	Radio Profile	Channel	Status
		W2003ac	10.10.10.13	BintecCo_48:69:c1	vss-1:Assistant	2.4 GHz Radio Profile		Discovered
	1:	W2005ac	10.10.10.13	Bintecco_46.69.c1	vss-2:Guests	5 GHz Radio Profile	11	Discovered

A 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. 62: Wireless LAN Controller->Wizard->Wireless LAN Controller Wizard

Now all discovered access points are displayed. By default, all defined wireless network profiles (VSS) and the previously selected radio profile are assigned to all access points. With the \checkmark symbol you can customise these standard settings and provide each device with an individual location description.

└── Note

In some cases, not all expected APs are displayed. The reason in that case is that not all APs were discovered by the WLAN controller. In this case **Back** can be used to update the display.

4.5.5 Start WLAN rollout to access points

After selecting the check box in the "Manage" field of all access points you want to use, you can launch the WLAN controller rollout and automatic frequency management with **Start**. The display now switches to a status screen indicating the WLAN controller's current activities:

			LAN MAC Address	Wireless Network Profile	Radio Profile	Channel	Status		
1:	W2003ac	10.10.10.13	BintecCo_48:69:c1	vss-1:Assistant vss-2:Guests	2.4 GHz Radio Profile 5 GHz Radio Profile	0	Oinitialising		
ogging									
Time		Message							
		Message 00:09:4F/6F/SE:7C: WTP starts configuration							

Fig. 63: Wireless LAN Controller->Wizard->Wireless LAN Controller Wizard

The configuration now is transfered sequentially to all access points. The configuration of an access point is finished and indicated with status *managed* after the best radio channel was found for it. When assigning radio channels, the WLAN controller ensures that only non-overlapping channels (e.g. 1, 6, 11) are assigned and that interference between the individual access points is kept to a minimum.

Managed access points are locked by the WLAN controller and all direct access to them is prohibited. An access point can only be locally configured after the WLAN controller released the access point.

After all access points are managed, the display changes once again and shows the final result:

	s Points						
Location	Device	IP Address	LAN MAC Address	Wireless Network Profile	Radio Profile	Channel	Status
1:	W2003ac	10.10.10.13	BintecCo_48:69:c1	vss-1:Assistant vss-2:Guests	2.4 GHz Radio Profile 5 GHz Radio Profile	11	⊘ _{Manage}
ease save t	he configuration	by pressing the "Sa	ve Configuration" Button.				
		by pressing the "Sa		New Neighbors	scan		
			ance	New Neighbor:	scan		STA

Fig. 64: Wireless LAN Controller->Wizard->Wireless LAN Controller Wizard

The configuration now needs to be saved on the WLAN controller device via the **Save configuration** button in the upper left. The access points themselves keep their current configuration in their volatile memory only and do not save it to their persistent memory. In the event of power failure, the configuration within the access points is lost and automatically re-loaded into the access point by the WLAN controller after power is restored. Keeping the configuration only in the volatile memory of the APs has the additional advantage that no sensitive access data (such as WLAN keys) can be compromised through theft of an access point installed at a public location.

After a power failure, all access points are re-initalised by the WLAN controller at once and radio management is not re-started, but the previously used channel is used instead. Thus recovery of WLAN infrastructure after power failure is much faster than the initial rollout.

Under **Configure the Alert Service for WLAN surveillance**, click **Start** to monitor your managed APs. You are taken to the **External Reporting-> Alert Service -> Alert Recipient** menu with the default setting **Event** = *Managed AP offline*. You can specify that you wish to be notified by e-mail if the *Managed AP offline* event occurs

4.6 Appendix

4.6.1 E-mail alert in case of access point failure

You can have an E-mail send from the WLAN Controller in case one of the managed access points is no longer reachable. This is especially helpful in larger and complex WLAN infrastructures where this kind of failure does not become immediately apparent. (The **notification settings** are not described here).

Add / Edit Alert Recipient	
Alert Service	E-mail
Recipient hotline@support.company.tld	
Message Compression	Enabled
Subject WLA-Status: Hotel Seeblick	
Event	Managed AP offline
Message Timeout 60	Seconds
Number of Messages 1	

Fig. 65: External Reporting-> Alert Service -> Alert Recipient

4.6.2 Configuration of a DHCP server on another Bintec router

The requirement is a Bintec router with software release 10.1.21 or higher.

First, you must define an IP address pool on the Local Services->DHCP Server-> IP Pool Configuration -> New menu.

Basic Parameters		
IP Pool Name WTPs		
P Address Range	10.10.10.10	- 10.10.10.50
DNS Server		
	Primary	
	Secondary	

Fig. 66: Local Services->DHCP Server-> IP Pool Configuration -> New

- (1) Enter any description at IP Pool Name, e. g. WTPs .
- (2) For IP Address Range, enter the first and the last IP address in the IP address pool, e. g. 10.10.10.10.10.10.50.
- (3) Confirm with OK.

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

Basic Parameters	
Interface	en1-0 v
IP Pool Name	WTPs 🔹
Pool Usage	Local
Description	

Advanced Settings:

Advanced Para	ameter		
Gateway			Use router as gateway v
Lease Time 120		Minutes	
DHCP Options	Option	Value	
	DNS Server	10.10.10.1	ĩ
	CAPWAP Controller	10.10.10.1	T
	ADD		
Vendor Specific	Information (DHCP Option 43)	
	Vendor ID	Vendor Specific Information	
	ADD VENDOR STRING	ADD VENDOR GROUP	

Fig. 68: Local Services->DHCP Server-> DHCP Configuration -> New

- (1) Select the interface over which the addresses defined in **IP Address Range** are to be assigned to DHCP clients.
- (2) Under IP Pool Name select a configured IP-Pool.
- (3) Under Advanced Settings on the DHCP Options menu add with the Add button the option *CAPWAP controller* and under Value enter the IP address of the WLAN Controller.
- (4) Confirm with **OK**.

4.6.3 Configuration of a DHCP server on Windows Server 2003/2008

First, your Windows DHCP server service must receive a basic set up, i.e. the DHCP IP address range needs to be defined, and standard options such as DNS server and standard gateway/router need to be configured according to your network infrastructure.

Фрнср				
<u>D</u> atei Ak <u>t</u> ion <u>A</u> n	sicht <u>?</u>			
$\Leftrightarrow \Rightarrow \blacksquare \textcircled{\texttt{B}}$	😫 💵 <u>.Q</u>			
P DHCP	DHCP			
i ⊡… 🔂 charon [10.1] ⊡… Bereich [Statistik anzeigen	rs	Status	
Serverop	<u>N</u> euer Bereich Neue Bereichsgr <u>u</u> ppierung Neuer <u>M</u> ulticastbereich	01]	Wird ausgeführt	
	<u>S</u> ichern <u>W</u> iederherstellen			
	Alle Bereiche abstimmen	-		
	Benutzerklassen definieren Herstellerklassen definieren Vordefinierte Optionen einstellen			
	Alle Aufgaben			
	<u>L</u> öschen A <u>k</u> tualisieren			
	Eigenschaften			
•	Hilfe			
Entfernt, ändert oder	fügt Optionen aus der vordefinierten Liste	hinzu.		

4.6.3.1 Step 1

In the DHCP service window (accessible via **Control Panel**, there under **Administration**), right-click on the existing DHCP service instance (you can identify it through the computer name and the IP address the DHCP service is linked to), then click on **Set Predefined Options** in the expanded context menu.

4.6.3.2 Step 2

LO DI	ICP		
Date	i Aktion <u>A</u> nsicht (2	
\	→ 🖪 😫 😫 [
	Vordefinierte Option	en und Werte	
⊡… [i	Optionsklasse:	DHCP-Standardoptionen Status Wird ausgeführt	
	Optionsname:	002 Zeitoffset	
		Hinzufügen	
	Beschreibung:	UCT-Offset in Sekunden	
	_ Wert		
	Lang:		
	0x0		
		OK Abbrechen	
<u> </u>			

In the window now opening, click Add to add the CAPWAP option.

4.6.3.3 Step 3

PHC 200	Р			
<u>D</u> atei	Akti	on <u>A</u> nsicht <u>?</u>		
\Leftrightarrow \Rightarrow		3 🖹 🖄 🖬	<u> </u>	
	orde	finierte Optionen	und Werte	
ſ			HCP-Standardoptionen Status Wird ausgeführt	
		optionstyp	IN2 Zaitoffeat	
		Klasse:	Global	
	Bes	<u>N</u> ame:	CAPWAP	
	FW	<u>D</u> atentyp:	IP-Adresse Agray	
	Ē	<u>C</u> ode:	138	
	l î	Beschreibung:	CAPWAP Wireless LAN Controller	
			OK Abbrechen	
			OK Abbrechen	

In the **Option Type** dialogue window, the CAPWAP option is now defined (but not yet activated). **Name** and **Description** can be freely selected, but should be plausible. Data type must be set to *IP* Address, and **Array** checked. In addition, **Code** must be set to *138*. If the code is already in use for another, self-defined DHCP option not matching the CAP-WAP DHCP option, the pre-existing one must first be deleted. Close the dialogue and the previous window by clicking **OK**.

4.6.3.4 Step 4

<u>D</u> atei Ak <u>t</u> ion <u>A</u> nsicht <u>?</u>				
← → 🗈 🖬 🖻 🗟 🔮 🖬	8			
	Bereichsoptionen			
	Optionsname	Hersteller	Wert	
Adresspool	🖑 003 Router	Standard	10.10.10.254	
Adressleases	🖑 006 DNS-Server	Standard	172.16.105.1	
🕀 🧰 Reservierungen 🤞	🖑 015 DNS-Domänenname	Standard	qa.bintec.de	
Bereichsoptin Optionen	konfigurieren			
Ansicht	•			
A <u>k</u> tualisien Liste e⊻po				
Hilfe				
	4			
Konfiguriert Bereichsoptionen.	<u> </u>			

Now, in the IP address range of the DHCP service already configured for future slave access points, right-click **Range options** and select **Configure Options** in the context menu.

Фрнср	Bereichoptionen	<u> </u>
Datei Aktion Ans	Allgemein Erweitert	
← → È II DHCP → thereich [10.10 → Bereich [1 → Adres: → C Adres: → C Adres: → C Adres: → C Adres:	Zur Verfügung stehende Optionen 075 StreetTalk-Server 076 STDA-Server (StreetTalk Directory Assistance) 138 CAPWAP 249 Statische Routen ohne Klassen	Beschreibung Auf Liste der für c Liste der für c Liste der für c CAPWAP W Ziel-, Masker V IO.254 5.105.1 tec.de
Serveropt	Dateneingabe <u>S</u> ervername: I <u>P</u> -Adresse:	Auflösen
	10.10.20 Hinzufügen Entfernen Nach oben	
	Nach unten	

4.6.3.5 Step 5

In the expanding dialogue window, select option **138** in the list of **Available Options**. In the **IP Address** entry field, enter the IP address of the WLAN controller; then, on the right, click **Add**. Theoretically, it is possible to enter several WLAN controller IP addresses here. At present, however, only the first IP address is taken into account by the Funkwerk access points. Now, also close this dialogue box by clicking **OK**.

4.6.3.6 Step 6

Фрнср			
<u>D</u> atei Ak <u>t</u> ion <u>A</u> nsicht <u>?</u>			
	1 🖑		
	Bereichsoptionen		
charon [10.10.10.201] dereich [10.10.0.0] Wireless	Optionsname	Hersteller	Wert
Adresspool	💞 003 Router	Standard	10.10.10.254
	💞 006 DNS-Server	Standard	172.16.105.1
🕀 🧰 Reservierungen	💞 015 DNS-Domänenname	Standard	qa.bintec.de
Bereichsoptionen	138 CAPWAP	Standard	10.10.10.20
Serveroptionen			
	•		► F

The DHCP service overview window should now also list the CAPWAP option. At this stage, the access points and the WLAN controller in the network for which the DHCP service ihas been configured, can go into operation.

4.6.4 Configuration of a DHCP server under Linux

In the configuration file /etc/dhcp/dhcpd.conf, add the following:

```
# Format definition of DHCP CAPWAP option for Wireless LAN Controller
option wifi-controller code 138 = array of ip-address;
# IP address range for Slave APs/WTPs<
subnet 10.10.0.0 netmask 255.255.255.0 {
range 10.10.10.10 10.10.100;
option domain-name-servers mydnsserver.mydomain.tld;
option routers 10.10.10.1;
option broadcast-address 10.10.10.255;
default-lease-time 600;
max-lease-time 7200;
# IP address of Wireless LAN Controller
option wifi-controller 10.10.10.5;
}
```

The lines beginning with **option wifi-controller** are the most crucial ones. The first line defines the data format of option 138, as it is not contained in the standard format definitions of the dhcpd. The second line specifies the IP address of the WLAN controller to which the individual slave AP's log in after they have received all data (own IP address, WLAN controller IP, etc.) from the DHCP server.

Any other information is standard for the definition of a DHCP pool: **subnet**, **range**, **do-main-name-servers**, **routers** etc. need to be configured according to the customer's own requirements.

Once the configuration file is saved, restart the DHCP server with the command / etc/init.d/dhcp-server restart.

4.6.5 Operation of APs with static IP address settings

As described in *DHCP server* on page 104 the DHCP server not only assigns IP addresses but also provides the access points to be managed with the IP address of the WLAN Controller. In case of static IP address settings for access points it is necessary not only to specify an IP address and a netmask at each access point that is to be managed, but also to manually specify the IP address of the WLAN controller. You can find the necessary configuration parameter in the menu **System Management->Global Settings->System** page:

Basic Settings		
System Name w2003ac		
Location		
Contact BINTECELMEG		
Maximum Number of Syslog Entries 50		
Maximum Message Level of Syslog Entries		Information •
Maximum Number of Accounting Log Entries		
NetManager communication	-	Enabled
NetManager address https://discover.networkcloudmanager.com		
LED mode		Status 🔻
Manual WLAN Controller IP Address 10.10.1		
Show Manufacturer Names	-	Enabled
Autosave Configuration		

Fig. 69: System Management->Global Settings->System

When starting the WLAN controller wizard, it is essential to choose **Extern** for DHCP Server in WLAN controller wizard step 1.

4.7 Overview of configuration steps

Feld	Menü	Wert
Region	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard ->Step 1	e.g. Germany
Interface	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard ->Step 1	e.g. . <i>LAN_EN1-0</i>
DHCP Server	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard ->Step 1	e.g. Internal
IP Address Range	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard ->Step 1	e.g. 10.10.10.10 - 10.10.10.50

Wireless	network	installation:	Step 1
----------	---------	---------------	--------

Wireless network installation: Step 2

Feld	Menü	Wert
Radio Profile for Radio 1	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard ->Step 2	e.g. 2,4 GHz Radio Profile
Radio Profile for Radio 2	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard ->Step 2	e.g. 5 GHz Radio Profile

Wireless network installation: Step 3

Feld	Menü	Wert
Network Name (SSID)	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard ->Step 3	e.g. Assistent
Network Name (SSID)	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard ->Step 3 ->Hinzufügen	e.g. Guests
Security Mode	Wireless LAN Controller -> Wizard	WPA-PSK

Feld	Menü	Wert
	-> Wireless LAN Controller Wizard ->Step 3 ->Hinzufügen	
Preshared Key	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard ->Step 3 ->Hinzufügen	e.g. supersecret
VLAN	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard ->Step 3 ->Hinzufügen	Enabled
VLAN ID	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard ->Step 3 ->Hinzufügen	e.g. 2

Wireless network installation: Step 4

Feld	Menü	Wert
Select device	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard ->Step 4	Enabled
Configure the Alert Service for WLAN sur- veillance	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard ->Step 4	START

E-mail alert

Feld	Menü	Wert
Recipient	External Reporting-> Alert Service -> Alert Recipient	e.g .hot- line@support.compa ny.ltd
Subject	External Reporting-> Alert Service -> Alert Recipient	e.g . <i>WLAN-Status:</i> <i>Hotel Seebliick</i>
Event	External Reporting-> Alert Service -> Alert Recipient	Managed AP offline

Configuration of a DHCP server on another router

Feld	Menü	Wert
IP-Pool Name	Local Services->DHCP Server-> IP Pool Configuration -> New	e.g WTPs
IP Address Range	Local Services->DHCP Server-> IP Pool Configuration -> New	e.g. 10.10.10.10 - 10.10.10.50
Interface	Local Services->DHCP Server-> DHCP Configuration -> New	e.g. en1-0

Feld	Menü	Wert
IP Pool Name	Local Services->DHCP Server-> DHCP Configuration -> New	e.g. WTPs
Pool Usage	Local Services->DHCP Server-> DHCP Configuration -> New	Local
DHCP Options	Local Services->DHCP Server-> DHCP Configuration -> New ->Ad- vanced Settings	Option <i>CAPWAP</i> Con- troller, Value e.g . 10.10.10.1

Operation with static IP address

Feld	Menü	Wert
Manual WLAN Control- ler IP Address	System Management->Global Set- tings->System	e.g. 10.10.10.1

Chapter 5 WLAN - VoWLAN Basics and Configuration

5.1 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**.

5.2 WLAN infrastructure

5.2.1 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).

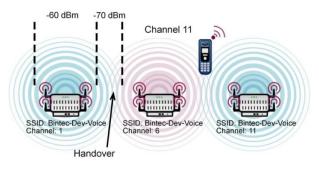


Fig. 70: List of minimum requirements for the WLAN radio frequency site survey for VoWLAN

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.

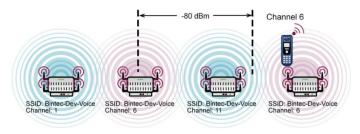


Fig. 71: Minimum space between two WLAN access points on the same transmit channel

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. 72: Typical result of a site survey

5.2.2 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.

5.2.3 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
802.11bg	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.

5.2.4 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.

5.2.5 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.

5.2.5.1 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.

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)

Mapping table based on 802.11e

The access points (**bintec W2003ac-ext**, **bintec W1003n**) 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	ВК	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		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.

5.2.5.2 U-APSD (Unscheduled Automatic Power Save Delivery)

U-APSD is a part of 802.11e and helps considerably in increasing the battery life of VoW-LAN 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 W11003n**) upwards of relay 10.1.609.

5.2.6 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.

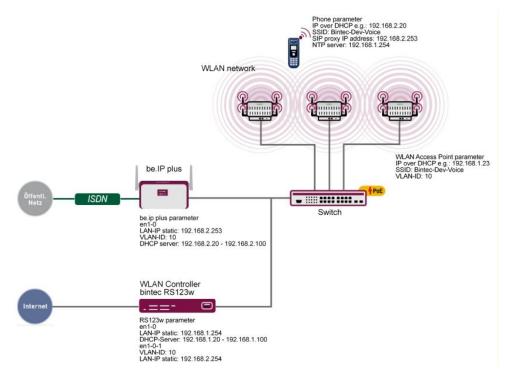
The **bintec WLAN Controller** solution works with mit intelligent access points (fat APs) that manage the basic data locally. This scenario has considerable performance benefits in comparison with thin client solutions. The **bintec WLAN Controller** is not obligatory for a VoWLAN installation, but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

5.2.7 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 tranmission 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 VoW-LAN 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.

5.3 Example configuration



5.3.1 Network plan

Fig. 73: 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.

5.3.2 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 GUIGUIGUI (Graphical Unit Interface) is used to do the configuration.

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

Radio Profile Definition		Performance Settings	
	_	Wireless Mode	802.11g/n 🔻
Description		Number of Spatial Streams	2 •
Operation Mode	Access Point •	Airtime fairness	Enabled
Operation Band	2.4 GHz In/Outdoor V	Cyclic Background Scanning	Enabled

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

Fig. 74: 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.

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

Fig. 75: 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**.

5.4 Ascom i62 Talker configuration

5.4.1 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

5.4.2 Configuration

5.4.2.1 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.

	rs Templates Licer	icense Options He				
Devices Number	rs Templates Licer	ises				
New Edit Dele	K					
Device types:	Search for:		in: Number	✓ Show all		
All)	Number	Device type	Parameter	version Device ID	Online	Status
52 Talker	1011	i62 Talker	13.3			Synchronized
	2011	i62 Talker	13.3	00013E11AF25	~	Synchronized
			New numbers	i62 Talker 🗸		
		D	evice type: arameter version:	162 Talker •		
		D	evice type: arameter version:	i62 Talker 👻		
		D P T T	evice type: arameter version: emplate: Prefix: Single Call nu	l62 Taker		

Fig. 76: Numbers -> New

Define a network

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

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

Device type:	i62 Talke	r		
Parameter version:	: 13.3			
Network		Name	Value	
Network		Network name	Bintec-Dev-Voice	0
Network	(C	DHCP mode 802.11 protocol	Enable 802.11b/g/n	0
Network	(D	ISSID	Bintec-Dev-Voice	0
⊡} Device ♦ Settings		Security mode WPA-PSK passphrase	WPA-PSK & WPA2-PSK	00
General General Message		Voice power save mode 802.11b/g/n channels	U-APSD 1,6,11	0
+ Audio		Advanced: 802.11 channels World mode regulatory domain Transmission power	ETSI Automatic	000
Location VoIP		IP DSCP for voice	0x2E (46) - Expedited Forwar	
General		IP DSCP for signalling	0x2E (46) - Expedited Forwar	2
H.323 SIP Headset Profiles Shortcuts		TSPEC Call Admission Control Transmit gratuitous ARP	Disable Disable	0
			OK Cance	el

Fig. 77: 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.

Parameter version: 13.3 Network Network A Name Value Automatic key lock Disable Phone lock Off User display text H.D.Wahl Active network B Phone lock Network B Brightness Normal Language Gernan
Network A Network B Network B Network C Network C
General G

Fig. 78: 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.

🖃 🌗 Network	Name	Value	
Network A Network B Network C Network C Network C Settings General Other Vilte Nessage centre Audio Presence Source Vilte Nessage centre Nessage centre Shortcuts	Max number of call completions Emergency number Dial pause time Time zone Backlight timeout Administration password Replace Call Rejected with Us NTP server Software TIFT IP address Shared phone license Block switch off Syslog Direct off hook from charger Clear lists in charger	10 1 Central European Time (GMT+1) 20 admin ********* Disable 192.168.1.254 0.0.0.0 No No Off No Off No No No	8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8

Fig. 79: 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.

	i62 Talker			
Parameter version:	13.3			
Network		Name	Value	
Network		/oIP protocol	SIP	0
 Network 	-	Codec configuration	G.711 A-law	2
 Network Network 	- /	Codec packetization time confi	20	0
	U I	nternal call number length	0	0
Device	E	Endpoint number	2011	2
Settings	E	Endpoint ID		0
General				
Presence Common Ontroit Location				

Fig. 80: 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 can- not be modified here. The number is spe- cified when the device's parameter set is generated.

SIP configuration

Go to VoIP -> SIP.

Parameter version:	13.3			
∃]) Network	. 1	Name	Value	
Network		SIP proxy IP address	192.168.2.253	0
Network	-	Secondary SIP proxy IP address	0.0.0	0
Network	- II	SIP proxy listening port	5060	0
Device		SIP proxy ID		8
Settings		SIP proxy password	********	8
General		Send DTMF using RFC 2833 or	RFC2833	8
		Hold type	Inactive	0
Message	contro	Registration identity	Endpoint number	0
	centre	Authentication identity	Endpoint number	8
Audio		Call forward locally	Disabled	0
General		MOH locally	Enabled	8
		Hold on Transfer	Disabled	8
Common		Direct signaling	Disabled	8
Netwise				
Common				
Ekahau				
General				
+ H.323				
SIP				
Headset				
Profiles				
in the mes				
+ Shortcuts				

Fig. 81: 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)

5.4.3 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

5.5 Configuring the elmeg hybird 300

5.5.1 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	O Untrusted 🖲 Trusted
Interface Mode	O Untagged (VLAN)	Address Mode	● Static ○ DHCP
VLAN ID 10		IP Address / Netmask	
MAC Address 00:a0:f9	Use built-in	IP Address ADD	Netmask

Fig. 82: 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**.

5.5.2 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.

Internal Number	10 (Benutzer 1 a/b1 Tel)
Type of Call Forwar	On busy / On no reply 🔻
Target Number (On Enter Target Number without	
	Target Number (On busy)
	123456789
Target Number (On	123456789
Target Number (On Enter Target Number without	123456789



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.

5.6 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

5.7 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 Net- works (VSS) -> New	e.g. Bintec- Dev-Voice
Intra-cell Repeating	Wireless LAN Controller -> Slave AP Configuration -> Wireless Net- works (VSS) -> New	Disabled
Security mode	Wireless LAN Controller -> Slave AP Configuration -> Wireless Net- works (VSS) -> New	WPA-PSK
WPA Mode	Wireless LAN Controller -> Slave AP Configuration -> Wireless Net- works (VSS) -> New	WPA2

Action	Menu	Value
WPA2 Cipher	Wireless LAN Controller -> Slave AP Configuration -> Wireless Net- works (VSS) -> New	AES and TKIP enabled
Preshared key	Wireless LAN Controller -> Slave AP Configuration -> Wireless Net- works (VSS) -> New	e.g. supersecret
ACL Mode	Wireless LAN Controller -> Slave AP Configuration -> Wireless Net- works (VSS) -> New	Disabled
VLAN ID	Wireless LAN Controller -> Slave AP Configuration -> Wireless Net- works (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. Bintec- Dev-Voice
Security mode	Network -> Network B	WPA-PSK & WPA2-PSK
WPA-PSK passphase	Network -> Network B	e.g. supersecret
Voice power save mode	Network -> Network B	U-APSD
802.11b/g/n channels	Network -> Network B	1,6,11
IP DSCP for voice = 0x2E (46)	Network -> Network B	0x2E (46)
IP DSCP for signaling = 0x2E (46)	Network -> Network B	0x2E (46)
User display text	Device -> Settings	e.g.bintec elmeg
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. supersecret

Field	Menu	Value
Authentication identity	VoIP -> SIP	Endpoint number

Configure interface

Field	Menu	Value
Based on Ethernet In- terface	LAN -> IP Configuration ->Inter- faces -> New	e.g. en1-4
Interface Mode	LAN -> IP Configuration ->Inter- faces -> New	Tagged (VLAN)
VLAN ID	LAN -> IP Configuration ->Inter- faces -> New	10

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	On busy/On no reply
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 6 WLAN Management for Multiple Locations: WLAN controller via VPN

6.1 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.

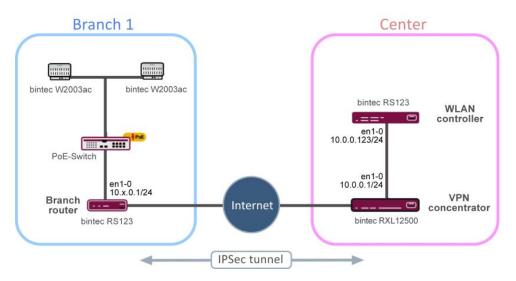


Fig. 84: Example scenario

6.1.1 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 W11003n 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).

6.1.2 About the test setup

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

Router	Interface	Description	IP address / ad- dress 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 ac- cess 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 / ad- dress range
head office		WLAN controller which must be ac- cessible 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	

6.2 Configuration

6.2.1 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.

6.2.2 Configure the router in the field office

6.2.2.1 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> >.

Basic Parameters			Basic IPv4 Parame	eters		
Interface Mode	 Untag 	gged O Tagged (VLAN)	Security Policy		O Untr	rusted 🔘 Trusted
MAC Address	00:09:4f:6f:5e:80	Use built-in	Address Mode		(Static 🔿 DHCP
00.08.41.01.02.00	_ Use built-in	IP Address / Netma	sk			
			IP Addre	55	Netmask	
			10.1.0.	1	255.255.255.0	Î
			ADD			

Fig. 85: 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**.

6.2.2.2 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.

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

Basic Parameters		
IP Pool Name Devices		
IP Address Range	10.1.0.10	- 10.1.0.254
DNS Server		
	Primary	
	Secondary	(

Fig. 86: 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.

Basic Parameters	
Interface	en1-0 v
IP Pool Name	Devices
Pool Usage	Local
Description	

			Advanced Settings:	
Advanced Parar	neter			
Gateway				Use router as gateway •
Lease Time 120		Minutes		
DHCP Options	Option		Value	
	DNS Server	T	10.1.0.1	î
	CAPWAP Controller	.▼	10.0.0.123	î
	ADD			
Vendor Specific Ir	nformation (DHCP Option 4	3)		
	Vendor ID	N	endor Specific Information	
	ADD VENDOR STRING	ADD VENDOR GR	OUP	

Fig. 88: 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**.

6.2.3 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> .

Basic Parameters		Basic IPv4 Parameters	
Interface Mode	O Tagged (VLAN)	Security Policy	O Untrusted () Trusted
MAC Address	00:09:4f.6f.5e:80 Use built-in	Address Mode	● Static ○ DHCP
		IP Address 10.0.0.1	Netmask 255 255 255 0
		ADD	

Fig. 89: 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.

6.2.4 Configure the WLAN controller at head office

6.2.4.1 IP configuration

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

(1) Go to LAN -> IP Configuration ->Interfaces -> <en1-0> \checkmark .

Basic Parameters		Basic II	Pv4 Parameters	
Interface Mode	 Untagged O Tagged (VLAN) 	Security	y Policy	🔿 Untrusted 🖲 Trusted
MAC Address	00:09:4f:6f:5e:80 Use built-in	Addres:	s Mode ess / Netmask IP Address 10.0.0.123 ADD	Static O DHCP Netmask 255 255 . 255 . 0

Fig. 90: 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.

6.2.4.2 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 •	
Route Class	● Standard ○ Extended	Metric 1 •

Fig. 91: 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								
Destination IP Address	Netmask	Gateway	Interface	Metric	Route Type	Extended Route		
0.0.0.0	0.0.0.0	10.0.0.1	LAN_EN1-0	1	Default Route via Interface		Î	1
10.0.0.0	255.255.255.0	10.0.0.151	LAN_EN1-0	0	Network Route via Interface		Î	1

Fig. 92: 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**.

6.2.4.3 Configure WLAN controller

The WLAN controller itself can be activated now.

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

Basic Settings	
Status	Enabled
Region	Germany
Interface	LAN_EN1-0 V
DHCP Server	DHCP Server with enabled CAPWAP option (138):
Slave AP location	Local (LAN)Remote (WAN)
Slave AP LED mode	Status 🔻

Fig. 93: 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.

6.2.4.4 Configure wireless network profile

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

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

To do this, for the existing entry $\langle vss-1 \rangle$ click the \checkmark symbol.

Service Set Parameters		Security Settings	
Network Name (SSID) Staff	Visible	Security Mode	WPA-PSK •
		WPA Mode	WPA and WPA 2 🔻
Intra-cell Repeating	Enabled	WPA Cipher	O AES TKIP O AES and TKIP
U-APSD		WPA2 Cipher	AES O TKIP O AES and TKIF
IGMP Snooping	Enabled	Preshared Key	
Client load balancing		MAC-Filter	
Max. number of clients - hard limit 32		Access Control	
02		Dynamic blacklisting	Enabled
Max. number of clients - soft limit 24		Failed attempts per Time	10 / 60 Seconds
Client Band select Disabled - c	optimized for fast roaming ▼	Blacklist blocktime 500	Seconds

Fig. 94: 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**.

6.2.4.5 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 \checkmark symbol.

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

Advanced Se	ettings
-------------	---------

Channel Plan		User defined •
User Defined Channel Plan		
Channel		
1. •		
5 •		
9 •	Î	I
13 🔻		
ADD		
Beacon Period	100	m
DTIM Period 2		
RTS Threshold 2347		
Short Guard Interval	-	Enabled
Max. Transmission Rate		Auto 🔻
Short Retry Limit 7		
Long Retry Limit		
4		

Fig. 96: 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.

6.2.4.6 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«.

Go to Wireless LAN Controller -> Slave AP Configuration-> Slave Access Points

Access Point Settings		Radio N	Nodule1		
Device	W2003ac	Operatio	on Mode		◉ On ⊖ Off
Location Nbg - Shop		Active R	adio Profile		2.4 GHz Radio Profile •
nug - Shop		Channel	I		Auto 🔻
Name W2003ac		Used Ch	annel		6
Description		Transmi	it Power		Max. 🔻
Marketing		Assigner	d Wireless Network (VSS)		
CAPWAP Encryption	Enabled		Profil	MAC Address	
			vss-1:Staff	00:a0:f9:0b:cf:e0	

Fig. 97: Wireless LAN Controller -> Slave-AP Configuration -> Slave Access Points

Proceed as follows:

- 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 Pont is to be managed by the WLAN Controller by clicking the \checkmark button or the \checkmark button in the **Action** column.

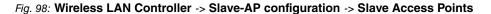
You can disconnect the Access Point from the WLAN Controller and therefore remove it from your WLAN infrastructure by click on the v button. The Access Point then receives the *Discovered* status, but is no longer *Managed*.

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 triggeri 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.

ocation *	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)	G	Managed	~ ~	Î	
Nbg - Back office	W2003ac	10.1.0.13	00:01:cd:0e:58:1a	9 HT20 (auto)	C	Managed	~ ~	Î	
Nbg - Warehouse	W2003ac	10.1.0.12	00:01:cd:0e:b3:d0	5 HT20 (auto)	C	Managed	~ ~	Ĩ	
Nbg - Show room	W2003ac	10.1.0.10	00:01:cd:0e:8e:fa	1 HT20 (auto)	C	Managed	~ ~		

The list of configured access points now looks like this:



6.2.4.7 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.

Basic Parameters	E-mail Parameters
Alert Service Enabled	Sender E-mail Address wic@it.company.tld
	SMTP Server smtp.mail.com
	SMTP Port 25 SSL
	SMTP Authentication None O ESMTP O SMTP after POP

Fig. 99: 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.

	E-mail
	Enabled
	Managed AP offline
Seconds	
	Seconds

Fig. 100: 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**.

6.3 Overview of Configuration Steps

Configure the router in the field office - IP configuration	on
---	----

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

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

Configure the VPN concentrator at head office

Configure the WLAN controller at head office - IP configuration

Field	Menu	Value
Address mode	LAN -> IP Configuration-> Inter- faces -> <en1-0></en1-0>	Static
IP Address / Netmask	LAN -> IP Configuration-> Inter- faces -> <en1-0></en1-0>	IP Address: e.g. 10.0.0.123 Netmask: e.g. 255.255.255.0
Interface Mode	LAN -> IP Configuration-> Inter- faces -> <en1-0></en1-0>	Untagged:
MAC address	LAN -> IP Configuration-> Inter- faces -> <en1-0></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 -> Con- troller Configuration -> General	e.g. Germany
Interface	Wireless LAN Controller -> Con- troller Configuration-> General	LAN_EN1-0
DHCP Server	Wireless LAN Controller -> Con- troller Configuration-> General	External or static
Slave AP location	Wireless LAN Controller -> Con- troller Configuration-> General	Remote (WAN)

Configure the WLAN controller at head office - wireless network profile

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

Field	Menu	Value
WPA2 Cipher	Wireless LAN Controller ->Slave AP Configuration ->Wireless Net- works (VSS)	AES
Preshared key	Wireless LAN Controller ->Slave AP Configuration ->Wireless Net- works (VSS)	String with 8 - 63 char- acters
ACL Mode	Wireless LAN Controller ->Slave AP Configuration ->Wireless Net- works (VSS)	Disabled
Allowed Addresses	Wireless LAN Controller ->Slave AP Configuration ->Wireless Net- works (VSS)	None
VLAN	Wireless LAN Controller ->Slave AP Configuration ->Wireless Net- works (VSS)	Disabled

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. 2.4 GHz Radio Profile
Operation Mode	Wireless LAN Controller -> Slave AP Configuration-> Radio Profiles- > 2.4 GHz Radio Profile>	Access Point
Operation Band	Wireless LAN Controller -> Slave AP Configuration-> Radio Profiles- > 2.4 GHz Radio Profile>	2.4 GFz In / Out- door
Number of Spatial Streams	Wireless LAN Controller -> Slave AP Configuration-> Radio Profiles- > 2.4 GHz Radio Profile>	2
Wireless Mode	Wireless LAN Controller -> Slave AP Configuration-> Radio Profiles- > 2.4 GHz Radio Profile>	802.11 g/n
Max. Transmission Rate	Wireless LAN Controller -> Slave AP Configuration-> Radio Profiles- > 2.4 GHz Radio Profile>	Auto
Burst Mode	Wireless LAN Controller -> Slave AP Configuration-> Radio Profiles-	Enabled

Field	Menu	Value
	> 2.4 GHz Radio Profile> 🇨	
Channel plan	Wireless LAN Controller -> Slave AP Configuration-> Radio Profiles- > 2.4 GHz Radio Profile>	User-defined
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 rofiles	Enabled
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 rofiles	4
Fragmentation Threshold	Wireless LAN Controller ->Slave AP Configuration -> Radio Profiles- > 2.4 GHz Radio rofiles	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. Nbg - Shop
CAPWAP Encryption	Wireless LAN Controller -> Slave AP Configuration-> Slave Access Points	Enabled

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 net- works (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. ad- min@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. WLAN status: branches
Event	External Reporting -> Alert Service -> Alert Recipient -> New	Managed AP offline
Message Timeout	External Reporting -> Alert Service -> Alert Recipient -> New	e. g. 60
Number of Messages	External Reporting -> Alert Service -> Alert Recipient -> New	e.g. 1

Chapter 7 WLAN - Wireless LAN Controller as Network Access Gateway

7.1 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.

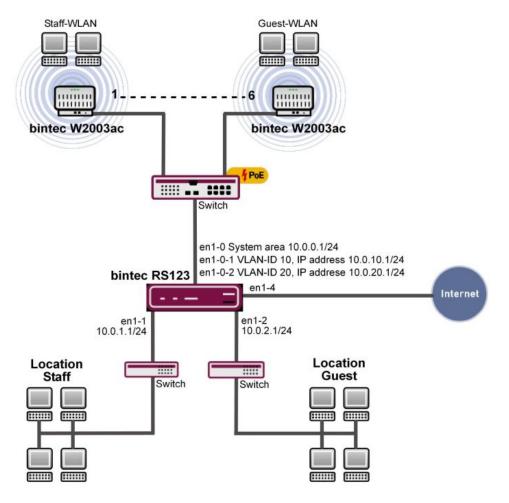


Fig. 101: Example scenario

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 WIx0xxn 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 em- ployee 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 em- ployee 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

7.2 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.

tomatic Refresh	Interval 60 Seconds APPLY			
Switch Port	Ethernet Interface Selection	Configured Speed / Mode	Current Speed / Mode	Flow Control
1	en1-0 ▼	Full Autonegotiation	100 mbps / Full Duplex	Disabled v
2	en1-1 ▼	Full Autonegotiation	Down	Disabled •
3	en1-2 ¥	Full Autonegotiation	Down	Disabled •
4	en1-3 V	Full Autonegotiation	Down	Disabled •
5	en1-4 🔻	Full Autonegotiation	Down	Disabled •

Fig. 102: Physical Interfaces -> Ethernet Ports -> Port Configuration

Proceed as follows to assign the ports to the interfaces:

- 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.

Select the physical Ethernet port the external gateway / cable modern is connected to:	Select your Internet Service Provider (ISP) from the list:			
connected to.		Internet Service Provider	User-defined 🔻	
Physical Ethernet Port	ETH5 V			
Are the IP parameters obtained dynamically?	9	Enter the IP settings of your Internet access:	?	
IP parameters obtained dynamically		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	
		DNS Server 2	0.0.0.0	

Fig. 103: 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. 255.255.25.0.
- (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.

L___ Note

This interface is not to be confused with the (underlying) *ethoa* 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.

```
 Go to LAN -> IP Configuration -> Interfaces -> .
```

Basic Parameters		Basic IPv4 Parameters			
Interface Mode	 Untagged O Tagged (VLAN) 	Security Policy O Untrusted			
MAC Address	00:09:4f:6f:5e:80 Use built-in	Address Mode Static O DHCP IP Address / Netmask IP Address Netmask 10.0.1 255 255 255 0 ADD			

Fig. 104: 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.

Basic Parameters			Basic IPv4 Parameters		
Based on Ethernet Interface		en1-0 🔻	Security	/ Policy	○ Untrusted ● Trusted
Interface Mode	O Untagged (Tagged (VLAN)	Address	s Mode	● Static ○ DHCP
VLAN ID 10			IP Addr	ess / Netmask	
MAC Address	00:a0:f9	Use built-in		IP Address 10.0.10.1	Netmask 255.255.255.0
				ADD	

Fig. 105: 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:

nterface	IPv4 Address/Netmask	IPv6 Address/Length	Status	Action			
en1-0	10.0.0.1/255.255.255.0	-	0	~ ~		1	Q
en1-4	1.2.3.4/255.255.255.0		0	~ ~		1	Q
en1-1	10.0.1.1/255.255.255.0		0	~ ~		1	Q
m1-2	10.0.2.1/255.255.255.0	<u>.</u>	0	~ ~		1	Q
en1-3	Not configured/Not configured		8	~ ~	Î	1	۹
thoa35-5	Not configured/Not configured		0	~ ~		1	Q
n1-0-1(VLAN-ID10)	10.0.10.1/255.255.255.0		Ø	~ ~		1	Q

Fig. 106: 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.

- Access SSH HTTP HTTPS SNMP Interface Telnet Ping en1-0 en1-4 en1-1 en1-2 en1-3 en1-0-1 en1-0-2 br0
- (1) Go to System Management -> Administrative Access -> Access .

Fig. 107: System Management -> Administrative Access -> Access

Proceed as follows:

- (1) For the Interface en1-0, select the router's configuration services *Telnet*, *SSH*, *HT*-*TP*, *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 Pa	rameters	
Descriptic Local-S	ervices	
Member	s	
	Service	Selection
	activity	
	ah	
	any	
	clients_1	
	clients_2	
	daytime	
	dhcp	•
	discard	
	dns	•
	echo-req	••
	echo-req-ipv6	
	esp	

Fig. 108: 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	Add	dress / Subnet 🔘 Address Range
Address / Subnet	255.255.255.255	/ 255.255.255.255
IPv6		Disabled

Fig. 109: 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.

L 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	î	1
Broadcast	255.255.255/32		Ť.	1
Staff-LAN-GW	10.0.1.1/32		Î	1
Guest-LAN-GW	10.0.2.1/32		ĩ	1
Staff-WLAN-GW	10.0.10.1/32		ĩ	1
Guest-WLAN-GW	10.0.20.1/32		Î	1

Fig. 110: 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	
Descrij Staff	otion	
Memb	ers	
	Interface	Selection
	LOCAL	
	LAN_EN1-0	
	LAN_EN1-5	
	LAN_EN1-1	-
	LAN_EN1-2	
	LAN_EN1-3	
	LAN_EN1-4	
	LEASED_EN1-0-1	-
	LEASED_EN1-0-2	

Fig. 111: 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	Î	1
Guests	LAN_EN1-2, LEASED_EN1-0-2	Î	1
Users	LAN_ENI-1, LAN_ENI-2, LEASED_ENI-0-1, LEASED_EN1-0-2	ĩ	1

Fig. 112: 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. 113: 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. 114: 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**.

ilter Rule									
Order	Source	Destination	Service	Action	Policy active				
1	LAN_EN1-4	ANY	any	Access	Enabled	†↓	=+	I	1
2	Staff	Users	any	Access	Enabled	ţ	≡+	Î	1
3	Guests	Guests	any	Access	Enabled	t↓	=+	T	1
4	Users	LAN_EN1-4	any	Access	Enabled	†↓	=+	Î	1
5	Users	Broadcast	Local-Services	Access	Enabled	†Ļ	=+	Ĩ	1
6	LAN_EN1-1	Staff-LAN-GW	Local-Services	Access	Enabled	ţ	=+	Ī	1
7	LAN_EN1-2	Guest-LAN-GW	Local-Services	Access	Enabled	†Ļ	≡+	T	1
8	LEASED_EN1-0-1	Staff-WLAN-GW	Local-Services	Access	Enabled	†↓	≡+	T	1
9	LEASED EN1-0-2	Guest-WLAN-GW	Local-Services	Access	Enabled	† _⊥	≡+		1

The list of configured filter rules now looks like this:

Fig. 115: 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 = N1-4) 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	Enabled	UDP Inactivity 180	Seconds
Logged Actions	All 🔻		
IPv4 Full Filtering	Enable	TCP Inactivity 3600	Seconds
STUN Handler	()))	PPTP Inactivity	
		86400	Seconds
		Other Inactivity	
		30	Seconds

Fig. 116: 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.

	20			
IP Pool Name Slave-APs				
IP Address Range	10.0.0.10		- 10.0.0.29	
DNS Server				
		Primary		
		Secondary		

Fig. 117: 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 v
Description	

Advanced Settings:

Advanced Para	meter			
Gateway				Use router as gateway •
Lease Time 120		Minutes		
DHCP Options	Option		Value	
	DNS Server	•	10.0.0.1	Î
	CAPWAP Controller	•	10.0.0.1	Î
	ADD			
Vendor Specific	Information (DHCP Option 43	i)		
	Vendor ID	V	endor Specific Information	
	ADD VENDOR STRING	ADD VENDOR	R GROUP	

Fig. 119: 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:

IP Pools:					
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	Î	1
Staff-Ethernet	10.0.1.10 - 10.0.1.254	0.0.0.0	0.0.0	ī	1
Slave-APs	10.0.0.10 - 10.0.0.29	0.0.0.0	0.0.0	Î	1
Guests-WLAN	10.0.20.10 - 10.0.20.254	0.0.0.0	0.0.0	Î	1
Guests-Ethernet	10.0.2.10 - 10.0.2.254	0.0.0.0	0.0.0.0		1

Fig. 120: 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		Germany
Interface		en1-0 ▼
DHCP Server	0	Server with enabled CAPWAP option (138): External or static Internal
IP Address Range	10.0.0.10	- 10.0.0.29
Slave AP location	10.0.0.10	 IO.0.29 Local (LAN) Remote (WAN)
Slave AP LED mode		Status V

Fig. 121: 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:

 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 \checkmark symbol.

Service Set Parameters		Security Settings	
Network Name (SSID) Staff	Visible	Security Mode	WPA-PSK V
otan	VISIDIE	WPA Mode	WPA and WPA 2 🔻
Intra-cell Repeating	Enabled	WPA Cipher	O AES O TKIP (AES and TKIP
U-APSD	() I	WPA2 Cipher	AES O TKIP O AES and TKIP
IGMP Snooping	Cabled Enabled	Preshared Key	
Client load balancing		MAC-Filter	
Max. number of clients - hard limit 32		Access Control	
		Dynamic blacklisting	Enabled
Max. number of clients - soft limit 24		Failed attempts per Time	10 / 60 Seconds
Client Band select	Disabled - optimized for fast roaming 🔻	Blacklist blocktime 500 Seco	nds
VLAN		Bandwidth limitation for each WLAN client	
VLAN	Enabled	Rx Shaping	No limit 🔻
VLAN ID 10		Tx Shaping	No limit 🔻

Fig. 122: 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 Preshared 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.

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

Service Set Parameters		Security Settings	
Network Name (SSID) Guest	Visible	Security Mode	WPA-PSK V
Guest	VISIBle	WPA Mode	WPA and WPA 2 V
Intra-cell Repeating	Enabled	WPA Cipher	O AES () TKIP O AES and TKIP
U-APSD	Enabled	WPA2 Cipher	AES O TKIP O AES and TKIP
IGMP Snooping	()))		
		Preshared Key	
Client load balancing		MAC-Filter	
Max. number of clients - hard limit 32		Access Control	
		Dynamic blacklisting	Enabled
Max, number of clients - soft limit 28		Failed attempts per Time	10 / 60 Seconds
Client Band select	Disabled - optimized for fast roaming v		
		Blacklist blocktime 500	econds
VLAN		Bandwidth limitation for each WLAN client	
VLAN	Enabled	Rx Shaping	No limit 🔻
VLAN ID 20		Tx Shaping	No limit 🔹

Fig. 123: 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 y symbol.

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

Advanced Settings

Chann	el Plan		User defined v
User D	efined Channel Plan		
	Channel		
	5 •		
	9 •		
	13 •	Î	
	ADD		
Beacor	n Period	100	m
DTIM P 2	eriod		
RTS Thr 2347	reshold		
Short (Guard Interval		Enabled
Max. T	ransmission Rate		Auto 🔻
Short R 7	etry Limit		
	etry Limit		
Long Re 4			

Fig. 125: 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.

ave Acces	s Points								
ocation .	Name	IP Address	LAN MAC Address	Channel	Search Channel	Status	Action		
le .	bintec W2003ac	10.0.0.11	00:01:cd:0e:ee:bc		C	Managed	~ ~	ĩ	1

Fig. 126: Wireless LAN Controller -> Slave-AP Configuration-> Slave Access Points



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.

Go to Wireless LAN Controller -> Slave AP Configuration-> Slave Access Points

Access Point Settings		Radio Module1
Device	W2003ac	Operation Mode O O O Off
Location Meeting Room		Active Radio Profile 2.4 GHz Radio Profile
incluing room		Channel Auto 🔻
Name W2003ac		Used Channel 6
Description Marketing		Transmit Power Max. Assigned Wireless Network (VSS)
CAPWAP Encryption	led	Profil MAC Address
		vss-1:Staff 00:a0:f9:0b:cf:e0
		vss-2:Guest

Fig. 127: 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)	C	Managed	~ ~	Î	1

Fig. 128: 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 Pont is to be managed by the WLAN Controller by clicking the \checkmark button or the \checkmark 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 v 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**.

י___ 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.

7.3 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 -> In- ternet Connections -> New	External gateway/ cable modem
Physical Ethernet Port	Assistants -> Internet Access -> In- ternet Connections -> Next	ETH5
Internet Service Pro- vider	Assistants -> Internet Access -> In- ternet Connections -> Next	- User-Specified -
IP parameters obtained dynamically	Assistants -> Internet Access -> In- ternet Connections -> Next	Disabled
Local IP Address	Assistants -> Internet Access -> In- ternet Connections -> Next	e.g. 1.2.3.4
Gateway IP address	Assistants -> Internet Access -> In- ternet Connections -> Next	e. g. 1.2.3.1
Netmask	Assistants -> Internet Access -> In- ternet 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-> Inter- faces -> <en1-0></en1-0>	10.0.0.1 and 255.255.255.0
IP Address / Netmask	LAN -> IP Configuration-> Inter- faces -> <en1-1></en1-1>	10.0.1.1 and 255.255.255.0
IP Address / Netmask	LAN -> IP Configuration-> Inter- faces -> <en1-2></en1-2>	10.0.2.1 and 255.255.255.0
Based on Ethernet In- terface	LAN -> IP Configuration-> Inter- faces -> New	en1-0
Address mode	LAN -> IP Configuration-> Inter- faces -> New	Static
IP Address / Netmask	LAN -> IP Configuration-> Inter- faces -> New	10.0.10.1 and 255.255.255.0
Interface Mode	LAN -> IP Configuration-> Inter- faces -> New	Tagged (VLAN)
VLAN ID	LAN -> IP Configuration-> Inter- faces -> New	10
Based on Ethernet In- terface	LAN -> IP Configuration-> Inter- faces -> New	en1-0
Address mode	LAN -> IP Configuration-> Inter- faces -> New	Static
IP Address / Netmask	LAN -> IP Configuration-> Inter- faces -> New	10.0.20.1 and 255.255.255.0
Interface Mode	LAN -> IP Configuration-> Inter- faces -> New	Tagged (VLAN)
VLAN ID	LAN -> IP Configuration-> Inter- faces -> New	20

Set up access

Field	Menu	Value
en1-0	System Management -> Adminis- trative Access -> Access	Telnet, SSH, HTTP, HTTPS, Ping, SNMP
en1-1 to en1-4	System Management -> Adminis- trative Access -> Access	Ping

Change password

Field	Menu	Value
System Admin Pass- word	System Management -> Global Set- tings -> Passwords	e. g. <i>test12345</i>
Confirm Admin Pass- word	System Management -> Global Set- tings -> Passwords	e.g. <i>test12345</i>

Set up firewall

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

Define addresses

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

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	any
Action	Firewall -> Policies -> IPv4 Filter Rules -> New	Access
Source	Firewall -> Policies -> IPv4 Filter Rules -> New	Users
Destination	Firewall -> Policies -> IPv4 Filter Rules -> New	LAN_EN1-4
Service	Firewall -> Policies -> IPv4 Filter Rules -> New	any
Action	Firewall -> Policies -> IPv4 Filter Rules -> New	Access

Create policies (IP addresses connected on the router)

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

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

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

Edit wireless networks

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

Field	Menu	Value
Security mode	Wireless LAN Controller -> Slave AP Configuration->Wireless Net- works (VSS)-> <vss-1></vss-1>	WPA-PSK
WPA Mode	Wireless LAN Controller -> Slave AP Configuration->Wireless Net- works (VSS)-> <vss-1></vss-1>	WPA and WPA 2
WPA Cipher	Wireless LAN Controller -> Slave AP Configuration->Wireless Net- works (VSS)-> <vss-1></vss-1>	TKIP
WPA2 Cipher	Wireless LAN Controller -> Slave AP Configuration->Wireless Net- works (VSS)-> <vss-1></vss-1>	AES
Preshared key	Wireless LAN Controller -> Slave AP Configuration->Wireless Net- works (VSS)-> <vss-1></vss-1>	Enter password
VLAN	Wireless LAN Controller -> Slave AP Configuration->Wireless Net- works (VSS)-> <vss-1></vss-1>	Enabled
VLAN ID	Wireless LAN Controller -> Slave AP Configuration->Wireless Net- works (VSS)-> <vss-1></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

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> vanced Settings	User-defined
User-defined Channel Plan	Wireless LAN Controller ->Slave AP Configuration -> Radio Profiles- > <2.4 GHz Radio Profile> vanced Settings	1, 5, 9, 13
Short Guard Interval	Wireless LAN Controller ->Slave AP Configuration -> Radio Profiles- > <2.4 GHz Radio Profile> > Ad- vanced Settings	Enabled

Edit radio profiles

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

New channel setting

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

Chapter 8 WLAN network with guest WLAN

8.1 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.

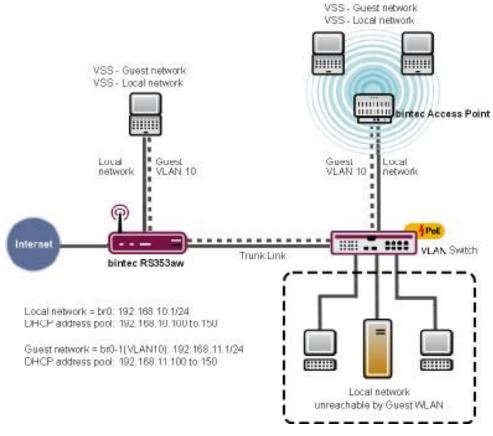


Fig. 129: Example WLAN scenario with guest WLAN



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.

8.2 Configuration

8.2.1 Configuring the IP address

Configure an IP address from the LAN interface.

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

Basic Parameters		Basic If	2v4 Parameters	
Interface Mode	 Untagged (VLAN) 	Security	r Policy	O Untrusted 🖲 Trusted
MAC Address	00:09:4f.6f.5e:80 Use built-in	Address IP Addr	s Mode ess / Netmask IP Address 192.168.10.1 ADD	Static O DHCP Netmask 255.255.255.0

Fig. 130: 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.

8.2.2 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.

Access Parameters		
#	Interface Description	Mode / Bridge Group
1	en1-0	New Bridge Group •
2	en1-4	Routing Mode •
3	vss7-10	Routing Mode •
Configuration Interl	face	
en1-0 🔻		

Fig. 131: System Management->Interface Mode / Bridge Groups->Interfaces

Proceed as follows to assign the LAN interface to a new bridge group and to transer 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> -> p menu.

8.2.3 Put Wireless LAN Controller into operation

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

F	Note
E	Non

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.

Basic Settings		
Region		Germany •
Interface		BRIDGE_BR0 •
DHCP Server	DHCP Server with enabled CAPWAP option (138): O External or static Internal	
IP Address Range	192.168.10.100	- 192.168.10.150

Fig. 132: Wireless LAN Controller->Wizard

Proceed as follows:

- 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 BRO.
- (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.

8.2.4 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

Select the Radio Profile			
Use two independent radio profiles	Enabled		
Radio Profile for Radio 1 (used for all Access Points)	2.4 GHz Radio Profile •		
Radio Profile for Radio 2 (only for dual radio APs)	5 GHz Radio Profile •		

Fig. 133: Wireless LAN Controller->Wizard

Proceed as follows:

 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

Wireless Networks (VSS)			
VSS Description	Network Name (SSID)	Security	
vss-1	default	WPA-P5K	1

Fig. 134: Wireless LAN Controller->Wizard

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

Step 3

Service Set Parameters	Security Settings	
Network Name (SSID) Local-Network	Security Mode	WPA-PSK T
	WPA Mode	WPA 2 •
IGMP Snooping 🛛 🛑 Ena	bled Preshared Key	

Fig. 135: 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.

8.2.5 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 configures your switches according yourself.

Click, in Wireless LAN Controller->Wizard Add.

Step 3

Service Set Parameters			Security Settings	
Network Name (SSID)	Guest-Network	Visible	Security Mode	WPA-PSK
			WPA Mode	WPA 2
IGMP Snooping		enabled Enabled	Preshared Key	
VLAN				
VLAN		Enabled		
vlan id 10				

Fig. 136: Wireless LAN Controller->Wizard->Add

- (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	Î	1
vss-2	Guest-Network	WPA-PSK	Î	1

Fig. 137: 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

Manage Select all/									
eselect all	Location	Device	IP Address	LAN MAC Address	Wireless Network	Radio Profile	Channel	Status	
•	1:	be.IP plus	192.168.0.251	Elmegt_6f:5e:7c	vss-1:Local-Network vss-2:Guest-Network	2.4 GHz Radio Profile	0	Discovered	1
					vss-1:Local-Network	2.4 GHz Radio Profile	0		/
	2:	W2003ac	192.168.0.100	BintecCo_48:69:c1	vss-2:Guest-Network	5 GHz Radio Profile	0	Gefunden	/

A Ready to apply the automatic installation! Select the access points that are to be managed with the Wireless LAN Controllier 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. 138: Wireless LAN Controller->Wizard

8.2.6 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.

W2003ac 192.168.0.100 BintecCo_48/69x1 vss.1:Local-Network 2.4 GHz Radio Profile 0 Vss.2:Guest-Network 5 GHz Radio Profile 0	Manage

Fig. 139: Wireless LAN Controller->Wizard

8.2.7 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. DHCHP, DNS and Echo. Configure an IP address for this interface.

Go to the following menu:

Go to LAN->IP Configuration->Interfaces->News.

Basic Parameters		Basic IPv4	Parameters	
Based on Ethernet Interface	br0 v	Security Pol	icy	Untrusted O Trusted
Interface Mode	O Untagged (VLAN)	Address Mo	de	Static O DHCF
VLAN ID 10	_	IP Address /	Netmask	
MAC Address	a0:19 Use built-in		P Address	Netmask 255.255.255.0
		A	DD	

Fig. 140: LAN->IP Configuration->Interfaces->New

- (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.

hernet/VLAN Ports							
interface	IPv4 Address/Netmask	IPv6 Address/Length	Status	Action			
en1-4	192.168.4.251/255.255.255.0	50 C	8	~ ~		1	Q
efm35-60	Not configured/Not configured	220	8	~ ~		1	Q
ethoa35-5	Not configured/Not configured	12	8	~ ~		1	Q
or0(VLAN ID1)	192.168.0.251/255.255.255.0	17.5	0	~ ~		1	Q
or0-1(VLAN ID10)	192.168.10.1/255.255.255.0	-	0	~ ~	i i	1	Q
r0-2(VLAN ID10)	192.168.11.1/255.255.255.0	-	0	~ ~		1	Q

Fig. 141: LAN->IP Configuration->Interfaces->New

8.2.8 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 Guest-Address-Pool		
IP Address Range	192.168.11.100	- 192.168.11.150
DNS Server		
	Primary	
	Secondary	

Fig. 142: 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	ĩ	1
	192.168.10.100 - 192.168.10.150	0.0.0	0.0.0	ĩ	1



8.2.9 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.

Basic Parameters	
Interface	br0 v
IP Pool Name	Guest-Address-Pool ▼
Pool Usage	Local
Description	

Fig. 144: 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.

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

Fig. 145: Local Services->DHCP Server->DHCP Configuration

8.2.10 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 ricon.

Basic	Basic Parameters					
Descri	ption	Trusted Interfaces				
Memb	ers					
	Interface	Trusted				
	LAN_EN1-4					
	WAN_ETHOA35-5					
	efm35-60					
	BRIDGE_BR0	-				
	BRIDGE_BR0-1					
	BRIDGE_BR0-2					

Fig. 146: 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		
Descrij Gues	ption t-Local Access		
Memb	bers		
	Service	Selection	
	activity		
	ah		
	any		
	dhcp		
	discard		
	dns	-	
	echo-req		
	echo-req-ipv6		

Fig. 147: 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	Î	1

Fig. 148: 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 V			

Fig. 149: 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.

Order	Source	Destination	Service	Action	Policy active				
1	BRIDGE_BR0-1	LOCAL	Guest-Local Access	Access	Enabled	† ₁	≡+	Î	-
2	BRIDGE_BR0-1	WAN_INTERNET	any	Access	Enabled	t ₁	=+		1
	ter Rules Source		Destination	Service	Action	Policy active			
efault Fili ^{Order} n+1		ces	Destination ANY	Service	Action				

Fig. 150: 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.

	Session Timer	
Enabled	UDP Inactivity 180	Seconds
All		
Enable	TCP Inactivity 3600	Seconds
	PPTP Inactivity	
	86400	Seconds
	Other Inactivity	Seconds
	All •	Lali Lali Lali Lali Lali Lali Lali Lali Lali

Fig. 151: **Firewall->Policies->Options**

- (1) Activate the IPv4 Firewall Status.
- (2) Press OK to confirm your entries.

8.3 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.

8.4 Overview of Configuration Steps

Configuring the IP address

Field	Menu	Value
Security Policy	LAN-> IP Configuration-> Inter- faces -> <en1-0-></en1-0->	Trusted
Address Mode	LAN ->IP Configuration-> Interface s-> <en1-0-></en1-0->	Static
IP Address / Netmask	LAN ->IP Configuration ->Inter- faces -> <en1-0-></en1-0->	192.168.10.1 / 255.255.255.0

Create bridge groups and assign LAN interface

Field	Menu	Value
Interface Description	System Management ->Interface Mode / Bridge Groups ->Interfaces	en1-0
Mode / Bridge Group	System Management ->Interface Mode / Bridge Groups ->Interfaces	New Bridge Group
Configuration Interface	System Management ->Interface Mode / Bridge Groups ->Interfaces	en1-0

Put Wireless LAN Controller into operation

Field	Menu	Value
Region	Wireless LAN Controller-> Wizard	Germany
Interface	Wireless LAN Controller ->Wizard	BRIDGE_BR0
DHCP Server	Wireless LAN Controller ->Wizard	Internal
IP Address Range	Wireless LAN Controller ->Wizard	e.g. 192.168.10.100 / 192.168.10.150

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 mod- ule 1 (for all Access Points)	Wireless LAN Controller-> Wizard - >Next	2.4 GHz Radio Pro- file
Radio profile for mod- ule 2 (only for APs with two radio modules)	Wireless LAN Controller-> Wizard - >Next	5 GHz Radio Pro- file
Network Name (SSID)	Wireless LAN Controller-> Wizard - >Next -> <vss-1>-></vss-1>	Local Network
Preshared Key	Wireless LAN Controller ->Wizard - >Next -> <vss-1>-></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 Control-	Wireless LAN Controller-> Wizard -	START
ler Wizard	>Next-> Next ->Next	

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	Tagged (VLAN)
VLAN ID	LAN ->IP Configuration ->Inter- faces-> New	10
Security Policy	LAN-> IP Configuration ->Inter- faces ->New	Untrusted
Address Mode	LAN-> IP Configuration ->Inter- faces-> New	Static
IP Address / Netmask	LAN ->IP Configuration ->Inter- faces-> New	192.168.11.1 / 255.255.255.0

Configure the IP Address Range for the guest network

Field	Menu	Value
IP Pool Name	Local Services ->DHCP Server-> IP Pool Configuration-> New	Guest-Address-Pool
IP Address Range	Local Services ->DHCP Server ->IP Pool Configuration ->New	e . g . 192.168.11.100 / 192.168.11.150

Configure DHCP use

Field	Menu	Value
Interface	Local Services-> DHCP Server-> DHCP Configuration ->New	br0-1
IP Pool Name	Local Services-> DHCP Server-> DHCP Configuration-> New	Guest-Address-Pool
Pool Usage	Local Services ->DHCP Server-> DHCP Configuration ->New	Local

Set up firewall

Field	Menu	Value
BRIDGE_BR0	Firewall-> Policies ->IPv4 Filter Rules ->Default Filter Rules	Trusted Enabled
Description	Firewall-> Services-> Groups-> New	e.g . <i>Guest-Lo-</i> <i>cl-Access</i>
Members	Firewall-> Services-> Groups-> New	e.g. dhcp, dns and echo
Source	Firewall ->Policies-> IPv4 Filter Rules-> New	BRIDGE_BR0-1

Field	Menu	Value
Destination	Firewall-> Policies ->IPv4 Filter Rules ->New	LOCAL
Service	Firewall-> Policies ->IPv4 Filter Rules ->New	<i>Guest-Local-Access</i>
Action	Firewall-> Policies ->IPv4 Filter Rules ->New	Access
Source	Firewall ->Policies-> IPv4 Filter Rules-> New	BRIDGE_BR0-1
Destination	Firewall-> Policies ->IPv4 Filter Rules ->New	WAN_INTERNET
Service	Firewall-> Policies ->IPv4 Filter Rules ->New	e.g. any
Action	Firewall-> Policies ->IPv4 Filter Rules ->New	Access
Status of the IPv4 Fire- wall	Firewall-> Policies-> Options	Enabled

Chapter 9 WLAN - WLAN controller installation with integrated HotSpot functionality

9.1 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.

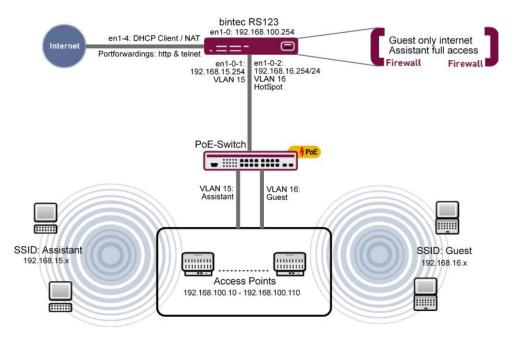


Fig. 152: Example scenario

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

9.2 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*.



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.

9.3 Configuration

9.3.1 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 Hot-Spot 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.

9.3.2 LAN configuration

First of all, change the IP address in the IP Configuration menu.

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

Basic Parameters			Basic II	Pv4 Parameters	
Interface Mode	 Untagg 	ged O Tagged (VLAN)	Security	y Policy	O Trust
00:a0.f9:3d;3d;b8	Use built-in	Address Mode		Static O DHCF	
				IP Address	Netmask 255.255.255.0
				ADD	

Fig. 153: 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.

Basic Parameters		Basic IPv4 Parameters	
Based on Ethernet Interface	en1-0 v	Security Policy	○ Untrusted
Interface Mode	O Untagged 💿 Tagged (VLAN)	Address Mode	Static O DHCP
VLAN ID 15		IP Address / Netmask	
		IP Address	Netmask
MAC Address 00:a0:f9	Use built-in	192.168.15.254	255.255.255.0
		ADD	

Fig. 154: LAN -> IP Configuration ->Interfaces -> New

- (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.

hernet/VLAN Ports							
nterface	IPv4 Address/Netmask	IPv6 Address/Length	Status	Action			
en1-0	192.168.100.254/255.255.255.0	2	0	~ ~		/	Q
en1-4	Not configured/Not configured	2	8	~ ~		/	Q
fm35-60	Not configured/Not configured	2	8	~ ~			Q
en1-0-1(VLAN ID15)	192.168.15.254/255.255.255.0	2	0	~ ~	T		Q
en1-0-2(VLAN ID16)	192.168.16.254/255.255.255.0	2	0	^ ¥	1	/	Q

Fig. 155: LAN -> IP Configuration -> Interfaces

9.3.3 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.

Basic Parameters	
Authentication Type	Accounting
Vendor Mode	bintec HotSpot Server ▼
Server IP Address 62.245.165.180	
RADIUS Secret	
Default User Password	
Priority	0 •
Entry active	Enabled
Group Description	Default Group 0 •

Fig. 156: 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.
- 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 O (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	-	0	1	
Login Authentication	62.245.165.180	Authoritative	0	-	0	ĩ	1

Fig. 157: 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.

		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
Terms & Conditions http://www.bintec-elmeg.cor	n	
Additional freely accessible Do	main Names	
Additional freely accessible Do Domain Name / IP Add		

Fig. 158: Local Services -> Hotspot Gateway -> Hotspot Gateway -> New

- (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 loggin 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**.

9.3.4 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).

 Go to Local Services -> DHCP Server -> IP Pool Configuration -> New to configure the IP pool.

IP Pool Name Employee		
P Address Rar	nge	
	192.168.15.10	- 198.168.15.110
DNS Server		
	Primary	
	Secondary	,

Fig. 159: 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.

Basic Parameters	
Interface	en1-0-1 🔻
IP Pool Name	Employee •
Pool Usage	Local
description	

Fig. 160: 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 ConfigurationI -> 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 validn IP Pool Name, here e. g. Guest.
- (8) For Pool Usage, select Local.
- (9) Confirm with OK.

The complete configuration looks like this:

Interface_	IP Pool Name	Gateway	Lease Time	Status		
en1-0-2	Guest	Use router as gateway	120Min.	Enabled	Î	1
en1-0-1	Employee	Use router as gateway	120Min.	Enabled	Î	1
en1-0		Use router as gateway	120Min.	Enabled	=	

Fig. 161: Local Services -> DHCP Server -> DHCP Configuration

9.3.5 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
	r with enabled CAPWAP option (138): l or static
IP Address Range	
192.168.100.10	- 192.168.100.110
Controller you have to Reset The selected interface is	ected your Access Point to the WLAN the Access Points now. not a bridge interface. The nnot be managed by the Wireless

LAN Controller.

Fig. 162: Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard

- (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.

Select the Radio Profile				
Use two independent radio profiles				
Radio Profile	2.4 GHz Radio Profile •			
Radio Profile	2.4 012 1400 11010			

Fig. 163: Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard

Click Next.

In the next step you define the SSID which is to be supplied later.

Service Set Parameters		Security Settings	
Network Name (SSID) Employee	Visible	Security Mode	WPA-PSK
	- Holoic	WPA Mode	WPA 2
IGMP Snooping	Enabled	Preshared Key	
VLAN			
VLAN	Enabled		
VLAN ID 15			

Fig. 164: Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard

- (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.

Service Set Parameters		Security Settings	
Network Name (SSID) Guest	Visible	Security Mode	Inactive
IGMP Snooping	Enabled		
VLAN			
VLAN	Enabled		
VLAN ID 16			

Fig. 165: 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.

Manage								
Select all/								
Deselect				LAN MAC	Wireless			
<u>all</u>	Location	Device	IP Address	Address	Network	Radio Profile	Channel	Status
•	1:	bintec W1002n	192.168.100.11	00:01:cd:0e:97:c4	vss-1:Mitarbeiter vss-2:Gaeste	2.4 GHz Radio Profile	0	Discovered

Fig. 166: 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.

Radio Module1	
Operation Mode	● On ○ Off
Active Radio Profile	2.4 GHz Radio Profile •
Channel	Auto 🔻
Transmit Power	Max. •
ĩ	
Ì	
	Operation Mode Active Radio Profile Channel Transmit Power

Fig. 167: 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.

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	Manageo

Fig. 168: 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.

Basio	: Parameters		
Descr Inter	iption net		
Mem	bers		
	Service	Selection	
	activity		
	ah		
	any		
	apple-qt		
	auth		

Fig. 169: 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	T	1
lokale dienste	echo-req, dns, dhcp, http, http (SSL), ntp		1

Fig. 170: Firewall -> Services -> Groups

In the last step, the local services are further restricted. Access to the http and ht-tp (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 v
Action	Access V

Fig. 171: 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.:

Filter Rule								
Order	Source	Destination	Service	Action	Policy active Deny			
1	LEASED_EN1-0-1	LOCAL	local services	Access	Enabled	† _↓	=+	/
2	LEASED_EN1-0-2	LOCAL	local services	Access	Enabled	†1	=+	1

Fig. 172: 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*.

Ē	No
	Fo

Spot functionality

ote

or WTP failure, we recommend that you configure an email notification to monitor the system.

9.4 Overview of configuration steps

LAN configuration

Field	Menu	Value
IP Address / Netmask	LAN -> IP Configuration -> Inter- faces -> <en1-0> .</en1-0>	e.g. 192.168.100.254
Interface Mode	LAN -> IP Configuration -> Inter- faces -> <en1-0> .</en1-0>	Untagged:
Based on Ethernet In- terface	LAN -> IP Configuration ->Inter- faces -> New	en1-0
IP Address / Netmask	LAN -> IP Configuration ->Inter- faces -> New	e.g. 192.168.15.254
Interface Mode	LAN -> IP Configuration ->Inter- faces -> New	Tagged (VLAN)
VLAN ID	LAN -> IP Configuration ->Inter- faces -> New	15
Based on Ethernet In- terface	LAN -> IP Configuration ->Inter- faces -> New	en1-0
IP Address / Netmask	LAN -> IP Configuration ->Inter- faces -> New	e.g. 192.168.16.254
Interface Mode	LAN -> IP Configuration ->Inter- faces -> New	Tagged (VLAN)
VLAN ID	LAN -> IP Configuration ->Inter- faces -> New	16

Hotspot configuration

Field	Menu	Value
Authentication Type	System Management -> Remote Authentication -> RADIUS -> New	Accounting
Vendor Mode	System Management -> Remote Authentication -> RADIUS -> New	bintec HotSpot Server
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. supersecret
Default User Password	System Management -> Remote Authentication -> RADIUS -> New	e.g. supersecret

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. supersecret
Default User Password	System Management -> Remote Authentication -> RADIUS -> New	e.g. supersecret
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. <i>LAN_EN1-0</i>
Domain at the HotSpot Server	Local Services -> Hotspot Gateway -> Hotspot Gateway -> New	e.g. training- fec_1.de
Walled Garden	Local Services -> Hotspot Gateway -> Hotspot Gateway -> New	Enabled
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	ht- tp://www.bintec-el meg.com
Terms & Conditions	Local Services -> Hotspot Gateway -> Hotspot Gateway -> New	ht- tp://www.bintec-el meg.com
Language for login window	Local Services -> Hotspot Gateway -> Hotspot Gateway -> New	e.g. German

DHCP configuration

Field	Menu	Value
IP Pool Name	Local Services -> DHCP Server -> IP Pool Configuration -> New	e.g. Assistant
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	en1-0-1
IP Pool Name	Local Services -> DHCP Server -> DHCP Configuration -> New	e.g. Assistant
Pool Usage	Local Services -> DHCP Server -> DHCP Configuration -> New	Local
IP Pool Name	Local Services -> DHCP Server -> IP Pool Configuration -> New	e.g. Guests
IP Address Range	Local Services -> DHCP Server -> IP Pool Configuration -> New	e . g . 192.168.16.10 - 192.168.16.110
Interface	Local Services -> DHCP Server -> DHCP Configuration -> New	en1-0-2
IP Pool Name	Local Services -> DHCP Server -> DHCP Configuration -> New	e.g. Guests
Pool Usage	Local Services -> DHCP Server -> DHCP Configuration -> New	Local

WLAN Controller Wizard

Field	Menu	Value
Region	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard.	Germany
Interface	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard.	LAN_EN1-0
DHCP Server	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard.	Internal
IP Address Range	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard.	e.g. 192.168.100.10 - 192.168.100.110
Radio profile	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard ->Next	2.4 GHz Radio Pro- file
Network Name (SSID)	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard ->Next	e.g. Employees
Security Mode	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard ->Next	WPA-PSK
WPA Mode	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard	WPA2

Field	Menu	Value
	->Next	
Preshared key	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard ->Next	e.g. supersecret
VLAN	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard ->Next	Enabled
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. Guests
Security Mode	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard -> Next-> Add	Inactive
VLAN	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard -> Next-> Add	Enabled
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.1:Office
Active Radio Profile	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard ->Next	2.4 GHz Radio Pro- file
Assigned Wireless Networks (VSS)	Wireless LAN Controller -> Wizard -> Wireless LAN Controller Wizard -> Next	e.g. <i>vss-</i> 1:Employees and <i>vss-2:Guests</i>

Add firewall rules

Field	Menu	Value
Description	Firewall -> Services -> Groups -> New	e.g. Internet
Members	Firewall -> Services -> Groups -> New	e. g. http, http (SSL)

Field	Menu	Value
Description	Firewall -> Services -> Groups -> New	e.g. Local Services
Members	Firewall -> Services -> Groups -> New	e. g. http, http (SSL)

Restrict local services

Field	Menu	Value
Source	Firewall -> Policies -> Filter Rules - > New	LEASED_EN1-0-1
Destination	Firewall -> Policies -> Filter Rules - > New	LOCAL
Service	Firewall -> Policies -> Filter Rules - > New	local services
Action	Firewall -> Policies -> Filter Rules - > New	Access
Source	Firewall -> Policies -> Filter Rules - > New	leased_en1-0-2
Destination	Firewall -> Policies -> Filter Rules - > New	LOCAL
Service	Firewall -> Policies -> Filter Rules - > New	local services
Action	Firewall -> Policies -> Filter Rules - > New	Access
Source	Firewall -> Policies -> Filter Rules - > New	LAN_EN1-0-1
Destination	Firewall -> Policies -> Filter Rules - > New	LAN_EN1-0-1
Service	Firewall -> Policies -> Filter Rules - > New	any
Action	Firewall -> Policies -> Filter Rules - > New	Deny
Source	Firewall -> Policies -> Filter Rules - > New	LAN_EN1-0-2
Destination	Firewall -> Policies -> Filter Rules - > New	LAN_EN1-0-2
Service	Firewall -> Policies -> Filter Rules - > New	any

Field	Menu	Value
Action	Firewall -> Policies -> Filter Rules - > New	Deny

Chapter 10 WLAN - Cloud NetManager

10.1 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

10.2 First steps in the portal

10.2.1 Creating a user

Open a browser and enter the URL into the address line: *ht-tps://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

Street	
Suedwestpark 94	
Country	
Germany	
	Suedwestpark 94

First name	Last name	Phone
John	Smith	091196731234
Email address	Login (the	default is your email address)
j-smith@company.com		

-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 <u>datenschutz@bintec-</u> elmen.com. Furthermore the data protection statement of bintec elmen	~
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.

Register Cancel

Fig. 173: 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.

10.2.2 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.

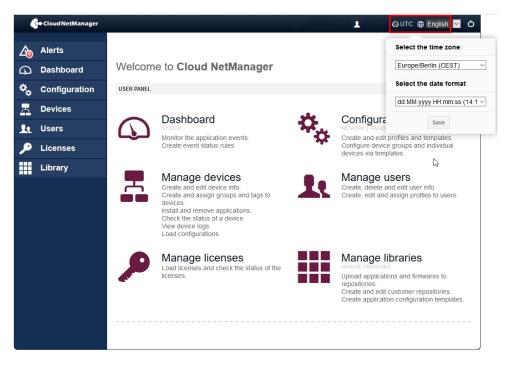


Fig. 174: Changing the time zone

10.2.3 Importing the licences

On the status page go to the Licences->Licences for this cloud server->New Licence menu.

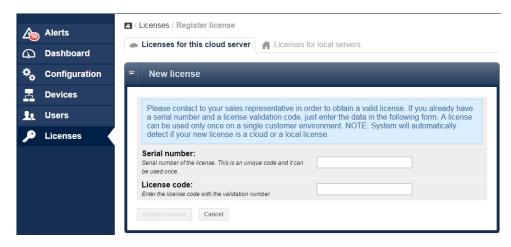


Fig. 175: New licence

- 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.

Δ	Alerts	/ Licenses / Reg						
4	Dashboard	Licenses for	this cloud se	rver 🔺 Licenses for local servers				
۰.	Configuration	= Manage licenses						
Ξ	Devices	+ NEW LICENSE	• NEWLICENSE					
1.	Users	Туре	Validity	Available	Status			
۶	Licenses	Managed devices	365 days	1 of 10	⊘ Valid license Q			
		Page 1 of 1		Resu	lts by page: 10 ▼			

Fig. 176: 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 be 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**.

∆ ₀	Alerts Dashboard	 / Licenses / Register license Licenses for this cloud server 	A Licenses for local servers					
۰.	Configuration	Devices assigned to the license						
R	Devices	Assign date	Serial Num.	Name				
1	Users	2015-02-25 16:37:16	RNEDDH014430001	AUTO_RNEDDH014430001				
	00010	2015-05-13 23:02:21	757/00120	DISCV_757/00120				
• مر	Licenses	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				
		Page 1 of 1		Results by page: 10 •				

Fig. 177: Devices that are associated with the licence

10.3 Creation of profiles

10.3.1 Creation of network profiles (SSID)

At least one network profile (SSID) must be created.

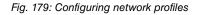
To do so, go to the **Configuration->Network** menu.

Click on New Network Profile.



Fig. 178: Network profiles

		Configurations	
Δ_{0}	Alerts	Configurations	
\bigcirc	Dashboard		
۰.	Configuration	New network profile	Additional features 🌣
-	Devices	Profile name [*]	
<u>I</u> t	Users	SERVICE SET PARAMETERS	
		Network name (SSID)	default
)	Licenses	Hidden	
	Library	Client isolation	v
		ARP processing	
		WMM	4
		SECURITY SETTINGS	
		Security mode	None 👻
		CLIENT LOAD BALANCING	
		Maximum number of clients - Hard limit	32 🔹
		Maximum number of clients - Soft limit	28 🕏
		Client band select	Disabled - optimized for fast roaming
		ACCESS CONTROL	
		ACL Mode	
		BLACKLISTING	
		Dynamic blacklisting	4
		Failed attempts	10 🗘
		Failed attempts time window	60 🔹
		Blacklist duration	500 🖈
		VLAN	
		Enable	
		BANDWIDTH LIMITATION FOR EACH WLAN CLIENT	
		Rx shaping	No limit v
		TX shaping	No limit
		iv outputs	NO IMMC
		Save Cancel	



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.

10.3.2 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.

	Cloud NetManager		L QE	urope/Berlin 🌐 E	nglish 🔽 🖒
∆ ₀	Alerts Dashboard	 / Configurations Configurations 		SHOW ADVANCED SE	ETTINGS
۰.	Configuration	New radio profile		Additiona	l features 🌣
Ξ	Devices	Name [*]			
Ŀ	Users	RADIO PROFILE DEFINITION			
P	Licenses	Description			
	Library	Operation mode	Access Point	~	С
	Listary	Operation band	2.4 GHz In/Outdoor	Ŧ	
		Bandwidth	20 MHz	-	
		Number of spatial streams	2	Ŧ	
		Country	Germany	~	
		PERFORMANCE SETTINGS			
		Wireless mode	802.11b/g/n	~	
		Burst mode			
		Airtime fairness			
		Save Cancel			

Fig. 180: 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.

10.3.3 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.

Δ	WLAN Profiles	Configurations		
	NETWORK	☆ Configurations		
\Box	RADIO			
۰.	RADIUS	New access point template		Additional features 🔅
	ANALYTICS	Template name [*]	Standard_AP	C
-	DHCP	Template description	Standard_AP	0
<u>.</u>	нотѕрот			,
	Device templates	SETTINGS		
۶	ACCESS POINT	Location	anywhere	0
		Administration password [*]	••••	0
		LED mode	normal	Ŧ
		Radius Server Profile	None	Ŧ
		RADIO MODULE 1		
		Radio profile	2,4 Standard Radio	· 0
		Channel	auto	
		TX Power	Max	The second secon
		Network profile	None	Ŧ
		RADIO MODULE 2		
		Radio profile	5 Standard Radio	· 0
		Channel	auto	
		TX Power	Max	· ·
		Network profile	None	w.
		Save Cancel		



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.

10.3.4 Administer devices

In the **Devices** menu, a list of all registered device is displayed. First, you must create a **Group**.

Alerts	Manage devices
Dashboar	rd 👝 Devices 🚠 Groups 🛷 Tags 🎄 Configuration templates
🍫 Configura	ation = Groups
- Devices	NEW GROUP
Le Users	Name Description Num. devices
🔎 Licenses	

Fig. 182: Administer devices

Go to the **Devices->Groups->New Group** menu.

Alerts	/ Manage devices / Group	
Dashboard	Name:	Standard Group
	Description:	Standard Group
♣ Configuration	Configuration template:	(g) Access Point: Standard _AP
E Devices	Monitoring period:	60 seconds
<u> I</u> Users	Automatic update:	7
🔎 Licenses	New group	

Fig. 183: 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.

10.4 Register and administer access points

To add a new device, go to the Devices->Managed Devices->Add Devices menu.

Alerts	☑ / Manage devices						
Dashboard	Bevices A Groups I Tags A Configuration templates						
🍫 Configuration	Filter						
E Devices	Devices Add Devices						
<u> I</u> Users							
🔎 Licenses	0 selected Search:						
	SN / MAC Annual Model Groups Last connection						

Fig. 184: Register and administer access points

10.4.1 Manually register devices

For manual registration, go to the **Devices->Add Devices->Manual registration** menu.

4	Alerts		Manage devices / Add devices		
9	Dashboard	69	Discovered devices 🗰 Manual registration	X Automatic registration	
۰.	Configuration	Ξ	Add devices - Manual registration		
Ξ	Devices	Г		Enter sorial numbers manually	
Ŀ	Le Users		Mode:	 Enter serial numbers manually 	
۶	🔎 Licenses		Serial numbers: Use semiclon between serials eg. AAA:DVC;BBB:DVC;CCC:DVC. Remember add the device verification code (DVC) after the serial number of each device.		
			Туре:	Access Point	
			Name:		
			Description:		
			IP:		
			Preview Add devices		

Fig. 185: Manual registration

Proceed as follows:

- If the **Mode Enter serial numbers manually** option is activated, you will need the **Serial number**, which is located on the device's name plate.
- If the **Mode Enter devices from data source** option is activated, you will need the **Device Verification Code (DVC)**, which is located on the device's name plate. If the DVC is not on the device's name plate, please contact our support.
- If you would like to register more than one device at a time, you can create and scan a CSV File.
- Click on Add devices to confirm your details.

10.4.2 Automatically register device

For automatic registration, go to the **Devices->Add Devices->Automatic registration** menu.

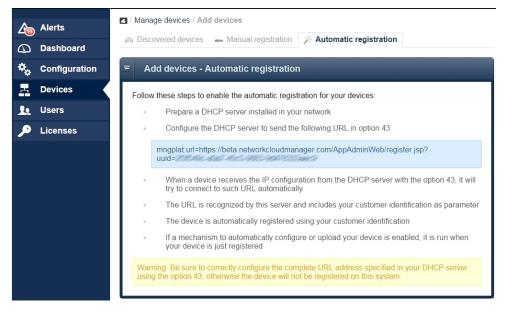


Fig. 186: Automatic registration

With the **DHCP option** *43*, the local DHCP server of the network in which the access point is located, can inform the access point, which user ID the access point is to use to login to Cloud NetManager. In doing so, an automatic registration and automatic commissioning without entering the serial number and DVC (see *Administer devices* on page 266) is enabled.

10.5 Device administration

In the **Devices** menu, registered devices are displayed.

Alerts	🖪 / Manage devices 🧰 Devices 🎿 Groups 🛷 Tags 🔅 Configure	ation templates						
Dashboard	Q + <u><u></u><u></u></u>	Q + 7						
🔅 Configuration	FILTERS:	Filter						
- Devices	= Devices	T Devices						
Le Users		ADD DEVICES Selected Search:						
🔎 Licenses								
	SN / MAC	Model Groups Last connection 💌						
	(1) RNHDAC013120018 HDWAHL_office2	W2004n ST GROUP 30.03.2015 11:40:49						
	Page 1 of 2	Results by page: 10 •						

Fig. 187: 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.

	RNFDEI01412001	0 - AUTO_RNFDEI01412	20010 +		LAST CON
ashboard	🗎 Info 🚜 Cor	figuration 🕒 Jobs	Re log Ale	arts	28 S
onfiguration					
evices			Details		
Isers			Name:	AUTO_RNFDEI014	4120010
icenses			S/N:	RNFDEI014120010	
		ACCESS POINT	MAC:	00:A0:F9:37:91:59	
	Device Model:	W2003n	Position:	40.412167 , -3.6993537	3
	System version:	V.9.1 Rev. 14 (Beta 5) IPSec	IP:	192.168.0.100	
	License:	access_point	Group:	Test	ŵ
	onfiguration evices	ashboard onfiguration evices sers icenses Device Model: System version:	ashboard onfiguration evices sers icenses Device Model: V2003n System version: V.9.1 Rev. 14 (Beta 5) IPSec	ashboard onfiguration evices sers icenses Device Model: W2003n System version: V.9.1 Rev. 14 (Beta 5) IPSec	ashboard onfiguration evices sers icenses Device Model: W2003n System version: V.9.1 Rev. 14 (Beta 5) IPSec

Fig. 188: Detailed view

10.5.1 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.

2	Alerts	Manage devices						
9	Dashboard	📥 Devices 🛓 Groups 🛷 Tags 🎄 Configuration templates						
۰.	Configuration	FILTERS:			Filter			
<u>.</u>	Devices	- Devices						
.	Users			BATCH OPERATIONS	≞ ~ ● ~			
۶	Licenses	ADD DEVICES DELETE DEVICES MANAGE DEVICES BATCH OPERATIONS A V V Search						
		SN / MAC	A Name	Model Group	s Last connection 👻			
		🕡 (ŋ) RNHDAC013	120018 HDWAHL_office2	W2004n ST GRO	30.03.2015 11:40:49			
		Page 1 of 2			Results by page: 10 •			

Fig. 189: Batch operations

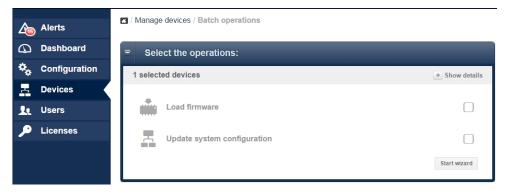


Fig. 190: Select operations

10.6 Appendix

10.6.1 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.

10.6.1.1 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 DCHP server.

If you are using the DCHP server of a **bintec** router, proceed as follows:

Enter **GUI** (Graphical User Interface) in the **Local Services->DHCP Server->DHCP Con**figuration menu.

Basic Parameters	
Select vendor	- Other - 🔻
Vendor Description :Cloud:	
Vendor ID Cloud	
Vendor Specific Information mngplat:url=https://bintec.networkcloudma	

Fig. 191: Local Services -> DHCP Server -> DHCP Configuration

- Choose the ricon 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 268).
- Click Apply.

10.6.1.2 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	
NetManager communication	Enabled
NetManager address https://discover.networkcloudmanager.com	
LED mode	Status •
Manual WLAN Controller IP Address	
Show Manufacturer Names	Enabled

Fig. 192: System Management->Global Settings ->System

- Enable the NetManager communication option.
- Enter the Address of the Cloud NetManager server in the NetManager address field.
- Press **OK** to confirm your entries.

10.6.2 Automatic configuration

With the Cloud NetManager, you have the option of automatically transferring a previouslydetermined configuration to every new Access Point which is connected to the local LAN. This method is suitable, for example, for small businesses which do not have their own inhouse IT staff, but which need to quickly and easily put new access points into operation.

In order to use this automatic configuration, three requirements must be met:

(a) The access point must be able to automatically log into the Cloud NetManager. To this end, the DCHP Option 43 must be set up with the User ID string, or the Cloud NetManager URL must be adjusted in the GUI of the Access Point. You can view the clientspecific URL and User ID under **Devices->Add Device->Automatic Login** in the Cloud NetManager.

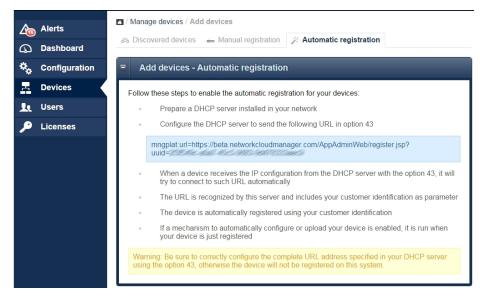


Fig. 193: Devices->Add Device->Automatic Login

- (b) In the Cloud NetManager, under Devices->Groups, a standard group must be defined.
- (c) In the Cloud NetManager, under Devices->Groups, under the Standard group the Automatic Update option must be activated.

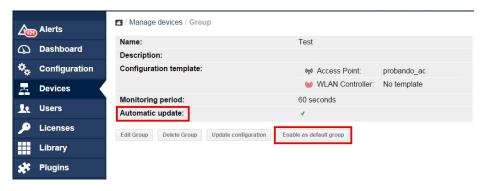


Fig. 194: Devices->Groups

10.7 Error search

10.7.1 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.

10.7.2 No more communication with an administered device

The logo that displays the communication state is no longer green but red.

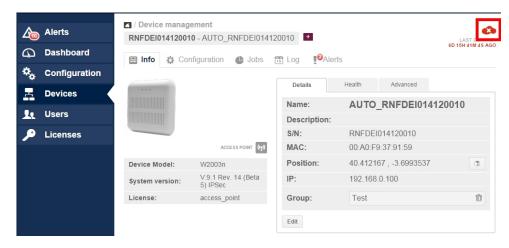


Fig. 195: Communication error

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 register 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.

Alerts		 / Device management RNFDEI014120010 - AUTO_RNFDEI014120010 			LAST CONTACT
Dashboard	🗎 Info 🎄 Co	🗎 Info 🎄 Configuration 🌰 Jobs 🛗 Log 🕫 Alerts			28 S AGO
🍫 Configuration					
Devices			Details Health	Advanced	
L Users			Remove security data	Present	
🔎 Licenses					
		ACCESS POINT	Advanced operations:		\$ 🎗 🏶
	Device Model:	W2003n	Last contact: 31.07.2015 18:28:44 License validity: 🥑 Valid license (Remaining days: 229)		
	System version:	V.9.1 Rev. 14 (Beta 5) IPSec			
	License:	access_point			

Fig. 196: Communication error

10.7.3 Further debug options

In the **Devices->Manage devices** menu, select a device. Go to **Manage devices->Con**figuration.

Alerts	 Manage devices Devices				
Dashboard					
🍫 Configuration	Filters: Filter				
	= Devices				
Le Users	ADD DEVICES DELETE DEVICES MANAGE DEVICES BATCH OPERATIONS E V				
🔎 Licenses	2 selected Search:				
	SN / MAC Anne Model Groups Last connection	-			
	RNHDAC013120018 HDWAHL_office2 W2004n ST GROUP 30.03.2015 11:40:49				
	Page 1 of 1 Results by page: 1	0 •			

Fig. 197: Communication error

Click on the small logo to display the configuration file.

A 200	Alerts	I / Device management I Test I +			
	Dashboard	🖺 Info 🔹 Configuration	n 🕒 Jobs 📅 Log	Alerts	
*.	Configuration				SHOW ADVANCED SETTINGS
-	Devices	✓ Configuration updated on of	levice		
1.	Users	Settings			
		Location	anywhere	*	
<i>,</i>	Licenses	Administrative password	•••••	-94	
		LED mode	normal	w 100	
		Radius Server Profile			
		Radio module 1			

Fig. 198: Debug options

Make sure that all passwords in this file are encrypted.

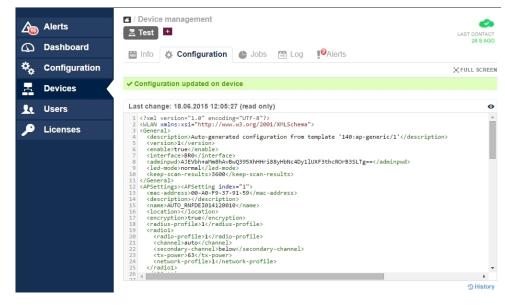


Fig. 199: Debug message

10.7.4 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 tremp". 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.