



HiPath 2000
HiPath 3000
HiPath 4000

optiPoint WL 2 professional

Administrator Manual

SIEMENS

Global network of innovation

Safety Precautions

The optiPoint WL 2 professional IP phone conforms to the European standard EN 60 950 which governs the safety of information technology equipment including electronic office equipment. Special emphasis was placed on personal and product safety when developing this telephone.



Only use the power supply provided as indicated on the underside of the charging unit.



Only use recommended rechargeable batteries. Never use other battery types or non-rechargeable batteries as this can cause serious damage to your health and property.



Insert the rechargeable battery making sure the poles are facing in the correct directions and use the battery as described in the operating manual.



The handset can interfere with medical equipment. Please refer to the technical specifications applicable to the relevant environment (medical practice, for instance).



The handset can cause unpleasant humming in hearing aids.



Do not install the charging unit in bathrooms or shower rooms. The handset and charging unit are not splash-protected.



Do not operate your handset in environments where there is risk of explosion (paintshops, for instance).



Remember to include all relevant documentation when passing on your handset to third parties.



Never open your handset. In the event of problems, consult your service personnel.



Use only original Siemens accessories. The use of other accessories is dangerous and will invalidate the warranty and the CE mark.

Location of the Telephone

- The telephone should be operated in a controlled environment with an ambient temperature between 5 °C and 40 °C (41 °F and 104 °F).
- To ensure good handsfree talking quality, the area in front of the microphone should be kept clear. The optimum handsfree distance is 20 inches (50cm).
- Do not install the telephone in a room where large quantities of dust accumulate; this can considerably reduce the service life of the telephone.
- Do not expose the telephone to direct sunlight or any other source of heat, as this is liable to damage the electronic equipment and the plastic casing.
- Do not operate the telephone in damp environments such as bathrooms.

Labels



The device conforms to the EU Guideline 1999/5/EG, as attested by the GE mark.



This device has been manufactured in accordance with our certified environmental management system (ISO 14001). This process ensures that energy consumption and the use of primary raw materials are kept to a minimum, thus reducing waste production.



All electrical and electronic products should be disposed of separately from the municipal waste stream via designated collection facilities appointed by the government or the local authorities.

The correct disposal and separate collection of your old appliance will help prevent potential negative consequences for the environment and human health. It is a precondition for reuse and recycling of used electrical and electronic equipment.

For more detailed information about disposal of your old appliance, please contact your city office, waste disposal service, the shop where you purchased the product or your sales representative.

The statements quoted above are only fully valid for equipment which is installed and sold in the countries of the European Union and is covered by the directive 2002/96/EC. Countries outside the European Union may have other regulations regarding the disposal of electrical and electronic equipment.

Contents

Safety Precautions.....2

Location of the Telephone..... 3

Labels 3

General Information.....6

About the Manual 6

Product Identification..... 6

Echo Effect 6

Overview 7

Notes and Symbols 8

 Safety..... 8

 References to Process Steps 8

 Using the Telephone 9

Setting Up the Telephone.....10

Preparing the handset..... 10

 Inserting the rechargeable batteries 10

 Placing the handset into the charger and charging the batteries... 10

Preparing for operation 11

 Activating/deactivating the handset..... 11

 Activating/deactivating the keypad lock..... 11

Set up WLAN Profile 12

 Set up and activate new profile 12

 Setting up additional profiles 14

Hidden "Service" menu 15

 Accessing the hidden "Service" menu 15

Administration19

Web Interface 20

 General Information..... 20

 Preparation..... 21

 "Admin" Main Menu..... 22

 Handset 23

 Network..... 24

 Profile Selection..... 24

 Audio Settings 29

 Dialling settings 29

 LDAP Settings 30

 DLS Settings 30

 Location Server 31

 VPN settings 31

Quality of Service 32

System settings 33

FTP Transfer 34

HTTP Transfer 36

Factory Reset 36

Certificates 37

Diagnostics 37

Alphabetic Reference 39

Functions 39

Abbreviations and Technical Terms 59

Administration Scenarios 67

Setup failed 67

Determine the Software Version 67

Check Connections 67

Set up FTP server 68

 Installation and configuration 68

Improve Voice Quality 69

Error Messages and Troubleshooting 70

Editors 72

Pre-defined entry fields 72

 Integer Editor 72

 IP Number Editor 72

 Options Editor 72

Text Editor 73

Appendix 74

Functions of Passwords and PINs 74

Technical Data 74

 Operating / Charging Hours 75

Factors influencing standby and talk times 75

Index 76

General Information

About the Manual

This Administration Manual will help you in administering and maintaining the optiPoint WL 2 professional. The instructions contain important information for safe and proper operation of the optiPoint WL 2 professional. Follow them carefully to avoid improper operation and get the most out of your multi-function telephone in a network environment.

You can set up and activate a WLAN profile on your optiPoint WL 2 professional → Page 12. We recommend to administer the optiPoint WL 2 professional via the web interface → Page 20 or using the Deployment Tool (see the Administration Manual of the Deployment Tool).

Telephone functions (local and communication platform) are described in the User Manual. A Quick Reference Guide provides short and reliable descriptions of frequently used functions.

Product Identification

The identification details of your telephone are given on the nameplate. The nameplate is located inside the battery compartment and contains the exact product label and serial number. Please have these ready whenever you call our service department in case of trouble with or defects on the unit itself.

Echo Effect

In some cases, while using the telephone you may hear an echo, which can be quite strong. This is not due to any design defect or other fault with your IP telephone, but caused by the other client.

For example, if a user reports an echo effect occurring during a teleconference, it may be that the loudspeakers and microphones need to be repositioned.

Overview

The → Access Point (AP) is the central component in the WLAN (Standard 802.11b). It manages network functions centrally and is connected to the cabled networks (e.g. HiPath 3000 or HiPath 4000) via a gateway.


The Access Point maintains both the radio connections to other nodes in the network and to wireless terminal devices (e.g. optiPoint WL 2 professional); it also determines the coverage area (the radio cell → Page 60). Depending on the size of the area to be covered, there may be more than one Access Points installed.


In order to make the wireless communication possible, you have to set up and activate a network profile (→ Page 12) in the optiPoint WL 2 professional.

Notes and Symbols

Safety



Information that is important for preventing injury or damages is marked specially, as they are important instructions for correct use of the unit.

 This symbol indicates a hazard. Failure to follow the instructions given may result in injury or in damage to the unit.

 This symbol indicates key information important for the proper use of the telephone.

References to Process Steps

The following symbols indicate various process descriptions:

-  Use the icons/keys on the optiPoint WL 2 professional.
-  Use the web interface.

Step-by-Step

Using the Telephone



Press the "talk" key.



Press the "end call" key.



Conduct a call.



Enter a telephone number or code.



or




Press the settings keys on the telephone.

Profile 1



The option appears on the display.


Press the  softkey to confirm your selection.



WLAN Settings



Search for an option.

Press the  control key until the option appears on the display.

Then press the  softkey to confirm your selection.

Setting Up the Telephone

This chapter describes how to set up (→ Preparing the handset) and prepare the optiPoint WL 2 professional for operation (→ Preparing for operation) as well as how to set up a WLAN profile for the optiPoint WL 2 professional (→ Set up WLAN Profile).

Preparing the handset

Inserting the rechargeable batteries

Please see the optiPoint WL 2 professional User Manual.



Only use the rechargeable batteries recommended by Siemens → Page 74! Never use conventional (non-rechargeable) or other battery types as this may cause significant damage to health or property. For example, the jacket of the battery could be destroyed or the battery could explode. The phone could also malfunction or be damaged.

Placing the handset into the charger and charging the batteries

1. Connect the power cord of the charger with a power outlet.
2. Place the handset into the charger with the display up.

Initial charging and discharging the batteries

The battery charging status is only displayed correctly after a complete charge/discharge cycle.

For the initial charge we recommend a continuous, uninterrupted charging period of five hours. After this, remove the handset from the charger and only put it back into the charger once the batteries are completely discharged.

After the initial charge/discharge cycle you can replace your handset into the charger after each call.



- You have to repeat this procedure whenever you remove the batteries from the handset or reinsert them.
- The batteries heat up during charging. This is normal and not dangerous.
- After a while the charge capacity of the batteries will decrease for technical reasons.

Preparing for operation

Please follow the procedure described below for preparing the optiPoint WL 2 professional.



The preparation procedure below describes the default configuration. Network configurations may be different and require additional steps.

In case of problems with the initial setting up or questions regarding individual settings please refer to the following chapters:

- For specialist information regarding the administration of the optiPoint WL 2 professional please go to "Alphabetic Reference" → Page 39.
- For descriptions of configuration scenarios please go to "Administration Scenarios" → Page 67.
- For error messages in the optiPoint WL 2 professional display please refer to "Error Messages and Troubleshooting" → Page 70.

Activating/deactivating the handset



Press the "end call" key **and hold**.



Enter the PIN (if set up - see the optiPoint WL 2 professional User Manual).


Activating/deactivating the keypad lock



Press the "hash" key **and hold**.

Step-by-Step

Set up WLAN Profile

 We recommend to set up network profiles via the web interface → Page 24.

Set up and activate new profile

After switching on the optiPoint WL 2 professional tries to establish a connection to the Access Point.

As you have not set up a profile, an error message is displayed.

Press the control key to the right and enter the Administrator PIN → Page 39.

You are now in the "Profile Selection" menu.

Confirm by pressing OK.
The cursor is placed in the field "Profile Name".

Enter a name for the new profile.

Scroll down to "WLAN Settings".

Copy settings from an existing profile

Press softkey.

Select and confirm.

Select and confirm.

Press softkey.

Select and confirm.

Manual input

The cursor is placed in the field "SSID:".

Enter the "SSID".

Go the the "Authentication:" menu and select the desired method → Page 13.



Go to the "Encryption Type:" menu and select the desired method → Page 13.


Go to the "DHCP:" menu.



Press the softkey.


Confirm by pressing OK to activate the profile.



No Access Point



 


New Entry 



AP 1 





 Copy from profile 



 Profile 3 







 Save Settings 

or



Main Building 

 <none> 

 <none> 

 <On> 

Save

AP 1  

Step-by-Step

<Off>

or



Switch off DHCP and enter additional settings manually
→ Page 14.

Select Authentication Mode

Select a security protocol in the "Authentication" menu
(→ 802.1x or → WPA) and enter the specifications.

Go to the "EAP Type" menu and select the desired method:

- → LEAP
- → TLS



<LEAP>



Go to the field "Login-Name:" and enter the login name.

Go to the field "Password:" and enter a password.

Press the softkey and enter additional settings in the
"Profile Selection" menu.

Save

Select the Encryption Type

Select an encryption method to protect wireless data
transmissions in the "Encryption Type:" menu:

1. Encryption using WEP → Page 44
 - WEP 64 or WEP 128 (→ WEP mode)

In this menu you also select the desired Authentication
Mode → Page 39.

Select the desired Password mode.



<Hexadezimal>



or

<ASCII>



Enter the → WEP key.



<Shared key>



or

<Open System>



2. Encryption using WPA PSK → Page 44
 - WPA PSK TKIP (→ TKIP)

Enter the → Pre-Shared Key.

Press the softkey and enter additional settings in the
"Profile Selection" menu.



Save

Step-by-Step

<Off>

[000.000.000.000]

[000.000.000.000]

[000.000.000.000]

Save

AP 1

or

Settings

Access Profile

<New Entry>

OK

OK

OK

OK

If there is no DHCP server available

Select "DHCP:".

Go to the field "IP Address:" and enter the IP address of the gateway.

Go to the field "Subnet Mask:" and enter the IP address.

Go to the field "Gateway:" and enter the IP address of the optiPoint WL 2 professional.

Press the softkey.

Confirm by pressing OK to activate the profile.

Setting up additional profiles

In order to enable fast and simple access in case of multiple parallel WLANs you can set up a maximum of 16 different network profiles.

Prerequisite: The handset must be in idle mode.

Open the main menu.

Enter the ID, select the ID and confirm by pressing OK.

Confirm by pressing OK.

Press the control key to the right and enter the Administrator PIN (→ Page 39).

Confirm by pressing OK.

Complete the profile as described under "Set up and activate new profile" → Page 12.

14

Step-by-Step

Hidden "Service" menu

This menu contains information about the WLAN connection, various settings of your optiPoint WL 2 professional as well as information for the services personnel.

Accessing the hidden "Service" menu

As you will have to press multiple keys simultaneously, we recommend that you place the handset onto a solid surface (e.g. your desk).

Prerequisite: The handset is switched of.
Press the key.

Press and hold keys simultaneously.

Short press the key.
The LEDs of the speakerphone key and mailbox key start blinking.

"Service" appears on the display.
Enter Code "76200".

Network Scan

The following information is displayed for all available profiles:

- **Field strength:** Signal strenth of the connection to the access point
- **SSID** → Page 50
- **Channel** → Page 40
- **MAC address**

Confirm.

Scan for all available profiles.

Select desired profile.

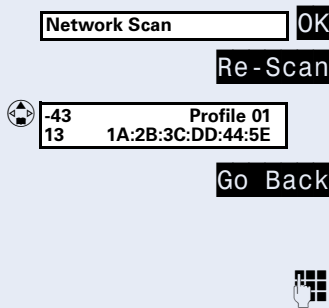
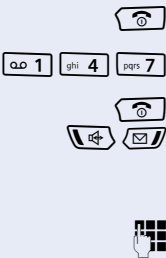
Close "Service" menu.

Other settings in the "Service" menu

Enter again Code "76200".

Leave "Service" menu

Long press key. The handset makes a restart.



Network Scan

OK

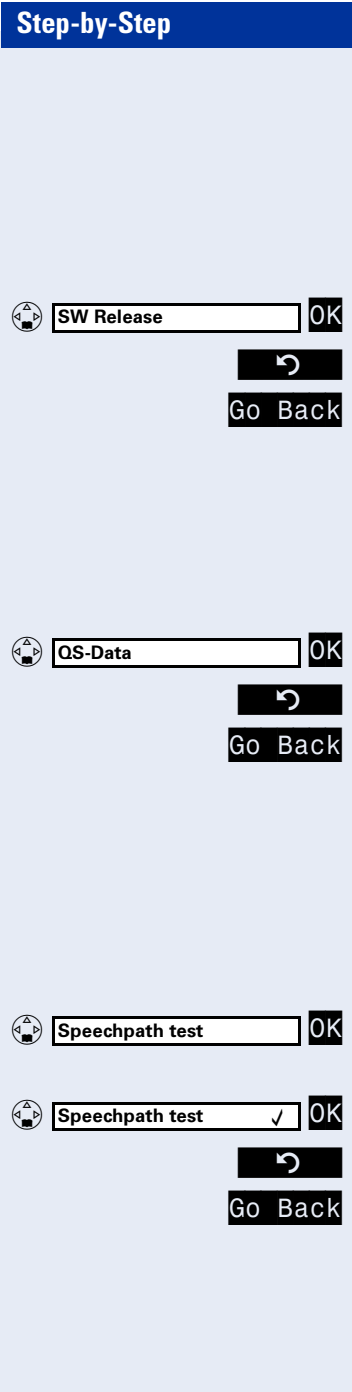
Re-Scan



-43	Profile 01
13	1A:2B:3C:DD:44:5E

Go Back





SW Release

The following information about the handset is displayed:

- **SW Release:** Version of the telephone software
- **MAC Address:** MAC adresse of the handset

Prerequisite: You are in the hidden "Service" menu
→ Page 15.

Select and confirm.

Back to menu.

Close "Service" menu.

QS-Data

This entry contains information regarding quality control during manufacturing (for service personnel only).

Prerequisite: You are in the hidden "Service" menu
→ Page 15.

Select and confirm.

Back to menu.

Close "Service" menu.

Speechpath test

Using this function the service personnel can do a quick check of the acoustic paths.

Prerequisite: You are in the hidden "Service" menu
→ Page 15.

Activate

Select and confirm.

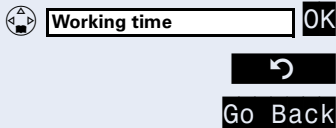
Deactivate

Select and confirm.

Back to menu.

Close "Service" menu.

Step-by-Step



Working time

Displays the entire operating hours of your optiPoint WL 2 professional.

Prerequisite: You are in the hidden "Service" menu
→ Page 15.

Select and confirm.

Back to menu.

Close "Service" menu.



Contrast

This function is used to set the display contrast for your handset. Possible values: 1 (low) to 9 (high).

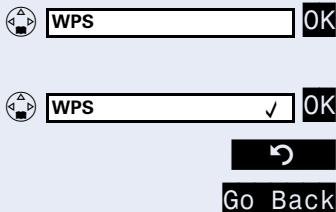
Prerequisite: You are in the hidden "Service" menu
→ Page 15.

Select and confirm.

Select the desired value.

Save settings.

Cancel, back to menu.



WPS

The WLAN Positioning System is a positioning system using access points. If this function is activated, a WPS server can identify the location of a handset using the data transmitted by the handset.

Prerequisite: You are in the hidden "Service" menu
→ Page 15.

Activate

Select and confirm.

Deactivate

Select and confirm.

Back to menu.

Close "Service" menu.

Step-by-Step



Factory default

OK

Yes

No

Factory default

This function resets all administration and user parameters to the factory default values.
You can also access this function via the web interface
→ Page 44.

Prerequisite: You are in the hidden "Service" menu
→ Page 15.

- Select and confirm.
- Confirm.
The handset makes a restart.
- Cancel, back to menu.

Clean up

This function deletes all user-initiated entries in the:

- phone book
- call list
- ringer tones

You can also access this function via the web interface
→ Page 40.

Prerequisite: You are in the hidden "Service" menu
→ Page 15.



Clean up

OK

Yes

No

- Select and confirm. A warning message is displayed.
- Confirm.
The handset makes a restart.
- Cancel, back to menu.

Backlight Switch

Using this function you can set the backlight duration when the handset is not used.

Possible values: 5 to 60 seconds.

Prerequisite: You are in the hidden "Service" menu
→ Page 15.



Backlight Switch

OK



Save

- Select and confirm.
- Select desired value.
- Cancel, back to menu.
- Save setting.

Administration

The execution of administration tasks requires a good general know-how about networking (similar to the know-how of network administrators). The chapter "Alphabetic Reference" → Page 39 provides more background information.

The **web interface** provides unlimited access to all administration menus.

- "Web Interface" → Page 20

There are some limitations for **local administration via the telephone**.

- "Set up WLAN Profile" → Page 12

If you use the Deployment Tool (see the Administration Manual for the Deployment Tool), you also have unlimited access to all administration menus.




Administration of an optiPoint WL 2 professional is only possible while the telephone is in idle mode.

Step-by-Step

Web Interface

General Information

The optiPoint WL 2 professional is equipped with a HTTP web server that permits the mapping of information from the handset to a web browser on a PC integrated into the WLAN ("web interface").

 The IP data for the optiPoint WL 2 professional and the PC must be configured correctly (please contact your administration staff).

The web interface contains the following form elements:

[Admin](#)

Click this link to access the relevant page.

 Apply

Click this button to accept the changes in the current form. This transfers the changes to the optiPoint WL 2 professional.

 Undo

Click this button to reset the changes in the current form to the values currently stored in the optiPoint WL 2 professional.

 No transfer

Select an option from the list field.

Click a checkbox or radio button to activate/deactivate a function.

Preparation

Open the web interface

To evoke the web interface, open a web browser and enter the following URL:

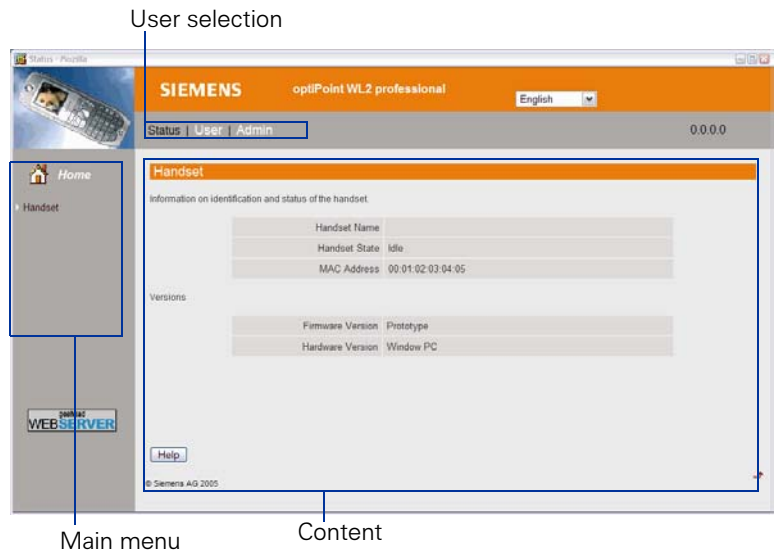
http://[IP of the optiPoint WL 2 professional]



Web browser settings:

- Java Script activated
- Frame Support active
- Popup windows permitted

The start screen is displayed in an additional window. The page "Status" (→ Page 23) is opened:



User Selection

[Status](#) See "Handset" → Page 23.

[User](#) User-specific settings for the handset (see the optiPoint WL 2 professional User Manual).

[Admin](#) Administration of the handset → Page 22.

Logout



When you have finished editing the settings, leave the Administration section through the "Logout" link in the Main Menu; otherwise the handset remains locked.

"Admin" Main Menu

- Network
 - Profile Selection → Page 24
 - Profile Name → Page 24
 - IP Addresses → Page 25
 - IP routing¹ → Page 25
 - WLAN → Page 26
 - WLAN Security → Page 26
 - Gatekeeper → Page 28
- Audio Settings → Page 29
- Dialling settings → Page 29
- LDAP Settings → Page 30
- DLS Settings → Page 30
- Location Server → Page 31
- VPN settings → Page 31
- Quality of Service → Page 32
 - Protocol Settings → Page 32
 - Monitoring Settings → Page 32
- System Settings
 - Handset PIN → Page 33
 - Reset User Data → Page 33
 - Admin PIN → Page 33
 - Handset Restart → Page 33
 - SNMP settings → Page 33
- FTP Transfer
 - FTP Settings → Page 34
 - Backup and Restore → Page 34
 - Firmware Update → Page 35
 - LDAP Update → Page 35
- HTTP Transfer
 - Backup and Restore → Page 36
 - Firmware Update → Page 36
- Factory Reset → Page 36
- Certificates → Page 37
- Diagnostics
 - Diagnostics → Page 37
 - RTP Statistics → Page 38
- Logout → Page 21

1. is only displayed if no DHCP server is available.

Handset



Click a field in one of the screenshots to obtain more information about the field.

Handset

Information on identification and status of the handset.

Handset Name	Einstein
Handset State	Idle
MAC Address	00:01:02:03:04:05


Versions

Firmware Version	Prototype
Hardware Version	Window PC

[Help](#)

© Siemens AG 2005

Network

 Click a field in one of the screenshots to obtain more information about the field.


Profile Selection


Network : Profile Selection

Choose a profile of the list (max. 16 entries) as active profile.
When activating a profile, the connection to the web server may be lost. After that the status page is shown.

Define a new profile

List of Profiles

Number	Profile Name	Network Name (SSID)	Line Quality	Encryption	DHCP Client	Active		
1	Profile1		-	None	Enabled		<input type="button" value="Edit"/>	

© Siemens AG 2005

Profile Name

Network : Profile Name


Configure a profile. Continue the settings sequence with the "Apply" button.

Profile Name


Copy profile settings from an existing profile.

Copy IP and WLAN settings from

Copy Gatekeeper settings from

© Siemens AG 2005

IP Addresses

 Click a field in one of the screenshots to obtain more information about the field.

Network : IP Addresses for profile "Profile3"

If the DHCP client is enabled the client will automatically obtain IP addresses and other configuration items.

DHCP Client	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Handset IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Subnet Mask	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Primary DNS IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Secondary DNS IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Default Gateway	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Domain Name	<input type="text"/>

Help

Undo Apply

© Siemens AG 2005

IP Routing

Network : IP Routing for profile "Profile3"

Route 1	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Mask 1	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Gateway 1	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>


Route 2	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Mask 2	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Gateway 2	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>

Help

Undo Apply

© Siemens AG 2005

WLAN

 Click a field in one of the screenshots to obtain more information about the field.

Network : WLAN for profile " Profile3"

Define the wireless network ID (SSID) for your WLAN access. The network name (SSID) can be selected from a list of found SSIDs (after scanning) or entered directly in the appropriate field. If there is interference with other wireless devices, you can improve transmission rates and link quality by changing the channel number. In addition you can adapt the transmission mode and the transmission rate.

SSID Scan	Detected SSIDs	Scan
Network Name (SSID)		
Channel	1	
Output Power (in %)	100	
Transfer Mode	Mixed Mode	
Transmission Rate	Auto	
Fragmentation Threshold	2346 (Value range: 256-2346 in Bytes)	
RTS/CTS Threshold	2347 (Value range: 1-2347 in Bytes)	
Roaming Threshold	100 (Value range: 0-100 in mW)	
Preamble Type	<input checked="" type="radio"/> Long <input type="radio"/> Short	

Help

UndoApply

© Siemens AG 2005

WLAN Security

Encryption using "WPA-PSK"

Network : WLAN Security for profile "Profile1"

Select from various security parameters to protect your data transfer and your handset from unauthorised access.

Encryption	WPA-PSK
------------	---------

Enter a password in the WPA Pre-Shared Key field. Length: 8 - 63 (64 in hex-format) characters.

Encryption Type	TKIP
Pre-Shared Key	

Authentication Description

Authentication	None
----------------	------

Help

UndoApply

© Siemens AG 2005

Encryption using "WEP"



Click a field in one of the screenshots to obtain more information about the field.

Network : WLAN Security for profile "Profile1"

Select from various security parameters to protect your data transfer and your handset from unauthorised access.

Encryption: WEP

WEP Mode 128 bit: Enter 13 characters (26 in hexformat).
WEP Mode 64 bit: Enter 5 characters (10 in hexformat).

WEP Mode: ☒ 128 bit ☐ 64 bit

WEP Key:

Authentication Mode: ☐ Shared Key ☒ Open System

Authentication Description

Authentication: None

[Help](#) [Undo](#) [Apply](#)

© Siemens AG 2005

Encryption using "WPA"

Network : WLAN Security for profile "Profile1"

Select from various security parameters to protect your data transfer and your handset from unauthorised access.

Encryption: WPA

WPA authentication is 802.1x (not changeable).

Encryption Type: AES

Authentication Description

Authentication: 802.1x

EAP Type: ☒ TLS ☐ LEAP

Login Name:

Password:

Certificate: cert1.cer

Validate Server Certificate: ☐

Gatekeeper

Network : Gatekeeper for profile "Profile3"

Set the gatekeeper parameters to connect to your HiPath.

System Type	HiPath3000V5
Gatekeeper Address	<input type="radio"/> Enter IP-Address <input checked="" type="radio"/> Enter Name
	<input type="text"/>
Port	<input type="text"/>
Subscriber Number	<input type="text"/>
Password	<input type="text"/>
Emergency Number	<input type="text"/>
Location Identifier Number	<input type="text"/>
Mobility Password	<input type="text"/>

Help

Undo Apply

© Siemens AG 2005

Audio Settings



Click a field in one of the screenshots to obtain more information about the field.

Audio Settings

Codec	G.711 preferred (normal quality) ▼
RTP Packet Size	Automatic ▼
Silence Suppression	<input type="checkbox"/>

[Help](#) [Undo](#) [Apply](#)

© Siemens AG 2005

Dialling settings


Dialling Settings

External Access Code (PABX)	<input type="text"/>
International Access Code:	<input type="text"/>
Local Country Code	<input type="text"/>
National Access Code	<input type="text"/>
Local Area Code	<input type="text"/>
Local District Code	<input type="text"/>
Redial List	<input type="radio"/> Active <input checked="" type="radio"/> Inactive
Prefer Preparation Editor	<input type="checkbox"/>

[Help](#) [Undo](#) [Apply](#)

© Siemens AG 2005

LDAP Settings

 Click a field in one of the screenshots to obtain more information about the field.

LDAP Settings

LDAP Server Address

☒ Enter IP-Address ☐ Enter Name

0000

Port

389

Help

Undo

Apply

© Siemens AG 2005

DLS Settings

DLS Settings

DLS Server Address

☒ Enter IP-Address ☐ Enter Name

0000

Port


Help

Undo

Apply

© Siemens AG 2005

Location Server

 Click a field in one of the screenshots to obtain more information about the field.

Location Server

Enter the Location Server data.

Location Server	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Location Server Address	<input checked="" type="radio"/> Enter IP-Address <input type="radio"/> Enter Name
	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Port	<input type="text"/>


[Help](#) [Undo](#) [Apply](#)

© Siemens AG 2005

VPN settings

VPN Settings


Configure VPN.

VPN	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
User Name	<input type="text"/>
Password	<input type="password"/>
Certificate	<input type="text" value="cert1.cer"/> 

[Help](#) [Undo](#) [Apply](#)

© Siemens AG 2005

Quality of Service

 Click a field in one of the screenshots to obtain more information about the field.

Protocol Settings

Quality of Service : Protocol Settings

QoS for IP

DSCP Class for Voice

Assured Forwarding 1

Drop Preference Levels for Voice

Low

DSCP Class for Signalling

Best Effort

VLAN Settings

VLAN Mode

☒ Manual ☐ Automatic (via DHCP) ☐ None

VLAN ID

0

(Value range: 0-4094)

QoS for Ethernet

Priority for Voice

4

Priority for Signalling

3

Help

Undo

Apply

© Siemens AG 2005

Monitoring Settings

Quality of Service (QoS): Monitoring Settings

Send a report (report mode)

EOS Threshold exceeded

QCU Server Address

☒ Enter IP-Address ☐ Enter Name

0000

Report Interval (in sec.):

60

Send to QCU

☐ Yes ☒ No

Send SNMP Traps

☐ Yes ☒ No

Minimal Session Length (in 100 ms)

20

Threshold Settings

Maximum Jitter (in ms)

15

Average Round Trip Delay (in ms)

100

Codec Type	Lost packets per 1000 packets	Consecutive lost packets	Consecutive good packets
non-compressing	10	2	8
compressing	10	2	8


Help

Undo

Apply

© Siemens AG 2005

System settings

 Click a field in one of the screenshots to obtain more information about the field.

Handset PIN

System Settings: Handset PIN

Specify a PIN for user security in order to limit the handset access to users with the correct credentials.

Handset PIN

Reset User Data

System Settings: Reset User Data

Delete all personal data relating to the user (including personal directory entries). Handset settings (such as contrast) and administration settings (such as network details) are not deleted.

Clear all user data

Delete all personal Handset settings (such as contrast) relating to the user. Personal data (including personal directory entries), and administration settings (such as network details) are not deleted.

User Settings

Admin PIN

System Settings: Admin PIN

Specify a PIN for admin security in order to limit the handset management to users with correct credentials.

Admin PIN

Set logout time

Handset Restart

System Settings: Handset Restart

Restart your handset if it does not function properly.

Handset Restart


SNMP settings

System Settings: SNMP settings

Trap Server Address ☒ Enter IP-Address ☐ Enter Name

Password

FTP Transfer

 Click a field in one of the screenshots to obtain more information about the field.

FTP Settings

FTP Settings

Configure the parameters to use FTP as transfer medium.

FTP Server Address

☒ Enter IP-Address ☐ Enter Name

0001

Port

21

FTP Account Name

User Name

Password

Help

UndoApply

© Siemens AG 2005

Backup and Restore

Backup and Restore

Backup and restore the handset configuration settings over FTP to/from a file server.

Configuration File

Backup

Save your current configuration settings

Backup

Restore

Retrieve a saved configuration

Restore

Help

UndoApply

© Siemens AG 2005

Firmware Update



Click a field in one of the screenshots to obtain more information about the field.

Firmware Update

Download new firmware over FTP from a file server. After the correct download the new firmware will be validated. If valid, it will replace the existing firmware and the handset will auto-restart.

Current Firmware	1.1
Firmware Download	<input type="text"/>
<input type="button" value="Update"/>	


LDAP Update

LDAP Update

Download a new LDAP template over FTP from a file server.

LDAP Template	<input type="text"/>
<input type="button" value="Load"/>	

HTTP Transfer

 Click a field in one of the screenshots to obtain more information about the field.

Backup and Restore

Backup and Restore

Backup and restore the handset configuration settings to/from your PC.

Backup

Save your current configuration settings

Restore

Retrieve a saved configuration

Firmware Update

Firmware Update

Download new firmware. After the correct download the new firmware will be validated. If valid, it will replace the existing firmware and the handset will auto-restart.

Current Firmware 1.1

Firmware Download

Factory Reset

Factory Reset

Restore the factory defaults. The current configuration is overwritten. Warning: all settings are deleted.

Restore the factory defaults

Certificates



Click a field in one of the screenshots to obtain more information about the field.

WLAN Client, WLAN Root, VPN

Certificates WLAN client

Update your certificates when required.

Retrieve a certificate

Browse...

Update

Delete old certificates when no longer required.

Select a certificate

cert1.cer ▼

Delete

Help

Diagnostics

Diagnostics

Diagnostics

Use the following tests to check for various problems.

Ping Test to

FTP Server Address ▼

Ping

Other Ping Test

☒ Enter IP-Address ☐ Enter Name

Ping

0

0

0


0

Help

Undo

Siemens AG 2005

RTP Statistics

 Click a field in one of the screenshots to obtain more information about the field.

Diagnostics: RTP Statistics

Show the RTP statistics records. They are collected and stored for the most recent calls.

Record Number	1
Address-of-record	
From	
To	
Call ID	
Request URI	
Session Begin	
Session End	
Transport Address - Local	
Transport Address - Remote	
Codec	
Frame Size	
Jitter	
Average Round Trip Delay	
Packets received	
Packets lost	

Packets discarded due to

Out-of-Sequence / Delay	
Buffer Overrun	
Other	



Help

Apply

© Siemens AG 2005

Alphabetic Reference

This glossary provides basic information required to perform configuration and diagnostic tasks on the optiPoint WL 2 professional.

- The section "Functions" explains terms found in the menus in alphabetic order.
Clicking the icons will bring you to the relevant function descriptions:
 Using the icons on the optiPoint WL 2 professional
 Using the icons via the web interface
- After this section you will find the chapter "Abbreviations and Technical Terms".

Functions

For more information please see the relevant documents about "networking technology", "→ WLAN" and "→ VoIP".

Admin PIN

- Password for accessing the administrator area.
- Permitted values: integer or no entry
- Length max.: 4

 → Page 33

Authentication

This task- or user-dependant access control feature protects system functions from being misused. Authentication ensures that the communicating partner really is the one he/she claims to be.

 → Page 26,  → Page 27,  → Page 27,

Authentication mode

- This is where you activate the process of identification (authentication mode) of WLAN stations.

Shared key (secure process)	During authentication the → Access Point (AP) checks whether a valid key is available via a challenge/response process. Associated stations can only transfer data after the check was completed successfully.
Open system (default process)	Any station can associate with an → Access Point (AP) and receive unencrypted data.

 → Page 13  → Page 26

Backup and Restore via FTP or HTTP

- Click "Backup" to save your personal settings in a file on your PC.
- If a HTTP connection is available, click "Browse" to locate and load the file you want.
- Click "Restore" to re-load the previous settings for your optiPoint WL 2 professional.
- In case of an FTP connection the following parameters must be set up or known:
 - File name
 - FTP Server Address
 - FTP Account Name
 - FTP User Name, → FTP Password

 → Page 34,  → Page 36

Certificate

- Select the desired certificate here.

 → Page 27

Channel



To make sure that different WLANs do not interfere with each other, the frequency range is divided into channels (recommended distance: 3 channels). All devices associated with a WAN have to use the same channel!

The channel used by the handset for transmission is predetermined by the access point. The handset scans for an access point with the SSID set in the handset. If there are several access points using the same SSID on different channels within the coverage of the handset, the channel setting determines the selection of the access point. The driver first attempts to locate the access point using the desired SSID on the desired channel. If this is not found, the driver searches the other channels.

- up to 13 channels
- Select the channel set in the access point.

 → Page 26

Clear all user data

- This function deletes all user-initiated entries in the optiPoint WL 2 professional (including phone book entries). Settings for handset and network are not deleted.

 → Page 33

Codec

- Select the desired audio transmission method from the list.

Codec	Audio Mode	Usage
G.722 preferred (high quality)		Suitable for broadband intranet connections and mobile telecommunication networks.
G.711 preferred (normal quality)	uncompressed	Use uncompressed voice transmission (→ G.711).
G.723 preferred (low bandwidth)	compressed only	Suitable for low bandwidth connections.
G.729 A/B preferred (low bandwidth)	compression preferred	Suitable for connections using different bandwidths.
G.723 only (low bandwidth)		
G.729 A/B only (low bandwidth)		

 → Page 29

Compressing Codec type

- Compressed → Codec
- **Lost packets** (in per thousand): These packets were lost during the transmission. The value is the ratio of packets lost to the total number of packets.
 - Permitted values: 1 ... 255
 - Default value: 10
- **Consecutive lost packets** (unit: no. of packets): This function counts how many packets were lost "in a row" (i.e. without interruption by transmitted packets). If the value counted is higher than the selected value, the threshold value has been exceeded.
 - Permitted values: 1 ... 255
 - Default value: 2
- **Consecutive good packets** (unit: no. of packets): This function counts how many packets were transmitted "in a row" (i.e. without interruption by lost packets). If the value counted is lower than the selected value, the threshold value has been exceeded.
 - Permitted values: 1 ... 255
 - Default value: 8

 → Page 32

Copy Gatekeeper settings from

To copy the gatekeeper settings of an existing profile when setting up a new WLAN profile select the desired profile here.

 → Page 24

Copy IP and WLAN settings from

To copy the IP addresses and WLAN settings of an existing profile when setting up a new WLAN profile select the desired profile here.

 → Page 24

Default Gateway

- Enter the → IP Address that was assigned to your → PBX (if this value is not provided dynamically by a → DHCP server).
- If the value was assigned dynamically, it can only be read.
- The change will only have effect if you restart the phone.

 → Page 25

Define a new profile

- Click "New" to set up a new WLAN profile.

 → Page 24

DHCP

- **Enabled:** Activate this option if the required IP data of the telephone should be assigned dynamically by a → DHCP server.
- **Disabled:** If no DHCP server is available in the IP network, please deactivate this option. In this case the data corresponding to the → Handset IP Address, → Subnet Mask, → DNS Addresses (Preminary/Secondary) (Preminary/Secondary), and → Default Gateway must be defined manually.
- The change will only have effect if you restart the phone.

 → Page 12  → Page 25

DLS Server Port

- Enter the → Port number for the communication with the → DLS server.

 → Page 30

DLS Server Address

- Select whether you want to use a → DNS name or an → IP Address; then enter the data for the → DLS server.

 → Page 30

DNS Addresses (Preminary/Secondary)

- Only enter the → IP Addresses of the → DNS server if these are not assigned dynamically by a → DHCP server and if the optiPoint WL 2 professional is not connected to a → PBX via → HFA.

 → Page 25

Domain Name

- Only enter the name of the domain if the optiPoint WL 2 professional is not connected to a → PBX via → HFA.

 → Page 25

Drop Preference Levels for Voice

- There are four priority classes (→ DSCP Class for Voice) defined for Assured Forwarding. Independently, resources (data rate/bandwidth, buffer memory) are reserved for these classes. In case of an overload, excess data packets are lost (packet loss). Using this function you can set the packet loss probability for each class (Assured Forwarding 1-4): Low, Medium, High.

 → Page 32

DSCP Class for Signalling

- DiffServ Code Point Class for Signalling.

 → Page 32

DSCP Class for Voice

- DiffServ Code Point Class for voice transmission.

 → Page 32

EAP Type

- Activate one of the methods → TLS or → LEAP for encryption of the authentication data in the → EAP protocol.

 → Page 27

External Access Code

- Enter the number that has to be dialled before an external phone number, e.g. "0".
- Canonical Format → Page 61.

 → Page 29

Emergency Number

- Special parameter for use in the USA.
- Enter the number that is to be dialled automatically after 1 second.
- Length max.: 20

 → Page 28

Encryption WEP

- Security feature based on a → RC4 encoding. For each WLAN device (e.g. optiPoint WL 2 professional) a secure key has to be stored. The → PMK is static and has to be entered manually on each client.

 → Page 13  → Page 27

Encryption WPA

- Security feature using an external → RADIUS server for authentication of the users.

 → Page 27

Encryption WPA-PSK

- Security feature using a → PSK for authentication. The → PMK is static and has to be entered manually on each client.

 → Page 13  → Page 26


Encryption Type

- Select one of the two encryption options: → TKIP oder → AES.

 → Page 26,  → Page 27

Factory Reset

- This function resets all administration parameters to the default factory settings.

 The reset can cause a complete failure of all functions of the optiPoint WL 2 professional. Please make sure you have all the necessary information for setting up the system again → Page 10.

 → Page 36

Firmware Update via FTP or HTTP

- This function updates the telephone software of your optiPoint WL 2 professional. The current → Firmware Version is displayed under "Current firmware:".
- In case of a **Download via HTTP** click "Browse" to search for the relevant file.
- In case of a **Download via FTP** the following parameters must be set up or known:
 - File name of the file to download
 - FTP Server Address
 - FTP Account Name
 - FTP User Name, → FTP Password
- Click "Update" to download the new firmware.

 → Page 35,  → Page 36

Firmware Version

- Displays the current version of the telephone software. This display includes information about the functions of the optiPoint WL 2 professional and can change after an update of the telephone software (→ Firmware Update via FTP or HTTP).

 → Page 23

Fragmentation Threshold

- This value determines whether and at what size data packets are fragmented. In a 802.11-WLAN packets with sizes above this threshold are fragmented, i.e. broken down into smaller pieces for transmission. Packets with sizes below the specified threshold are not fragmented. If the transmission error rate is increasing, you should increase the fragmentation threshold. A low fragmentation threshold may reduce the transmission performance.
- Permitted Values: 256-2346 bytes
- Default Value: 2346

 → Page 26

FTP Account Name

- Length min.: 1 character
- Length max.: 32 characters

 → Page 34

FTP Password

- Enter the password defined in the → FTP server as password for accessing this server.
- The password must correspond to the → FTP User Name.
- Length min.: 1 character
- Length max.: 32 characters

 → Page 34

FTP Port

- Enter the → Port number for the communication with the → FTP server.

 → Page 34

FTP Server Address

- Select whether you want to use a → DNS name or an → IP Address and enter the corresponding data of the → FTP server in order to be able to execute uploads and downloads from and to the optiPoint WL 2 professional.

 → Page 34

FTP User Name

- Enter the name defined in the → FTP server as user for accessing the server.
- The name must correspond to the → FTP Password.
- Length min.: 1 character
- Length max.: 32 characters

 → Page 34

Gatekeeper address

- Select whether you want to use a → DNS name or an → IP Address and enter the corresponding data of the → PBX the optiPoint WL 2 professional is connected to.

 → Page 28

Gatekeeper Port

- Enter the → Port number for the communication with the Gatekeeper.

 → Page 28

Handset IP Address

- Enter the → IP Address for the optiPoint WL 2 professional unless this value is provided dynamically by a → DHCP server (→ DHCP).
- The change will only have effect if you restart the phone.

 → Page 25

Handset PIN

- Change the User PIN.
- Permitted Values: numeric
- Length min.: 4
- Length max.: 9

 → Page 33


Handset Restart

- This function triggers a restart of the optiPoint WL 2 professional.

 → Page 33

Hardware Version

- This function displays the current hardware version of the optiPoint WL 2 professional.

 → Page 23

Handset Name

- This function displays the name you assigned to your optiPoint WL 2 professional (see User Manual).

 → Page 23

Handset State

- This function displays the current state of the optiPoint WL 2 professional.

 → Page 23

International Access Code

- Enter the prefix number for international phone numbers, e.g. "001".
- Canonical Dialling → Page 61.

 → Page 29

IP Routing

- To have constant access to network subscribers of other domains you can enter (in addition to the → Default Gateway) a total of two more network destinations (Route 1 and Route 2).
- An → IP Address of the domain and gateway and a → Subnet Mask must be entered for any other domain you wish to use.

 → Page 25

LDAP Server Address

- If an → LDAP server is used, select whether you want to use a → DNS name or an → IP Address and then enter the corresponding data for this server.

 → Page 30

LDAP Port

- If an → LDAP server is used, enter the → Port number for the communication with this server.
- Valid values: 1 ... 65535.
- Default value: 389

 → Page 30

LDAP Update

- This function loads an LDAP template.
- Click "Load" to load the template file.
- To complete the load procedure, the following parameters must be set up or known:
 - Name of the LDAP template
 - FTP Server Address
 - FTP Account Name
 - FTP User Name, → FTP Password

 → Page 35

Local Area Code

- Enter the local area code for your company location, e.g. "972" for Dallas/TX.
- Canonical Dialling → Page 61.

 → Page 29

Local Country Code

- Enter the country code for the country your company is located in, e.g. "+1" for the USA.
- Canonical Dialling → Page 61.

 → Page 29

Local District Code

- Enter the main phone number of your company (i.e. the front desk number without any extension, e.g. "443").
- Canonical Dialling → Page 61.

 → Page 29

Location Identifier Number

- Number for uniquely identifying a location. In case of e.g. an emergency this number can be used to identify where the emergency call was initiated.

 → Page 28

Location Server

- Mark **Enable** if a location server is integrated into your system.

 → Page 31

Location Server Address

- If a location server is used, select whether you want to use a → DNS name or an → IP Address and then enter the corresponding data for this server.

 → Page 31

Location Server Port

- If a location server is used, enter the → Port number for the communication with this server.

 → Page 31

Login Name

- Login name for identification of a handset within the WLAN.

 → Page 27

MAC Address

- Displays the → MAC address of a network device (e.g. optiPoint WL 2 professional).

 → Page 23

Minimal Session length

- If the session (e.g. a call) is shorter than the defined minimum length, no QoS report is sent.

 → Page 32

Mobility Password

- If you forgot to cancel the subscriber number at the "host" telephone, you can catch up on this at your "home" telephone after entering the mobility password.
- Permitted Values: alphanumeric
- Length min.: 6
- Length max.: 32

 → Page 28


National Access Code

- Enter the number that has to be dialled before an external phone number within your country, e.g. "0".
- Canonical Dialling → Page 61.

 → Page 29

Network Name (SSID)

- Enter a name for the WLAN profile.

 If you scanned for existing SSIDs and selected an available SSID (→ SSID Scan), the corresponding name as well as all settings are already entered; this can be used as a basis (overwrite is enabled).

- To enable access to the → WLAN, all stations have to be configured with the correct → SSID (Network name). If the SSIDs do not match, the user is denied access to the network.
- Permitted Values: alphanumeric
- Length max.: 32 characters

 → Page 26

Non-Compressing Codec type

- non-compressing → Codec.
- Explanation → Page 41.

 → Page 32

Output power

- Specification (in percent) of the transmitting power.

 → Page 26

Password

- Password for access to the WLAN.

 → Page 27

PING Test

- Run this → PING test to check whether a server or another terminal device (e.g. the optiPoint WL 2 professional) can be reached in the network. Available addresses from the list:
 - Gatekeeper address
 - DLS address
 - FTP server address
 - SNMP Trap server address
 - LDAP server
 - Gateway
 - DNS 1
 - DNS 2
- **other Ping test:**
Select whether you want to use a → DNS name or an → IP Address.
- Enter the address or the name of the test target.
- Click "Ping" to test the connection.


 → Page 37




Preamble Type

- Define the length of the → CRC to detect errors in data transmissions.

 → Page 26

Prefer Preparation Editor

- Using this checkbox you can change the function of the talk key  in idle mode.

Checkbox marked	 short press: open redial list
	 long press: start dial (normal)
Checkbox unmarked	 short press: start dial (normal)
	 long press: start "dial preparation"

 → Page 29


Pre-Shared Key

- Enter the → PSK here.
- Permitted Values: alphanumeric
- Length min.: 8 characters
- Length max.: 32 characters

 → Page 13  → Page 26

Priority for Signalling

- Can only be set if → VLAN Mode is active.
- Select a value from the list to set the priority for signalling.
- Permitted Values: None, 0-7

 → Page 32

Priority for Voice

- Can only be set if → VLAN Mode is active.
- Select a value from the list to set the priority for voice transmissions.
- Permitted Values: None, 1-7

 → Page 32

Profile list

- Displays all profiles set up (max. 16) and the most important data about these profiles.
- Click "Edit" to edit one of the profiles.
- Mark the checkbox "Active" to activate one of the profiles.
- Click "Delete" to delete a profile without being asked for confirmation.

 → Page 24

Profile Name

- Enter the name for the new profile.
- Permitted Values: alphanumeric
- Length max.: 32

 → Page 24

Profile number

- You can set up up to 16 profiles.
- Select the number of the profile to be edited.

 → Page 24

QCU server address

- Select whether you want to use a → DNS name or an → IP Address and then enter the corresponding data for the QCU server that will be used for logging the → QoS data.

 → Page 32

Redial list

- Mark this checkbox to store the last 10 numbers dialled from the optiPoint WL 2 professional in a redial list.

 → Page 29

Report interval

- Time interval (in seconds) after which reports are sent.
- A QoS report is sent for each report interval if the report mode (→ Send a report (report mode)) was set accordingly.
- Valid values: 10 ... 3600.

 → Page 32

Retrieve a certificate

- Select a page from the main menu to load the appropriate certificates for your Ihr optiPoint WL 2 professional:
 - WLAN client
 - WLAN server
 - VPN
- Click "Browse" to select the corresponding file on your PC.
- Click "Update" to load the file.

 → Page 37

Roaming Threshold

- If the WLAN comprises multiple access points using the same SSID and the same channel, the handset can change between the access points without interrupting the connection. In case the handset is moved outside of the coverage of an access point it is supposed to set up a connection with the next access point of the WLAN.
- Set the minimum value for the signal strength from the access point.
- Permitted Values: integers from 0 - 100 (mW)

 → Page 26

RTS/CTS Threshold

- This is a virtual collision recognition method. One station tells all the other stations how long it will use the line to send a data frame and receive the acknowledgment.
- Enter the packet size at which the → RTS/→ CTS method shall be triggered.
- Permitted Values: 1-2347 bytes

 → Page 26

RTP Packet Size

- Depending on the → Codec selected you can select the → RTP packet size here. In case of "G.723 preferred/only" there is no selection possible - the value is determined automatically.

 → Page 29

RTP Statistics

- Displays statistical data about → RTP that can be retrieved by entering the report number.

 → Page 38

Select a certificate

- Select a page from the main menu to delete certificates no longer needed:
 - WLAN client
 - WLAN server
 - VPN
- Select the appropriate certificate from the list.
- Click "Delete".

 → Page 37

Send a report (report mode)

- Select the mode for report generation:
 - **OFF**: deactivate report mode
 - **EOS Threshold exceeded**: A report will be sent at the end of the session only if the threshold was exceeded.
 - **EOR Threshold exceeded**: A report will be sent at any report interval (→ Report interval) if the threshold was exceeded.
 - **EOR (End of Report Interval)**: At the end of each session a report will be sent.
 - **EOS (End of Session)**: A report will be sent at any report interval (→ Report interval).

 → Page 32

Send to QCU

- Select **Yes** if a QCU server is set up and if the QoS data are to be logged on this server.

 → Page 32

Send SNMP Traps

- Select **Yes** if errors occurring in network components are to be logged.

 → Page 32

Set logout time

- Set the time interval after which the optiPoint WL 2 professional shall leave the administration mode automatically if there is no activity.

 → Page 33

Silence Suppression

- Mark this switch to suppress the background noise during breaks in a communication.

 → Page 29

SNMP Password

- Specify the password that was defined in the → SNMP server as the password for accessing this server.
- Permitted Values: alphanumeric

 → Page 33

SNMP Trap Server Address

- If an → SNMP server exists in the network, select whether you want to use a → DNS name or an → IP Address and enter the corresponding data for this server.

 → Page 33

SSID Scan

- Click "Scan" to display the existing SSIDs (→ SSID (Network name)). Select the desired SSID from the list. All settings are displayed; this can be used as a basis (overwrite is enabled).

 → Page 26

Subnet Mask

- Enter the → Subnet Mask for the optiPoint WL 2 professional if this value is not provided dynamically by a → DHCP server (→ DHCP).
- The change will only have effect if you restart the phone.

 → Page 25

Subscriber number

- Enter the subscriber number for the optiPoint WL 2 professional.
- The number can be between 1 and 20 digits.
- The subscriber number is the number that is used as the internal calling number.

 → Page 28

Subscriber Password

- Using this password you can transfer the subscriber number including the configuration settings to another telephone.
- Permitted Values: alphanumeric
- Length min.: 6
- Length max.: 32

 → Page 28

System type

- Select your communication platform.

 → Page 28

Transfer mode

- Select the WLAN transfer mode:

Mixed Mode	various modes
only 802.11b	802.11b only (11 Mbit/s)
only 802.11g	802.11g only (up to 54 Mbit/s)

 → Page 26

Transmission Rate

- The WLAN transmission rate depends on the → Transfer mode.

 → Page 26

Threshold settings

- **Maximum jitter (in ms):** The jitter value is checked against this threshold. The jitter value is measured between two consecutive → RTP packets.
 - Valid Values: 1 ... 255
 - Default Value: 15 ms
- **Average Round Trip Delay (in ms):** Round Trip Delay is the total of the transmission duration in both directions.
 - Valid Values: 1 ... 65535
 - Default Value: 100 ms

 → Page 32

User Settings

- This function deletes all user settings in the optiPoint WL 2 professional. Phone book entries and network settings will be maintained.

 → Page 33

Validate Certificate

- Mark this checkbox to validate the selected certificate.

 → Page 27

VLAN id

- Can only be set if the → VLAN Mode is set to "Manual".
- Enter a value from 0 to 4094. If → VLANs are used, this value determines the affiliation to a certain VLAN.

 → Page 32

VLAN Mode

- Determine the location from where the → VLAN id shall be retrieved if → VLANs are used.
- **Manual:** The ID entered under → VLAN id is used.
- **Automatic (over DHCP):** If a → DHCP server is used, the ID provided by this server is used.
- **None:**

 → Page 32

VPN Certificate

- Select the appropriate certificate.

 → Page 31

VPN settings

- Use this function if you want to secure your WLAN using a → VPN.

 → Page 31

VPN User Name and Password

- This option is only displayed if → VPN settings are activated.

 → Page 31

WEP key

- Enter the → WEP key.
- Permitted Values: alphanumeric
- Length max.: 26, length depends on the → WEP mode

 → Page 13  → Page 27

WEP mode

- Select the desired encryption (64 or 128 bit) for the → WEP key.



WEP encryption 128 Bit in the optiPoint WL 2 professional is defined with 13/26 characters. This value has to match the number of characters defined for the WEP encryption of the access point used. Please read the section about WEP encryption in the access point documentation!

Example: The optiPoint WL 2 professional is set to WEP encryption 128 bit. In the optiPoint WL 2 professional, this is defined as **13/26** characters.

In the access point WB500, however, **16/32** characters are defined for WEP encryption using 128 bit. The number of characters in the optiPoint WL 2 professional and the WB500 do not match. Therefore, set the WEP encryption in the WB500 to 104 bit as this matches the number of characters of 13/26.



→ Page 13  → Page 27

Abbreviations and Technical Terms

For further information please refer to the literature available about network technologies and → VoIP.

802.1x

Port Based Network Access Control. This standard defines client-server based access control and authorization and prevents access of unauthorized clients to networks using public ports.

Access Point (AP)

The AP in a WLAN transports data packets between the various participants and is the "bridge" to cabled networks. The AP has a wireless connection to all associated network nodes, and handles central functions such as filtering, roaming, and security.

AES

Abbreviation for "**A**dvanced **E**ncryption **S**tandard".

Symmetric encryption algorithm specifying three different key sizes (128, 192 and 256 bit).

Codec

Software or hardware entity that converts audio or video signals in realtime based on a predefined method.

CRC

Abbreviation for "**C**yclic **R**edundancy **C**heck".

Error correction method that creates checksums for binary numbers by calculating the sums of data blocks prior to transmission.

CTS

Abbreviation for "**C**lear **t**o **s**end".

Port control signal. A station with data to send transmits an → RTS packet. If the path to the target is free, it receives a CTS packet in response.

DHCP

Abbreviation for "**D**ynamic **H**ost **C**onfiguration **P**rotocol".

Dynamic assignment of IP addresses for endpoints in an IP network using a central DHCP server.

DLS

Abbreviation for "**D**eployment **L**icense **S**ervice".

DLS is a HiPath Management application for the administration of work-points (optiPoint telephones and optiClient installations) in HiPath- and non-HiPath networks.

DNS

Abbreviation for "**D**omain **N**ame **S**ystem".
Internet service for the translation of human-readable hostnames into → IP Addresses.

EAP

Abbreviation for "**E**xtensible **A**uthentication **P**rotocol".
The EAP protocol is a basic component for secure centralized environments. It is an extension of the PPP protocol which in turn is based on → 802.1x.

E.164

An addressing standard for telephone numbers according to the international ITU standard using a maximum of 15 digits. Usually, these numbers comprise: CC (**C**ountry **C**ode), NDC (**N**ational **D**estination **C**ode), and SN (**S**ubscriber **N**umber).

FTP

Abbreviation for "**F**ile **T**ransfer **P**rotocol".
Is used for transferring files in networks, e.g. to update telephone software → Page 45.

Radio Cell

A radio cell is the geographical area covered by a cellular telephone transmitter.

G.711

Audio protocol for uncompressed voice transmission. Requires a bandwidth of 64 kbit/s.

G.722

Audio protocol for uncompressed voice transmission. Requires a bandwidth of 128 kbit/s. This voice transmission method provides best quality.

G.723

Audio protocol for compressed voice transmission. The quality is lower than in → G.711 and → G.729. Requires a bandwidth of about 6 kbit/s.

G.729

Audio protocol for compressed voice transmission. The quality is lower than in → G.711 and higher than in → G.723. Requires a bandwidth of about 8 kbit/s.

Gateway

Mediation component between two different network types, e.g. → IP network and ISDN network.

HFA

Abbreviation for "**H**icom **F**eature **A**ccess".

Provides the connection between → IP telephones and a → PBX via a gateway (e.g. HG 1500 or HG 3530) .

HTTP

Abbreviation for "**H**ypertext **T**ransfer **P**rotocol".

Protocol for the transfer of data in → IP networks.

IP

Abbreviation for "**I**nternet **P**rotocol".

IP Address

Also abbreviated to → IP. The unique address of a terminal device in the network. It consists of four number blocks of 0 to 255 each, separated by dots. To simplify the notation voice names can be translated into IP addresses by a → DNS.

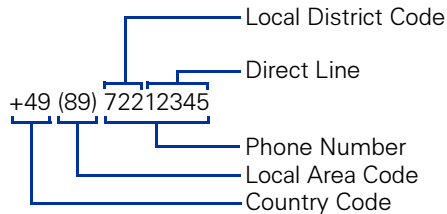
Jitter

Runtime fluctuations in data transmissions in → IP networks.

Canonical dialling

Canonical format is an international standard for dialling numbers. In order to be able to dial numbers in this format, certain rules (conversion information) have to be set.

Example for a number in canonical format:



LAN

Abbreviation for "**L**ocal **A**rea **N**etwork".

Layer 2

2nd layer (Data Link Layer) of the 7-layer OSI model for describing data transmission interfaces.

Layer 3

3rd layer (Data Link Layer) of the 7-layer OSI model for describing data transmission interfaces.

LDAP

Abbreviation for "**L**ightweight **D**irectory **A**ccess **P**rotocol".
Simplified protocol for accessing standardized directory systems, e.g. a company telephone directory.

LCD

Abbreviation for "**L**iquid **C**rystal **D**isplay".
Display of numbers, text or graphics using liquid crystal technology.

LEAP

Abbreviation for "**L**ightweight **E**xtensible **A**uthentication **P**rotocol".
LEAP is an authentication method using a common user name and password for the server and the wireless client.

LED

Abbreviation for "**L**ight **E**mitting **D**iode".
Cold light illumination in different colors at low power consumption.

MAC

Abbreviation for "**M**edium **A**ccess **C**ontrol **A**ddress".
A 48 bit address with the help of which any terminal device in a network (e.g. → IP telephone or network card) identifies itself uniquely all over the world.

MIB

Abbreviation for "**M**anagement **I**nformation **B**ase".
Database containing descriptions and error messages of the devices and functions within a network.

PBX

Abbreviation for "**P**rivate **B**ranch **eX**change".
Private telephone system that connects the different internal devices to the ISDN network.

PING

Abbreviation for "**P**acket **I**nternet **G**roper".

Program used for testing whether a connection to a specific → IP target can be established. In this test, data are sent to the target and sent back by the target. The result displays success/failure of the transmission and - if available - additional information such as duration of the transmission.

PKI

Abbreviation for "**P**ublic **K**ey **I**nfrastructure".

Environment providing services for encryption and digital signatures based on public key methods.

Port

Ports are used in → IP networks to enable several communication connections simultaneously. Different services often have different port numbers.

PMK

Abbreviation for "**P**airwise **M**aster **K**ey".

PSK

Abbreviation for "**P**re-**S**hared **K**ey".

Common key. A key is a pre-generated bit combination; this is used - on the sender's side - to convert normal text into an encrypted text and - on the receiver's side - to convert the encrypted text back into normal text.

QoS

Abbreviation for "**Q**uality of **S**ervice".

Describes the quality (performance) of a voice connection via → IP networks. Factors determining the QoS are e.g. packet loss rate, round trip delay, reserved bandwidth, type of bitrate (variable, constant or unspecified), or bitrate.

RAM

Abbreviation for "**R**andom **A**ccess **M**emory".

Memory with read / write access.

RADIUS

Abbreviation for "**R**emote **A**uthentication **D**ial-In **U**ser".

Client-server based security protocol for authentication and checking network access rights.

RC4

Symmetric encryption algorithm where keys are generated by a random number generator. RC4 uses a secret key known only to sender and destination. The key can be up to 2,048 bits long. Every character is individually encrypted. Although RC4 is quite straightforward, it is considered very secure.

ROM

Abbreviation for "**R**ead **O**nly **M**emory".
Memory with read only access.

RSA

Abbreviation for "**R**ivest **S**hamir **A**dleman".
Asymmetric encryption algorithm named after it's inventors.

RTP

Abbreviation for "**R**ealtime **T**ransport **P**rotocol".
This protocol is used for network-based video and audio communication. The protocol detects and corrects missing, duplicate or incorrectly sequenced data packets using a 16-bit sequence number.

RTS

Abbreviation for "**R**equest **T**o **S**end".

SIP

Abbreviation for "**S**ession **I**nitiation **P**rotocol".
Protocol standard for initializing calls in → IP networks.

VLAN

Abbreviation for "**V**irtual **L**ocal **A**rea **N**etwork".
Division of a → IP network in separately managed sections (domains). One option for identification of membership in a VLAN is the use of → VLAN ids.

SNMP

Abbreviation for "**S**imple **N**etwork **M**anagement **P**rotocol".
This protocol is used to communicate with servers executing network management functions, e.g. logging of errors in network components (SNMP traps).

SNTP

Abbreviation for "**S**imple **N**etwork **T**ime **P**rotocol".
This protocol is used between time servers and terminal devices in a network to synchronize the time settings of the terminal devices.

SRSR

Abbreviation for "**S**mall **R**emote **S**ites **R**edundancy".

SSID (Network name)

Abbreviation for "**S**ervice **S**et **I**dentification".

Network key in a WLAN. The → Access Point (AP) sends the SSID at regular intervals.

Subnet Mask

Classifies networks into type A, B, and C networks. Each class comprises a subnet mask, masking out the relevant bits. 255.0.0.0 for Class A, 255.255.0.0 for Class B, and 255.255.255.0 for Class C. Example: In a Class C network 254 → IP Addresses are available.

Switch

Switching center in a network.

TKIP

Abbreviation for "**T**emporal **K**ey **I**ntegrity **P**rotocol".

Encryption standard using (like → WEP) the → RC4 algorithm. The key changes on the fly when a data packet of 10 KB was transmitted. Is used in → WPA.

TLS

Abbreviation for "**T**ransport **L**ayer **S**ecurity".

Security protocol using a 128 bit encryption technology. In WLANs, TLS is used in combination with the → EAP protocol to provide a secure exchange of authorization data. EAP-TLS requires certification from both client and server.

URL

Abbreviation for "**U**niform **R**esource **L**ocator".

A URL is an address format for a file that can be accessed via the internet. The type of file is determined by the access protocol (not the file type!). The HTTP protocol, for example, supports HTML pages, Java applets, CGI scripts, etc. The URL consist of:

- the access protocol;
- a host name (the domain);
- a specific filename.

VoIP

Abbreviation for "**V**oice **o**ver **I**P".

Voice transmission using → IP technology.

VPN

Abbreviation for "**V**irtual **P**rivate **N**etwork".

Virtual private networks are set up to ensure secure data transfer via the insecure internet. For the transmission an encrypted connection (VPN tunnel) is set up.

WAP

Abbreviation for "**W**ireless **A**pplication **P**rotocol".

Synonym for graphical applications on mobile phones, organizers and other suitable terminal devices which are transferred according to the standards of the wireless application protocol.

WEP

Abbreviation for "**W**ired **E**quivalent **P**rivacy".

Encryption method used in a WLAN.

WLAN

Abbreviation for "**W**ireless **L**AN".

Wireless local network based on radio or infrared transmission.

WPA

Abbreviation for "**W**iFi **P**rotected **A**ccess".

Encryption method used in a WLAN. WPA provides higher security than → WEP.

WPS

Abbreviation for "**W**LAN **P**ositioning **S**ystem".

Administration Scenarios

Setup failed

Check your configuration against one or more of the following questions:

Is the optiPoint WL 2 professional operated within a → VLAN?

- Enter the VLAN ID manually or (if a → DHCP server is used) set "VLAN Mode" → Page 57 to "DHCP" so that the VLAN ID provided by the DHCP server is used.
 - For more information about "VLAN id" → Page 57.

 → Page 32

Is the optiPoint WL 2 professional operated behind a → Gateway?

- Enter the → IP Address of the gateway in the → Default Gateway field.

 → Page 25

Determine the Software Version

You can determine which software version the optiPoint WL 2 professional is operating on, e.g. before an upcoming software update.

 → Page 20


Check Connections

- Check the connections using the PING test.
 - For more information about the "PING Test" → Page 51.

 → Page 24

Set up FTP server

There are various upload / download options for for the optiPoint WL 2 professional.

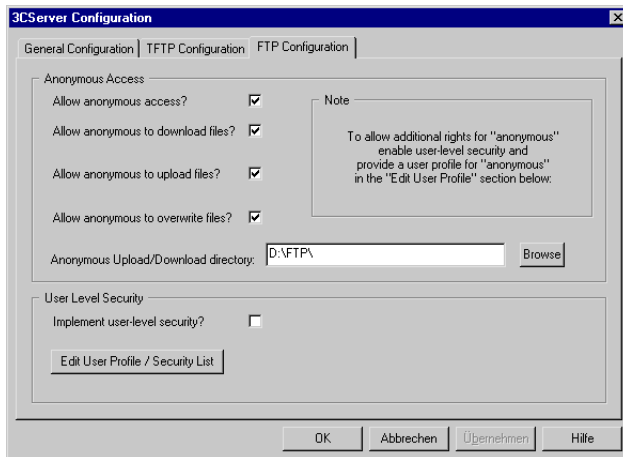
- Using a web interface in an internet browser (e.g. Internet Explorer 5.5),  → Page 20.
- Using the "Deployment Tool" (part of HiPath Manager E). This is useful for managing more than one telephone simultaneously. For more information see the Administration Manual of the Deployment Tool.

In both cases you need a fully configured FTP server to exchange data via → FTP. The server program must be running on a computer (e.g. PC) in the same → LAN as the optiPoint WL 2 professional.

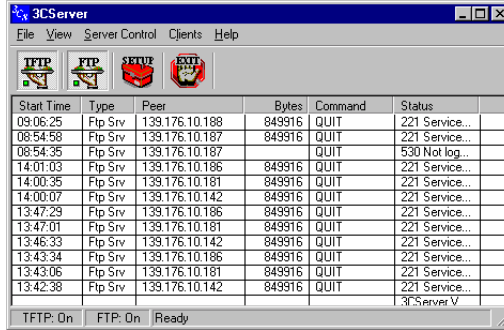
The following section describes (as an example) the setup of the server program "3CServer" produced by "3Com".

Installation and configuration

1. Install the software (e.g. "3CServer", can be downloaded from <http://www.3com.com>).
2. Start the server program.
3. You can set up user profiles or enable anonymous access (as in the example). This is the easier version; however, assigning different rights for different users is not possible in this case. Select **File** → **Config** → **FTP configuration** and enter a directory path and name into the field **Anonymous Upload/Download directory**; this is the directory that will be used for data exchange.



4. Confirm with **OK**. In the main window of the program you see the connection data as soon as there is a data transfer.






The screenshot shows the 3CServer application window with a menu bar (File, View, Server Control, Clients, Help) and four icons (TFTP, FTP, SFTP, RTSP). Below is a table of active sessions.

Start Time	Type	Peer	Bytes	Command	Status
09:06:25	Ftp Srv	139.176.10.188	849916	QUIT	221 Service...
08:54:58	Ftp Srv	139.176.10.187	849916	QUIT	221 Service...
08:54:35	Ftp Srv	139.176.10.187		QUIT	530 Not log...
14:01:03	Ftp Srv	139.176.10.186	849916	QUIT	221 Service...
14:00:35	Ftp Srv	139.176.10.181	849916	QUIT	221 Service...
14:00:07	Ftp Srv	139.176.10.142	849916	QUIT	221 Service...
13:47:29	Ftp Srv	139.176.10.186	849916	QUIT	221 Service...
13:47:01	Ftp Srv	139.176.10.181	849916	QUIT	221 Service...
13:46:33	Ftp Srv	139.176.10.142	849916	QUIT	221 Service...
13:43:34	Ftp Srv	139.176.10.186	849916	QUIT	221 Service...
13:43:06	Ftp Srv	139.176.10.181	849916	QUIT	221 Service...
13:42:38	Ftp Srv	139.176.10.142	849916	QUIT	221 Service...

At the bottom, there are status indicators: TFTP: On, FTP: On, Ready, and a version string: 3C Server V.

Improve Voice Quality

- Change the QoS parameters.
 - For more information → QoS.
 -  → Page 32
- Change the audio compression setting.
 - For more information → Codec
 -  → Page 29
- Activate the suppression of background noise during breaks in a communication for the optiPoint WL 2 professional.
 - For more information → Silence Suppression
 -  → Page 29.

Step-by-Step

No IP address

No Network

No System

Error:
<Error string>

FTP parameter missing
EXIT?

Error Messages and Troubleshooting

No IP Address

The DHCP cannot assign an IP address to the handset
→ Page 47.

Possible solution:

Check the DHCP server.

No Network

The handset cannot find the network.

Possible solution:

Check the network profile.

Registration failed

Invalid PBX number → Page 46, subscriber number
→ Page 55, and/or subscriber password → Page 56.

Possible solution:

Change gateway address → Page 46.
Change subscriber number → Page 55.
Change subscriber password → Page 56.

FTP error messages

Error during file upload/download:
There was an error during the data transmission. The
display shows a corresponding error message.

Not all of the necessary FTP parameters are set.

Possible solution:

Enter FTP Account Name → Page 45.
Enter FTP Password → Page 46.
Enter FTP User Name → Page 46.

Step-by-Step

No Database

PABX not found

Client not registered

Reject cause unknown



Other Error Messages

The connection to or the registration with the database failed.

No IP connection to the gateway.

The telephone is not properly set up for the PABX.

No client licenses available in the gateway.

(Empty display) Power failure → Page 10.

Editors

Most entry fields are pre-defined or offer options for selection (exception: → Text Editor).

Navigation in entry fields



The blinking signal shows the current position of the cursor.



During entry pre-defined numbers or wildcards are overwritten.



Press this key to move the cursor to the left.



Press this key to move the cursor to the right.

Cancel an entry

The entry is cancelled without saving.



Press the display key.



Press the end call or talk key.

Pre-defined entry fields

Integer Editor

Permitted: 0 ... , if necessary * # .



Press key **long** to enter "+" (only available at the first place place in the entry field).

Example: International country code +22



Press the display key to delete highlighted characters.

IP Number Editor

Permitted: Integer values from 0 to 255

Pre-defined default value: 000.000.000.000

Example: 192.168.001.050

Options Editor

Permitted: Pre-defined values





Select value.















Press the display key to save the selected option.

Text Editor

Character entry is performed by multiple presses of the keypad keys according to the following tables. This also applies to the entry of alphanumeric passwords.

Example: "R" = press the key  1x time and the key  3x times.

Key	1x	2x	3x	4x	5x	6x	7x	8x	9x	10x	11x	12x	13x	14x	15x
 [1]		1	€	£	\$	¥	¤								
 2	a	b	c	2	ä	á	à	â	ã	ç					
 3	d	e	f	3	ë	é	è	ê							
 4	g	h	i	4	ï	í	ì	î							
 5	j	k	l	5											
 6	m	n	o	6	ö	ñ	ó	ò	ô	õ					
 7	p	q	r	7	ß										
 8	t	u	v	8	ü	ú	ù	û							
 9	w	x	y	9	ÿ	ý	æ	ø	å						
 0	.	,	?	!	0	+	-	:	¿	¡	/	"	'	;	_
 [2]	[3]	*													
 #	@	\	&	§											

[1]Space

[2]Next character as capital letter (max. active for 1 second)

[3]Switch to numeric input

Appendix

Functions of Passwords and PINs

Password	Function
User PIN	Saves the user-specific settings in the optiPoint WL 2 professional.
Administrator PIN	Protects the administration area from unauthorized access.
FTP Password	Protects file transfers (e.g. firmware downloads).
HiPath Password	Protects the settings for communication with other HiPath devices.
SNMP Password (Community string)	Protects the SNMP server (e.g. error protocol evaluation) from unauthorized access.
Subscriber Password	Protects the transfer of the subscriber number (incl. configuration settings) to another telephone.
Cancel Mobility Password	Protects cancellation if the subscriber number was transferred to another telephone.

Technical Data

WLAN Standard	802.11g (Fall-Back to 802.11b)
Frequency range	2,4 - 2,497 GHz
Selectable channels	13 (ETSI) or 11 (North America)
Distance ^[1]	up to 300 m outside of buildings, up to 30 m inside buildings
Power requirements	Li-Ion-Akku 3,7 V
Environmental specifications (operating)	+5 °C to +45 °C; 20 % to 75 % humidity
Physical dimensions handset	132 x 52 x 22 mm (L x B x H)
Weight handset incl. batteries	approx. 110 g

[1]The distance depends on the environment, in particular the materials between the Access Point and the WLAN telephone.

Operating / Charging Hours

Stand-by time	up to 60 hours ^[1]
Operating hours	up to 4 hours ^[1]
Charging hours	approx. 2 hours ^[1]

[1])These values are only valid if the recommended batteries are used.

Factors influencing standby and talk times

Standby time is the time when the handset is not in use (for example, no calls or other user operation). **Talk time** is the time the handset is used for making calls

Both periods are influenced by the battery charging status and the following factors:

- **Field strength:** he handset's range is heavily influenced by its surroundings and particularly by materials located between the access point and the WLAN phone.
The further away the handset is from the WLAN access point, the shorter the standby and talk times.
- **Display lighting:** Frequently activating the display for long periods of time reduces standby time.
- **Vibration alarm:** Activating the vibration alarm reduces standby and talk times.
- **Codec:** Power consumption is influenced by the packet length used for voice transmission. In the case of G.711, for example, processing packet lengths of 10 ms requires more power than processing packet lengths of 20 ms.
- **Volume setting:** Je lauter ein Parameter eingestellt ist, desto geringer ist die Standby- und Sprechzeit.
- **Further factors:** Environmental conditions (for example, temperature) also influence standby and talk times.

Index

The colored page numbers take you to the description of the operation via the following device/interface:

- **Red:** optiPoint WL 2 professional
- **Green:** web interface
- **Bold:** Explanation in the Alphabetic Reference

Numerics

802.11x

Authentication mode	39
WEP key	57
WEP mode	58

A

Abbreviations	59
Administration Scenarios	67
Administrator PIN	39
Authentication mode	39

B

Backup and restore	40
Batteries	10
Battery power	75

C

Certificate	
select	54
Channel	40
Charging hours	75
Check connections	67
Clear all user data	40
Codec	29, 41
Compression	29
Contrast setting	17
Create backup file	40

D

Deactivate lock	21
Default Gateway	42
Define a new profile	42
Determine the Software Version	67
DHCP	42
Dial with preparation editor	51
Display MAC address	16
Display operating hours	17
Display software version	16
DLS Server Address	30, 42
DLS Server Port	42
DNS Addresses	43
Domain Name	43
Drop Preference Levels for Voice	43

E

E.164 (Subscriber number)	28, 55
EAP	60
Echo effect	6
Emergency number	28, 44
Encryption mode	44
Error messages	70
Explanation of technical terms	59
External Access Code	29, 43

F

Factory settings	
password,Function	74
Firmware update	45, 48
Firmware Version	45
Fragmentation Threshold	45
FTP	
Account Name	34, 45
Password	34, 46
Port	46
Server Address	34, 46
Username	34, 46

G

G722 codec	29
Gatekeeper address	28, 46
Gatekeeper Port	46
Gateway Port	28

H

Handset IP Address	47
Handset Name	23, 47
Handset PIN	47
Handset restart	47
Handset State	23, 47
Handset Version	23
Hardware Version	47
Hidden menu "Service"	15

I

Installation of the telephone	10
IP Routing	48

K

Keypad lock	11
-------------	----

L

LDAP	
Port number	30, 48
Server address	30, 48
Local Area Code	29, 48
Local Country Code	29, 49
Local District Code	29, 49
Location Identifier Number	28, 49
Location Server	31, 49
Location Server Address	49
Location Server enable	49
Location Server Port number	49
Logout	21

M

MAC Address	23, 49
Mobility Password	50

N

Nameplate	6
National Access Code	50
National Dial Prefix	29
Navigation in entry fields	72
Network mode	50

Network Name	50
Non-compressing Codec Threshold	
Values	50
Notes	8

O

Operating hours	75
Output power	50

P

Packet size	29
Password	39
Phone Identity	23
PING Test	37, 51
Positioning system	17
Preamble Type	51
Profile list	52
Profile Name	52
Profile number	52
Profile selection	24

Q

QCU server address	52
QoS for Ethernet	
Priority for Signalling	52
Priority for Voice	52
QoS for IP	
Drop Preference Levels for Voice	43
DSCP Class for Signalling	43
DSCP Class for Voice	43

R

Redial list	53
Release handset	21
Report interval	53
Report mode	54
Reset to factory default	18
Reset User Data	33
Reset user parameters	18
Restart Handset	33
Restore to factory defaults	36, 44
Retrieve certificate	53
Roaming Threshold	53
RTS/CTS Threshold	53

S

Safety precautions	2
Serial number	6
Service menu	
Access	15
Service menu, hidden	15
Set backlight duration	18
Set logout time	55
Set up FTP server	68
Set up profile	39, 43
Setting Up	10
Setting Up the Telephone	10
Settings for WLAN profile	26
Setup failed	67
Silence Suppression	29, 55
SNMP	
active	33
Password	33, 55
Server Address	33, 55
Trap Port	33
SSID	50
Standby time	75
Subnet Mask	55
Subscriber number	28, 55
Subscriber Password	28, 56
Symbols	8, 39
System Type	56

T

Talk time	75
Technical Data	
optiPoint WL 2 professional	74
Technical terms	59
Telephone software update	45
Threshold Settings	56
TLS	65
Transfer mode	56
Transmit rate	56

U

User PIN	47
User Settings	56

V

VLAN	
ID	57
Mode	57
VPN	57
IP Address	57
VPN settings	31

W

WEP	
Authentication mode	39
WEP key	57
WEP mode	58
WLAN	
Settings	26
WLAN Profile	24
WPA	
Encryption type	44
Group Rekey Intervall	47
WPA-PSK	
Encryption type	44
Group Rekey Intervall	47
Pre Shared Key	51

www.siemens.com/hipath



The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products.

An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract.

The trademarks used are owned by Siemens AG or their respective owners.

© Siemens AG 2005
Siemens Communications
Hofmannstr. 51 • D-81359 München

Ref. No.: A31003-A2056-W200-2-76A9

Subject to availability. Right of modification reserved.
Printed in the Federal Republic of Germany.
05.12.05