SIEMENS

blue2net
LAN Access Point

Bluetooth™

User Guide

Issue August 2002, Version 2.0

Copyright 2002 by Siemens AG Österreich. All rights reserved.

BLUETOOTH is a trademark owned by Bluetooth SIG, Inc., U.S.A, and licensed to Siemens AG.

Linux and Embedded Linux are trademarks of Linus Torvalds

Windows, Internet Explorer and MS Media Player are trademarks of Microsoft Corporation

Real Player™ is a trademark of Real Systems.

Quick Time™ is a trademark of Apple Corp.

The information contained in this manual and the software it describes are subject to change without notice for the purpose of technical improvement.

Information on Siemens Bluetooth™ products

http://www.siemens.at/bluetooth

Issue August 2002, Version 2.0

Safety Precautions

Power supply:

Only use the power supply unit supplied:

Part number: N4 EFS3 3W 4.4V (EU-version)
N4 GFS3 3W 4.4V (UK-version)
N4 UFS3 3W 4.4V (US-version)

Only use the device where the mains voltage is in accordance with the input voltage printed on the power supply unit.

A certain temperature rise is normal and harmless.

Ensure that while in use the device is not covered and not situated near a heater or exposed to direct sunlight.

Use only for information technology devices.

For indoor use only - do not expose device to rain.

To clean device, wipe with a dry cloth. Do not use solvents.

blue2net:

Other electrical equipment (e.g. medical equipment in a medical clinic) may be affected by the use of the device. Therefore, set up the device only in locations where it causes no interference with such equipment.

Do not install blue2net in bathrooms or shower rooms.

Do not operate the device in environments where there is a risk of explosion (e.g. paint shops, gas stations).

Ensure that the operating instructions are included when passing on your blue2net to a third party.

At the end of its life cycle the device has to be disposed of in an environmentally friendly way. As environmental regulations and facilities vary from country to country, Contact your local authorities, the relevant person in your company or your local dealer for advice on how best to dispose of the device.

The device should not be opened under any circumstances. Any modifications will invalidate both its approval for use and warranty.

Contents

Safety Precautions ..... **iii**

1 Introduction **1**

2 First Installation of blue2net **2**

2.1 Checking Package Contents 2
2.2 Installation Notes 2
2.3 Connecting blue2net to Your Ethernet 3
2.4 Explanation of LED Behavior 6
2.5 Connecting to blue2net via Bluetooth 6
2.6 Accessing the Built-In blue2net Web Server 6
2.7 How to Get to the Configuration Page 8
2.8 Choosing Security Settings 9
2.9 Important Default Settings 10

3 Configuration **11**

3.1 Main Configuration Page 11
3.2 General Procedure for Changing Parameters 13
3.3 Hierarchy of Pages for Configuration Settings 14
3.4 Bluetooth Parameters [1] 16
3.5 IP Parameters for blue2net [2] 24
3.6 IP Parameters for Terminals [3] 32
3.7 Current Configuration [4] 37
3.8 Configuration Access [5] 42
3.9 Activation Commands [6] 43

4 Use Scenarios **48**

4.1 Business Scenario with Controlled Access 48
4.2 Public Use Scenario (Hot Spot) 49
4.3 Home Use Scenario with Cable Modem 50
4.4 Home Use Scenario with xDSL Modem 51

5 Preventing Lockout **53**

5.1 Lockout from Access via Bluetooth and Ethernet (LAN) 53
5.2 Lockout from Access via Bluetooth 54
5.3 Lockout from Access via Ethernet (LAN) 54

6 Update Software **55**

6.1 How to Download New Software 55

7 Store Specific Homepage **59**

7.1 How to Load Your Specific Homepage 59

8 Troubleshooting **62**

8.1 Hardware 62
8.2 Bluetooth Connection 62
8.3 LAN/Internet Access 63
8.4 Software Update 64
8.5 Configuration Access 65

9 Firewall in blue2net 66

10 Regulatory Statement 67

10.1 General..... 67
10.2 European Union (EU) and EFTA Member States..... 67
10.3 United States of America (USA) 68

11 Bluetooth Compliance 69

12 Default Values 70

13 Abbreviations and Terms 72

14 Service / Contact 74

15 Warranty and Product Liability 75

16 Technical Data 76

17 Index 77

18 CE-Declaration 80

Dimension Diagram 81

List of Figures

Figure 1 blue2net's directivity and how to achieve good transmission results 2
Figure 2 blue2net bottom view; connectors, mounting holes, LED, and label 4
Figure 3 blue2net Web interface 8
Figure 4 Main configuration page [0] 11
Figure 5 Authentication 11
Figure 6 Bluetooth Parameters [1] 16
Figure 7 Bluetooth Device Name [1.1] 19
Figure 8 Service Table [1.8] 20
Figure 9 Terminal Table [1.10] 22
Figure 10 IP Parameters for blue2net [2] 24
Figure 11 Fixed blue2net IP Configuration [2.2] 26
Figure 12 DHCP blue2net IP Objects, DHCP setup [2.3] 27
Figure 13 Firewall Settings [2.6] 28
Figure 14 Tunnel Configuration (PPPoE / PPTP) [2.7] 29
Figure 15 Authentication Parameters [2.7.3] 31
Figure 16 IP Parameters for Terminals [3] 32
Figure 17 Terminal IP Address Pool Table [3.3] 34
Figure 18 Terminal Fixed Servers [3.5] 35
Figure 19 Current Configuration [4] 37
Figure 20 blue2net IP Configuration [4.2] 38
Figure 21 Terminal Server Configuration [4.3] 39
Figure 22 Version Information [4.4] 40
Figure 23 Tunnel Status [4.5.1] 41
Figure 24 Configuration Access [5] 42

Figure 25 Change of the blue2net Configuration Password [5.2.1] 43
Figure 26 Activation Commands [6] 44
Figure 27 Saving blue2net parameters 44
Figure 28 Software update: Login to blue2net 56
Figure 29 Software update: Dragging the software image file to blue2net 56
Figure 30 Software update: Progress of copying the software image file 57
Figure 31 Saving the software update 57
Figure 32 Progress of the Software Update process 58
Figure 33 Specific homepage: Login to blue2net 60
Figure 34 Specific homepage: Storing the specific homepage 60
Figure 35 CE Conformity Marking 67
Figure 36 Declaration of Conformity 80
Figure 37 Dimension Diagram 81

List of Tables

Table 1 Important default settings 10
Table 2 Parameters on the main configuration page [0] 12
Table 3 Hierarchy of pages for configuration settings (1) 14
Table 4 Hierarchy of pages for configuration settings (2) 15
Table 5 Bluetooth Parameters [1] 18
Table 6 Bluetooth Device Name [1.1] 19
Table 7 Service Table [1.8] 21
Table 8 Terminal Table [1.10] 23
Table 9 IP Parameters for blue2net [2] 25
Table 10 Fixed blue2net IP Configuration [2.2] 26
Table 11 DHCP blue2net IP Objects, DHCP setup [2.3] 27
Table 12 Firewall Settings [2.6] 28
Table 13 Tunnel Configuration (PPPoE / PPTP) [2.7] 30
Table 14 Authentication Parameters [2.7.3] 31
Table 15 IP Parameters for Terminals [3] 33
Table 16 Terminal IP Address Pool Table [3.3] 34
Table 17 Terminal Fixed Servers [3.5] 36
Table 18 Current Configuration [4] 37
Table 19 blue2net IP Configuration [4.2] 38
Table 20 Terminal Server Configuration [4.3] 39
Table 21 Version Information [4.4] 40
Table 22 Tunnel Status [4.5.1] 41
Table 23 Status messages (examples) 41
Table 24 Configuration Access [5] 42
Table 25 Use scenarios: settings for a business scenario w. controlled access 48
Table 26 Use scenarios: settings for public use scenarios (hot spot) 49
Table 27 Use scenarios: settings for home use with cable modem 50
Table 28 Use scenarios: Settings for home use with xDSL modem 52
Table 29 Lockout scenarios: Lockout from Bluetooth and Ethernet (LAN) 53
Table 30 Lockout scenarios: Lockout from Bluetooth access 54
Table 31 Lockout scenarios: Lockout from access via Ethernet (LAN) 54
Table 32 Troubleshooting: Hardware 62
Table 33 Troubleshooting: Bluetooth connection 63
Table 34 Troubleshooting: LAN access 64
Table 35 Troubleshooting: Software update 64
Table 36 Troubleshooting: Configuration access 65
Table 37 Services that can be used while the firewall is enabled 66
Table 38 Conformity with standards and specifications 67
Table 39 Factory settings (default values) (1) 70
Table 40 Factory settings (default values) (2) 71
Table 41 Abbreviations and terms (1) 72
Table 42 Abbreviations and terms (2) 73
Table 43 Technical Data 76

1 Introduction

What is blue2net?

blue2net provides the user with the possibility to gain access to all services and resources of a LAN (Local Area Network) via a radio connection.

Up to 7 Bluetooth clients may be connected simultaneously to an IP network via Ethernet. In line with the Bluetooth specification 1.1, blue2net uses the LAN Access Profile, which means full IP integration over a PPP link.

A broad range of security options along with an integrated firewall regulate access rights and prevent unauthorized connections from being set up.

You simply connect the LAN Access Point to an Ethernet interface. Within a short period of time, the device will be ready to receive signals within a range of approximately 10 to 30 meters.

As a user you need nothing but a PC, laptop or PDA with an appropriate Bluetooth module. Such an adapter can be plugged in via USB or PCMCIA.
A number of notebooks already have Bluetooth on board.

The Embedded Linux-based Siemens LAN Access Point works with all commonly used Bluetooth adapters. You can configure the device via a Web interface from all commonly used browsers. If you have to administrate a larger number of access points, you can carry out the configuration via SNMP.

Fields of application:

Conference participants are able to work on their corporate network without the nuisance of cables. In an office building, field service staff is able to comfortably and quickly update and synchronize their data with that stored on the server.

Public places, such as airports, train stations, hotels, restaurants, shopping malls, or Internet cafés can provide travellers or their customers with the most diverse range of information and services. This information is made available free of charge, as radio connections via Bluetooth do not give rise to license fees.

Home users are able to surf the Internet and retrieve e-mails wirelessly – while sitting on their sofas – with the LAN Access Point providing the connection over a cable modem (e.g. Chello) or an xDSL modem.

2 First Installation of blue2net

2.1 Checking Package Contents

1 blue2net unit

1 power supply unit, either EU-version: N4 EFS3 3W 4.4V or
UK-version: N4 GFS3 3W 4.4V or
US-version: N4 UFS3 3W 4.4V

1 blue2net User Guide CD-ROM or booklet ,

4 adhesive rubber feet

2 screws and 2 wall plugs

2.2 Installation Notes

- Please pay attention the safety precautions
- Install only indoors within a temperature range of 0 to +40 °C (+32 to +104°F)
- A 220/230V~ (110/120V~) mains socket and Ethernet connection should be available close to where blue2net is installed and be easily accessible.
- Only use the original power supply unit that comes with the package.
- Upon first installation, where a connection to the LAN will be established for the first time and where basic configuration settings will be carried out, the device may be placed on the table beside the laptop. Do not mount the device in its final position until the first installation has been completed.
- blue2net's built-in antenna is directional (see Figure 1). The farther the distance between blue2net and the Bluetooth devices, the more important does it become to take account of that directivity in order to achieve optimum reach and data transmission rates. We would advise you to try out various wall-mounted and other installation positions to find the optimum place for your blue2net unit before you start drilling holes for the fastening screws.

Directivity-based transmission results:

B ....Best results
L.....Less favorable
W ...Worst results

Figure 1 blue2net's directivity and how to achieve good transmission results

- You can also use blue2net's directivity to position the unit in such a way that the amount of radiation emitted into neighboring areas remains as low as possible (privacy, interference).

- The installation site should not be located in the immediate vicinity of devices, such as microwave ovens, that use the same or adjacent frequencies.
- The device can be mounted on a wall or ceiling or can be placed on a flat, but non-slippery, surface. Do not place it directly on the floor (danger of damage).
- Install it in a central location, e.g. in a hallway. Try to avoid placing blue2net where the Bluetooth radio signals can be shadowed by obstacles (e.g. thick walls).
- If you want to mount the device close to surrounding objects, leave enough room for cables on the connector side (min. 60 mm). On the opposite side leave enough room for moving the device in order to mount it on the screws (min. 20 mm). A dimension diagram is provided at the end of the user guide.
- The device feet usually do not leave marks on surfaces. However, due to the variety of varnishes and polishes in use, marks cannot be entirely excluded.

2.3 Connecting blue2net to Your Ethernet

There are two ways to operate blue2net:

- on a LAN (e.g. corporate network, Internet Service Provider cable modem)
- on an xDSL modem

When shipped, blue2net comes configured for LAN operation.

2.3.1 LAN Operation

Basically, what you need to operate a device such as blue2net on a LAN is an IP address.

DHCP (Dynamic Host Configuration Protocol) is the most common mechanism used in corporate LANs and used by cable modem providers to assign IP addresses to clients such as blue2net. Contact your network administrator or ISP (Internet Service Provider) to check if your LAN provides DHCP. For DHCP administration purposes, you might be asked for the *MAC address* of your blue2net. This information is provided on the label at the bottom side of the blue2net case (see Figure 2).

blue2net tries to get its IP address via DHCP. If DHCP service is not available, blue2net will use its own fallback IP address, and the IP address will have to be assigned manually.

How to proceed:

1. Connect **first the Ethernet cable** (cable is not part of the shipment) to the Ethernet cable connector (RJ45) and then the power supply unit to the power supply connector (RJ11)
   (see Figure 2).

2. After about 40 seconds, check if the indicator LED (see Figure 2) displays a steady light. If so, you can be sure that blue2net got its IP address assigned by a DHCP server.

blue2net is now ready to use ***but not secured***.

To choose suitable settings for your requirements (particularly security) please proceed with chapter 2.8

3. If the LED displays a steady light only after about 2 minutes, DHCP service is not available and blue2net will use its own fallback IP address (192.168.1.2). to be able to start up. However, with this IP address, you cannot get a connection to the LAN. Now you have two options:
   - Call the network administrator or ISP (Internet Service Provider) to find out why a DHCP service was not available.
   - If there is no way for you to make use of a DHCP service, you have to configure blue2net manually to predefined values.

     Please consult an expert in network technology (e.g. a network administrator for the company LAN or one from the ISP) to get a connection to the LAN.

     After the manual configuration has been successfully carried out and a connection to the network is established, blue2net is basically ready to use. However, you still need to define the *security settings*. To choose suitable settings for your requirements please proceed with chapter 2.8.

Figure 2 blue2net bottom view; connectors, mounting holes, LED, and label

2.3.2 xDSL Modem Operation

When shipped, blue2net comes configured for LAN or cable modem operation.

To operate blue2net on an xDSL modem, you have to define specific settings for certain parameters (these parameters are listed (in bold print) in Chapter 4.4. For a detailed description of all the paramters for the tunnel configuration to be used for that purpose, refer to chapter 3.5.4).

Remember not to set up the cable connection to the xDSL modem until you have configured blue2net accordingly for your xDSL access.

As a rule, home users will rely on a Bluetooth connection to define the configuration on the Bluetooth terminal (e.g. laptop). Configuration via Ethernet is possible, too, but requires more in-depth network know-how.

How to proceed:

1. Connect the power supply unit to the power outlet (RJ11 connector) (see Figure 2).

   Note: It takes about 2 minutes until you can proceed to the next step, as blue2net has to go through its startup phase after having been connected to the power supply.

2. Make xDSL configuration settings and then save settings to permanent memory:
   - For a listing of the paramters affected, refer to chapter 4.4. (bold print).
   - For information on how to set up a Bluetooth connection and how to access the configuration setttings, refer to chapters 2.5 to 2.6.2 and 3.
   - For instructions on how to save data to permanent memory, refer to chapter 3.9.2.

   Note: Once the configuration is completed, a reset and subsequent restart will take place. All Bluetooth connections will be terminated.

3. Wait until the configuration is completed before you set up the cable connection (cable is not part of the shipment) to the xDSL modem (RJ45 connector) (see Figure 2).

blue2net is now ready to use, ***but not secure yet***.

To make it secure, you still have define the security settings. Continue with chapter 2.8 to select the settings best suited for your requirements, especially your security requirements.

2.4 Explanation of LED Behavior

Behavior	Explanation
Not lit	No power
Steadily lit	Ready for operation, IP address assigned
Flashing normally	Starting up
Flashing slowly	Trying to get an Ethernet connection
Flashing rapidly	Software update

2.5 Connecting to blue2net via Bluetooth

Make sure that your Bluetooth terminal, such as a laptop or a PDA, supports this technology and is fully compliant with the Bluetooth LAN access profile.

Follow the steps described in the **User Guide** of your **Bluetooth terminal**.

Basically, what you need to do is:

- Start the Bluetooth application on your terminal.
- Search with your Bluetooth terminal for reachable Bluetooth devices (Bluetooth Device Inquiry).
- Choose your blue2net from the list of devices displayed and connect to it. In order to identify your blue2net device among other devices displayed, look for the Bluetooth address of your blue2net. This information is provided on the label at the bottom side of the blue2net case (see Figure 2).
- When a login window appears on your terminal you have to enter a Bluetooth Passkey. By default, this Bluetooth passkey is set to '**1234**' on blue2net.
- Please ensure that your terminal starts a PPP-connection such as Windows RAS (Remote Access Service).

2.6 Accessing the Built-In blue2net Web Server

blue2net provides a Web interface for configuring parameters, checking the settings and device information, and also for carrying out software upgrades. There are two possibilities to access the Web server – Access via Bluetooth or access via Ethernet.

2.6.1 Required Browser Settings

- **Disable** the **proxy settings** on the Web browser of your PDA or laptop.
- **Enable** the **cookies!**

2.6.2 Access via Bluetooth

- You need an established Bluetooth connection to blue2net as described in chapter 2.5.

- Access blue2net's Web interface by entering http**s**://192.168.2.2 (Note that blue2net only supports secure access via http**s**) in the location/URL field of your Web browser. This is the default IP address for terminals connected via Bluetooth. Figure 3 shows the homepage of the blue2net Web interface.

2.6.3 Access via Ethernet (LAN)

Access via Ethernet is recommended for experts only. Basically follow the instructions below:

- If the IP address of your blue2net was assigned via DHCP, you have to find out the value of this IP address. There are three ways to do so:
  a) On Bluetooth-Terminal: When shipped, blue2net comes configured in such a way that upon Bluetooth device inquiry the display on your Bluetooth terminal will show the current IP address after the Bluetooth device name of your blue2net unit.
  b) Ask your network administrator or Internet Service Provider.
  c) Access blue2net via Bluetooth (see 2.6.2) and read the value of the parameter 'blue2net IP Address' (see 3.7.1).
- If the IP address was not assigned via DHCP, blue2net uses the fallback IP address (192.168.1.2). Make sure your network configuration on the client matches the segmentation of the IP address of blue2net.
- Access blue2net's Web interface by entering **https://<IP address of blue2net>** in the location/URL field of your Web browser (see Figure 3).

2.7 How to Get to the Configuration Page

Figure 3 blue2net Web interface

- Click on **Configuration** on the first page of blue2net's Web interface (see Figure 3).
- The default password for configuration access is "**changeme**". It is recommended to change the password after the first time you use it (see chapter 3.8). Keep the password in a safe place separate from your blue2net, user guide, laptop, PDA, or PC.

Caution: If you forget your *configuration password*, you can no longer access the blue2net settings. You will then be locked out of the configuration settings. The same applies for other important parameters. For more information on this essential issue, see chapter 5, "Preventing Lockout".

2.8 Choosing Security Settings

After your blue2net has completed its start up phase it is basically ready to use. However, the access to the LAN and to the configuration page of blue2net is *not yet secure*. With the given default settings anybody can access blue2net from any nearby Bluetooth terminal or from PCs via LAN.

To make your configuration secure you have the following options:

- Chapter 4 provides settings for 4 typical use scenarios for users who want to have quick results but are not yet acquainted with the configuration functions.
- Chapter 3 provides details on each of the configuration settings that enable you may be able to adjust blue2net to your own specific requirements.

Depending on your personal approach choose the settings and then continue with the actual configuration process as described below.

2.9 Important Default Settings

Your blue2net comes with the following important factory settings for Bluetooth and IP parameters:

Parameter	Hierarchy level [1)]	Factory Setting
Bluetooth Device Name	[1.1.1]	blue2net
IP Address Suffix Mode	[1.1.2]	enabled
Multipoint Mode	[1.3]	enabled
Discoverability Mode	[1.4]	discoverable
Connectability Mode	[1.5]	connectable
Default Access Mode	[1.11]	enabled
Default Bluetooth Passkey	[1.12]	1234
blue2net IP Address Resolution	[2.1]	dhcp
IP Masquerading [2)]	[2.5]	192.168.2.2
Fallback blue2net IP Address	[2.3.1]	192.168.1.2
Fallback blue2net Netmask	[2.3.2]	255.255.255.0
Fallback blue2net Gateway	[2.3.3]	192.168.1.1
Terminal IP Address Resolution	[3.1]	masquerading
Terminal DNS Server 1	[3.5.1]	192.168.3.11
Terminal DNS Server 2	[3.5.2]	192.168.3.12
Terminal WINS Server 1	[3.5.3]	192.168.3.13
Terminal WINS Server 2	[3.5.4]	192.168.3.14
Terminal Domain Name	[3.5.5]	my.domain.at
blue2net Gateway	[4.2.3]	192.168.1.1
Configuration Password	[5.2]	changeme
Server Channel [3)]		2

Table 1 Important default settings

[1)] See chapter 3.3
[2)] Default IP address for accessing the Web server via Bluetooth
[3)] This value has to be defined manually for some Bluetooth terminals (see the user guide of your Bluetooth terminal)

A complete list of default values for all parameters is provided in chapter 12

3 Configuration

3.1 Main Configuration Page

Click on **Configuration** on the Web interface (see Figure 3) to get the following overview (Figure 4). The numbers between square brackets indicate the place of a parameter in the hierarchy of the Web interface (see chapter 3.3 for details).

Figure 4 Main configuration page [0]

Click on one of the <edit> buttons. You will then be prompted to enter the configuration password. The initial password is "**changeme**"

Figure 5 Authentication

Click on the <Submit> button and the main configuration page will be displayed.

For security reasons, you should then immediately change the password. Then save your changes: Do not forget to save your changes using the *activation commands* (see chapter 3.9)!

Note: Make sure you remember your new password or store it in a safe place. Once the password has been changed, configuration access is possible only with the new password! See also chapter 5

Objects (see Figure 4)	**Hierarchy level**	**Explanation**
Bluetooth Parameters	[1]	Here you can change all parameters relevant for Bluetooth, e.g. Bluetooth device name, multipoint mode, discoverability, connectability, default access mode and default Bluetooth passkey.
IP Parameters for blue2net	[2]	Here you can define the IP parameter settings such as *predefined* or *dhcp*.
IP Parameters for Terminals	[3]	Here you can define the IP parameter settings for the connected terminals, such as Terminal IP address resolution and Terminal IP address pool.
Current Configuration	[4]	Here you can see the current configuration for blue2net IP values, terminal IP values, and the version information of the device.
Configuration Access	[5]	Here you can change the configuration password or enable/disable SNMP access.
Activation Commands	[6]	Here you can save your configuration changes either just temporarily or permanently. You can also update your blue2net to a new software version, if available, or load your own specific home page on your blue2net. Further commands provided force a reset to factory settings or values stored in permanent memory.

Table 2 Parameters on the main configuration page [0]

3.2 General Procedure for Changing Parameters

Click the <edit> button next to the parameter you want to change. In the following input window, set or enter the value.

If you want to reset your changes, click on the <Undo> button in order to get the value initially displayed.

If you click on the Web browser's <Back> button, you will return to the previous page and none of your changes will take effect.

Once you are sure your input is correct, click on the <Submit> button. After that, you will get a confirmation of the change or an error message.

Any changes you perform on blue2net settings will only take effect when you save them with one of the *activation commands* (see chapter 3.9).

Bluetooth connections will be terminated if you use one of the activation commands to save changes (see chapter 3.9) !.

After having made configuration changes, it is recommended to close the browser using the [Close Session] function. Otherwise, for safety reasons blue2net will generate waiting periods of up to 10 minutes before you can have access to the configuration menu.

3.3 Hierarchy of Pages for Configuration Settings

The purpose of this table is to make it easier for you to find the place of the various parameters on the pages of the built-in Web interface where you can perform the settings. Each parameter or set of parameters has a number reflecting its place in the hierarchy. This number, shown between square brackets such as [#.#], is always referred to in figures, tables, and cross references, e.g. [1.8.4] for 'Auth. Level'.

On the right-hand side you can see

- an action you can perform for this parameter (edit, Submit) or
- a value that is displayed (number, address, domain, version)
- a table to be displayed
- objects to be displayed

[0] **Main Configuration Page** (chapter 3.1)		action / display of	page
[1] **Bluetooth Parameters** (chapter 3.4)			**16**
[1.1]	Bluetooth Device Name	➡ Objects	16
[1.1.1]	Bluetooth Device Name	edit, ▶ Submit	19
[1.1.2]	IP Address Suffix Mode	edit, ▶ Submit	19
[1.2]	Bluetooth Device Address	unique fixed address	17
[1.3]	Multipoint Mode	edit, ▶ Submit,	17
[1.4]	Discoverability Mode	edit, ▶ Submit	17
[1.5]	Connectability Mode	edit, ▶ Submit	17
[1.6]	Max. No. of Terminals Connected	edit, ▶ Submit	17
[1.7]	Number of Services	number	18
[1.8]	Service Table	➡ Table (1 row)	18 & 19
[1.8.1]	Service Index	number	20
[1.8.2]	Service Name	edit, ▶ Submit	20
[1.8.3]	Service Description	edit, ▶ Submit	20
[1.8.4]	Auth. Level	edit, ▶ Submit	21
[1.8.5]	Service Provider	edit, ▶ Submit	21
[1.8.6]	Service URL	edit, ▶ Submit	21
[1.8.7]	Service ID	edit, ▶ Submit	19
[1.9]	Number of Terminals	number	18
[1.10]	Terminal Table	➡ Table (10 rows)	18
[1.10.1]	Terminal Index	number	23
[1.10.2]	Terminal Bluetooth Address	edit, ▶ Submit	23
[1.10.3]	Terminal Bluetooth Passkey	edit, ▶ Submit	23
[1.10.4]	Terminal IP Address	edit, ▶ Submit	23
[1.11]	Default Access Mode	edit, ▶ Submit	18
[1.12]	Default Bluetooth Passkey	edit, ▶ Submit	18
[2] **IP Parameters for blue2net** (chapter 3.5)			**24**
[2.1]	blue2net IP Address Resolution	edit, ▶ Submit	24
[2.2]	Fixed blue2net IP Configuration	➡ Objects	24
[2.2.1]	Fixed blue2net IP Address	edit, ▶ Submit	26
[2.2.2]	Fixed blue2net Netmask	edit, ▶ Submit	26
[2.2.3]	Fixed blue2net Gateway	edit, ▶ Submit	26
[2.3]	DHCP blue2net IP Objects	➡ Objects	25
[2.3.1]	Fallback blue2net IP Address	edit, ▶ Submit	27
[2.3.2]	Fallback blue2net Netmask	edit, ▶ Submit	27
[2.3.3]	Fallback blue2net Gateway	edit, ▶ Submit	27
[2.4]	Time Server IP	edit, ▶ Submit	25
[2.5]	IP Masquerading	edit, ▶ Submit	25

Table 3 Hierarchy of pages for configuration settings (1)

[2.6]	Firewall Settings		➡ Objects	25
	[2.6.1]	Default Firewall	edit, ▸ Submit	28
[2.7]	Tunnel Configuration		➡ Objects	25
	[2.7.1]	Tunnel Mode	edit, ▸ Submit	30
	[2.7.2]	Tunnel Establishment Control	edit, ▸ Submit	30
	[2.7.3]	Authentication Parameters	➡ Objects	30
		[2.7.3.1] Tunnel User Name	edit, ▸ Submit	31
		[2.7.3.2] Tunnel User Pasword	edit, ▸ Submit	31
	[2.7.4]	PPTP Server IP Address	edit, ▸ Submit	30
[3]	**IP Parameters for Terminals** (chapter 0)			**29**
[3.1]	Terminal IP Address Resolution		edit, ▸ Submit	33
[3.2]	Number of Terminal IP Address Pool Entries		number	33
[3.3]	Terminal IP Address Pool Table		➡ Table (7 rows)	33
	[3.3.1]	Terminal IP Address Index	number	34
	[3.3.2]	Terminal IP Address Pool Value	edit, ▸ Submit	34
[3.4]	Terminal Net Mask		edit, ▸ Submit	33
[3.5]	Terminal Fixed Servers		➡ Objects	33
	[3.5.1]	Terminal DNS Server 1	edit, ▸ Submit	35
	[3.5.2]	Terminal DNS Server 2	edit, ▸ Submit	36
	[3.5.3]	Terminal WINS Server 1	edit, ▸ Submit	36
	[3.5.4]	Terminal WINS Server 2	edit, ▸ Submit	36
	[3.5.5]	Terminal Domain Name	edit, ▸ Submit	36
[4]	**Current Configuration** (chapter 3.7)			**37**
[4.1]	MAC Address		unique fixed address	37
[4.2]	blue2net IP Configuration		➡ Objects	38
	[4.2.1]	blue2net IP Address	address	38
	[4.2.2]	blue2net Netmask	address	38
	[4.2.3]	blue2net Gateway	address	38
[4.3]	Terminal Server Configuration		➡ Objects	39
	[4.3.1]	Terminal DNS Server 1	address	39
	[4.3.2]	Terminal DNS Server 2	address	39
	[4.3.3]	Terminal WINS Server 1	address	39
	[4.3.4]	Terminal WINS Server 2	address	39
	[4.3.5]	Terminal Domain Name	domain	39
[4.4]	Version Information		➡ Objects	40
	[4.4.1]	Module Firmware Version	version	40
	[4.4.2]	PPCBoot Version	version	40
	[4.4.3]	blue2net Software Version	version	40
	[4.4.4]	blue2net Hardware Version	version	40
	[4.4.5]	SieMo Module Info	version	40
[4.5]	Tunnel Status (PPPoE/PPTP)		➡ Objects	37
	[4.5.1]	Tunnel Status	status of tunnel conn.	41
[5]	**Configuration Access** (chapter 3.8)			**42**
[5.1]	SNMP Access		edit, ▸ Submit	42
[5.2]	Configuration Password		edit	42
	[5.2.1]	Change of configuration password	▸ Submit	43
[6]	**Activation Commands** (chapter 3.9)			**43**
[6.1]	Save Settings Temporarily		edit, ▸ Submit	45
[6.2]	Save Settings Permanently		edit, ▸ Submit	46
[6.3]	Reset blue2net		edit, ▸ Submit	46
[6.4]	Update Software		edit, ▸ Submit	47
[6.5]	Restore Default Settings		edit, ▸ Submit	47
[6.6]	Store Specific Homepage		edit, ▸ Submit	47

Table 4 Hierarchy of pages for configuration settings (2)

3.4 Bluetooth Parameters [1]

This chapter describes the Bluetooth parameters for the blue2net device and the Bluetooth terminals.

You can change the values that come with an <edit> button or are accessible in the secondary level when you click "Table". Click on one of the underlined object names to get an online description.

Bluetooth Parameters

	Object	Value
[1.1]	Bluetooth Device Name	Objects
[1.2]	Bluetooth Device Address	08:00:06:58:27:74
[1.3]	Multipoint Mode	enabled edit
[1.4]	Discoverability Mode	discoverable edit
[1.5]	Connectability Mode	connectable edit
[1.6]	Max. No. of Terminals Connected	7 edit
[1.7]	Number of Services	1
[1.8]	Service Table	Table
[1.9]	Number of Terminals	10
[1.10]	Terminal Table	Table
[1.11]	Default Access Mode	enabled edit
[1.12]	Default Bluetooth Passkey	1234 edit

Figure 6 Bluetooth Parameters [1]

Objects (see Figure 6)	Hier. level	Factory setting, other values, value range	Explanation
Bluetooth Device Name	[1.1]	blue2net other name (1...16 characters)	Access to configuration of user-friendly blue2net name and to activation of IP address display

Objects (see Figure 6)	**Hier. level**	**Factory setting, other values, value range**	**Explanation**
Bluetooth Device Address	[1.2]	fixed unique value	This is the unique Bluetooth address of your blue2net. You can also find this address (Bluetooth-Adr.) printed on the label at the bottom side of the blue2net case.
Multipoint Mode	[1.3]	enabled disabled	If 'Multipoint Mode' is set to *enabled*, up to 7 clients can establish a connection to blue2net simultaneously. If 'Multipoint Mode' is *disabled*, only one client can connect in this mode, because no master-slave switch is forced from blue2net. Note: Some older Bluetooth terminals will work only if 'Multipoint Mode' is *disabled*
Discoverability Mode	[1.4]	discoverable nondiscoverable	When blue2net is set to *discoverable*, it is visible to other devices upon Bluetooth device inquiry. When blue2net is set to *nondiscoverable*, it is not visible to other devices upon Bluetooth device inquiry.
Connectability Mode	[1.5]	connectable nonconnectable	When blue2net is set to *connectable*, a terminal can establish a connection to it. When blue2net is set to *nonconnectable*, it is not possible to establish a connection to it from any Bluetooth terminal. **Caution!** Danger of lockout! Verify this parameter carefully! (see chapter 5)
Max. No. of Terminals Connected	[1.6]	7 (seven) other value (range: 0…7)	This specifies the maximum number of terminals that can be connected to blue2net simultaneously. If this value is set to "0", no terminal will be able to establish a connection to blue2net. **Caution!** Danger of lockout! Verify this parameter carefully! (see chapter 5)

Objects (see Figure 6)	**Hier. level**	**Factory setting, other values, value range**	**Explanation**
Number of Services	[1.7]	1 (one) (read only)	This is the number of services presented to the terminals.
Service Table	[1.8]		A list of entries regarding services (see chapter 3.4.1).
Number of Terminals	[1.9]	10 (ten) (read only)	The maximum number of terminal entries that may be contained in the terminal table of blue2net.
Terminal Table	[1.10]		A list of entries regarding terminals (see chapter 3.4.3).
Default Access Mode	[1.11]	enabled disabled	If 'Default Access Mode' is set to *enabled*, terminals not contained in the terminal table [1.10] can also establish a connection to blue2net. The 'Default Bluetooth Passkey' [1.12] is used for Bluetooth authentication. **Security note:** If 'Default Access Mode' is enabled, any terminal will be granted access to blue2net. If 'Default Access Mode' is set to *disabled*, only terminals contained in the terminal table [1.10] can establish a connection to blue2net. **Caution!** Danger of lockout! Verify this parameter carefully! (see chapter 5)
Default Bluetooth Passkey	[1.12]	1234 other passkey of your choice (1...16 characters)	Bluetooth passkey assigned to terminals that are not listed in the terminal table. This passkey grants access for such a terminal only if Default Access Mode [1.11] is set to enabled. **Security note**: You should immediately change this value after the installation of blue2net. **Caution!** Danger of lockout! Verify this parameter carefully! (see chapter 5)

Table 5 Bluetooth Parameters [1]

3.4.1 Bluetooth Device Name [1.1]

The 'Bluetooth Device Name' [1.1.1] and 'IP Address Suffix Mode' [1.1.2] parameters help you to identify and/or select blue2net among a number of different Bluetooth devices. A Bluetooth device inquiry can retrieve the user-friedly name of your blue2net unit plus its current IP address and display it on your Bluetooth terminal.

Figure 7 Bluetooth Device Name [1.1]

Objects (see Figure 8)	**Hier. level**	**Factory setting, other values, value range**	**Explanation**
Bluetooth Device Name	[1.1.1]	blue2net other name (1...16 characters)	This is the user friendly name for your blue2net
IP Address Suffix Mode	[1.1.2]	enabled disabled	If 'IP Address Suffix Mode' is set to *enabled*, the current IP address of your blue2net will be suffixed to the 'Bluetooth Device Name'. This allows you to use the Bluetooth device inquiry to see the IP address on the Bluetooth terminal instead of having to search through the configuration pages.

Table 6 Bluetooth Device Name [1.1]

3.4.2 Service Table [1.8]

The most important value in this table is 'Auth.Level' [1.8.4]. It controls the Bluetooth security features (authentication and encryption) used on blue2net.

The other values are presented to Bluetooth devices via SDP upon Bluetooth device inquiry and may be displayed on the terminal side.

Figure 8 Service Table [1.8]

Objects (see Figure 8)	**Hier. level**	**Factory setting, other values, value range**	**Explanation**
Service Index	[1.8.1]	1 (one) (read-only)	A unique value for each service.
Service Name	[1.8.2]	LAN ACCESS 1 other name of your choice (1...23 characters)	The name of the service presented to a client using SDP.
Service Description	[1.8.3]	LAN ACCESS via blue2net other description of your choice (1...31 characters)	Description of the service presented to a client using SDP Read-only (does not influence the functionality).

Objects (see Figure 8)	**Hier. level**	**Factory setting, other values, value range**	**Explanation**
Auth. Level	[1.8.4]	noauth auth authandenc	There is a security mechanism required for using the services. Services with the attribute *noauth* (no authentication) can be used without any security mechanism. **Security note:** If Auth. Level is set to *noauth*, there is no restriction for any Bluetooth terminal to access blue2net and the LAN behind it. For services with the attribute *auth* (authentication), a Bluetooth passkey [1.10.3] is requested from the user before a data transfer will be performed. For services with *authandenc* (authentication and encryption), a Bluetooth passkey [1.10.3] is requested from the user before an encrypted data transfer will be performed. **Caution!** Danger of lockout! Verify this parameter carefully! (see chapter 5)
Service Provider	[1.8.5]	SIEMENS other entry of your choice (1...15 characters)	Provider of the service presented to a client using SDP.
Service URL	[1.8.6]	http://www.siemens.at/bluetooth other entry of your choice (1…47 characters)	URL of the service presented to a client using SDP.
Service ID	[1.8.7]	1 (one)	Service Record Handle subfield presented to a client using SDP. (Prepared only for use by future applications)

Table 7 Service Table [1.8]

3.4.3 Terminal Table [1.10]

This terminal table may be used to grant access to blue2net for selected Bluetooth terminals identified by their specific Bluetooth device address [1.10.2].

If you want to exclude all other terminals not registered in this table, you have to set 'Default Access Mode' [1.11] to disabled.

For each of the terminals registered in this table, you can configure a specific terminal Bluetooth passkey [1.10.3] and a unique IP address. In order to get a unique IP address for a specific terminal, 'Terminal IP Address Resolution' [3.1] has to be set to predefined or masqueradingpool.

If the terminal IP address [1.10.4] is not configured (IP address is set to 0.0.0.0), terminals get their IP addresses assigned from the 'Terminal IP Address Pool Table' [3.3].

Figure 9 Terminal Table [1.10]

Objects (see Figure 9)	**Hier. level**	**Factory setting, other values, value range**	**Explanation**
Terminal Index	[1.10.1]	1-10 (read-only)	A unique value for each terminal. It ranges between 1 and the value of 'Number of Terminals' [1.9]
Terminal Bluetooth Address	[1.10.2]	00:00:00:00:00:00 other Bluetooth address	The unique Bluetooth address of the terminal which is allowed to use this blue2net. Note: If the Terminal Bluetooth Address is set to 00:00:00:00:00:00 (default value), blue2net will not recognize this terminal as registered even if the passkey [1.10.3] and/or the terminal IP address [1.10.4] are configured. In case another Bluetooth address has been entered: **Caution!** Danger of lockout! Verify this parameter carefully! (see chapter 5 and 5.1)
Terminal Bluetooth Passkey	[1.10.3]	1234 other value of your choice (1...16 characters)	Bluetooth passkey assigned to this terminal for access to blue2net (relevant only, if 'Terminal Bluetooth Address' [1.10.2] is not 00:00:00:00:00:00). **Caution!** Danger of lockout! Verify this parameter carefully! (see chapter 5)
Terminal IP Address	[1.10.4]	0.0.0.0 other IP address	If 'Terminal IP Address Resolution' [3.1] is set to *predefined* or *masqueradingpool*, the 'Terminal IP Address' will be assigned to the terminal (relevant only, if 'Terminal Bluetooth Address' [1.10.2] is not 00:00:00:00:00:00). If 'Terminal IP Address' contains *0.0.0.0*, a value from 'Terminal IP Address Pool Entries' [3.2] will be assigned to this terminal.

Table 8 Terminal Table [1.10]

3.5 IP Parameters for blue2net [2]

This chapter describes the IP parameters relevant for the blue2net device itself.

Figure 10 IP Parameters for blue2net [2]

Objects (see Figure 10)	Hier. level	Factory setting, other values, value range	Explanation
blue2net IP Address Resolution	[2.1]	dhcp predefined	This object controls the mechanism for assigning IP address values to blue2net. If the mode is set to *dhcp*, blue2net will send a DHCP request in order to receive values during startup. If the mode is set to *predefined*, blue2net will use the value set in 'Fixed blue2net IP Configuration' [2.2]. Set *predefined* if you want to use blue2net on an xDSL modem. **Caution!** Danger of lockout! Verify this parameter carefully! (see chapter 5)
Fixed blue2net IP Configuration	[2.2]		The IP addresses assigned to blue2net if the blue2net address resolution mode [2.1] is set to *predefined*.

Objects (see Figure 10)	**Hier. level**	**Factory setting, other values, value range**	**Explanation**
DHCP blue2net IP Objects ("Fallback" IP's).	[2.3]		The IP addresses assigned to blue2net if 'blue2net IP-Address Resolution' [2.1] is set to *dhcp* and there is no DHCP service available.
Time Server IP	[2.4]	0.0.0.0 other IP address	The IP address of a time server in your network.
IP Masquerading	[2.5]	192.168.2.2 other private IP address	The IP address of blue2net in the masqueraded net, in cases where 'Terminal IP Address Resolution' [3.1] is set to *masquerading* or *masqueradingpool* Note: Make sure that this value is different from the IP address of your blue2net.
Firewall Setting	[2.6]		If 'Default Firewall'[2.6.1] is set to *enabled*, a default set of firewall rules will be activated. Updating the software via Ethernet (LAN) is only possible if the firewall is *disabled*. (see Figure 13)
Tunnel Configuration (PPPoE / PPTP)	[2.7]		Many Internet service providers use a tunnel protocol in order to provide broadband internet access based on DSL technology. blue2net supports 2 frequently used tunnel protocols: PPPoE (RFC 2516) and PPTP (RFC 2637).

Table 9 IP Parameters for blue2net [2]

3.5.1 Fixed blue2net IP Configuration [2.2]

If blue2net IP Address Resolution [2.1] is set to *predefined*, the following values will take effect. These values are allocated by the network administrator or Internet Service Provider.

Figure 11 Fixed blue2net IP Configuration [2.2]

Objects (see Figure 11)	Hier. level	Factory setting, other values, value range	Explanation
Fixed blue2net IP Address	[2.2.1]	192.168.1.2 other IP address	The IP address assigned to blue2net, provided the 'blue2net Address Resolution' [2.1] is set to *predefined*.
Fixed blue2net Netmask	[2.2.2]	255.255.255.0 other netmask	The subnet mask associated with the IP address 'Fixed blue2net IP Address' [2.2.1]in cases where 'blue2net Address Resolution' [2.1] is set to *predefined*.
Fixed blue2net Gateway	[2.2.3]	192.168.1.1 other gateway	The IP address of the default gateway on blue2net, in cases where 'blue2net Address Resolution Mode' [2.1] is set to *predefined*.

Table 10 Fixed blue2net IP Configuration [2.2]

3.5.2 IP Address Resolution: DHCP [2.3]

If 'blue2net IP Address Resolution' [2.1] is set to *dhcp* and DHCP service is not available, the following values will take effect. In order to find out whether DHCP service works on your network, read the explanations in chapter 2.3.

Figure 12 DHCP blue2net IP Objects, DHCP setup [2.3]

Objects (see Figure 12)	**Hierarchy level**	**Factory setting, other values, value range**	**Explanation**
Fallback blue2net IP Address	[2.3.1]	192.168.1.2 other IP address	The IP address assigned to blue2net, if 'blue2net Address Resolution' [2.1] is set to *dhcp*, but the DHCP request for this value failed.
Fallback blue2net Netmask	[2.3.2]	255.255.255.0 other netmask	The subnet mask associated with the IP address 'Fallback blue2net IP Address' [2.3.1] in cases where 'blue2net Address Resolution' [2.1] is set to *dhcp*, but the DHCP request for this value failed.
Fallback blue2net Gateway	[2.3.3]	192.168.1.1 other gateway	The IP address of the default gateway on blue2net in cases where 'blue2net Address Resolution' [2.1] is set to *dhcp*, but the DHCP request for this value failed.

Table 11 DHCP blue2net IP Objects, DHCP setup [2.3]

3.5.3 Firewall Option [2.6]

The firewall in blue2net may be established in order to prevent attacks coming from the Ethernet side (e.g. over LAN, cable modem or xDSL connection).

Note: Activating the firewall may cause restrictions with certain applications (e.g. games over the Internet) due to default safety options.

The firewall in blue2net may be established in order to prevent attacks from the LAN side (e.g. cable modem).

Figure 13 Firewall Settings [2.6]

Objects (see Figure 13)	Hier. level	Factory setting, other values, value range	Explanation
Default Firewall	[2.6.1]	disabled enabled	If 'Default Firewall' is set to *enabled*, a default set of firewall rules (see chapter 9) will be activated. Updating the software via LAN is only possible if the firewall is *disabled*. (see also chapters 6.1 and 9)

Table 12 Firewall Settings [2.6]

3.5.4 Tunnel Configuration (PPPoE / PPTP) [2.7]

When an xDSL modem is connected to a terminal device, in most cases a tunnel protocl will be applied in addition to the Ethernet protocol. Before it is possible to exchange data with the Internet, the tunnel protocol to the xDSL modem must be set up. blue2net support tunnel protocols PPPoE (RFC 2516) and PPTP (RFC 2637).

Figure 14 Tunnel Configuration (PPPoE / PPTP) [2.7]

Objects (see Figure 14)	**Hier. level**	**Factory setting, other values, value range**	**Explanation**
Tunnel Mode	[2.7.1]	none pppoe pptp	If Tunnel Mode is set to 'none', no tunnel protocol will be activated by blue2net. If Tunnel Mode is set to 'pppoe', blue2net will activate the PPPoE tunnel protocol (RFC 2516). If Tunnel Mode is set to 'ppptp', blue2net will activate the PPTP tunnel protocol (RFC 2637). To find out which tunnel protocol to use for your xDSL access, contact your xDSL provider.
Tunnel Establishment Control	[2.7.2]	disabled enabled	This parameter is relevant only, if 'Tunnel Mode' is set to *pppoe* or *pptp*. If 'Tunnel Establishment Control' is set to *disabled*, blue2net establishes a tunnel connection at startup. The tunnel remains established until blue2net is switched off. Use this option if 'Flat-Rate' is the tariff model of your xDSL provider. If 'Tunnel Establishment Control' is set to *enabled*, blue2net establishes a tunnel when the first Bluetooth terminal connects to blue2net. The tunnel connection is terminated when the last Bluetooth terminal disconnects from blue2net. Use this option if online-time is the determining factor for the tariff model of your xDSL provider.
Authentication Parameters	[2.7.3]		Authentication (user name and user password) for tunnel connections.
PPTP Server IP Address	[2.7.4]	10.0.0.138 other IP adress	This parameter is relevant only, if 'Tunnel Mode' is set to *pptp*. 'PPTP Server IP Address' is the IP address of the PPTP server/xDSL-modem. To find out this IP address, refer to the documentation of your xDSL modem or contact your xDSL provider.

Table 13 Tunnel Configuration (PPPoE / PPTP) [2.7]

Authentication Parameters [2.7.3]

Tunnel protocols PPPoE and PPTP perform an authentication based on 'User Name' and 'User Password' upon tunnel establishment. The values for 'User Name' and 'User Password' have been assigned by your xDSL provider.

Figure 15 Authentication Parameters [2.7.3]

Objects (see Figure 15)	Hier. level	Factory setting, other values, value range	Explanation
User Name	[2.7.3.1]	pppoeuser other value of your choice (1...100 characters)	'User Name' is the name used for authentication (e.g. user ID assigned by your xDSL provider.
User Password	[2.7.3.2]	pppoepassw other value of your choice (1...100 characters)	'User Password' is the password used for authentication (e.g. the password assigned to your user ID by your xDSL provider.

Table 14 Authentication Parameters [2.7.3]

3.6 IP Parameters for Terminals [3]

This chapter describes the IP parameters for terminals connected to blue2net. While the PPP connection is being established these parameters (except for [3.1] and [3.2]) will be sent to the Bluetooth terminal.

IP Parameters for Terminals

	Object	Value
[3.1]	Terminal IP Address Resolution	masquerading edit
[3.2]	Number of Terminal IP Address Pool Entries	7
[3.3]	Terminal IP Address Pool Table	Table
[3.4]	Terminal Net Mask	255.255.255.0 edit
[3.5]	Terminal Fixed Servers	Objects

Figure 16 IP Parameters for Terminals [3]

Objects (see Figure 16)	**Hier. level**	**Factory setting, other values, value range**	**Explanation**
Terminal IP Address Resolution	[3.1]	masquerading dhcp predefined masqueradingpool	This object controls the mechanism for assigning an IP address to a terminal connected to blue2net. If the mode is set to *masquerading*, no IP address configuration will be required for terminals (this is the recommended setting for home users with cable modem or xDSL modem). If the mode is set to *dhcp*, blue2net will send a DHCP request containing the Bluetooth address of the terminal during the terminal's connection phase. If the mode is set to *predefined*, blue2net will use an IP address from a pool of fixed IP addresses. This pool is defined in 'Terminal IP Address Pool Table' [3.3]. If the terminal is registered in the terminal table [1.10], blue2net will use the IP address assigned there (see 3.4.3). If the mode is set to *masqueradingpool,* the IP address assignment is the same as for the masquerading mode, except for those terminals that are listed in the 'Terminal Table' [1.10] (see 3.4.3). **Caution!** Danger of lockout! Verify this parameter carefully! (see chapter 5)
Number of Terminal IP Address Pool Entries	[3.2]	7 (read only)	The number of IP addresses in the Terminal IP address pool.
Terminal IP Address Pool Table	[3.3]		A list of IP addresses which blue2net may assign to terminals.
Terminal Netmask	[3.4]	255.255.255.0 other value	The subnet mask associated with the IP address out of 'Terminal IP Address Pool Table' [3.3]
Terminal Fixed Servers	[3.5]		While the PPP connection is being established these parameters will be sent to the Bluetooth terminal.

Table 15 IP Parameters for Terminals [3]

3.6.1 Terminal IP Address Pool Table [3.3]

A list of IP addresses that blue2net may assign to terminals. These parameters are only relevant if 'Terminal IP Address Resolution' [3.1] is not set to *dhcp*.

[3.3.1] [3.3.2]

Terminal IP Address Pool Table

Object	Terminal IP Address Index	Terminal IP Address Pool Value
Row 1	1	192.168.1.11 edit
Row 2	2	192.168.1.12 edit
Row 3	3	192.168.1.13 edit
Row 4	4	192.168.1.14 edit
Row 5	5	192.168.1.15 edit
Row 6	6	192.168.1.16 edit
Row 7	7	192.168.1.17 edit

Figure 17 Terminal IP Address Pool Table [3.3]

Objects (see Figure 17)	Hier. level	Factory setting, other values, value range	Explanation
Terminal IP Address Index	[3.3.1]	1-7 (read only)	A unique value.
Terminal IP Address Pool Value	[3.3.2]	192.168.1.11…17	These are the IP addresses that will be assigned to terminals in the case where 'Terminal IP Address Resolution' [3.1] is set to *predefined*.

Table 16 Terminal IP Address Pool Table [3.3]

3.6.2 Terminal Fixed Servers [3.5]

Server IP addresses in cases where the Terminal IP Address Resolution mode [3.1] is not set to *dhcp*.

Figure 18 Terminal Fixed Servers [3.5]

Objects (see Figure 18)	**Hier. level**	**Factory setting, other values, value range**	**Explanation**
Terminal DNS Server 1	[3.5.1]	192.168.3.11 other IP address	IP address of DNS server 1 assigned to terminals if the 'Terminal IP Address Resolution' [3.1] is not set to *dhcp* and 'blue2net IP Address Resolution' [2.1] is set to *predefined*. Please enter the correct DNS IP address manually if this DNS IP address cannot be transmitted correctly by the DHCP server.

Objects (see Figure 18)	**Hier. level**	**Factory setting, other values, value range**	**Explanation**
Terminal DNS Server 2	[3.5.2]	192.168.3.12 other IP address	IP address of DNS server 2 assigned to terminals if the 'Terminal IP Address Resolution' [3.1] is not set to *dhcp* and 'blue2net IP Address Resolution' [2.1] is set to *predefined*. Please enter the correct DNS IP address manually if this DNS IP address cannot be transmitted correctly by the DHCP server.
Terminal WINS Server 1	[3.5.3]	192.168.3.13 other IP address	IP address of WINS server 1 assigned to terminals if the 'Terminal IP Address Resolution' [3.1] is not set to *dhcp* and 'blue2net IP Address Resolution' [2.1] is set to *predefined*.
Terminal WINS Server 2	[3.5.4]	192.168.3.14 other IP address	IP address of WINS server 2 assigned to terminals if the 'Terminal IP Address Resolution' [3.1] is not set to *dhcp* and 'blue2net IP Address Resolution' [2.1] is set to *predefined*.
Terminal Domain Name	[3.5.5]	my.domain.at other domain name (1…100 characters)	Domain name assigned to terminals if the 'Terminal IP Address Resolution' [3.1] is not set to *dhcp* and 'blue2net IP Address Resolution' [2.1] is set to *predefined*.

Table 17 Terminal Fixed Servers [3.5]

3.7 Current Configuration [4]

The purpose of the objects in this section is only to display the current values of important Bluetooth parameters, IP parameters and version information for the blue2net device.

Figure 19 Current Configuration [4]

Objects (see Figure 19)	Hier. level	Explanation
MAC Address	[4.1]	The MAC address is a fixed unique address of the Ethernet controller on blue2net. You can also find this address (MAC-Adr.) printed on the label at the bottom side of the blue2net case.
blue2net IP Configuration	[4.2]	see Table 19
Terminal Server Configuration	[4.3]	see Table 20
Version Information	[4.4]	see Table 21
Tunnel Status (PPPoE / PPTP)	[4.4]	see Table 22 and Table 23

Table 18 Current Configuration [4]

3.7.1 blue2net IP Configuration [4.2]

These objects show you the IP address values assigned to your blue2net.

Figure 20 blue2net IP Configuration [4.2]

Objects (see Figure 20)	Hier. level	Explanation
blue2net IP Address	[4.2.1]	The IP address assigned to blue2net. If the 'blue2net IP Address Resolution' [2.1] is set to *dhcp*, this value was retrieved via a DHCP request.
blue2net Netmask	[4.2.2]	The subnet mask assigned to blue2net. If the 'blue2net IP Address Resolution' [2.1] is set to *dhcp*, this value was retrieved via a DHCP request.
blue2net Gateway	[4.2.3]	The gateway IP address for blue2net. If the 'blue2net IP Address Resolution' [2.1] is set to *dhcp*, this value was retrieved via a DHCP request.

Table 19 blue2net IP Configuration [4.2]

3.7.2 Terminal Server Configuration [4.3]

These objects show you the IP address values assigned to the terminals.

Figure 21 Terminal Server Configuration [4.3]

Objects (see Figure 21)	Hier. level	Explanation
Terminal DNS Server 1	[4.3.1]	IP address of DNS server 1 assigned to terminals. If the 'Terminal IP Address Resolution' [3.1] is set to *dhcp*, this value was retrieved via a DHCP request.
Terminal DNS Server 2	[4.3.2]	IP address of DNS server 2 assigned to terminals. If the 'Terminal IP Address Resolution' [3.1] is set to *dhcp*, this value was retrieved via a DHCP request.
Terminal WINS Server 1	[4.3.3]	IP address of WINS server 1 assigned to terminals. If the 'Terminal IP Address Resolution' [3.1] is set to *dhcp* , this value was retrieved via a DHCP request.
Terminal WINS Server 2	[4.3.4]	IP address of WINS server 2 assigned to terminals. If the 'Terminal IP Address Resolution' [3.1] is set to *dhcp*, this value was retrieved via a DHCP request.
Terminal Domain Name	[4.3.5]	Domain name assigned to terminals. If the 'Terminal IP Address Resolution' [3.1] is set to *dhcp* , this value was retrieved via a DHCP request.

Table 20 Terminal Server Configuration [4.3]

3.7.3 Version Information [4.4]

These objects provide version information on the hardware, firmware and software used in your blue2net. You might need to provide this information when contacting the service hotline.

Version Information

	Object	Value
[4.4.1]	Module Firmware Version	013501010a003501
[4.4.2]	PPCBoot Version	ppcboot-1.0.1.5-20020207
[4.4.3]	blue2net Software Version	blue2net-2.0.0
[4.4.4]	blue2net Hardware Version	1
[4.4.5]	SieMo Module Info	S50037-Q5-X105-2 Si-4.0a-V0000 (02-06-24) UART-4.0-c2(02-06-24) 00-00-013.10-0135-01

Figure 22 Version Information [4.4]

Objects (see Figure 22)	Hier. level	Explanation
Module Firmware Version	[4.4.1]	Firmware version information of the Bluetooth module.
PPCBoot Version	[4.4.2]	Version of boot loader software.
blue2net Software Version	[4.4.3]	Version of blue2net application software.
blue2net Hardware Version	[4.4.4]	Version of blue2net hardware.
SieMo Module Info	[4.4.5]	Version information for Siemens Bluetooth module SieMo-S50037.

Table 21 Version Information [4.4]

3.7.4 Tunnel Status [4.5]

These objects provide information on the current status of the tunnel protocol.

Figure 23 Tunnel Status [4.5.1]

Objekte (siehe Figure 23)	Hier. stufe	Erklärung
Tunnel Status	[4.5.1]	Current status of the "tunnel".

Table 22 Tunnel Status [4.5.1]

A few examples of such status messages::

Meldung	Bedeutung
... pptp process running...	Tunnel established successfully
... pptp	xDSL mode was set but without connection
... none	Tunnel mode was not established
... peer not responding	The modem/server doesn't respond, the xDSL connection was interrupted or a wrong PPTP server address was set
... authentication failed	Password and/or User Name rejected, e.g. due to input error

Table 23 Status messages (examples)

3.8 Configuration Access [5]

This chapter describes the items controlling the access to the configuration of blue2net.

Figure 24 Configuration Access [5]

Objects (see Figure 24)	Hier. level	Factory setting, other values, value range	Explanation
SNMP Access	[5.1]	disabled enabled	This object controls access to an SNMP interface for the configuration of blue2net. A change of the setting will take effect only after this change has first been saved permanently and the blue2net device then been reset by the user. It is possible to configure blue2net via Web Interface while SNMP Access is enabled.
Configuration Password	[5.2]	changeme password of your choice (4…22 characters)	This password is used to authenticate persons who are authorized to configure blue2net via the Web interface. **You should never forget this password!** **Security note**: You should immediately change this password after the installation of blue2net. **Caution!** Danger of lockout! Verify this parameter carefully! (see chapter 5)

Table 24 Configuration Access [5]

3.8.1 Change of the Configuration Password [5.2]

You have to enter the password twice (see Figure 25).

Figure 25 Change of the blue2net Configuration Password [5.2.1]

Your changes have not been activated yet. In order to store and activate the changes you made, run one of the activation commands 'Save Settings Temporarily' or 'Save Settings Permanently' (see chapters 3.9.1 and 3.9.2).

3.9 Activation Commands [6]

Any changes you perform on blue2net settings will only take effect when you save them with either one of the *activation commands* 'Save Settings Temporarily' or 'Save Settings Permanently'.

If you want to restore default settings (factory settings) or if you want to perform a reset to settings stored in permanent memory, you will find the appropriate command here.

After downloading updated software or loading a file for your own specific homepage, you have to save the changes you made in order to let them take effect.

Please mind the warnings below in order to prevent locking yourself out from access via Bluetooth or LAN (see also chapter 5).

Figure 26 Activation Commands [6]

Click on the <edit> button to get a page like the one below displayed.

Once you click <Submit>, the changes will take effect.

Figure 27 Saving blue2net parameters

3.9.1 Save Settings Temporarily [6.1]

Any changes you make in one or more blue2net parameters will not take effect unless you save them (mind the relevance especially for security settings).

You can save them either

- for the current session by selecting 'Save Settings Temporarily', or
- permanently (until further changes are made) by selecting 'Save Settings Permanently'.

'Save Settings Temporarily' saves the changed parameters in temporary memory only. They will be valid only during the current session and will not be stored in permanent memory.

So, after you disconnect your blue2net from the power supply or if you perform a reset, these changes will be lost. They will not be lost if you only close the configuration session by clicking on [Close Session] or [Home].

Advantage: You can test your settings (with the exception of all blue2net IP parameters [2]) before saving them to permanent memory. So, if you lock yourself out (from LAN access and/or Bluetooth access) by specifying the wrong settings, you still have the option to return to the previous permanent settings by disconnecting your blue2net from the power supply or by performing a reset via LAN (see options below). The parameters stored in permanent memory will then become active again. You can then review your settings and apply the correct ones.

If you have configured 'Bluetooth Parameters' and/or 'IP Parameters for Terminals' and then select 'Save Settings Temporarily' while connected via Bluetooth, you will have to reestablish the Bluetooth connection to blue2net.

Note: Make sure that any Bluetooth connections existing to other terminals are terminated in an orderly fashion before you perform this function.

Caution: It is possible to lock yourself out by saving wrong settings. For more information see chapter 5, Preventing Lockout.

In such a case, you have 2 options for resetting blue2net to the previous settings stored in permanent memory:

1. Disconnect your blue2net from the power supply.

2. Access your blue2net from a Web browser via LAN or Bluetooth. Log in to the blue2net configuration function (blue2net IP address required!), click the <edit> button next to 'Activation Commands', click the <edit> button next to 'Reset blue2net' and activate the function by clicking <Submit>.

Note: If you are not sure what to do, contact the network administrator or look at the respective chapters in this user manual.

3.9.2 Save Settings Permanently [6.2]

Any changes you make in one or more blue2net parameters will not take effect unless you save them (mind the relevance especially for security settings).

You can save them either

- for the current session by selecting 'Save Settings Temporarily', or
- permanently (until further changes are made) by selecting 'Save Settings Permanently'.

'Save Settings Permanently' saves the changed parameters in permanent memory (until further changes are made).

If you have configured 'Bluetooth Parameters' and/or 'IP Parameters for Terminals' and then select 'Save Settings Permanently' while connected via Bluetooth, you will have to reestablish the Bluetooth connection to blue2net.

Note: Make sure that any Bluetooth connections existing to other terminals are terminated in an orderly fashion before you perform this function.

Caution: Consider testing your settings first as described under 'Save Settings Temporarily' - for in case you locked yourself out by saving the wrong settings in permanent memory, your only option is to send the unit in to the service center (chapter 14) and have it reset to the default settings there. For more information see chapter 5, Preventing Lockout.

Note: If you are not sure what to do, contact the network administrator or look at the respective chapters in this user manual.

3.9.3 Reset blue2net [6.3]

This function lets you reactivate the settings that are stored in permanent memory.

The blue2net unit will be rebooted with the settings from permanent memory. This function has the same effect as disconnecting the unit from the power supply and is particularly useful if the installation location of the unit or the power supply/mains plug are not easily accessible. Mind that any settings you saved only temporarily will be lost in that case.

Note: Make sure that Bluetooth connections established by other terminals have been terminated in an orderly fashion before performing this function.

A Bluetooth connection may only be reestablished after 2 minutes of waiting after having submitted the activation command „Reset blue2net“.

Note: If you are not sure what to do, contact the network administrator or look at the respective chapters in this user manual.

3.9.4 Update Software [6.4]

The blue2net manufacturer might supply a software update to improve the performance of the device or to eliminate faults or flaws.

Visit the blue2net homepage from time to time to check for updates.

'Update Software' must be activated after the updated software has been downloaded from a service homepage and transferred into your blue2net's file system.

For details on how to proceed, please see chapter 6

Note: If you are not sure what to do, contact the network administrator or look at the respective chapters in this user manual.

3.9.5 Restore Default Settings [6.5]

'Restore Default Settings' resets all configuration values in the permanent memory to the default settings (factory settings). To see what exactly these values are, refer to the list in chapter 12.

All customized configuration values will be irreversibly reset. In order to restore your own configuration values, you have to reenter them one by one.

Use 'Restore Default Settings' if you want to clear all settings as a way to regain control of all parameters.

Note: If you are not sure what to do, contact the network administrator or look at the respective chapter in this user manual.

3.9.6 Store Specific Homepage [6.6]

Use the 'Store Specific Homepage' function to load your own applications (e.g. HTML files, games) into blue2net's permanent memory. For details on how to proceed, please see chapter 7.1.

Note: If you are not sure what to do, contact the network administrator or look at the respective chapter in this user manual

4 Use Scenarios

This chapter should make it easier for you to get typical configuration settings right, especially at the beginning when you are not yet fully acquainted with the configuration functions. It is not intended to cover all possible scenarios. Other settings might be required to properly adjust blue2net to your specific security requirements and /or preferences. Please pay attention to chapter 5, Preventing Lockout

4.1 Business Scenario with Controlled Access

Typical scenarios: meeting rooms or conference rooms where participants are granted the default Bluetooth passkey [1.12] or temporary access.
Characteristics: The security level is high. Only selected persons have access to the LAN, only authorized persons have access to the configuration settings.

Parameter	Hier. lev.	Set to	Reason
Bluetooth Device Name	[1.1]	Name of your choice (1...16 characters)	In an environment with many blue2net units, they should all have a unique name for clear differentiation.
Terminal Table	[1.10]	All terminals unregistered (BT address set to 00:00:00:00:00:00)	All users should get access with the 'Default Bluetooth Passkey' [1.12]
Default Access Mode	[1.11]	enabled (default value)	Any terminal can access the LAN but needs the 'Default Bluetooth Passkey' [1.12] as the 'Auth. Level' [1.8.4] is set to *auth* or *authandenc*
Default Bluetooth Passkey	[1.12]	Passkey of your choice (1…16 characters)	The passkey is disclosed to authorized persons only. For security reasons, change this value frequently!
Auth. Level	[1.8.4]	auth or authandenc	In order to avoid access by unauthorized persons. The 'Default Bluetooth Passkey' [1.12] is required to gain access.
Terminal IP Address Resolution	[3.1]	masquerading (default value)	No IP addresses are required for terminals.
Configuration Password	[5.2]	Password of your choice (4…22 characters)	Only authorized persons (e.g. a system administrator) can configure blue2net. Attention! Do not forget the new password!

Table 25 Use scenarios: settings for a business scenario with controlled access

4.2 Public Use Scenario (Hot Spot)

Typical scenarios: airport lounges, hotel bars, Internet cafes.
Characteristics: Quick and easy access, no authorization, unselected users, only authorized persons have access to the blue2net configuration settings.

Parameter	Hier. lev.	Set to	Reason
Bluetooth Device Name	[1.1]	Name of your choice (1...16 characters)	Required to identify your blue2net among other Bluetooth devices. In an environment with many blue2net units, they should all have a unique name for clear differentiation.
Terminal Table	[1.10]	Bluetooth device addresses of your most frequently used terminals, Bluetooth Passkey and IP address	If you want to support "VIPs" with a fixed terminal IP address. In this case set 'Terminal IP Address Resolution' [3.1] to *masqueradingpool*.
Default Access Mode	[1.11]	enabled (default value)	Easy access for everyone.
Auth. Level	[1.8.4]	noauth (default value)	In Hot Spot scenarios you will allow access to your facilities for everyone.
Terminal IP Address Resolution	[3.1]	masqueradingpool	Use this setting when support for "VIPs" is your choice. For the "VIP" terminals, you have to configure IP addresses in the Terminal Table [1.10]
Terminal IP Address Resolution	[3.1]	masquerading (default value)	No IP addresses are required for terminals.
Configuration Password	[5.2]	Password of your choice (4…22 characters)	Only authorized persons (e.g. a system administrator) can configure blue2net. Attention! Do not forget the new password!

Table 26 Use scenarios: settings for public use scenarios (hot spot)

4.3 Home Use Scenario with Cable Modem

Typical scenarios: Several family members want to have access to the Internet via one cable modem. A DHCP server is available on the Internet Service Provider's server. Only authorized persons have access to the blue2net configuration settings.
Characteristics: For security reasons, the blue2net unit needs to be protected against access by neighbors or unauthorized users outside the apartment or house. A firewall may be installed to protect the PCs.

Parameter	Hier. lev.	Set to	Reason
Bluetooth Device Name	[1.1]	Name of your choice (1...16 characters)	Required to identify your blue2net among other Bluetooth devices.
Default Access Mode	[1.11]	enabled (default value)	You can use any of your Bluetooth terminals.
Default Bluetooth Passkey	[1.12]	Passkey of your choice (1…16 characters)	To avoid access by non-family members. Attention! Do not forget the new Default Bluetooth Passkey!
Auth. Level	[1.8.4]	authandenc	To avoid access by non-family members Attention! Do not forget the configured Bluetooth Passkey!
Firewall Settings	[2.6.1]	enabled	In order to prevent attacks from the LAN side (e.g. cable modem). Refer to chapter 9 "Firewall" for detailed rules.
Terminal IP Address Resolution	[3.1]	masquerading (default value)	No IP addresses are required for terminals.
Configuration Password	[5.2]	Password of your choice (4…22 characters)	Only authorized persons may configure blue2net. Attention! Do not forget the new password!

Table 27 Use scenarios: settings for home use with cable modem

Note: If web addresses are not recognized once typed into the location bar of the web browser (error message: page cannot be displayed...) this might be caused by a failed transmission of DNS-IP addresses 1 and 2 via the DHCP server. If this is the case, please enter addresses manually ([3.5.1] und [3.5.2]). You will obtain DNS-IP address values from your ISP.

4.4 Home Use Scenario with xDSL Modem

Typcial scenario: Several family members need Internet access via an xDSL modem. Only one person is authorized to access the configuration settings.
Characteristics: For security reasons, blue2net has to be protected against access by neighbors and unauthorized persons outside the apartment or house (secure Bluetooth connections!).

Parameter	Hier. lev.	Set to	Reason / Note
Bluetooth Device Name	[1.1.1]	Name of your choice (1...16 character)	Required to identify your blue2net among other devices.
Default Access Mode	[1.11]	enabled (default value)	You can use any of your Bluetooth terminals.
Default Bluetooth Passkey	[1.12]	Password of your choice (1…16 characters)	Prevents access by non-family members Attention! Make sure you remember the new Bluetooth password.
Auth. Level	[1.8.4]	authandenc	Prevents access by non-family members. Attention! Make sure you remember the set Bluetooth password.
blue2net IP Address Resolution	[2.1]	predefined	The xDSL modem cannot reply to DHCP queries.
PPTP Server IP Address	[2.7.4]	predefined IP address (could be e.g. 10.0.0.138)	If the PPTP protocol is used for your xDSL access, enter the predefined IP address here. To find out this IP address, refer to the documentation of your xDSL modem or contact your xDSL provider.

Parameter	Hier. lev.	Set to	Reason / Note
Fixed blue2net IP Address	[2.2.1]	Example: [2.7.4]: 10.0.0.138 (predefined value obtained from the xDSL provider or from the user manual of the xDSL modem) [2.2.2]: 255.255.255.0 (default value of blue2net) [2.2.1]: 10.0.0.140 'Fixed blue2net IP Address', which is in the same IP net as [2.7.4].	If 'Tunnel Mode' [2.7.1] is set to *pptp*, the values of these parameters have to be set in such a way that 'Fixed blue2net IP Address' is in the same IP network as the IP address assigned by the xDSL modem, 'PPTP Server IP Address'. If 'Tunnel Mode' [2.7.1] is set to *pppoe*, the factory settings for these values (see chapter 12) can remain unchanged.
Fixed blue2net Netmask	[2.2.2]		
Fixed blue2net Gateway	[2.2.3]	0.0.0.0.	For this mode of operation this value is required.
Tunnel Mode	[2.7.1]	pppoe or pptp	Ask your xDSL service provider which tunnel protocol to use for your xDSL access.
Tunnel User Name	[2.7.3.1]	assigned User Name	Ask your xDSL service provider for your 'User Name'
Tunnel User Password	[2.7.3.2]	assigned User Password	Ask your xDSL service provider for your 'User Password'
Terminal IP Address Resolution	[3.1]	masquerading (default value)	With this kind of setting, the terminals do not require IP addresses.
Configuration Password	[5.2]	Password of your choice (4…22 characters)	Only authorized persons (e.g. the system administrator) can configure blue2net. Attention! Make sure you remember the new password.

Table 28 Use scenarios: Settings for home use with xDSL modem

5 Preventing Lockout

Among the settings there are some that deserve particular attention. Wrong settings, passwords or addresses may lock you out from access to blue2net either both via Bluetooth and Ethernet (LAN) or only one of the two.

This is not a malfunction of blue2net. For security reasons some settings are unavoidable, but may cause lockout from access under the circumstances mentioned below.

It is therefore recommended to pay particular attention to these settings.

Keep records of the following settings:

- Configuration Password [5.2]
- Default Bluetooth Passkey [1.12]
- blue2net IP Address Resolution [2.1]
- Fixed blue2net IP Addresses [2.2]
- Fallback blue2net IP Addresses [2.3]
- IP Masquerading [2.5]
- Terminal IP Address Resolution [3.1]
- Terminal Bluetooth Address [1.10.2] (in combination with [1.10.3])
- Terminal Bluetooth Passkey [1.10.3] (in combination with [1.10.2])

Keep them in places separate from the blue2net unit, the PDA or laptop.

Please also keep in mind the instructions regarding the saving of settings as described in chapter 3.9.2, as you should only record permanently saved settings.

5.1 Lockout from Access via Bluetooth and Ethernet (LAN)

Parameter	Hier. level	Before setting it to	Keep in mind
Configuration Password	[5.2]	Other than default	When you change the Configuration Password (which you should always do for security reasons), make sure not to forget the new password, otherwise you will be locked out from configuration access. You would have to bring or send your blue2net to your next service support center for having it restored to its default settings.

Table 29 Lockout scenarios: Lockout from Bluetooth and Ethernet (LAN)

5.2 Lockout from Access via Bluetooth

Parameter	Hier. level	Before setting it to	Keep in mind
Connectability Mode	[1.5]	nonconnectable	The only possibility to access your blue2net again is via Ethernet (LAN). No Bluetooth connection is possible any more!
Max. No. of Terminals Connected	[1.6]	0	
Auth. Level	[1.8.4]	auth or authandenc	If you activate authentication (which you should do for security reasons), make sure you remember the configured Bluetooth passkeys of your terminals, [1.12] and [1.10.3].
Default Access Mode	[1.11]	disabled	Only terminals contained in the terminal table [1.10] have access rights. Make sure you remember the Bluetooth device addresses [1.10.2] and the appropriate Bluetooth passkeys [1.10.3] for these terminals. If you have no terminals registered in the terminal table [1.10], you will have no access.
Default Bluetooth Passkey	[1.12]	Other than default	When you change the 'Default Bluetooth Passkey' (which you should always do for security reasons), make sure not to forget the new passkey. If you have no terminals registered in the terminal table [1.10], you will have no access.
Terminal IP Address Resolution	[3.1]	dhcp	If no DHCP service is available, blue2net never gets an IP address for a terminal and so no connection is possible.

Table 30 Lockout scenarios: Lockout from Bluetooth access

5.3 Lockout from Access via Ethernet (LAN)

Parameter	Hier. level	Before setting it to	Keep in mind
blue2net IP Address Resolution	[2.1]	predefined	Remember your fixed blue2net IP addresses [2.2.1] and [2.2.2]
blue2net IP Address Resolution]	[2.1]	dhcp but DHCP service not available	Remember your fallback blue2net IP addresses [2.3.1] and [2.3.2]

Table 31 Lockout scenarios: Lockout from access via Ethernet (LAN)

6 Update Software

The software update function enables you to make use of the latest features and improvements.

Note: After a software update, you will have the same parameter settings as before. There is no need to reenter settings that were stored in permanent memory.

Visit the blue2net homepage in order to check for updates of both the software and the user guide.

A software update takes effect after the reboot was performed by blue2net.

6.1 How to Download New Software

Note: During the update it is very important not to interrupt the power supply. If you unplug your blue2net, you will have to send it in for service.

Updating the software via the Ethernet (LAN) is only possible if the firewall is disabled. On how to disable the firewall see chapters 2.7, 3.5, and 3.5.3. It is not necessary to disable the Firewall if you are performing the update from your Bluetooth terminal.

During the update the LED flashes very rapidly.

Note: If you are not sure what to do, contact the network administrator.

How to obtain updated software:

1. Use a PC or laptop that is connected to the Internet.
2. Visit our homepage '**http://www.siemens.at/bluetooth**' from your PC or laptop.
3. Download the latest software version (b2n_image) and save it on your hard disk (e.g. under C:\temp\).
4. Open your Web browser and the file manager (e.g. Windows Explorer) and preferably arrange both windows on the screen side by side (see Figure 28).
5. Establish a connection via LAN (Firewall disabled!) or Bluetooth to your blue2net.
6. If you connect via Bluetooth, the Bluetooth device inquiry will indicate the blue2net IP address after the Bluetooth device name.

   If you connect via the LAN, you have to query your blue2net IP address

[4.2.1], for example via the blue2net Web interface (see Figure 3): Click on 'Configuration' / click on <edit> next to 'Current Configuration' / click on 'Objects' next to 'blue2net IP Configuration' / read the IP address next to 'blue2net IP Address') and click on [Close Session].

7. Enter '**ftp://config@< blue2net IP Address >/tmp/**' in your Web browser's location/URL field (see Figure 28) and press the 'Enter' key.

8. When prompted for login information, enter the user name "config" and your configuration password ("changeme" by default).

Figure 28 Software update: Login to blue2net

9. Copy the "**b2n_image...**" file from the hard disk directory (e.g. C:\temp\) to the blue2net file system. This can be done e.g. by "drag and drop".

Figure 29 Software update: Dragging the software image file to blue2net

Figure 30 Software update: Progress of copying the software image file

Save the new software:

10. After copying, change to the blue2net main configuration page (see Figure 4).

11. Make all other users exit the Bluetooth connections they have established.

12. Click on the <edit> button next to 'Activation Commands' [6].

13. Click on the <edit> button next to 'Update Software' [6.4].

14. Click on the <Submit> button to save the new software and make the changes take effect after a reboot.

Figure 31 Saving the software update

The update process has now been started, which is indicated by rapid blinking of the LED.

If you have initiated the update via a Bluetooth connection, this connection will now have been interrupted due to the update. You should keep an eye on the LED to be able to recognize, after 2 to 10 minutes, whether or not the update has been completed successfully.

If you have initiated the update via a LAN connection, you can monitor its progress on the Web browser.

Warning! During the update process you must not activate any functions on the web browser (by clicking) or cut the power supply, as this may cause damage and even render blue2net useless.

Update Progress Info

```
Version Check:          started ... OK
     part:             |     old version      |      new version      |   update ?
   SieMo Firmware ...  011b                      0135 means 013.10        yes
   PS-Key         ...  01 UART                   01 UART                 yes
   b2n Software   ...  blue2net-1.1.2            blue2net-2.0.0          yes
Update SieMo Firmware: started ... 100 percent OK
Write all PS-Keys:     started ... OK
Update b2n Software:   started ... 100 percent OK
*UPDATE_FINISHED* ... OK
```

Figure 32 Progress of the Software Update process

Progress of the update process:

During the update, a check is made to verify which parts (Bluetooth module, blue2net software, keys) need to be updated. Then the required updates are performed. This may take from 2 to 10 minutes.

15. Checking the result of the update process

- **If the update was successful**, the LED will be switched to permanent blinking for about 30 seconds or a message to that effect will be displayed by the Web browser (NOT if update was initiated via Bluetooth!).

  Then blue2net will be restarted with the new software version (reboot). This take 2 minutes (normal, slow blinking of the LED). Settings already stored in permanent memory will remain unchanged.

  The new software is then ready for use.

- **If the update was not successful**, the LED will be switched "off" for about 30 seconds. Then blue2net will be rebooted (normal, slow blinking of the LED)

  If the update was not successful, you should try again. If this does not work either, please contact service (see chapter 14), keeping the Web browser output ready in the case of questions.

7 Store Specific Homepage

To be able to use this feature, you should be familiar with designing Web pages and with the Linux tool “tar”.

There is the possibility to store your own specific homepage on blue2net. In order to do so, use the Linux tool “tar" to pack and compress your HTML files into a file named **b2n_user.gz**. The size of the compressed file b2n_user.gz must not exceed 60 Kbytes.

The appropriate command line for the Linux tool is:
`tar –cvzf b2n_user.gz <your HTML source directory>`.

The specific homepage is permanently available after the reboot was performed by blue2net.

7.1 How to Load Your Specific Homepage

Loading your own specific homepage file onto your blue2net is similar to performing a software update (see chapter 6).

Loading your specific homepage via the Ethernet (LAN) is only possible if the firewall is disabled. On how to disable the firewall see chapters 2.7, 3.5, and 3.5.3. It is not necessary to disable the Firewall if you are performing the loading from your Bluetooth terminal.

Loading the file for the specific homepage:

1. Open your Web browser and the file manager (e.g. Windows Explorer) and preferably arrange both windows on the screen side by side (see Figure 33).

2. Establish a connection via LAN (Firewall disabled!) or Bluetooth to your blue2net.

3. Find out your 'blue2net IP address' [4.2.1] (e.g. via the blue2net Web interface (see Figure 3): click on 'Configuration' / click on the <edit> button next to 'Current Configuration' / click on 'Objects' next to 'blue2net IP Configuration' / get the value next to 'blue2net IP Address').

4. Enter '**ftp://config@< blue2net IP Address >/tmp/**' in the location/URL field of your Web browser.

5. When prompted for login information, enter the user name "config" and your configuration password ("changeme" by default).

Figure 33 Specific homepage: Login to blue2net

6. Copy the '**b2n_user.gz**' file from the hard disk directory (e.g. C:\temp\) to the blue2net file system. This can be done e.g. by 'drag and drop'.

7. After copying, change to the blue2net main configuration page (see Figure 4).

Storing the specific homepage:

8. Click on the <edit> button next to 'Activation Commands' [6].

9. Click on the <edit> button next to 'Store Specific Homepage' [6.6].

10. Store the homepage to blue2net (temporarily) by clicking on <Submit>.

    ATTENTION! After this step, the homepage will not yet have been saved permanently. However, what you can do now is to check whether your homepage is displayed correctly. If you then want to save your specific homepage permanently, proceed as follows.

Figure 34 Specific homepage: Storing the specific homepage

Saving the specific homepage:

11. Make all other users exit the Bluetooth connections they have established.
12. Open the blue2net main configuration page (see Figure 4).
13. Click on the <edit> button next to 'Activation Commands' [6].
14. Click on the <edit> button next to 'Save Settings Permanently' [6.2].
15. Save your specific homepage by clicking on the <Submit> button.
16. blue2net will now be rebooted (this might take up to 2 minutes).

Now your specific homepage is ready to use.

8 Troubleshooting

This section provides useful information to help you resolve difficulties you might encounter. Fault symptoms, possible causes, and remedies are described below.

Please bear in mind that any malfunction (e.g. not being able to establish or maintain a stable Bluetooth connection) or reduction of the data transmission rate could also result from flaws in your Bluetooth terminal, sometimes in combination with the operating system on terminal side.

8.1 Hardware

Symptoms	Possible cause	Possible solution
The LED indicator is not lit	Faulty power supply	Check the power supply
The LED indicator is not steadily lit	Faulty system settings	Unplug the power supply and plug in again
No network access	Faulty network cable or socket	Check the network connection

Table 32 Troubleshooting: Hardware

8.2 Bluetooth Connection

Symptoms	Possible cause	Possible solution
You cannot "find" the blue2net unit with your Bluetooth terminal	See for possible cause on symptom “The data rate is very low.” in this table below	See for possible solutions on symptom “The data rate is very low.” in this table below
	blue2net Discoverability Mode [1.4] is set to *nondiscoverable*	Set the blue2net discoverability mode [1.4] to *discoverable*
You cannot see a service from blue2net	The maximum number of terminals has already been connected to blue2net	Check the value of 'Max. No. of Terminals Connected' [1.6] and 'Multipoint Mode' [1.3]
	'Connectability Mode' [1.3] is set to *disabled*	Set 'Connectability Mode' [1.3] to *enabled*
You cannot connect to blue2net with your Bluetooth terminal	Some terminals do not support the LAN access profile	blue2net currently supports only the LAN access profile

Symptoms	Possible cause	Possible solution
	You have changed 'Default Access Mode' [1.11] to *disabled*	Set the 'Default Access Mode' [1.11] to *enabled* or put the 'Terminal BT Address' [1.10.2] of your Bluetooth terminal in the 'Terminal Table' [1.10].
	Your Bluetooth terminal is a member of the 'Terminal Table' [1.10]	Use the 'Terminal Bluetooth Passkey' [1.10.3] you have assigned for your terminal in the 'Terminal Table' [1.10].
The data rate is very low.	The radio signal level is low	1. Check the orientation of the blue2net case (see Figure 1). 2. Try to reduce the distance between blue2net and the Bluetooth terminals. 3. Check if you have any absorbing or shielding objects between blue2net and the Bluetooth terminals.
	The radio signal is subject to interference (e.g. microwave oven)	Move the blue2net to another position (see chapter 2.2).

Table 33 Troubleshooting: Bluetooth connection

8.3 LAN/Internet Access

Symptoms	Possible cause	Possible solution
You cannot reach the LAN (e.g. no Internet access possible).	The IP parameters for blue2net [2] are not suitable for your LAN.	Check the IP parameters for blue2net [2]. Ask your system administrator or Internet Service Provider for correct IP parameters for blue2net [2].
You can reach external computers (Internet) via their IP address, but not via their names (e.g. www.siemens.at). (Error Message: page cannot be displayed…)	The DNS IP address configuration is wrong (see chapter 3.6.2 regarding 'Terminal Fixed Servers' [3.5]).	Ask your system administrator or Internet Service Provider for the correct DNS IP address and enter them manually ([3.5.1] and [3.5.2]).

Your Bluetooth terminal is connected to blue2net but cannot be reached from outside (e.g. you cannot provide a Web server on your Bluetooth terminal).	'Terminal IP Address Resolution' [3.1] is set to *masquerading.*	Exclude certain terminals from masquerading by assigning them a fixed IP address in the Terminal Table [1.10]. Then set 'Terminal IP Address Resolution' [3.1] to *masqueradingpool*. All terminals listed in the terminal table [1.10] will be visible from outside.
	'Default Firewall' [2.6.1] is set to *enabled*	That is one of the reasons for using the firewall: being invisible from outside. Carefully consider disabling the firewall.

Table 34 Troubleshooting: LAN access

8.4 Software Update

Symptoms	Possible cause	Possible solution
The image file cannot be stored on blue2net.	You have copied too many files to the blue2net /tmp directory. Memory exceeded.	Reset blue2net (see chapter 3.9.3). It is recommended to copy only blue2net software files (b2n_image) to your blue2net.

Table 35 Troubleshooting: Software update

8.5 Configuration Access

Symptoms	Possible cause	Possible solution
A Bluetooth connection is established to blue2net, but you cannot reach the built-in Web server.	You typed in a wrong IP address for accessing blue2net.	Check the IP address of blue2net (see chapter 2.6).
	You have configured a proxy for PPP connection on your Web browser.	Change the configuration on the Web browser to "no proxy" or exclude the IP address of blue2net.
	You typed http://... instead of http**s**://.... in the location/URL field of the browser.	Please change it to http**s**://....
You are prompted repeatedly for the configuration pwd.	Cookies are not enabled on your Web browser.	Enable cookies on you Web browser.

Table 36 Troubleshooting: Configuration access

9 Firewall

The firewall in blue2net may be established in order to prevent attacks coming from the Ethernet side (e.g. over LAN, cable modem or xDSL connection).

Note: Activating the firewall may cause restrictions with certain applications (e.g. games over the Internet) due to default safety options.

It is assumed that all devices being able to connect via Bluetooth are trustworthy, and no countermeasures are taken against them (except that using SNMP configuration via Bluetooth is not allowed).

If you enable the firewall you will still be able to use the following services:

Service Name	Protocols	Ports
HTTP	tcp / udp	80
HTTP webcaching	tcp / udp	8080
HTTPS	tcp / udp	443
FTP	tcp / udp	20, 21, over 1500
MS MEDIA PLAYER	tcp	1755, 7007
QUICKTIME	tcp	458, 545
REALPLAYER	tcp	1090, 554, 7070
DHCP	tcp / udp	67 (in), 68 (out)
DNS	tcp	53
DNS	udp	53 (only to servers)
POP2/3	tcp / udp	109/110
POP3 SEC	tcp / udp	995
POPPASSD	tcp / udp	106
KPOP	tcp / udp	1109
SMTP	tcp / udp	25
SMTP SEC	tcp / udp	465
IMAP 2	tcp / udp	143
IMAP SEC	tcp / udp	993
TIME	tcp / udp	37

Table 37 Services that can be used while the firewall is enabled

For all these services it is necessary that the transactions be started from inside the firewall (from a device connected via Bluetooth).

When the firewall is enabled the only thing you can do from outside (LAN side) is to configure blue2net (because this is done via https and password protection is used). Updating the software and loading of a specific homepage are not possible via the Ethernet if the firewall is enabled.

On how to enable/disable the firewall see chapters 2.7, 3.5, and 3.5.3.

10 Regulatory Statement

10.1 General

- The Siemens Bluetooth™ Radio Module SieMo S50037 is integrated into this piece of equipment.
- This piece of equipment has to be installed and used in accordance with the instruction manual.
- This piece of equipment is intended to be placed on the market in all States where the Bluetooth™ technology and the used frequency band is released.
- For detailed information regarding type approval of this equipment (e.g. where this equipment is already approved) please contact the authorized local distributor or the manufacturer.

10.2 European Union (EU) and EFTA Member States

Based on the assessed Siemens Bluetooth™ radio module SieMo S50037 inside this equipment complies with the R&TTE directive 1999/5/EC and has been provided with the CE mark accordingly. It conforms to the following specifications/standards:

Applied specifications / standards	Essential Requirement (corresponding article of R&TTE)
EN 60950/ IEC 60950:2000	Safety (Art. 3.1a)
EN 300 328 (ETS 300 328): Part 1, V1.1.1 and Part 2, V1.2.2 (2000-07) EN 301 489-17 (ETS 300 826): V1.1.1 (2000-09)	Electromagnetic Compatibility (Art. 3.1b)
EN 300 328 (ETS 300 328): Part 1, V1.1.1 and Part 2, V1.2.2 (2000-07)	Radio Frequency Spectrum Efficiency (Art. 3.2)

Table 38 Conformity with standards and specifications

Note that the radio frequency band used by this equipment is not harmonized throughout the European Community. According to the R&TTE directive 1999/5/EC is this equipment

a ‘Class 2’ equipment and marked accordingly with the assigned Class Identifier.

Figure 35 CE Conformity Marking

10.3 United States of America (USA)

This equipment complies with part 15 of the Federal Communications Commission (FCC) rules and is labeled in accordance with the FCC rules.

FCC ID: P6L-blue2net

Operation is subject to the following two conditions:

1. This device must not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

Note: Any changes or modifications to this equipment not expressly approved by the manufacturer could void the user's authority to operate this equipment.

11 Bluetooth Compliance

This product is a qualified Bluetooth™ product and compliant with Bluetooth™ specifications version 1.1.

BLUETOOTH is a trademark owned by Bluetooth SIG, Inc., U.S.A, and licensed to Siemens AG.

12 Default Values

[Hier.level]	Parameters & Objects	Factory setting (default value)
[1]	**Bluetooth Parameters**	–
[1.1]	Bluetooth Device Name	–
[1.1.1]	Bluetooth Device Name	blue2net
[1.1.2]	IP Address Suffix Mode	enabled
[1.2]	Bluetooth Device Address	unique value for the Bluetooth device
[1.3]	Multipoint Mode	enabled
[1.4]	Discoverability Mode	discoverable
[1.5]	Connectability Mode	connectable
[1.6]	Max. No. of Terminals Connected	7
[1.7]	Number of Services	– (read-only)
[1.8]	Service Table	–
[1.8.1]	Service Index	– (read-only)
[1.8.2]	Service Name	LAN ACCESS 1
[1.8.3]	Service Description	LAN ACCESS via blue2net
[1.8.4]	Auth. Level	noauth
[1.8.5]	Service Provider	SIEMENS
[1.8.6]	Service URL	http://www.siemens.at/bluetooth
[1.8.7]	Service ID	1
[1.9]	Number of Terminals	– (read-only)
[1.10]	Terminal Table	–
[1.10.1]	Terminal Index	– (read-only)
[1.10.2]	Terminal Bluetooth Address	00:00:00:00:00:00
[1.10.3]	Terminal Bluetooth Passkey	1234
[1.10.4]	Terminal IP Address	0.0.0.0
[1.11]	Default Access Mode	enabled
[1.12]	Default Bluetooth Passkey	1234
[2]	**IP Parameters for blue2net**	–
[2.1]	blue2net IP Address Resolution	dhcp
[2.2]	Fixed blue2net IP Configuration	–
[2.2.1]	Fixed blue2net IP Address	192.168.1.2
[2.2.2]	Fixed blue2net Netmask	255.255.255.0
[2.2.3]	Fixed blue2net Gateway	192.168.1.1
[2.3]	DHCP blue2net IP Objects	–
[2.3.1]	Fallback blue2net IP Address	192.168.1.2
[2.3.2]	Fallback blue2net Netmask	255.255.255.0
[2.3.3]	Fallback blue2net Gateway	192.168.1.1
[2.4]	Time Server IP	0.0.0.0
[2.5]	IP Masquerading	192.168.2.2
[2.6]	Firewall Settings	–
[2.6.1]	Default Firewall	disabled
[2.7]	Tunnel Configuration	–
[2.7.1]	Tunnel Mode	none
[2.7.2]	Tunnel Establishment Control	disabled
[2.7.3]	Authentication Parameters	–
[2.7.3.1]	Tunnel User Name	pppoeuser
[2.7.3.2]	Tunnel User Pasword	pppoepassw
[2.7.4]	PPTP Server IP Address	10.0.0.138

Table 39 Factory settings (default values) (1)

[Hier.level]	Parameters & Objects	Factory setting (default value)
[3]	**IP Parameters for Terminals**	–
[3.1]	Terminal IP Address Resolution	masquerading
[3.2]	Number of Terminal IP Addr. Pool Entries	– (read-only)
[3.3]	Terminal IP Address Pool Table	–
[3.3.1]	Terminal IP Address Index	– (read-only)
[3.3.2]	Terminal IP Address Pool Value	192.168.1.11....17
[3.4]	Terminal Net Mask	255.255.255.0
[3.5]	Terminal Fixed Servers	–
[3.5.1]	Terminal DNS Server 1	192.168.3.11
[3.5.2]	Terminal DNS Server 2	192.168.3.12
[3.5.3]	Terminal WINS Server 1	192.168.3.13
[3.5.4]	Terminal WINS Server 2	192.168.3.14
[3.5.5]	Terminal Domain Name	my.domain.at
[4]	**Current Configuration**	–
[4.1]	MAC Address	fixed unique value for this device
[4.2]	blue2net IP Configuration	–
[4.2.1]	blue2net IP Address	– (read-only)
[4.2.2]	blue2net Netmask	– (read-only)
[4.2.3]	blue2net Gateway	– (read-only)
[4.3]	Terminal Server Configuration	–
[4.3.1]	Terminal DNS Server 1	– (read-only)
[4.3.2]	Terminal DNS Server 2	– (read-only)
[4.3.3]	Terminal WINS Server 1	– (read-only)
[4.3.4]	Terminal WINS Server 2	– (read-only)
[4.3.5]	Terminal Domain Name	– (read-only)
[4.4]	Version Information	–
[4.4.1]	Module Firmware Version	– (shows version)
[4.4.2]	PPCBoot Version	– (shows version)
[4.4.3]	blue2net Software Version	– (shows version)
[4.4.4]	blue2net Hardware Version	– (shows version)
[4.4.5]	SieMo Module Info	– (shows version)
[4.5]	Tunnel Status (PPPoE/PPTP)	–
[4.5.1]	Tunnel Status	tunnel mode none (read-only)
[5]	**Configuration Access**	–
[5.1]	SNMP Access	disabled
[5.2]	Configuration Password	changeme
[5.2.1]	Change of configuration pwd	–
[6]	**Activation Commands**	–
[6.1]	Save Settings Temporarily	– (activation command)
[6.2]	Save Settings Permanently	– (activation command)
[6.3]	Reset blue2net	– (activation command)
[6.4]	Update Software	– (activation command)
[6.5]	Restore Default Settings	– (activation command)
[6.6]	Store Specific Homepage	– (activation command)

Table 40 Factory settings (default values) (2)

To restore default settings use the activation command 'Restore Default Settings' as described in chapter 3.9.5.

13 Abbreviations and Terms

Term	Explanation
Authentication	A security procedure
Authorization	A security procedure where a device is given permission to access a particular service
BT	Bluetooth
CE	Conformity Europe
connectable	A Bluetooth device is connectable if it will respond to paging, so it is possible for another device to connect to it
DHCP	Dynamic Host Configuration Protocol
discoverable	A Bluetooth device is discoverable if it will respond to inquiries of other Bluetooth devices so other devices in the area can discover its presence
DNS	Domain Name Server
DRAM	Dynamic Read and Write Memory
FCC	Federal Communications Commission
FTP	File Transfer Protocol
HTTP	HyperText Transfer Protocol
HTTPS	secure HyperText Transfer Protocol
HW	Hardware
IMAP	Internet Mail Access Protocol
IMAP SEC	Internet Mail Access Protocol secure
IP	Internet Protocol
ISP	Internet Service Provider
KPOP	Post Office Protocol Kerberos
blue2net	LAN Access Point
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Medium Access Control
Passkey	Another name for PIN
PCMCIA	Personal Computer Memory Card Int'l Association, synonym for a standard für PC-Cards, such as Bluetooth cards, modem cards and Fax cards
PDA	Personal Digital Assistant
PIN	Personal Identification Number

Table 41 Abbreviations and terms (1)

Term	Explanation
POP	Post Office Protocol
POP3 SEC	Post Office Protocol 3 secure
POPPASSD	Post Office Protocol with Password
PPCBoot	Power PC Booting
PPP	Point to Point Protocol
PPPoE	Point to Point Protocol over Ethernet
PPTP	Point to Point Tunnel Protocol
PROM	Programmable Read Only Memory
RAM	Read and Write Memory
RAS	Remote Access Service
SDP	Service Discovery Protocol
SIG	Special Interest Group
SMTP	Simple Mail Transfer Protocol
SMTP SEC	Simple Mail Transfer Protocol secure
SNMP	Simple Network Management Protocol
SW	Software
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
UDP	Universal Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
WINS	Windows Internet Naming Service
xDSL	x Digital Subscriber Line (x…depending on the provider)

Table 42 Abbreviations and terms (2)

14 Service / Contact

In the case of malfunctions of your blue2net unit, please contact your local dealer.

For technical information, software updates, and FAQs, please refer to www.siemens.at/bluetooth.

15 Warranty and Product Liability

Siemens AG offers a 12-month warranty to distributors following the date of purchase.

Any configuration action which results in lockout is not subject to warranty. In this case please contact your local dealer.

The device should not be opened under any circumstances, otherwise the warranty and liability shall expire.

Outside the scope of the Product Liability Act, seller shall be liable only if the damage in question is proved to be due to intentional acts or acts of gross negligence, within the limits of statutory provisions. Seller shall not be liable for damage due to acts of ordinary negligence nor for consequential damages or damages for economic losses, loss of savings or interest or damage resulting from third-party claims against buyer. Neither does the scope of product liability extend to medical applications and hospital environments. Siemens shall not be liable for consequential damages resulting from the use of blue2net particularly as regards safety critical applications, applications in healthcare and lifesaving.

Seller shall not be liable for damages in case of non-compliance with instructions for assembly, commissioning and operation (such as are contained in instructions for use) or non-compliance with licensing requirements.

16 Technical Data

Radio Technology	Bluetooth V1.1, power class 2, 2 dBm
Frequency Range	2.402 to 2.480 GHz
Transmission Range	20m
Data rates (maximum)	asymmetric: 723 Kbits/s downlink 57 Kbits/s uplink symmetric: 434 Kbits/s downlink and uplink
Multipoint	yes, master / slave switch; connecting up to 7 simultaneous data users
Bluetooth Profiles	LAN Access Profile Generic Access Profile Serial Port Profile PAN prepared
Receiver Sensitivity	better -80 dBm
Antenna	patch antenna integrated
Bluetooth Module	Siemens SieMo S50037
Bluetooth Stack	Siemens SurfBlue
Processor	Power PC
Memory DRAM / Flash	16 MB / 2 MB
Operating System	Embedded Linux
Ethernet	10 Mbit/s, connector RJ45
Power Supply	4.5 V, 1 A, external supply, connector RJ11
Power Consumption	< 2,5 W
Dimensions	150 x 140 x 32 mm (5.90 x 5.51 x 1.26 inches)
Weight	200 g (7.05 oz)
Operating Conditions	indoor use only
Temperature	0 to +40 °C (+32 to +104 °F)
Configuration	built-in Web server
blue2net IP address assignment	DHCP or predefined (fixed)
Terminal IP address assignment	masquerading or DHCP or predefined (fixed)
Security	configuration: Password and HTTPS Bluetooth passkeys built-in firewall
Software upgrades	Software upgrade is available at http://www.siemens.at/bluetooth
More information	http://www.siemens.at/bluetooth

Table 43 Technical Data

17 Index

A

abbreviations ... 73
access via Bluetooth ... 6
access via Ethernet (LAN) ... 7
activation commands [6] ... 12, 43, 57, 60, 61
Auth. Level ... 21, 48, 49, 50, 51, 54
authentication ... 20
  before configuration ... 11
  Bluetooth passkey requested ... 21
  for security reasons ... 54
  for tunnel connection ... 31
  no authentication used ... 21
  passkey for Bluetooth ... 18
authentication and encryption ... 21

B

blue2net
  assigned gateway ... 38
  assigned IP address ... 38
  assigned netmask ... 38
blue2net IP address
  how to display it ... 19
  fallback ... 27
  fixed ... 26
blue2net IP addresses
  predefined, fixed ... 24
Bluetooth
  accessing the Web server via BT ... 6
  authentication, passkey ... 18
  BT address of blue2net, how to get it ... 6
  BT Device Address ... 17
  BT Device Name ... 16
  BT parameters ... 12
  BT passkey ... 18
  BT values via SDP ... 20
  compliance with BT spec. v 1.1 ... 70
  compliant with LAN access profile ... 6
  connectability ... 17
  connecting to blue2net via Bluetooth ... 6
  device inquiry ... 6, 20
  discoverability ... 17
  discoverable, connectable ... 73
  establishing a Bluetooth connection ... 6
  how to place BT devices ... 3
  important BT parameters, display ... 37
  IP address for terminals ... 33
  IP parameters for terminals ... 32, 33
  need for reestablishing the BT connection ... 45, 46
  no restrictions for BT terminals!!! ... 21
  parameters for blue2net device and terminals ... 16
  passkey ... 6, 23, 48, 76
  preventing lockout from access via BT ... 43, 45
  security features ... 20
  security measures for access ... 22, 23
  selected terminals only ... 22
  specification ... 1
  terminal BT Address ... 23
  terminal not recognizable ... 23
  with older terminals ... 17
Bluetooth Device Name ... 19
  use scenario
    business (controlled access) ... 48
    home use ... 51
    home use (cable modem) ... 50
    hot spot (public) ... 49
Bluetooth passkey ... 48, 76
Bluetooth Passkey ... 23
Bluetooth profiles ... 77
browser settings ... 6

C

configuration over Ethernet ... 5
configuration password ... 42
configuration (xDSL) ... 5
configuration access ... 12
Configuration Password ... 50, 52
configuration password (default) ... 8
conformity
  CE, Conformity Europe ... 73
  CE, standards, BT, specifications ... 68
  declaration ... 81
conformity marking ... 68
connectability mode ... 10, 17, 54, 62
contact ... 75
cookies ... 6, 65

D

default Bluetooth passkey
  use scenario ... 48
Default Bluetooth Passkey ... 51
default settings ... 10
  reset to ... 46
  restore ... 43, 47
  restored after lockout ... 53
default values
  list ... 71
DHCP ... 3, 50, 66, 77
  choosing between 'dhcp' and 'predefined' ... 24
  define the correct IP parameter setting ... 12
  fallback IP address, if service is not available ... 25
  fallback IP if DHCP is not available ... 7
  find out IP assigned by DHCP ... 7
  if service not available ... 54
  IP address resolution ... 10
  meaning ... 73

what if DHCP service is not available....3, 4, 27
when IP address is assigned by DHCP....3
where to find out whether it's available....4
dhcp (setting)
if service not available....54
dhcp (when set to)
retrieved blue2net gateway....38
retrieved blue2net IP address....38
retrieved blue2net netmask....38
retrieved domain name assigned if available....39
retrieved IP address of DNS server....39
retrieved IP address of WINS server....39
directivity of antenna....2
discoverability mode....17
DNS IP addresses
enter manually....35, 63
DSL
configuration....5, 53
make the settings....5, 53
tunnel connection....30, 41

E

encryption....20, 21
Ethernet
accessing the Web server via Ethernet....6
exclude all other terminals from access....22

F

factory settings....10, 12, 71, 72
list....71
reset to....47
restore....43
firewall....25, 28, 66
default firewall....28
disabling/enabling....64
home use scenario....50
troubleshooting....64
firewall settings....50
first installation of blue2net....2
fixed servers for terminals
relevant parameters if not 'dhcp'....35
FTP....59

G

gateway
fallback....27
fixed....26

H

hierarchy of pages/parameters....14
hierarchy of parameters....11

I

installation....2
interference with
medical equipment....iii
microwave ovens....3
IP address
how to display it....19
unique, fixed....22
IP address pool....33
terminals, relevant parameters if not 'dhcp'....34
IP Address pool....22
IP Address Suffix Mode....19

L

LAN Access Point....1
LED, behavior....6
lockout
danger of lockout....17, 18, 21, 23, 24, 33, 42
not subject to warranty....76
preventing lockout....53
lockout scenarios
lockout from access via BT....54
lockout from access via BT and LAN....53
lockout from access via LAN....54

M

MAC address
where to find it....3, 37
masquerading....25
medical equipment
interference with....iii
microwave ovens
interference with....3
multipoint mode....17

N

netmask
fallback....27
fixed....26

O

operation modes
LAN operation....26
xDSL operation....26

P

package contents....2
passkey....6, 18, 21, 22, 23, 31, 48, 50, 53, 54
password for configuration (default)....8
PDA....6
power supply....45, 55, 62
disconnect for reset....46
power supply unit....iii, 2
before connecting....3
PPP....6, 32, 33, 65
preventing lockout....53
procedure for changing parameters....13
product liability....76

R

registered terminals 23
Reset 12, 46
Reset blue2net 46
resetting the device to
  default settings/factory settings 46, 47
Restore Default Settings 47

S

safety precautions iii
Save Settings Permanently 46
Save Settings Temporarily 45
security 9, 12, 48, 50, 51, 53, 54, 77
security level 48
service description 20
service table 20
service URL 21
service/contact 75
services 18, 66
  availability in case of firewall 66
  security 21
SNMP access 42
  enable/disable 12
SNMP configuration 66
software update 47, 55
  progress of the update process 58
specific homepage
  how to load it 59
  how to store it 47, 60
startup 3, 24
Store Specific Homepage 47

T

technical data 77
terminal BT passkey 23
terminal IP address pool 23
terminal IP address pool value 34
terminal IP address resolution 50
  set to 'dhcp' 33
  set to 'masquerading' or 'masqueradingpool' 33
  set to 'predefined' 33
Terminal IP Address Resolution 52
terminals
  registered 23
troubleshooting 62
  Bluetooth connection 63
  configuration access 65
  hardware 62
  LAN access 64
  software update 64
tunnel
  status messages 41
  status of the tunnel connection 41
  Tunnel Mode 30
  tunnel status 41
Tunnel Status 41

U

update software 55
  how to download software updates 55
Update Software 47
use scenarios
  business with controlled access 48
  hot spot (public) 49
  with cable modem (home use) 50
  with xDSL modem (home use) 51
User Name 31
User Password 31

V

version
  firmware 40
  hardware 40
  software 40

W

warranty 76
Web interface 7

X

xDSL
  configuration 5, 30, 53
  make settings 5, 53
  tunnel connection 30, 41

18 CE-Declaration

Declaration of Conformity
in accordance with the Radio and Telecommunications Terminal Equipment Directive 1999/05/EC (R&TTE Directive)

We, **SIEMENS AG**
PSE PRO RCD

of **Erdberger Lände 26**
A-1031 Vienna
Austria

declare that the product

Type Designation: **blue2net Bluetooth™ LAN Access Point, S50037-D*-***
(Siemens Bluetooth™ Module SieMo-S50037 integrated inside)

Equipment class: **Class 2**

Product Description: **Wireless Access Point to Local Area Networks based on the Bluetooth™ Technology.**

complies with all the relevant essential requirements referred to in Article 3 of the Directive 1999/05/EC (R&TTE Directive).

Essential Requirement (Corresponding Article of R&TTE Directive)	Harmonised standards applied / other means of proving conformity
Electromagnetic Compatibility (EMC): (Art. 3(1)(b))	**EN 300 328 (ETS 300 328): Part 1, V1.1.1 and Part 2, V1.2.2 (2000-07)** **EN 301 489-17 (ETS 300 826): V1.1.1 (2000-09)**
Radio Frequency Spectrum Efficiency: (Art. 3(2))	**EN 300 328 (ETS 300 328): Part 1, V1.1.1 and Part 2, V1.2.2 (2000-07)**
Health and Safety: (Art. 3(1)(a))	**EN 60950 : 2000** **SAR:** - Manufacturer Declaration of Conformity - max. output power of radio module < 10 mW.

The conformity assessment procedure referred to in Article 10(4) and detailed in Annex IV of the Directive 1999/05/EC has been followed with the involvement of the following Notified Body:

Address: **CETECOM ICT Services GmbH, Untertürkheimer Strasse 6–10, D-66117 Saarbrücken, Germany.**

Notified Body number: **0682**

The technical documentation relevant to the above equipment will be held at:

SIEMENS AG, PSE PRO RCD
Erdberger Lände 26
A-1031 Vienna, Austria

Point of contact: **Mr. Diyap Canbolant**
Tel.: +43 5 1707 36313, Fax: +43 5 1707 57679, E-Mail: diyap.canbolant@siemens.com

Head of Development
Günther Hraby
Vienna, 18.3.

Head of Quality Assurance
Herbert Haunschmid
Vienna, 15.3.02

Figure 36 Declaration of Conformity

Figure 37 Dimension diagram